Name: Jinal Sojitra Enrollment No: 19012021081

Subject: FCL

Practical 4 to 7

Class: CEIT-A

**Practical - 4**

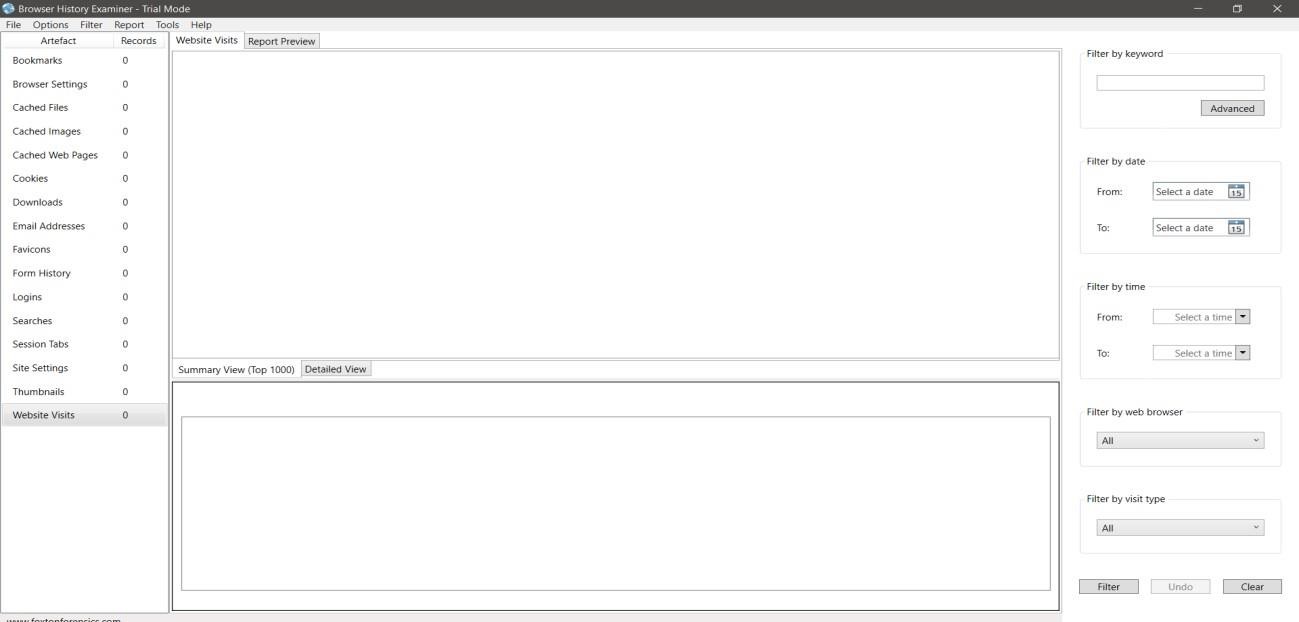
**Aim: Browser Forensic**

Web browsers are used in mobile devices, tablets, netbooks, desktops, etc., and often can be used not just for web surfing, but for navigation through the file system of the device. The web browser’s cache can contain downloaded images, videos, documents, executable files, and scripts. Web browsers also can contain data entered into forms: search queries, logins, and passwords for web email accounts, social networks, other websites, and financial information (for example, credit card numbers). Favorites and searches can give the researcher an idea of the device owner’s interests.

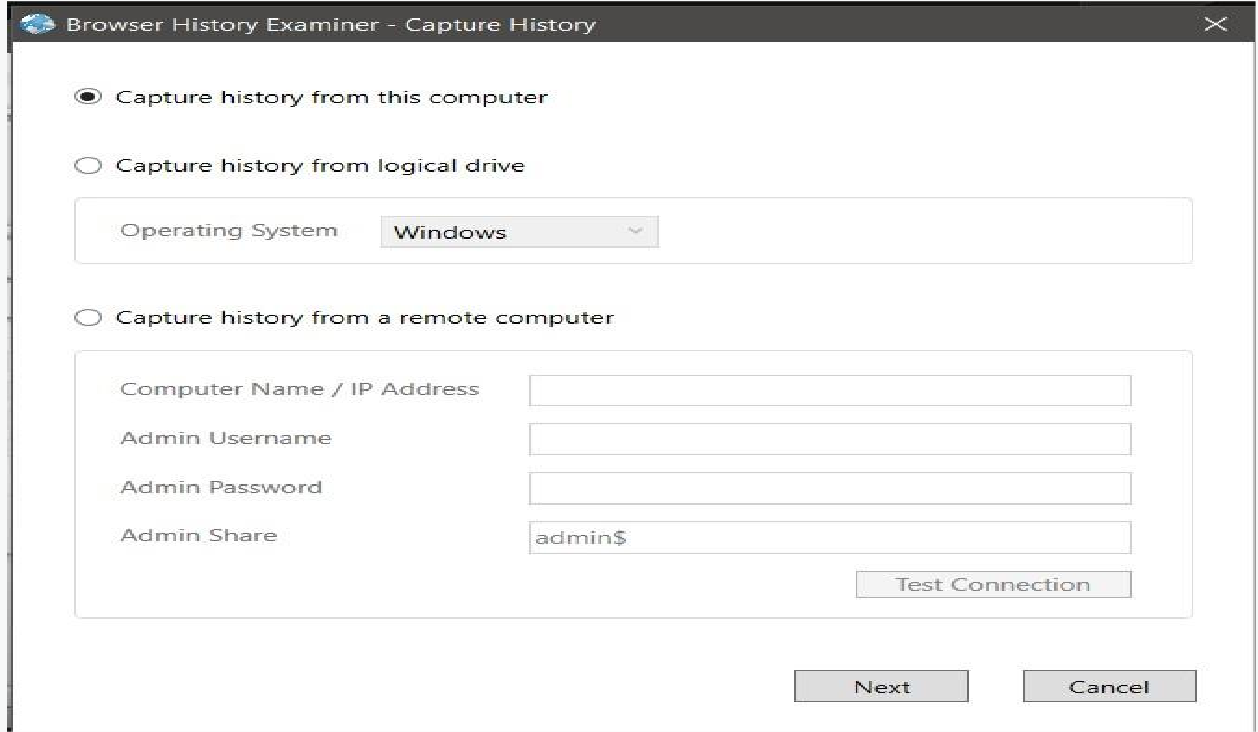
Browser Forensics is of no small importance in incident response for understanding how an attack on a computer or computer network began and finding the source of compromise.

The main sources of malware/spyware/adware are emails (including web mail), social networks, and other compromised sites. Typically, a user accesses all these sources (web emails, social networks, sites) using web browsers.

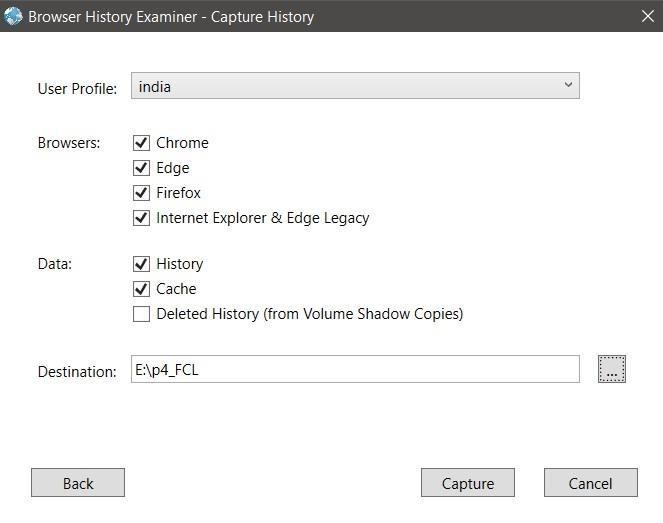
Install Browser History Examiner on your computer:



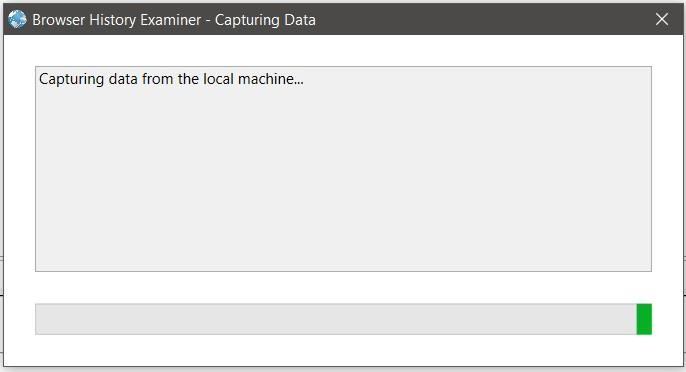
Go to in file and select Capture History and next:



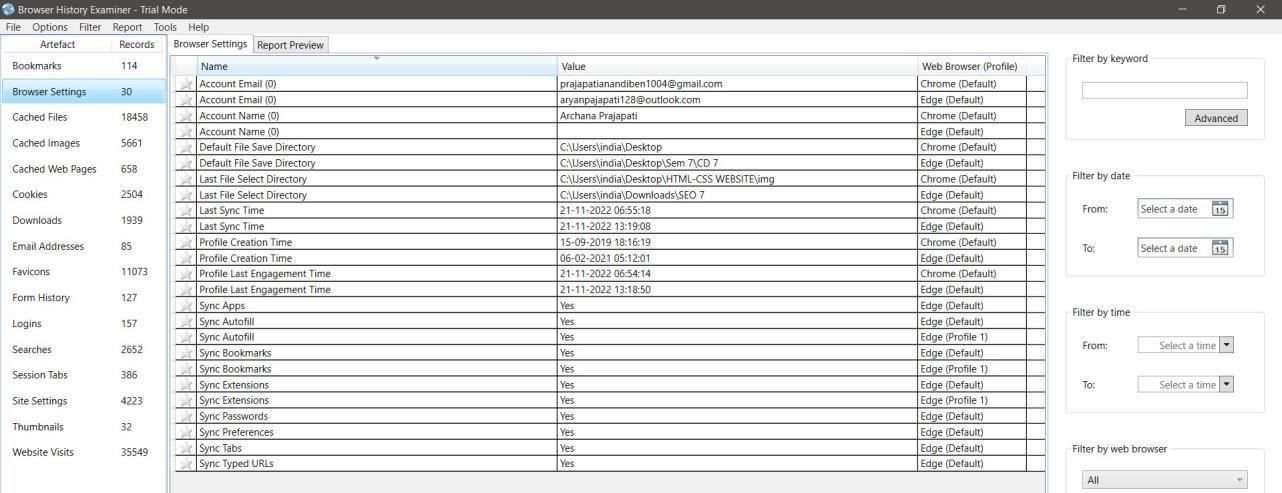
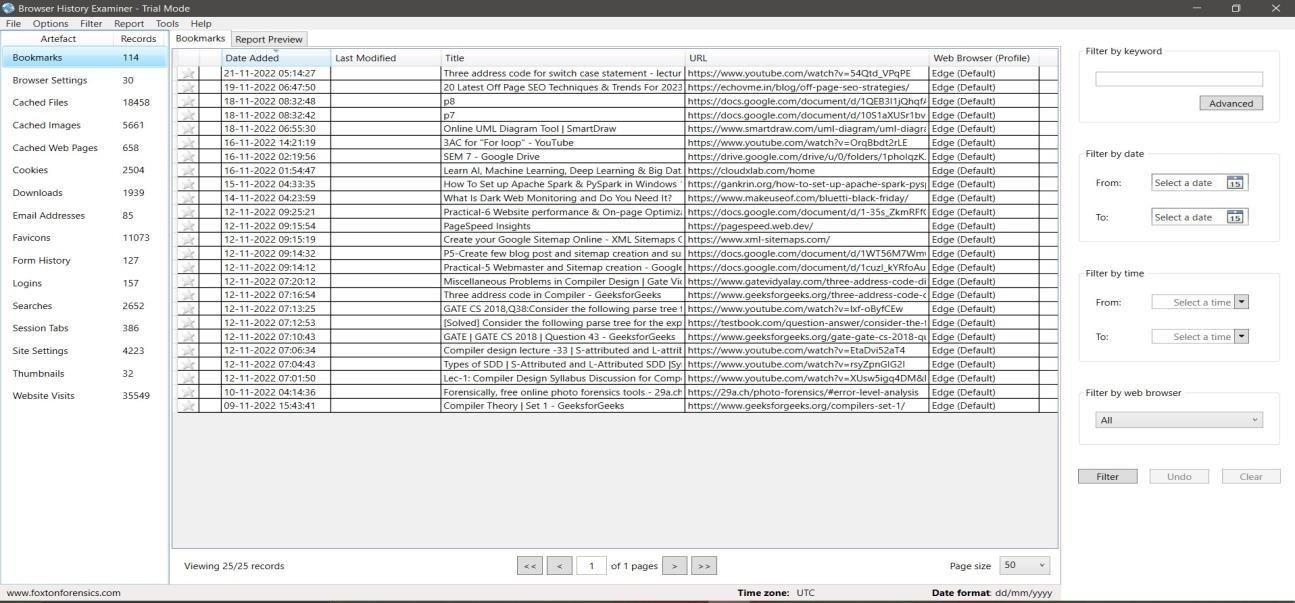
And Select Destination where you want to store this file:



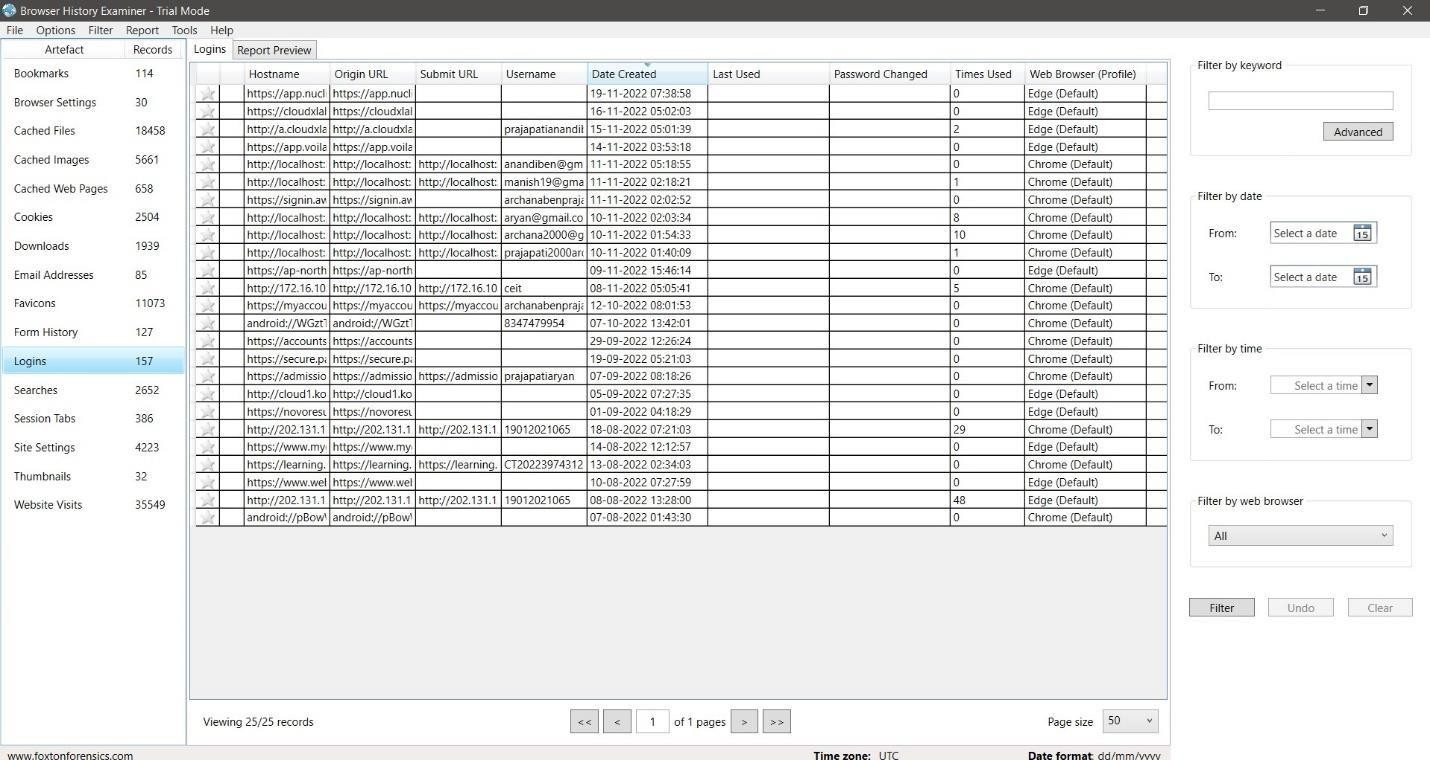
And click Capture



|  |  |
| --- | --- |
|  | |
| After Execute this process: |  |
|  | |



|  |
| --- |
|  |
|  |
|  |



**Practical - 5**

**Aim: Email Forensic**

# Email Forensic Investigation Techniques

Email forensics refers to analyzing the source and content of emails as evidence. Investigation of email-related crimes and incidents involves various approaches.

# Header Analysis

Email header analysis is the primary analytical technique. This involves analyzing metadata in the email header. It is evident that analyzing headers helps to identify the majority of email-related crimes. Email spoofing, phishing, spam, scams, and even internal data leakages can be identified by analyzing the header.

# Server Investigation

This involves investigating copies of delivered emails and server logs. In some organizations, they do provide separate email boxes for their employees by having internal mail servers. In this case, the investigation involves the extraction of the entire email box related to the case and the server logs.

# Network Device Investigation

In some investigations, the investigator requires the logs maintained by the network devices such as routers, firewalls, and switches to investigate the source ofan email message. This is often a complex situation where the primary evidence isnot percent (when the ISP or proxy does not maintain logs or lacks operation by ISP [2]).

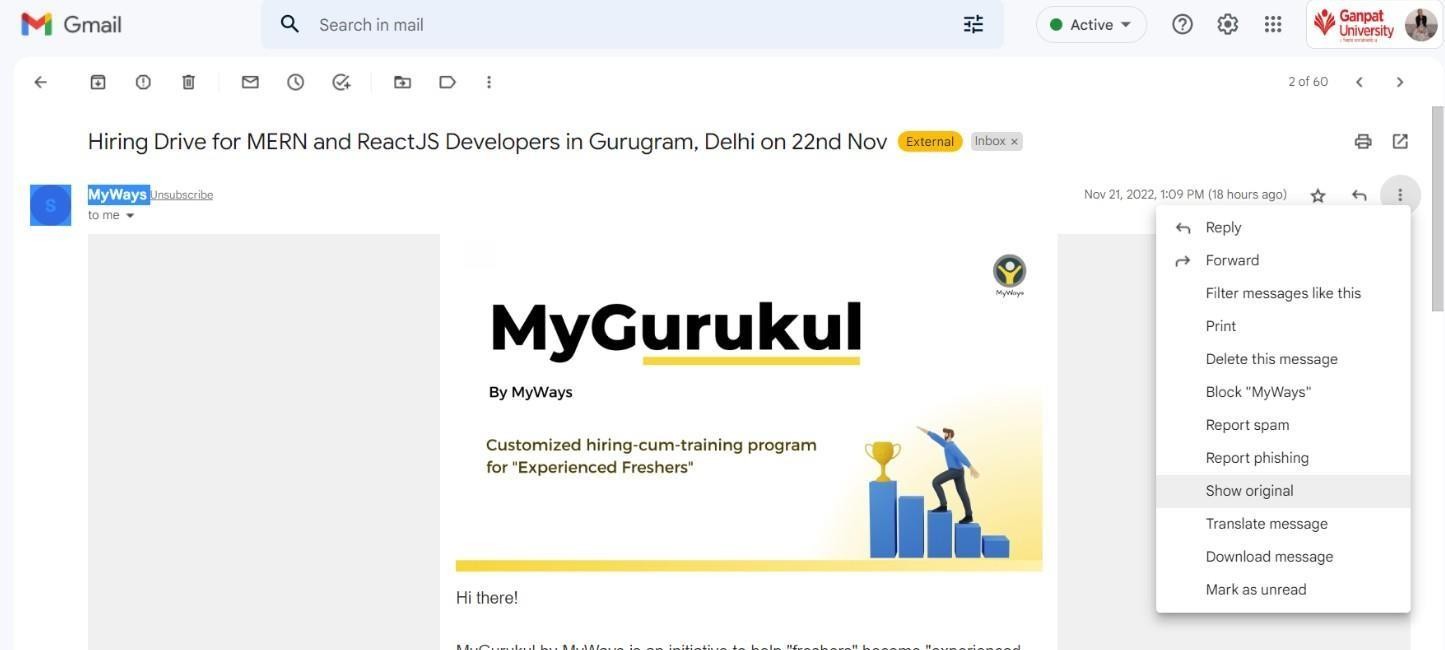
# Software Embedded Analysis

Some information about the sender of the email, attached files or documents may be included with the message by the email software used by the sender for composing the email [2]. This information may be included in the form of custom headers or in the form of MIME content as a Transport Neutral Encapsulation Format (TNEF)[2].

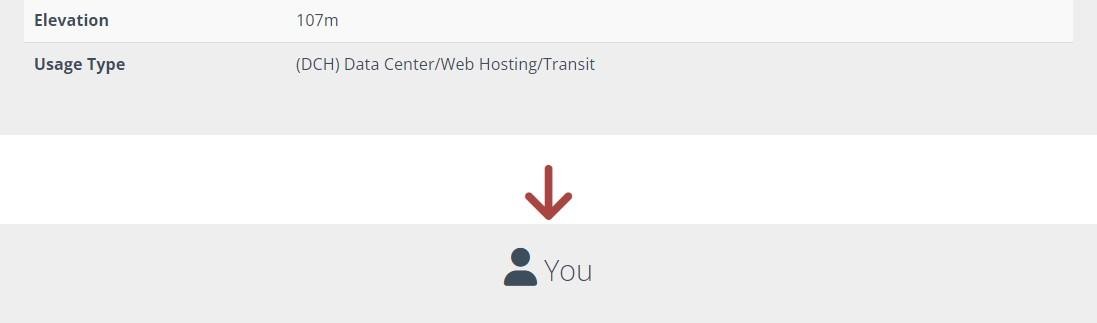
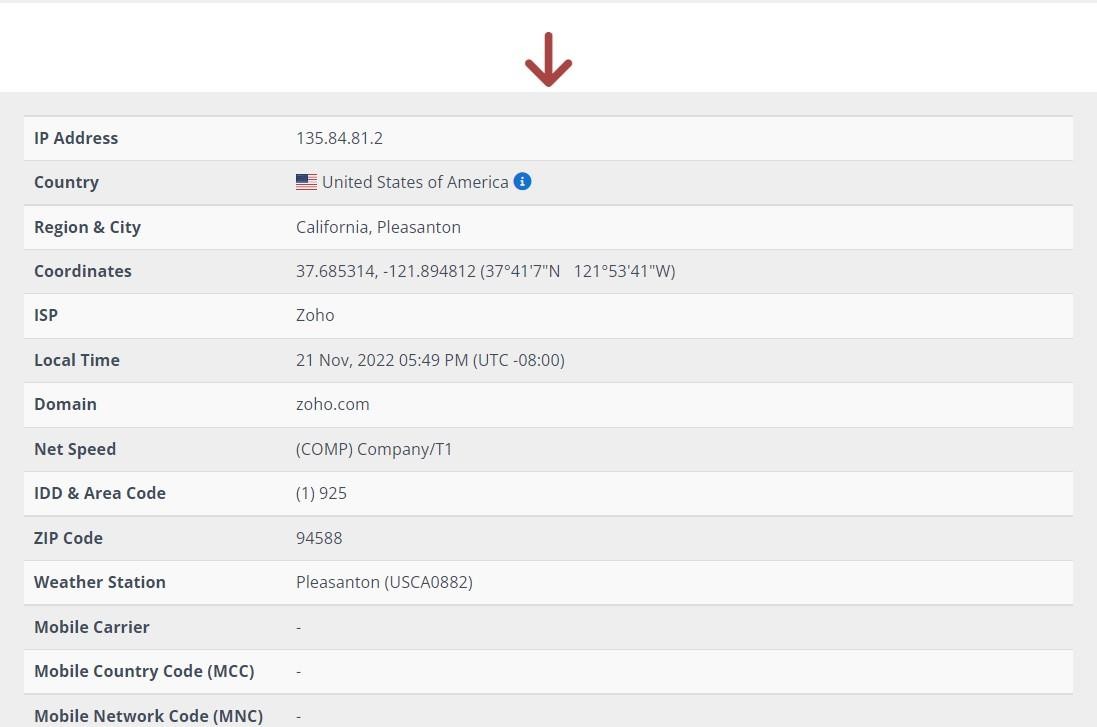
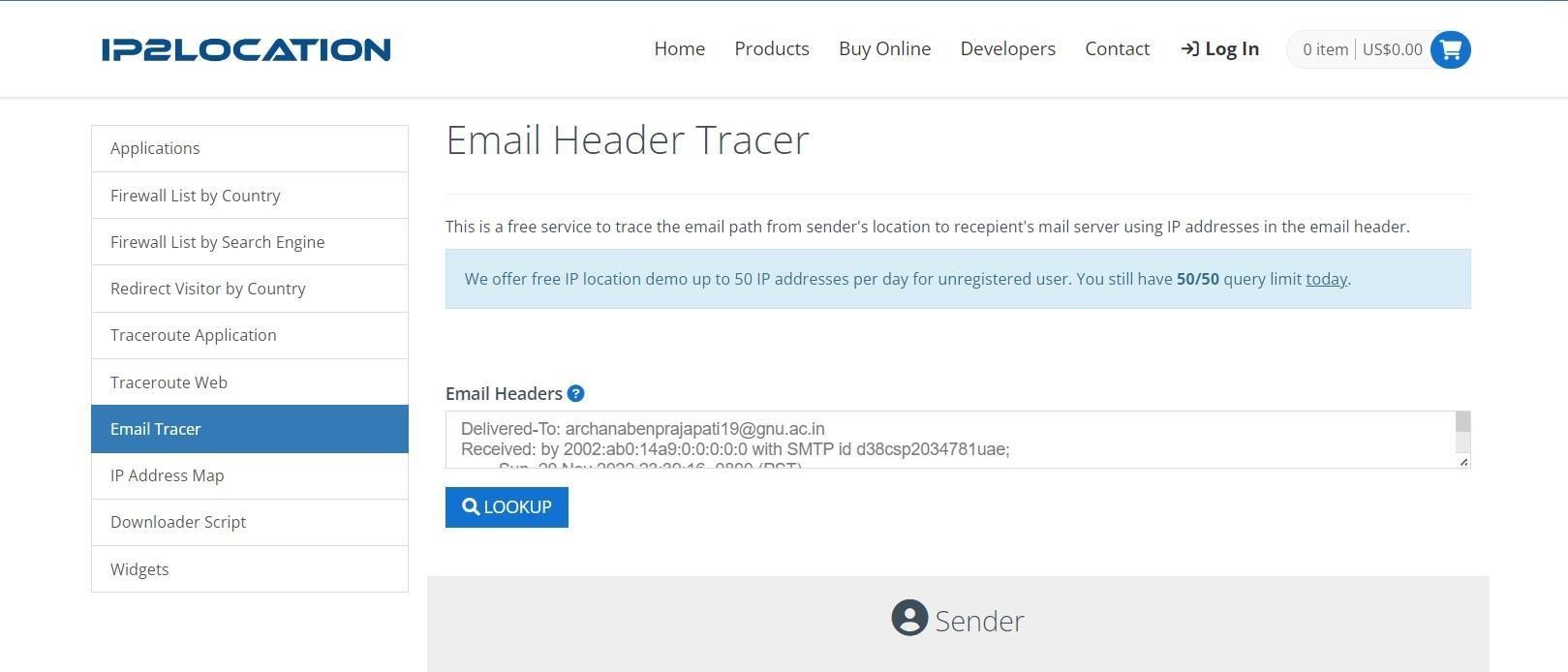
# Sender Mail Fingerprints

The “Received” field includes tracking information generated by mail servers that have previously handled a message, in reverse order. The “X-Mailer” or “User- Agent” field helps to identify email software. Analyzing these fields helps to understand the software and the version used by the sender.

Using Email Header Tracer:

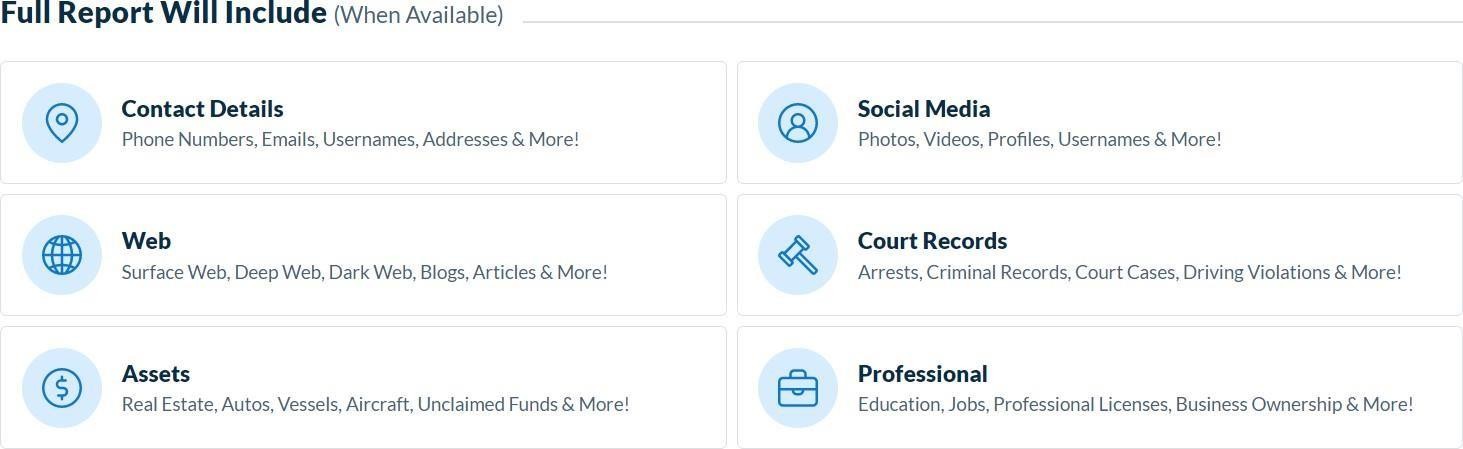
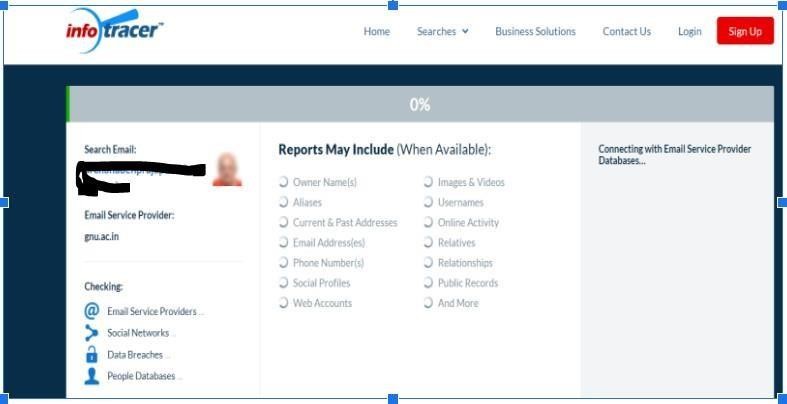
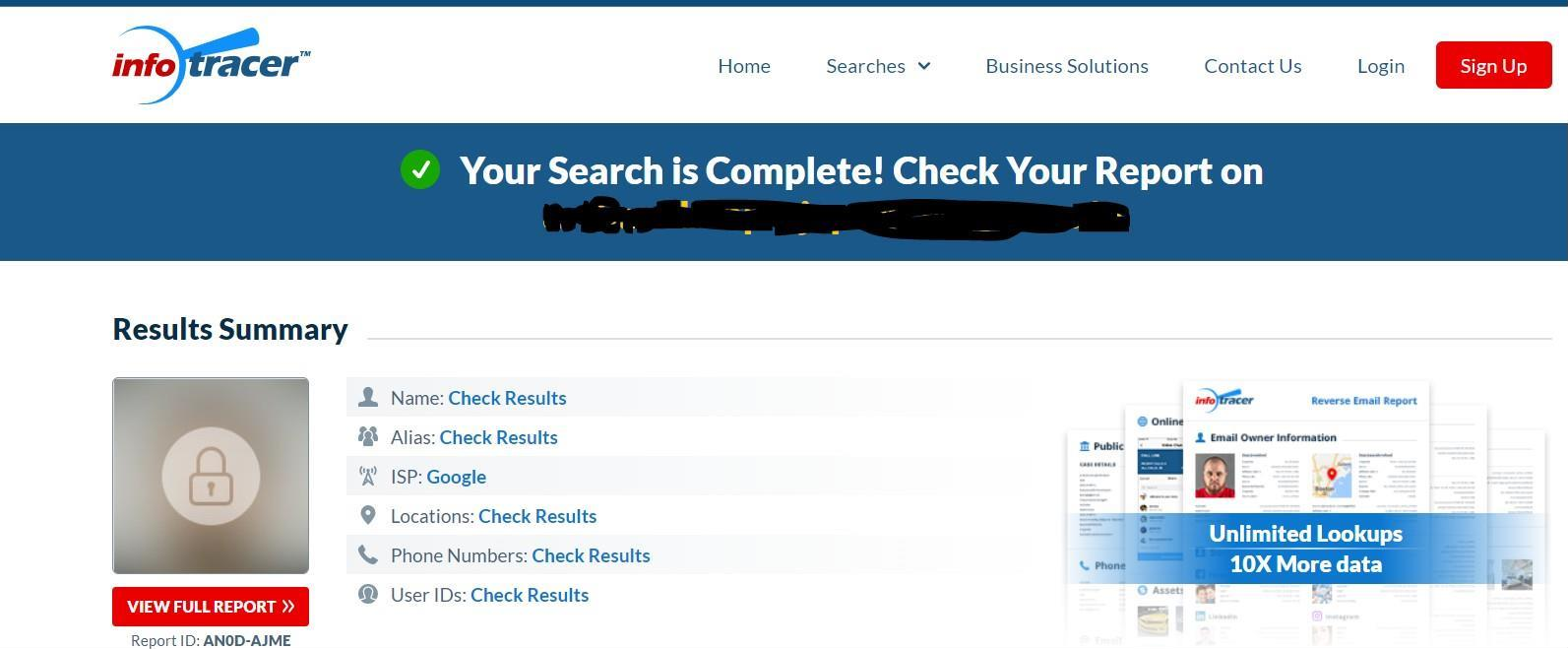
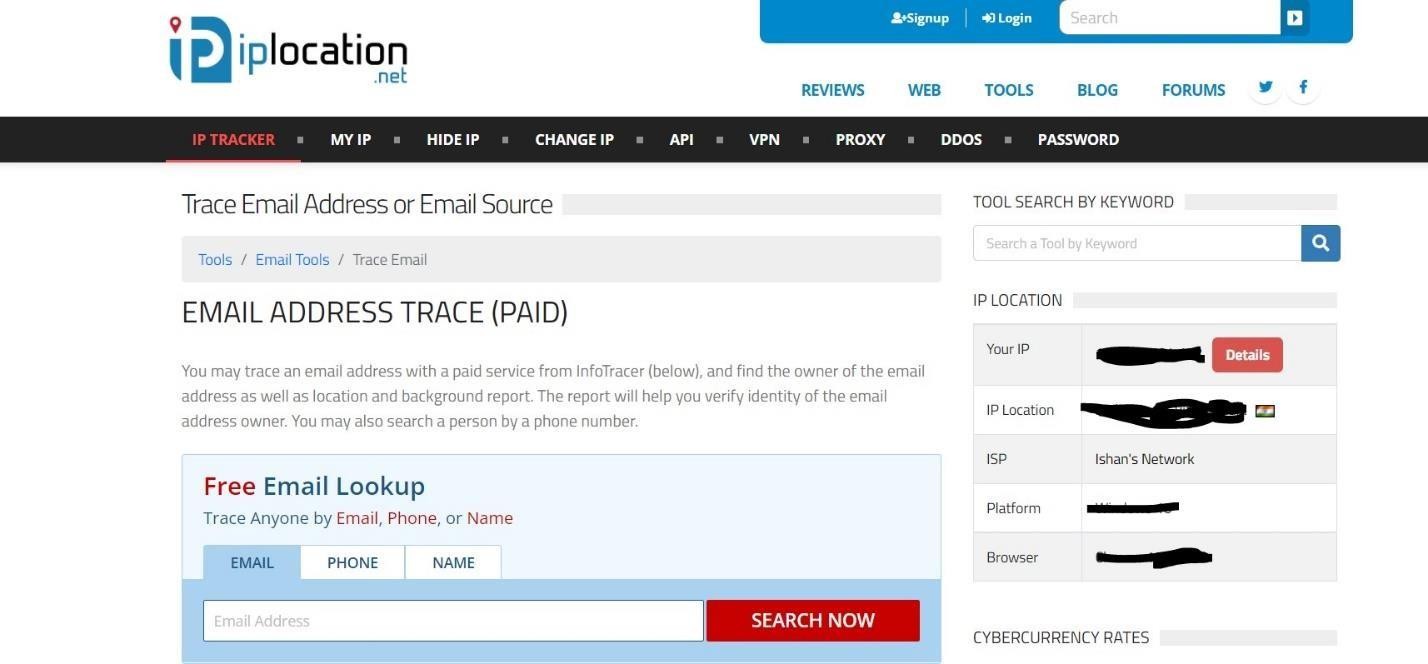


Copy the Original email header and paste it into this URL [Free Email Header Tracer | IP2Location](https://www.ip2location.com/free/email-tracer)

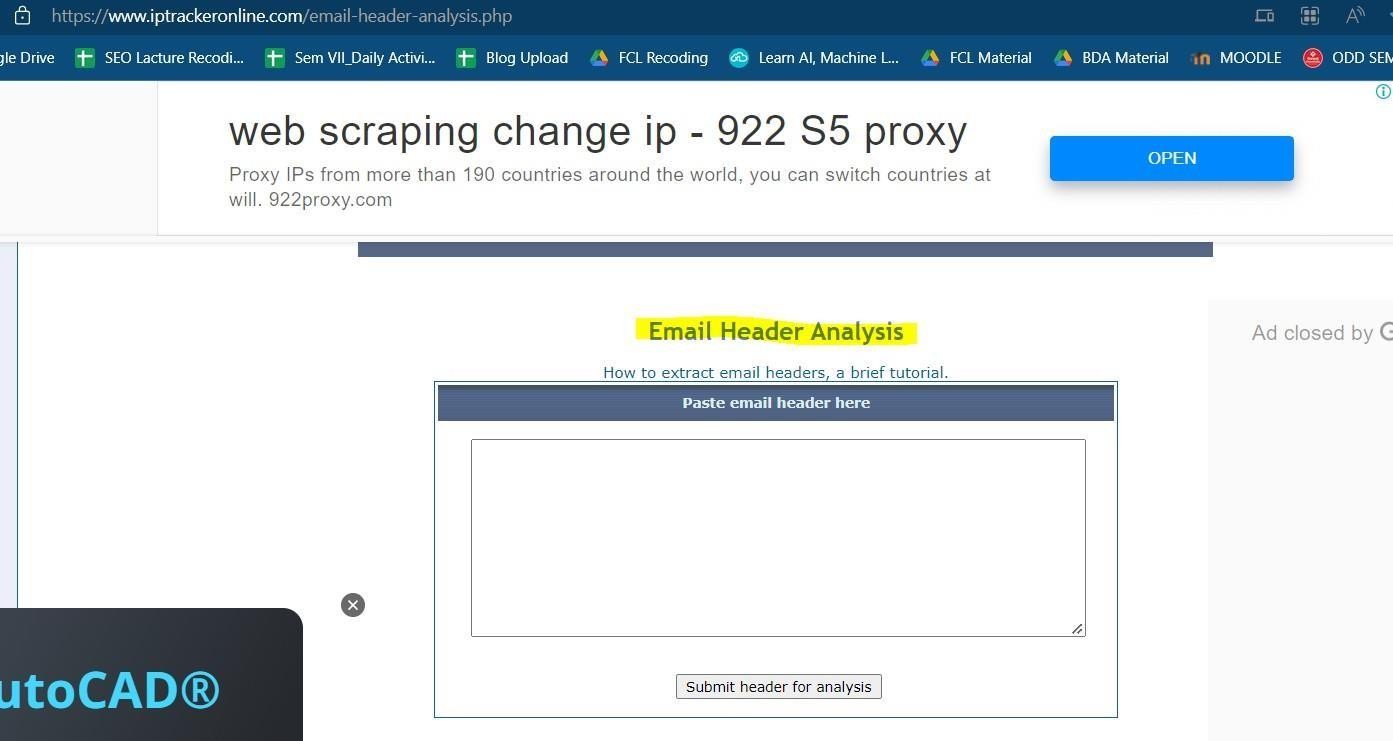


Also Using Trace Email Source: [Trace Email Source | IP Location](https://tools.iplocation.net/trace-email)

Enter any email address and search any email address person:



Now using Complete email header analysis in this link [Complete email header](https://www.iptrackeronline.com/email-header-analysis.php) [analysis. Analyse, track ip here (iptrackeronline.com)](https://www.iptrackeronline.com/email-header-analysis.php)

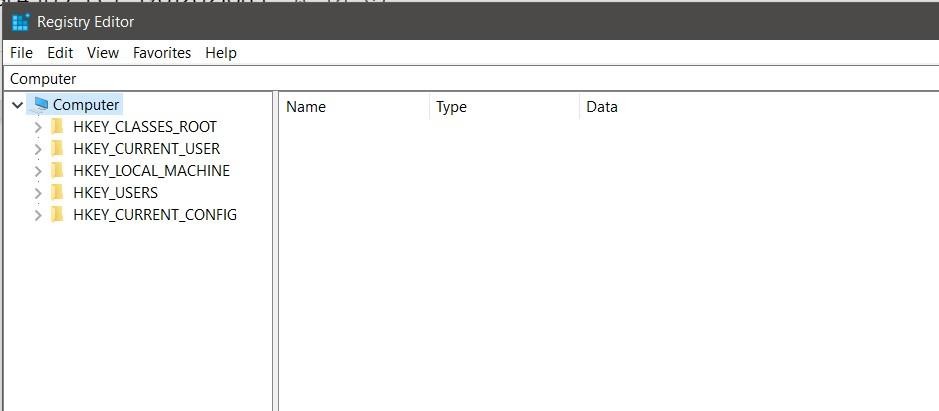
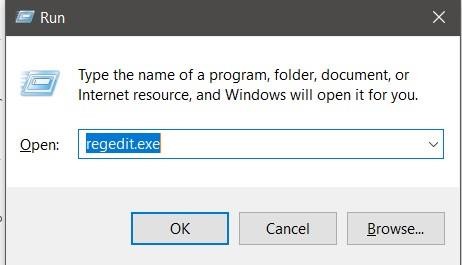


**Practical - 6**

**Aim: Registry Forensics**

Suppose your computer lies in the hand of a malicious person without your consent. Then how can you determine, what exactly he would have done to your computer? You can track his activity by inspecting the registry as follows −

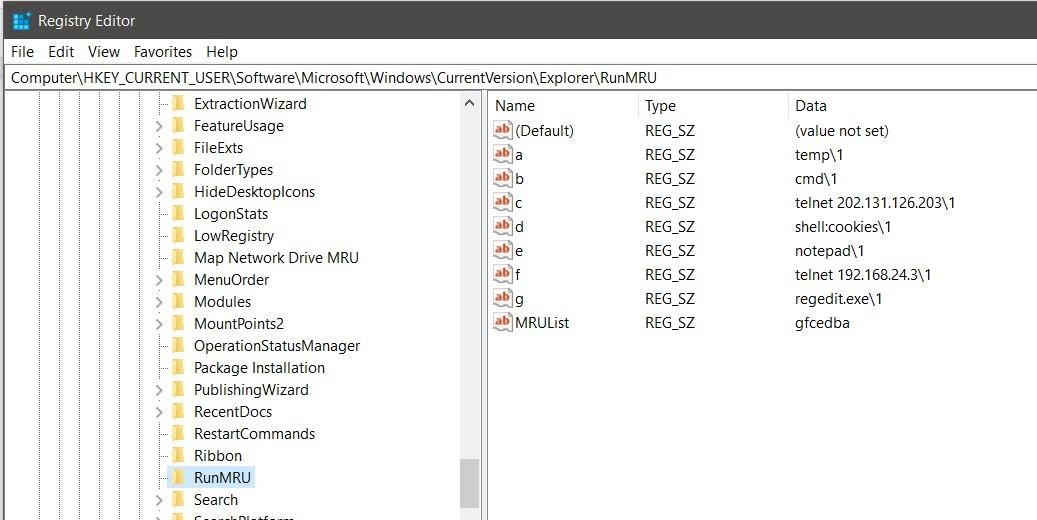
First Step you have type in Run in windows. And enter regedit.exe



# Most Recent User list

(HKEY\_CURRENT\_USER\software\microsoft\windows\currentversion\Explorer\ RunMRU)

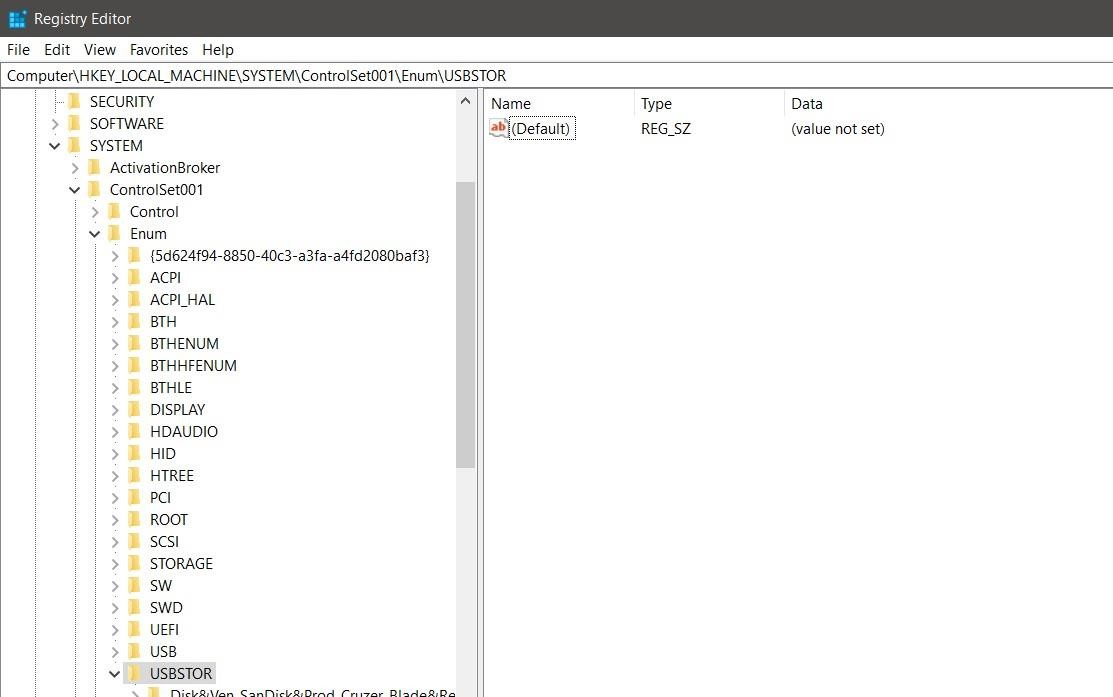
It contains the information provided from the RunMRU key, an examiner can gain a better understanding of the user they are investigating and the application that is being used. In the above figure, you can see the user has opened cmd, Notepad, MSPaint, etc.



# USB Connection

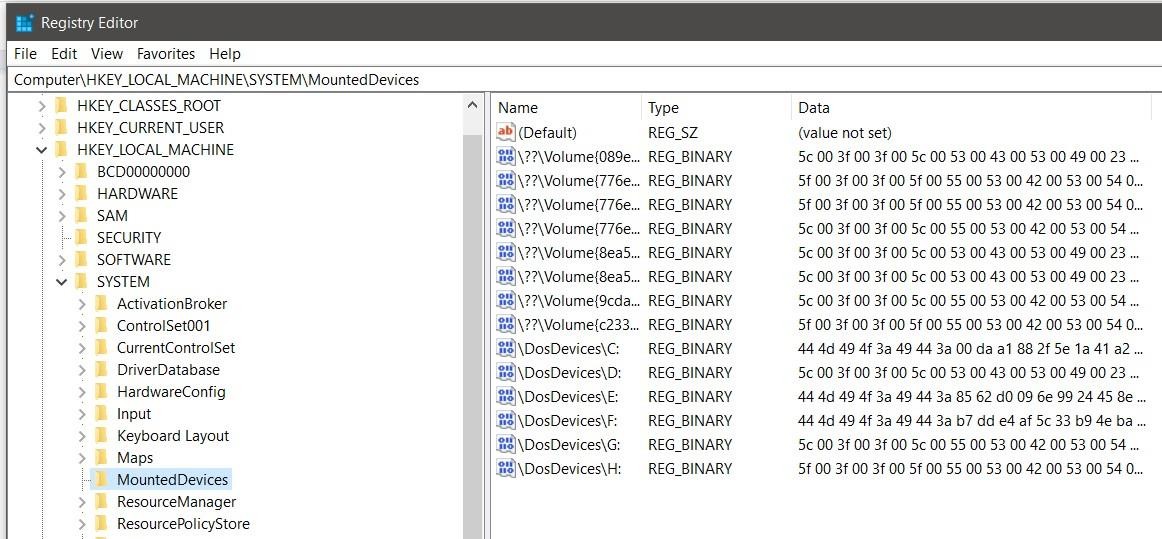
(HKEY\_LOCAL\_MACHINE\SYSTEM\controlset001\Enum\USBSTOR.)

This key stores the contents of the product and device ID values of any USB devices that have ever been connected to the system.



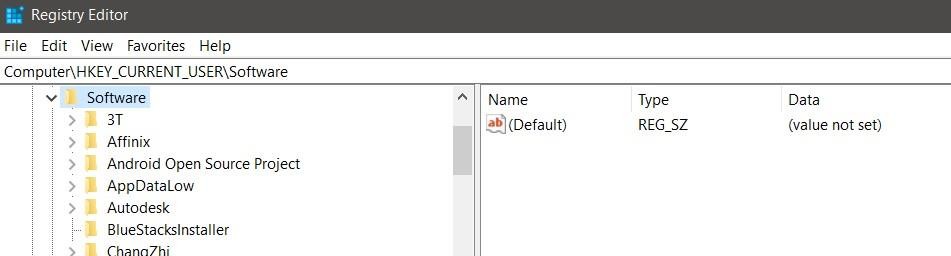
# Attached Hardware List − ( HKEY\_LOCAL\_MACHINE\SYSTEM|MountedDevices.)

This information can be useful to a forensic examiner as it shows any connected storage device has been recognized by the operating system. If the examiner notes a discrepancy between the physically attached devices and the ones reported here, it can be an indication that some device was removed prior to the evidence being seized.



# Malicious Software Running − (HKEY\_CURRENT\_USER\Software\ )

This information will be quite informatic for Forensics Examiner as it could see the hacker used VPN such as CyberGhost which is used for being anonymous.



# Recent Applications Used−

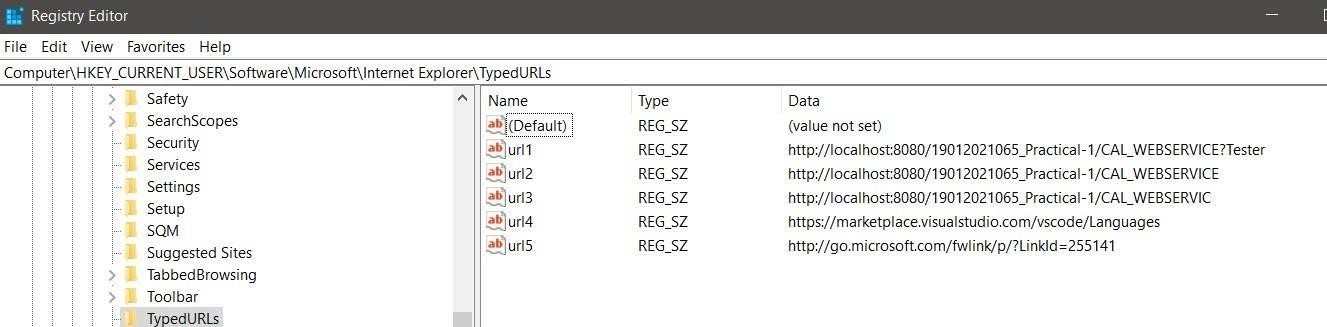
(HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Currentversion\Search\Recent Apps)

By navigating to the said key will give information for the last accessed applications list by the user.

# Internet Explorer information

(HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\TypedURLs.)

Internet Explorer is the native Web browser in Windows operating system. It utilizes the Registry extensively in the storage of data, like many applications.From the said key, we can obtain such information.



**Practical - 7**

**Aim: USB Forensics**

Having information about USB devices connected to a system can be essential for some investigations and analyses. Most of the removable storages used nowadays are USB pen drives so knowing how to identify and investigate these is crucial. The main purpose of USB drive forensic analysis is to identify the connected devices and find some of the following information about it: connection andremoval time, files copied to or from the device, opened and executed files and software from the attached drive. USB pen drives are heavily used by malicious actors for data stealing and malware propagation. Thus, related artifacts can be an essential part of many investigations.

There are three major USB device types in use nowadays. The one that is used the most for storage purposes is the Mass Storage Class (MSC). This is the class I am testing and documenting in this blog post. While lots of artifacts are the same for other classes as well, these were not tested by me. Here are the mentioned types and basic information about them:

# Mass Storage Class (MSC):

Used by thumb drives, mp3 players, some smartphones

On Windows, it is recognized as Hard Disk Driver, or device with Removable Storage

Files can be copied to or from the drive

# Picture Transfer Protocol (PTP):

Supported devices are: cameras, some smartphones

Can be used in case of image or video download from an external storage

User can download files from the drive but can’t upload anything to it (unidirectional)

# Media Transfer Protocol (MTP):

Technically a successor of PTP

Bi-directional file moving (from/to the drive) Can be used in case of any filetypes unlike PTP

Supported devices: cameras, smartphones

Download autopsy for the perform USB forensics using below link: [Autopsy - Download](https://www.autopsy.com/download/)

