# DIGITAL NOTES
# ON
# DIGITAL FORENSICS

## B.TECH III YEAR - I SEM
## (2022-23)


## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

**MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY**
**(Autonomous Institution – UGC, Govt. of India)**
(Affiliated to JNTUH, Hyderabad, Approved by AICTE - Accredited by NBA & NAAC – 'A' Grade - ISO 9001:2015 Certified)
Maisammaguda, Dhulapally (Post Via. Hakimpet), Secunderabad – 500100, Telangana State, INDIA.

# MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY

## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

## (R20A0514) DIGITAL FORENSICS

**COURSE OBJECTIVES:**

1. This *course* will cover the fundamentals of *digital forensics.*
2. Provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
3. Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
4. Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools E-evidence collection
5. It provides preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics.

**UNIT – I:**

Digital Forensics Science: Forensics science, computer forensics, and digital forensics. Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber-criminalistics area, challenges faced by digital forensics.

**UNIT – II:**

Cyber Crime Scene Analysis: Identifying digital evidence, collecting evidence in private-sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene, seizing digital evidence at the scene.

**UNIT – III:**

Evidence Management & Presentation: Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Types of Evidence, Define who should be notified of a crime, parts of gathering evidence.

**UNIT – IV:**

Computer Forensics: Preparing a computer case investigation, Procedures for corporate hi-tech investigations, conducting an investigation, Complete and critiquing the case.

Network Forensics: Overview of network forensics, open-source security tools for network forensic analysis.

**UNIT – V:**

Mobile Forensics: mobile forensics techniques, mobile forensics tools, recent trends in mobile forensic technique and methods to search and seizure electronic evidence. Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008.

**TEXT BOOKS:**

1. B. Nelson, A. Phillips, and C. Steuart, Guide to Computer Forensics and Investigations, 4th Edition, Course Technology, 2010

**REFERENCE BOOKS:**

1. John Sammons, The Basics of Digital Forensics, 2nd Edition, Elsevier, 2014
2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, Laxmi Publications, 2005.

**COURSE OUTCOMES:**

1. Understand relevant legislation and codes of ethics.
2. Investigate computer forensics and digital detective and various processes, policies and procedures data acquisition and validation, e-discovery tools.
3. Analyze E-discovery, guidelines and standards, E-evidence, tools and environment.
4. Apply the underlying principles of Email, web and network forensics to handle real life problems
5. Use IT Acts and apply mobile forensics techniques

# UNIT -1
# DIGITAL FORENSIC

## FORENSIC SCIENCE :

### Definition

Forensic science involves the application of the natural, physical, and social sciences to matters of law.

Forensic science refers to the application of natural, physical, and social sciences to matters of the law. Most forensic scientists hold that investigation begins at the scene, regardless of their associated field. The proper investigation, collection, and preservation of evidence are essential for fact-finding and for ensuring proper evaluation and interpretation of the evidence, whether the evidence is bloodstains, human remains, hard drives, ledgers, and files or medical records. Scene investigations are concerned with the documentation, preservation, and evaluation of a location in which a criminal act may have occurred and any associated evidence within the location for the purpose of reconstructing events using the scientific method. The proper documentation of a scene and the subsequent collection, packaging, and storage of evidence are paramount. Evidence must be collected in such a manner to maintain its integrity and prevent loss, contamination, or deleterious change. Maintenance of the chain of custody of the evidence from the scene to the laboratory or a storage facility is critical. A chain of custody refers to the process whereby investigators preserve evidence throughout the life of a case. It includes information about: who collected the evidence, the manner in which the evidence was collected, and all individuals who took possession of the evidence after its collection and the date and time which such possession took place.

Significant attention has been brought to the joint scientific and investigative nature of scene investigations. Proper crime scene investigation requires more than experience; it mandates analytical and creative thinking as well as the correct application of science and the scientific method. There is a growing movement toward a shift from solely experiential-based investigations to investigations that include scientific methodology and thinking. One critic of the experience based approach lists the following pitfalls of limiting scene investigations to lay individuals and law enforcement personnel: lack of scientific supervision and oversight, lack of understanding of the scientific tools employed and technologies being used at the scene, and an overall lack of understanding of the application of the scientific method to develop hypotheses supported by the evidence (Schaler 2012). Another criticism is that some investigators (as well as attorneys) will draw conclusions and then obtain (or present) evidence to support their version of events while ignoring other types of evidence that do not support their version or seem to contradict their version

(i.e., confirmation bias). Many advocates of the scientific-based approach believe that having scientists at the scene will minimize bias and allow for more objective interpretations and reconstructions of the events under investigation.

**HISTORY OF FORENSIC**

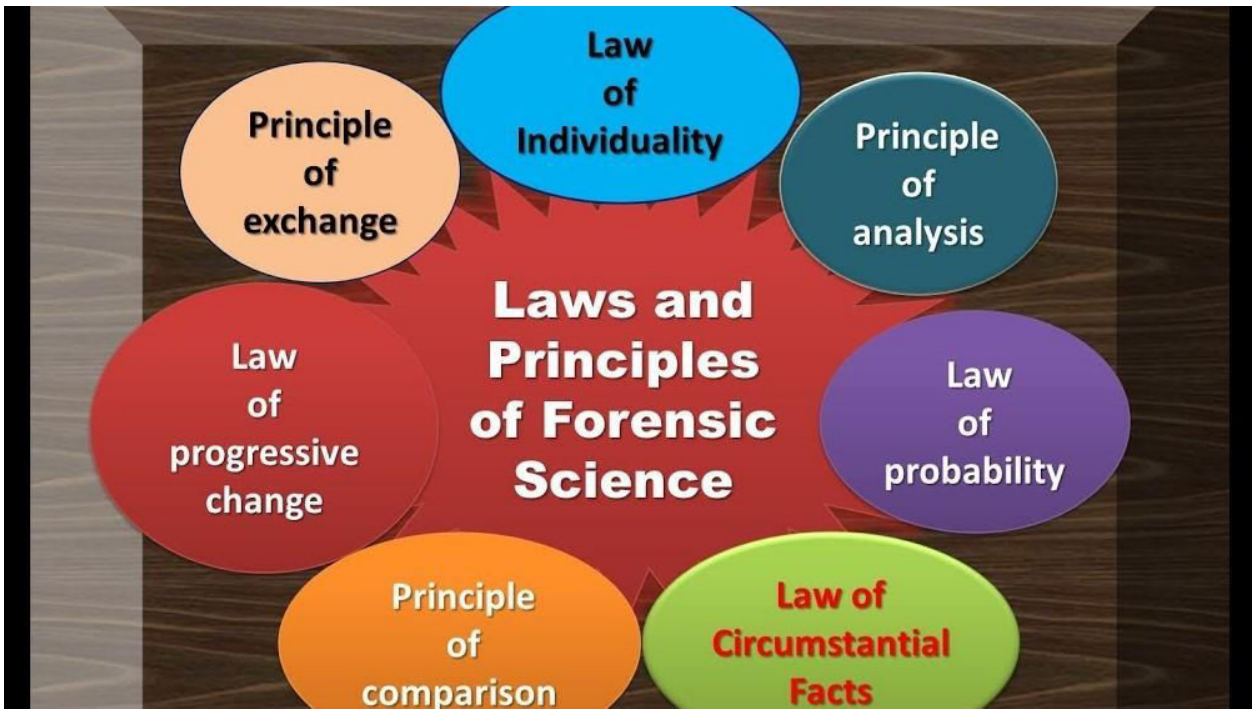
| Date | Event |
|---|---|
| 44 BC | **Death of an emperor**<br><br>Julius Caesar is assassinated. Following this event, a physician performed an autopsy, and determined that of the 23 wounds found on the body, only one was fatal. |
| 400 | **Who determines cause of death(400s)**<br><br>Germanic and Slavic societies made law that medical experts must be the ones to determine cause of death in crimes. |
| 600 | **Use of fingerprints for the first time (600s)**<br><br>Fingerprints first used to determine identity. Arabic merchants would take a debtor's fingerprint and attach it to the bill. |
| 1248 | **First forensic science book**<br><br>First forensic science manual published by the Chinese. This was the first known record of medical knowledge being used to solve criminal cases. |
| 1600 | **Reporting cases (1600s)**<br><br>First pathology reports published. |
| 1784 | **Physical evidence used in criminal case**<br><br>First recorded instance of physical matching of evidence leading to a murder conviction (John Toms, England). Evidence was a torn edge of newspaper in a pistol that matched newspaper in his pocket. |
| 1806 | **Investigating poisoning**<br><br>German chemist Valentin Ross developed a method of detecting arsenic in a victim's stomach, thus advancing the investigation of poison deaths. |
| 1816 | **More physical evidence discovered to work in forensics**<br><br>Clothing and shoes of a farm laborer were examined and found to match evidence of a nearby murder scene, where a young woman was found drowned in a shallow pool. |
| 1836 | **Chemical testing utilized** |

| | |
|---|---|
| | James Marsh, an English chemist, uses chemical processes to determine arsenic as the cause of death in a murder trial. |
| 1854 | **First uses of photos in identification (1854-59 )**<br><br>San Francisco uses photography for criminal identification, the first city in the US to do so. |
| 1880 | **Fingerprints found to be unique**<br><br>Henry Faulds and William James Herschel publish a paper describing the uniqueness of fingerprints. Francis Galton, a scientist, adapted their findings for the court. Galton's system identified the following patterns: plain arch, tented arch, simple loop, central pocket loop, double loop, lateral pocket loop, plain whorl, and accidental. |
| 1887 | **Sherlock Holmes and the coroner**<br><br>Coroner's act established that coroners' were to determine the causes of sudden, violent, and unnatural deaths. Arthur Conan Doyle also publishes the first Sherlock Holmes story. |
| 1892 | **Fingerprint ID used in crime**<br><br>Juan Vucetich, an Argentinean police officer, is the first to use fingerprints as evidence in a murder investigation. He created a system of fingerprint identification, which he termed dactyloscopy. |
| 1888 | **Criminal features reduced to numerical measurements**<br><br>Anthropometry, a system using various measurements of physical features and bones, used throughout the US and Europe. Using the system, a criminal's information could be reduced to a set of numbers. |
| 1901 | **Investigations into blood markers**<br><br>Human blood grouping, ABO, discovered by Karl Landsteiner and adapted for use on bloodstains by Dieter Max Richter. |
| 1901 | **Fingerprint ID more common**<br><br>Galton-Henry system of fingerprint identification officially used by Scotland Yard, and is the most widely used fingerprinting method to date. |
| 1903 | **First fingerprint prisoner ID used**<br><br>NY state prison system implemented fingerprint identification. |
| 1909 | **Learning about forensics**<br><br>First school of forensic science founded by Rodolphe Archibald Reiss, in Switzerland. |

| | |
|---|---|
| 1910 | **Hair now used in forensics**<br><br>Victor Balthazard and Marcelle Lambert publish first study on hair, including microscopic studies from most animals. First legal case ever involving hair also took place following this study. |
| 1912 | **Guns are unique**<br><br>Victor Balthazard realizes that tools used to make gun barrels never leave the same markings, and individual gun barrels leave identifying grooves on each bullet fired through it. He developed several methods of matching bullets to guns via photography. |
| 1923 | **Crime labs built**<br><br>First police crime lab established in Los Angeles. |
| 1930 | **Lie detection**<br><br>Prototype polygraph, which was invented by John Larson in 1921, developed for use in police stations. |
| 1932 | **Crime experts build lab**<br><br>FBI establishes its own crime laboratory, now one of the foremost crime labs in the world. This same year, a chair of legal medicine at Harvard was established. |
| 1960 | **Voice recording, used as evidence (1960s)**<br><br>A sound spectrograph discovered to be able to record voices. Voiceprints began to be used in investigations and as court evidence from recordings of phones, answering machines, or tape recorders. |
| 1967 | **First national crime system**<br><br>FBI established the National Crime Information Center, a computerized national filing system on wanted people, stolen vehicles, weapons, etc. |
| 1974 | **Advances in residue detection**<br><br>Technology developed at Aerospace Corporation in the US to detect gunshot residue, which can link a suspect to a crime scene, and can show how close that suspect was to the gun. |
| 1975 | **Advanced manual fingerprints**<br><br>First fingerprint reader installed at the FBI |
| 1979 | **Auto fingerprint system first used**<br><br>Royal Canadian Mounted Police implement first automatic fingerprint identification |

| | |
|---|---|
| | system. |
| 1984 | **DNA technique for unique ID**<br><br>DNA fingerprinting techniques developed by Sir Alec Jeffreys. |
| 1983 | **Advances in DNA lead to conviction (1983-86)**<br><br>DNA fingerprinting led to conviction of Colin Pitchfork in the murder of two teenage girls. This evidence cleared the main suspect in the case, who likely would have been convicted without it. |
| 1987 | **DNA catches the criminal**<br><br>Tommy Lee Andrews convicted of a series of sexual assaults, using DNA profiling. |
| 1996 | **DNA evidence certified**<br><br>National Academy of Sciences announces DNA evidence is reliable. |
| 1999 | **Faster fingerprint IDs**<br><br>FBI establishes the integrated automated fingerprint identification system, cutting down fingerprint inquiry response from two weeks to two hours. |
| 2001 | **Faster DNA IDs**<br><br>Technology speeds up DNA profiling time, from 6-8 weeks to between 1-2 days. |
| 2007 | **Footwear detection system**<br><br>Britain's Forensic Science Service develops online footwear coding and detection system. This helps police to identify footwear marks quickly. |
| 2008 | **Detection after cleaning**<br><br>A way for scientists to visualize fingerprints even after the print has been removed is developed, relating to how fingerprints can corrode metal surfaces. |
| 2011 | **Facial sketches matched to photos**<br><br>Michigan state university develops software that automatically matches hand-drawn facial sketches to mug shots stored in databases. |
| 2011 | **4 second dental match**<br><br>Japanese researchers develop a dental x-ray matching system. This system can automatically match dental x-rays in a database, and makes a positive match in less than 4 seconds. |

## LAWS AND PRINCIPLES OF FORENSIC SCIENCE




***Laws and Principles of Forensic Science***

Forensic Science is the scientific discipline which is engaged to the recognition, identification, individualization and evaluation of physical evidence by using the laws and principles of natural science for the purpose of administration to terminate doubtful questions in the court of law.

The term "forensics" taken from latin word "forensis" which mean 'the forum'. Forensic scientist also play an active role in civil proceedings (such as violate of agreement and negligence) and in regulatory issues. The principles of forensic science have a straight impact on criminal proceedings.

**Laws and Principles of Forensic Science -**

**Law of Individuality**

**Law of Progressive change**

**Principle of Comparison**

**Principle of Analysis**

**Principle of Exchange (Locard's principle of Exchange)**

**Law of Probability**

**Law of Circumstantial facts.**

**i**) ***Law of Individuality*** -

This law states that, "Every object whether natural or man-made has a distinctive quality or characteristic in it which is not duplicated in any other object," in other words, no two things in this universe are alike. Most common example is the human fingerprints; they are unique, permanent and prove individuality of a person. Even the twins did not have the same fingerprints.

Consider grains of sand, salt, seeds or man-made objects such as currency notes, laptop, typewriter, etc. they may look similar but a unique characteristic is always present between them.

This principle considered as the most basic elementary unit of Forensic Science. Fingerprints, footprints, tool marks, obtained from the crime scene are studied and analyzed on the principle of individuality.

2) ***Law of Progressive Change***

This principle emphasizes that, "Everything changes with the passage of time and nothing remains constant. " The changing frequency varies from sample to sample and on different objects.

The crime scene must be secured in time otherwise a change in weather (rain, heat, wind), presence of animals/humans, etc. affects the crime scene. For example, a road accident on a busy highway may lose all essential evidence if not properly secured on time.

A bullet fragments may grow rust, firearm barrels loosen, shoes suffer wear and tear marks, wooden objects may suffer due to presence of termite, etc. Longer the delay, greater the changes.

When samples are not much durable, several complications occur in an investigation as the process of identification is affected due to the variations in the main features of identification. Without an appropriate preservative, tissue samples start degrading immediately and they need immediate

analysis.

The criminals undergo progressive changes with time. If he is not apprehended in time he becomes unrecognizable except his fingerprints or other characteristics of permanent nature.

3) ***Locard's principle of Exchange (Law of exchange)***

This principle was stated by French scientist -Edmond Locard (a pioneer in criminology and forensic science). Law of exchange states that, "As soon as two things come in connection with each other, they mutually interchange the traces between them."

Whenever criminal or his weapon/instrument made connection with the victim or the things surrounding him he left some traces at crime scene and also picked up the traces from the area or person he has been in contacted with (mutual exchange of matter). These traces are very helpful for investigation purposes as these traces are identified by the expert and linked to its original source resulted in the decisive linkage of the criminal with the crime scene and the victim. This law forms the basis of scientific crime investigation.

This principle is validated in all cases where there is a contact such as fingerprints, tyre marks, bullet residues, foot marks, hair sample, skin, muscles, bodily fluids, blood, pieces of clothing etc. DNA analysis is a straight application of this principle, where any such items are under analysis which was believed to be held by the perpetrator.

Basic requirement of this law is the correct location of the physical evidence -

i) What are the areas and things with which the perpetrator or tool actually came in contact during the crime?

ii) Investigating officer should establish the correct points of contact, its lead the investigation in correct direction.

4) ***Principle of Comparison*** – For laboratory Investigation this law is very important. The law state that "Only the likes can be compared". It highlights the requirement of providing like samples and specimens for evaluation with the questioned items'.

For example, if the murder is done by a firearm weapon then it is useless to send a knife for comparison.

So, the important condition of this principle is to supply specimen/samples of like nature for proper assessment with the questioned sample discovered from the crime scene.

5) ***Principle of Analysis***

This principle states that, "The quality of any analysis would be better by collection of correct sample and its correct preservation in the prescribed manner". This leads to better result and avoid tampering, contamination and destruction of a sample.

If you collect a hard disk in a paper bag, it can be damaged when it falls within the range of a strong electromagnetic field resulted in poor results. Hence, always appropriate and effective collection and packaging techniques must be used.

6) ***Law of Probability***

This law states that, "All identifications (definite or indefinite), made consciously or unconsciously on the basis of probability."

The perpetrator blood group is also the blood group of various people is high, but the probability of the same occurring in the case is low.

A woman with a tattoo bear on its right hand and an old injury mark on head is reported missing, an unknown woman is found murdered with these characteristics then the probability for cops that the unknown corpse is of that missing woman is high. The probability that the dead body is of another woman will be 1 in millions.

7) ***Law of Circumstantial facts***

According to this law, “Facts cannot be wrong, they cannot lie not wholly absent but men can and do.” This law emphasizes the significance of circumstantial facts and supports that a statement given by a human may or may not be accurate. In an investigation identified and discovered facts are more accurate and reliable than any eyewitness.

***Conclusion***

Forensic science by these principles is used for recognition, identification; individualization of pieces of evidence collected from the scene of crime and guides the criminal proceedings from the discovery of a crime to the conviction of the accused, helping the process of investigation.

**COMPUTER FORENSIC**

WHAT IS COMPUTER FORENSICS?

Computer forensics is the process of methodically examining computer media (hard¬ disks, diskettes, tapes, etc.) for evidence. In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence. Computer forensics also referred to as computer forensic analysis, electronic discovery,¬ electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination. Computer evidence can be useful in criminal cases, civil disputes, and human resources/¬ employment proceedings.

1.2 USE OF COMPUTER FORENSICS IN LAW ENFORCEMENT

Computer forensics assists in Law Enforcement. This can include:

**Recovering deleted files** such as documents, graphics, and photos.¬

**Searching unallocated space** on the hard drive, places where an abundance of data often¬ resides.

**Tracing artifacts**, those tidbits of data left behind by the operating system. Our expert know how to find these artifacts and, more importantly, they know how to evaluate the value of the information they find.

**Processing hidden files** — files that are not visible or accessible to the user that contain past usage information. Often, this process requires reconstructing and analyzing the date codes for each file and determining when each file was created, last modified, last accessed and when deleted.

**Running a string-search** for e-mail, when no e-mail client is obvious.

**COMPUTER FORENSICS ASSISTANCE TO HUMAN RESOURCES / EMPLOYMENT PROCEEDINGS**

Computers can contain evidence in many types of human resources proceedings, including sexual harassment suits, allegations of discrimination, and wrongful termination claims. Evidence can be found in electronic mail systems, on network servers, and on individual employee's computers.

**EMPLOYER SAFEGUARD PROGRAM**

Employers must safeguard critical business information. An unfortunate concern today is the possibility that data could be damaged, destroyed, or misappropriated by a discontented individual. Before an individual is informed of their termination, a computer forensic specialist should come on-site and create an exact duplicate of the data on the individual's computer. In this way, should the employee choose to do anything to that data before leaving, the employer is protected. Damaged or deleted data can be re-placed, and evidence can be recovered to show what occurred. This method can also be used to bolster an employer's case by showing the removal of proprietary information or to protect the employer from false charges made by the employee. You should be equipped to find and interpret the clues that have been left behind. This includes situations where files have been deleted, disks have been reformatted, or other steps have been taken to conceal or destroy the evidence. For example, did you know?

What Web sites have been visited?

What files have been downloaded?

When files were last accessed?

Of attempts to conceal or destroy evidence?

Of attempts to fabricate evidence?

That the electronic copy of a document can contain text that was removed from the final printed version?

That some fax machines can contain exact duplicates of the last several hundred pages received?

That faxes sent or received via computer may remain on the computer indefinitely?

That email is rapidly becoming the communications medium of choice for businesses?

That people tend to write things in email that they would never consider writing in a memorandum or letter?

That email has been used successfully in criminal cases as well as in civil litigation?

That email is often backed up on tapes that are generally kept for months or years?

That many people keep their financial records, including investments, on computers?

**COMPUTER FORENSICS SERVICES**

Computer forensics professionals should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to your case. For example, they should be able to perform the following services:

1. **DATA SEIZURE**

Following federal guidelines, computer forensics experts should act as the⎫ representative, using their knowledge of data storage technologies to track down evidence.

The experts should also be able to assist officials during the equipment seizure process.

2. **DATA DUPLICATION/PRESERVATION**

When one party must seize data from another, two concerns must be addressed; the data must not be altered in any way the seizure must not put an undue burden on the responding party

The computer forensics experts should acknowledge both of these concerns by making an exact duplicate of the needed data. ‘

When experts works on the duplicate data, the integrity of the original is maintained.

3. **RECOVERY**

Using proprietary tools, your computer forensics experts should be able to safely recover and analyze otherwise inaccessible evidence.

The ability to recover lost evidence is made possible by the expert’s advanced⎫ understanding of storage technologies

**4. DOCUMENT SEARCHES**

Computer forensics experts should also be able to search over 200,000 electronic documents in

seconds rather than hours.

The speed and efficiency of these searches make the discovery process less complicated and less intrusive to all parties involved.

**5. MEDIA CONVERSION**

Computer forensics experts should extract the relevant data from old and un-readable devices, convert it into readable formats, and place it onto new storage media for analysis.

**6. EXPERT WITNESS SERVICES**

Computer forensics experts should be able to explain complex technical processes in an easy-to-understand fashion. This should help judges and juries comprehend how computer evidence is found, what it consists of, and how it is relevant to a specific situation.

**7. COMPUTER EVIDENCE SERVICE OPTIONS**

Computer forensics experts should offer various levels of service, each designed to suit your individual investigative needs. For example, they should be able to offer the following services:

**Standard service**: Computer forensics experts should be able to work on your case during nor-mal business hours until your critical electronic evidence is found.

**On-site service:** Computer forensics experts should be able to travel to your location to per-form complete computer evidence services. While on-site, the experts should quickly be able to produce exact duplicates of the data storage media in question.

**Emergency service:** Your computer forensics experts should be able to give your case the highest priority in their laboratories. They should be able to work on it without interruption until your evidence objectives are met.

**Priority service**: Dedicated computer forensics experts should be able to work on your case during normal business hours (8:00 A.M. to 5:00 P.M., Monday through Friday) until the evidence is found. Priority service typically cuts your turnaround time in half.

**Weekend service:** Computer forensics experts should be able to work from 8:00 A.M. to 5:00 P.M., Saturday and Sunday, to locate the needed electronic evidence and will continue 14 Computer Forensics, Second Edition working on your case until your evidence objectives are met.

**8. OTHER MISCELLANEOUS SERVICES**

Computer forensics experts should also be able to provide extended services. These services

include:

Analysis of computers and data in criminal investigations

On-site seizure of computer data in criminal investigations

Analysis of computers and data in civil litigation.

On-site seizure of computer data in civil litigation

Analysis of company computers to determine employee activity

Assistance in preparing electronic discovery requests

Reporting in a comprehensive and readily understandable manner

Court-recognized computer expert witness testimony

Computer forensics on both PC and Mac platforms

Fast turnaround time.

**BENEFITS OF PROFESSIONAL FORENSIC METHODOLOGY**

A knowledgeable computer forensics professional should ensure that a subject computer system is carefully handled to ensure that:

1. No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer.
2. No possible computer virus is introduced to a subject computer during the analysis process.
3. Extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage.
4. A continuing chain of custody is established and maintained.
5. Business operations are affected for a limited amount of time, if at all.
6. Any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged.

**DIGITAL FORENSIC**

Digital forensics or digital forensic science is a branch of cybersecurity focused on the recovery and investigation of material found in digital devices and cybercrimes. Digital forensics was originally used as a synonym for computer forensics but has expanded to cover the investigation of all devices that store digital data.

As society increases reliance on computer systems and cloud computing, digital forensics becomes a crucial aspect of law enforcement agencies and businesses.

Digital forensics is concerned with the identification, preservation, examination and analysis of digital evidence, using scientifically accepted and validated processes, to be used in and outside of a court of law.

While its root stretch back to the personal computing revolution in the late 1970s, digital forensics begun to take shape in the 1990s and it wasn't until the early 21st century that countries like the United States begun rolling out nation-wide policies.

Today, the technical aspect of an investigation is divided into five branches that encompass the seizure, forensic imaging and analysis of digital media.

**What is the Purpose of Digital Forensics?**

The most common use of digital forensics is to support or refute a hypothesis in a criminal or civil court:

- **Criminal cases:** Involve the alleged breaking of laws and law enforcement agencies and their digital forensic examiners.
- **Civil cases:** Involve the protection of rights and property of individuals or contractual disputes between commercial entities where a form of digital forensics called electronic discovery (eDiscovery) may be involved.

Digital forensics experts are also hired by the private sector as part of cybersecurity and information security teams to identify the cause of data breaches, data leaks, cyber attacks and other cyber threats. Digital forensic analysis may also be part of incident response to help recover or identify any sensitive data or personally identifiable information (PII) that was lost or stolen in a cybercrime.

**What is Digital Forensics Used For?**

Digital forensics is used in both criminal and private investigations.

Traditionally, it is associated with criminal law where evidence is collected to support or negate a hypothesis before the court. Collected evidence may be used as part of intelligence gathering or to locate, identify or halt other crimes. As a result, data gathered may be held to a less strict standard than traditional forensics.

In civil cases, digital forensics may help with electronic discovery (eDiscovery). A common example is following unauthorized network intrusion. A forensics examiner will attempt to understand the nature and extent of the attack, as well as try to identify the attacker.

As encryption becomes more widespread, forensic investigation becomes harder, due to the limited laws compelling individuals to disclose encryption keys.

**What is the Digital Forensics Investigation Process?**

There are a number of process models for digital forensics, which define how forensic examiners should gather, process and analyze data. That said, digital forensics investigations commonly consist of four stages:

1. **Seizure:** Prior to actual examination digital media is seized. In criminal cases, this will be performed by law enforcement personnel to preserve the chain of custody.
2. **Acquisition:** Once exhibits are seized, a forensic duplicate of the data is created. Once created using a hard drive duplicator or software imaging tool then the original drive is returned to a secure storage to prevent tampering. The acquired image is verified with SHA-1 or MD5 hash functions and will be verified again throughout analysis to verify the evidence is still in its original state.
3. **Analysis:** After acquisition, files are analyzed to identify evidence to support or contradict a hypothesis. The forensic analyst usually recovers evidence material using a number of methods (and tools), often beginning with the recovery of deleted information. The type of data analyzed varies but will generally include email, chat logs, images, internet history and documents. The data can be recovered from accessible disk space, deleted space or from the operating system cache.

4. **Reporting:** Once the investigation is complete, the information is collated into a report that is accessible to non-technical individuals. It may include audit information or other meta-documentation.

**What is the History of Digital Forensics?**

Before the 1970s, cybercrimes were dealt with existing laws.

The first cyber crimes were recognized in the 1978 Florida Computer Crimes Act. The 1978 Florida Computer Crimes Act included legislation against the unauthorized modification or deletion of data.

As the range of computer crimes increased, state laws were passed to deal with copyright, privacy, harassment and child pornography.

In the 1980s, federal laws began to incorporate computer offences. Canada was the first country to pass legislation in 1983, with the United States following in 1986, Australia in 1989 and Britain's Computer Misuse Act in 1990.

1980s-1990s

The growth in cyber crime in the 1980s and 1990s force law enforcement agencies to establish specialized groups at a national level to handle technical investigations.

In 1984, the FBI launched a *Computer Analysis and Response Team* and in 1985, the British Metropolitan Police fraud squat launched a computer crime department.

One of the first practical examples of digital forensics was Cliff Stoll's pursuit of Markus Hess in 1986. Hess is best known for hacking networks of military and industrial computers based in the United States, Europe and East Asia. He then sold the information to the Soviet KGB for $54,000. Stoll was not a digital forensic expert but used computer and network forensic techniques to identify Hess.

In the 1990s there was a high demand for digital forensic resources and the strain on the central units led to regional or even local groups to handle the load. This led to the science of digital forensic maturing from an ad-hoc set of tools and techniques to a more developed discipline.

By 1992, "computer forensics" was used in academic literature in a paper by Collier and Spaul that attempted to justify digital forensics as a new discipline. That said, digital forensic remained a haphazard discipline due to a lack of standardization and training.

By the late 1990s, mobile phones were more widely available and advancing beyond simple communication devices. Despite this, digital analysis of cell phones has lagged behind traditional computer media due to the proprietary nature of devices.

**2000s**

Since 2000, various bodies and agencies have published guidelines for digital forensics in response to the need for standardization. Standardization became more important as law enforcement agencies moved away from central units to regional or even local units to try keep up with demand.

For example, the British National Hi-Tech Crime Unit was set up in 2001 to provide national infrastructure for computer crime, with personnel located centrally in London and with the various regional police forces.

In 2002, the Scientific Working Group on Digital Evidence (SWGDE) produced *Best practices for Computer Forensics.*

A European lead international treaty, the Convention of Cybercrime came into force in 2004 with the aim of reconciling national computer crime laws, investigation techniques and international cooperation. The treaty has been signed by 43 nations (including the United States, Canada, Japan, South Africa, United Kingdom and other European nations) and ratified by 16.

In 2005, an ISO standard for digital forensics was released in ISO 17025, *General requirements for the competence of testing and calibration laboratories.*

This was when digital forensics training began to receive more attention with commercial companies beginning to offer certified forensic training programs.

The field of digital forensics still faces issues. A 2009 paper, *Digital Forensic Research: The Good, the Bad and the Unaddressed* identified a bias towards Windows operating systems in digital forensics research despite widespread use of smartphones, unix and linux based operating systems.

In 2010, Simson Garfinkel pointed out the increasing size of digital media, widespread encryption, growing variety of operating systems and file formats, more individuals owning multiple devices and legal limitations as key risks to digital forensics investigations. The paper also identified training issues and the high cost of entering the field as key issues. Other key issues include the shift toward Internet crime, cyber warfare and cyber terrorism.

**What Tools Do Digital Forensic Examiners Use?**

In the 1980s, very few digital forensic tools existed forcing forensic investigators to perform live analysis, using existing sysadmin tools to extract evidence. This carried the risk of modifying data on the disk which led to claims of evidence tampering.

The need for software to address this problem was first recognized in 1989 at the Federal Law Enforcement Training Center and resulted in the creation of IMDUMP and SafeBack. DIBS, a hardware and software solution, was released commercially in 1991.

These tools create an exact copy of a piece of digital media to work on while leaving the original disk intact for verification.

By the end of the 1990s, the demand for digital evidence meant more advanced tools such as EnCase and FTK were developed, allowing analysts to examine copies of media without live forensics.

There is now a trend towards live memory forensics using tools such as WindowsSCOPE and tools for mobile devices.

Today, there are single-purpose open-source tools like Wireshark, a packet sniffer, and HashKeeper, a tool to speed up examination of database files. As well as commercial platforms with multiple functions and reporting capabilities like Encase or CAINE, an entire Linux distribution designed for forensics programs.

In general tools can be broken down into the following ten categories:

1. Disk and data capture tools
2. File viewers

3. File analysis tools
4. Registry analysis tools
5. Internet analysis tools
6. Email analysis tools
7. Mobile devices analysis tools
8. Mac OS analysis tools
9. Network forensics tools
10. Database forensics tools

**What are the Legal Considerations of Digital Forensics?**

The examination of digital media is covered by national and international legislation. For civil investigations, laws may restrict what can be examined. Restrictions against network monitoring or reading personal communications are common.

Likewise, criminal investigations may be restricted by national laws that dictate how much information can be seized. As an example, seizure of evidence by law enforcement is governed by the PACE act in the United Kingdom. The 1990 computer misuse act legislates against unauthorized access to computer material which makes it hard for civil investigators in the UK.

One of the common considerations which is largely undecided is an individual's right to privacy. The US Electronic Communications Privacy Act places limitations on the ability for law enforcement and civil investigators to intercept and access evidence.

The act makes a distinction between stored communication (e.g. email archives) and transmitted communication (e.g. VOIP). Transmitted communication is considered more of a privacy invasion and is harder to obtain a warrant for.

Digital evidence falls into the same legal guidelines as other evidence.

In general, laws dealing with digital evidence are concerned with:

- **Integrity:** Ensuring the act of seizing and acquiring digital media does not modify the evidence (either the original or the copy).
- **Authenticity:** The ability to confirm the integrity of information. The chain of custody from crime scene through analysis and ultimately to the court, in the form of an audit trail, is an important part of establishing the authenticity of evidence.

Each of the branches of digital forensics have their own guidelines on how to conduct investigations and handle data.

**What are the Different Branches of Digital Forensics?**

Digital forensics is no longer synonymous with computer forensics. It is increasingly concerned with data from other digital devices such as tablets, smart phones, flash drives and even cloud computing.

In general, we can break digital forensics into five branches:

1. Computer forensics
2. Mobile device forensics
3. Network forensics
4. Forensic data analysis
5. Database forensics

**What is Computer Forensics?**

Computer forensics or computer forensic science is a branch of digital forensics concerned with evidence found in computers and digital storage media. The goal of computer forensics is to examine digital data with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

It is used in both computer crime and civil proceedings. The discipline has similar techniques and principles to data recovery, with additional guidelines and practices designed to create a legal audit trail with a clear chain of custody.

Evidence from computer forensics investigations is subjected to the same guidelines and practices of other digital evidence.

**What is Mobile Device Forensics?**

Mobile device forensics is a branch of digital forensics focused on the recovery of digital evidence from mobile devices using forensically sound methods.

While the phrase mobile device generally refers to mobile phones, it can relate to any device that has internal memory and communication ability including PDA devices, GPS devices and tablets.

While the use of mobile phones in crime has been widely recognized for years, the forensic study of mobile phones is a new field, beginning in the late 1990s.

The growing need for mobile device forensics is driven by:

- Use of mobile phones to store and transmit personal and corporate information
- Use of mobile phones in online transactions

That said, mobile device forensics is particularly challenging due to:

- Evidential and technical challenges such as cell site analysis which makes it possible to determine roughly the cell site zone from which a call was made or received but not a specific location such as an address
- Changes in mobile phone form factors, operating systems, data storage, services, peripherals and even pin connectors and cables
- Storage capacity growth
- Their proprietary nature
- Hibernation behavior where processes are suspended when the device is off or idle

As a result of these challenges, many tools exist to extract evidence from mobile devices. But no one tool or method can acquire all evidence from all devices. This has forced forensic examiners, especially those who wish to be expert witnesses, to undergo extensive training to understand how each tool and method acquires evidence, how it maintains forensic soundness and how it meets legal requirements.

### What is Network Forensics?

Network forensics is a branch of digital forensics focused on monitoring and analyzing computer network traffic for information gathering, legal evidence or intrusion detection.

Unlike other branches of digital forensics, network data is volatile and dynamic. Once transmitted, it is gone so network forensics is often a proactive investigation.

Network forensics has two general uses:

1. Monitoring a network for anomalous traffic and identifying intrusions.
2. Law enforcement may analyze capture network traffic as part of criminal investigations.

### What is Forensic Data Analysis?

Forensic data analysis (FDA) is a branch of digital forensics that examines structured data in regards to incidents of financial crime. The aim is to discover and analyze patterns of fraudulent activities. Structured data is data from application systems or their databases.

This can be contrasted to unstructured data that is taken from communication, office applications and mobile devices. Unstructured data has no overarching structure and analysis therefore means applying keywords or mapping patterns. Analysis of unstructured data is usually done by computer forensics or mobile device forensics experts.

### What is Database Forensics?

Database forensics is a branch of digital forensics related to databases and their related metadata. Cached information may also exist in a server's RAM requiring live analysis techniques.

A forensic examination of a database may relate to timestamps that apply to the update time of a row in a relational database that is being inspected and tested for validity to verify the actions of a database user. Alternatively, it may focus on identifying transactions within a database or application that indicate evidence of wrongdoing, such as fraud.

## CHALLENGES FACED BY DIGITAL FORENSIC

Development is severely challenged by the growing popularity of digital devices and the heterogeneous hardware and software being utilised.

- The increasing variety of file formats and OSs hampers the development of standardized DF tools and processes.
- The emergence of smart phones that increasingly utilize encryption renders the acquisition of digital evidence an intricate task.

Also, advancements in cybercrime have culminated in the substantial challenge, such as Crime as a Service (CaaS), which provides the attackers with easy access to the tools, programming frameworks, and services needed to conduct cyber attacks.

• Digital forensics has become an important tool in the investigation/identification of computer-based and computer-assisted crime.

- Eric Holder (Deputy Attorney General of the United States Subcommittee on Criminal Oversight for the Senate) has classified the challenges into three categories

1. Technical challenges
2. Legal challenges
3. Resource challenge

Technical challenges:Finding the forensics evidences have been hindered by:

➢Different Media format

➢Encryption

➢Anti-forensics

➢ Steganography.

➢Live acquisition and analysis

Legal challenges:

➢ Jurisdictional issue.

➢ Lack of standard legislation creates the legal challenges.

➢ Status as scientific evidence.

➢ What is the known or potential rate of error of the method used.

➢ whether the theory or method has been generally accepted by the scientific community.

Resource challenges: It is severely challenged by the growing popularity of digital devices and the heterogeneous hardware and software platforms being utilized.

➢ Volume of data.

➢ Time taken to acquire and analyze forensic media.

➢ To ensure to satisfied critical investigative and prosecutorial needs at all levels of government

**COMPUTER CRIME**

Alternatively referred to as **cyber crime**, **e-crime**, **electronic crime**, or **hi-tech crime**. **Computer crime** is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

**Why do people commit computer crimes?**

In most cases, someone commits a computer crime to obtain goods or money. Greed and desperation are powerful motivators for some people to try stealing by way of computer crimes. Some people may also commit a computer crime because they are pressured, or forced, to do so by another person.

Some people also commit a computer crime to prove they can do it. A person who can successfully execute a computer crime may find great personal satisfaction in doing so. These types of people, sometimes called black hat hackers, like to create chaos, wreak havoc on other people and companies.

Another reason computer crimes are sometimes committed is because people are bored. They want something to do and don't care if they commit a crime.

**Examples of computer crimes**

Below is a list of the different types of computer crimes today. Clicking any of the links gives further information about each crime.

- **Child pornography** - Making, distributing, storing, or viewing child pornography.
- **Copyright violation** - Stealing or using another person's Copyrighted material without permission.
- **Cracking** - Breaking or deciphering codes designed to protect data.
- **Cyber terrorism** - Hacking, threats, and blackmailing towards a business or person.
- **Cyberbully or Cyberstalking** - Harassing or stalking others online.

- **Cybersquatting** - Setting up a domain of another person or company with the sole intention of selling it to them later at a premium price.
- **Creating Malware** - Writing, creating, or distributing malware (e.g., viruses and spyware.)
- **Data diddling** - Computer fraud involving the intentional falsification of numbers in data entry.
- **Denial of Service attack** - Overloading a system with so many requests it cannot serve normal requests.
- **Doxing** - Releasing another person's personal information without their permission.
- **Espionage** - Spying on a person or business.
- **Fraud** - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud.
- **Green Graffiti** - A type of graffiti that uses projectors or lasers to project an image or message onto a building.
- **Harvesting** - Collect account or account-related information on other people.
- **Human trafficking** - Participating in the illegal act of buying or selling other humans.
- **Identity theft** - Pretending to be someone you are not.
- **Illegal sales** - Buying or selling illicit goods online, including drugs, guns, and psychotropic substances.
- **Intellectual property theft** - Stealing practical or conceptual information developed by another person or company.
- **IPR violation** - An intellectual property rights violation is any infringement of another's Copyright, patent, or trademark.
- **Phishing** or **vishing** - Deceiving individuals to gain private or personal information about that person.
- **Ransomware** - Infecting a computer or network with ransomware that holds data hostage until a ransom is paid.
- **Salami slicing** - Stealing tiny amounts of money from each transaction.
- **Scam** - Tricking people into believing something that is not true.
- **Slander** - Posting libel or slander against another person or company.
- **Software piracy** - Copying, distributing, or using software that was not purchased by the user of the software.
- **Spamming** - Distributed unsolicited e-mail to dozens or hundreds of different addresses.

- **Spoofing** - Deceiving a system into thinking you are someone you're not.
- **Swatting** - The act of calling in a false police report to someone else's home.
- **Theft** - Stealing or taking anything (e.g., hardware, software, or information) that doesn't belong to you.
- **Typosquatting** - Setting up a domain that is a misspelling of another domain.
- **Unauthorized access** - Gaining access to systems you have no permission to access.
- **Vandalism** - Damaging any hardware, software, website, or other object.
- **Wiretapping** - Connecting a device to a phone line to listen to conversations.

## CRIMINALISTICS

The criminal justice system in America is the overarching establishment through which crimes and those who commit them are discovered, tried, and punished. This includes all of the institutions of government aimed at upholding social order, deterring and mitigating crime, and sanctioning those who violate the law, such as law enforcement and the court and jail systems.

Criminology and criminalistics are two subsets of the criminal justice system. Criminology relates to studying and preventing crime—typically with behavioral sciences like sociology, psychology, and anthropology. Criminalistics refers to a type of forensics—the analysis of physical evidence from a crime scene.

While criminology has preventative components, criminalistics comes into effect only after a crime has been committed. A criminalist applies scientific principles to the recognition, documentation, preservation, and analysis of physical evidence from a crime scene. Criminalistics can also include crime scene investigations. The Bureau of Labor Statistics (BLS) classifies criminalists as forensic science technicians. Most professionals regard criminalistics as a specialty within the field of forensic science.

## WHAT DO CRIMINALISTS DO?

Criminalists use their knowledge of physical and natural science to examine and analyze every piece of evidence from a crime scene. They prepare written reports of their findings and may have to present their conclusions in court. A criminalist is not involved in determining the guilt or innocence of an accused individual. Their job, rather, is to present an objective analysis of the evidence.

There are several critical skills that criminalists need to be successful in their work. First, they must be detail-oriented and have excellent written and verbal communication skills. Second, they should also have strong critical-thinking and problem-solving skills and a solid background in science, statistics, physics, math, and ethics. Finally, criminalists should be comfortable testifying in court.

Most of a criminalist's work is performed in a laboratory unless they specialize in crime scene investigation. Their job typically includes recognizing what information is important, collecting and analyzing evidence without contaminating it, and organizing all information and evidence coherently.

Criminalistics has many fields of specialization. Specialties include, but are not limited to:

- Alcohol and drugs
- Arson
- Blood and tissue spatter
- Computer forensics
- DNA
- Explosions
- Serology (examining and analyzing body fluids)
- Toxicology
- Firearms and tool marks
- Trace evidence
- Wildlife (analyzing evidence against poachers)

As long as crimes continue to be committed, there will always be work for criminalists. A criminal will always leave evidence, no matter how minute, according to forensic scientist and "Father of Criminalistics" Paul L. Kirk:

> "Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as silent evidence against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen that he deposits or collects – all these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent

because human witnesses are. It is factual evidence. Physical evidence cannot be wrong; it cannot perjure itself; it cannot be wholly absent. Only its interpretation can err. Only human failure to find it, study and understand it, can diminish its value."

As soon as a crime is reported, an investigation is opened by the police or law enforcement agency with jurisdiction.

Police detectives and investigators use criminalistics in crime-scene investigations. Criminalistics is "the scientific study and evaluation of physical evidence in the commission of crimes." Criminalistics plays a vital role in organizing crime scenes, helping victims, ensuring justice, and serving the public.

Criminalists cover a broad range of criminal justice jobs within the forensic science field that examine physical evidence to link crime scenes with victims and offenders. Criminalists are sometimes referred to as lab technicians or crime scene investigators, a term made famous by the TV drama *CSI*.

These criminalists consult with experts, examine and analyze a variety of evidence including fingerprints, hair, fibers, skin, blood, and more. The criminalists then use their analysis to determine answers to how a crime was committed.

CRIMINALISTICS IN POLICE INVESTIGATIONS

A report from the National Institute of Justice outlined the role of criminalistics in police work. Criminalists investigate a variety of crimes, including domestic and aggravated assaults, burglary, robbery, sexual violence, and homicide.

Here are the basic functions completed by criminalists:

**Establishing an element of the crime**

- It's important for criminalists to establish proof that a crime occurred and to determine the cause and manner of death. Autopsies will help confirm the latter, while sending crime scene samples of blood, drugs, or semen, for example, could help determine the crime itself.

**Identification of a suspect or victim**

- Fingerprint and DNA testing are two examples of forensic evidence that criminalists use to identify an offender.

**Associative evidence**

- This type of scientific finding can help link the offender to the victim. Examples of associative evidence include hair follicles, blood, semen, fingerprints left on an object, foot impressions, and more.

**Reconstruction**

- Criminalists try to reconstruct how the crime happened using evidence from the crime scene. For example, certain evidence on a gunshot victim can discern the distance between a victim and the shooter.

**Corroboration**

- Physical evidence from a crime scene can corroborate or refute information that investigators collect during interviews with witnesses, victims and suspects.

CRIMINALISTICS IN REAL TIME

The FBI and U.S. Department of Justice distribute a guide for criminalist protocols when responding to a crime scene.

Here's what the Justice Department recommends takes place.

**Arrival/Initial Response**

- Upon arriving on the scene, criminalists should attempt to preserve the crime scene with minimal disturbance of the physical evidence.
- Criminalists should make initial observations to assess the scene while ensuring officer safety and security.
- They should react with caution. Offenders could still be at the crime scene and criminalists should remain alert and attentive until the crime scene is declared clear of danger.

**Documentation and Evaluation**

- The investigator(s) in charge should set responsibilities, share preliminary information and develop investigative plans in compliance with department policy and local, state and federal laws.
- Criminalists should speak with the first responders regarding observations from the crime scene before evaluating safety issues at the scene, establishing a path of exit and entry, and initial scene boundaries.
- If multiple scenes exist, criminalists should establish and maintain communication with personnel at those sites.

**Processing the Scene**

- Based on the type of incident and complexity of the crime scene, criminalists should determine team composition on site.
- Criminalists will assess the scene to determine which specialized resources are required. For example, forensic examiners could be called to the scene, or a coroner to investigate a cadaver.

**Completing and Recording the Crime Scene Investigation**

- Criminalists should establish a crime scene debriefing team, which enables all law enforcement bodies to share information about findings before the scene is released.
- Criminalists determine what evidence was collected, discuss the preliminary scene findings with scene personnel, discuss potential forensic tests that will take place, and initiate any action required to complete the crime scene investigation.

**The object and categories of criminalistics**

The structure of criminalistics in Europe is not uniform. Western European countries took the British-American model which describes "criminalistics" as close to equal with "forensic science". According to this model, forensic science uses criminalistic techniques, employed for technical solution of judicial problems. Additionally, this model contains crime scene investigation techniques. Some of these techniques are used in central European models within the field of criminalistic tactics. For a number of central European law practitioners, criminalistics falls within the broad category of legal sciences31. Owing to the legal aspect of the criminalistics, forensic science and the science of criminalistics cannot be linked to each other. Not being identified in the Criminal Code, some of the forensic science techniques, such as electro-technical examination, examination of digital evidence, or metallographic examination, do not belong to legal methods, and therefore forensic science is viewed as a different discipline than criminalistics. The legal aspect plays a critical role in the differentiation between the two models32. Criminalistics is an independent science that "examines the manifestation of the event in form of physical and memory characteristics"33. In criminalistics, this manifestation is called trace evidence. Trace evidence is the object of the science of criminalistics. Criminalistics differentiates two types of trace evidence: physical (material) and mental (memory). Naturally, criminal investigation based on material evidence provides a higher level of precision and certainty34 (It is necessary to note that in criminalistics, we differentiate between evidence and trace evidence. Evidence is a term for proving something, and is basically regarded as a proof, whereas trace evidence is meant as an imprint used for identification). Contemporary criminalistics is broken down to two main groups, criminalistic techniques and criminalistic tactics. Criminalistic techniques focus on an examination of material (physical) trace evidence, while criminalistic tactics examine mainly memory trace evidence. Regardless of the different categories of evidence, criminalistics is focused on finding, seizing and examining the evidence35. Criminalistics distinguishes between three categories of achieving this goal: (a) modus operandi – method of committing a crime, (b) criminalistics trace evidence and (c) criminalistics identification.

**Modus operandi/method of committing a crime**

Considerable emphasis in criminal investigation is placed on a detailed description of the method of committing the crime, which is known as modus operandi (or MO). Three major components of MO play a role in criminal investigation, and they are listed as follows: The components pertaining to an action characterize the physical and psychological activity of the offender while committing a crime. Material components consist of tools and items necessary for committing the crime. Finally, multifaceted components are a complex group of activities and information required for committing the crime.

Human behaviour is determined by numerous factors. Similarly, the behaviour of the offender depends on the interaction between these factors. Criminalistics divides these factors on objective and subjective determinants. Objective determinants do not depend on offender's choice. In general, they are social/cultural conditions, victim(s)/target(s), the relationship between the offender and the victim/target, the crime scene, the time, the accessibility of tools (weapon, etc.), and the existence of co-offender(s). Subjective determinants depend on and are connected to the offender(s) specifically. They are the physical (somatic) characteristics of the offender (ie. his/her strength, body build), psychological and motor characteristics of the offender (his/her level of intelligence, ease of mobility, hobbies, and sexual behaviour), age, gender, criminal experience and educational level (qualification, skills)36. Knowledge of the method of committing a crime offers additional important information. It enables investigators to create criminalistic versions, and provides data for criminal profiling37 .

**Criminalistic trace evidence**

In criminal investigation, trace evidence gives investigators a picture of the criminal act along with the indications about behaviour of the perpetrator and his/her victim(s) at the scene. The knowledge of the trace evidence mechanism and its creation lays the foundation for criminal investigation methods and techniques. The essence of trace evidence is the mutual association of two objects that provide information about criminal act. When two objects have an effect on one another, they create changes. These changes illustrate and reproduce characteristics of affected objects. Each change in a physical environment or a human mind that is influenced by a criminal act is considered to be trace evidence. As a result of this, criminalistics distinguishes between material (physical) trace evidence and

memory trace evidence. Three major changes must come into effect in order to produce trace evidence: change that is generated by the criminal act, change that exists until the time of its seizing, and change that can be assessed by criminalistics methods and techniques38. Trace evidence is widely recognized as one of the subjects of scientific examination39 .

Material (physical) trace evidence is divided into five categories: Trace evidence that gives information about (a) the structure of outer surface of the objects, such as finger-prints or ballistics evidence, (b) the structure of the inner surface of the objects, such as biological, chemical or pyrotechnical evidence, (c) the functional and dynamic features of the objects, such as voice, posture while walking, or hand-writing, (d) characteristics of the objects that created the trace evidence, such as finger-prints created by blood, foot-prints that provide insight into walking patterns, and (e) features of the objects created by change, such as peripheral trace evidence, (moving an object from one place to another), slits or bruises40. Although memory trace evidence has physical features (like changes in brain cells) methods of their examination are quite complex. Memory trace evidence is formed by the five human senses (sight, hearing, touch, smell and taste), but it is very difficult to examine the exact way in which it is created. Additionally, it is influenced by the personality of the person who created it (the person's short and long term memory as well as his/her emotional state, etc.) and is not accessible immediately. Once the person dies or if he/she is not willing to share his/her memory, the trace evidence is lost. All memory trace evidence is formed as a reflection of the human mind, which is influenced by the organic or inorganic environment. The basic impulse that creates the memory trace evidence is a perception that is generated by the pressure of the environment on the human senses41 .

The examination of memory trace evidence is achievable merely by methods which allow a person to interpret his/her own experience through recollection of a specific event. This can be done using legal methods of psychological manipulation. As a result of this, memory trace evidence is examined using a combination of methods of criminalistic tactics, such as criminalistic versions, interrogation, confrontation, verification of the statement on the scene, recognition, and in some cases, criminalistic experiment and criminalistic reconstruction42.

**Criminalistic identification**

Once trace evidence is formed during a criminal act, the investigators strive to find out who created the evidence and what object were used. Criminalistic identification includes examining objects (living and non-living) which may have contributed to the formation of trace evidence. During the process of criminalistic identification, the object is not only identified, but also individualized. Individualization of the object is the process by which investigators examine general and specific features of the object. Criminalistics identification is divided according to four categories. In relation to the subject (person who performed the identification), criminalistics distinguishes identification made by an expert witness or recognition by the witness (lay person). Identification made by scientific methods of examination consists of finger-print examination, ballistics, biological identification etc. In relation to the identified objects criminalistics differentiates between identification of people and identification of non-living objects. Identification of people is usually made on the base of anatomic and anthropological features of the human body, functional characteristics of motor signs, (human gesticulation, hand-writing), the human voice, biological traces, and track traces (foot-print, lip-print, teeth). Identification of non-living objects is conducted more often by ballistics, track traces, tool marks and microscopes. The last category distinguishes identification on the basis of results; for instance, whether the object was identified or not. Individual identification is achieved by confirmation (witnesses, DNA, etc). In the case of the process of incomplete identification, the identification is finished, but the object was not identified. Here, examiners conduct partial identification by grouping the object into a bigger category (type of vehicle). Identification according to identifying features is made on the basis of specific characteristics of the object, such as functional, dynamic, structural, etc. As a result of its capability to be scientifically examined, criminalistics identification belongs to both criminalistics sub-categories: criminalistic tactics and criminalistic techniques. Therefore, identification enables the examination of material and memory trace evidence43 .

**Methods of criminalistics**

Criminalistic methods developed during the historical progress of criminalistics through its own scientific growth and through the adaptation and adjustment of methods developed in other sciences. However, criminalistic examination can be done by criminalistic methods only. These methods must meet four strict criteria. The methods must (a) not contravene

lawful norms, (b) be scientifically based, (c) be verified by criminalistic practice and (d) be accepted by criminalistic practice. Satisfaction of the lawful (legal) norm is a central criterion for the application of criminalistic methods. Its importance lies in the outcome of the criminal investigation. If the evidence was gathered using an illegal method (for instance, the use of physical or psychological force during the interrogation), evidence usually becomes inadmissible in court. Scientific base criterion is determined by the current situation of the progress in the scientific world. When new knowledge is scientifically recognized, the method can be changed or altered and the old method is eventually discarded. Verifica-tion criterion is fulfilled when the scientific basis of the method is confirmed in an existing practical situation. Recognition criterion is linked to the verification principle, however, the time that elapses from the verification of a particular method to the complete application of this method into the practice is essentially longer44. Porada et al.45 identify three groups of criminalisticc methods. The first group consists of "methods of universal perception". These methods are generally employed by all examiners, such as observation, description, comparison, measurement and experiment. The second group involves "methods taken from other sciences". These methods of examination were created by other sciences, such as physics, chemistry, and biology, and criminalistics includes them in its method of examination. The last group is composed of "specific methods of criminalistics science" and these are applied exclusively in the field of criminalistics, such as knowledge gathered from criminal investigation, law enforcement or judicial practice46 . Criminalistic methods are divided into two major groups. The first, methods of criminalistics techniques, examines material (substantive) trace evidence (finger-print analysis, DNA, etc.), while the second, methods of criminalistics tactics, usually studies memory trace evidence (crime scene examination, interrogation, search, etc.)47 . Methods of criminalistic techniques The rapid development of scientific disciplines and the colossal growth of modern technologies has improved the methods and techniques of criminal investigation, along with the process of the identification of material trace evidence. Therefore, criminalistic techniques focus on the identification of people, items, and occasionally animals. With respect to the scientific procedure used for the examination of trace evidence, criminalistics techniques are divided into more categories. The first, methods that use procedures based on optical principles, takes advantage of the miniature structure of trace evidence and the possibility of examining it without causing any further damage. Magnifying glasses and microscopes are tools widely

used by forensic specialists. The application of microscopes (binocular, comparing, biological, metallographic, and electronic scanning) is exclusively achievable at forensic laboratories. Magnifying glasses can be used both at the crime scene and forensic laboratory. The second category, methods of criminalistics techniques that use procedures based on electromagnetic light, employs X-rays, ultra-violet, infrared and nucleus light for further identification of material trace evidence. Lastly, methods that use chemical and physical procedures, are used in analyses of drugs, blood, toxins, fuels, emissions, plastics, etc. andare commonly applied48. The application of knowledge incorporated from various scientific disciplines into forensic science is the key factor that helps link the offender to the crime by means of material trace evidence. Forensic specialists employ numerous techniques appropriate to the characteristics of the crime. Frequently used techniques are finger-print analysis, (daktyloscopy), DNA analysis, forensic pathology, forensic biology, forensic anthropology, ballistics, forensic audio-expertise, firearm and tool mark examination, digital imaging enhancement, forensic data recovery, and accounting.

**Methods of criminalistic tactics**

The significance of criminalistic tactics as a method of collection, examination, exploration and application of evidence lies in its contribution to the process of criminal investigation. In the 1950s, Bohuslav Nemec defined criminalistic tactics as (a) a science about crime and criminal acts, (b) study about methods of offenders' activities, (c) generalization of criminalistic knowledge and its practical application, (d) active summary and statistics, (e) effective functioning of law enforcement, and (f) investigative process"49. Later on in the 60s, the objects of criminalistic tactics shifted to investigative methods and techniques of criminal investigation. Additionally, characteristics of the offender, methods of committing crimes, and their classification were added. During the 70s, academics agreed that criminalistic tactics should focus on the issues of examination and application of methods related to the investigation and prevention of dangerous activities. Criminalistic tactics assist in finding the facts in issue, and therefore they have to satisfy numerous requirements. A specific tactic must be legally approved, scientifically verifiable, appropriate, and accessible; finally, their application is required to be ethical. At present, methods of criminalistics tactics focus on the examination of memory trace evidence. Each method examines evidence from a specific point of view. However, this type of evidence does not exist in a vacuum; memory

isfrequently interconnected with material evidence and the material environment. Existing methods of criminalistic tactics include (a) crime scene investigation, (b) criminalistic search, (c) criminalistic versions, (d) interrogation/interview, (e) confrontation, (f) verification of the statement on the scene, (g) recognition, (h) criminalistic experiment, and (i) criminalistic reconstruction. In some cases, criminalistic documentation, planning and management of criminalistics examination are added to the methods of criminalistic tactics50 .

**Crime scene investigation**

The key role of the crime scene investigation (or CSI) is the comparison between an object's material condition and trace evidence obtained from this object, as well as their mutual relationship. The core of the CSI lies in direct observation of the scene and the object while searching for material changes in the object, which can become evidence. However, this process is not just mere observation. It is also empirical examination, continuous evaluation and documentation of a crime scene's physical condition and objects connected to it. Observation can be made by the senses or using electronic/technical equipment.

The goal of the CSI is to (a) find evidence, (b) discover relationships and associations, and (c) detect other circumstances, such as conditions, motives and hypotheses for the creation of criminalistics versions51. The significance of the CSI as one of criminalistic methods is remarkable. It enables investigators to understand the characteristics of the event that took place at the crime scene including plausible causes and conditions that gave rise to the criminal event, or to understand the offender who committed crime. Success of a criminal investigation often depends on the quality of the CSI, which is one criminalistic tactic that cannot be replaced by any other method. The level of its quality essentially influences the quality of the gathered evidence. Insufficient knowledge and skills or an irresponsible approach of law enforcement officers may lead to a lesser punishment or even acquittal of a true offender. CSI provides initial information about evidence and the event itself which took place at the crime scene. A shoe print might be an example, as it may lead to knowledge one's height. Facts derived from preliminary information about evidence depend considerably on experience and knowledge. The crime scene investigation is considered to be a team effort made by the police officers, investigators, and forensic specialists52. The

first officers at the crime scene are the members of the "permanent access group". Additional participants of the CSI are witnesses, any victims or even the accused. It is crucial to use good judgement in deciding whether the attendance of such people is necessary or not because it might put the investigation at risk. A phone call made to 112 initiates four major tasks: (a) completion of initial, emergency activities, (b) preparation for crime scene examination, (c) completion of crime scene examination along with proper documentation of its results and (d) evaluation of accomplished results and their application53 .

**Criminalistic documentation**

The aim of criminalistic documentation is to secure trace evidence (verbally and acoustically) and to take control of the course and outcome of the criminal investigation. In criminalistic examination, (investigation), trace evidence and comparing material have the nature of documented marks and seized objects54. Documented marks are delivered in written form, (transcript), phonogram (audio recording), photographic form (photographs, hologram video, film, and digital recording), and topographic form (sketch, plan, and drawing). Standard criminalistic documentation comes in the form of a transcript. In other words, it describes a situation that was observed by its author. A transcript must consist of objectively true statement of facts – the subjective feelings of the author are not allowed. In addition to an oral description of the observed situation, investigators can choose the form of an audio (phonographic) recording. Furthermore, this form of documentation is frequently used at the interrogation/interview, where the statements made by the accused, witnesses or the victim are recorded. However, photographic form provides the most precise documentation. Written, phonographic and photographic forms are supplemented by topographic form, usually consisting of sketches, plans, and drawings. Seized objects are submitted in their natural form, and the exact location where they were found is documented along with all of the circumstances and conditions surrounding their discovery. Not only trace evidence but also any manipulation to it must be documented in order to protect the chain of evidence. Each and every piece of evidence, its manipulation and the circumstances around it is important for a criminal investigation, therefore thorough documentation is crucial.

# Unit-2

**Cyber Crime Scene Analysis:** Identifying digital evidence, collecting evidence in private-sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene, seizing digital evidence at the scene.

**Identifying digital evidence:**

Digital evidence can be any information stored or transmitted in digital form. Because you can't see or touch digital data directly, it's difficult to explain and describe. Is digital evidence real or virtual? Does data on a disk or other storage medium physically exist, or does it merely represent real information? U.S. courts accept digital evidence as physical evidence, which means that digital data is treated as a tangible object, such as a weapon, paper document, or visible injury, that's related to a criminal or civil incident. Courts in other countries are still updating their laws to take digital evidence into account. Some require that all digital evidence be printed out to be presented in court. Groups such as the Scientific Working Group on Digital Evidence (SWGDE; www.swgde.org) and the International Organization on Computer Evidence (IOCE; www.ioce.org) set standards for recovering, preserving, and examining digital evidence. For more information on digital evidence, visit www.ojp.usdoj.gov/nij/ pubs-sum/187736.htm and read "Electronic Crime Scene Investigation: A Guide for First Responders," which provides guidelines for U.S. law enforcement and other responders who protect an electronic crime scene and search for, collect, and preserve electronic evidence.

Following are the general tasks investigators perform when working with digital evidence:

• Identify digital information or artifacts that can be used as evidence.

• Collect, preserve, and document evidence.

• Analyze, identify, and organize evidence.

• Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably.Collecting computers and processing a criminal or incident scene must be done systematically.

To minimize confusion, reduce the risk of losing evidence, and avoid damaging evidence, only One person should collect and catalog digital evidence at a crime scene or lab, if practical. If there's too much evidence or too many systems to make it practical for one person to perform these tasks, all examiners must follow the same established operating procedures, and a lead or managing examiner

should control collecting and cataloging evidence. You should also use standardized forms (discussed later in "Documenting Evidence") for tracking evidence to ensure that you consistently handle evidence in a safe, secure manner. An important challenge investigators face today is establishing recognized standards for digital evidence.

For example, cases involving several police raids are being conducted simultaneously in several countries. As a result, you have multiple sites where evidence was seized and hundreds of pieces of digital evidence, including hard drives, cell phones, memory sticks, PDAs, and other storage devices. If law enforcement and civil organizations in those countries have agreed on proper procedures (generally, the highest control standard should be applied to evidence collection in all jurisdictions), the evidence can be presented in any jurisdiction confidently.

**Understanding Rules of Evidence**

Consistent practices help verify your work and enhance your credibility, so you must handle all evidence consistently. Apply the same security and accountability controls for evidence in a civil lawsuit as in a major crime to comply with your state's rules of evidence or with the Federal Rules of Evidence. Also, keep in mind that evidence admitted in a criminal case might also beAs part of your professional growth, keep current on the latest rulings and directives on collecting, processing, storing, and admitting digital evidence. The following sections discuss some key concepts of digital evidence. You can find additional information at the U.S. Department of Justice Web site (www.usdoj.gov) and by searching the Internet for "digital evidence," "best evidence rule," "hearsay," and other relevant keywords. Consult with your prosecuting attorney, Crown attorney, corporate general counsel, or the attorney who retained you to learn more about managing evidence for your investigation.

In Chapter 2, you learned how to make an image of a disk as part of gathering digital evidence.

The data you discover from a forensic examination falls under your state's rules of evidence or the Federal Rules of Evidence. However, digital evidence is unlike other physical evidence because it can be changed more easily. The only way to detect these changes is to compare the original data with a duplicate. Furthermore, distinguishing a duplicate from the original electronically is impossible, so digital evidence requires special legal consideration. Most courts have interpreted computer records as hearsay evidence. The rule against hearsay evidence is deceptively simple and full of exceptions. Hearsay is any out-of-court statement presented in court to prove the truth of an assertion. In other words, hearsay is evidence of a statement made other than by a witness while testifying at the hearing and is offered to

prove the truth of a statement. The definition of hearsay isn't difficult to understand, but it can become confusing when considering all the exceptions to the general rule against hearsay.

Twenty-four exceptions in the federal rules don't require proof that the person who made the statement is unavailable. The following are the ones most applicable to computer forensics practice:

• Business records, including those of a public agency.

• Certain public records and reports.

• Evidence of the absence of a business record or entry.

• Learned treatises used to question an expert witness.

• Statements of the absence of a public record or entry.

• The catchall rule, which doesn't require that the declarant be unavailable to testify. It does say that evidence of a hearsay statement not included in one of the other exceptions can be admitted if it meets the following conditions:

• It has sound guarantees of trustworthiness.

• It is offered to help prove a material fact.

• It is more probative than other equivalent and reasonably obtainable evidence.

• Its admission would forward the cause of justice.

• The other parties have been notified that it will be offered into evidence. The business-record exception, for example, allows "records of regularly conducted activity," such as business memos, reports, records, or data compilations. Business records are authenticated by verifying that they were created "at or near the time by, or from information transmitted by, a person with knowledge …" and are admissible "if the record was kept in the course of a regularly conducted business activity, and it was the regular practice of that business activity to make the record" (Federal Rules of Evidence, 803(6); see Section V, Evidence," in Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm). Generally, computer records are considered admissible if they qualify as a business record. Computer records are usually divided into computer-generated records and computer-stored records. Computer-generated records are data the system maintains, such as system log files and proxy server logs. They are output generated from a computer process or algorithm, not usually data a person creates. Computer-stored records, however, are electronic data that a person creates and saves on a computer, such as a spreadsheet or word processing document. Some records combine computer-generated and computer-stored evidence, such as a spreadsheet containing mathematical operations (computer-generated records)

generated from a person's input (computer-stored records).

Computer records must also be shown to be authentic and trustworthy to be admitted into evidence. Computer-generated records are considered authentic if the program that created the output is functioning correctly. These records are usually considered exceptions to the hearsay rule. For computer-stored records to be admitted into court, they must also satisfy an exception to the hearsay rule, usually the business-record exception, so they must be authentic records of regularly conducted business activity. To show that computer-stored records are authentic, the person offering the records (the "offeror"—the plaintiff, or defense) must demonstrate that a person created the data and the data is reliable and trustworthy—in other words, that it wasn't altered when it was acquired or afterward.

Collecting evidence according to the proper steps of evidence control helps ensure that the computer evidence is authentic, as does using established computer forensics software tools. Courts have consistently ruled that computer forensics investigators don't have to be subject matter experts on the tools they use. In United States v. Salgado (250 F.3d 438, 453, 6th Cir., 2001), the court stated, "It is not necessary that the computer programmer testify in order to authenticate computer-generated records." In other words, the witness must have firsthand knowledge only of facts relevant to the case. If you have to testify about your role in acquiring, preserving, and analyzing evidence, you don't have to know the inner workings of the tools you use, but you should understand their purpose and operation. For example, Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1) tools use complex algorithms. During a cross-examination, an opposing attorney might ask you to describe how these forensics tools work. You can safely testify that you don't know how the MD5 hashing algorithm works, but you should know how to describe the steps for using the MD5 function in AccessData Forensic Toolkit, for instance. When attorneys challenge digital evidence, often they raise the issue of whether computer generated records were altered or damaged after they were created. Attorneys might also question the authenticity of computer-generated records by challenging the program that created them. To date, courts have been skeptical of unsupported claims about digital evidence.

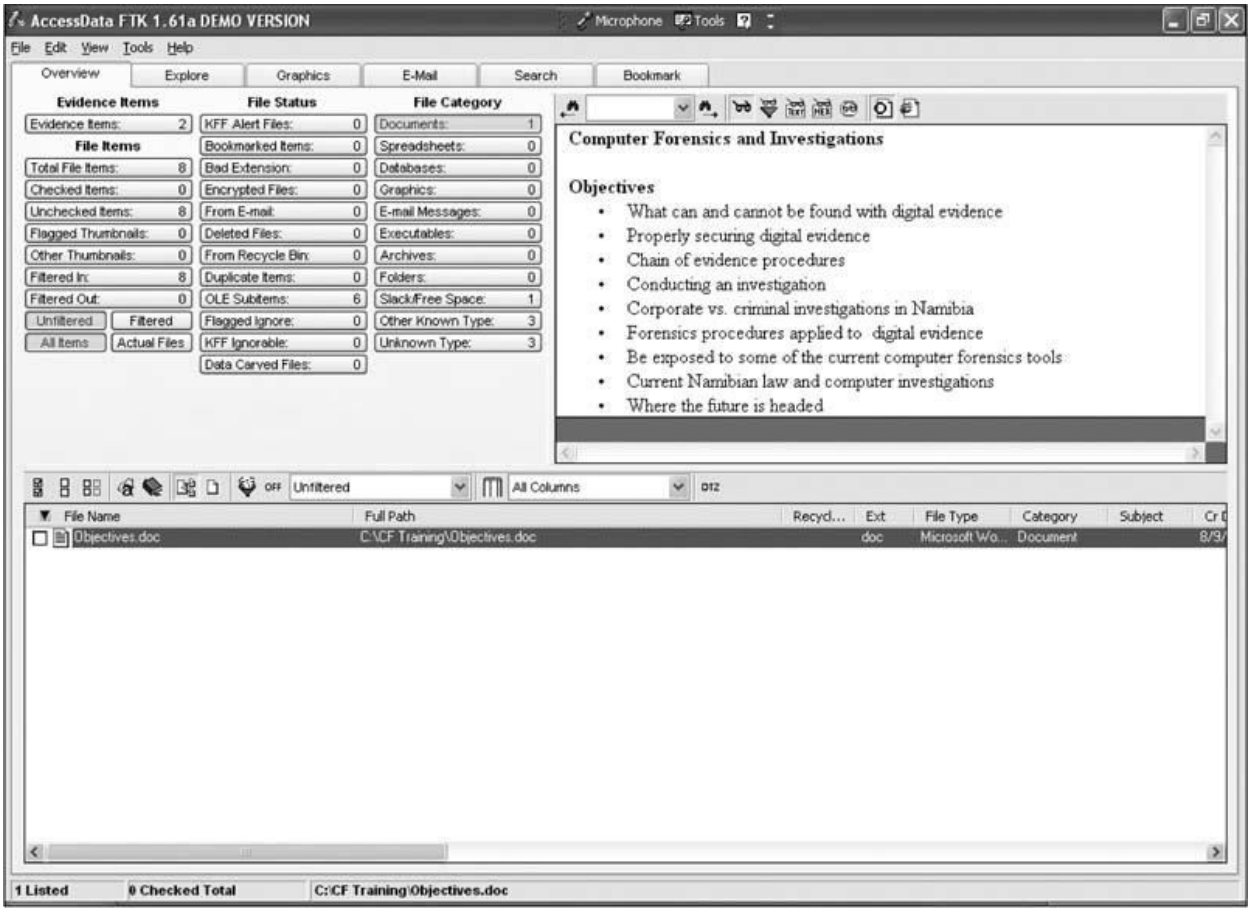
Asserting that the data changed without specific evidence is not sufficient grounds to discredit the digital evidence's authenticity. Most federal courts that evaluate digital evidence from computer-generated records assume that the records contain hearsay. Federal courts then apply the business-

records exception to hearsay as it applies to digital evidence. As mentioned, one test to prove that computer-stored records are authentic is to demonstrate that a specific person created the records. Establishing who created digital evidence can be difficult, however, because records recovered from slack space or unallocated disk space usually don't identify the author. The same is true for other records, such as anonymous e-mail messages or text messages from instant-messaging programs. To establish authorship of digital evidence in these cases, attorneys can use circumstantial evidence, which requires finding other clues associated with the suspect's computer or location. The circumstantial evidence might be that the computer has a password consistent with the password the suspect used on other systems, a witness saw the suspect at the computer at the time the offense occurred, or additional trace evidence associates the suspect with the computer at the time of the incident. In a recent case, the attorney chose not to use the digital evidence because although it could be proved that a particular camera was used to create the suspect's movies, CDs, and DVDs, there was no way to prove that the suspect was the person using the camera. Therefore, there was no circumstantial or corroborating evidence to prove that the suspect was guilty.

Although some files might not contain the author's name, in the arrest of the BTK strangler, the author of a Microsoft Word document was identified by using file metadata. In February 2005, the man claiming to be the BTK strangler sent a floppy disk to FOX News in Wichita. The police he had been taunting told him that they wouldn't be able to trace him via the floppy disk. Forensics analysis of the disk came back with the name of the church and a user named Dennis, who turned out to be Dennis Radar, president of the congregation. The police had enough physical evidence to link him to the crimes. They arrested him, and he confessed to the murders of 10 people over the course of 30 years. He was sentenced to nine life terms. (For the full story, visit the TruTV Web site at www.crimelibrary.com/serial_killers/unsolved/btk/index_1.html.) The following activity shows an easy way to identify this file metadata. Follow these steps in the demo version of AccessData Forensic Toolkit: Start Microsoft Word, and in a new document, type By creating a file, you can identify the author with file metadata. Save it in your work folder as InChp05-01. doc, and then exit Microsoft Word.

1. To start FTK, click Start, point to All Programs, point to AccessData, point to Forensic Toolkit, and click Forensic Toolkit. If you're prompted with a warning dialog box and/or notification, click OK to continue, and click OK, if necessary, in the message box thanking you for evaluating the program.

2. Click Go directly to working in program, and then click OK. Click File, Add Evidence from the menu.
3. In the Add Evidence dialog box, enter your name as the investigator, and then click Next. In the Evidence Processing Options dialog box, accept the default setting, and then click Next.
4. In the main Add Evidence to Case dialog box, click the Add Evidence button. In the next Add Evidence to Case dialog box, click the Individual File option button, and then click Continue.
5. In the Browse for Folder dialog box, navigate to your work folder, click InChp05-01.doc, click Open, and then click OK. Click Next, and then click Finish.
6. In the main window, click the Overview tab, if necessary. Under the File Category heading, click the Documents button. Click to select the InChp05-01.doc file in the bottom pane; its contents are then displayed in the upper-right pane. Figure 5-1 shows an example (although the filename in this figure is different).




8. On the File List toolbar at the upper right, click the View files in native format button, if the button isn't already selected. (Hint: Hover your mouse over buttons to see their names displayed.)

9. Next, click the View files in filtered text format button. If you entered your username and

organization when you installed Word, that information is displayed (see Figure 5-2).

10. Exit FTK, clicking No if prompted to back up your work. In addition to revealing the author, computer-stored records must be proved authentic, which is the most difficult requirement to prove when you're trying to qualify evidence as an exception to the hearsay rule. The process of establishing digital evidence's trustworthiness originated with written documents and the best evidence rule, which states that to prove the content of a written document, recording, or photograph, ordinarily the original writing, recording, or photograph is required (see Federal Rules of Evidence, 1002). In other words, the original of a document is preferred to a duplicate. The best evidence, therefore, is the document created and saved on a computer's hard disk.

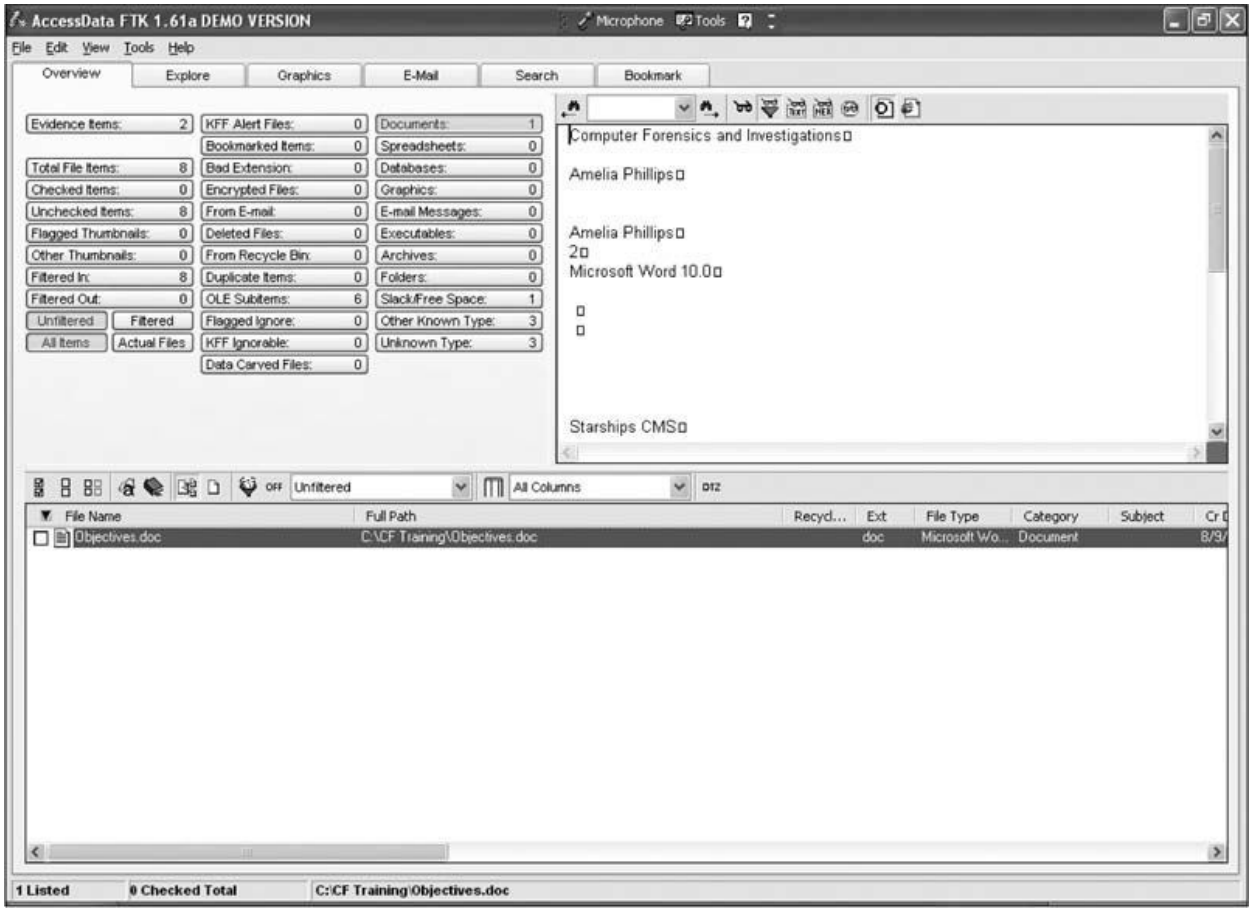



Figure 5-2 Viewing file metadata

Agents and prosecutors occasionally express concern that a printout of a computer-stored electronic file might not qualify as an original document, according to the best evidence rule. In its most fundamental form, the original file is a collection of 0s and 1s; in contrast, the printout is the result of manipulating the file through a complicated series of electronic and mechanical processes (Federal Rules of Evidence, 803(6); see Searching and Seizing from Computers and Obtaining Electronic Evidence in Criminal Investigations, p. 152). To address this concern about original

evidence, the Federal Rules of Evidence state: "[I]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" Instead of producing hard disks in court, attorneys can submit printed copies of files as evidence. In contrast, some countries allow only the printed version to be presented in court, not hard disks.

In addition, the Federal Rules of Evidence, 1001(4), allow duplicates instead of originals when the duplicate is "produced by the same impression as the original … by mechanical or electronic re-recording … or by other equivalent techniques which accurately reproduce the original." Therefore, as long as bit-stream copies of data are created and maintained properly, the copies can be admitted in court, although they aren't considered best evidence. The copied evidence can be a reliable working copy, but it's not considered the original. Courts understand that the original evidence might not be available, however. For example, you could make one image of the evidence drive successfully but lose access to the original drive because it has a head crash when you attempt to make a backup image. Your first successful copy then becomes secondary evidence. The attorney must be able to explain to the judge that circumstances beyond the examiner's control resulted in loss of the original evidence; in this case, the hard drive is no longer available to be examined or imaged. Mishaps with evidence happen routinely in all aspects of evidence recovery.

Another example of not being able to use original evidence is investigations involving network servers. Removing a server from the network to acquire evidence data could cause harm to a business or its owner, who might be an innocent bystander to a crime or civil wrong. For example, Steve Jackson Games was the innocent party in a case in which evidence of criminal activity had been stored in e-mail on company computers. The network administrator had reported evidence of a crime committed by users of the company's bulletin board system (BBS) to the Secret Service. Secret Service agents seized all the computers at Steve Jackson Games and effectively put the company out of business. SJG sued the Secret Service, which was found liable for damages under the Privacy Protection Act and Title II of the Electronic Communications Privacy Act. For more information, see Steve Jackson Games v. United States Secret Service and United States of America (36 F.3d 457, USCA 5, 1994).

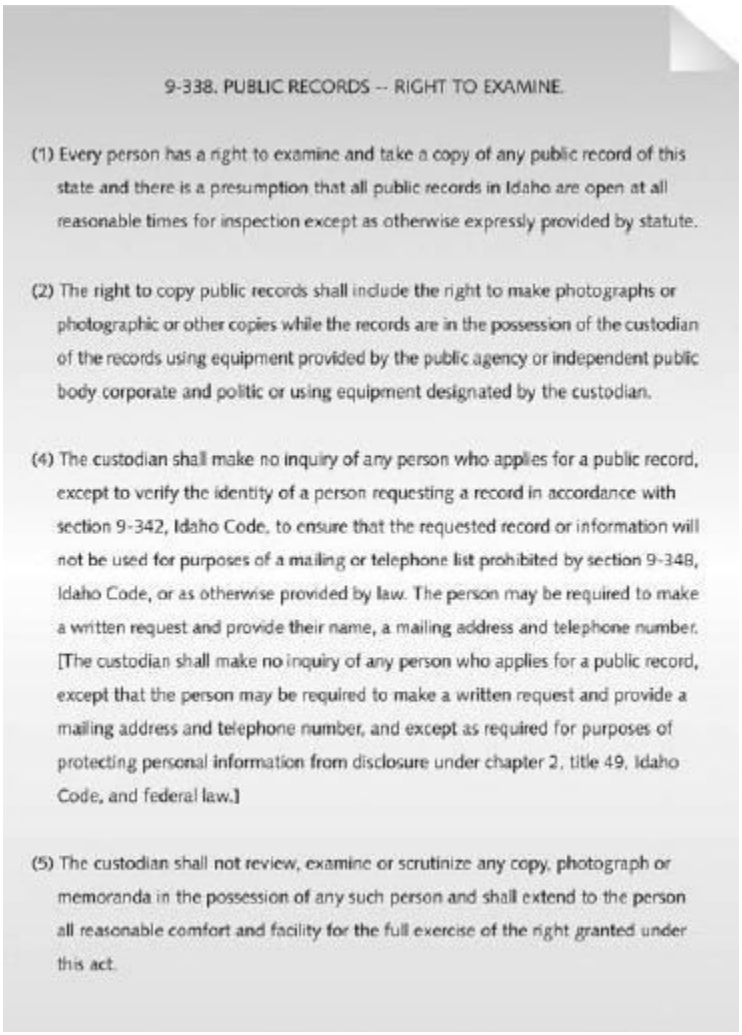
In this situation, you might not have the authority to create an image or remove the original drive. Instead, make your best effort to acquire the digital evidence with a less intrusive or disruptive method. In this context, the recovered materials become the best evidence because of the circumstances. In summary, computer-generated records, such as system logs or the results of a

mathematical formula in a spreadsheet, aren't hearsay. Computer-stored records that a person generates are subject to rules governing hearsay, however. For the evidence to qualify as a businessrecord exception to the hearsay rule, a person must have created the computer-stored records, and the records must be original. The Federal Rules of Evidence treat images and printouts of digital files as original evidence.

**Collecting Evidence in Private-Sector Incident Scenes:**

Private-sector organizations include businesses and government agencies that aren't involved in law enforcement. In the United States, these agencies must comply with state public disclosure and federal Freedom of Information Act (FOIA) laws and make certain documents available as public records. State public disclosure laws define state public records as open and available for inspection. For example, divorces recorded in a public office, such as a courthouse, become matters of public record unless a judge orders the documents sealed. Anyone can request a copy of a public divorce decree. Figure 5-3 shows an excerpt of a public disclosure law for the state of Idaho.

State public disclosure laws apply to state records, but the FOIA allows citizens to request copies of public documents created by federal agencies. The FOIA was originally enacted in the 1960s, and several subsequent amendments have broadened its laws. Some Web sites now provide copies of publicly accessible records for a fee. A special category of private-sector businesses includes ISPs and other communication companies. ISPs can investigate computer abuse committed by their employees, but not by customers. ISPs must preserve customer privacy, especially when dealing with e-mail. However, federal regulations related to the Homeland Security Act and the Patriot Act of 2001 have redefined how ISPs and large corporate Internet users operate and maintain their records.



9-338. PUBLIC RECORDS -- RIGHT TO EXAMINE.

(1) Every person has a right to examine and take a copy of any public record of this state and there is a presumption that all public records in Idaho are open at all reasonable times for inspection except as otherwise expressly provided by statute.

(2) The right to copy public records shall include the right to make photographs or photographic or other copies while the records are in the possession of the custodian of the records using equipment provided by the public agency or independent public body corporate and politic or using equipment designated by the custodian.

(4) The custodian shall make no inquiry of any person who applies for a public record, except to verify the identity of a person requesting a record in accordance with section 9-342, Idaho Code, to ensure that the requested record or information will not be used for purposes of a mailing or telephone list prohibited by section 9-348, Idaho Code, or as otherwise provided by law. The person may be required to make a written request and provide their name, a mailing address and telephone number. [The custodian shall make no inquiry of any person who applies for a public record, except that the person may be required to make a written request and provide a mailing address and telephone number, and except as required for purposes of protecting personal information from disclosure under chapter 2, title 49, Idaho Code, and federal law.]

(5) The custodian shall not review, examine or scrutinize any copy, photograph or memoranda in the possession of any such person and shall extend to the person all reasonable comfort and facility for the full exercise of the right granted under this act.

Figure 5-3 Idaho public disclosure law

ISPs and other communication companies now can investigate customers' activities that are deemed to create an emergency situation. An emergency situation under the Patriot Act is the immediate risk of death or personal injury, such as finding a bomb threat in an e-mail message. Some provisions of those laws have been revised over the past few years, so you should stay abreast of their implications. Investigating and controlling computer incident scenes in the corporate environment is much easier than in the criminal environment. In the private sector, the incident scene is often a workplace, such as a contained office or manufacturing area, where a policy violation is being investigated. Everything from the computers used to violate a company policy to the surrounding facility is under a controlled authority—that is, company management. Typically, businesses have inventory databases of computer hardware and software. Having access to this database and knowing what applications are on suspected computers help identify the computer forensics tools needed to analyze a policy violation and the best way to conduct the analysis. For example, most companies use a single Web browser, such as Microsoft Internet Explorer, Mozilla Firefox, or KDE Konqueror. Knowing which browser a suspect used helps you develop standard examination procedures to identify data downloaded to the suspect's workstation. To investigate employees suspected of improper use of company computing assets, a corporate policy statement about misuse of computing assets allows corporate investigators to conduct

covert surveillance with little or no cause and access company computer systems without a warrant, which is an advantage for corporate investigators. Law enforcement investigators cannot do the

same, however, without sufficient reason for a warrant. However, if a company doesn't display a warning banner or publish a policy stating that it reserves the right to inspect computing assets at will, employees have an expectation of privacy (as explained in Chapter 1). When an employee is being investigated, this expected privacy prevents the employer from legally conducting an intrusive investigation. A well-defined corporate policy, therefore, should state that an employer has the right to examine, inspect, or access any company-owned computing assets. If a company issues a policy statement to all employees, the employer can investigate computing assets at will without any privacy right restrictions; this practice applies in most countries. As a standard practice, companies should use both warning banners and policy statements. For example, if an incident is escalated to a criminal complaint, prosecutors prefer showing juries warning banners rather than a policy manual. A warning banner leaves a much stronger impression on a jury. In addition to making sure a company has a policy statement or a warning banner, corporate investigators should know under what circumstances they can examine an employee's computer. With a policy statement, an employer can freely initiate any inquiry necessary to protect the company or organization. However, every organization must also have a well-defined process describing when an investigation can be initiated. At a minimum, most corporate policies require that employers have a "reasonable suspicion" that a law or policy is being violated. For example, if a policy states that employees may not use company computers for outside business and a supervisor notices a change in work behavior that could indicate an employee is violating this rule, generally it's enough to warrant an investigation. Note that some countries require notifying employees that they're being investigated if they are suspected of criminal behavior at work.

If a corporate investigator finds that an employee is committing or has committed a crime, the employer can file a criminal complaint with the police. Some businesses, such as banks, have a regulatory requirement to report crimes. In the United States, the employer must turn over all evidence to the police for prosecution. If this evidence had been collected by a law enforcement officer, it would require a warrant, which would be difficult to obtain without sufficient probable cause. In "Processing Law Enforcement Crime Scenes," you learn more about probable cause and how it applies to a criminal investigation. Employers are usually interested in enforcing company policy, not seeking out and prosecuting employees, so typically they approve computer investigations only to identify employees who are misusing company assets. Corporate investigators are, therefore, primarily concerned with protecting company assets. Finding evidence of a criminal act during an investigation escalates the investigation from an internal civil matter to an external criminal complaint. If you discover evidence of a crime during a company policy investigation, first determine whether the incident meets the elements of criminal law. You might have to consult with your corporate attorney to determine whether the situation is a potential crime. Next, inform management of the incident; they might have other concerns, such as protecting confidential business data that might be included with the criminal evidence (referred to as "commingled data"). In this case, coordinate with management and the corporate attorney to determine the best way to protect commingled data. After you submit evidence containing sensitive information to the police, it becomes public record. Public record laws do include exceptions for protecting sensitive corporate information; ultimately, however, a judge decides what to protect.

After you discover illegal activity and document and report the crime, stop your investigation to make sure you don't violate Fourth Amendment restrictions on obtaining evidence. If the information you supply is specific enough to meet the criteria for a search warrant, the police are responsible for obtaining a warrant that requests any new evidence. If you follow police instructions to gather additional evidence without a search warrant after you have reported the crime, you run the risk of becoming an agent of law enforcement. Instead, consult with your corporate attorney on how to respond to a police request for information. The police and prosecutor

should issue a subpoena for any additional new evidence, which minimizes your exposure to potential civil liability. In addition, you should keep all documentation of evidence collected to investigate an internal company policy violation. Later in this section, you learn more about using affidavits in an internal investigation.

One example of a company policy violation involves employees observing another employee accessing pornographic Web sites. If your organization's policy requires you to determine whether any evidence supports this accusation, you could start by extracting log file data from the proxy server (used to connect a company LAN to the Internet) and conducting a forensic examination of the subject's computer. Suppose that during your examination, you find adult and child pornography. Further examination of the subject's hard disk reveals that the employee has been collecting child pornography in separate folders on his workstation's hard drive. In the United States, possessing child pornography is a crime under federal and state criminal statutes. These situations aren't uncommon and make life difficult for investigators who don't want to be guilty of possession of contraband, such as child pornography, on their forensic workstations.

You survey the remaining content of the subject's drive and find that he's a lead engineer for the team developing your company's latest high-tech bicycle. He placed the child pornography images in a subfolder where the bicycle plans are stored. By doing so, he has commingled contraband with the company's confidential design plans for the bicycle. Your discovery poses two problems in dealing with this contraband evidence. First, you must report the crime to the police; many states require reporting evidence of sexual exploitation of children. Second, you must also protect sensitive company information. Letting the high-tech bicycle plans become part of the criminal evidence might make it public record, and the design work will
then be available to competitors. Your first step is to ask your corporate attorney how to deal with the commingled contraband data and sensitive design plans. Your next step is to work with the corporate attorney to write an affidavit confirming your findings. The attorney should indicate in the affidavit that the evidence is commingled with company secrets and releasing the information will be detrimental to the company's financial health. When the affidavit is completed, you sign it before a notary, and then deliver the affidavit and the recovered evidence with log files to the police, where you make a criminal complaint. At the same time, the corporate attorney goes to court and requests that all evidence recovered from the hard disk that's not related to the complaint and is a company trade secret be protected from public viewing. You and the corporate attorney have reported the crime and taken steps to protect the sensitive data. Now suppose the detective assigned to the case calls you. In the evidence you've turned over to the police, the detective notices that the suspect is collecting most of his contrab and from e-mail attachments. The prosecutor instructed the detective to ask you to collect more evidence to determine whether the suspect is transmitting contraband pictures to other potential suspects. In this case, you should immediately inform the detective that collecting more evidence might make you an agent of law enforcement and violate the employee's Fourth Amendment rights. Before collecting any additional information, consult with your corporate attorney or wait until you receive a subpoena or other court order.

**Processing Law Enforcement Crime Scenes:**

To process a crime scene properly, you must be familiar with criminal rules of search and eizure. You should also understand how a search warrant works and what to do when you process one. For all criminal investigations in the United States, the Fourth Amendment limits how governments search and seize evidence. A law enforcement officer can search for and seize criminal evidence only with probable cause. Probable cause refers to the standard specifying whether a police officer has the right to make an arrest, conduct a personal or property search, or obtain a warrant for arrest. With probable cause, a police officer can obtain a search warrant from a judge that authorizes a

search and the seizure of specific evidence related to the criminal complaint.

The Fourth Amendment states that only warrants "particularly describing the place to be searched, and the persons or things to be seized" can be issued. Note that this excerpt uses the word "particularly." The courts have determined that this phrase means a warrant can authorize a search only of a specific place for a specific thing. Without specific evidence and the description of a particular location, a warrant might be weak and create problems later during prosecution. For example, stating that the evidence is in a house located on Elm Avenue between Broadway and Main Street is too general, unless only one house fits that description, because several houses might be located in that area. Instead, provide specific information, such as "123 Elm Avenue." Most courts have allowed more generality for computer evidence. For example, you can state that you want to seize a "computer" rather than specify a "Dell Optiplex GXA." Figure 5-4 shows sample search warrant language for computer evidence that the state of Maryland makes available for computer crime investigators (available at http://ccu.mdsp.org; do a search for guidelines on seizing digital evidence).

Although several court cases have allowed latitude when searching and seizing computer evidence, making your warrant as specific as possible to avoid challenges from defense attorneys is a good practice. Often a warrant is written and issued in haste because of the nature of the investigation. Law enforcement officers might not have the time to research the correct language for stating the nature of the complaint to meet probable cause requirements. However, because a judge can exclude evidence obtained from a poorly worded warrant, you should review these issues with your local prosecutor before investigating a case.

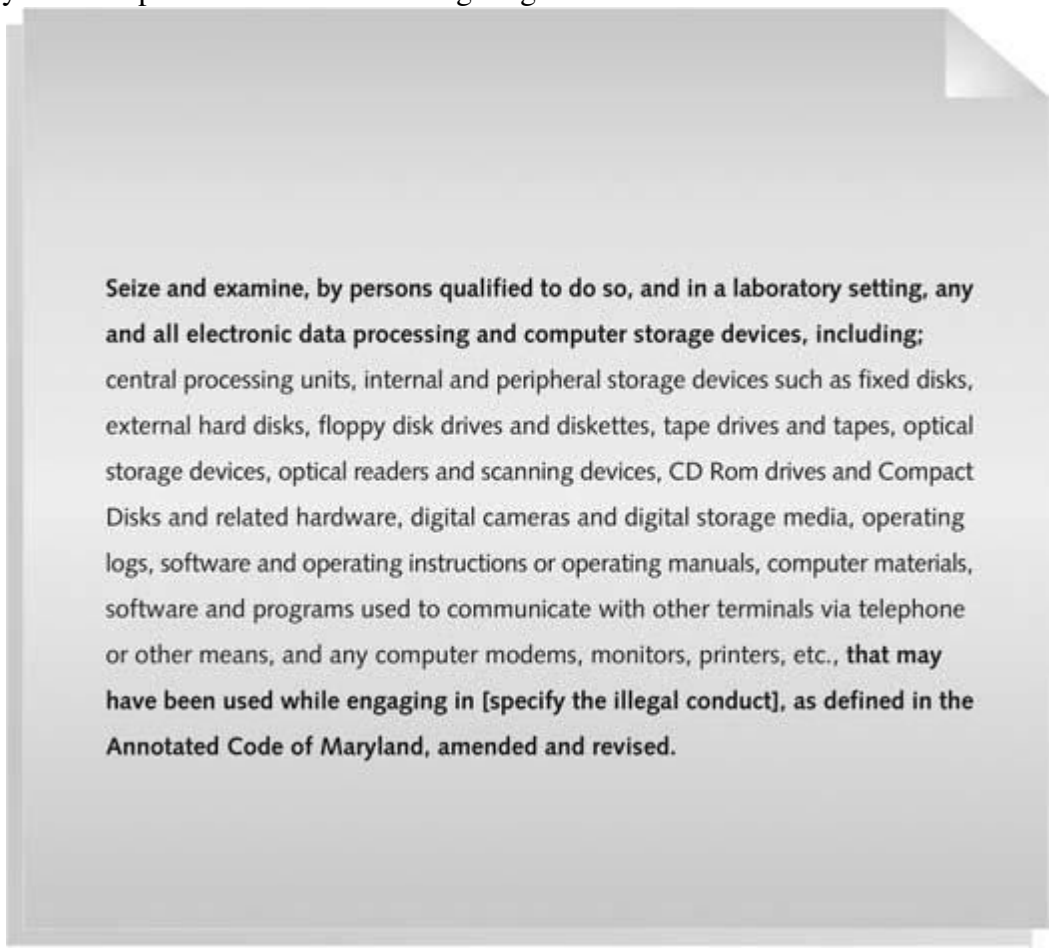



Figure 5-4 Sample search warrant wording for computer evidence

**Understanding Concepts and Terms Used in Warrants**

You should be familiar with warrant terminology that governs the type of evidence that can be seized. Many computing investigations involve large amounts of data you must sort through to find evidence; the Enron case, for example, involved terabytes of information. Unrelated information (referred to as innocent information) is often included with the evidence you're trying to recover. This unrelated information might be personal and private records of innocent people or confidential business information. When you find commingled evidence, judges often issue a limiting phrase to the warrant, which allows the police to separate innocent information from evidence. The warrant must list which items can be seized. When approaching or investigating a crime scene, you might find evidence related to the crime but not in the location the warrant specifies. You might also find evidence of another unrelated crime. In these situations, this evidence is subject to the plain view doctrine. The plain view doctrine states that objects falling in the direct sight of an officer who has the right to be in a location are subject to seizure without a warrant and can be introduced into evidence. For the plain view doctrine to apply, three criteria must be met:

- The officer is where he or she has a legal right to be.
    - Ordinary senses must not be enhanced by advanced technology.
    - Any discovery must be by chance.

For the officer to seize the item, he or she must have probable cause to believe the item is evidence of a crime or is contraband. In addition, the police aren't permitted to move objects to get a better view. In Arizona v. Hicks (480 U.S. 321, 1987), the officer was found to have acted unlawfully because he moved stereo equipment, without probable cause, to record the serial numbers. The plain view doctrine has also been expanded to include the sub doctrines of plain feel, plain smell, and plain hearing.

In Horton v. California (496 U.S. 128, 1990), the court eliminated the requirement that the discovery of evidence in plain view be inadvertent. Previously, "inadvertent discovery" was required, which led to difficulties in defining this term. The three-prong Horton test requires the following:

• The officer must be lawfully present at the place where the evidence can be plainly viewed.
• The officer must have a lawful right of access to the object.
• The incriminating character of the object must be "immediately apparent."

The plain view doctrine does not extend to supporting a general exploratory search from one object to another unless something incriminating is found (Coolidge v. New Hampshire, 403 U.S. 443, 466, 1971). The plain view doctrine's applicability in the digital forensics world is subject to development. Only the United States Court of Appeals for the Ninth Circuit has directly addressed this doctrine and has used it to give wide latitude to law enforcement (United States V. Wong, 334 F.3d 831, 9th Cir., 2003). Other circuit courts have been less willing to address
applying the doctrine to computer searches. For example, police investigating a case have a search warrant authorizing the search of a computer for evidence related to illegal drug trafficking, during the search, the examiner observes an .avi file, opens it, and sees that it's child pornography. At that point, he must get an additional warrant or an expansion of the existing warrant to continue the search for child pornography. This approach is consistent with rulings in United States v. Carey (172 F.3d 1268, 10th Cir., 1999) and United States v. Walser (275 F.3d 981, 10th Cir. 2001).

**Preparing for a Search**

Preparing for a computer search and seizure is probably the most important step in computing investigations. The better you prepare, the smoother your investigation will be. The following sections discuss the tasks you should complete before you search for evidence. To perform these

tasks, you might need to get answers from the victim (the complainant) and an informant, who could be a police detective assigned to the case, a law enforcement witness, or a manager or co-worker of the person of interest to the investigation.

**Identifying the Nature of the Case**

Recall from Chapter 2 that when you're assigned a computing investigation case, you start by identifying the nature of the case, including whether it involves the private or public sector. For example, a corporate investigation might involve an employee abusing Internet privileges by surfing the Web excessively or an employee who has filed an equal employment opportunity (EEO) or ethics complaint. Serious cases might involve an employee abusing company computing assets to acquire or deliver contraband. Law enforcement cases could range from a check fraud ring to a homicide. The nature of the case dictates how you proceed and what types of assets or resources you need to use in the investigation (discussed in more detail in "Determining the Tools You Need" later in this chapter).

**Identifying the Type of Computing System**

Next, determine the type of computing systems involved in the investigation. For law enforcement, this step might be difficult because the crime scene isn't controlled. You might not know what kinds of computers were used to commit a crime or how or where they were used. In this case, you must draw on your skills, creativity, and sources of knowledge, such as the Uniform Crime Report discussed in Chapter 3, to deal with the unknown. If you can identify the computing system, estimate the size of the drive on the suspect's computer and how many computers you have to process at the scene. Also, determine which OSs and hardware might be involved and whether the evidence is located on a Microsoft, Linux, UNIX, Macintosh, or mainframe computer. For corporate investigators, configuration management databases (discussed in Chapter 3) make this step easier. Consultants to the private sector or law enforcement officers might have to investigate more thoroughly to determine these details.

**Determining Whether You Can Seize a Computer**

Generally, the ideal situation for incident or crime scenes is seizing the computers and taking them to your lab for further processing. However, the type of case and location of the evidence determine whether you can remove computers from the scene. Law enforcement investigators need a warrant to remove computers from a crime scene and transport them to a lab.

If removing the computers will irreparably harm a business, the computers should not be taken offsite, unless you have disclosed the effect of the seizure to the judge. An additional complication is files stored offsite that are accessed remotely. You must decide whether the drives containing those files need to be examined. Another consideration is the availability of online data storage services that rent space, which essentially can't be located physically.

The data is stored on drives where data from many other subscribers might be stored. If you aren't allowed to take the computers to your lab, determine the resources you need to acquire digital evidence and which tools can speed data acquisition. With large drives, such as a 200 GB drive, acquisition times can increase to several hours. In Chapter 4, you examined data acquisition software and learned which tools meet specific needs for acquiring disk images. Some software, such as EnCase, compresses data while making forensic images. For large drives, this compression might be necessary.

**Obtaining a Detailed Description of the Location**

The more information you have about the location of a computer crime, the more efficiently you can gather evidence from a crime scene. Environmental and safety issues are the primary concerns during this process. Before arriving at an incident or crime scene, identify potential hazards to your safety as well as that of other examiners. Some computer cases involve dangerous settings, such as a drug bust of a methamphetamine lab or a terrorist attack using biological, chemical, or nuclear

contaminants. For these types of investigations, you must rely on the skills of hazardous materials (HAZMAT) teams to recover evidence from the scene. The recovery process might include decontaminating computing components needed for the investigation, if possible. If the decontamination procedure might destroy electronic evidence, a HAZMAT specialist or an investigator in HAZMAT gear should make an image of a suspect's drive. If you have to rely on a HAZMAT specialist to acquire data, coach the specialist on how to connect cables between the computer and drives and how to run the software. You must be exact and articulate in your instructions. Ambiguous or incorrect instructions could destroy evidence. Ideally, a computer forensics investigator trained in dealing with HAZMAT environments should acquire drive images. However, not all organizations have funds available for this training. Whether you or a HAZMAT technician is the one acquiring an image, you should keep some guidelines in mind. Before acquiring the data, a HAZMAT technician might suggest that you put the target drive in a special HAZMAT bag, leaving the IDE and power cables out of the bag but providing an airtight seal around the cables to prevent any contaminants from entering the bag and affecting the target drive. When the data acquisition is completed, power down the computer and then cut the IDE and power cables from the target drive. The HAZMAT technician can then decontaminate the bag. When dealing with extreme conditions, such as biological or chemical hazardous contaminants, you might have to sacrifice equipment, such as IDE and power cables, to accomplish a task. In certain instances, such as a meth lab bust, the contaminants might be so toxic that hazards to the safety of others prohibit acquiring any digital evidence.

In addition, if the temperature in the contaminated room is higher than 80 degrees, you should take measures to avoid damage to the drive from overheating. In a dry desert region, consider cooling the target drive by using sealed ice packs or double-wrapped bags of ice so that moisture doesn't leak out and damage the drive. In extreme conditions, consider the risks to evidence and your equipment. You'll need to brainstorm for solutions to overcome these problems. Moving the equipment to a controlled environment is ideal; however, doing so isn't always possible.

**Determining Who Is in Charge**

Corporate computing investigations usually require only one person to respond to an incident or crime scene. Processing evidence involves acquiring an image of a subject's drive. In law enforcement, however, many investigations require additional staff to collect all evidence quickly. For large-scale investigations, a crime or incident scene leader should be designated. Anyone assigned to a large-scale investigation scene should cooperate with the designated leader to ensure that the team addresses all details when collecting evidence.

**Using Additional Technical Expertise**

After you collect evidence data, determine whether you need specialized help to process the incident or crime scene. For example, suppose you're assigned to process a crime scene at a data center running Microsoft Windows servers with several RAID drives and high-end UNIX servers. If you're the leader of this investigation, you must identify the additional skills needed to process the crime scene, such as enlisting help with a high-end server OS. Other concerns are how to acquire data from RAID servers and how much data you can acquire. RAID servers typically process several terabytes of data, and standard imaging tools might not be able to handle these large data sets.

When working at high-end computing facilities, identify the applications the suspect uses, such as Oracle databases. You might need to recruit an Oracle specialist or site support staff to help extract data for the investigation. Finding the right person can be an even bigger challenge than conducting the investigation. If you do need to recruit a specialist who's not an investigator, develop a training program to educate the specialist in proper investigative techniques. This advice also applies to specialists you plan to supervise during search-and-seizure tasks. When dealing with computer evidence, an untrained specialist can easily and unintentionally destroy evidence, no

matter how careful you are in providing instructions and monitoring his or her activities.

**Determining the Tools You Need**

After you have gathered as much information as possible about the incident or crime scene, you can start listing what you need at the scene. Being overprepared is better than being underprepared, especially when you determine that you can't transfer the computer to your lab for processing.

To manage your tools, consider creating an initial-response field kit and an extensive response field kit. Using the right kit makes processing an incident or crime scene much easier and minimizes how much you have to carry from your vehicle to the scene. Your initial-response field kit should be lightweight and easy to transport. With this kit, you can arrive at a scene, acquire the data you need, and return to the lab as quickly as possible. Figure 5-5 shows some items you might need, and Table 5-1 lists the tools you might need in an initial-response field kit.


Figure 5-5 Items in an initial-response field kit

**Table 5-1 Tools in an initial-response field kit**

| Number needed | Tools |
|---|---|
| 1 | Small computer toolkit |
| 1 | Large-capacity drive |
| 1 | IDE ribbon cable (ATA-33 or ATA-100) |
| 1 | SATA cable |
| 1 | Forensic boot media containing your preferred acquisition utility |
| 1 | Laptop IDE 40- to 44-pin adapter, other adapter cables |
| 1 | Laptop computer |
| 1 | FireWire or USB dual write-protect external bay |
| 1 | Flashlight |
| 1 | Digital or 35mm camera with film and flash |
| 10 | Evidence log forms |
| 1 | Notebook or dictation recorder |
| 10 | Computer evidence bags (antistatic bags) |
| 20 | Evidence labels, tape, and tags |
| 1 | Permanent ink marker |
| 10 | External USB devices or a portable hard drive |

An **extensive-response** field kit should include all the tools you can afford to take to the field. When you arrive at the scene, you should extract only those items you need to acquire evidence. Doing so protects your equipment and minimizes how many items you have to keep track of at the scene. Table 5-2 lists the tools you might need in an extensive-response field kit, including external USB drives.

**Table 5-2 Tools in an extensive-response field kit**

| Number needed | Tools |
|---|---|
| Varies | Assorted technical manuals, ranging from OS references to forensics analysis guides |
| 1 | Initial-response field kit |
| 1 | Portable PC with SCSI card for DLT tape drive or suspect's SCSI drive |
| 2 | Electrical power strips |
| 1 | Additional hand tools, including bolt cutters, pry bar, and hacksaw |
| 1 | Leather gloves and disposable latex gloves (assorted sizes) |
| 1 | Hand truck and luggage cart |
| 10 | Large garbage bags and large cardboard boxes with packaging tape |
| 1 | Rubber bands of assorted sizes |

Table 5-2 Tools in an extensive-response field kit (*continued*)

| Number needed | Tools |
|---|---|
| 1 | Magnifying glass |
| 1 | Ream of printer paper |
| 1 | Small brush for cleaning dust from suspect's interior CPU cabinet |
| 10 | USB drives of varying sizes |
| 2 | External hard drives (200 GB or larger) with power cables |
| Assorted | Converter cables |
| 5 | Additional assorted hard drives for data acquisition |

When deciding what items to include in initial-response and extensive-response field kits, you need to analyze your specific needs in your region or organization. Refer to Tables 5-1 and 5-2 for guidelines.

**Preparing the Investigation Team**

Before you initiate the search and seizure of digital evidence at an incident or crime scene, you must review all the available facts, plans, and objectives with the investigation team you have assembled. The goal of scene processing is to collect and secure digital evidence successfully. The better prepared you are, the fewer problems you encounter when you carry out the plan to collect data. Keep in mind that digital evidence is volatile. Develop the skills to assess the facts quickly, make your plan, gather the needed resources, and collect data from the incident or crime scene. In some computing investigations, responding slowly might result in the loss of important evidence for the case.

**Securing a Computer Incident or Crime Scene**

Investigators secure an incident or crime scene to preserve the evidence and to keep information about the incident or crime confidential. Information made public could jeopardize the investigation. If you're in charge of securing a computer incident or crime scene, use yellow barrier tape to prevent bystanders from accidentally entering the scene. Use police officers or security guards to prevent others from entering the scene. Legal authority for a corporate incident scene includes trespassing violations; for a crime scene, it includes obstructing justice or failing to comply with a police officer. Access to the scene should be restricted to only those people who have a specific reason to be there. The reason for the standard practice of securing an incident or crime scene is to expand the area of control beyond the scene's immediate location. In this way, you avoid overlooking an area that might be part of the scene. Shrinking the scene's perimeter is easier than expanding it. For major crime scenes, computer investigators aren't usually responsible for defining a scene's security perimeter. These cases involve other specialists and detectives who are collecting physical evidence and recording the scene. For incidents primarily involving computers, the computers can be a crime scene within a crime scene, containing evidence to be processed. The evidence is in the computer, but the courts consider it physical evidence. Computers can also contain actual physical evidence, such as DNA evidence or fingerprints on keyboards. Crime labs can use special vacuums to extract DNA residue from a keyboard to compare with other DNA samples. In a major crime scene, law enforcement usually retains the keyboard. Evidence is commonly lost or corrupted because of professional curiosity, which involves police officers and other professionals who aren't part of the crime scene processing team.

They just have a compelling interest in seeing what happened. Their presence could contaminate the scene directly or indirectly. Keep in mind that even those authorized and trained to search crime

scenes can inadvertently alter the scene or evidence. For example, during one homicide investigation, the lead detective collected a good latent fingerprint from the crime scene. He compared it with the victim's fingerprints and those of others who knew the victim. He couldn't find a fingerprint matching the latent fingerprint from the scene. The detective suspected he had the murderer's fingerprint and kept it on file for several years until his police department purchased an Automated Fingerprint Identification Systems (AFIS) computer. During acceptance testing, the software vendor processed sample fingerprints to see how quickly and accurately the system could match fingerprints in the database. The detective asked the acceptance testing team to run the fingerprint he found at the homicide scene. He believed the suspect's fingerprints were in the AFIS database. The acceptance testing team complied and within minutes, AFIS found a near-perfect match of the latent fingerprint: It belonged to the detective. Always remember that professional curiosity can destroy or corrupt evidence, including digital evidence. When working at an incident or crime scene, be aware of what you're doing and what you have touched, physically or virtually. A police detective can take elimination prints of everyone who had access to the crime scene to identify the fingerprints of known people; computer evidence doesn't have an equivalent elimination process. You must protect all digital evidence, so make sure no one examines a suspect's computer before you can capture and preserve an image of the hard disk. Starting a computer without forensic boot media alters important data, such as the date and time stamps of last access to certain files.

**Seizing Digital Evidence at the Scene**

With proper search warrants, law enforcement can seize all computing systems and peripherals. In corporate investigations, you might have similar authority; however, you might have the authority only to make an image of the suspect's drive. Depending on company policies, corporate investigators rarely have the authority to seize all computers and peripherals. When seizing computer evidence in criminal investigations, follow the U.S. DOJ standards for seizing digital data (described later in this chapter, or see www.usdoj.gov/criminal/cybercrime/ searching.html). For civil investigations, follow the same rules of evidence as for criminal investigation. You might be looking for specific evidence, such a particular e-mail message or spreadsheet. In a criminal matter, investigators seize entire drives to preserve as much information as possible and ensure that no evidence is overlooked. If you have any questions, doubts, or concerns, consult with your attorney for additional guidance. Preparing to Acquire Digital Evidence The evidence you acquire at the scene depends on the nature of the case and the alleged crime or violation. For a criminal case involving a drug dealer's computer, for example, you need to take the entire computer along with any peripherals and media in the area, including cell phones, USB devices, CDs, DVDs, printers, cameras, and scanners. Seizing peripherals and other media ensures that you leave no necessary system components behind; often, predicting what components might be critical to the system's operation is difficult. On the other hand, if you're investigating employee misconduct, you might need only a few specific items. Before you collect digital evidence, ask your supervisor or senior forensics examiner in the organization the following questions:

• Do you need to take the entire computer and all peripherals and media in the immediate area? How are you going to protect the computer and media while transporting them to your lab?

• Is the computer powered on when you arrive? (This question is discussed in more detail later in "Processing an Incident or Crime Scene.")

• Is the suspect you're investigating in the immediate area of the computer? Is it possible the suspect damaged or destroyed the computer, peripherals, or media?

Will you have to separate the suspect from the computer?

For example, suppose a company employee, Edward Braun, is suspected of using a company computer at his desk to write a book. You suspect that Edward is saving personal files on the computer's hard drive. Using imaging software, such as Norton Ghost from Symantec, you can copy

the hard drive onto another drive, install the duplicate hard drive in the computer, and take the original drive to your forensics lab for examination. This procedure doesn't create a bit-for-bit copy; you're creating a working copy for continued business operations and taking the original for examination. Because Edward's supervisors don't want him to know he's being investigated, you must create the working copy when he's not at his desk and isn't expected to return. Because most people notice when something is out of order on their desks, you should photograph the scene, measure the height of his chair, and record the position of items on his desk you need to move before removing the hard drive. (The following section has more tips on photographing and documenting the scene.) After you create an image of his hard drive and substitute the copy, return Edward's belongings to their original locations.

**Processing an Incident or Crime Scene**

The following guidelines offer suggestions on how to process an incident or crime scene. As you gain experience in performing searches and seizures, you can add to or modify these guidelines to meet the needs of specific cases. Use your judgment to determine what steps to take when processing a civil or criminal investigation. For any difficult issues, seek out legal counsel or other technical experts. Keep a journal to document your activities. Include the date and time you arrive on the scene, the people you encounter, and notes on every important task you perform. Update the journal as you process the scene. To secure the scene, use whatever is practical to make sure that only authorized people can access the area. Remove anyone who isn't investigating the scene unless you need his or her help to process the scene. For example, the company's network administrator might need to help you collect and recover data. As mentioned earlier, you should secure a wider scene perimeter than necessary. Make sure nothing in this area, including computer evidence, moves until you have had time to record it. Be professional and courteous to any curious onlookers, but don't offer information about the investigation or incident or answer questions. Refer journalists to a public information officer or the organization's public relations manager.

Take video and still recordings of the area around the computer. Start by recording the overall scene, and then record details with close-up shots, including the back of all computers. Before recording the back of each computer, place numbered or lettered labels on each cable to help identify which cable is connected to which plug, in case you need to reassemble components at the lab. Make sure you take close-ups of all cable connections, including keyloggers (devices used to record keystrokes) and dongle devices used with software as part of the licensing agreement. Record the area around the computer, including the floor and ceiling, and all access points to the computer, such as doors and windows. Be sure to look under any tables or desks for anything taped to the underside of a table or desk drawer or on the floor out of view. If the area has ceiling panels—false ceiling tiles—remove them and record that area, too. Slowly pan or zoom the camera to prevent blurring in the video image, and maintain a camera log for all shots you take. When you finish videotaping or photographing the scene, sketch the incident or crime scene. This sketch is usually a rough draft with notes on objects' dimensions and distances between fixed objects. For example, a note might read "The suspect's computer is on the south wall, three meters from the southeast corner of the room." When you prepare your report, you can make a clean, detailed drawing from your sketch, preferably using a computer drawing program so that the sketch is in electronic form.

Because computer data is volatile, check the state of each computer at the scene as soon as possible. Determine whether the computer is powered on or off or in hibernation or sleep mode. If it's off, leave it off. If it's on, use your professional judgment on what to do next. Standard computer forensics practice has been to kill the computer's power to make sure data doesn't become corrupt through covert means. Typically, this procedure is still acceptable on legacy Windows and MS-DOS systems because turning off the power usually preserves data. On Windows XP/Vista, UNIX, and Linux computers, generally you should perform an orderly shutdown first. Every shutdown process

has inherent risks, however; to avoid data loss, you or your supervisor might have to determine the best shutdown procedure. In addition, there are many urban legends about criminals placing self-destruct mechanisms both hardware and software devices—in computers. Many years ago, a common trick was altering the DOS program Command.com by changing the Dir (directory) command to the Deltree (delete the directory tree) command. When an investigator entered the Dir command on a suspect's computer, he would inadvertently start the Deltree command, which deletes all files and folders and their contents. More advanced computer criminals have been known to create similar command-altering methods that overwrite a drive's contents. In addition, computer owners who suspect someone will investigate their computers might set the computer to delete the hard drive's contents if the correct screensaver password isn't entered. As a general rule, don't cut electrical power to a running system unless it's an older Windows 9x or MS-DOS system. However, it's a judgment call because of recent trends in computer crimes. More computing investigations now revolve around network- and Internet-related cases, which rely heavily on log file data. Certain files, such as the Event log and Security log in Windows XP, might lose essential network activity records if power is terminated without a proper shutdown.

If you're working on a network or Internet investigation and the computer is on, save data in any current applications as safely as possible and record all active windows or shell sessions. Don't examine folders or network connections or press any keys unless it's necessary. For systems that are powered on and running, photograph the screens. If windows are open but minimized, expanding them so that you can photograph them is safe. As a precaution, write down the contents of each window. As you're copying data on a live suspect computer, make notes in your journal about everything you do so that you can explain your actions in your formal report to prosecutors and other attorneys. When you've finished recording screen contents, save them to external media. For example, if one screen shows a Word file, save it to an external drive. Keep in mind that the suspect might have changed the file since last using the Save command. If another screen is a Web browser, take a screenshot or save the Web page to a USB drive or an external hard drive. If the suspect computer has an active connection to a network server with enough storage, you can save large files to a folder on the server. To do so, you need
the cooperation of the network administrator to help direct you to the correct server and folder for storing the file. If you can't save an open application to external media, save the open application to the suspect drive with a new filename. Changing the filename avoids overwriting an existing file that might not have been updated already. This method isn't ideal and should be done only in extreme emergency conditions. Remember that your goal is to preserve as much evidence in as good a condition as is practical. After you have saved all active files on the suspect computer, you can close all applications. If an application prompts you to save before closing, don't save the files. When all applications are closed, perform an orderly shutdown. If you're not familiar with the correct shutdown method for the computer you're examining, consult someone who has expertise in this procedure. After you record the scene and shut down the system, bag and tag the evidence, following these steps:

1. Assign one person, if possible, to collect and log all evidence. Minimize the number of people handling evidence to ensure its integrity.
2. Tag all the evidence you collect with the current date and time, serial numbers or unique features, make and model, and name of the person who collected it.
3. Maintain two separate logs of collected evidence to be reconciled for audit control purposes and to verify everything you have collected.
4. Maintain constant control of the collected evidence and the crime or incident scene.

If the nature of the case doesn't permit you to seize the computer, create an image of the hard drive, as you learned in Chapter 4.

During the data acquisition or immediately after collecting the evidence, look for information related to the investigation, such as passwords, passphrases, personal identification numbers (PINs), and bank account numbers (particularly offshore bank accounts, often used to hide evidence of financial transactions). This information might be in plain view or out of sight in a drawer or trash can. At the scene, collect as much personal information as possible about the suspect or victim. Collect all information related to facts about the crime or incident, particularly anything that connects the suspect to the victim. To complete your analysis and processing of a scene, collect all documentation and media related to the investigation, including the following material:

- Hardware, including peripheral devices
- Software, including OSs and applications
- All media, such as backup tapes and disks
- All documentation, manuals, printouts, and handwritten notes

**Processing Data Centers with RAID Systems**

Computer investigators sometimes perform forensics analysis on RAID systems or server farms, which are rooms filled with extremely large disk systems and are typical of large business data centers, such as the Department of Motor Vehicles (DMV), banks, insurance companies, and ISPs. As you learned in Chapter 4, one technique for extracting evidence from large systems is called sparse acquisition. This technique extracts only data related to evidence for your case from allocated files and minimizes how much data you need to analyze. A drawback of this technique is that it doesn't recover data in free or slack space. If you have a computer forensics tool that accesses unallocated space on a RAID system, work with the tool on a test system first to make sure it doesn't corrupt the RAID system.

**Using a Technical Advisor**

When working with advanced technologies, recruit a technical advisor who can help you list the tools you need to process the incident or crime scene. At large data centers, the technical advisor is the person guiding you about where to locate data and helping you extract log records or other evidence from large RAID servers. In law enforcement cases, the technical advisor can help create the search warrant by itemizing what you need for the warrant. If you use a technical advisor for this purpose, you should list his or her name in the warrant. At the scene, a technical advisor can help direct other investigators to collect evidence correctly. Technical advisors have the following responsibilities:

- Know all aspects of the system being seized and searched.
- Direct investigators on how to handle sensitive media and systems to prevent damage.
- Help ensure security of the scene.
- Help document the planning strategy for the search and seizure.
- Conduct ad hoc training for investigators on the technologies and components being seized and searched.
- Document activities during the search and seizure.
- Help conduct the search and seizure.

**Documenting Evidence in the Lab**

After you collect digital evidence at the scene, you transport it to a forensics lab, which should be a controlled environment that ensures the security and integrity of digital evidence. In any investigative work, be sure to record your activities and findings as you work. To do so, you can maintain a journal to record the steps you take as you process evidence. Your goal is to be able to reproduce the same results when you or another investigator repeat the steps you took to collect evidence. If you get different results when you repeat the steps, the credibility of your evidence becomes questionable. At best, the evidence's value is compromised; at worst, the evidence will be disqualified. Because of the nature of electronic components, failures do occur. For example, you

might not be able to repeat a data recovery because of a hardware failure, such as a disk drive head crash. Be sure to report all facts and events as they occur. Besides verifying your work, a journal serves as a reference that documents the methods you used to process digital evidence. You and others can use it for training and guidance on other investigations.

**Processing and Handling Digital Evidence**

You must maintain the integrity of digital evidence in the lab as you do when collecting it in the field. Your first task is to preserve the disk data. If you have a suspect computer that hasn't been copied with an imaging tool, you must create a copy. When you do, be sure to make the suspect drive read-only (typically by using a write-blocking device), and document this step. If the disk has been copied with an imaging tool, you must preserve the image files. With most imaging tools, you can create smaller, compressed volume sets to make archiving your data easier. In Chapter 4, you learned how to use imaging tools, and in Chapter 2, you examined the steps for preserving digital evidence with chain-of-custody controls. You use the following steps to create image files:

1. Copy all image files to a large drive. Most forensics labs have several machines set up with disk-imaging software and multiple hard drives that can be exchanged as needed for your cases. You can use these resources to copy image files to large drives. Some might be equipped with large network storage devices for ongoing cases.
2. Start your forensics tool to analyze the evidence.
3. Run an MD5 or SHA-1 hashing algorithm on the image files to get a digital hash. Later in "Obtaining a Digital Hash," you learn how to compare MD5 or SHA-1 hashes to make sure the evidence hasn't changed.
4. When you finish copying image files to a larger drive, secure the original media in an evidence locker. Don't work with the original media; it should be stored in a locker that has an evidence custody form. Be sure to fill out the form and date it.

## UNIT-3

**Create and manage shared folders using operating system**

**Definition:** Operating System Forensics is the process of retrieving useful information from the Operating System (OS) of the computer or mobile device in question. The aim of collecting this information is to acquire empirical evidence against the perpetrator.

What are the types of Operating systems?

The most popular types of Operating Systems are Windows, Linux, Mac, iOS, and Android.

**Windows**

Windows is a widely used OS designed by Microsoft. The file systems used by Windows include FAT, exFAT, NTFS, and ReFS. Investigators can search out evidence by analyzing the following important locations of the Windows:

**Recycle Bin**: This holds files that have been discarded by the user. When a user deletes files, a copy of them is stored in recycle bin. This process is called "Soft Deletion." Recovering files from recycle bin can be a good source of evidence.

**Registry:** Windows Registry holds a database of values and keys that give useful pieces of information to forensic analysts. For example, see the table below that provides registry keys and associated files that encompasses user activities on the system.

**Thumbs.db Files:** These have images' thumbnails that can provide relevant information.
**Browser History:** Every Web Browser generates history files that contain significant information. Microsoft Windows Explorer is the default web browser for Windows OSs. However, some other supported browsers are Opera, Mozilla Firefox, Google Chrome, and Apple Safari.
**Print Spooling:** This process occurs when a computer prints files in a Windows environment. When a user sends a print command from a computer to the printer, the print spooling process creates a "print job" to some files that remain in the queue unless the print operation is completed successfully. Moreover, the printer configuration is required to be set in either EMF mode or RAW mode. In a RAW mode, the print job merely provides a straight graphic dump of itself, whereas with an EMF mode, the graphics are converted into the EMF image format (Microsoft Enhanced Metafile). These EMF files can be indispensable and can provide an empirical evidence for forensic purposes. The path to EMF files is:For Windows NT and2000: Winntsystem32spoolprintersFor Windows XP/2003/Vista/2008/7/8/10: Windowssystem32spoolprintersOS forensic tools can automatically detect the path; there is no need to define it manually.

**importance of the forensic mindset**

An organization can carry out digital investigations on its own whereby evidence is not going to court, such as for employee monitoring (where that is considered acceptable). Such a case may not necessarily require handling the evidence in a legally acceptable manner (chain of custody), but there is the possibility that such investigations could open a can of worms: Something that requires legal action may be uncovered (e.g., sabotage, fraud). In such a case, evidence being presented in court must be collected and documented in a legally acceptable manner for admissibility. Digital forensics can also be used for audit investigations and can be very useful when investigating fraud. Auditors can use forensic tools and techniques to monitor and review compliance with organizational policies and regulatory requirements. For example, digital forensics can help discover and trace unauthorized Internet access by employees, loopholes and vulnerabilities in the network, and malware incidents such as attacks and intrusions can be analyzed to determine how the breach occurred to prevent future attacks. Having a forensic readiness plan in place goes a long way toward ensuring such investigations and any discovery therein can be handled and presented so that the organization does not lose a case.

**Define the workload of law enforcement**

**Law enforcement** is the activity of some members of government who act in an organized manner to enforce the law by discovering, deterring, rehabilitating, or punishing people who violate the rules and norms governing that society. The term encompasses police, courts, and corrections. These three components may operate independently of each other or collectively, through the use of record sharing and mutual cooperation.

Modern state legal codes use the term peace officer, or law enforcement officer, to include every person vested by the legislating state with police power or authority, traditionally, anyone "sworn or badged, who can arrest any person for a violation of criminal law, is included under the umbrella term of law enforcement.

Although law enforcement may be most concerned with the prevention and punishment of crimes, organizations exist to discourage a wide variety of non-criminal violations of rules and norms, effected through the imposition of less severe consequences such as probation.

Law enforcement agencies

Most law enforcement is conducted by some type of law enforcement agency, with the most typical agency fulfilling this role being a police force. Social investment in enforcement through such organizations can be massive, both in terms of the resources invested in the activity, and in the number of people professionally engaged to perform those functions.

Law enforcement agencies tend to be limited to operating within a specified jurisdiction. In some cases, jurisdiction may overlap in between organizations; for example, in the United States, each state has its own statewide law enforcement arms, but the Federal Bureau of Investigation is able to act against certain types of crimes occurring in any state. Various segments of society may have their own specialist law enforcement organizations. For example, military organizations may have military police. Some segments of society, such as private companies that are responsible for significant and critical infrastructure, may have their own law enforcement agencies. For example, in the United States, the protection of the Union Pacific Railroad network is carried out by the Union Pacific Police Department.

Depending on a variety of factors, such as whether an agency is autonomous or dependent on other organizations for its operations, the governing body that funds and oversees the agency may decide to dissolve or consolidate operations. Dissolution of an agency may occur when the governing body or the department itself decides to end operations. This can occur due to multiple reasons, including police reform, a lack of population in the jurisdiction, or because of mass resignations.

According to the International Association of Chiefs of Police, agency consolidation can occur to improve efficiency, consolidate resources, and when forming a new type of government.

Until today, law enforcement department professions are dominantly served by Caucasian males in America, even with a growing number of organizations emphasizing on recruitment of females and minorities.

**TYPES OF EVIDENCE:**

1. ANALOGICAL EVIDENCE
2. ANECDOTAL EVIDENCE
3. CHARACTER EVIDENCE
4. CIRCUMSTANTIAL EVIDENCE
5. DEMONSTRATIVE EVIDENCE
6. DIGITAL EVIDENCE
7. DIRECT EVIDENCE
8. DOCUMENTARY EVIDENCE
9. EXCULPATORY EVIDENCE
10. FORENSIC EVIDENCE

11. HEARSAY EVIDENCE

12. PHYSICAL EVIDENCE

13. PRIMA FACIE EVIDENCE

14. STATISTICAL EVIDENCE

15. TESTIMONIAL EVIDENCE

**Define who should be notified of a crime**

Serving notice is critical in legal proceedings. Due process requires that legal action cannot be taken against anyone unless the requirements of notice and an opportunity to be heard are observed. Legal proceedings are initiated by providing notice to the party concerned. If an individual is accused of a crime, he has a right to be notified of the charges. In addition, formal papers must be prepared to give the accused notice of the charges. An individual who is being sued in a civil action must be provided with notice of the nature of the suit.

As per Section 27 of the General Clauses Act, 1897, service of notice can be presumed in respect of a letter containing a document which was addressed prepaid and posted by registered post. In Alavi Haji's case, the full bench of the Supreme Court has held that when the notice was sent by registered post by correctly addressing the drawer of the cheque, the mandatory requirement of issue of notice in terms of clause (b) of proviso to Section 138 of the Act stands complied with.

In a case before the High Court, the accused person borrowed a sum of Rs 1.5 lakh from another person (complainant) for his urgent necessities and executed a bond in favour of the latter agreeing to repay the debt amount with interest. After few months the accused issued a cheque for Rs 1.25 lakh towards part payment of the total debt.

When the said cheque was presented in the bank, the same was dishonoured due to insufficient funds. Therefore, the complainant issued legal notice to the accused and the same was returned with postal acknowledgement that the "addressee is continuously absent, hence sent to the sender".

**Not maintainable**

When a complaint was lodged, the magistrate concerned took cognizance of it against the accused for the offence under Section 138 of Negotiable Instruments Act, 1881 and registered the case. Though it was held that there was no material alteration with regard to date in the bond paper as alleged and that cheque was issued by the accused to discharge the legally enforceable debt, the trial court dismissed the complaint on the ground that complainant could not prove issuance of statutory notice under Section 138(b) of NI Act and therefore, complaint was not maintainable and accordingly, acquitted the accused. Aggrieved with the same, the complainant filed an appeal before the High Court.

The counsel for the appellant/complainant told the High Court that the address mentioned in the registered postal cover, the address mentioned in the complaint as well as address mentioned in the summons sent to the accused was one and the same. The accused earlier received the court summons and appeared and contested the criminal case. Whereas the notice was returned with the endorsement "addressee is continuously absent for seven days, hence returned to the sender".

Therefore, it is evident that though the accused was a resident of the same address for long, he managed it to see that the notice cover was not served on him and returned to the complainant. In

those circumstances, the trial court ought to have drawn a presumption that notice was duly served on the accused. When the complainant was able to establish that the statutory notice under the Act was sent to the correct address of the accused, a presumption can be drawn that the notice has been received by the accused in spite of the fact that it was not actually received by him, he argued. Service of notice

After hearing the case and perusing the material on record, the HC found that the accused had earlier received the court summons and appeared and contested the criminal case. Hence, the complainant could establish that the statutory notice under Section 138(b) of NI Act was sent to the accused to the correct address. Therefore, service of the notice to the accused can be presumed under Section 27 of General Clauses Act, 1897, the court noted.

Relying on the Apex Court judgment in N Parameswaran Unni's case, the High Court said it was clear that in the instant case service of notice on accused was a presumed fact, which was not rebutted by the accused. Hence, the mandatory requirement under Section 138(b) of NI Act was amply complied with. In such circumstances, the finding of the trial court that the complainant could not serve the notice under the Act on accused is unsustainable, the Court observed.

The High Court allowed the appeal by setting aside the order of the trial court and convicted the accused for the offence under Sec 138 of NI Act. The court directed the accused to pay a fine of Rs 1.5 lakh and on deposit of the fine amount, the same should be paid to the appellant/complainant as compensation.

**parts of gathering evidence.**

Evidence that May be Gathered Digitally

Computer documents, emails, text and instant messages, transactions, images and Internet histories are examples of information that can be gathered from electronic devices and used very effectively as evidence. For example, mobile devices use online-based based backup systems, also known as the "cloud", that provide forensic investigators with access to text messages and pictures taken from a particular phone. These systems keep an average of 1,000– 1,500 or more of the last text messages sent to and received from that phone. In addition, many mobile devices store information about the locations where the device traveled and when it was there. To gain this knowledge, investigators can access an average of the last 200 cell locations accessed by a mobile device. Satellite navigation systems and satellite radios in cars can provide similar information. Even photos posted to social media such as Facebook may contain location information. Photos taken with a Global Positioning System (GPS)-enabled device contain file data that shows when and exactly where a photo was taken. By gaining a subpoena for a particular mobile device account, investigators can collect a great deal of history related to a device and the person using it.

## UNIT – IV

**Computer Forensics**: Preparing a computer case investigation, Procedures for corporate hi-tech investigations, conducting an investigation, Complete and critiquing the case.

**Network Forensics:** Overview of network forensics, open-source security tools for network forensic analysis

**Preparing a computer case investigation:**

Your role as a computer forensics professional is to gather evidence from a suspect's computer and determine whether the suspect committed a crime or violated a company policy. If the evidence suggests that a crime or policy violation has been committed, you begin to prepare ase, which is a collection of evidence you can offer in court or at a corporate inquiry. This process involves investigating the suspect's computer and then preserving the evidence on a different computer. Before you begin investigating, however, you must follow an accepted procedure to prepare a case. By approaching each case methodically, you can evaluate the evidence thoroughly and document the chain of evidence, or chain of custody, which is the route the evidence takes from the time you find it until the case is closed or goes to court. The following sections present two sample cases—one involving a computer crime and another involving a company policy violation. Each example describes the typical steps of a forensics investigation, including gathering evidence, preparing a case, and preserving the evidence.

**An Overview of a Computer Crime**

Law enforcement officers often find computers and computer components as they're investigating crimes, gathering other evidence, or making arrests. Computers can contain information that helps law enforcement officers determine the chain of events leading to a crime or information providing evidence that's more likely to lead to a conviction. As an example of a case in which computers were involved in a crime, the police raided a suspected drug dealer's home and found a computer, several floppy disks and USB drives (also called keychain drives or memory sticks), a personal digital assistant (PDA), and a cell phone in a bedroom (see Figure 2-1). The computer was "bagged and tagged," meaning it was placed in evidence bags along with the storage media and then labeled with tags as part of the search and seizure.

Figure 2-1 The crime scene

The lead detective on the case wants you to examine the computer to find and organize data that could be evidence of a crime, such as files containing names of the drug dealer's contacts. The acquisitions officer gives you documentation of items the investigating officers collected with the

computer, including a list of other storage media, such as removable disks and CDs. The acquisitions officer also notes that the computer is a Windows XP system, and the machine was running when it was discovered. Before shutting down the computer, the acquisitions officer photographs all open windows on the Windows desktop, including one showing Windows Explorer, and gives you the photos. (Before shutting down the computer, a live acquisition should be done to capture RAM, too. This procedure is discussed in Chapter 11.)

As a computer forensics investigator, you're grateful the officers followed proper procedure when acquiring the evidence. With digital evidence, it's important to realize how easily key data, such as the last access date, can be altered by an overeager investigator who's first on the scene. The U.S. Department of Justice (DOJ) has a document you can download that reviews proper acquisition of electronic evidence, including the search and seizure of computers (www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm). If this link has changed because of site updates, use the search feature. In your preliminary assessment, you assume that the hard disk and storage media include intact files, such as e-mail messages, deleted files, and hidden files. A range of software is available for use in your investigation; your office uses the tool Technology Pathways Pro Discover After your preliminary assessment, you identify the potential challenges in this case. Because drug dealers don't usually make information about their accomplices available, the files on the disks you received are probably password protected. You might need to acquire password-cracking software or find an expert who can help you decrypt a file. Later, you perform the steps needed to investigate the case, including how to address risks and obstacles. Then you can begin the actual investigation and data retrieval.

**An Overview of a Company Policy Violation:**

Companies often establish policies for employee use of computers. Employees surfing the Internet, sending personal e-mail, or using company computers for personal tasks during work hours can waste company time. Because lost time can cost companies millions of dollars, computer forensics specialists are often used to investigate policy violations. The following example describes a company policy violation.

Manager Steve Billings has been receiving complaints from customers about the job performance of one of his sales representatives, George Montgomery. George has worked as a representative for several years. He's been absent from work for two days but hasn't called in sick or told anyone why he wouldn't be at work. Another employee, Martha, is also missing and hasn't informed anyone of the reason for her absence. Steve asks the IT Department to confiscate George's hard drive and all storage media in his work area. He wants to know whether there's any information on George's computer and storage media that might offer a clue to George's whereabouts and job performance concerns. To help determine George and Martha's whereabouts, you must take a systematic approach, described in the following section, to examining and analyzing the data found on George's desk.

## Procedures for Corporate High-Tech Investigations

As an investigator, you need to develop formal procedures and informal checklists to cover all issues important to high-tech investigations. These procedures are necessary to ensure that correct techniques are used in an investigation. Use informal checklists to be certain that all evidence is collected and processed properly. This section lists some sample procedures that computing investigators commonly use in corporate high-tech investigations.

Employee Termination Cases The majority of investigative work for termination cases involves employee abuse of corporate assets. Incidents that create a hostile work environment, such as

viewing pornography in the workplace and sending inappropriate e-mail messages, are the predominant types of cases investigated. The following sections describe key points for conducting an investigation that might lead to an employee's termination. Consulting with your organization's general counsel and Human Resources Department for specific directions on how to handle these investigations is recommended. Your organization must have appropriate policies in place, as described in Chapter 1.

**Internet Abuse Investigations**

The information in this section applies to an organization's internal private network, not a public ISP. Consult with your organization's general counsel after reviewing this list, and make changes according to their directions to build your own procedures. To conduct an investigation involving Internet abuse, you need the following:

• The organization's Internet proxy server logs
• Suspect computer's IP address obtained from your organization's network administrator
• Suspect computer's disk drive
• Your preferred computer forensics analysis tool (ProDiscover, Forensic Toolkit, EnCase, X-Ways Forensics, and so forth)

The following steps outline the recommended processing of an Internet abuse case:

1. Use the standard forensic analysis techniques and procedures described in this book for the disk drive examination.
2. Using tools such as DataLifter or Forensic Toolkit's Internet keyword search option, extract all Web page URL information.
3. Contact the network firewall administrator and request a proxy server log, if it's available, of the suspect computer's network device name or IP address for the dates of interest. Consult with your organization's network administrator to confirm that these logs are maintained and how long the time to live (TTL) is set for the network's IP address assignments that use Dynamic Host Configuration Protocol (DHCP).
4. Compare the data recovered from forensic analysis to the proxy server log data to confirm that they match.
5. If the URL data matches the proxy server log and the forensic disk examination, continue analyzing the suspect computer's drive data, and collect any relevant downloaded inappropriate pictures or Web pages that support the allegation. If there are no matches between the proxy server logs, and the forensic examination shows no contributing evidence, report that the allegation is unsubstantiated. Before investigating an Internet abuse case, research your state or country's privacy laws. Many countries have unique privacy laws that restrict the use of computer log data, such as proxy server logs or disk drive cache files, for any type of investigation. Some state or federal laws might supersede your organization's employee policies. Always consult with your organization's attorney. For companies with international business operations, jurisdiction is a problem; what is legal in the United States, such as examining and investigating a proxy server log, might not be legal in Germany, for example. For investigations in which the proxy server log doesn't match the forensic analysis that found inappropriate data, continue the examination of the suspect computer's disk drive. Determine when inappropriate data was downloaded to the computer and whether it was through an organization's intranet connection to the Internet. Employees might have used their employer's laptop computers to connect to their own ISPs to download inappropriate Web content. For these situations, you need to consult your organization's employee policy guidelines for what's considered appropriate use of the organization's computing assets.

**E-mail Abuse Investigations**

E-mail investigations typically include spam, inappropriate and offensive message content, and harassment or threats. E-mail is subject to the same restrictions as other computer evidence data, in

that an organization must have a defined policy, as described in Chapter 1. The following list is what you need for an investigation involving e-mail abuse:
• An electronic copy of the offending e-mail that contains message header data; consult with your e-mail server administrator
• If available, e-mail server log records; consult with your e-mail server administrator to see whether they are available
• For e-mail systems that store users' messages on a central server, access to the server; consult with your e-mail server administrator
• For e-mail systems that store users' messages on a computer as an Outlook .pst or .ost file, for example, access to the computer so that you can perform a forensic analysis on it
• Your preferred computer forensics analysis tool, such as Forensic Toolkit or ProDiscover This is the recommended procedure for e-mail investigations:
1. For computer-based e-mail data files, such as Outlook .pst or .ost files, use the standard forensic analysis techniques and procedures described in this book for the drive examination.
2. For server-based e-mail data files, contact the e-mail server administrator and obtain an electronic copy of the suspect and victim's e-mail folder or data.
3. For Web-based e-mail investigations, such as Hotmail or Gmail, use tools such as Forensic Toolkit's Internet keyword search option to extract all related e-mail address information.

4. Examine header data of all messages of interest to the investigation.

**Attorney-Client Privilege Investigations**
When conducting a computer forensics analysis under attorney-client privilege (ACP) rules for an attorney, you must keep all findings confidential. The attorney you're working for is the ultimate authority over the investigation. For investigations of this nature, attorneys typically request that you extract all data from drives. It's your responsibility to comply with the attorney's directions. Because of the large quantities of data a drive can contain, the attorney will want to know about everything of interest on the drives. Many attorneys like to have printouts of the data you have recovered, but printouts can present problems when you have log files with several thousand pages of data or CAD drawing programs that can be read only by proprietary programs. You need to persuade and educate many attorneys on how digital evidence can be viewed electronically. In addition, learn how to teach attorneys and paralegals to sort through files so that you can help them efficiently analyze the huge amount of data a forensic examination produces.
You can also encounter problems if you find data in the form of binary files, such as CAD drawings. Examining these files requires using the CAD program that created them. In addition, engineering companies often have specialized drafting programs. Discovery demands for lawsuits involving a product that caused injury or death requires extracting design plans for attorneys and expert witnesses to review. You're responsible for locating the programs for these design plans so that attorneys and expert witnesses can view the evidence files.
The following list shows the basic steps for conducting an ACP case:
1. Request a memorandum from the attorney directing you to start the investigation. The memorandum must state that the investigation is privileged communication and list your name and any other associates' names assigned to the case.
2. Request a list of keywords of interest to the investigation.
3. After you have received the memorandum, initiate the investigation and analysis. Any findings you made before receiving the memorandum are subject to discovery by the opposing attorney.
4. For drive examinations, make two bit-stream images (discussed later in this chapter) of the drive using a different tool for each image, such as EnCase for the first and ProDiscover or SafeBack for the second. If you have large enough storage drives, make each bit-stream image uncompressed so

that if it becomes corrupt, you can still examine uncorrupted areas with your preferred forensic analysis tool.
5. If possible, compare hash values on all files on the original and re-created disks. Typically, attorneys want to view all data, even if it's not relevant to the case. Many GUI forensics tools perform this task during bit-stream imaging of the drive.
6.Methodically examine every portion of the drive (both allocated and unallocated data areas) and extract all data.
7. Run keyword searches on allocated and unallocated disk space. Follow up the search results to determine whether the search results contain information that supports the case.
8. For Windows OSs, use specialty tools to analyze and extract data from the Registry, such as AccessData Registry Viewer or a Registry viewer program (discussed in more detail in Chapter 6). Use the Edit, Find menu option in Registry Editor, for example, to search for keywords of interest to the investigation.
9. For binary files such as CAD drawings, locate the correct program and, if possible, make printouts of the binary file content. If the files are too large, load the specialty program on a separate workstation with the recovered binary files so that the attorney can view them.
10. For unallocated data (file slack space or free space, explained in Chapter 6) recovery, use a tool that removes or replaces nonprintable data, such as X-Ways Forensics Specialist Gather Text function.
11. Consolidate all recovered data from the evidence bit-stream image into wellorganized folders and subfolders. Store the recovered data output, using a logical and easy-to-follow storage method for the attorney or paralegal.
Here are some other guidelines to remember for ACP cases:
• Minimize all written communication with the attorney; use the telephone when you need to ask questions or provide information related to the case.
• Any documentation written to the attorney must contain a header stating that it's "Privileged Legal Communication—Confidential Work Product," as defined under the attorney-work-product rule.
• Assist the attorney and paralegal in analyzing the data. If you have difficulty complying with the directions or don't understand the directives from the memorandum, contact the attorney and explain the problem. Always keep an open line of verbal communication with the attorney during these types of investigations. If you're communicating via e-mail, use encryption (such as PGP) or another secure e-mail service for all messages.

**Media Leak Investigations**

In the corporate environment, controlling sensitive data can be difficult. Disgruntled employees, for example, might send an organization's sensitive data to a news reporter. The reasons for media leaks range from employees' efforts to embarrass management to a rival conducting a power struggle between other internal organizations. Another concern is the premature release of information about new products, which can disrupt operations and cause market share loss for a business if the information is made public too soon. Media leak investigations can be time consuming and resource intensive. Because management wants to find who leaked information, scope creep during the investigation is not uncommon. Consider the following guidelines for media leak investigations:
• Examine e-mail, both the organization's e-mail servers and private e-mail accounts (Hotmail, Yahoo!, Gmail, and so on), on company-owned computers. Examine Internet message boards, and search the Internet for any information about the company or product. Use Internet search engines to run keyword searches related to the company, product, or leaked information. For example, you might search for "graphite-composite bicycle sprocket" for a bicycle manufacturer that was the victim of a media leak about a new product in development.
• Examine proxy server logs to check for log activities that might show use of free e-mail services,

such as Gmail. Track back to the specific workstations where these messages originated and perform a forensic analysis on the drives to help determine what was communicated.
• Examine known suspects' workstations, perform computer forensics examinations on persons of interest, and develop other leads on possible associates.
• Examine all company phone records for any calls to known media organizations. The following list outlines steps to take for media leaks:
1. Interview management privately to get a list of employees who have direct knowledge of the sensitive data.
2. Identify the media source that published the information.
3. Review company phone records to see who might have had contact with the news service.
4. Obtain a list of keywords related to the media leak.
5. Perform keyword searches on proxy and e-mail servers.
6. Discreetly conduct forensic disk acquisitions and analysis of employees of interest.
7. From the forensic disk examinations, analyze all e-mail correspondence and trace any sensitive messages to other people who haven't been listed as having direct knowledge of the sensitive data. Expand the discreet forensic disk acquisition and analysis for any new persons of interest.
9. Consolidate and review your findings periodically to see whether new clues can be discovered.
10. Report findings to management routinely, and discuss how much further to continue the investigation. Industrial Espionage Investigations Industrial espionage cases, similar to media leaks, can be time consuming and are subject to the same scope creep problems. This section offers some guidelines on how to deal with industrial espionage investigations. Be aware that cases dealing with foreign nationals might be violations of International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). For more information on ITAR, see the U.S. Department of State's Web site (www.state.gov; substitute the actual state name or a shortened version of it for state) or do an Internet search for "International Traffic in Arms Regulations." For EAR information, see the U.S. Department of Commerce Web site (www.doc.gov) or do an Internet search for "Export Administration Regulations." Unlike the other corporate investigations covered in this section, all suspected industrial espionage cases should be treated as criminal investigations. The techniques described here are for private network environments and internal investigations that haven't yet been reported to law enforcement officials. Make sure you don't become an agent of law enforcement by filing a complaint of a suspected espionage case before substantiating the allegation. The following list includes staff you might need when planning an industrial espionage investigation. This list isn't exhaustive, so use your knowledge to improve on these recommendations:
• The computing investigator who is responsible for disk forensic examinations
• The technology specialist who is knowledgeable about the suspected compromised technical data
• The network specialist who can perform log analysis and set up network monitors to trap network communication of possible suspects
• The threat assessment specialist (typically an attorney) who is familiar with federal and state laws and regulations related to ITAR or EAR and industrial espionage In addition, consider the following guidelines when initiating an international espionage investigation:
• Determine whether this investigation involves a possible industrial espionage incident, and then determine whether it falls under ITAR or EAR.
• Consult with corporate attorneys and upper management if the investigations must be conducted discreetly.
• Determine what information is needed to substantiate the allegation of industrial espionage.
• Generate a list of keywords for disk forensics and network monitoring.
• List and collect resources needed for the investigation.

• Determine the goal and scope of the investigation; consult with management and the company's attorneys on how much work you should do.
• Initiate the investigation after approval from management, and make regular reports of your activities and findings.
The following are planning considerations for industrial espionage investigations:
• Examine all e-mail of suspected employees, both company-provided e-mail and free Web-based services.
• Search Internet newsgroups or message boards for any postings related to the incident.
• Initiate physical surveillance with cameras on people or things of interest to the investigation.
• If available, examine all facility physical access logs for sensitive areas, which might include secure areas where smart badges or video surveillance recordings are used.
• If there's a suspect, determine his or her location in relation to the vulnerable asset that was compromised.
• Study the suspect's work habits.
• Collect all incoming and outgoing phone logs to see whether any unique or unusual places were called.
When conducting an industrial espionage case, follow these basic steps:
1. Gather all personnel assigned to the investigation and brief them on the plan and any concerns.
2. Gather the resources needed to conduct the investigation.
3. Start the investigation by placing surveillance systems, such as cameras and network monitors, at key locations.
4. Discreetly gather any additional evidence, such as the suspect's computer drive, and make a bit-stream image for follow-up examination.
5. Collect all log data from networks and e-mail servers, and examine them for unique items that might relate to the investigation.
6. Report regularly to management and corporate attorneys on your investigation's status and current findings.
7. Review the investigation's scope with management and corporate attorneys to determine whether it needs to be expanded and more resources added.

**Interviews and Interrogations in High-Tech Investigations**

Becoming a skilled interviewer and interrogator can take many years of experience. Typically, a corporate computing investigator is a technical person acquiring the evidence for an investigation. Many large organizations have full-time security investigators with years of training and experience in criminal and civil investigations and interviewing techniques. Few of these investigators have any computing or network technical skills, so you might be asked to assist in interviewing or interrogating a suspect when you have performed a forensic disk analysis on that suspect's machine. An interrogation is different from an interview. An interview is usually conducted to collect information from a witness or suspect about specific facts related to an investigation. An interrogation is the process of trying to get a suspect to confess to a specific incident or crime. An investigator might change from an interview to an interrogation when talking to a witness or suspect. The more experience and training investigators have in the art of interviewing and interrogating, the more easily they can determine whether a witness is credible and possibly a suspect.
Your role as a computing investigator is to instruct the investigator conducting the interview on what questions to ask and what the answers should be. As you build rapport with the investigator, he or she might ask you to question the suspect. Watching a skilled interrogator is a learning experience in human relations skills. If you're asked to assist in an interview or interrogation, prepare yourself by answering the following questions:

- What questions do I need to ask the suspect to get the vital information about the case?
    - Do I know what I'm talking about, or will I have to research the topic or technology related to the investigation?
    - Do I need additional questions to cover other indirect issues related to the investigation?

Common interview and interrogation errors include being unprepared for the interview or interrogation and not having the right questions or enough questions to increase your depth of knowledge. Make sure you don't run out of conversation topics; you need to keep the conversation friendly to gain the suspect's confidence. Avoid doubting your own skills, which might show the suspect you lack confidence in your ability. Ingredients for a successful interview or interrogation require the following:
• Being patient throughout the session
• Repeating or rephrasing questions to zero in on specific facts from a reluctant witness or suspect

• Being tenacious

**Conducting an Investigation**
Now you're ready to return to the Domain Name case. You have created a plan for the investigation, set up your forensic workstation, and installed the necessary forensic analysis software you need to examine the evidence. The type of software to install includes your preferred analysis tool, such as ProDiscover, EnCase, FTK, or X-Ways Forensics; an office suite, such as OpenOffice; and a graphics viewer, such as IrfanView. To begin conducting an investigation, you start by copying the evidence using a variety of methods. No single method retrieves all data from a disk, so using several tools to retrieve and analyze data is a good idea. Start by gathering the resources you identified in your investigation plan. You need the following
items:
• Original storage media
• Evidence custody form
• Evidence container for the storage media, such as an evidence bag
• Bit-stream imaging tool; in this case, the ProDiscover Basic acquisition utility
• Forensic workstation to copy and examine the evidence

• Secure evidence locker, cabinet, or safe

**Gathering the Evidence**
Now you're ready to gather evidence for the Domain Name case. Remember, you need antistatic bags and pads with wrist straps to prevent static electricity from damaging digital evidence. To acquire George Montgomery's storage media from the IT Department and then secure the evidence, you perform the following steps:
1. Arrange to meet the IT manager to interview him and pick up the storage media.
2. After interviewing the IT manager, fill out the evidence form, have him sign it, and then sign it yourself.
3. Store the storage media in an evidence bag, and then transport it to your forensic facility.
4. Carry the evidence to a secure container, such as a locker, cabinet, or safe.
5. Complete the evidence custody form. As mentioned, if you're using a multi-evidence form, you can store the form in the file folder for the case. If you're also using single-evidence forms, store them in the secure container with the evidence. Reduce the risk of tampering by limiting access to the forms.

6. Secure the evidence by locking the container. Understanding Bit-stream Copies

A bit-stream copy is a bit-by-bit copy (also known as a sector copy) of the original drive or storage medium and is an exact duplicate. The more exact the copy, the better chance you have of retrieving the evidence you need from the disk. This process is usually referred to as "acquiring an image" or "making an image" of a suspect drive. A bit-stream copy is different from a simple backup copy of a disk. Backup software can only copy or compress files that are stored in a folder or are of a known file type. Backup software can't copy deleted files and e-mails or recover file fragments. A bit-stream image is the file containing the bit-stream copy of all data on a disk or disk partition. For simplicity, it's usually referred to as an "image," "image save," or "image file." Some manufacturers also refer to it as a forensic copy. To create an exact image of an evidence disk, copying the image to a target disk that's identical to the evidence disk is preferable (see Figure 2-4). The target disk's manufacturer and model, in general, should be the same as the original disk's manufacturer and model. If the target disk is identical to the original, the size in bytes and sectors of both disks should also be the same. Some image acquisition tools can accommodate a target disk that's a different size than the original. These imaging tools are discussed in Chapter 4. Older computer forensics tools designed for MS-DOS
work only on a copied disk. Current GUI tools can work on both a disk drive and copied data sets that many manufacturers refer to as "image saves."

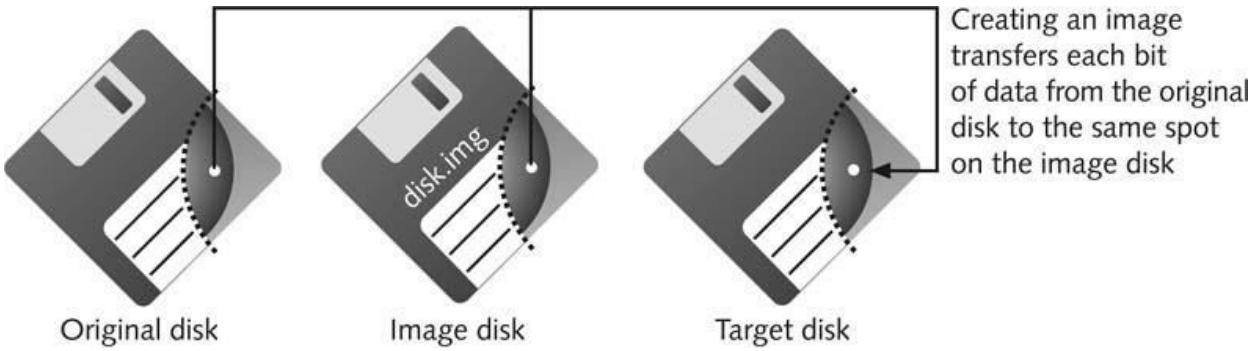



Figure 2-4 Transfer of data from original to image to target

**Acquiring an Image of Evidence Media**

After you retrieve and secure the evidence, you're ready to copy the evidence media and analyze the data. The first rule of computer forensics is to preserve the original evidence. Then conduct your analysis only on a copy of the data—the image of the original medium. Several vendors provide MS-DOS, Linux, and Windows acquisition tools. Windows tools, however, require a write-blocking device (discussed in Chapter 4) when acquiring data from FAT or NTFS file systems.

**Using ProDiscover Basic to Acquire a USB Drive**

ProDiscover Basic from Technology Pathways is a forensics analysis tool. You can use it to acquire and analyze data from several different file systems, such as Microsoft FAT and NTFS, Linux Ext2 and Ext3, and other UNIX file systems, from a Windows XP or older OS. To use ProDiscover Basic in Windows Vista, you need to run it in Administrator mode. See the Tip in the following steps for instructions on selecting this mode. Before starting this activity, you need to create a work folder on your computer for data storage and other related files ProDiscover creates when acquiring and analyzing evidence. You can use any location and name for your work folder, but you'll see it

referred to in activities as C:\Work or simply "your work folder." To keep your files organized, you should also create subfolders for each chapter. For this chapter, create a Work\Chap02\Chapter folder to store files from in-chapter activities. Note that you might see work folder pathnames in screenshots that are slightly different from your own pathname. The following steps show how to acquire an image of a USB drive, but you can apply them to other media, such as disk drives and floppy disks. You can use any USB drive already containing files to see how ProDiscover acquires data. To perform an acquisition on a USB drive
with ProDiscover Basic, follow these steps:

1. First, on the USB drive, locate the write-protect switch (if one is available) and place the drive in write-protect mode. Now connect the USB drive to your computer.
2. To start ProDiscover Basic, click Start, point to All Programs, point to ProDiscover, and click ProDiscover Basic. If the Launch Dialog dialog box opens (see Figure 2-5), click Cancel.

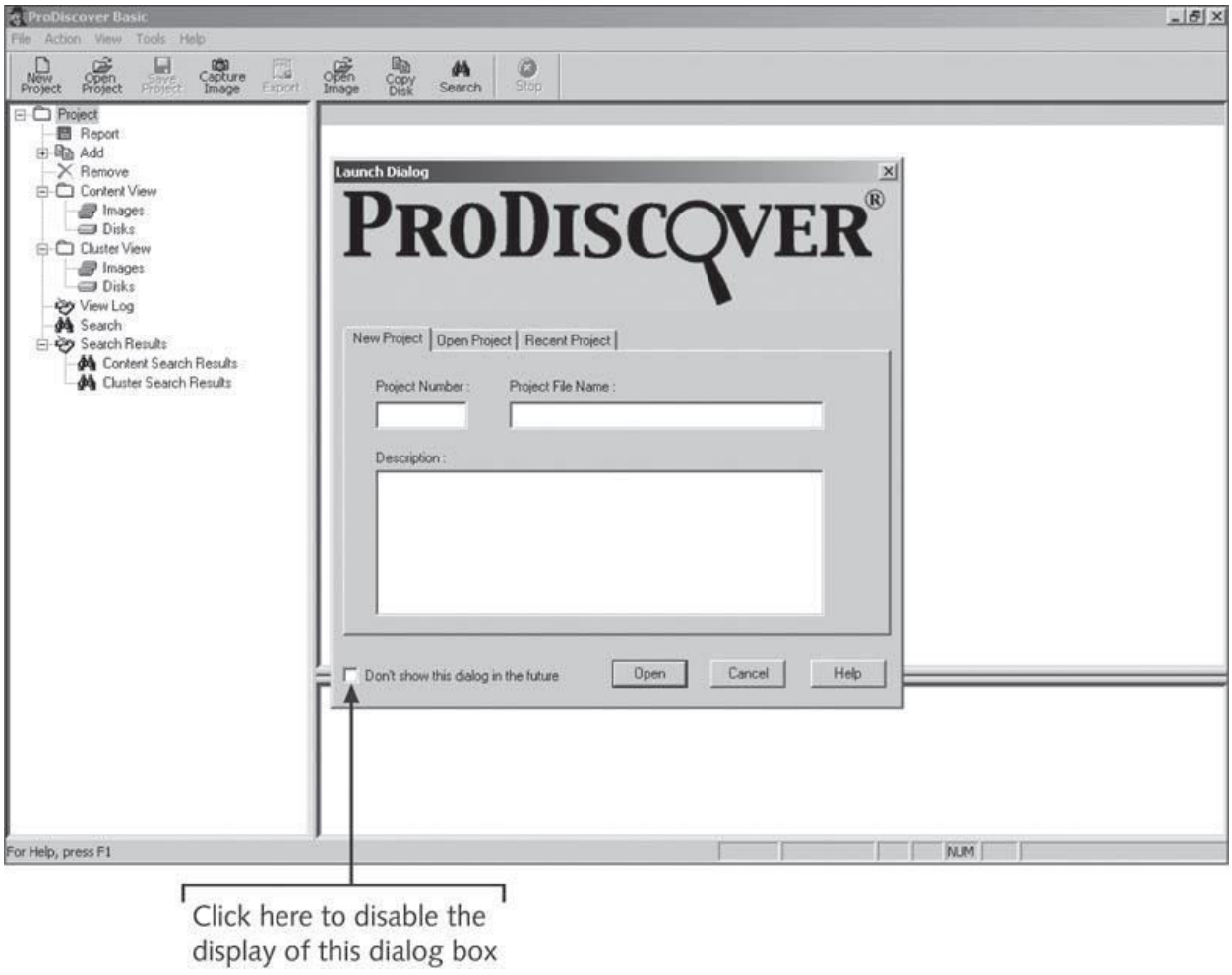



Figure 2-5 The main window in ProDiscover

3.In the main window, click Action, Capture Image from the menu.
4. In the Capture Image dialog box shown in Figure 2-6, click the Source Drive list

arrow, and select the USB drive.

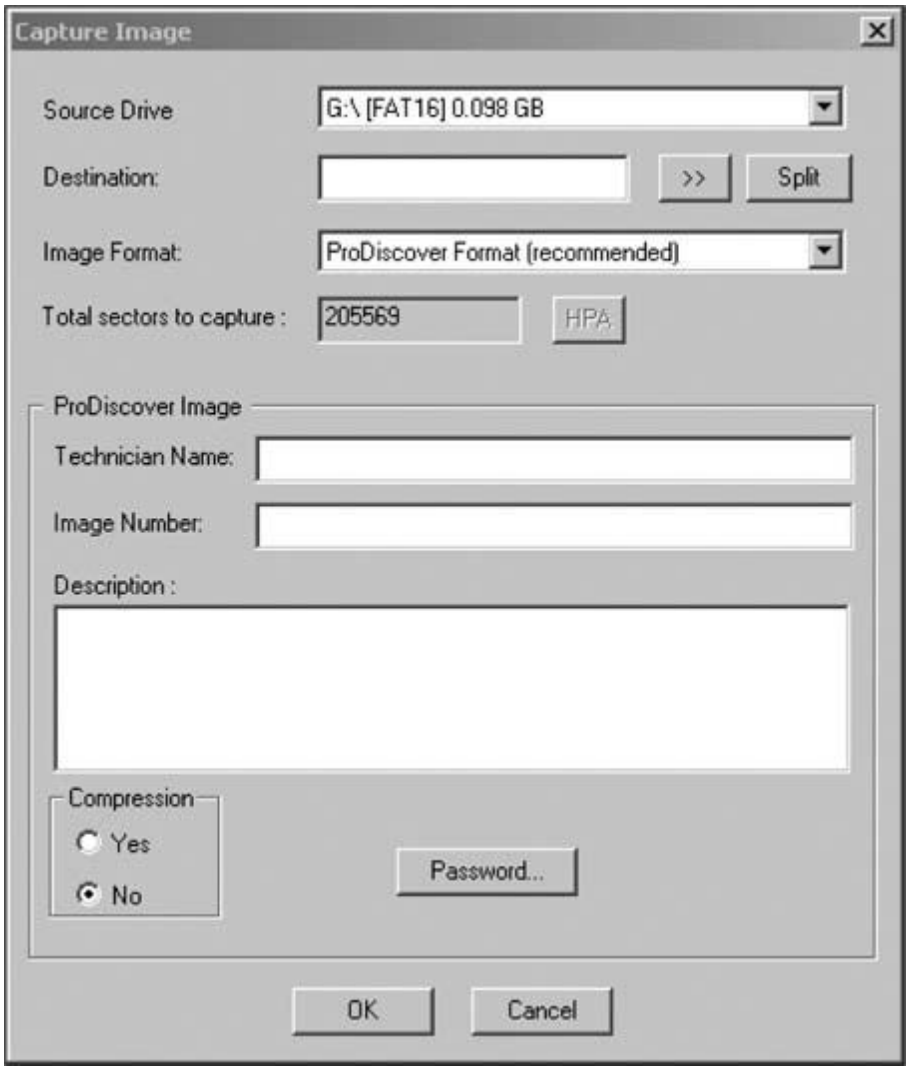



Figure 2-6 The Capture Image dialog box

5. Click the >> button next to the Destination text box. When the Save As dialog box opens, navigate to your work folder (Work\Chap02\Chapter) and enter a name for the image you're making, such as InChp-prac. Click Save to save the file.
6. Next, in the Capture Image dialog box, type your name in the Technician Name text box and InChp-prac-02 in the Image Number text box (see Figure 2-7). Click OK.
7. When ProDiscover is finished, click OK in the completion message box. Click File, Exit from the menu to exit ProDiscover.

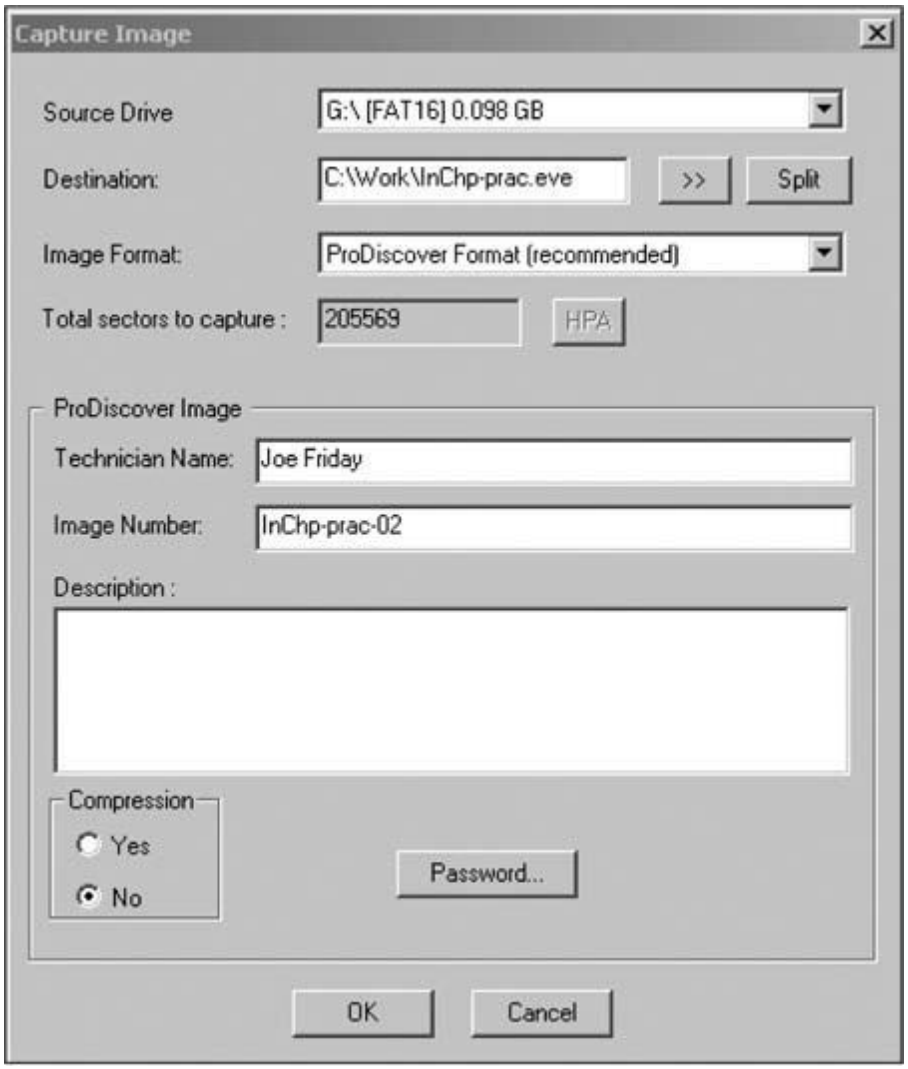



Figure 2-7 The completed Capture Image dialog box

This activity completes your first forensics data acquisition. Next, you learn how to locate data in an acquisition.

**Analyzing Your Digital Evidence**

When you analyze digital evidence, your job is to recover the data. If users have deleted or overwritten files on a disk, the disk contains deleted files and file fragments in addition to existing files. Remember that as files are deleted, the space they occupied becomes free space—meaning it can be used for new files that are saved or files that expand as data is added to them. The files that were deleted are still on the disk until a new file is saved to the same physical location, overwriting the original file. In the meantime, those files can still be retrieved. Forensics tools such as ProDiscover Basic can retrieve deleted files for use as evidence.

In the following steps, you analyze George Montgomery's USB drive. Before beginning, extract all compressed files from the Chap02 folder on the book's DVD to your work folder. The first task is loading the acquired image into ProDiscover Basic by following these steps:

1. Start ProDiscover Basic, as you did in the previous activity.
2. To create a new case, click File, New Project from the menu.
3. In the New Project dialog box, type InChp02 in the Project Number text box and again in the Project File Name text box (see Figure 2-8), and then click OK.

4. In the tree view of the main window (see Figure 2-9), click to expand the Add item and then click Image File.

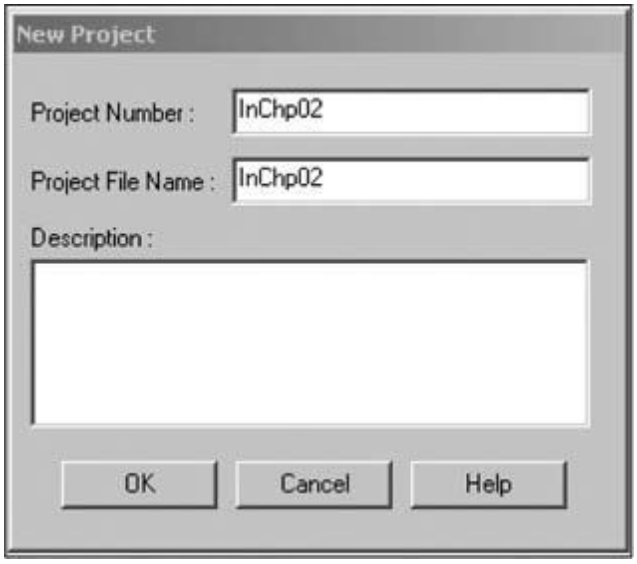



Figure 2-8 The New Project dialog box

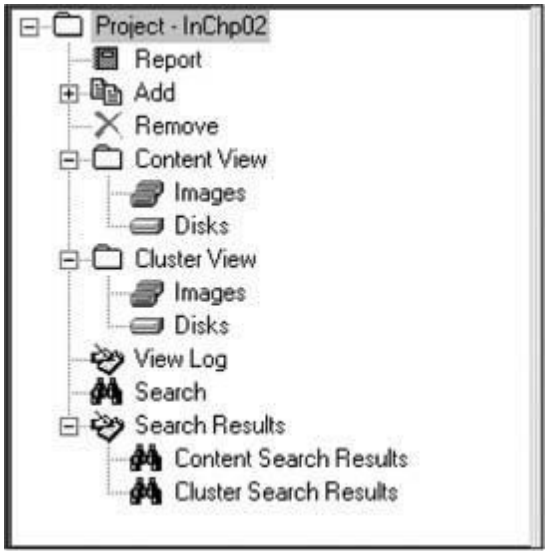



Figure 2-9 The tree view in ProDiscover

5. In the Open dialog box, navigate to the folder containing the image, click the InChp02.eve file, and click Open. Click Yes in the Auto Image Checksum message box, if necessary. The next task is to display the contents of the acquired data. Perform the following steps:

1. In the tree view, click to expand Content View, if necessary. Click to expand Images, click the image filename path C:\Work\InChp02.eve (substituting your folder path for "Work"—for example, C:\Work\Chap02\Chapter), and then click to expand the path.
2. Next, click All Files under the image filename path. When the CAUTION dialog box opens, click Yes. The InChp02.eve file is then loaded in the main window, as shown in Figure 2-10.
3. In the upper-right pane (the work area), click the letter1 file to view its content in the data area (see Figure 2-11).
4. In the data area, you see the contents of the letter1 file. Continue to navigate through the work and

data areas and inspect the contents of the recovered evidence. Note that many of these files are deleted files that haven't been overwritten. Leave ProDiscover Basic running for the next activity.

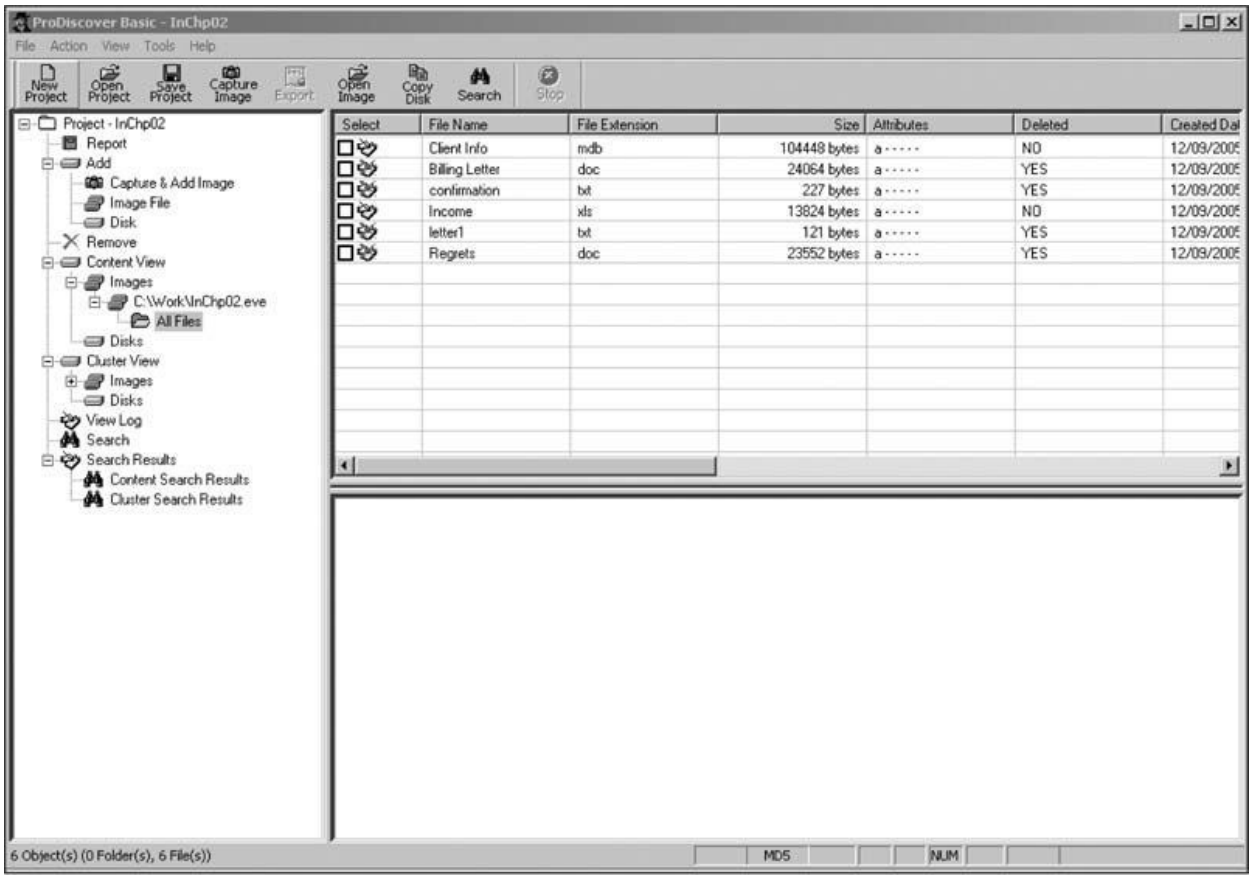



Figure 2-10 The loaded InChp02.eve file

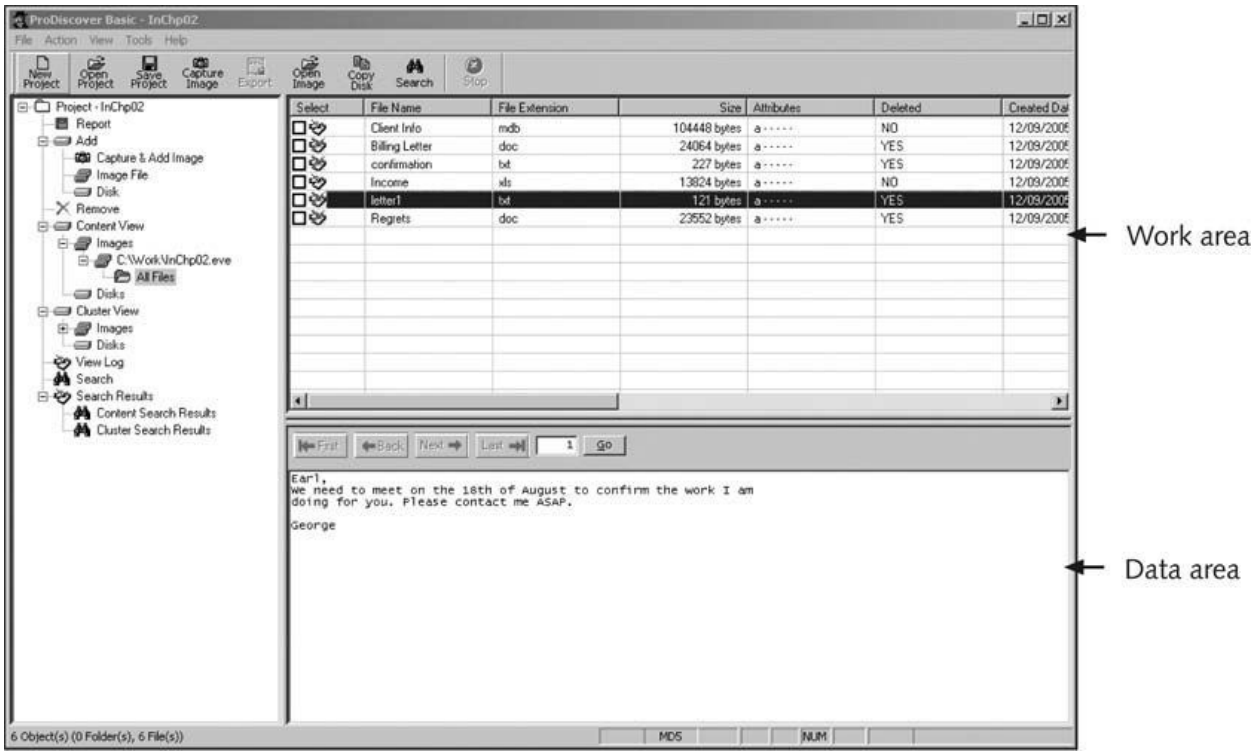



Figure 2-11 Selecting a file in the work area and viewing its contents in the data area

The next step is analyzing the data and searching for information related to the complaint. Data analysis can be the most time-consuming task, even when you know exactly what to look for in the evidence. The method for locating evidentiary artifacts is to search for specific known data values. Data values can be unique words or nonprintable characters, such as hexadecimal codes. There are also printable character codes that can't be generated from a keyboard, such as the copyright (©) or registered trademark (™) symbols. Many computer forensics programs can search for character strings (letters and numbers) and hexadecimal values, such as A9 for the copyright symbol or AE for the registered trademark symbol. All these searchable data values are referred to as "keywords." With ProDiscover Basic, you can search for keywords of interest in the case. For this case, follow these steps to search for any reference to the name George:

1. In the tree view, click Search.
2. In the Search dialog box, click the Content Search tab, if necessary. Click the Select all matches check box, the ASCII option button, and the Search for the pattern(s) option button, if they aren't already selected.
3. Next, in the text box under the Search for the pattern(s) option button, type George (see Figure 2-12).

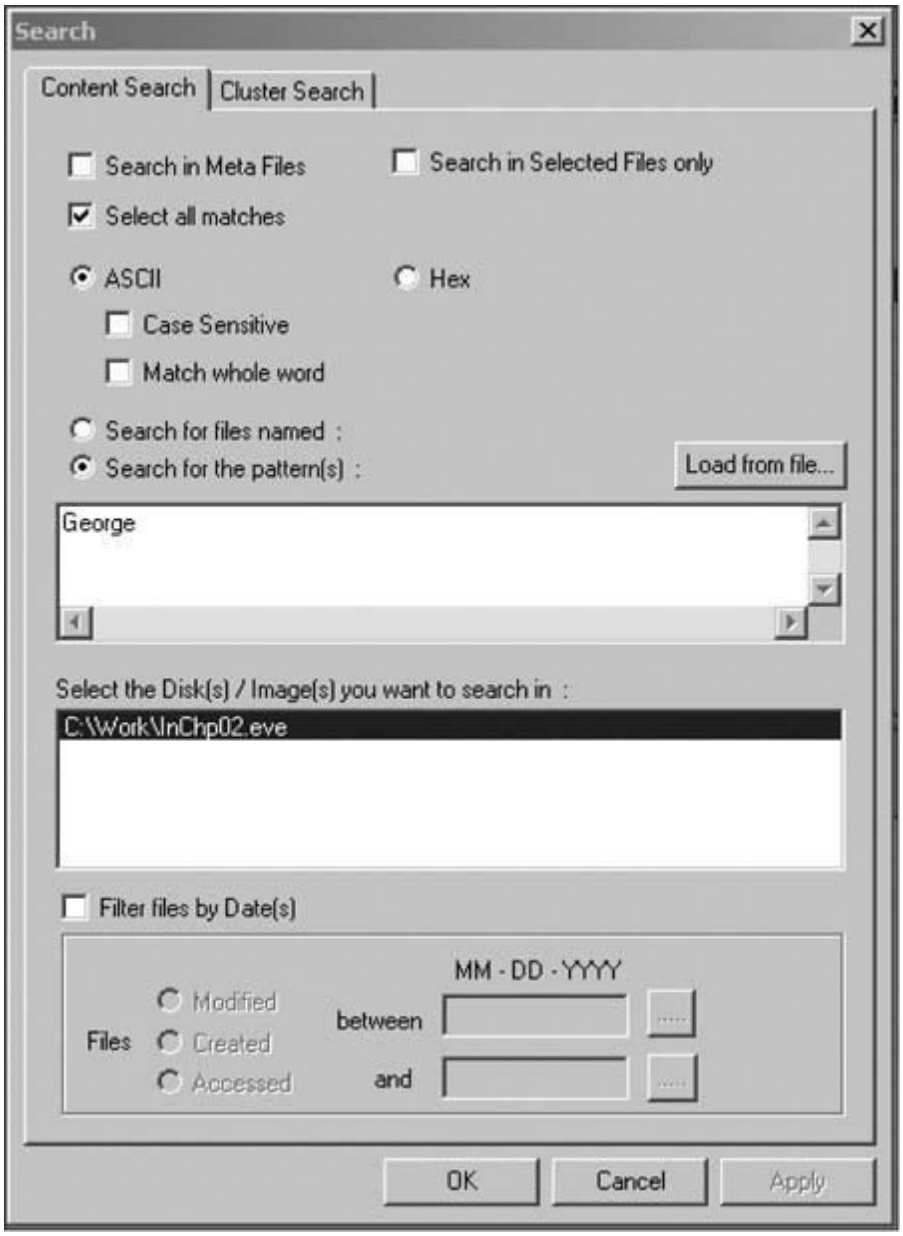



Figure 2-12 Entering a keyword in the Search dialog box

Under Select the Disk(s)/Image(s) you want to search in, click C:\Work\InChap02.eve (substituting the path to your work folder), and then click OK to initiate the search. Leave ProDiscover Basic running for the next activity. When the search is finished, ProDiscover displays the results in the search results pane in the work area. Note the tab labeled Search 1 in Figure 2-13. For each search you do in a case, ProDiscover adds a new tab to help catalog your searches.

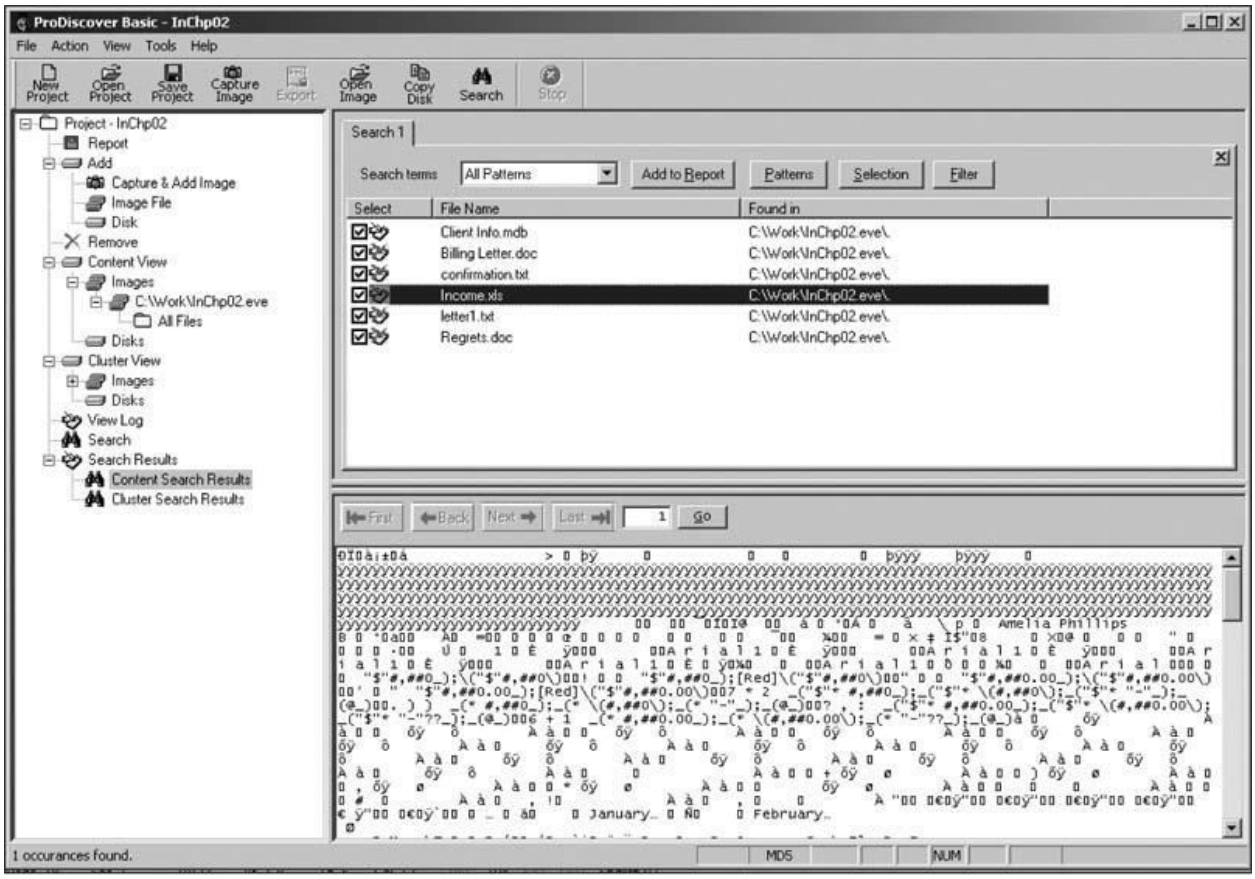



Figure 2-13 The search results pane

Click each file in the search results pane and examine its content in the data area. If you locate a file of interest that displays binary (nonprintable) data in the data area, you can double-click the file to display the data in the work area. Then you can double-click the file in the work area, and an associated program, such as Microsoft Excel for a spreadsheet, opens the file's content. If you want to extract the file, you can right-click it and click Copy File. For this example, an Excel spreadsheet named Income.xls is displayed in the search results pane. The information in the data area shows mostly unreadable character data. To examine this data, you can export the data to a folder of your choice, and then open it for follow-up examination and analysis. To export the Income.xls file, perform the following steps:

1. In the search results pane, double-click the Income.xls file, which switches the view to the work area.
2. In the work area, right-click the Income.xls file and click Copy File.
3. In the Save As dialog box, navigate to the folder you've selected, and click Save.
4. Now that the Income.xls file has been copied to a Windows folder, start Excel (or another spreadsheet program, such as OpenOffice Calc) to examine the file's content. Figure 2-14 shows the extracted file open in OpenOffice Calc. Repeat this data examination and file export process for the remaining files in the search results pane. Then close all open windows except ProDiscover Basic for the next activity.

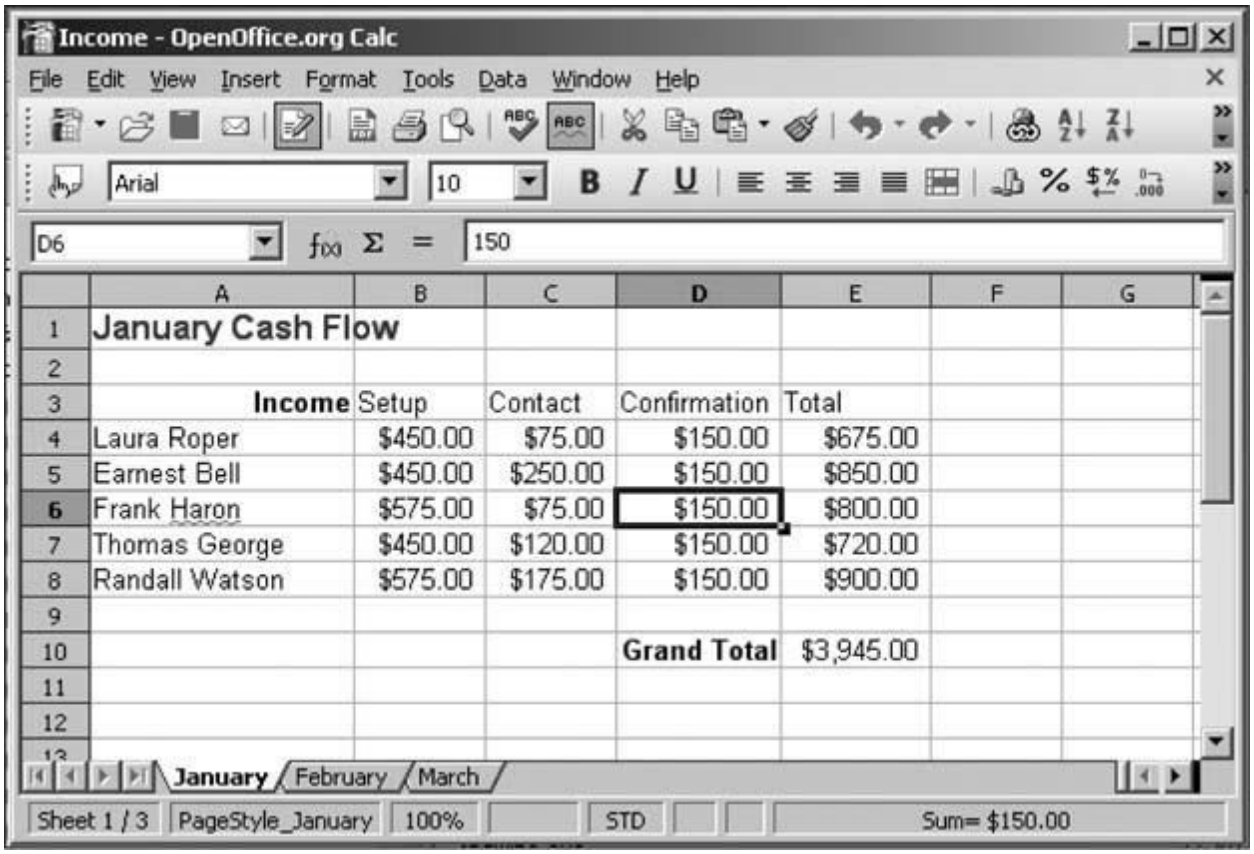



Figure 2-14 The extracted Income.xls file

With ProDiscover's Search feature, you can also search for specific filenames. To use this feature, click the "Search for files named" option button in the Search dialog box. When you're dealing with a very large drive with several thousand files, this useful feature minimizes human error in looking at data. After completing the detailed examination and analysis, you can then generate a report of your activities. Several computer forensics programs provide a report generator or log file of actions taken during an examination. These reports and logs are typically text or HTML files. The text files are usually in plaintext or Rich Text Format (RTF). ProDiscover Basic offers a report generator that produces an RTF or a plaintext file that most word processing programs can read. You can also select specific items and add them to the report. For example, to select a file in the work area, click the check box in the Select column next to the file to open the Add Comment dialog box. Enter a description and click OK. The descriptive comment is then added to the ProDiscover Basic report. To create a report in ProDiscover Basic, perform the following steps:

1. In the tree view, click Report. The report is then displayed in the right pane, as shown in Figure 2-15.

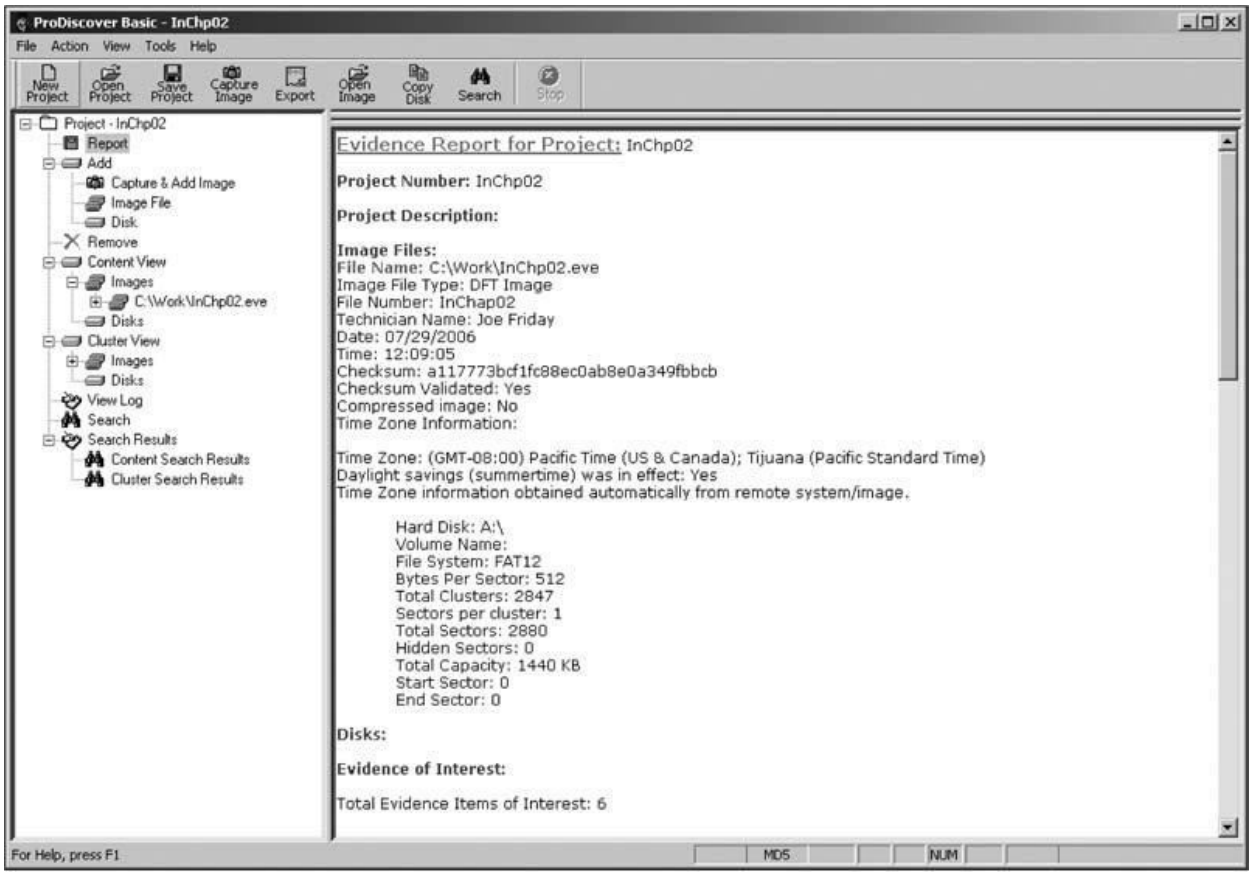



Figure 2-15 A ProDiscover report

2. To print the report, click File, Print Report from the menu.
3. In the Print dialog box, click OK.

If the report needs to be saved to a file, you use ProDiscover Basic's Export feature and choose RTF or plaintext for the file format. To export the report to a file, do the following:

1. In the tree view, click Report.
2. Click Action, Export from the menu.
3. In the Export dialog box, click the RTF Format or Text Format option button, type InChp02 in the File Name text box, and then click OK.

4. Review the report, and then click File, Exit from the menu to exit ProDiscover Basic. This activity completes your analysis of the USB drive. In the next section, you learn how to complete the case. In later chapters, you learn how to apply more search and analysis techniques.

**Completing the Case**

After analyzing the disk, you can retrieve deleted files, e-mail, and items that have been purposefully hidden, which you do in Chapters 9, 10, and 12. The files on George's USB drive indicate that he was conducting a side business on his company computer. Now that you have retrieved and analyzed the evidence, you need to find the answers to the following questions to write the final report:

- How did George's manager acquire the disk?
- Did George perform the work on a laptop, which is his own property? If so, did he conduct business transactions on his break or during his lunch hour?
- At what times of the day was George using the non-work-related files? How did you retrieve that

information?
• Which company policies apply?
• Are there any other items that need to be considered?
When you write your report, state what you did and what you found. The report you generated in ProDiscover gives you an account of the steps you took. As part of your final report, depending on guidance from management or legal counsel, include the ProDiscover report file to document your work. In any computing investigation, you should be able to repeat the steps you took and produce the same results. This capability is referred to as repeatable findings; without it, your work product has no value as evidence. Keep a written journal of everything you do. Your notes can be used in court, so be mindful of what you write or e-mail, even to a fellow investigator. Often these journals start out as handwritten notes, but you can transcribe them to electronic format periodically. Basic report writing involves answering the six Ws: who, what, when, where, why, and how. In addition to these basic facts, you must also explain computer and network processes. Typically, your reader is a senior personnel manager, a lawyer, or occasionally a judge who might have little computer knowledge. Identify your reader and write the report for that person. Provide explanations for processes and how systems and their components work.
Your organization might have templates to use when writing reports. Depending on your organization's needs and requirements, your report must describe the findings from your analysis. The report generated by ProDiscover lists your examination and data recovery findings.
Other computer forensics tools generate a log file of all actions taken during your examination and analysis. Integrating a computer forensics log report from these other tools can enhance your final report. When describing the findings, consider writing your narrative first and then placing the log output at the end of the report, with references to it in the main narrative. Chapter 14 covers writing final reports for investigations in more detail. In the Domain Name case, you want to show conclusive evidence that George had his own business registering domain names and list the names of his clients and his income from this business. You also want to show letters he wrote to clients about their accounts. The time and date stamps on the files are during work hours, so you should include this information, too. Eventually, you hand the evidence file to your supervisor or to Steve, George's manager, who then decides on a course of action.

**Critiquing the Case**

After you close the case and make your final report, you need to meet with your department or a group of fellow investigators and critique the case in an effort to improve your work. Ask yourself assessment questions such as the following:
• How could you improve your performance in the case?
• Did you expect the results you found? Did the case develop in ways you did not expect?
• Was the documentation as thorough as it could have been?
• What feedback has been received from the requesting source?
• Did you discover any new problems? If so, what are they?
• Did you use new techniques during the case or during research?
Make notes to yourself in your journal about techniques or processes that might need to be changed or addressed in future investigations. Then store your journal in a secure place.

## NETWORK FORENSICS:

### OVERVIEW OF NETWORK FORENSICS:

The word “forensics” means the use of science and technology to investigate and establish facts in criminal or civil courts of law. Forensics is the procedure of applying scientific knowledge for the purpose of analyzing the evidence and presenting them in court.

Network forensics is a subcategory of digital forensics that essentially deals with the examination of the network and its traffic going across a network that is suspected to be involved in malicious activities, and its investigation for example a network that is spreading malware for stealing credentials or for the purpose analyzing the cyber-attacks. As the internet grew cybercrimes also grew along with it and so did the significance of network forensics, with the development and acceptance of network-based services such as the World Wide Web, e-mails, and others.

With the help of network forensics, the entire data can be retrieved including messages, file transfers, e-mails, and, web browsing history, and reconstructed to expose the original transaction. It is also possible that the payload in the uppermost layer packet might wind up on the disc, but the envelopes used for delivering it are only captured in network traffic. Hence, the network protocol data that enclose each dialog is often very valuable.

For identifying the attacks investigators must understand the network protocols and applications such as web protocols, Email protocols, Network protocols, file transfer protocols, etc.

Investigators use network forensics to examine network traffic data gathered from the networks that are involved or suspected of being involved in cyber-crime or any type of cyber-attack. After that, the experts will look for data that points in the direction of any file manipulation, human communication, etc. With the help of network forensics, generally, investigators and cybercrime experts can track down all the communications and establish timelines based on network events logs logged by the NCS.

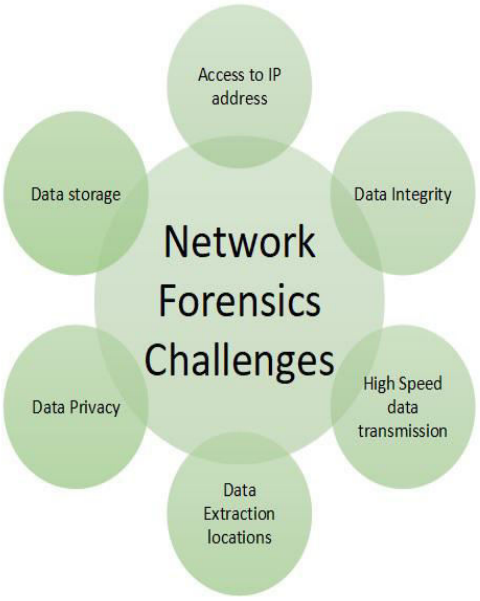
Processes Involved in Network Forensics:

Some processes involved in network forensics are given below:

- **Identification:** In this process, investigators identify and evaluate the incident based on the network pointers.
- **Safeguarding:** In this process, the investigators preserve and secure the data so that the tempering can be prevented.
- **Accumulation:** In this step, a detailed report of the crime scene is documented and all the collected digital shreds of evidence are duplicated.
- **Observation:** In this process, all the visible data is tracked along with the metadata.
- **Investigation:** In this process, a final conclusion is drawn from the collected shreds of evidence.
- **Documentation:** In this process, all the shreds of evidence, reports, conclusions are documented and presented in court.

Challenges in Network Forensics:

- The biggest challenge is to manage the data generated during the process.
- Intrinsic anonymity of the IP.
- Address Spoofing.




Advantages:

- Network forensics helps in identifying security threats and vulnerabilities.
- It analyzes and monitors network performance demands.
- Network forensics helps in reducing downtime.
- Network resources can be used in a better way by reporting and better planning.
- It helps in a detailed network search for any trace of evidence left on the network.

Disadvantage:

- The only disadvantage of network forensics is that It is difficult to implement.

## OPEN SOURCER SECURITY TOOLS FOR NETWORK FORENSIC ANALYSIS:

### Tcpdump:

Tcpdump is a popular command line tool available for capturing and analyzing network traffic primarily on Unix based systems. Using tcpdump, we can capture the traffic and store the results in a file that is compatible with tools like Wireshark for further analysis. Tcpdump can either be used to do a quick packet capture for troubleshooting or for capturing traffic continuously in large volumes for future analysis. It is worth noting that tcpdump can be used to capture both layer 2 and layer 3 data. The latter may cause disk space problems as the size of the resulting capture file can grow depending on the volume of the network traffic. In addition to the ability to capture large amounts of traffic, tcpdump also supports the use of filters to avoid capturing unnecessary traffic or to capture only the traffic we are interested in. One should be extra cautious with this feature, as applying filters can lead to missing potential evidence. So, it is recommended to capture as much traffic as possible and filter out the unnecessary traffic during analysis later.

### Wireshark:

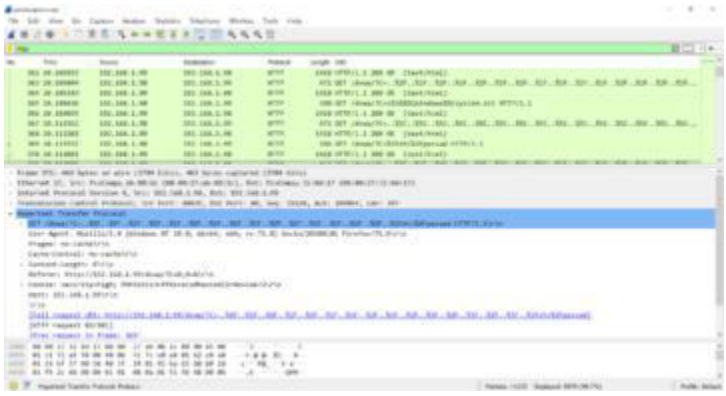
It would be a surprise if someone worked in the Cyber Security field and not heard of the tool Wireshark. Wireshark is an open-source tool available for capturing and analyzing traffic with

support for applying filters using the graphical user interface. On the system, where Wireshark is running one can choose the interface on which traffic needs to be captured.

The following figure shows a sample of Wireshark with the packets captured by tcpdump.

It would be a surprise if someone worked in the Cyber Security field and not heard of the tool Wireshark. Wireshark is an open-source tool available for capturing and analyzing traffic with support for applying filters using the graphical user interface. On the system, where Wireshark is running one can choose the interface on which traffic needs to be captured.

The following figure shows a sample of Wireshark with the packets captured by tcpdump.



**Network Miner**

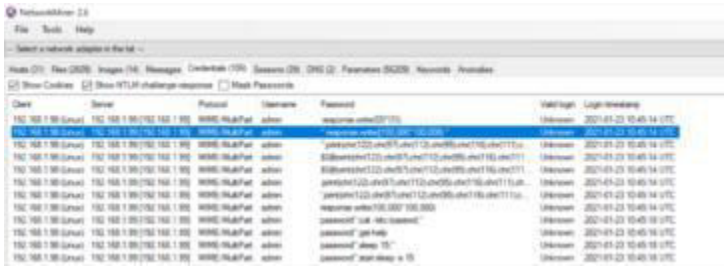
According to the official website netresec.com, "NetworkMiner is an open source Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux / Mac OS X / FreeBSD). NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.

NetworkMiner makes it easy to perform advanced Network Traffic Analysis (NTA) by providing extracted artifacts in an intuitive user interface. The way data is presented not only makes the analysis simpler, it also saves valuable time for the analyst or forensic investigator.

NetworkMiner has, since the first release in 2007, become a popular tool among incident response teams as well as law enforcement. NetworkMiner is today used by companies and organizations all over the world".

NetworkMiner also comes as a professional version.

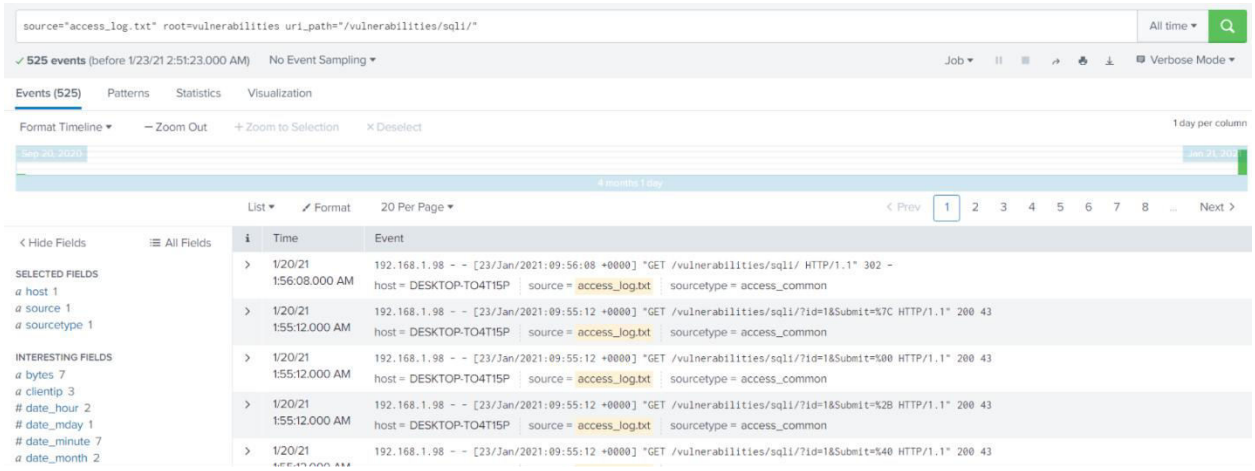
The following figure shows Network Miner being used on Windows to analyse a packet capture.



### Splunk

Splunk is a proprietary, portable, highly extensible log aggregation and analysis tool. Splunk performs capturing, indexing, and correlating the real time data in a searchable container and produces graphs, alerts, dashboards and visualizations. When it comes to network forensics, splunk plays a crucial role in providing evidence from various sources. While Splunk is a popular commercial tool, a free version is offered with limited features. It comes with an easy to use Graphical User Interface.

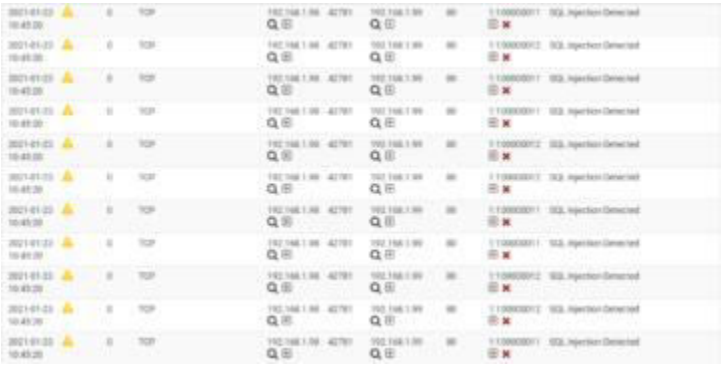
The following figure shows a sample search result of web access logs from Splunk.




### Snort

Snort is one of the most popular network Intrusion Detection Systems available for free. There is a commercial version of Snort available, which is currently offered by Cisco. Snort is highly configurable, which allows the users to add custom plugins called preprocessors. In addition to it, it comes with a great set of output options. At its core, Snort provides alerts based on rulesets provided to it. The Snort administrator needs to feed the rules as the default installation doesn't come with any rules by default. However, Snort website provides rulesets that can be fed into Snort. In addition to these rules, one can write custom alert rules.

The following figure shows a sample alert from Snort, which shows that there is an SQL Injection attempt.



**Network forensics**

Network forensics is a subcategory of digital forensics that essentially deals with the examination of the network and its traffic going across a network that is suspected to be involved in malicious activities, and its investigation for example a network that is spreading malware for stealing credentials or for the purpose analyzing the cyber-attacks. As the internet grew cybercrimes also grew along with it and so did the significance of network forensics, with the development and acceptance of network-based services such as the World Wide Web, e-mails, and others.

**Overview of Network forensics:**

**Processes Involved in Network Forensics:**

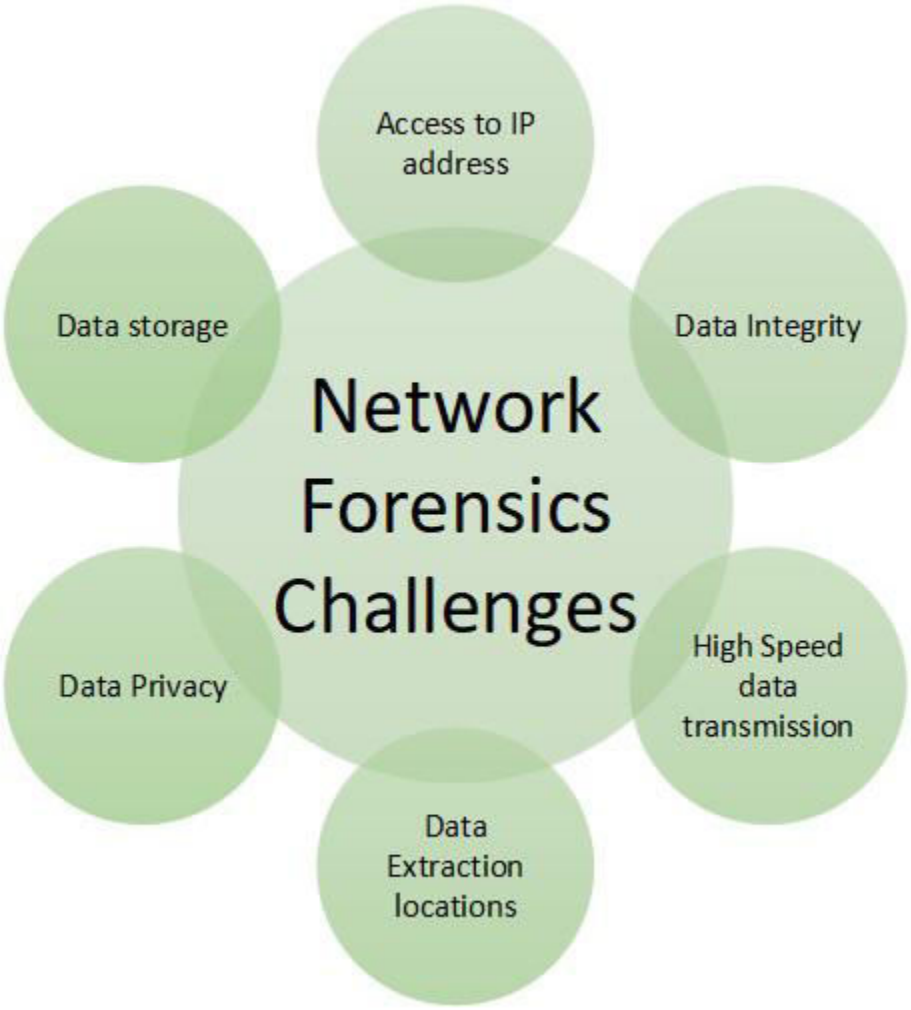
Some processes involved in network forensics are given below:

- **Identification:** In this process, investigators identify and evaluate the incident based on the network pointers.
- **Safeguarding:** In this process, the investigators preserve and secure the data so that the tempering can be prevented.
- **Accumulation:** In this step, a detailed report of the crime scene is documented and all the collected digital shreds of evidence are duplicated.
- **Observation:** In this process, all the visible data is tracked along with the metadata.
- **Investigation:** In this process, a final conclusion is drawn from the collected shreds of evidence.
- **Documentation:** In this process, all the shreds of evidence, reports, conclusions are documented and presented in court.

**Challenges in Network Forensics:**

- The biggest challenge is to manage the data generated during the process.
- Intrinsic anonymity of the IP.

- Address Spoofing.




**Advantages:**

- Network forensics helps in identifying security threats and vulnerabilities.
- It analyzes and monitors network performance demands.
- Network forensics helps in reducing downtime.
- Network resources can be used in a better way by reporting and better planning.
- It helps in a detailed network search for any trace of evidence left on the network.

**Disadvantage:**

- The only disadvantage of network forensics is that It is difficult to implement.

open-source security tools for network forensic analysis

Various tools are available for Network forensics to investigate network attacks.

Which of the following tools can be used for network forensic?

**Network Forensics Tools:**

- tcpdump
- Wireshark.
- Network Miner.
- Splunk.
- Snort.
- Sources.

**tcpdump**

Tcpdump is a popular command line tool available for capturing and analyzing network traffic primarily on Unix based systems. Using tcpdump, we can capture the traffic and store the results in a file that is compatible with tools like Wireshark for further analysis. Tcpdump can either be used to do a quick packet capture for troubleshooting or for capturing traffic continuously in large volumes for future analysis. It is worth noting that tcpdump can be used to capture both layer 2 and layer 3 data. The latter may cause disk space problems as the size of the resulting capture file can grow depending on the volume of the network traffic. In addition to the ability to capture large amounts of traffic, tcpdump also supports the use of filters to avoid capturing unnecessary traffic or to capture only the traffic we are interested in. One should be extra cautious with this feature, as applying filters can lead to missing potential evidence. So, it is recommended to capture as much traffic as possible and filter out the unnecessary traffic during analysis later.

The following excerpt shows the help output of tcpdump command line tool.

```
$ tcpdump -
h
```

tcpdump version 4.9.3

libpcap version 1.9.1 (with TPACKET_V3)

OpenSSL 1.1.1g 21 Apr 2020

Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]

[ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]

[ -i interface ] [ -j tstamptype ] [ -M secret ] [ –number ]

[ -Q in|out|inout ]

[ -r file ] [ -s snaplen ] [ –time-stamp-precision precision ]

[ –immediate-mode ] [ -T type ] [ –version ] [ -V file ]

[ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]

[ -Z user ] [ expression ]

Following is the simplest tcpdump command to capture packets on a specific interface (eth0 in this case) and write them to a file named packet.pcap

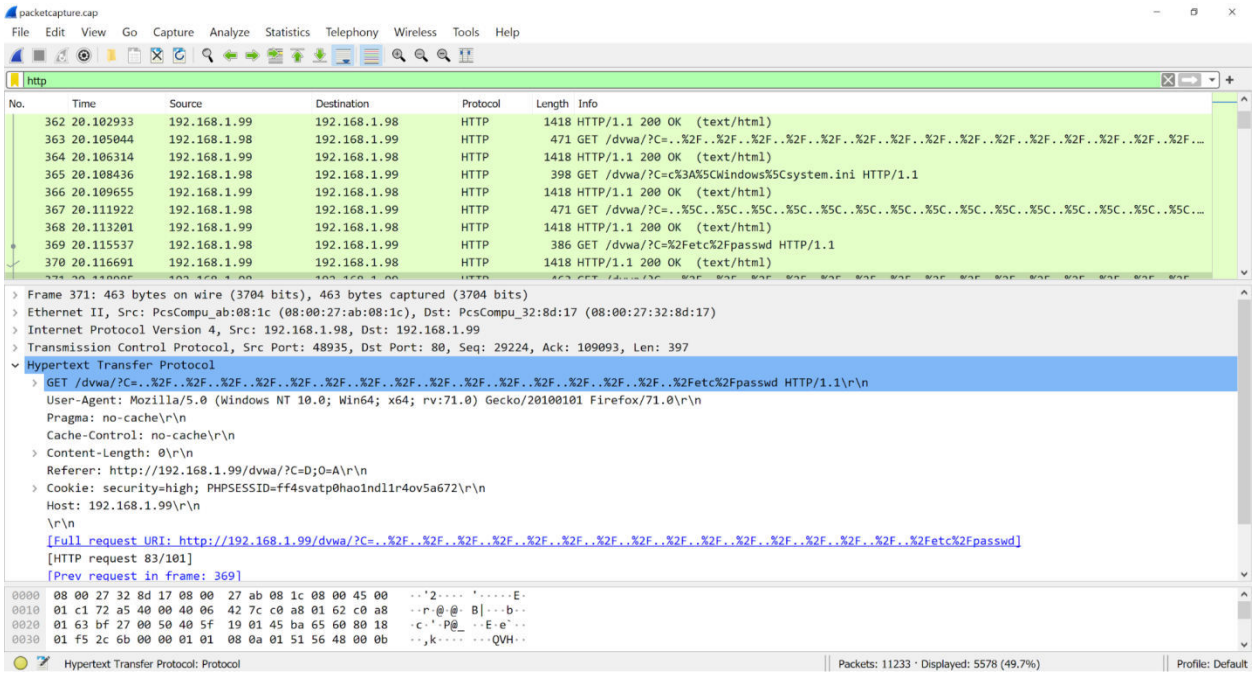
$ tcpdump -i eth0 -w

packet.pcap

**Wireshark**

It would be a surprise if someone worked in the Cyber Security field and not heard of the tool Wireshark. Wireshark is an open-source tool available for capturing and analyzing traffic with support for applying filters using the graphical user interface. On the system, where Wireshark is running one can choose the interface on which traffic needs to be captured.

The following figure shows a sample of Wireshark with the packets captured by tcpdump.




**Network Miner**

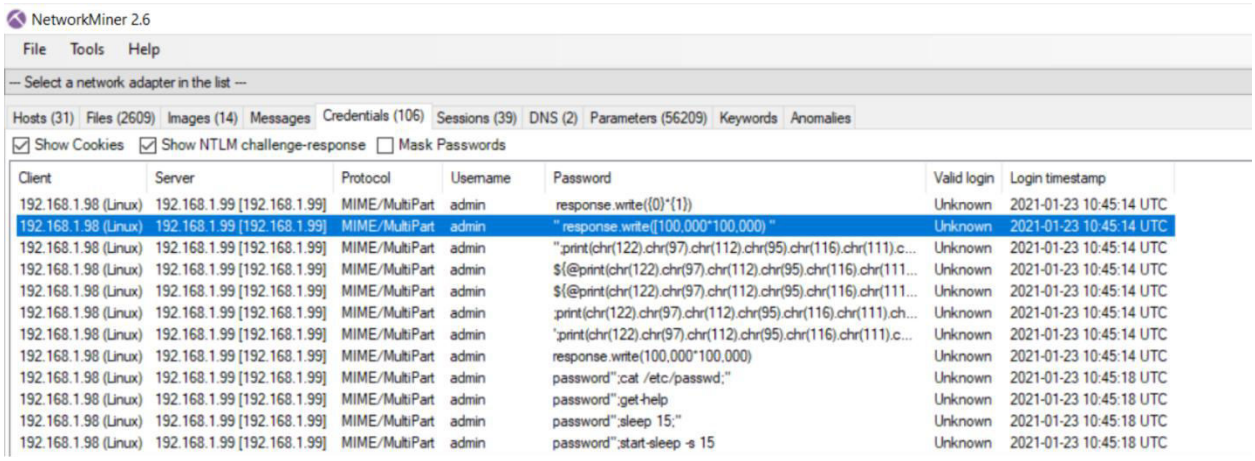
According to the official website netresec.com, "*NetworkMiner is an open source Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux / Mac OS X / FreeBSD). NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.*

*NetworkMiner makes it easy to perform advanced Network Traffic Analysis (NTA) by providing extracted artifacts in an intuitive user interface. The way data is presented not only makes the analysis simpler, it also saves valuable time for the analyst or forensic investigator.*

*NetworkMiner has, since the first release in 2007, become a popular tool among incident response teams as well as law enforcement. NetworkMiner is today used by companies and organizations all over the world*".

NetworkMiner also comes as a professional version.

The following figure shows Network Miner being used on Windows to analyse a packet capture.




### Splunk

Splunk is a proprietary, portable, highly extensible log aggregation and analysis tool. Splunk performs capturing, indexing, and correlating the real time data in a searchable container and produces graphs, alerts, dashboards and visualizations. When it comes to network forensics, splunk plays a crucial role in providing evidence from various sources. While Splunk is a popular commercial tool, a free version is offered with limited features. It comes with an easy to use Graphical User Interface.

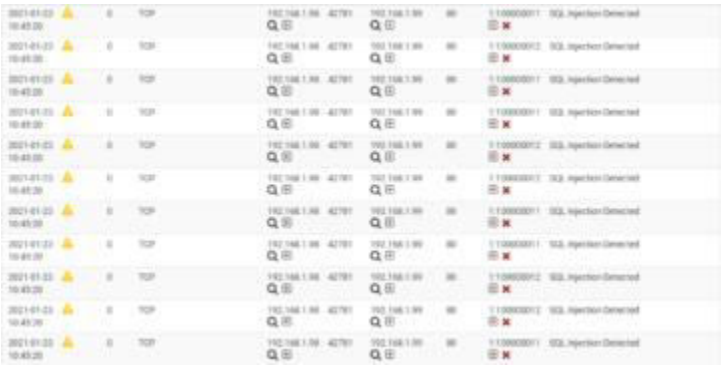
The following figure shows a sample search result of web access logs from Splunk.

### Snort

Snort is one of the most popular network Intrusion Detection Systems available for free. There is a commercial version of Snort available, which is currently offered by Cisco. Snort is highly configurable, which allows the users to add custom plugins called preprocessors. In addition to it, it comes with a great set of output options. At its core, Snort provides alerts based on rulesets provided to it. The Snort administrator needs to feed the rules as the default installation doesn't

come with any rules by default. However, Snort website provides rulesets that can be fed into Snort. In addition to these rules, one can write custom alert rules.

The following figure shows a sample alert from Snort, which shows that there is an SQL Injection attempt.



## Conclusion

Network forensic investigations revolve around evidence collection, indexing and analysis. Investigators must rely on good tools that can extract the evidence and assist in analysis. This article has provided a short list of tools that can come handy in network forensics.

### Sources


1. Network Forensics by Ric Messier – https://www.amazon.com/Network-Forensics-Ric-Messier/dp/1119328284
2. Internet Forensics by R Jones – https://www.amazon.com/Internet-Forensics-Digital-Evidence-Computer/dp/059610006X
3. Network Forensics by Sheriff Davidoff, Jonathan Ham – https://www.amazon.com/Network-Forensics-Tracking-Hackers-Cyberspace/dp/0132564718


## UNIT-V

### Mobile Forensics – Definition, Uses, and Principles

Mobile forensics, a subtype of digital forensics, is concerned with retrieving data from an electronic source. The recovery of evidence from mobile devices such as smartphones and tablets

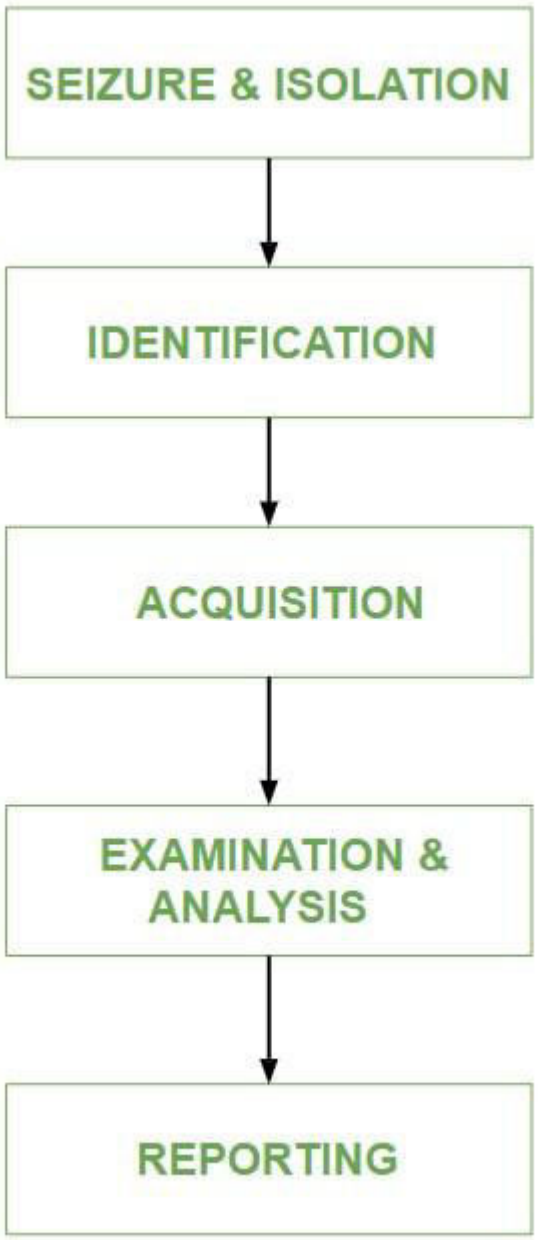
is the focus of mobile forensics. Because individuals rely on mobile devices for so much of their data sending, receiving, and searching, it is reasonable to assume that these devices hold a significant quantity of evidence that investigators may utilize.

Mobile devices may store a wide range of information, including phone records and text messages, as well as online search history and location data. We frequently associate mobile forensics with law enforcement, but they are not the only ones who may depend on evidence obtained from a mobile device.

**Uses of Mobile Forensics:**

The military uses mobile devices to gather intelligence when planning military operations or terrorist attacks. A corporation may use mobile evidence if it fears its intellectual property is being stolen or an employee is committing fraud. Businesses have been known to track employees' personal usage of business devices in order to uncover evidence of illegal activity. Law enforcement, on the other hand, may be able to take advantage of mobile forensics by using electronic discovery to gather evidence in cases ranging from identity theft to homicide.

**Process of Mobile Device Forensics:**




- **Seizure and Isolation:** According to digital forensics, evidence should always be adequately kept, analyzed, and accepted in a court of law. Mobile device seizures are followed by a slew of legal difficulties. The two main risks linked with this step of the mobile forensic method are lock activation and network / cellular connectivity.
- **Identification:** The identification purpose is to retrieve information from the mobile device. With the appropriate PIN, password, pattern, or biometrics, a locked screen may be opened. Passcodes are protected, but fingerprints are not. Apps, photos, SMSs, and messengers may

all have comparable lock features. Encryption, on the other hand, provides security that is difficult to defeat on software and/or hardware level.

- **Acquisition:** Controlling data on mobile devices is difficult since the data itself is movable. Once messages or data are transmitted from a smartphone, control is gone. Despite the fact that various devices are capable of storing vast amounts of data, the data itself may be stored elsewhere. For example, data synchronization across devices and apps may be done either directly or via the cloud. Users of mobile devices commonly utilize services such as Apple's iCloud and Microsoft's One Drive, which exposes the possibility of data harvesting. As a result, investigators should be on the lookout for any signs that data may be able to transcend the mobile device from a physical object, as this might have an impact on the data collecting and even preservation process.
- **Examination and analysis:** Because data on mobile devices is transportable, it's tough to keep track of it. When messages or data from a smartphone are moved, control is lost. Despite the fact that numerous devices can hold vast amounts of data, the data itself may be stored elsewhere.
- **Reporting:** The document or paper trail that shows the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence is referred to as forensic reporting. It is the process of verifying how any type of evidence was collected, tracked, and safeguarded.

**Principles of Mobile Forensics:**

The purpose of mobile forensics is to extract digital evidence or relevant data from a mobile device while maintaining forensic integrity. To accomplish so, the mobile forensic technique must develop precise standards for securely seizing, isolating, transferring, preserving for investigation, and certifying digital evidence originating from mobile devices.

The process of mobile forensics is usually comparable to that of other fields of digital forensics. However, it is important to note that the mobile forensics process has its own unique characteristics that must be taken into account. The use of proper methods and guidelines is a must if the investigation of mobile devices is to give positive findings.

III. CHALLENGES ASSOCIATED WITH MOBILE PHONE FORENSICS A. Mobile phone forensics is challenging field due to fast changes in technology. Several models of mobile phones exist in the world today. Manufacturers lack standardized methods of storing data. Most of the mobile phones use closed operating systems and has proprietary interfaces. To meet this challenge there is always a need for development of new forensics tools and techniques.

B. Signals of mobile phone need to be blocked while carrying forensics analysis. Blocking RF signals quickly drains the battery. This can be minimized while carrying forensics analysis of mobile phones in properly shielded labs. Shielding methods for lab include such as EMI/EMC protection.

C. Large variety of data cables exist for mobile phones. Identification and collection of cables required for forensics analysis of mobile phones is challenging task. Small databases for defining mobile phone models and their associated cables with tags can help a great deal.

D. Most of the commercially available forensic tools do not provide solutions to deal with physically damaged mobile phones. Forensic examiners must be trained and equipped to handle such situations.

E. Conflicts can occur due to different operating system, vendor and version specific device drivers. It is therefore recommended to have separate machines for each type of forensic software. However to economize resources Virtual Machine environments can be created.

F. Data on active mobile phone tends to change constantly due to lack of conventional write-blocking mechanism. Analysis must be done on a phone that is powered ON but it is ideal that the phone does not receive any calls, text messages, or other communications. Shielded labs can address this issue.

G. Most of the international trainings available in the field are vendor specific. There is need of for neutral and standard trainings.

H. Status of unopened emails and messages will change after reading them. Care must be taken while recoding such type of evidence.

J. Mobile phones may lose data or ask for security measures on next restart once shut down. Owner of the mobile phone (if available) may be asked about security codes.

K. Authentication mechanisms can confine access to data. Finding of Personal Identification Number (PIN), Phone Unlock Key (PUK), and handset and memory card passwords can become difficult at times.

L. Now days there are various methods available to remotely destroy or change data on a mobile phone. Such happening can be avoided in shielded lab environments while carrying forensic investigations. Care must also be taken to protect mobile phones while carrying them to labs.

M. Data from mobile phone internal memory is restricted without the use of SIM card. Inserting another SIM can cause the loss of mobile phone data.

N. Many commercial mobile phone forensic tools only provide logical acquisition of data. Deleted data can only be recovered using physical acquisition.

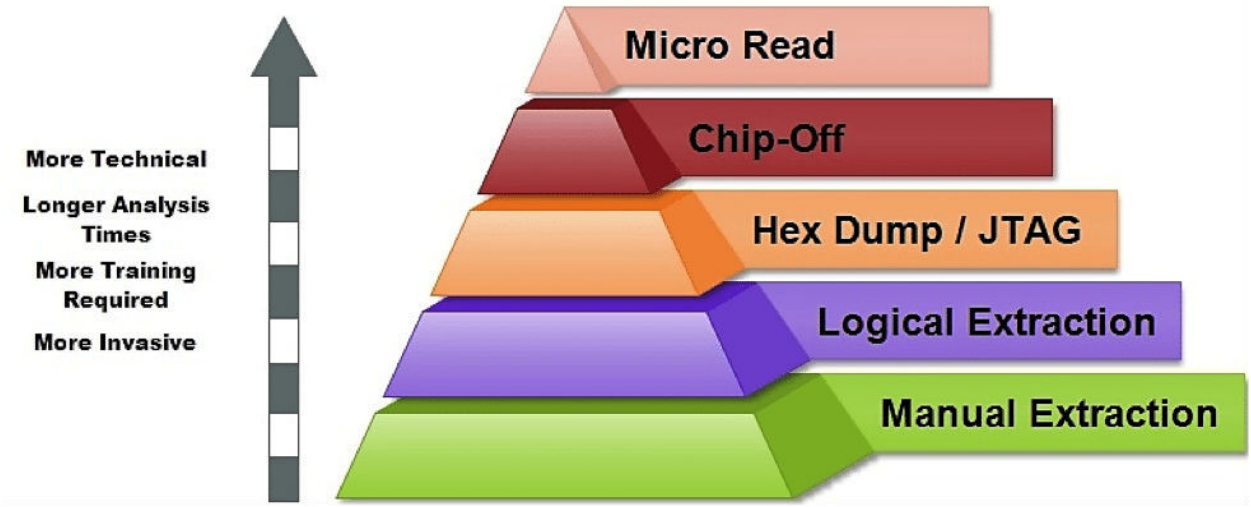
O. Introduction of Mobile Number Portability (MNP) can result into improper identification of subscriber. Mobile Phone network operators may be consulted for proper identification.

P. IMEI changing for few mobile handsets is possible with the use flashing tools like Universal Flasher UFS-3. This can result improper identification of phones. These illegal activities shall be banned.

LEVELS OF ANALYSIS FOR DATA ACQUISITION FROM MOBILE PHONES

Methods for data acquisition from mobile phones mainly depend upon the condition, model, time and nature of the case. There is currently no standard method for analyzing mobile phone internal memory. Results obtained after forensic examination of mobile phones are different for different manufacturers. Each forensics extraction product does well in some areas and not so well in other areas. It is therefore recommended for forensic examiner to not focus on low hanging fruit. Methods that are currently used in the field of mobile phone forensics focus on extracting information by utilizing a cable, infrared or Bluetooth connection to the phone, and then extracting information by u sing the AT-command set which has been specified for communication with serial modems as per GSM specifications [8]. To aid investigators with information extraction, several software packages exist to perform this process. CellSeizure, TULP and Oxygen Phone Manager are examples of such software packages [9] [10] [11]. For complete Mobile Phone Forensic examination we need both Logical and Physical extractions. Logical extraction methods are quick, easy to use, reliable, 100% forensically secure and extract" all" data including contacts, calls, calendar, SMS, photos etc. While Physical extraction can creates a "complete" memory image, extracts even deleted data (including system and network provider information like previous IMSI etc) , can retrieve data from devices where no SIM is present, bypass (and retrieve) handset security codes and is also useful for memory card analysis. The extracted data while carrying Physical extraction is in raw Hex-format and decoding of binary data is required. Using both logical and physical extractions give the investigators a better view. Physical tools can successfully be used to enable phones for logical

extraction. Decoding of Physical data is hard as there are no standards in mobile phones. Based on the various extraction methods different levels of analysis can be logically made for evidence acquisition from mobile phones as shown in Figure-1. Figure-1.




**Manual extraction**

The manual extraction technique allows investigators to extract and view data through the device's touchscreen or keypad. At a later stage, this data is documented photographically. Furthermore, manual extraction is time-consuming and involves a great probability of human error. For example, the data may be accidentally deleted or modified during the examination.

Popular tools for manual extractions include:

- Project-A-Phone
- Fernico ZRT
- EDEC Eclipse

**Logical extraction**

In this technique, the investigators connect the cellular device to a forensic workstation or hardware via Bluetooth, Infrared, RJ-45 cable, or USB cable. The computer—using a logical extraction tool—sends a series of commands to the mobile device. As a result, the required data is collected from the phone's memory and sent back to the forensic workstation for analysis purposes. The tools used for logical extraction include:

- XRY Logical
- Oxygen Forensic Suite
- Lantern

**Hex dump**

A hex dump, also called physical extraction, extracts the raw image in binary format from the mobile device. The forensic specialist connects the device to a forensic workstation and pushes the boot-loader into the device, which instructs the device to dump its memory to the computer. This process is cost-effective and supplies more information to the investigators, including the recovery of phone's deleted files and unallocated space. The common tools used for hex dump include:

- XACT
- Cellebrite UFED Physical Analyzer
- Pandora's Box

**Chip-off**

The chip-off technique allows the examiners to extract data directly from the flash memory of the cellular device. They remove the phone's memory chip and create its binary image. This process is costly and requires an ample knowledge of hardware. Improper handling may cause physical damage to the chip and renders the data impossible to retrieve. The popular tools and equipment used for chip-off include:

- iSeasamo Phone Opening Tool
- Xytronic 988D Solder Rework Station

- FEITA Digital inspection station
- Chip Epoxy Glue Remover
- Circuit Board Holder

**Micro read**

This process involves interpreting and viewing data on memory chips. The investigators use a high-powered electron microscope to analyze the physical gates on the chips and then convert the gate level into 1's and 0's to discover the resulting ASCII code. This process is expensive and time-consuming. Also, it requires an ample knowledge of hardware and file systems. There is no tool available for micro read (Ayers, Brothers, Jansen, 2014).

V. TOOLS CATEGORIZATION BASED ON LEVELS OF MOBILE PHONE FORENSICS ANALYSIS The core objective of any Mobile Phone Forensic tool is to extract digital evidence. In addition, these tools also support examination and reporting functions. It is important for any forensic tool to preserve the integrity of acquired and extracted data. This is achieved by blocking and eliminating write requests to the device containing the data and calculating hashes of the evidence files. Mobile Phone Forensic tools can be placed in various levels as shown in Figure-2 corresponding to the levels of analysis (Figure-1).

Generica free tools

- **AFLogical OSE - Open source Android Forensics app and framework** is an application in APK format that must be installed beforehand in the Android terminal. Once the process is completed it allows varied information to be extracted to the SD card (call log, contact list and list of applications installed, text messages and multimedia), which must subsequently be recovered either by connecting the card to an external device or through the ADB.
- **Open Source Android Forensics** is a framework that is distributed via a virtual machine image that brings together various tools which allow the analysis of applications for mobile devices, including both a static and a dynamic analysis or even a forensic analysis.

- **Andriller** is an application for Windows operating systems that brings together different forensic utilities. It allows a lot of interesting information to be obtained that is related, amongst others, both to social media and to messaging programmes (Skype, Tinder, Viber, WhatsApp, etc.).
- **FTK Imager Lite** allows us to work with memory dumps of mobile devices to analyse them and obtain evidence.
- **NowSecure Forensics Community Edition** is distributed as a virtual image that brings together various tools to carry out a forensic analysis, and can carry out different types of evidence extraction or even file carving in its commercial version.
- **LIME- Linux Memory Extractor** is software that allows a volatile memory dump to be obtained from a Linux-based device, as is the case for Android phones. Likewise, it has the advantage that it can be executed remotely via a network.

Specific free tools

- **Android Data Extractor Lite (ADEL)** is a tool developed in Python that allows a forensic flowchart to be obtained from the databases of the mobile device. To carry out the process, it is necessary for the mobile device to be rooted or have personalised recovery installed.
- **WhatsApp Xtract** allows WhatsApp conversations to be viewed on the computer in a simple and user-friendly way. As such, the different databases that store information corresponding to messages should be obtained beforehand.
- **Skype Xtractor** is an application, supported both on Windows and Linux that allows us to view information of the Skype main.db file, which stores information about contacts, chats, calls, transferred files, deleted messages etc.

Paid tools

- **Cellebrite Touch** is one of the most well-known and complete evidence extraction devices. It allows us to work with over 6,300 different terminals with the main mobile operating systems. It is also very simple and intuitive.
- **Encase Forensics**, in addition to Cellebrite, is a worldwide reference in forensic analysis. Its wide range of features includes that which identifies encrypted files and that which attempts

to decipher them through **Passware Kit Forensic**, a tool that incorporates specific algorithms for this purpose.

- **Oxygen Forensic Suite** is capable of obtaining information from more than 10,000 different mobile device models and even obtaining information from services on the cloud and import backups or images.
- **MOBILedit! Forensic** allows a lot of information to be received and advanced operations to be carried out such as obtaining a complete memory dump, avoiding terminal-locking measures, and flexibly creating reports.
- **Elcomsoft iOS Forensic Toolkit** allows for physical acquisition on iOS devices such as iPhone, iPad or iPod. It also includes other utility features such as that of deciphering the keychain that stores user passwords in the terminal analysed or registering each action that is performed during the whole process to keep a record of them.

To carry out the evidence-gathering process in an Android mobile device, many of the tools require enabling of the "**USB debugging**" option, preferably the "**Stay awake**" option and disabling of any time-out screen lock option. In the event that the terminal has any screen lock option configured, it is necessary to circumvent it.

Most of the tools described above, mainly paid tools, include mechanisms to bypass these protections so it is only necessary to follow the steps that they indicate, although this is not always possible. If the process is going to be carried out manually, one or more of the following actions have to be performed:

- If the device is rooted we can try to remove the gesture.key or password.key file in accordance with the mode of protection established, which are stored in /data/system/ or copy them and decipher the pattern through a hash dictionary, such as AndroidGestureSHA1, using a tool such as **Android Pattern Lock Cracker** for this.
- Install a personalised recovery such as **ClockWorkMod** or **Team Win Recovery Project** (**TWRP**)and subsequently deactivate device access locking.
- The problem of fragmentation on mobile platforms causes the vast majority of devices to be affected with vulnerabilities that will not be resolved for these models and, as such, depending on the Android version, it is possible to use some of themto obtain access to the device, such as CVE-2013-6271.

- Using brute force. When a 4-digit pin is used as a security measure it has been demonstrated that it is possible to obtain it in a short period of time, in around a maximum period of 16 hours.
- A more sophisticated technique could even be used, as was demonstrated by various members of the IT department of the University of Pennsylvania in what they called a «**Smudge Attack**», which consists of obtaining the locking pattern from fingerprints on the screen of the mobile device, using photographs from different angles for this purpose, modifying the properties of light and colour.

Recent trend in mobile forensic technique

In modern criminal investigations, mobile devices are seized at every type of crime scene, and the data on those devices often becomes critical evidence in the case. Various mobile forensic techniques have been established and evaluated through research in order to extract possible evidence data from devices over the decades. However, as mobile devices become essential tools for daily life, security and privacy concerns grow, and modern smartphone vendors have implemented multiple types of security protection measures - such as encryption - to guard against unauthorized access to the data on their products. This trend makes forensic acquisition harder than before, and data extraction from those devices for criminal investigation is becoming a more challenging task. Today, mobile forensic research focuses on identifying more invasive techniques, such as bypassing security features, and breaking into target smartphones by exploiting their vulnerabilities. In this paper, we explain the increased encryption and security protection measures in modern mobile devices and their impact on traditional forensic data extraction techniques for law enforcement purposes. We demonstrate that in order to overcome encryption challenges, new mobile forensic methods rely on bypassing the security features and exploiting system vulnerabilities. A new model for forensic acquisition is proposed. The model is supported by a legal framework focused on the usability of digital evidence obtained through vulnerability exploitation.

- **Previous** article in issue
- **Next** article in issue

**Keywords**

Mobile forensics

Encryption

Vulnerability exploitation

## 1. Introduction

Mobile devices frequently contain data relevant to criminal investigations, and forensic analysis of those devices has become an increasingly critical investigative capability for law enforcement agencies. Over the last decades, various forensic science researchers have established methods and processes to extract evidence data from mobile devices in a forensically sound manner (Barmpatsalou et al., 2013; Al-Dhaqm et al., 2020; Reedy, 2020). Those methods have been widely used for forensic purposes in real cases, and have tackled general challenges in mobile forensics, such as the lack of standardization within the mobile industry and the rapid rate at which mobile device technology changes. On the other hand, however, new challenges have recently been imposed by the strong security features in modern mobile devices (Chernyshev et al., 2017). Encryption, together with other security guard features has clearly created challenges for forensic investigators seeking to extract data from mobile devices seized at crime scenes. Those security features have disabled many of the data acquisition methods that have been used historically, and new methods to acquire data from modern mobile devices must be explored.

The challenges posed by encryption were publicly highlighted during the 2015 dispute between Apple and the FBI following the widely reported San Bernardino, California, terrorist attack. That case not only sparked an intense legal debate about the regulation of cryptography and governmental access to encrypted devices, but it also brought public attention to issues around the security and privacy of data stored on personal mobile devices. Not surprisingly, mobile device vendors have been implementing higher levels of security features in their products to address personal data protection. Currently, in modern mobile devices, user data is highly secured from malicious access by unauthorized attackers as long as the user configurations are properly set up.

The impact of encryption on forensic analysis, as well as effective data acquisition processes has been widely researched in the computer forensics domain (Casey et al., 2011; Hargreaves and Chivers, 2008; Kornblum, 2009). It has been suggested that temporary files, data on volatile memory, metadata of encryption scheme, or access to the key management system can decrypt the target data, thereby allowing examiners to extract original data, which can then be used for criminal investigations. Challenges in data acquisition from encrypted mobile devices, however, come from the fact that those pieces of listed data are not accessible by default, requiring modification of the exhibit device. While some of the traditional forensic data acquisition methods are still effective, the

target device needs to be directly unlocked and modified for effective data acquisition, which often requires invasive operations.

In this paper, we investigate modern mobile forensic techniques, and compare them with traditional mobile forensic techniques. Looking at the paradigm shift in mobile forensic techniques, it is clear that following the traditional forensic data extraction model is no longer effective. Therefore, a new model for forensic acquisition is proposed, and modern forensic data extraction techniques are evaluated in the context of the controversial, and underdeveloped regulation of encryption and governmental access to encrypted devices.

## 2. Background: paradigm shift in mobile forensics

Advanced technologies used in modern mobile devices have greatly impacted the effectiveness of mobile forensic techniques. In this section, we provide an overview of traditional mobile device forensic data acquisition techniques, discuss the widespread adoption of encryption and other security features in mobile devices, and then assess the impacts of those security features on traditional mobile forensic techniques.

### 2.1. Traditional mobile forensic techniques

Forensic data acquisition techniques have been researched for multiple mobile device platforms. Their forensic-soundness are evaluated prior to the implementation, and they are currently available through multiple commercial forensic tools (Barmpatsalou et al., 2013; Al-Dhaqm et al., 2020; Reedy, 2020). The acquisition techniques used in mobile forensics have been categorized using the classification system suggested by National Institute of Standards and Technology (NIST). The classification system includes the following five levels (Ayers et al., 2014; Chernyshev et al., 2017):

- Level 1: Manual Extraction

An examiner directly manipulates the target mobile device using the device's input interface (i.e., keypads and buttons), and records the content shown on the display of the device.

- Level 2: Logical Extraction

Data (i.e., files and folders) on the target mobile device is extracted through communicating with its wired/wireless connection interfaces. The extracted data is human-readable since it is in a format that is recognizable by computer applications.

- Level 3: Hex Dumping/JTAG

The full or partial raw data (hex dump) stored in the storage media on the target mobile device is acquired if the techniques categorized in this level are used. The debug interface on the target mobile device, such as JTAG (Join Test Action Group), is generally used to perform hex dumping. Techniques that can acquire raw data without hardware destruction are generally categorized into this level.

- Level 4: Chip-off

Chip-off requires physical removal of the non-volatile memory chip from the target mobile device. An examiner can obtain an identical copy of the entire raw data of the target mobile device, which possibly contains remnants of deleted data.

- Level 5: Micro Read

Micro read is a highly-specialized technique, where the stored data in non-volatile memory is extracted in electrical property form through the direct observation of the memory die inside the non-volatile memory chip.

Data acquired through Level 1 and 2 techniques is usually called logical data, while data acquired via Level 3 to 5 techniques is called physical data and has the advantage of including remnants of deleted data. Generally, data parsing is required to present human-readable data after acquiring physical data.

The common understanding in traditional mobile forensic models has been that the higher the acquisition level, the higher the chance of forensic data recovery. As examiners use a higher acquisition level, the accessible range of data becomes wider. Furthermore, physical acquisition can bypass the user authentication mechanisms on smartphones such as pin-codes and passwords in the

course of accessing stored data, and it does not require the target device to be in the normal-booting status. Therefore, law enforcement agencies have widely adopted chip-off data acquisition as the highest-level data extraction technique from various mobile devices. Note that even though micro read is ranked as the highest level in the above mentioned classification system, and although past research had proved that reading the data directly from the memory die is possible (Courbon et al., 2017), in practice, it is not regarded as the practical mobile data extraction technique in mobile forensics to the best of the authors' knowledge.

### 2.2. Encryption and other security features in modern mobile devices

In order to protect user privacy and provide confidentiality of data, encryption techniques are currently implemented in modern mobile devices by default. Traditionally, in mobile devices, encryption techniques were applied at the application level in order to protect individual user data such as emails and photos. With the growing concerns over security and privacy, however, encryption techniques are now implemented at the system level with hard-coded unique passwords which are not accessible, even by device manufacturers. Therefore, mobile device data at rest is stored in an encrypted manner. Two types of encryption schemes are frequently used in mobile devices. One is Full Disk Encryption (FDE) and the other is File Based Encryption (FBE) (Loftus and Baumann, 2017). FDE is a technique where the entire user data partition is encrypted with a single encryption key, while FBE encrypts data per file bases with different keys, allowing files to be decrypted independently. In Apple devices, FDE was first introduced in iPhone 3 GS with iOS 3.X (Teufl et al., 2013). Apple devices with iOS versions higher than 8 use FBE. In Android devices, FDE was introduced in Android 4.4, and was supported up until Android 9. Starting with Android 7.0, FBE has been used as the standard encryption technique. Today, it is reported that more than 80 percent of the Android devices on the market are running on an Android version higher than 6 (Statista, 2013). This means that user data in the Android devices that are seized during the criminal investigation is now mostly encrypted.

In addition to encryption techniques, other "security by design" features are implemented in modern mobile devices. One example is Root of Trust (RoT). When a mobile device boots, each hardware and software component in the boot-chain is validated to ensure that only authorized components are executed on the system. If the validation fails due to unsigned software or for other reasons, the target device does not boot, denying access to the device by malicious users. This makes traditional data acquisition techniques such as the ones suggested by Vidas et al. (2011) unworkable. The Trusted Execution Environment (TEE), which is also heavily used, provides an isolated

environment for security critical components in a system, by separating a normal operating system from a much smaller secure operating system, both running on the same hardware device. Hence a secure world and a normal world can co-exist on a system. ARM's TrustZone technology is largely used in Android devices. While Apple uses a similar technology called Secure Enclave Processor (SEP) for isolating the cryptographic key and other sensitive information processing. When implementing the TEE, even "rooting", or acquiring the highest privilege in the system does not allow access to the key data. By including those security features, mobile device manufacturers are protecting not only user data, but also their corporate proprietary data and technologies. As a result, users have little freedom to control their own mobile devices, and they are limited to using them within the device vendor's closed ecosystem.

### 2.3. Impact of security features on traditional mobile forensic techniques

As discussed, the popular use of encryption, along with complicated security measures on modern mobile devices, is impacting the capability of traditional forensic data acquisition techniques. The effectiveness of the five-level model of mobile forensic extraction techniques which we discussed in section 2.1 can be evaluated as follows in the presence of security features. Note that we assume that the user configurations are set up in a way to enable all the security features on the target device.

- Manual Extraction

In order to perform manual extraction on a modern encrypted mobile device, an examiner needs to know and possess the legitimate user authentication credentials (i.e., pin-codes, passwords, or fingerprints), to properly unlock the target smartphone in a fully operating state. A proper control will display the user data on the target smartphone screen, and the examiner can record its contents using an appropriate recording device. The remaining problems are application security mechanisms for which access codes are needed.

- Logical Extraction

The same requirements for manual extraction can be applied to logical extraction. Once an examiner can take control of the target data with correct user authentication credentials, then the examiner needs to proceed to modifying the system settings such as authorization of the debugging operation, in order to extract logical data through connection interfaces.

- Hex Dumping/JTAG

While JTAG and other debugging interfaces are still used on modern mobile devices, in many instances, those interfaces are disabled or locked before devices are shipped from the factory. Therefore, examiners may first need to find a way to utilize those debugging interfaces for hex dumping on the target device. Once enabled, hex dumping is still an effective data acquisition method to bypass the device lock. However, as the acquired physical data is in an encrypted state on modern smartphones, decryption procedures are required after data acquisition. The encryption keys are often derived from both the user defined access code, and a cryptographic key stored in the phone which is protected in such a way that it can only be used by authorized software on the device (Apple, 2020).

- Chip-off

Similar to hex dumping, chip-off lets an examiner acquire the physical data of the target device by bypassing the device lock. As discussed for hex dumping, however, the acquired data is unreadable until it is decrypted.

- Micro Read

Past research shows that reading memory data at die level is possible (Courbon et al., 2017). However, the miniaturization of the modern semiconductor fabrication process along with its ever-increasing capacities make this procedure impossible. Additionally, even if an examiner can successfully extract the contents of the non-volatile memory from the target mobile device, the data is encrypted. Techniques used in micro read may still allow examiners to extract key materials and analyze hidden security mechanisms from components on the target device, however it remains as an arduous task.

Contrary to traditional beliefs, going higher in the five-level model is not necessarily more effective in forensic data recovery for modern smartphones. Unless decryption techniques are established, acquiring physical data does not yield meaningful data.

**3. Currently used data extraction techniques from encrypted mobile devices**

In this section, current major forensic data extraction techniques from modern mobile devices, along with drawbacks with device security features, are introduced. While there are some exceptions in practice where more data extraction methods are available, for example when the target device is already "jailbroken" or "rooted", we exclude those scenarios in this paper.

### 3.1. Manual/logical extraction

In cases where an examiner can obtain the user authentication credentials required to unlock the device, or the target device is not locked, the examiner can manually manipulate the device, and perform manual or logical extraction. The user authentication credential required for unlocking the device could be a password, a passcode, pattern-drawing, or a biometric characteristic (fingerprint, voice, face, or other biometric features). If one of the biometric characteristics is used for user authentication, law enforcement investigators in some jurisdictions may be able to spoof the authentication by seizing and copying the fingerprint of the device owner, then use it to unlock the target device. Note that in most cases biometric authentication only works if the target device is in After First Unlock (AFU) state, and not equipped with other advanced security features such as inactivity-time detection measures. AFU means that the target device is in a state where it has been turned on, and unlocked with user secret at least once after booting, and never turned off since then. When the target mobile device is in Before First Unlock (BFU) state (it has never been unlocked since last booting, or it is turned off), a password, a passcode, or pattern-drawing is required to unlock the device and enable the biometric authentication. Additionally, most biometric authentication methods have a limited timespan (e.g. 48 h for current iOS devices) in which biometric characteristics can be used before the BFU code would be required again. For unlocking the device, examiners should note that there is a "panic" password option available in some modern smartphones. When set up, the panic password can execute a hidden rule, such as wiping data, or disabling some functions of a phone. If the panic password was used instead of the legitimate unlocking password prior to data extraction, manual extraction would fail, and there is a great chance that the data is unrecoverable. Modern mobile devices are also equipped with anti-brute-forcing techniques. After a set number of failed authentication attempts with incorrect user authentication credentials, the device becomes unavailable for a set amount of time. In the worst case, data on the target device can be erased and become unrecoverable.

Once the target device is unlocked successfully, logical extraction can be performed by sending backup commands through user level communication interfaces on the device, such as USB, external storage, Wi-Fi, and Bluetooth. The target phone needs to be configured to accept

commands from the connected computer for data extraction. On some modern mobile devices, rooting it (escalating the administrator privilege) is required. Data access management is generally controlled at the application level, and forensic software can use this function to copy selected app-relevant data to a connected storage device. However, in modern mobile devices, applications may choose not to be part of the backup operations supported by the OS. If the user data from an opted-out app is required for extraction, downgrading the app version on the target smartphone may allow examiners to extract the user data. However, since this operation directly modifies the target smartphone, it should be regarded as the last option.

### 3.2. File system extraction

When basic manual or logical extraction is performed for data acquisition, an examiner can only collect files and folders related to selected apps or communication protocols, and deleted data cannot be recovered. Traditionally, this is where mobile forensic examiners decide whether they proceed to physical acquisition or not. However, since most modern mobile devices use known file systems (i.e. APFS for Apple iOS devices, and ext4 for Android devices), and their data is stored on non-volatile memory in a file system structured format, acquiring full or partial file system data through non-destructive methods is currently a popular data extraction technique for forensic purposes. Compared to traditional logical extraction, file system extraction allows examiners to acquire more data, potentially including deleted data remnants. All data related to the apps is collected, and a forensic tool does not have to communicate and acquire individual data through an app-level API. An examiner can therefore access app-related databases, system files and logs. As long as the deleted data remnants remain in the database, an examiner can recover some deleted data through file system extraction. In order to conduct effective file system extraction, rooting the device is required. Without rooting, examiners can only acquire partial data, and data recovery may be limited.

### 3.3. Cloud data acquisition

Modern mobile devices store data not only on the physical device, but also on cloud servers provided by manufacturers or OS vendors. Indeed, since the physical device has limited storage capacity, some apps upload old data to the cloud server, and then delete it from the local storage. Once a law enforcement investigator acquires information required to access the cloud server from the target devices (i.e., user credentials) the investigator may access the cloud server, and collect information belonging to the target device. While some forensic tools already have cloud data acquisition capabilities, as this acquisition process requires the use of user credentials, as well as

data transfer through the internet from different jurisdictions, court orders and other additional legal procedures are often required. Legal issues regarding this procedure are discussed in Section 5.

### 3.4. Bypassing device lock/extracting lock-related information

Accessing the user data stored in the internal memory in the locked and encrypted devices typically require unlocking with the correct user authentication credential. However, chances are that user credentials remain unknown to investigators in most cases. Moreover, as mentioned before, brute-forcing all the possible passcodes/passwords/patterns is not realistic due to the preventive technologies implemented on modern mobile devices as discussed in 3.1. Therefore, methods to either bypass or disable device locks of modern mobile devices have been explored by security researchers. Methods such as deleting the lock-related data on the target device, or modifying boot processes to skip the lock operation, have been developed in order to bypass the lock mechanisms and access the user data. In addition to disabling and bypassing the lock, methods to disable the timing restrictions against brute-forcing have also been explored, enabling the brute-forcing directly on the target device (Skorobogatov, 2016). When identifying lock or timing restriction bypassing procedures, often times, system vulnerabilities are exploited (Fenollosa, 2019; Austinlog and Andro, 2015). Through exploitation, an examiner can brute-force the user authentication credential on the device itself, or extract intermediate information from the device which can be used for recovering the user authentication credential through computation on a designated system off the device. If the intermediate information only resides on the volatile memory on the target device, acquiring required information through vulnerability exploitation is only effective when the device is in AFU state.

### 3.5. Physical data extraction

Acquiring the physical data of the target mobile device lets examiners bypass its lock mechanism, and allows them to access the internal data directly. Since data decryption procedures are required on modern mobile devices after acquiring physical data, extensive reverse-engineering has been performed by security researchers to identify decryption methods. Through the authors' experience, data decryption methods have been established for several models of modern mobile devices. For these models, physical data can be acquired through the methods described below.

#### *3.5.1. Physical chip-off*

Chip-off analysis (Willassen et al., 2005; Fukami et al., 2017; Breeuwsma et al., 2007) refers to a forensic operation where the memory chip of the target device is physically detached, and then the

internal data is dumped for subsequent reconstruction of human-readable data. Detailed chip-off analysis procedures can be found in Breeuwsma et al. (2007). During chip-off, the non-volatile memory chip is physically removed from the circuit board, and its content is extracted through the specialized reader. Since physical chip-off is a destructive procedure, it is important for an examiner to know if any other component on the board is required for decrypting the data. This is especially important if chip transplant procedures (Heckmann et al., 2018) need to be performed for severely damaged phones.

*3.5.2. In-System-Programming (ISP)*

While chip-off requires a destructive operation to the target device, if the required device pins for reading the target memory chip are accessible without detaching the chip itself from the circuit board, an examiner can perform In-System-Programming (ISP) for physical data extraction (Silveira et al., 2020). By connecting a memory reader to electrical traces connected to the memory chip on the circuit board, an examiner can access the memory chip and create a bit-by-bit copy of the target memory without damaging the operative state of the target mobile device. In order to successfully acquire data through ISP, the related part of the circuit board of the target device needs to be non-defective. In some cases, where no trace is available on the surface of the circuit board, partial chip decapsulation with laser ablation may be required to perform ISP. When performing ISP, an examiner needs to have a proper understanding of signal integrity and other electrical details. eMMCs (embedded Multi-Media Cards) and eMCPs (embedded Multi-Chip Packages), which have been widely used in embedded devices, use single-ended signals, therefore simply connecting the traces may let examiners read the memory data. However, new memory technologies like UFS (Universal Flash Storage) use high speed differential signals (JEDEC, 2020). Performing ISP is therefore becoming challenging as making external connection on a circuit board can greatly disturb the signal integrity.

**3.6. Data acquisition with custom boot loaders**

If an examiner can load a custom boot loader into the target device during the boot process and run it, there is a great chance that the device can be manipulated by running arbitrary code, making physical data acquisition possible. Traditionally, loading a custom boot loader was enabled by the device manufacturer. Special modes (i.e., download mode or rescue mode) allowed users to run a custom boot loader on the target system during the boot-up. In modern devices, however, in order to maintain system integrity, manufacturers enable boot loaders to run only after they are properly verified to be signed, allowing only their codes to run on the device. The boot loaders are

responsible for initializing hardware components and loading the operating system which then starts device operation including encryption. When a modern mobile device is powered on, multiple boot loaders are executed in chain. The first boot loader which is hard-coded in the ROM of the application processor is called bootROM or primary boot loader (PBL), and the one that is loaded by this bootROM is called the secondary boot loader (SBL). The SBL normally loads another boot loader that finally loads the operating system (Hay, 2017). Only when the verification processes are passed, is the boot loader loaded into the system memory, allowing the system to start the normal booting operations. Loading boot loaders through download mode is performed at the SBL level. The verification processes are usually done by checking if each boot loader is properly digitally signed. This process uses the initial verification key, which is stored in the one-time-programmable memory area in the application processor, thereby ensuring the key is never tampered with.

For some models of modern mobile devices, signed boot loaders may be publicly available (Hay, 2017). By flashing those boot loaders with known vulnerabilities into the target smartphone, an examiner may gain the highest privilege in the target phone, which in turn leads to full control of the device, allowing successful acquisition of the memory data. An examiner can also try to downgrade parts of the boot chain to lower versions as long as anti-rollback mechanisms are not implemented on the target mobile device. By doing so, the examiner can exploit known vulnerabilities that are fixed with security updates in the actual version of the boot chain. Nevertheless, the most powerful way of breaking into the boot chain to run the arbitrary code is to exploit the bootROM vulnerability, and this technique has been explored and used for accessing data in modern mobile devices (Katalov, 2019).

While modern mobile devices prohibit users from loading custom boot loaders, it is now widely known that PBL-level flashing is possible by booting the device into the processor-level special boot mode. The name of this boot mode is different by each manufacturer. It is called Emergency Download (EDL) for Qualcomm chipset, Device Firmware Update (DFU) mode for Apple chipset, and Download mode for MediaTek chipset. Those modes allow the phone manufacturers to flash software on their devices. Forensic examiners can thus utilize those modes and flash crafted boot loaders into the target smartphone, which helps them acquire user data without modifying it. Unless any additional authorization mechanism is implemented, a set of commands, a special cable, or hardware modifications make the target devices go into those special modes. Data acquisition using custom boot loaders is becoming popular since the same technique could work on wide range of devices with the same chipset, and it is typically hard for mobile device manufacturers to patch the

vulnerabilities at processor level. Research has already proved that vulnerabilities on boot-loader level on popular chipsets can be useful for user data acquisition (Hay, 2017; Alendal et al., 2018).

## 4. Emerging techniques

In addition to the forensic data acquisition techniques described in the previous section, the following methods have been researched as possible techniques useful for forensic data extraction from modern mobile devices.

### 4.1. Side-channel analysis

When Integrated Circuits (ICs) operate on a circuit board, information related to these ICs may leak in the form of current flow or electromagnetic (EM) emanations. This information can sometimes be used to extract internal secrets such as cryptographic keys (Sayakkara et al., 2019). This type of analysis is called side-channel-analysis (SCA), which has been a popular security research field for smart card and other security technologies. Recent work has proved that SCA can be used to retrieve a cryptographic key from the application processor in a modern mobile device (Vasselle et al., 2019). Although research is required for each application processor since the processors are unique, SCA is a promising technique for acquiring cryptographic keys from modern mobile devices. Once acquired, the key can be used to decrypt bootloaders. Meanwhile, in addition to shrinking technology size, device manufacturers are adding features like heterogeneous operation and voltage frequency optimization in order to minimize SCA vulnerabilities.

### 4.2. Fault injection

Fault injection is a technique where inputs of the controller device are manipulated for the purpose of causing illegitimate behaviors to the target system. Examples of fault injection techniques are glitching or underfeeding the power supply, transmission of electromagnetic signals, and injecting optical beams. Research has already been performed to show the efficiency of fault injection for attacking the boot sequence and extract the code with the highest privileges from an Android device (Vasselle et al., 2020). Fault injection may also be useful for disabling the lock of debugging interfaces such as JTAG on the target device.

### 4.3. SoC reverse engineering

System on a Chip (SoC) die-level reverse engineering physically accesses inside SoCs on mobile devices, and examine the internal circuits using highly specialized lab equipment. Through SoC die-level reverse engineering, one can learn how the system is structured by checking internal circuit connections. A semiconductor die consists of multiple layers interconnected with each other. By delayering each layer, and translating the connection into a circuit, one can retrieve the overall

design and try to learn and understand how the target system works. SoC reverse-engineering have been performed for multiple intentions, including piracy or counterfeiting reasons (Quadir et al., 2016). One key motivation for SoC die-level reverse engineering for forensic purposes is to retrieve hardware-bound key information, which is stored in the one-time-programmable memory area in a SoC, as discussed in section 3.6.

## 5. Legal issues related to modern forensic technologies

Since the data provided through forensic analysis may subsequently be relied upon in court, it is always important for forensic examiners to be aware of the legal framework regulating decryption for digital evidence acquisition. In a historical perspective, there are four legislative approaches for granting decryption powers to law enforcement – *(i)* exceptional access; *(ii)* decryption orders; *(iii)* vulnerability exploitation; and *(iv)* cloud data access. Details of each approach are discussed in this section.

### 5.1. Exceptional access

Methods providing law enforcement with exceptional access to encrypted data were proposed in the past and are related to backdoors in hardware and software, key escrow systems, and weak cryptography schema. Key escrow allows covert cooperation of independent parties with law enforcement to facilitate the use of the backdoor to decrypt the communication (ENISA, 2016). Examples of weak cryptographic algorithms are Simon and Speck (Beaulieu et al., 2015), which were rejected by the International Organisation for Standardisation due to discovered NSA-designed backdoors (Schneier, 2018). Currently, exceptional access is rejected both by legislators and security experts as it is imposing a high risk for human rights and civil liberties, especially with respect to data protection and privacy (Liguori, 2020), results in a golden age of surveillance, undermining security globally (Europol and ENISA, 2016), renders the systems vulnerable to attacks by criminals (Koops and Kosta, 2018), and requires significant development costs (Penney and Gibbs, 2017). ENISA and EUROPOL stated that backdoors and key escrow must be prohibited (Europol and ENISA, 2016). This means that technical cooperation between mobile device manufacturers and LEAs is currently unlikely, even for forensic data extraction.

### 5.2. Decryption orders

In order to address encryption challenges in criminal investigations without exceptional access, multiple countries introduced decryption orders. Such orders allow compelled disclosure or assistance by service providers or manufacturers (Lewis et al., 2017), and the orders are enforced with penalties in some countries. In the United Kingdom and France, refusal to disclose the

encryption key can lead to criminal penalty. Similarly service providers carry civil liability, and in Belgium even criminal liability for failing to comply with obligations to assist law enforcement in criminal investigations (Walden, 2018). Norway is one of the first countries to update its legislation in 2017 allowing law enforcement to obtain biometrics for unlocking devices (Koops and Kosta, 2018). Less trivial is the question of compelled disclosure of password by suspects since unlike biometrics, a password does not exist independent of the suspect's will. Compelled disclosure for suspects is likely to remain controversial and for exceptional cases (Koops and Kosta, 2018) since it creates concerns about the privilege against self-incrimination, right to silence and abuse of state power. Moreover, this solution is unsuitable when the user was unidentified, unable or unwilling to provide the key (Penney and Gibbs, 2017; Shah, 2015). Decryption orders for cooperation with providers or manufacturers also have significant drawbacks for privacy and security. Given that backdoors are forbidden it is hard to understand how providers must comply with a requirement to decrypt communication in transit or at rest. Propositions for in-house digital forensics by providers and manufacturers are also dubious considering that law enforcement agencies will be provided only with the decrypted data without information on the used forensic method, its reliability and the accuracy of the results.

### 5.3. Vulnerability exploitation

Considering the manifold drawbacks and limitations of exceptional access and compelled disclosure, new legislation regulating "lawful hacking" has already been introduced in several countries (Gutheil et al., 2017). Most types of lawful or governmental hacking are considered exceptional and highly intrusive. We focus here on exploitation of known system vulnerabilities since it proves to be highly useful for mobile evidence acquisition and less-intrusive in comparison to interception or development of malware. Vulnerability exploitation is broadly understood as use of any type of vulnerability, including social engineering and side-channel analysis. According to law, exploiting vulnerabilities must be employed by law enforcement agencies as a last resort after other less intrusive investigation measures have failed (Liguori, 2020). This is understandable since such practice creates an increased risk for privacy violations and data leakage, may undermine security, requires a vulnerability disclosure framework, and has international economic, political and technological effects (Budish et al., 2018; Liguori, 2020). However, as demonstrated in section 3 and Section 4, in practice often times this is the only viable solution to access encrypted mobile phone. Liguori argues that a legal framework for lawful hacking must be developed to address the following key issues: *(i)* legal concept/scope; *(ii)* prerequisites for

deployment; *(iii)* development and sharing of hacking tools; *(iv)* accountability and disclosure of vulnerabilities; and *(v)* jurisdictional issues (Liguori, 2020).

The existing few national legislations on lawful hacking provide some safeguards for human rights and to prevent abuse of power by law enforcement (Gutheil et al., 2017). Ex ante safeguards include judicial authorization and limiting the measure by crime type and duration. Importantly, ex post control includes strict reporting and oversight of lawful hacking, as well as notification of targets of hacking practices and remedies in case of abuse of powers. However, new lawful hacking regulation in the US, France, Australia, and Germany still faces major challenges related to lack of vulnerability disclosure processes and ensuring transparency and accountability of law enforcement agencies (Liguori, 2020).

A report on government disclosure processes in Europe stated that only a limited number of countries have a transparent procedure for vulnerability disclosure (Pupillo et al., 2018). Similar to the US Vulnerabilities Equities Process (VEP), the report recommends adoption of procedures by all law enforcement agencies, where they have: *(i)* an obligation to report vulnerabilities; *(ii)* may only temporarily restrict knowledge of a vulnerability; and *(iii)* an oversight body ensures compliance. In the absence of clear legislation in relation to obligations of law enforcement to disclose vulnerabilities, to whom and under which condition, forensic examiners might be put in a position to take legislative decisions. This inevitably leads to undesirable practices. Law enforcement might be reluctant to disclose vulnerabilities to providers or users in order to exploit them further for evidence acquisition. Even on trial proceedings, investigators might be unwilling to disclose sensitive investigation methods related to security flaws in systems, and unfortunately we have seen the use of alternative explanations for how evidence was found, a practice known as “parallel construction.” (Criminal Legal News, 2018; Human Rights Watch, 2018).

Consequently, exploiting known vulnerabilities for mobile forensics is a justifiable and reasonable approach, as long as it is strictly regulated and assures protection of civil rights and liberties. As examined, very few countries have regulation in place and due to the international effects of such activity a European Regulation or an International treaty might be preferable (Budish et al., 2018). Unlike known vulnerabilities for access to evidence, the use of zero-day exploits might create vulnerability market for law enforcement (Liguori, 2020). Therefore, they are unlikely to meet the requirements of proportionality and subsidiarity, and might be permitted only for serious crimes or terrorism (Koops and Kosta, 2018).

### 5.4. Access to cloud evidence

Since data from phones is often copied to cloud storage and duplicated in multiple back-ups, lawful access to cloud data is another alternative for law enforcement to obtain information, by directing a search order to the cloud provider (Pell, 2016;Walden, 2018). Cloud data from mobile devices is a rich source of evidence, however the legal and technical challenges for law enforcement are not trivial. So far, only the United States (US) has introduced legislation to regulate lawful access to cloud storage. According to the CLOUD Act (The CLOUD Act, 2018) foreign governments can compel US-based Cloud Service Providers (CSPs) to directly disclose stored data or intercept communications in real time, if they have entered a bilateral agreement with the US government.[1] The CLOUD act explicitly states that it shall "not create any obligation that providers be capable of decrypting data (Walden, 2018). Therefore, in case of 'zero knowledge privacy', meaning that the provider never knows the plain text content of the data being stored, law enforcement must rely on other techniques to decrypt the data themselves. In the European Union (EU), there is a pending proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, that would allow law enforcement access to service provider datam including in encrypted form, but the proposal has been on hold for the past two years (Sippel, 2021). The European data protection board criticized it for lack of sufficient safeguards (Board, 2020). Despite the struggles to establish EU-based e-evidence regime, the EU Commission entered further negotiations with the United States to reach an agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters (Council of the European Union, 2019), that might result in deepening the existing legislative loopholes. In the US, the CLOUD act imposes further challenges since there is no clear procedure to ensure that data disclosure to a foreign government meets the requirements laid out in the bill while service providers are inappropriately empowered to mediate between their business interests, human rights, and law enforcement interests (Abraha, 2019). The legislation is broadly criticized on the grounds that it (i) fails to clarify who should be subject to a search warrant in a layered cloud service arrangement; (ii) does not define digital evidence, categories of data, and types of "serious crimes" where cloud access is justified; (iii) lacks judicial review; and (iv) has weak protection of privacy and procedural rights.[2] Moreover, from a cloud forensics perspective, there are specific risks to the reliability of cloud evidence related to remote acquisition, reliance on CSP assistance, loss of volatile data in virtual machines, and encryption (Zawoad and Hasan, 2013; Pichan et al., 2015). It should also be noted that due to synchronization issues cloud back-ups might not contain all the data available in mobile phones (Jacobsen, 2017). Currently, neither the EU nor the US legislator mention any

requirements for reliability of digital evidence or digital forensics procedure. Same gap is identified in the proposed Second Additional Protocol to the Cybercrime Convention (Council of Europe, 2018). As of today, a EU–US consensus has not been reached, and the patchwork legislation shows the need for an international treaty for regulating encryption, access to cloud data, and digital evidence exchange according to internationally-agreed digital forensic standards.

### 5.5. Alternative solutions

Some authors discuss alternatives to the existing types of legislation. Proposals include (i) restricting the design, use and sale of encryption; (ii) improving law enforcement data analytics capabilities, or regional decryption labs (Lewis et al., 2017); and (iii) criminalization of the supply, possession or use of cryptographic technologies for criminal conducts. However, most of them suffer unfavorable limitations. Law enforcement agencies need to develop new decryption methods continuously, which is time and resource consuming. Moreover, law enforcement agencies can hardly compete with new security by default solutions included in mobile devices and operating systems. As discussed in section 4, law enforcement examiners need to keep performing reverse engineering to access encrypted phones. Reverse engineering is an indispensable method for law enforcement in order to correctly interpret the system structure, security features, file systems, and other software details for the purpose of evidence acquisition and tool testing. However, current legislation insufficiently addresses the tension with vendors' intellectual property and trade secrets protection and the need of law enforcement to perform reverse engineering to collect digital evidence. Moreover, legislation often does not addresses issues with reverse engineering techniques for evidence acquisition in relation to obligations for data protection, security and vulnerabilities disclosure, and procedural obligations like cross-examination in court.

The new model for mobile acquisition proposed in this paper includes vulnerability exploitation capabilities and contributes for the standardization and minimisation of forensic hacking techniques in evidence collection. It will provide a clear understanding regarding the intrusiveness of each level in the model, and when it is justified to exploit vulnerabilities for mobile forensics purposes. The model also accommodates cloud and reverse engineering acquisition.

## 6. New mobile forensic model

As we have seen through section 3 and section 4, current approaches for accessing user data in modern mobile devices have changed greatly from traditional ones. Traditionally, forensic data extraction techniques have focused on acquiring physical data, which when subsequently parsed can

recover deleted data. This approach used to be effective because the data was stored in clear-text on non-volatile memory on mobile devices. As a result, the five-level data extraction model has been followed as a standard model. However, with the implementation of encryption and other complex security features, simply acquiring raw data does not help recover user data any more. Worse, destructive procedures such as chip-off may destroy key components needed to decrypt acquired data. Moreover, secure deleting features on mobile devices can effectively delete data remnants on the system, and recovering deleted data from physical data is becoming almost impossible. Additionally, without user authentication credentials, acquiring user data, be it logical or physical, is becoming a great challenge, regardless of the acquisition level. Therefore, categorizing the mobile data extraction method by the extracted data type is becoming less effective. Currently, either extracting the data in clear-text, or extracting the encryption key is the major objective in forensic data extraction. Without the right user authentication, this can only be achieved either by exploiting system vulnerabilities on the target device or by identifying and accessing the stored cryptographic keys. However both methodologies require extensive reverse-engineering prior to working on the target mobile device. Taking this current situation into account, we propose a new mobile forensic data extraction model as follows:

- User secret based acquisition

If an examiner can unlock the phone with the correct user authentication, the target smartphone can be manually operated, and can be set up in a way that it authorizes data extraction through its user interfaces. Manual and logical extraction introduced in section 3.1 fall into this category. As discussed in section 5, compelled disclosure of the password from the device owner is not regarded as an appropriate method. However acquisition may be available through seizing biometric information of the device owner. After unlocking the device, an examiner can modify the device setting, and extract either logical, file system, or physical data by rooting the device.

- Reverse-engineering based acquisition

Reverse-engineering of modern mobile devices is essential in forensic study. Reverse-engineering can be done both in software and hardware. Once an examiner learn the internal structure of the target mobile device operation through reverse-engineering, the examiner may be able to reconstruct the original user data. One example is to identify encryption mechanism and to retrieve the

encryption key. Once those information can be retrieved, an examiner can acquire the physical data from the target smartphone with methods discussed in section 3.5, and then decrypt the data off-device.

•

Vulnerability exploitation based acquisition

When the target device is locked and encrypted, these features need to be either bypassed or disabled for data extraction. Bypassing or disabling the device lock, encryption, and other security features generally require exploiting system vulnerabilities. The vulnerability exploitation may require the combination of hardware and software attacks. Once those features are bypassed, examiners can choose to acquire either full or partial logical, file system, or physical data. As discussed in section 5, use of open and unpatched vulnerabilities is justified from a legal perspective. However, in many cases zero-day vulnerabilities found through extensive reverse-engineering are required for effective data extraction. Multiple works have already shown the effectiveness of vulnerability exploitation in digital forensic domain (Alendal et al., 2018; Hay, 2017; Shwartz et al., 2017).

Fig. 1 shows a simple flowchart for choosing a proper data extraction technique. Each technique is categorized according to the above mentioned model.

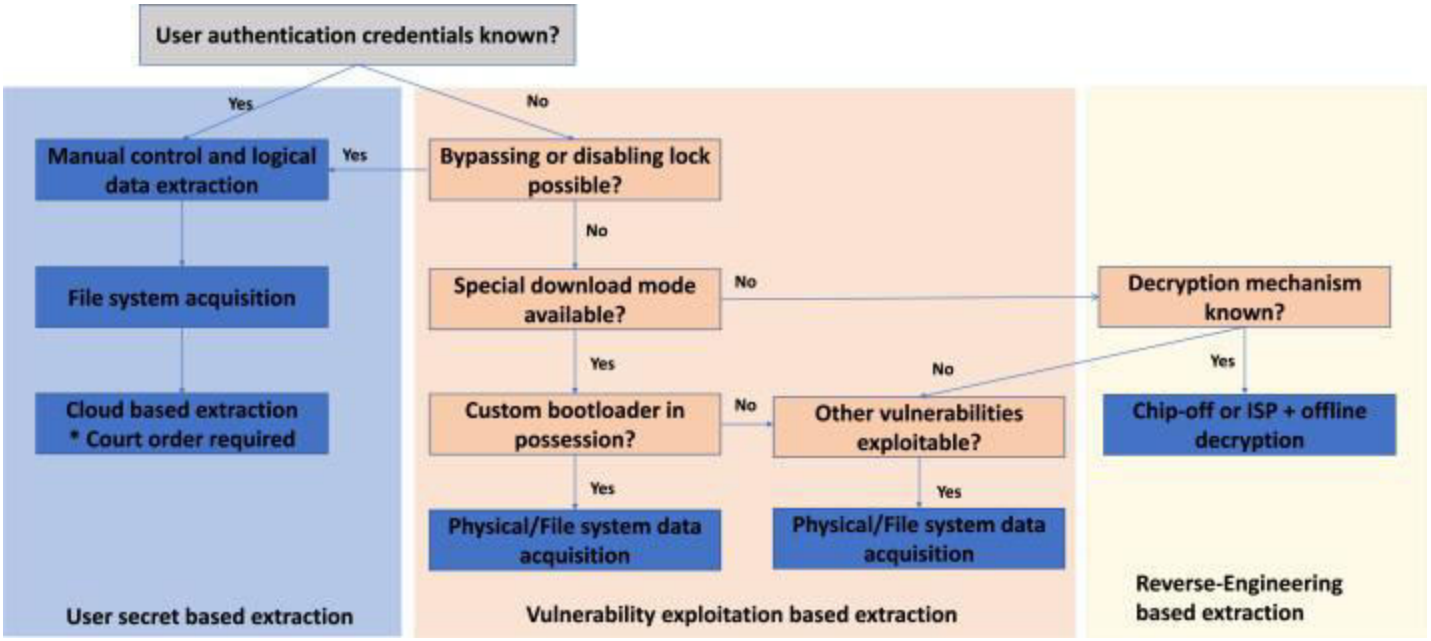



Fig. 1. New mobile forensic data extraction model.

Essentially, without the proper user authentication credentials, system vulnerability exploitation needs to be performed. On the other hand, once the user secret is available, an examiner can use it to manually operate the target phone. Some mobile forensic tool vendors already provide automated versions of those vulnerability exploitation and data extraction procedures shown in Fig. 1. When testing and evaluating those tools, the acquisition level can be categorized using this new model.

**7. Conclusions and recommendations**

Due to growing security and privacy concerns by mobile device users, manufacturers are aggressively implementing encryption and other complicated security mechanisms. This trend is greatly affecting traditional forensic data acquisition capabilities. Traditionally, acquiring raw data from non-volatile memory on a mobile device would yield meaningful data - including deleted info - which could then be used for criminal investigations. Therefore chip-off and micro read have long been regarded as the highest level of effective technologies in forensic data acquisition. However, as we discussed in this paper, current physical data acquisition practices cannot provide human-readable data due to encryption. Also, effective data erasing functions at the OS level make it difficult to find data remnants in physical data. At the same time, other security features are making it difficult for forensic examiners to acquire even live data on the target device. Therefore, bypassing or disabling device lock and encryption while keeping user data integrity is becoming the most important forensic technique for modern mobile devices. Extensive reverse-engineering, as well as exploiting vulnerabilities, is therefore becoming essential for forensic examiners when performing mobile forensics. Vulnerabilities found through reverse-engineering have already been used for acquiring evidence data from locked and encrypted mobile devices.

In the meantime, however, the use of backdoors and vulnerabilities in forensic analysis has generated controversy and sparked policy discussions by lawmakers and human rights organizations. While exceptional access is less likely to be granted by manufacturers, the use of known vulnerabilities can be justified in the absence of less intrusive investigative measures to access evidence. Currently, there is no clear legislative rule about the use of zero-day exploits for acquiring data from encrypted devices. Responsible disclosure may, however, provide a reasonable ground rule for forensic examiners to follow.

In order to standardize and validate mobile forensic data extraction techniques, further research and efforts are needed. This may be performed by organizations such as a multi-disciplinary EU commission to evaluate the methodology, along with its proportionality and reliability. Additionally,

the legislative debate must be enriched by including forensic examiner subject matter expertise. National legislation on lawful exploitation of vulnerabilities will have negative extraterritorial political, economical, and human rights effects. Preferably, strong protection of privacy and system security with encryption must be codified in international treaty, which explicitly regulates exceptions for investigative purposes and implements universal safeguards for human rights.
As suggested in our new mobile forensic data extraction model, exploiting mobile device system vulnerabilities is essential in extracting evidence data from modern encrypted mobile devices for forensic.

**Methods to Search and seizure electronic evidence**

**Search and seizure**

Search and seizure orders along with preservation of evidence orders are often approved by the court to ensure critical evidence is not destroyed. Using the element of surprise, digital devices and data can be captured by forensic experts and preserved for future proceedings.

**LEGAL ASPECTS OF Digital FORENSICS**

Anyone overseeing network security must be aware of the legal implications of forensic activity. Security professionals need to consider their policy decisions and technical actions in the context of existing laws. For instance, you must have authorization before you monitor and collect information related to a computer intrusion. Digital Forensic is a relatively new discipline to the courts and many of the existing laws used to prosecute computer-related crimes, legal precedents, and practices related to digital forensics are in a state of flux. New court rulings are issued that affect how digital forensics is applied.

The site lists recent court cases involving digital forensics and computer crime, and it has guides about how to introduce computer evidence in court and what standards apply. Forensic investigators need to collect the evidence in a way that is legally admissible in a court case. Increasingly, laws passed that require organizations to safeguard the privacy of personal data. It is becoming necessary to prove that your organization is complying with computer security best practices.

If there is an incident that affects critical data, for instance, the organization that has added a digital forensics capability to its arsenal will be able to show that it followed a sound security policy. And potentially avoid lawsuits or regulatory audits.

There are three areas of law related to computer security that are important to know about. The first is in the United States Constitution. The Fourth Amendment allows for protection against unreasonable search and seizure, and the Fifth Amendment allows for protection against self-incrimination. Although the amendments were written before there were problems caused by people misusing computers. The principles in them apply to digital forensics practiced.

**IT act 2000**

The Act **provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures**. It also defines cyber crimes and prescribes penalties for them. The Act directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures.

The Information Technology Act, 2000 also Known as an **IT Act** is an act proposed by the Indian Parliament reported on 17th October 2000. This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997. It is the most important law in India dealing with Cybercrime and E-Commerce.

The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 90 sections. The last four sections that starts from 'section 91 – section 94', deals with the revisions to the Indian Penal Code 1860.

**The IT Act, 2000 has two schedules:**

- **First Schedule –**
  Deals with documents to which the Act shall not apply.
- **Second Schedule –**
  Deals with electronic signature or electronic authentication method.

**The offences and the punishments in IT Act 2000 :**

The offences and the punishments that falls under the IT Act, 2000 are as follows :-

1. Tampering with the computer source documents.

2. Directions of Controller to a subscriber to extend facilities to decrypt information.
3. Publishing of information which is obscene in electronic form.
4. Penalty for breach of confidentiality and privacy.
5. Hacking for malicious purposes.
6. Penalty for publishing Digital Signature Certificate false in certain particulars.
7. Penalty for misrepresentation.
8. Confiscation.
9. Power to investigate offences.
10. Protected System.
11. Penalties for confiscation not to interfere with other punishments.
12. Act to apply for offence or contravention committed outside India.
13. Publication for fraud purposes.
14. Power of Controller to give directions.

Sections and Punishments under Information Technology Act, 2000 are as follows :

| SECTION | PUNISHMENT |
|---|---|
| Section 43 | This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages. |
| Section 43A | This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party. |
| Section 66 | Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both. |
| Section 66 B, C, | Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both. |

D

| | |
|---|---|
| Section 66 E | This Section is for Violation of privacy by transmitting image or private area is punishable with 3 years imprisonment or 2,00,000 fine or both. |
| Section 66 F | This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment. |
| Section 67 | This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine of Rs. 10,00,000 or both. |

**Amendment of it act 2008:**

The IT (Amendment) Act, 2008 (ITAA 2008) has established a strong data protection regime in India. It addresses industry's concerns on data protection, and creates a more predictive legal environment for the growth of e-commerce that includes data protection and cyber crimes measures, among others.

These changes included expanding the definition of cybercrime and adding new penalties for offenses such as identity theft, publishing private images without consent, cheating by impersonation, and sending offensive messages or those containing sexually explicit acts through electronic means.