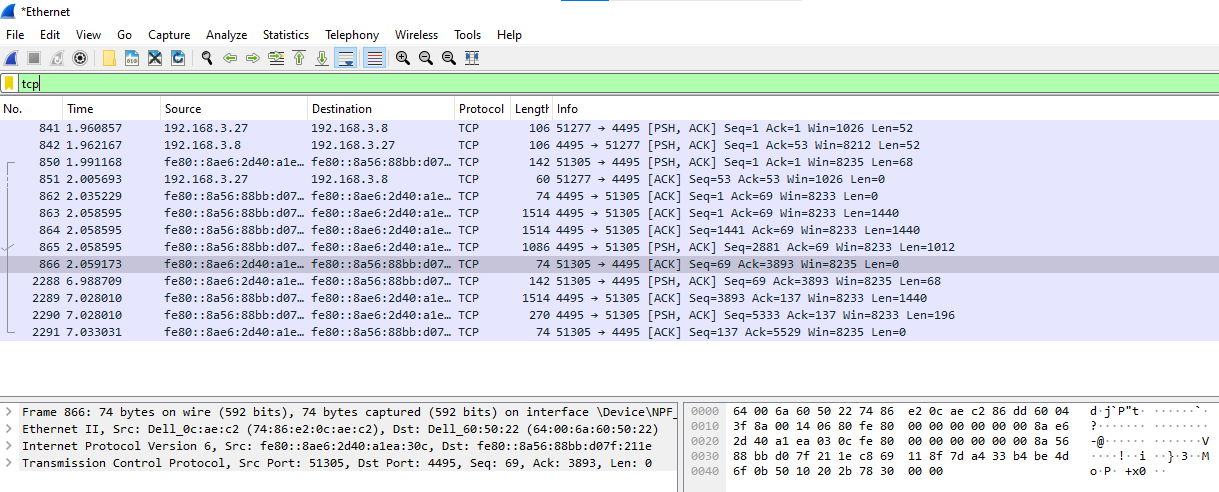
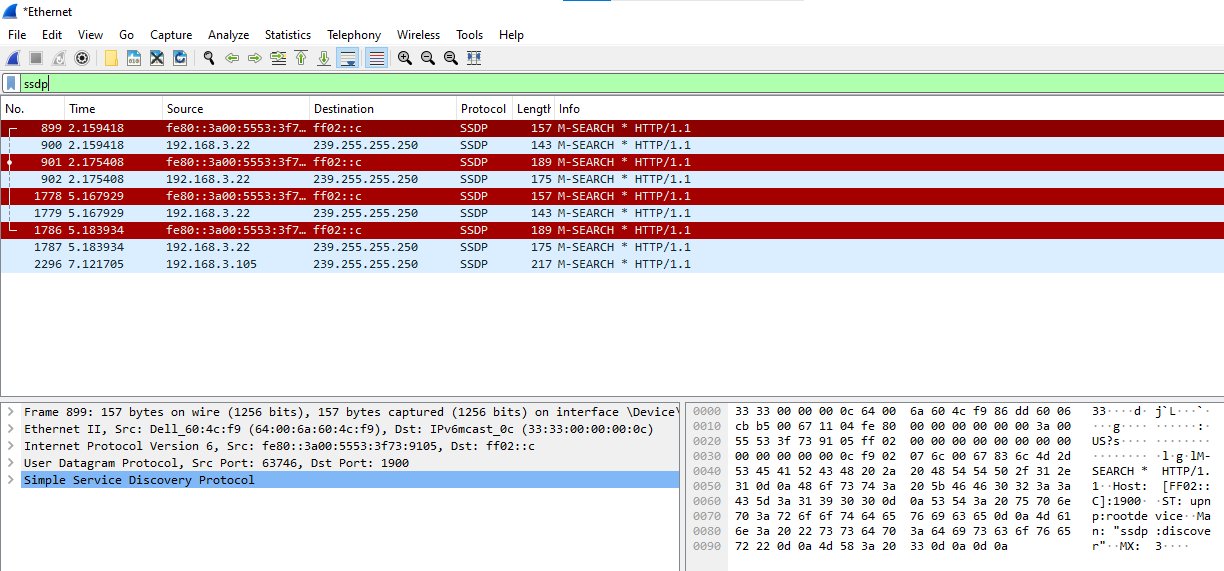
**Aim: Capturing and analysing network packets using Wireshark.**

**1)Identifying the live networks.**

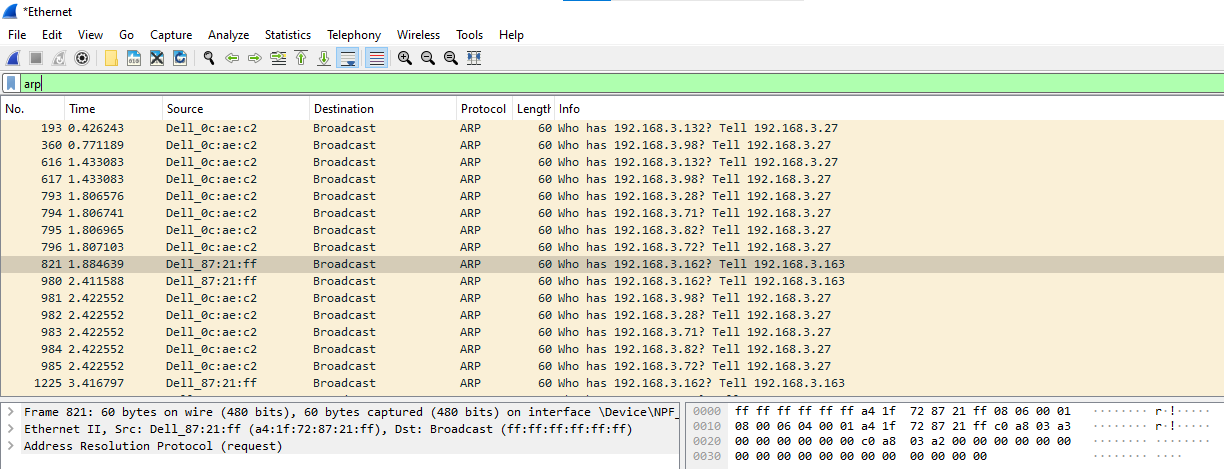
TCP



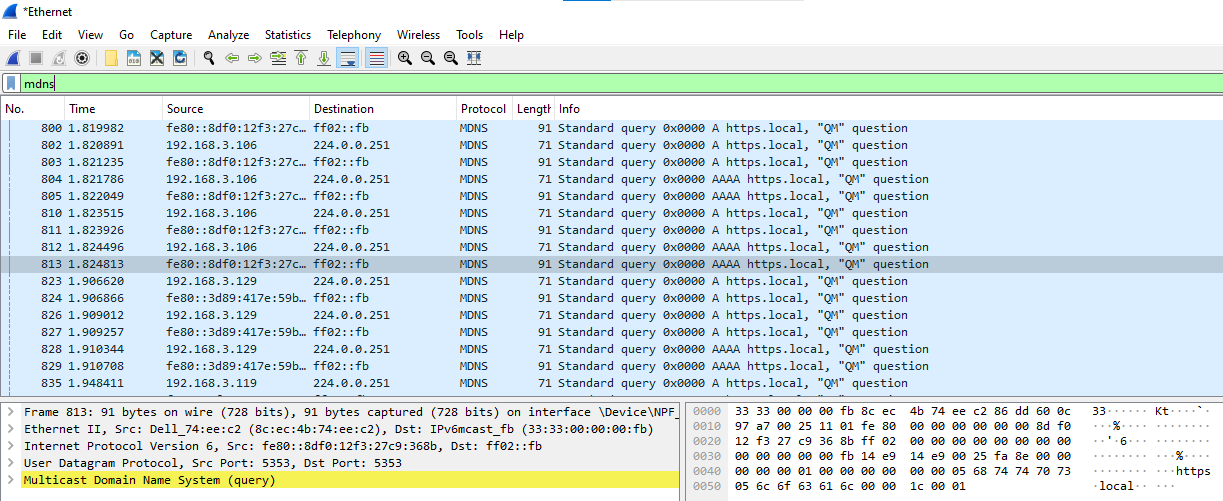
SSDP



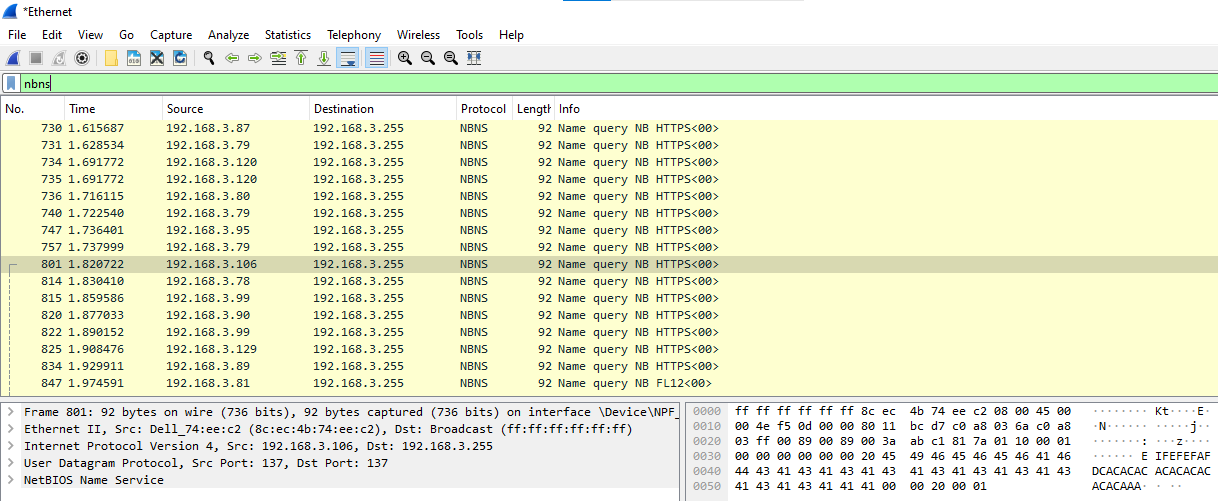
ARP



MDNS



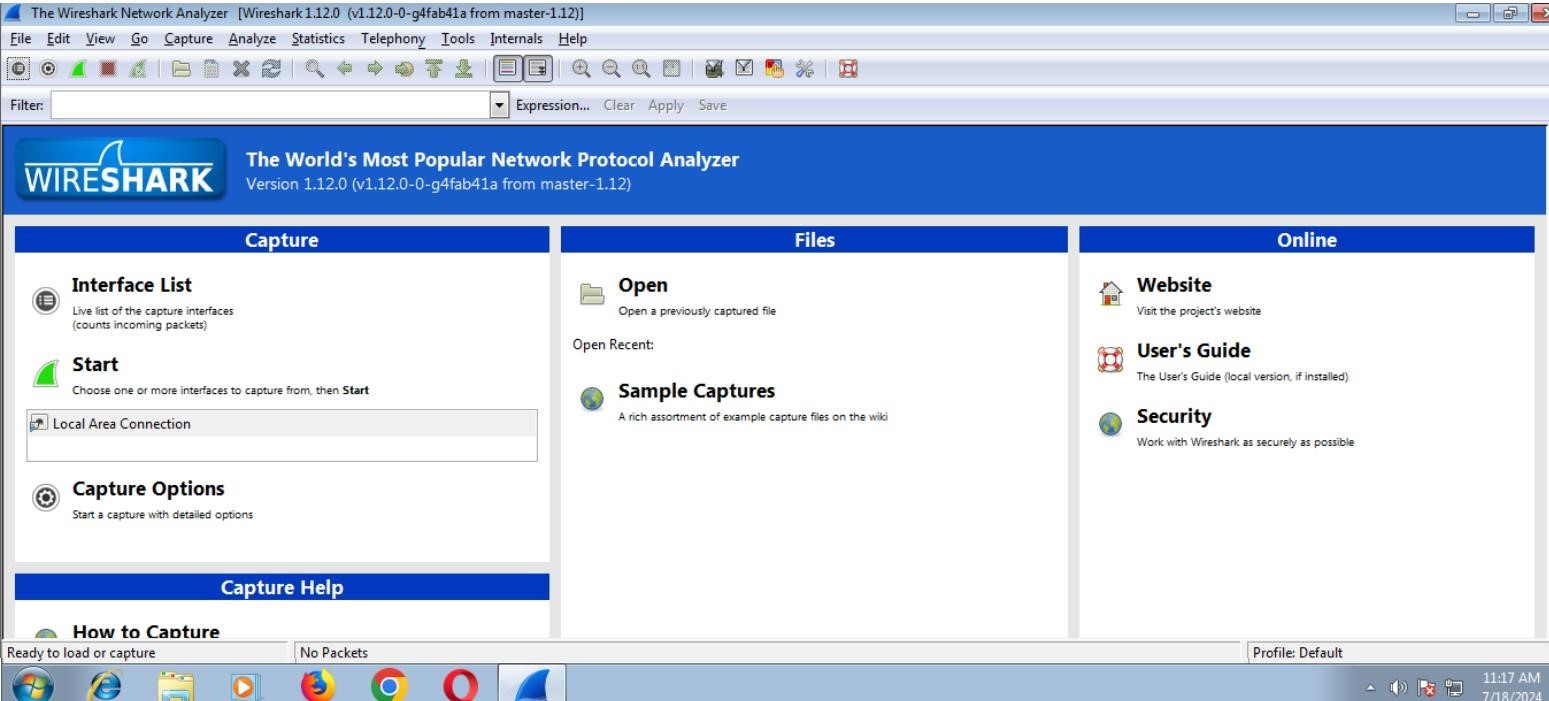
NBNS



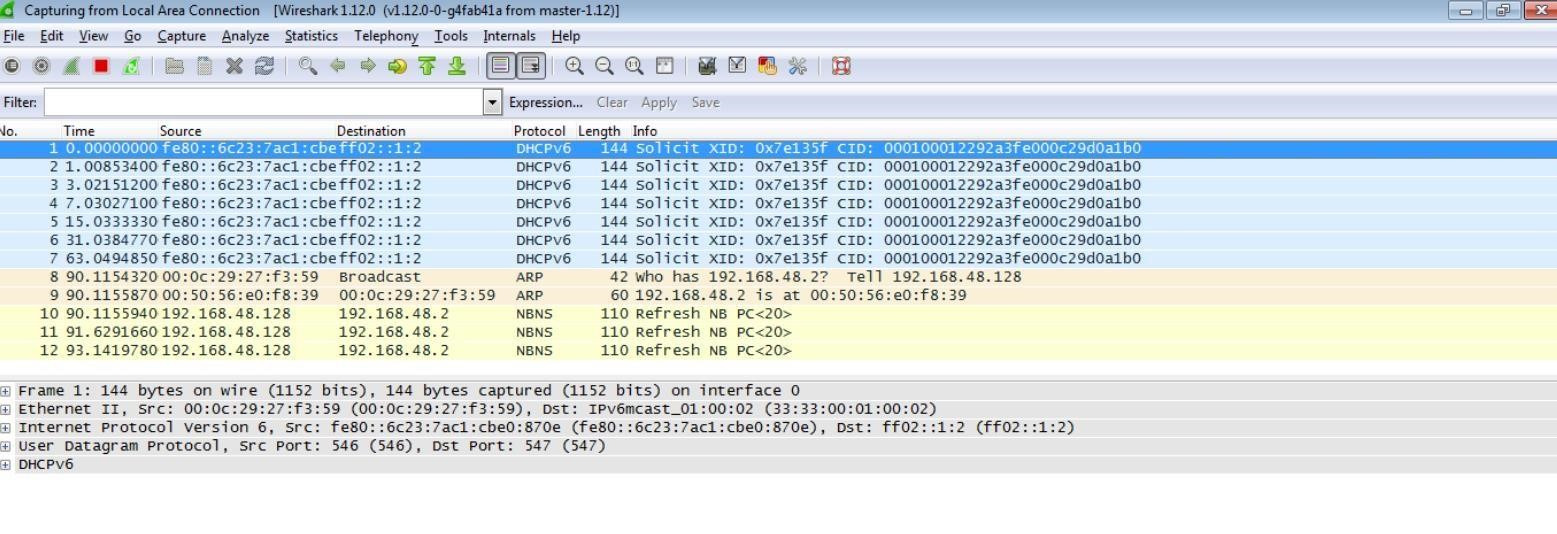
**2)Capture packets.**

**3)Analyse the captured packets.**

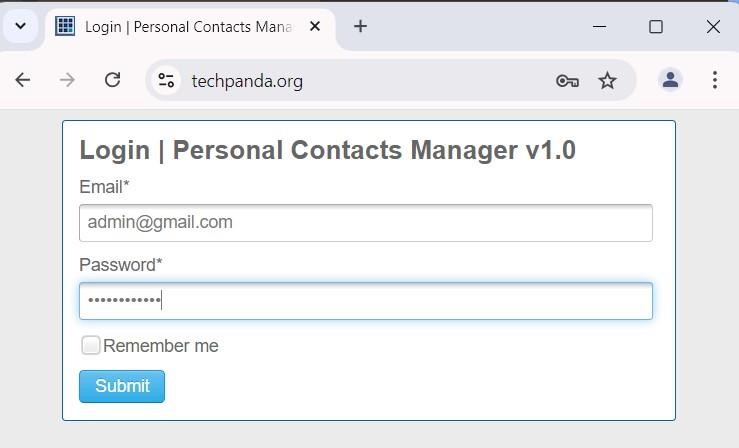
Step 1: Open Wireshark tool and click on the start button.



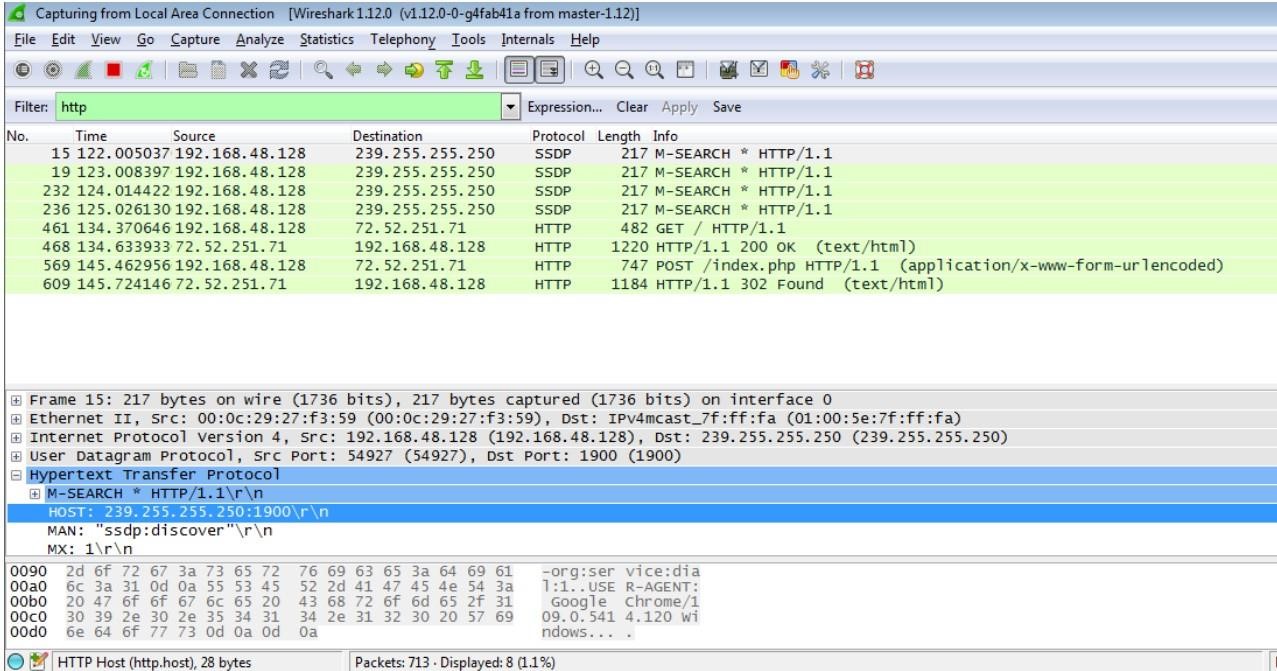
Step 2: It will show the list of packets going through the network.



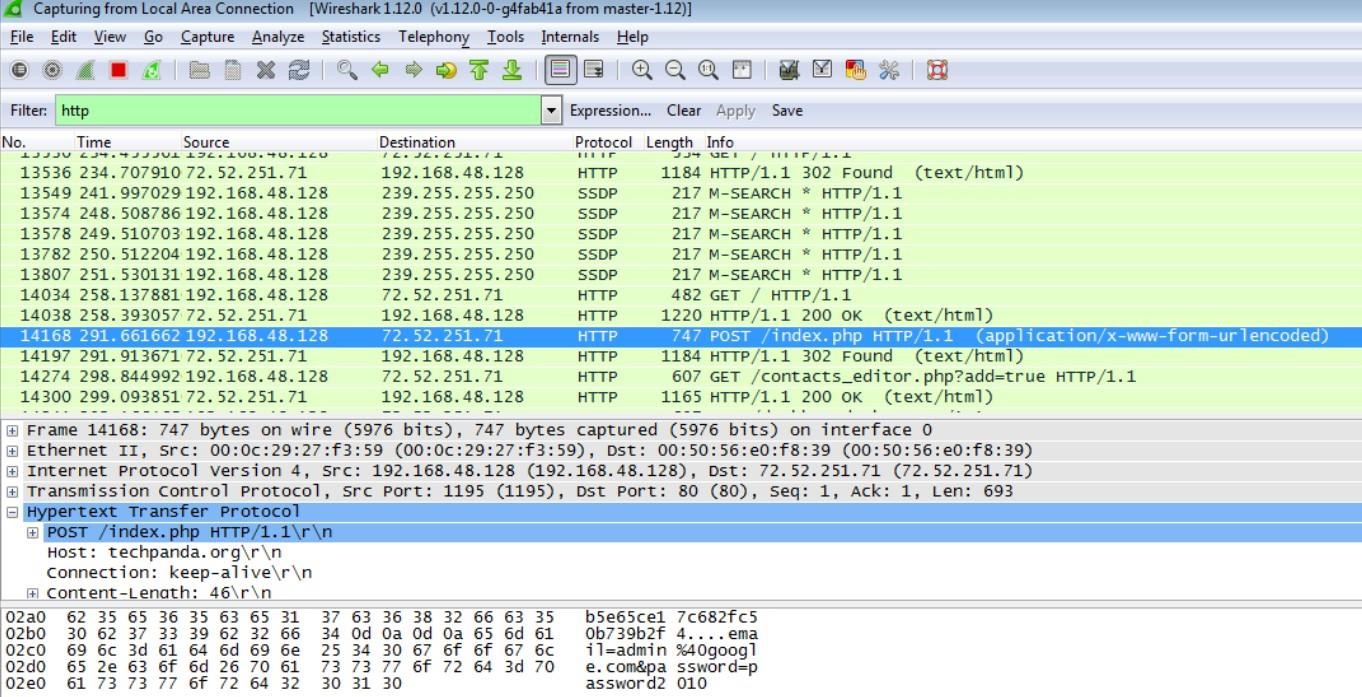
Step 3: Open Google > search techpanda.org and get logged in to the website.



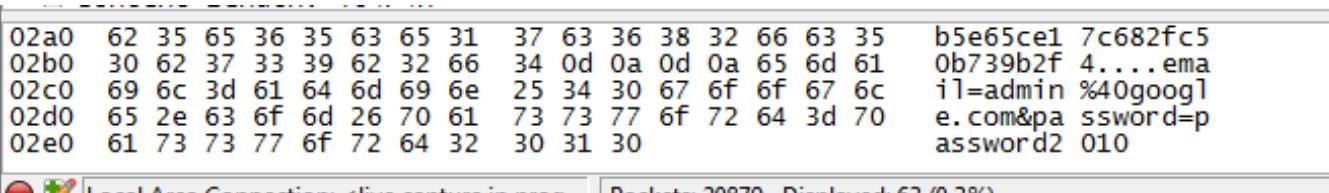
Step 4: Now go back to the Wireshark application and in filter option search http.



Step 5: Now click on index.php and then click on Hypertext Transfer Protocol



Step 6: As now you can see that the username and the password, we used for logged in is now showing below.



**Aim: Creating a Forensic Image using FTK Image/Encase Imager.**

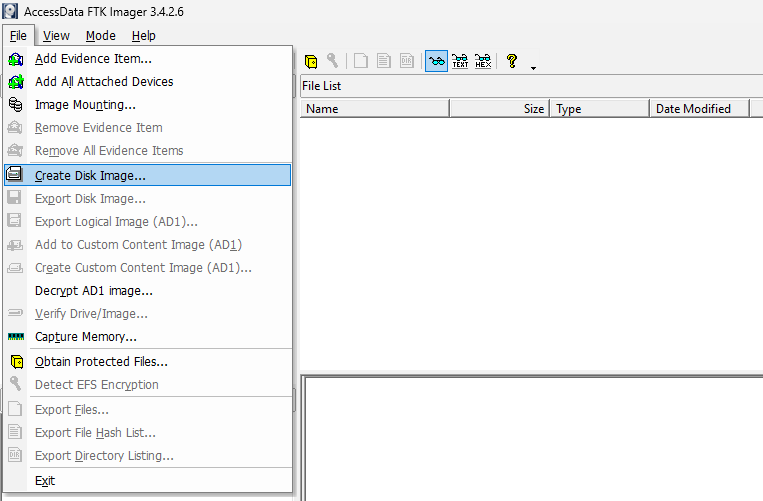
1)Creating Forensic Image

2)Check Integrity of Data

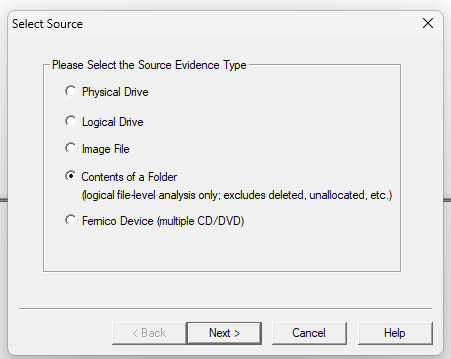
3)Analyze Forensic Image

**1)Creating Forensic Image**

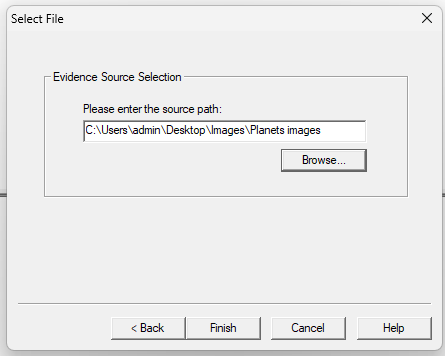
**Step 1: File create disk image**

****

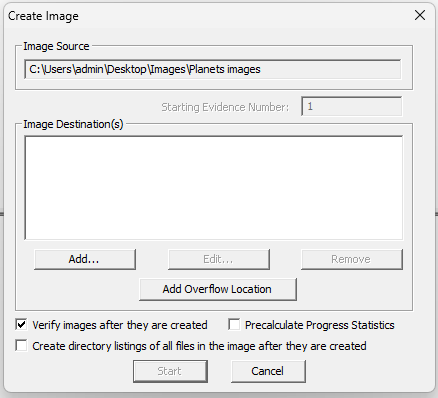
**Step 2:   Select source, contents of a folder**

****

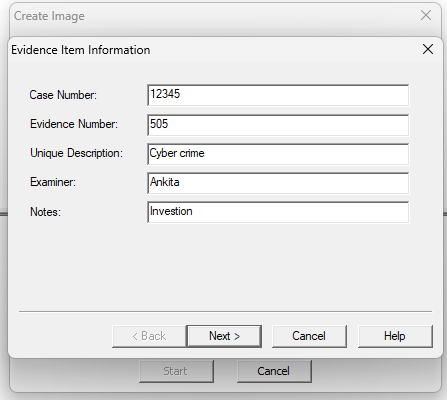
**Step 3:  select the folder directory that you want to create image file**

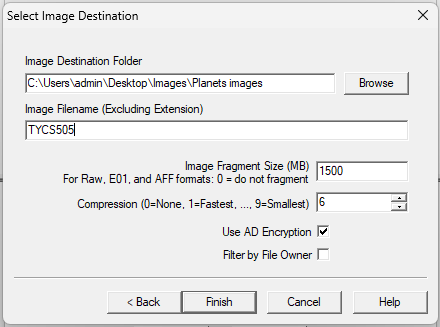
****

**Step 4:  Then finish verify image and click on Add**

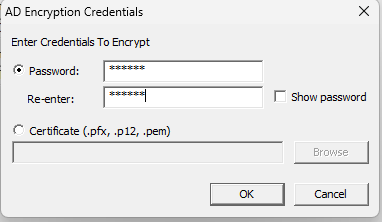
****

**Step 5: Add evidence information**

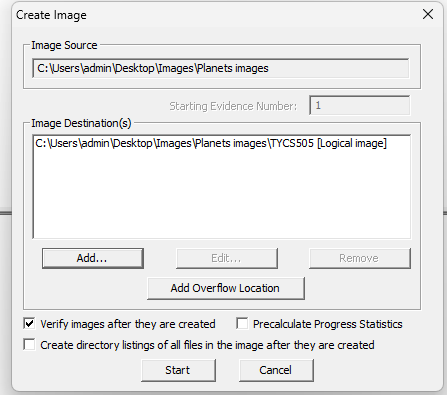
****

**Step 6: Create image destination AD encryption**

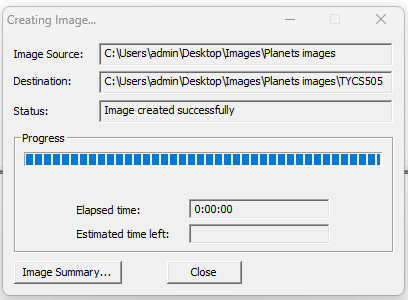
**Step 7: Put AD Encryption Credentials**

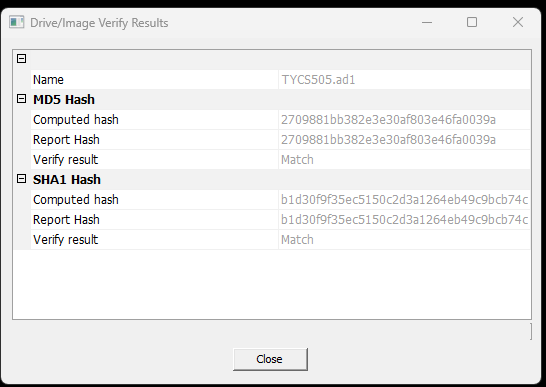
****

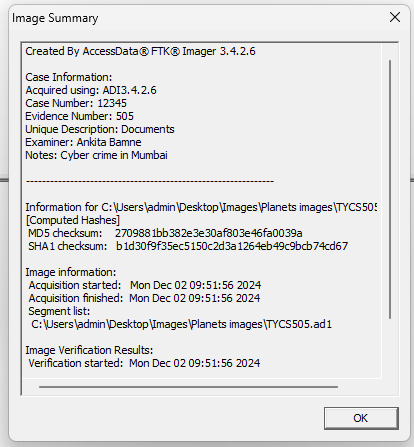
**Step 8: Create Image and click on Start**

****\

**Step 9: Image created.**

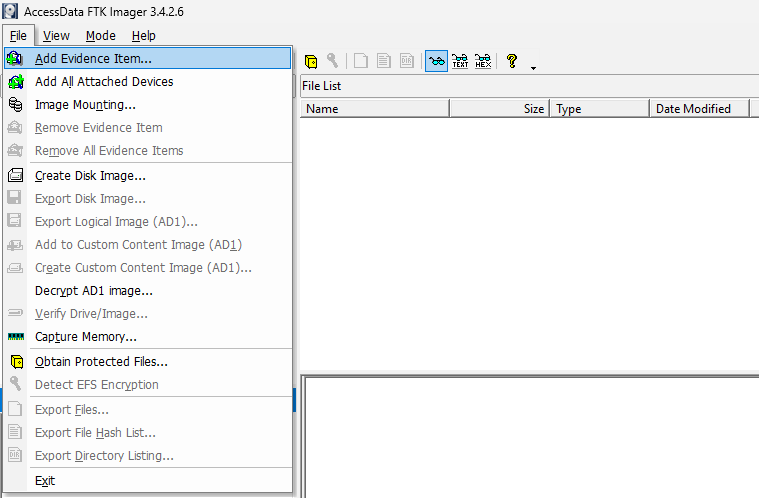
****



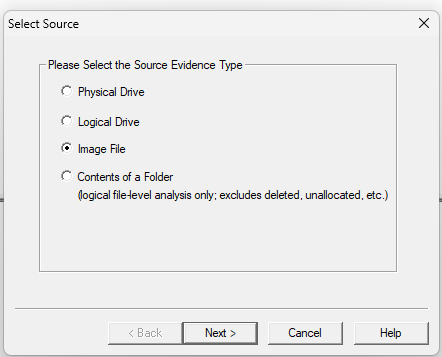


**2)Check Integrity of Data**

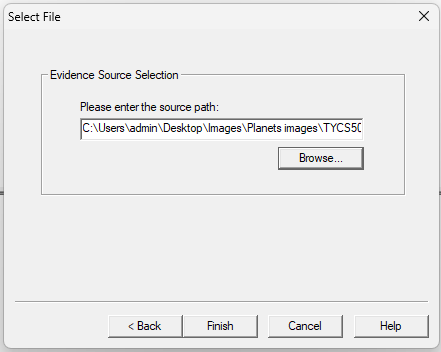
**Step 1: Select File and add evidence item**



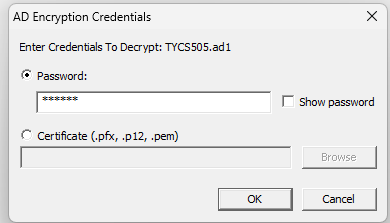
**Step 2: Select source, Image File**



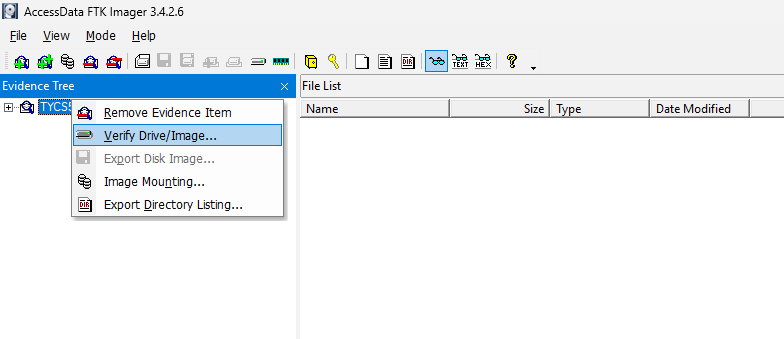
**Step 3: Browse and add ad1 file which you have already created.**



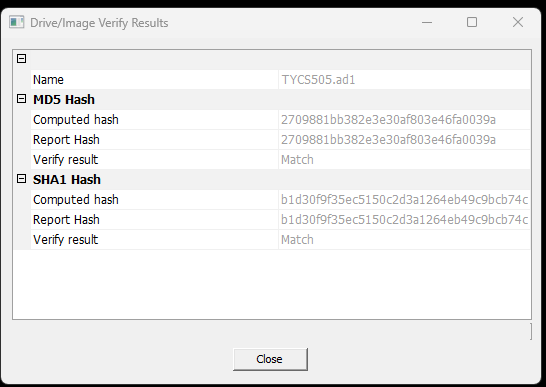
**Step 4: Enter password, in AD Encryption Credentials**



**Step 5: Select evidence Tree and verify drive/Image.**



**Step 6: View Results.**



**3)Analyze Forensic Image**

**Autopsy**



**Aim: Using Sysinternals tools for Network Tracking and Process Monitoring.**

1)Check Sysinternals tools

2)Monitor Live Processes

3)Capture RAM

4)Capture TCP/UDP packets

5)Monitor Hard Disk

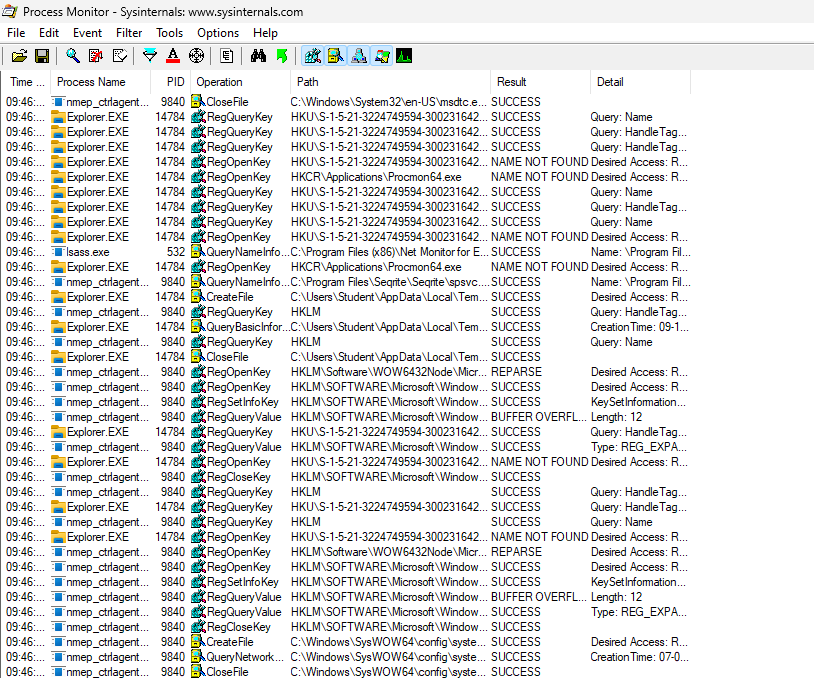
6)Monitor Virtual Memory

7)Monitor Cache Memory

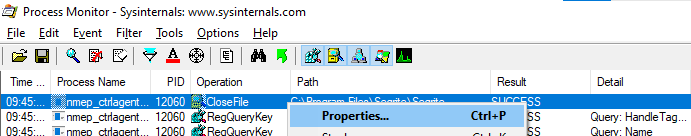
**2)Monitor Live Processes**

**STEP 1:** Go to SOFT THEN msc folder then sysinternals folder.

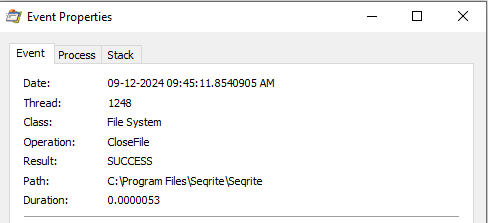
**ProcMon**

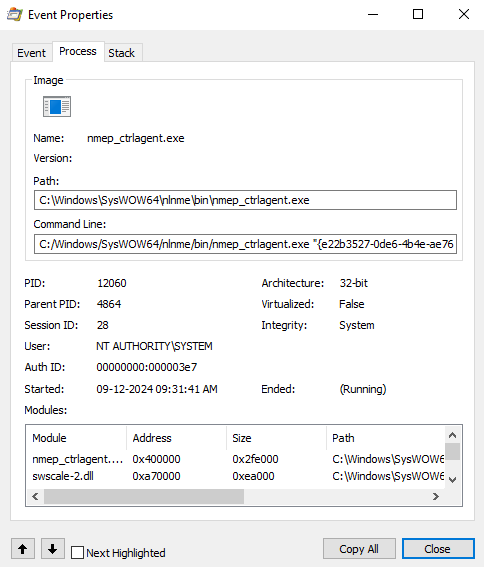


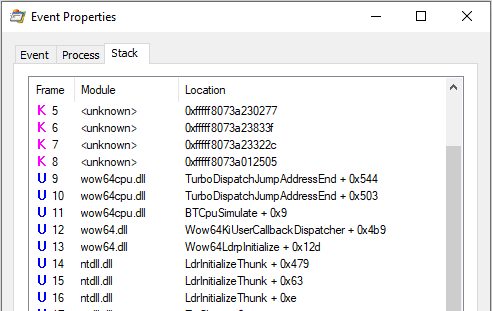
**Step 2:** right click on process that is success select properties



**Step 3:** Event properties details

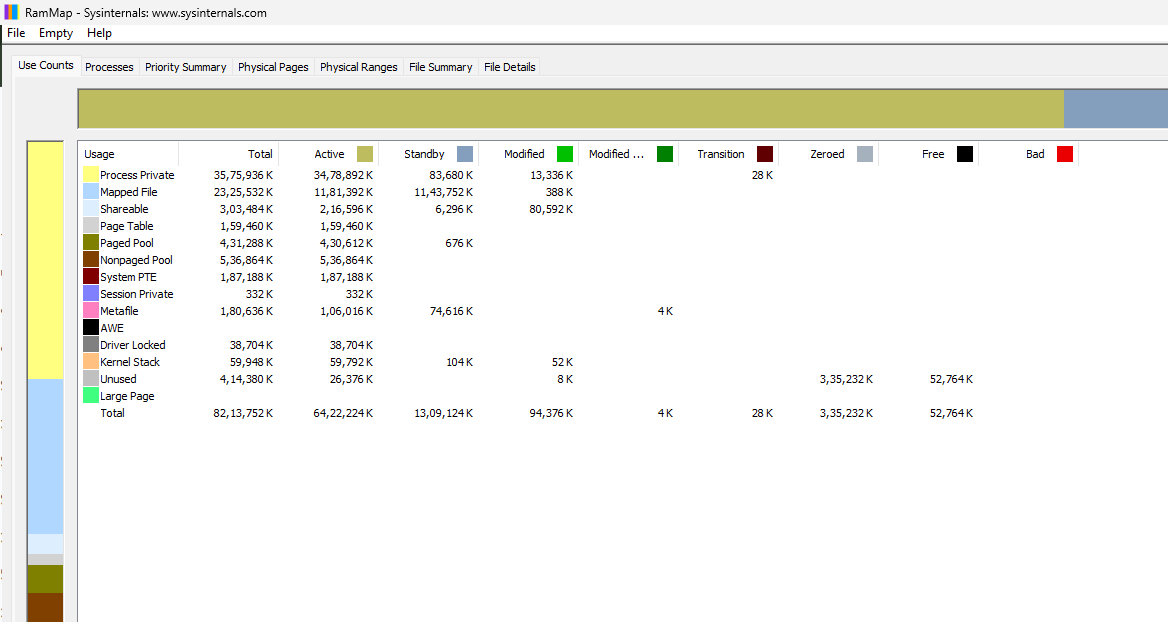




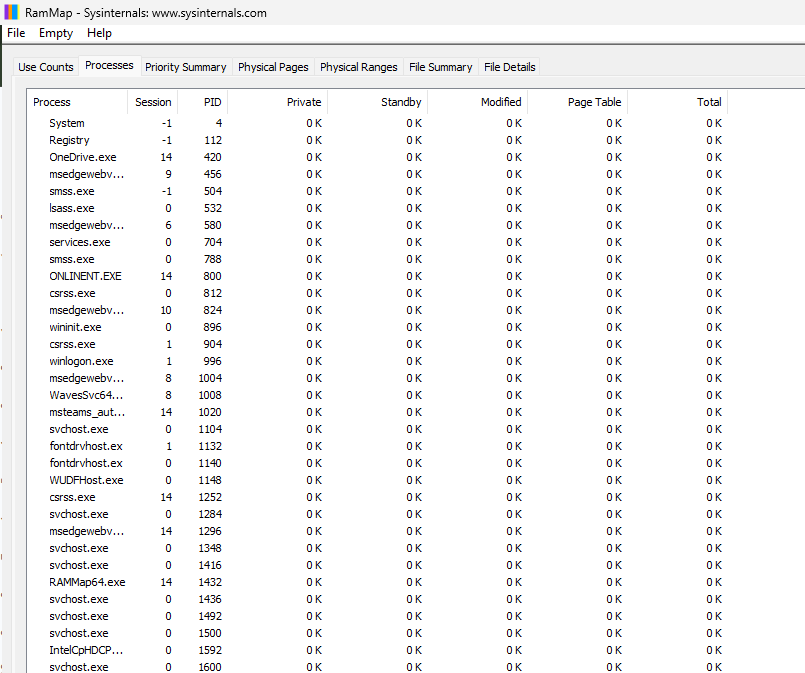


**3)Capture RAM**

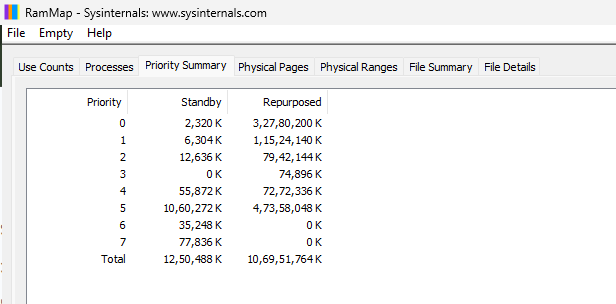
Soft -> Sysinternal -> install RamMap application



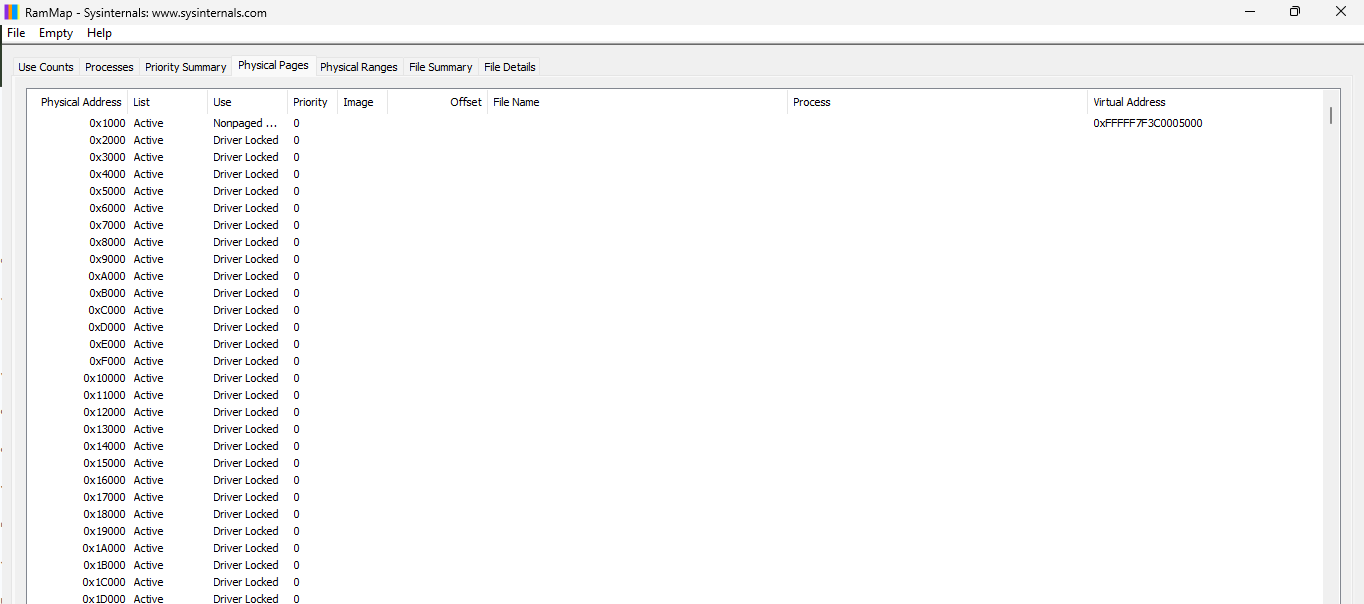
**RamMap Process**



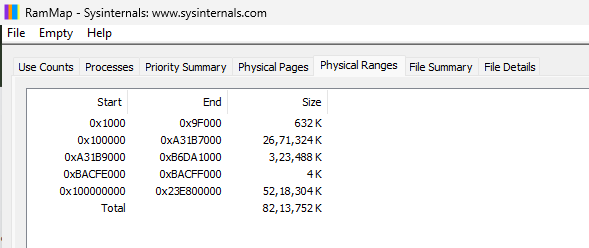
**RamMap Priority**



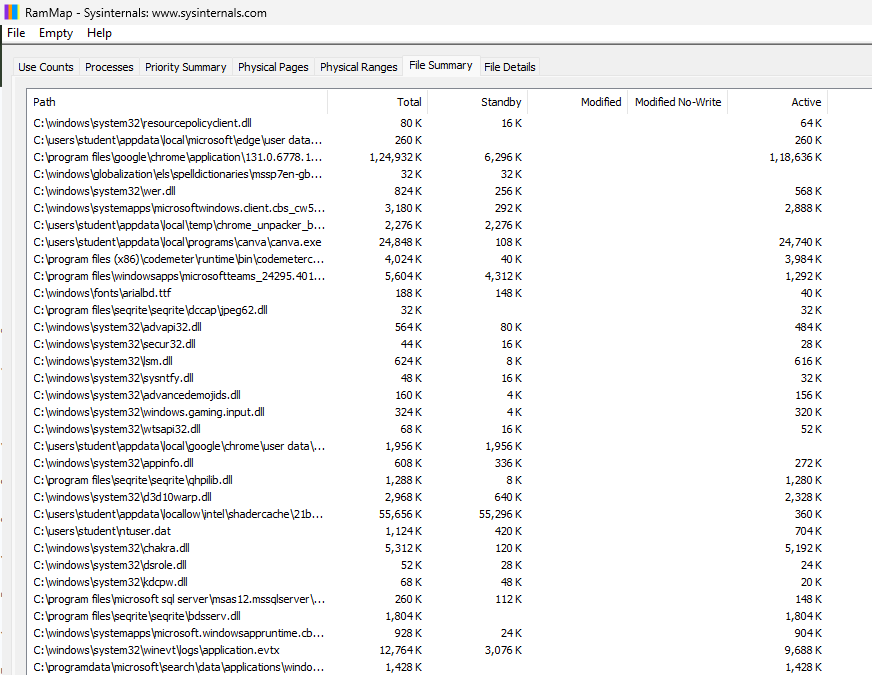
**Physical Pages**

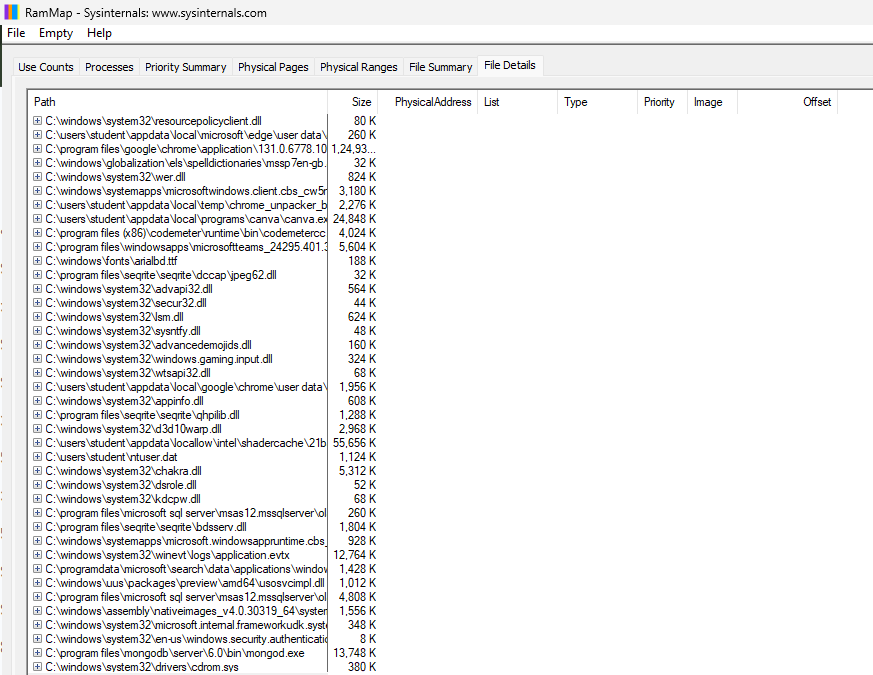


**Physical Ranges**



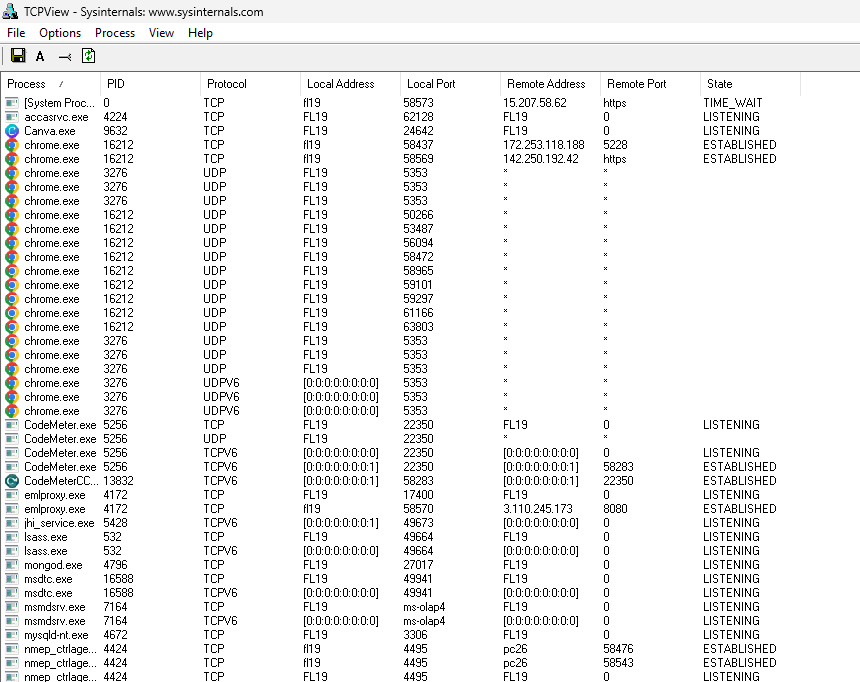
**File summary**



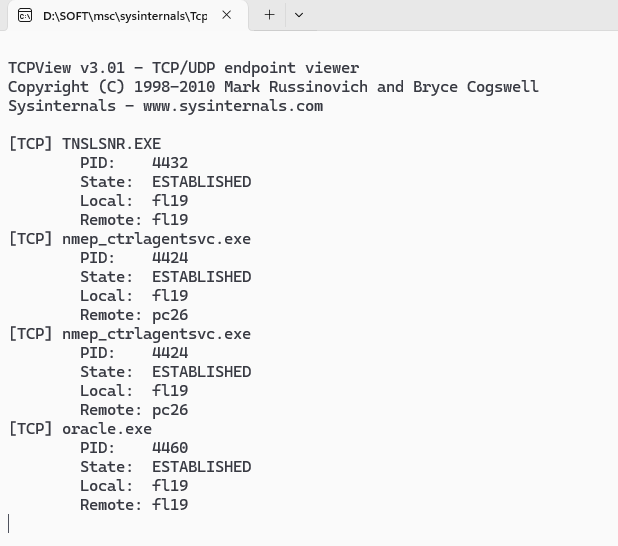
**File Details**

4)Capture TCP/UDP packets

Soft -> Sysinternal -> install tcpview application



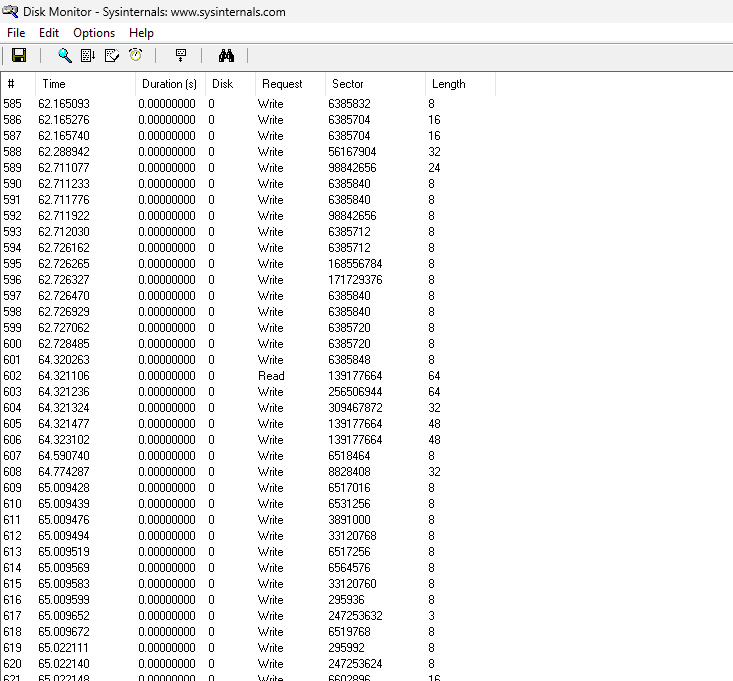
**TcpView**



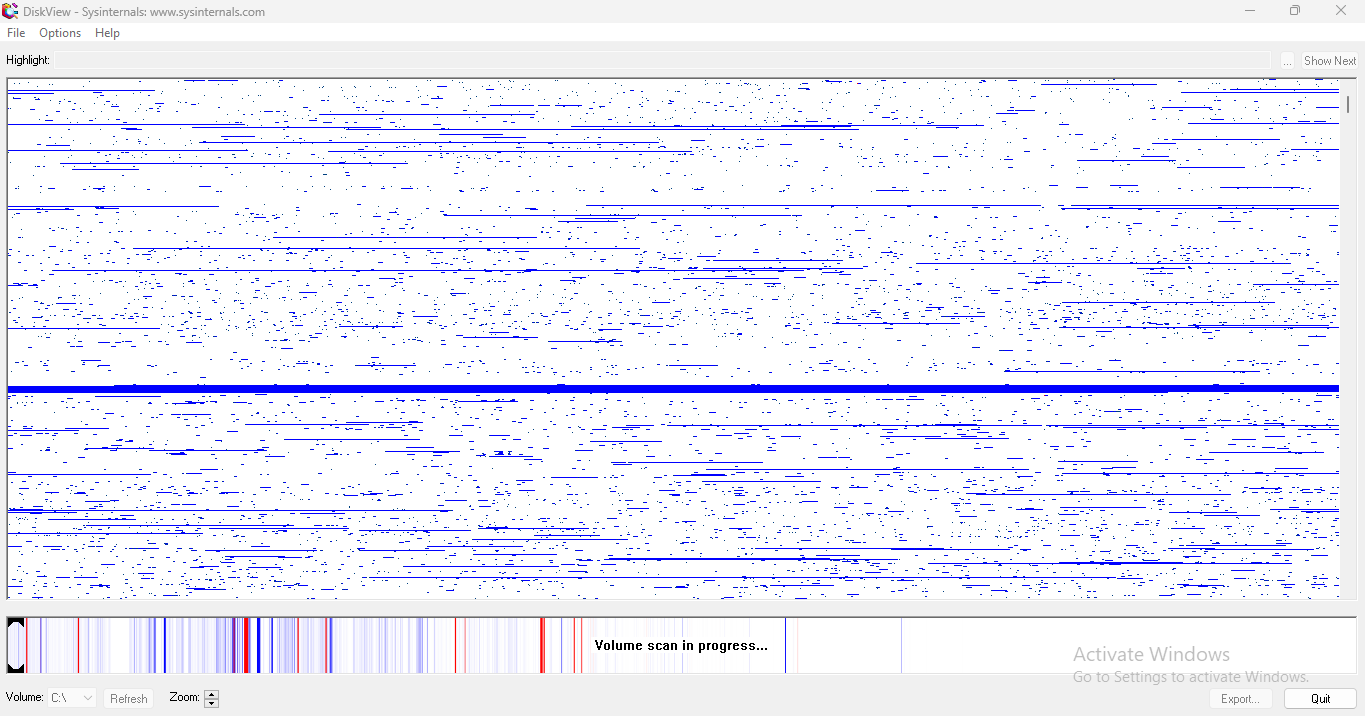
5)Monitor Hard disk

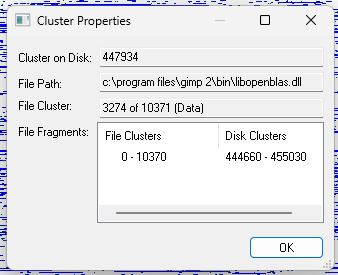
Soft -> Sysinternal -> install diskmon application

**DiskMon**



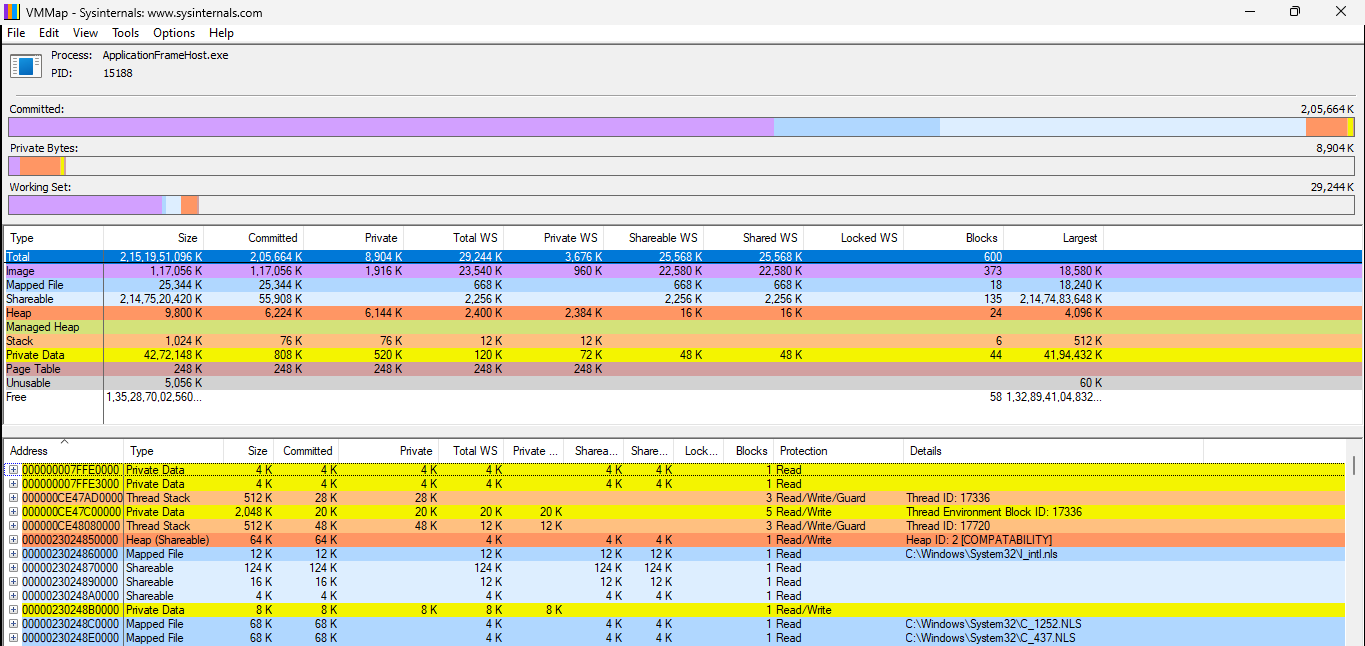
Soft -> Sysinternal -> install **DiskView** application.





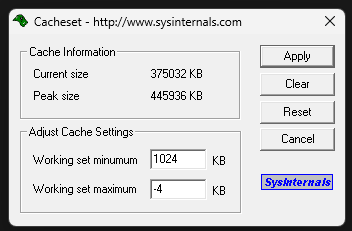
**6.Monitor virtual memory**

Soft -> Sysinternal -> install vmmap application



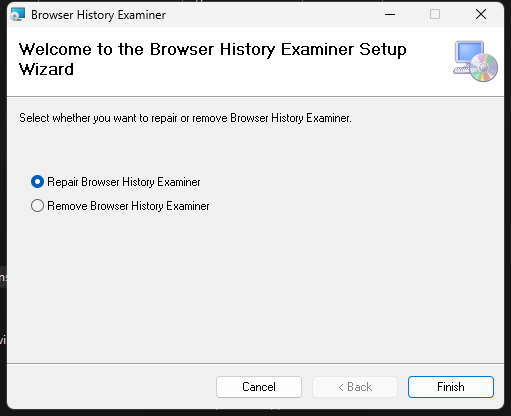
**7.Monitor Cache memory**

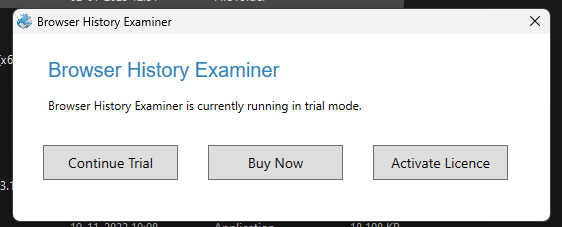
Soft -> Sysinternal -> install cacheset application

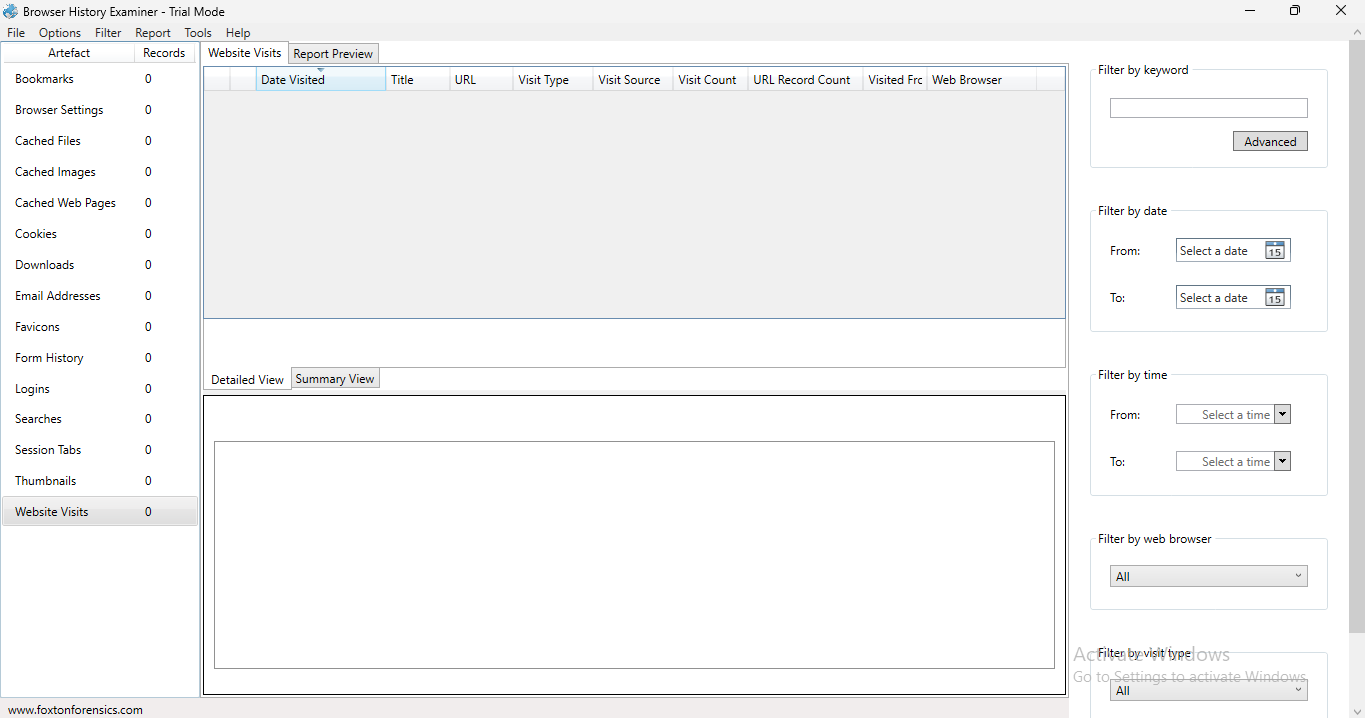


**Aim: Browser History Examiner**

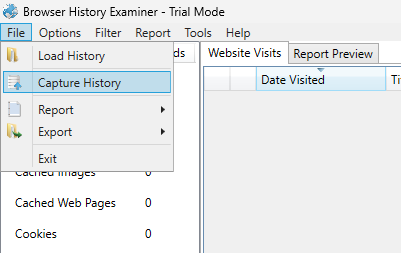
**Step 1: Select repair Browser History Examiner.**



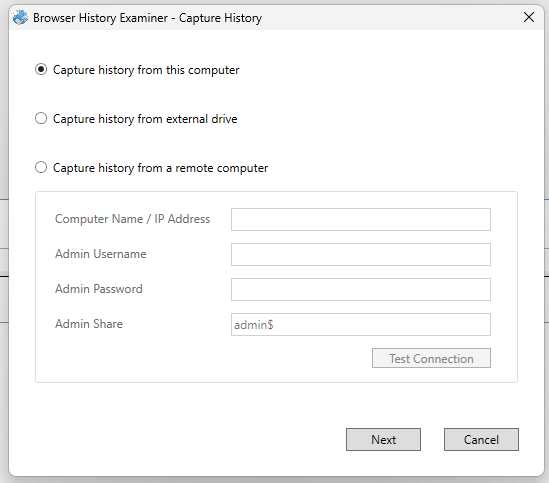




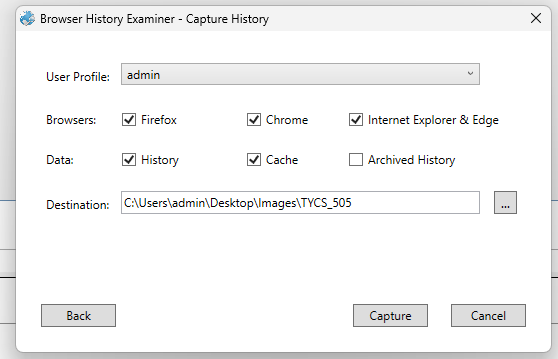
**Step 2: Click file, select capture history.**



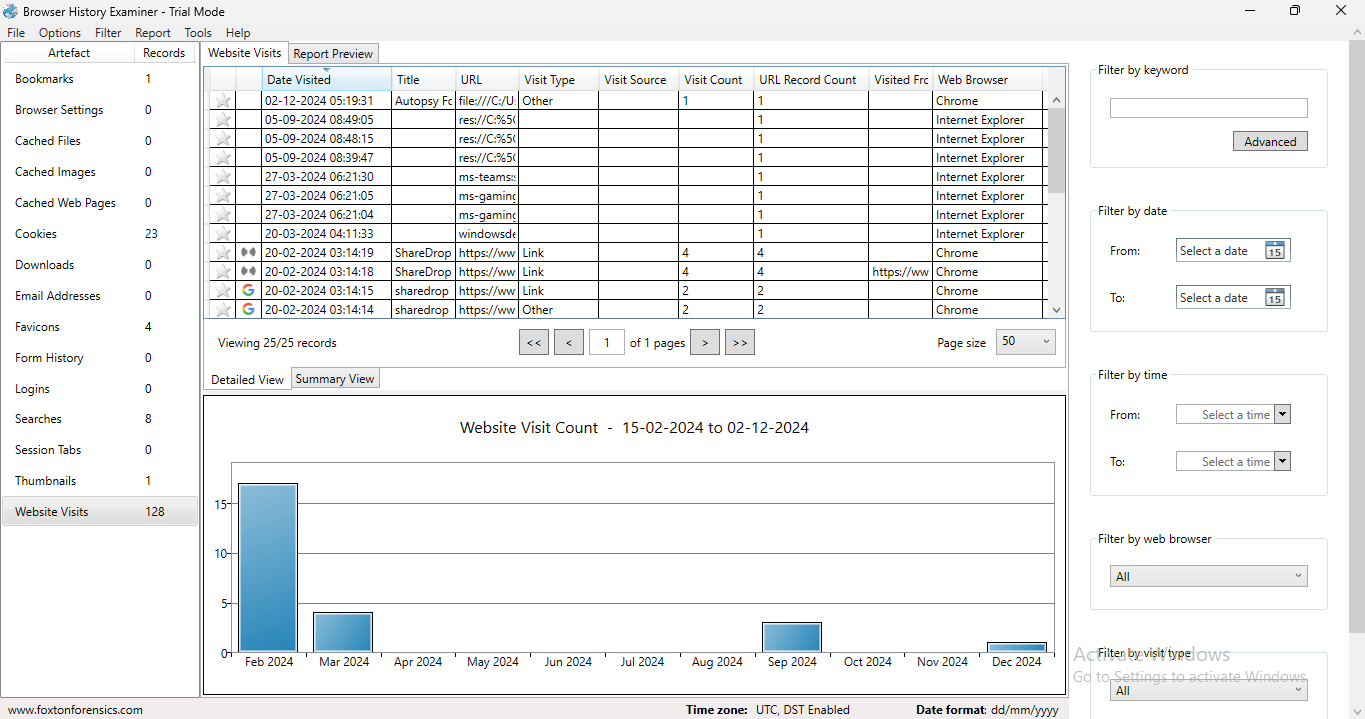
**Step 3: Select capture history from this computer.**

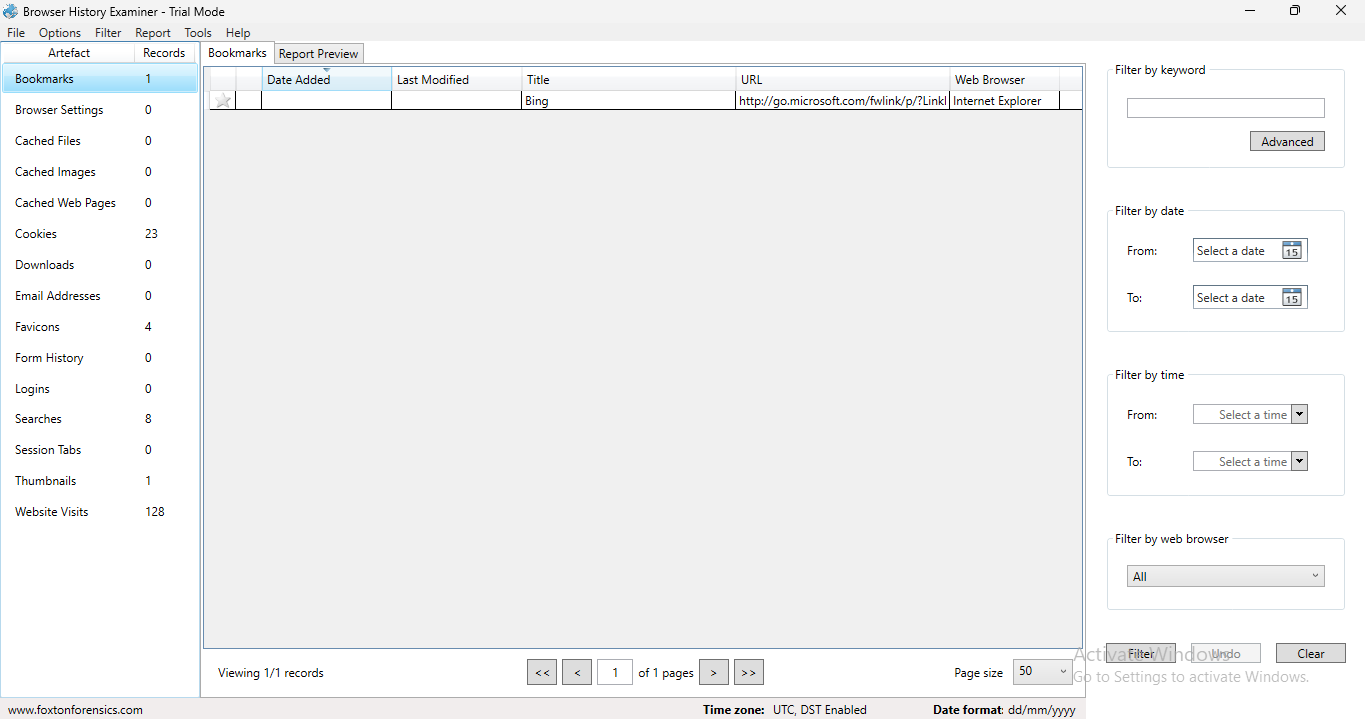


**Step 4: Select browsers, data and give destination path, click capture.**

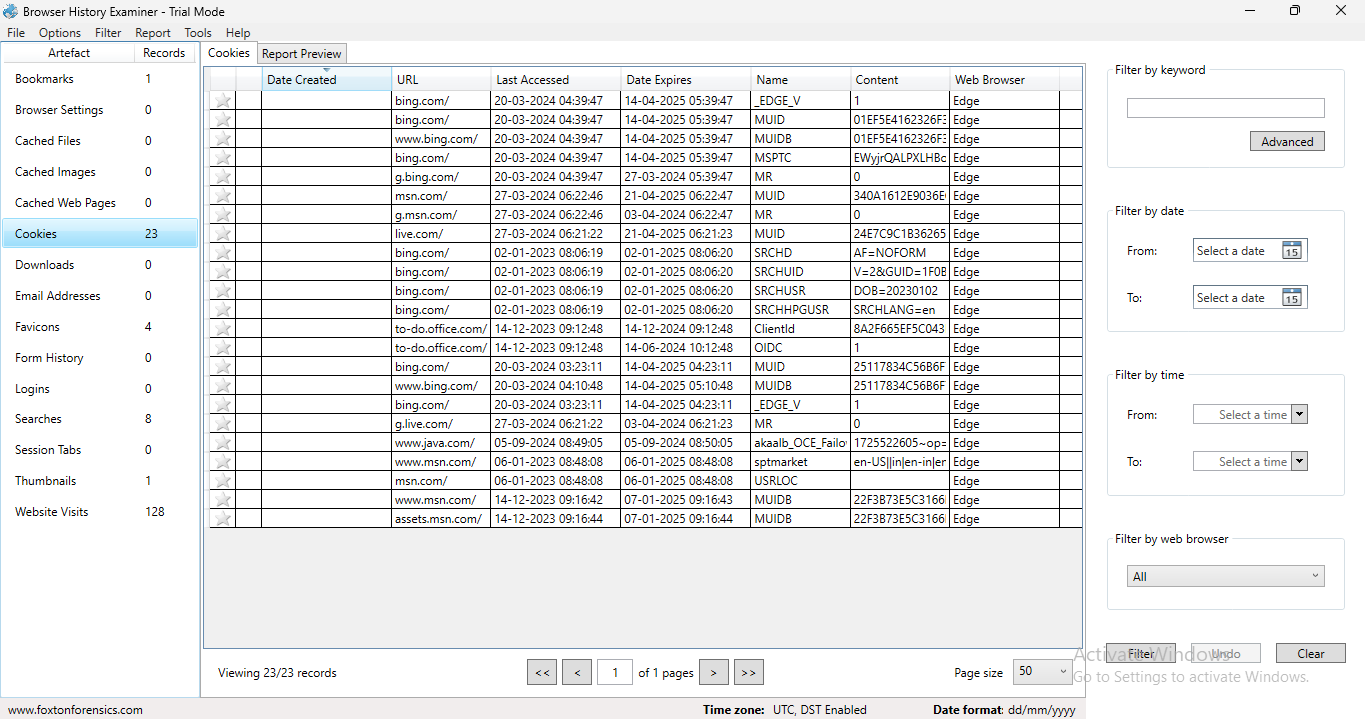


**Step 5: Displays all captured details.**

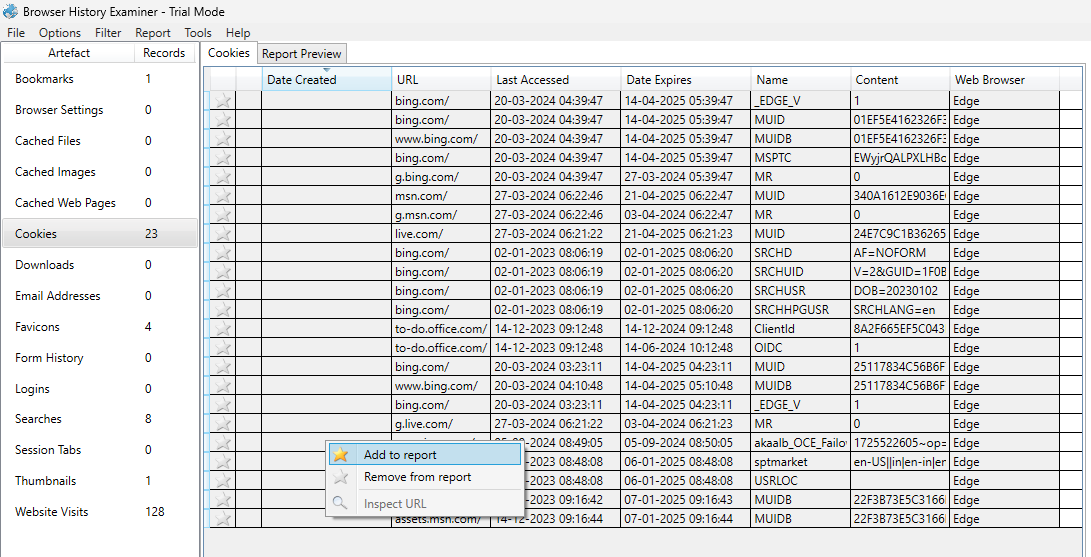




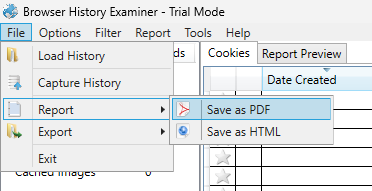
**Step 6: You can view bookmarks, Cookies.**



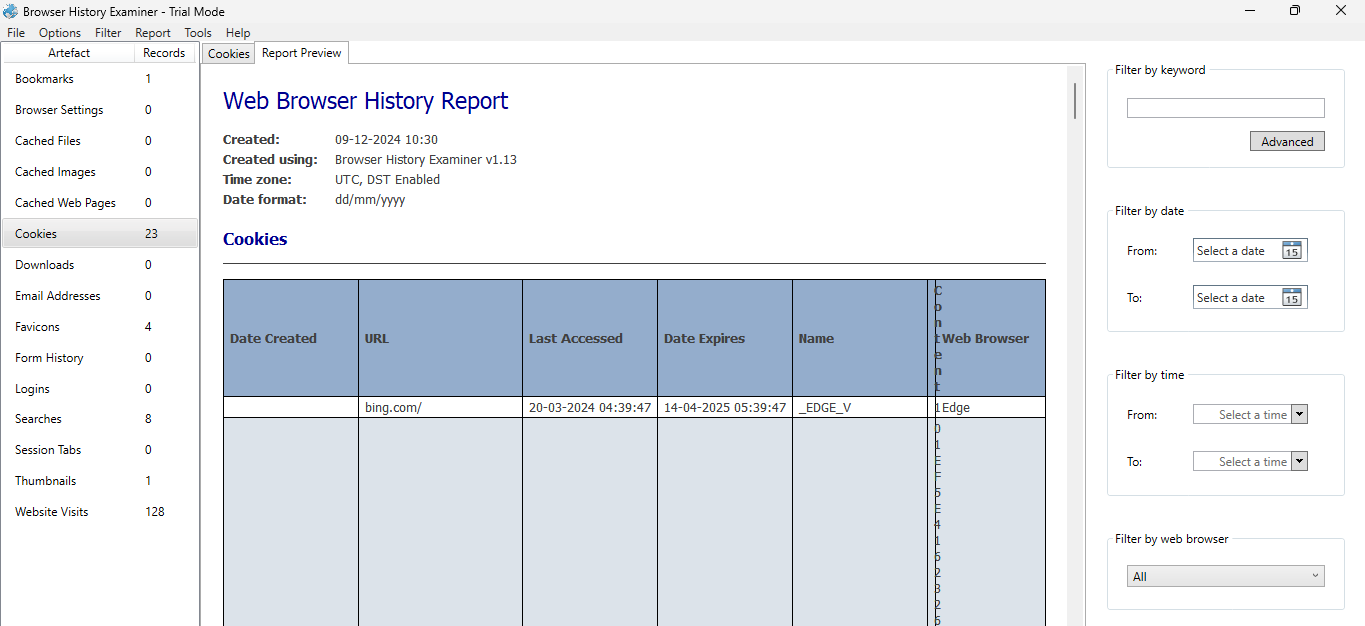
**Step 7: Right click on the records and click on add to report.**



**Step 8: Then go to file click report and save.**



**Step 9: You can preview the report as you saved.**



**Aim: Web Browser Forensics**

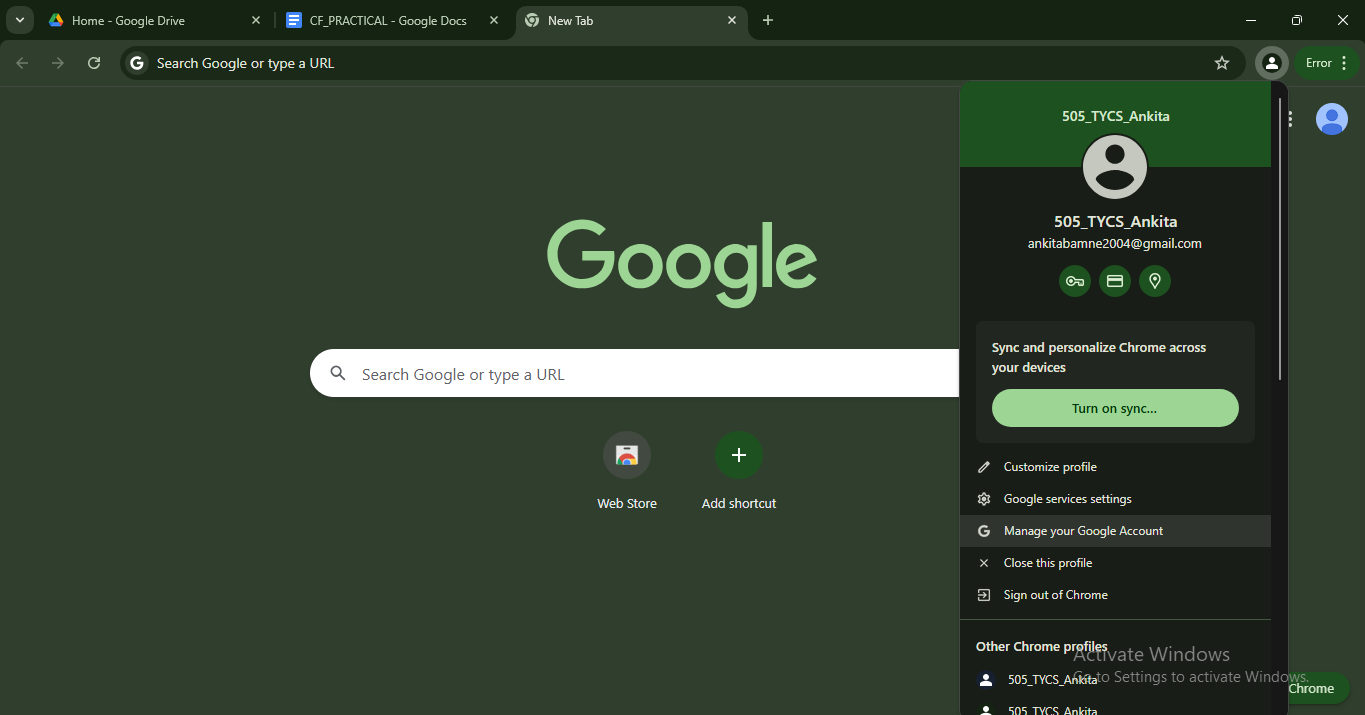
1)Web browser working

2)Forensics activities on browser

3)Cache/Cookies analysis

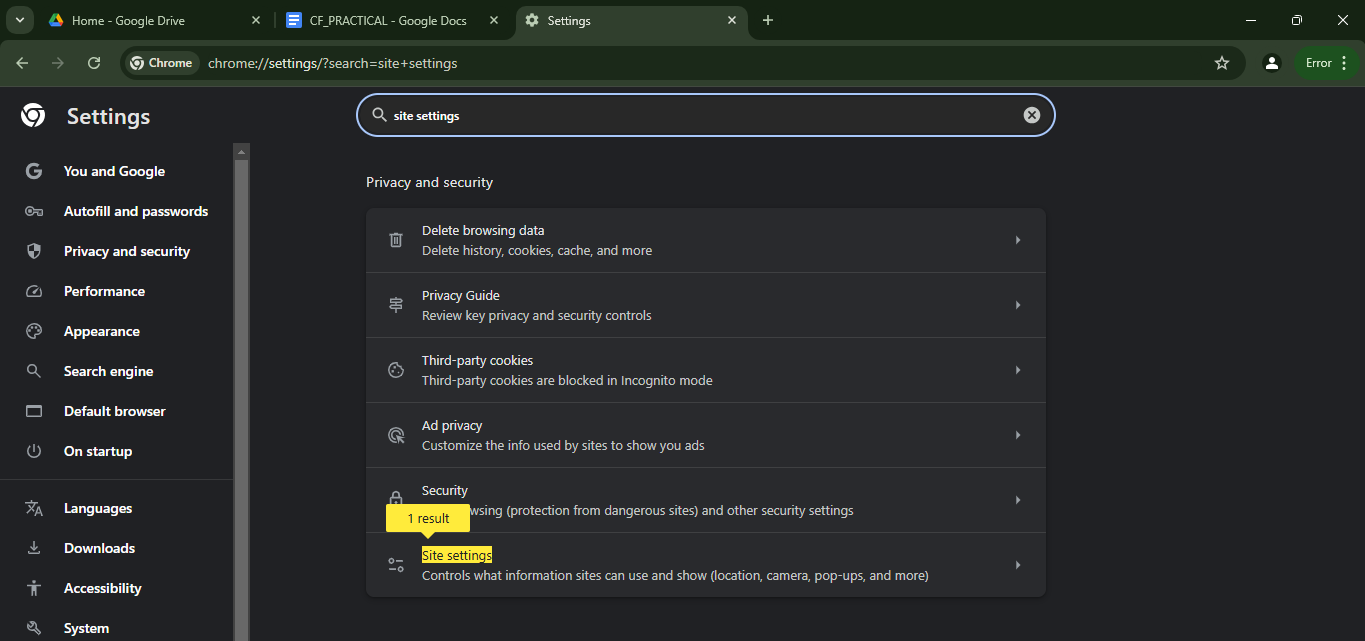
4)Last internet activity

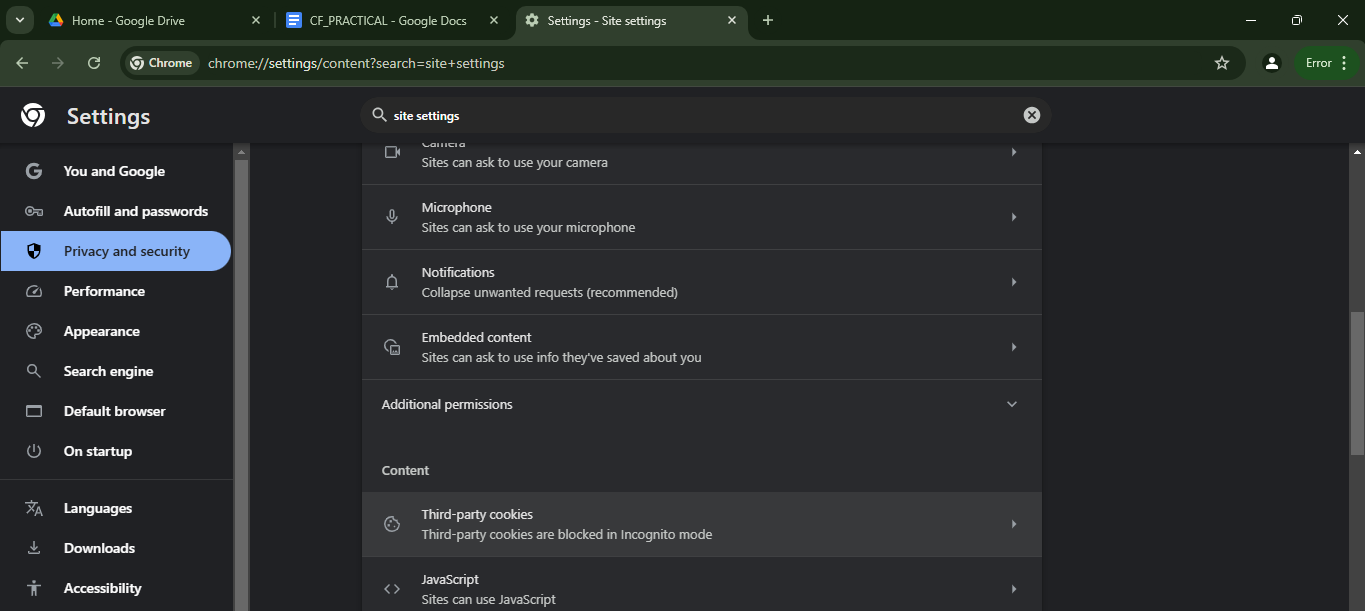
**1)Web browser working**

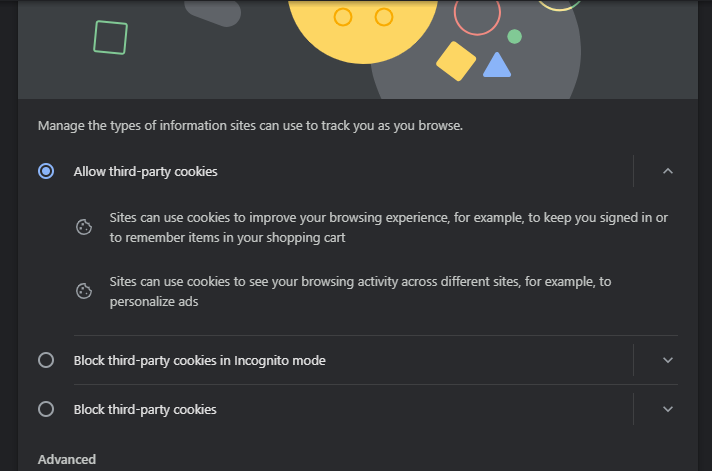


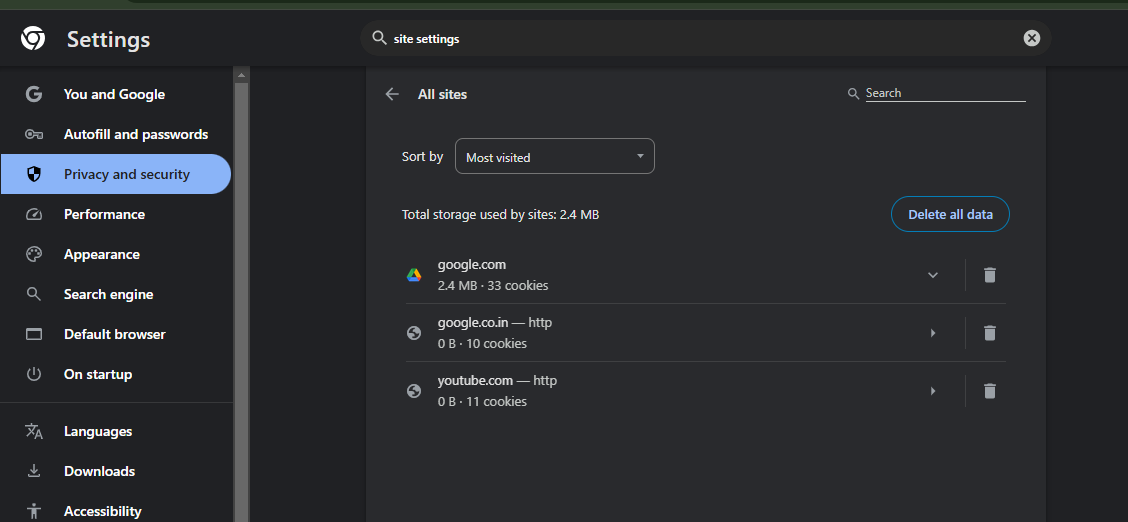
**Forensics activities browser**

**Go to browser setting -> search site setting -> open**



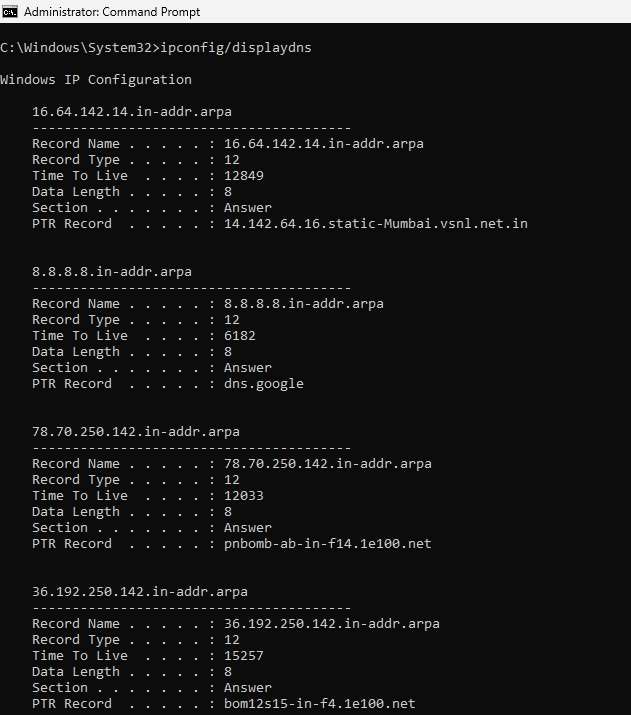






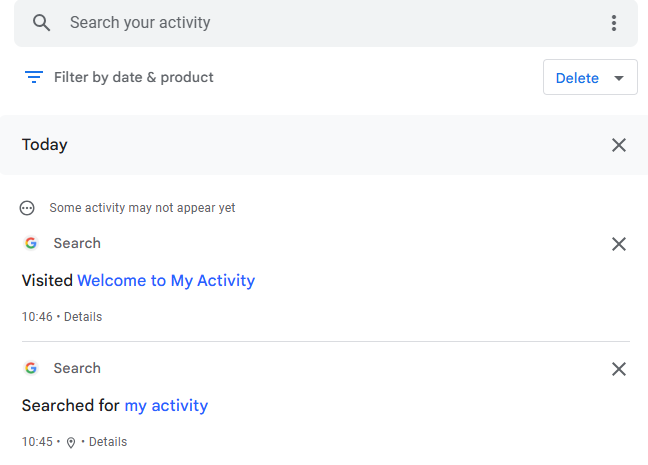
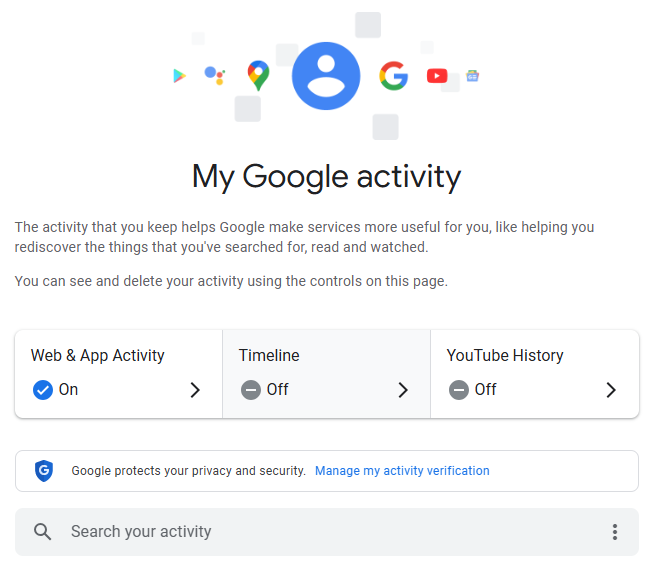
**3) Cache cookies analysis**

**cmd-> run as administrator**



**4)Last internal activity**

**Go to myactivity.google.com**

****