LAB MANUAL

ON

CYBER CRIME INVESTIGATION AND DIGITAL FORENSICS LAB

(R22A6283)

B.TECH III YEAR – II SEM (R22)

(2024-2025)

DEPARTMENT OF EMERGING TECHNOLOGIES

MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY

(Autonomous Institution – UGC, Govt. of India)

Recognized under 2(f) and 12 (B) of UGC ACT 1956

(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 ANDTECHNOLOGY

III Year B.Tech CSE(CyS) - II Sem (R22) L/T/P/C

0/-/2/1

(R22A6281) – CYBER CRIME INVESTIGATION AND DIGITAL FORENSICS LAB (R22A6283)

Course Objectives:

1. To provide students with a comprehensive overview of collecting, investigating, preserving, and presenting evidence of cybercrime left in digital storage devices, emails, browsers, mobile devices using different Forensics tools.
2. To Understand file system basics and where hidden files may lie on the disk, as well as how to extract the data and preserve it for analysis.
3. Understand some of the tools of e-discovery.
4. To understand the network analysis, Registry analysis and analyze attacks using different forensics tools.

Course Outcomes:

1. Learn the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong-doing.
2. To Learn the file system storage mechanisms and retrieve files in hidden format.
3. Learn the use of computer forensics tools used in data analysis.
4. Learn how to find data that may be clear or hidden on a computer disk, find out the open ports for the attackers through network analysis, Registry analysis.

List of Experiments

1. Perform email analysis using the tools like Exchange EDB viewer, MBOX viewer and View user mailboxes and public folders, Filter the mailbox data based on various criteria, Search for particular items in user mailboxes and public folders
2. Perform Browser history analysis and get the downloaded content, history, saved logins, searches, websites visited etc using Foxton Forensics tool, Dumpzilla.
3. Perform mobile analysis in the form of retrieving call logs, SMS log, all contacts list using the forensics tool like SAFT
4. Perform Registry analysis and get boot time logging using process monitor tool
5. Perform Disk imaging and cloning the using the X-way Forensics tools
6. Perform Data Analysis i.e History about open file and folder, and view folder actions using Lastview activity tool
7. Perform Network analysis using the Network Miner tool.
8. Perform information for incident response using the crowd Response tool
9. Perform File type detection using Autopsy tool
10. Perform Memory capture and analysis using the Live RAM capture or any forensic tool

TEXT BOOKS:

1. Real Digital Forensics for Handheld Devices, E. P. Dorothy, Auerback Publications, 2013.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.

REFERENCE BOOKS:

1. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010.
2. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C. H. Malin, E. Casey and J. M. Aquilina, Syngress, 2012.
3. The Best Damn Cybercrime and Digital Forensics Book Period, J. Wiles and A.Reyes, Syngress, 2007.

EXPERIMENT 1

Aim: To perform email analysis using tools like MBOX Viewer and View, and to filter and search mailbox data based on various criteria, you can follow these steps:

Tool:Mbox viewer

Procedure:

To perform email analysis using tools like MBOX Viewer and View, and to filter and search mailbox data based on various criteria, you can follow these steps:

1. Obtain the MBOX File: Obtain the MBOX file that contains the email data you want to analyze. MBOX is a common file format used to store email messages.

How to obtain MBOX File from gmail account:

1. To download specific messages, apply a label to those messages. For example, create a label titled **messages to download** and apply it to the messages you want to download.

2. Go to **https://takeout.google.com/settings/takeout.**

3. Select **Select None**.

Gmail only stores emails, it cannot store the other data on the export screen.

4. Scroll to **Mail**, select the gray **X** to the right, then:

- To download only certain messages, select **All Mail**.or
- Check **Select Labels**.(any folder which contains less mails,may be DRAFT Folder)
- Check the labels that tag the emails you want to download.
- Select **Next**.
- Do not change the file type, then select **Create Archive**

5. **A zip file** transmits to your selected delivery method (by default, you will get an email with a link to download the zip).Please select a folder in your inbox which contains less mails,so that you get mbox file zip file at the earliest).

2. Install MBOX Viewer: Download and install a reliable MBOX viewer tool like "MBOX Viewer" or "MBOX File Viewer." These tools allow you to open and view the content of MBOX files.

3. Open the MBOX File: Launch the MBOX viewer tool and open the MBOX file by either selecting the file from the application's interface or by using the "Open" or "Import" option. This action will load the email data from the MBOX file into the viewer.

4. View User Mailboxes and Public Folders: Once the MBOX file is loaded, you should be

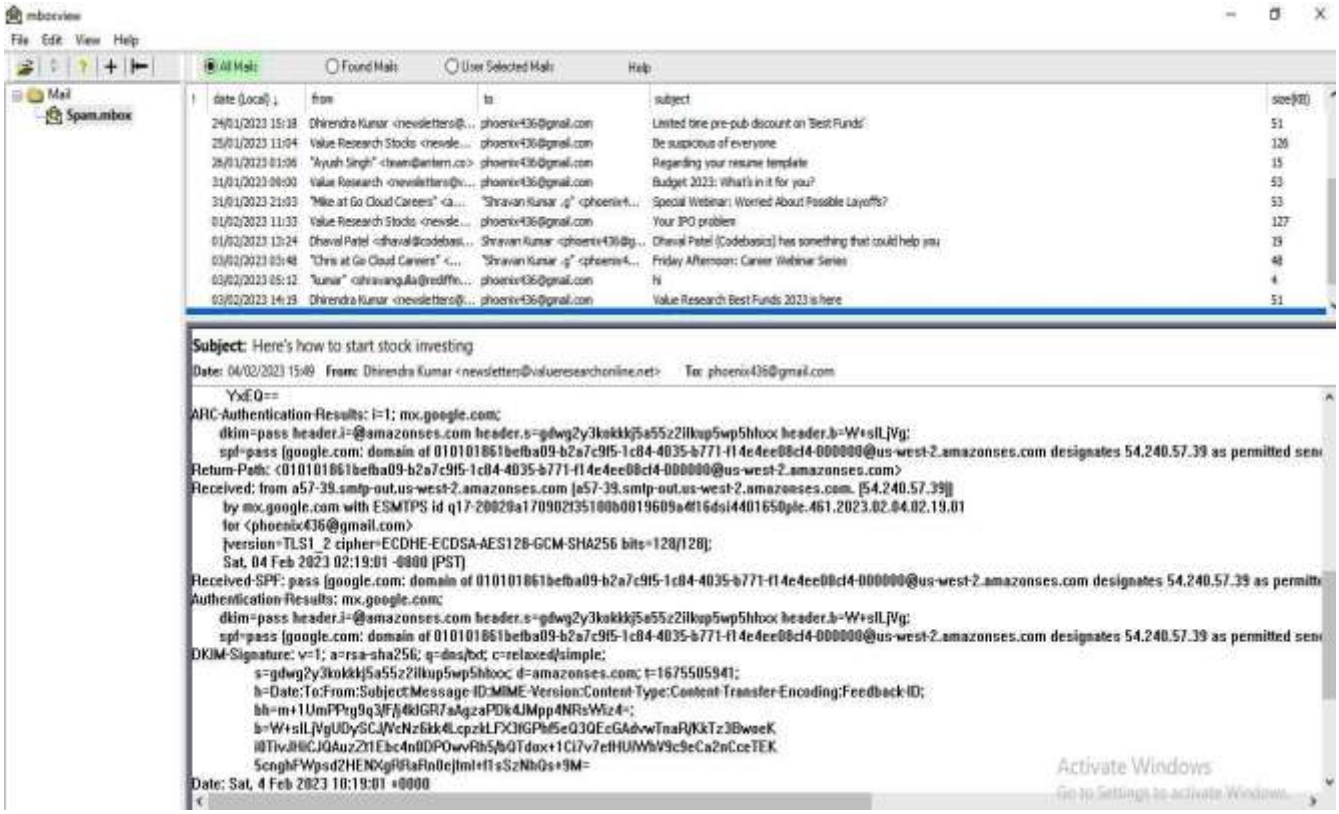
able to see the user mailboxes and any public folders that are present in the email data. These folders organize the emails based on different criteria, such as sender, recipient, subject, date, etc.

5. Filter Mailbox Data: Use the filtering options provided by the MBOX viewer tool to filter the mailbox data based on various criteria. For example, you can filter emails by date range, sender, recipient, subject keywords, or any other available metadata. Applying filters helps narrow down the data and focus on specific subsets of emails that are relevant to your analysis.

6. Search for Particular Items: Utilize the search functionality provided by the MBOX viewer tool to search for particular items within user mailboxes and public folders. You can search for specific keywords, email addresses, subject lines, or any other relevant information. The tool will display the search results, allowing you to access and analyze the emails that match your search criteria.

7. Analyze Email Content: With the filtered and searched email data, you can perform various analysis tasks, such as examining email headers, inspecting email attachments, reviewing email conversations, identifying email patterns, and extracting relevant information.

Output:



Experiment 2: The aim of this experiment is to perform browser history analysis and extract downloaded content, history, saved logins, searches, websites visited, etc. using the Foxton Forensics tool and lastviewactivity tool from nirsoft.

Tool used : Browserhistoryview and browsercapture are free tools developed by Foxton Forensics that allows for the extraction of various types of information from web browsers. This tool can be used to extract data from Firefox, Chrome, and Edge browsers. The tool can extract information such as browsing history, downloads, saved logins, cookies, and more .Browsercapture tool is used to capturebrowser data and keep it in one folder in desktop.Browserview tool is used view all data captured using Browserhistoryview.Lastview activity tool is from nirsoft.You can download this also,Both have similar kind of operation.

Procedure:

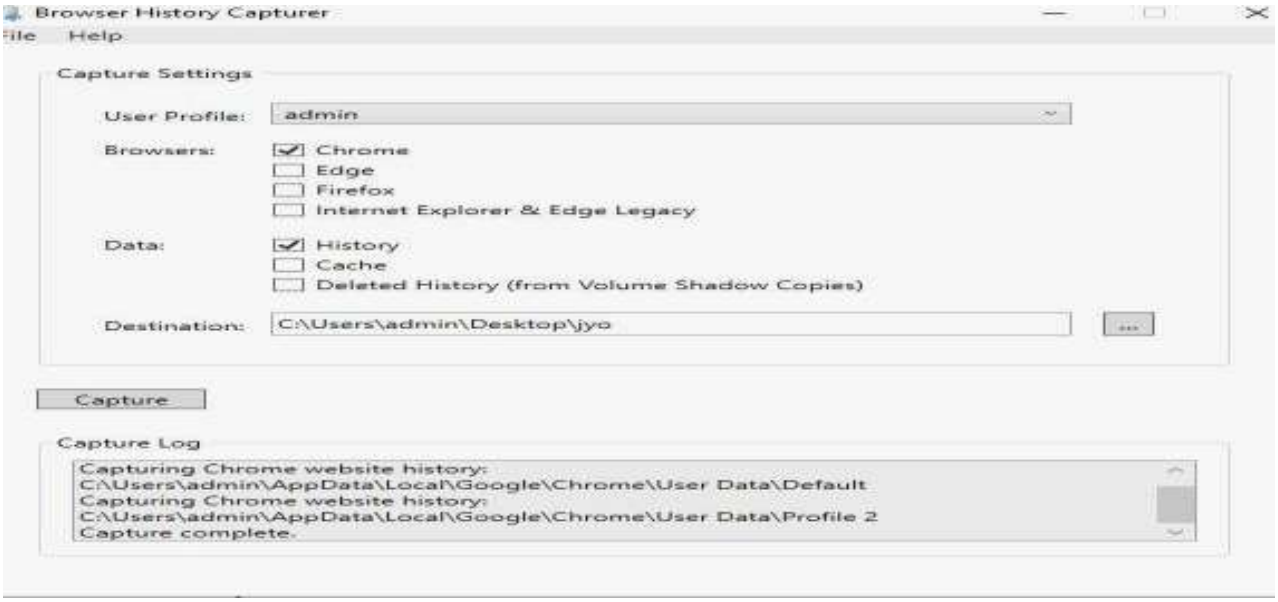
Here are the steps on how to perform browser history analysis and extract downloaded content, history, saved logins, searches, websites visited, etc. using the browser history view:

Download **Browserhistorycapture** and **Browserhistoryview** from download site of

WWW.FOXTONFORENSICS.COM by giving your emailids.You will get download

Link in your inbox for downloading.

1. Open the browser history capturer.You will get screen like this: **Fig:1**



2. Please check the marks as mentioned below as seen in below picture(admin,chrome,history).Create one folder on c folder desktop on your system and name it **xyz** .I have created JYO in the destination text box. You can create your own name. Like **xyz** and use it in the Destination text box. Once you upload the destination path of the created folder, Click on capture button. It will take some time. All details of browser will be in capture folder for further forensics.

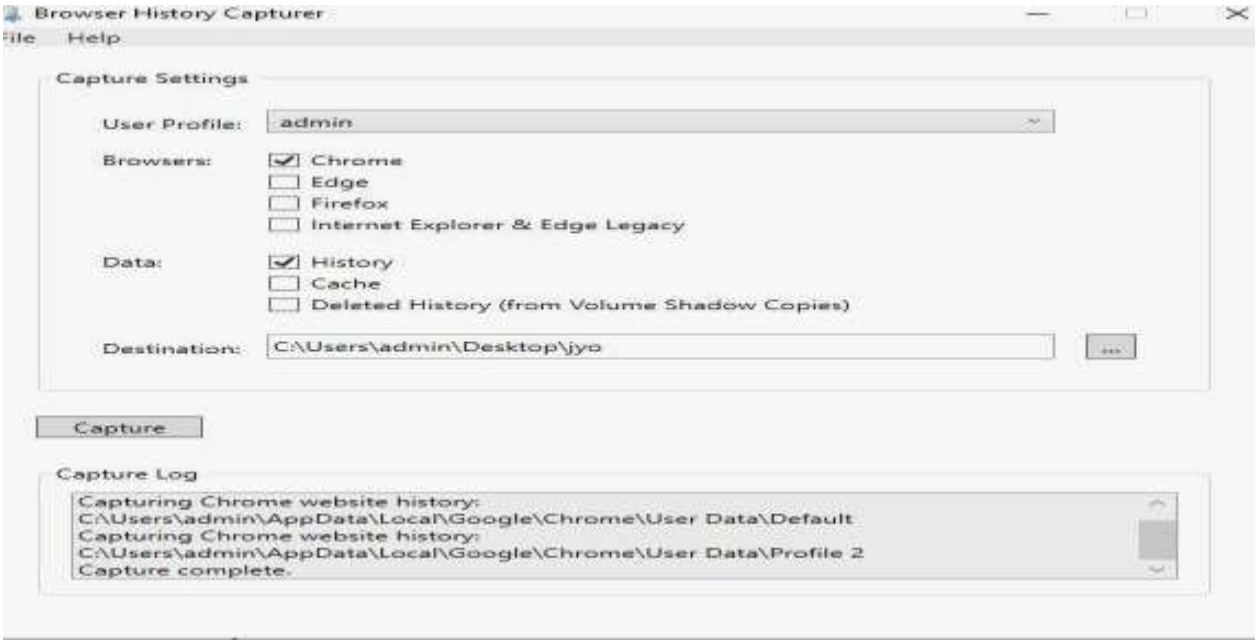


Fig 2:

3. Now your **xyz**

Folder on Desktop Contains All browser data.

4. Click on second **tool browser history view tool** now. You will get window like this. Select radio button (load history) as mentioned below and upload the folder path you have given in previous tool. You can see the down figure to fill the things. You can also set dates .Click on load button after you give details as in the screen and wait for some time.

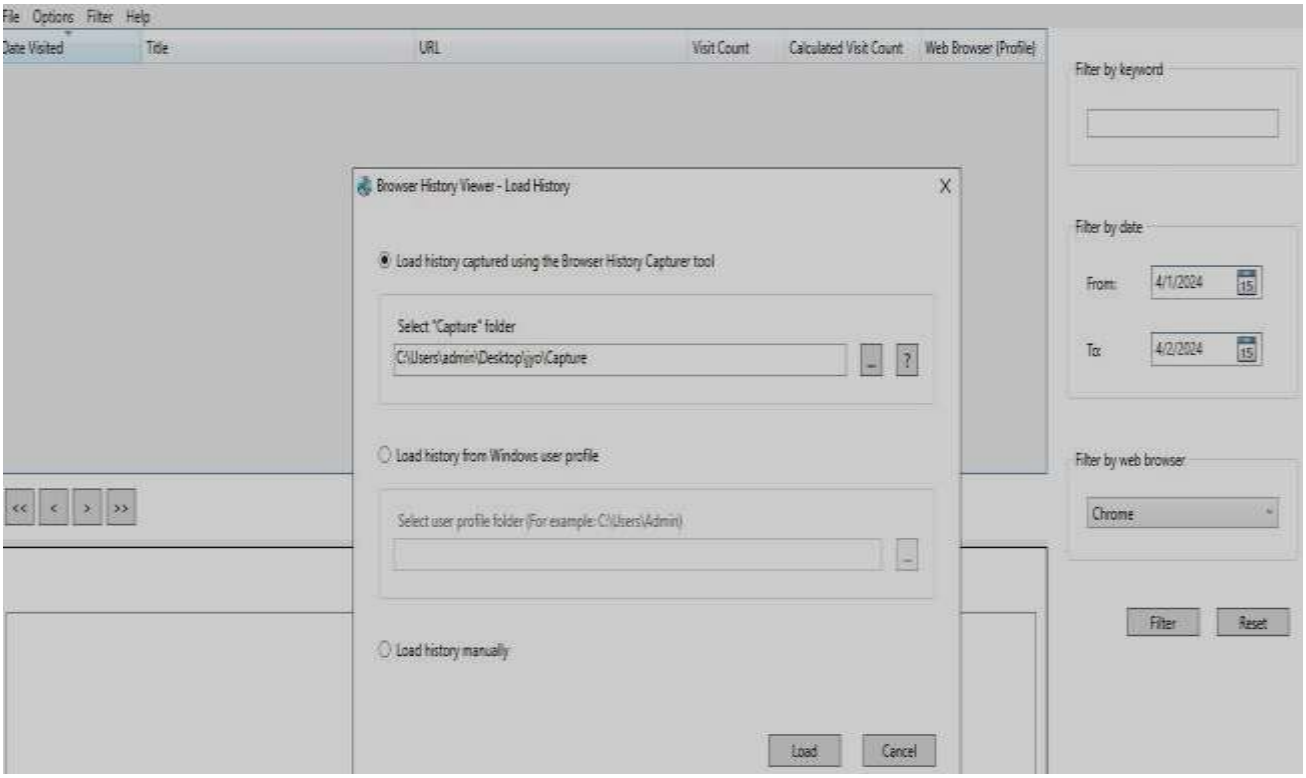


Fig3

5. In the browser history view, you will see a list of all the websites that the user has visited.
6. You can filter the list of websites by date, time, or keyword.
7. To view more information about a website, click on the website name.
8. You will see a list of all the information that the browser has stored about the website, including the website address, the date and time that the website was visited, the number of times the website was visited, and the amount of time that was spent on the website.
9. You can also view the downloaded content, history, saved logins, searches, and websites visited for a specific website.
10. To do this, click on the "Downloaded Content" tab, the "History" tab, the "Saved Logins" tab, the "Searches" tab, or the "Websites Visited" tab.
11. You will see a list of all the information that the browser has stored for the selected website as follows.

Fig4

Here are some additional tips for performing browser history analysis:

- Use the filter options to narrow down the list of websites.
- View the information about each website to see if there is anything suspicious.
- If you find anything suspicious, take a screenshot of the information and save it for future reference.
- If you are unsure about what something means, consult with a security expert.