Contemporaneous Notes

Computer Crime and Digital Evidence

Submitted by
Name: Ajaj Ahmed
Cyber Security and Digital Forensics
Kathmandu, Nepal
Dec 24, 2024

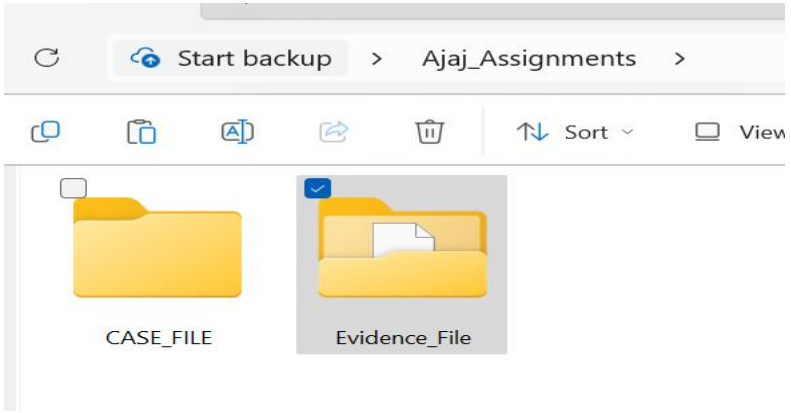
Contemporaneous Notes

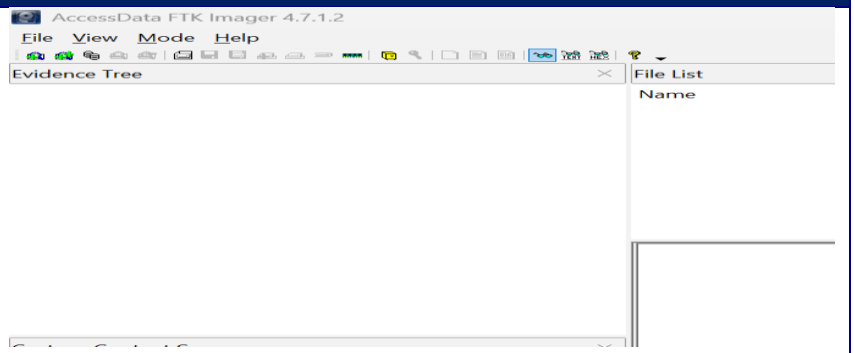
Examiner	AJAJ AHMED	Exam commenced	26th November, 2024
Other relevant information	UWE ID: 24000864	Software used, versions, and licensing.	1. AccessData FTK Imager 4.7.1.2 2. Autopsy 4.21.0 3. Event Log Explorer 4.8 4. Registry Viewer 6.0 5. RegRipper 3.0 6. HXD 2.5 7. SAMDUMP2 (used in Linux)

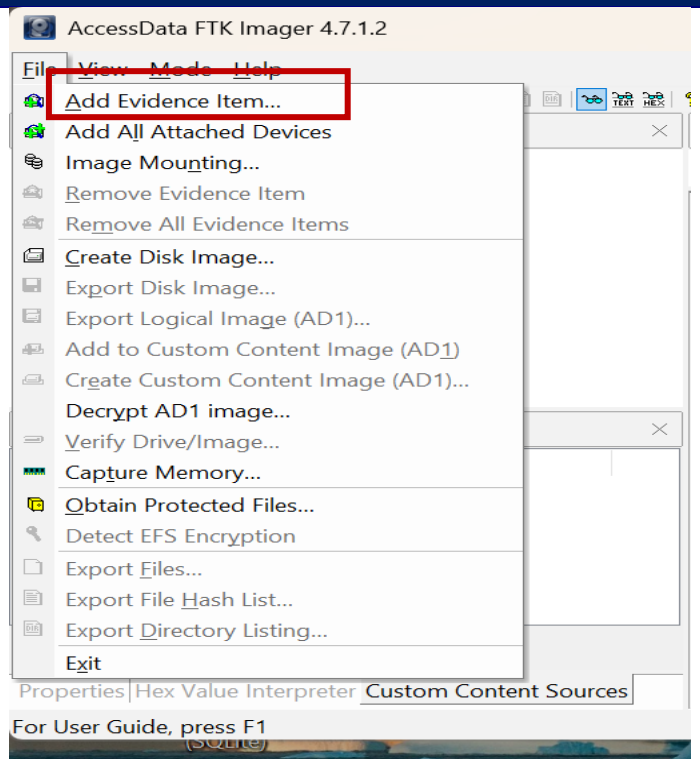
			

Note: If you decide to omit a process, you should provide your reasons. You may add additional rows, as appropriate.

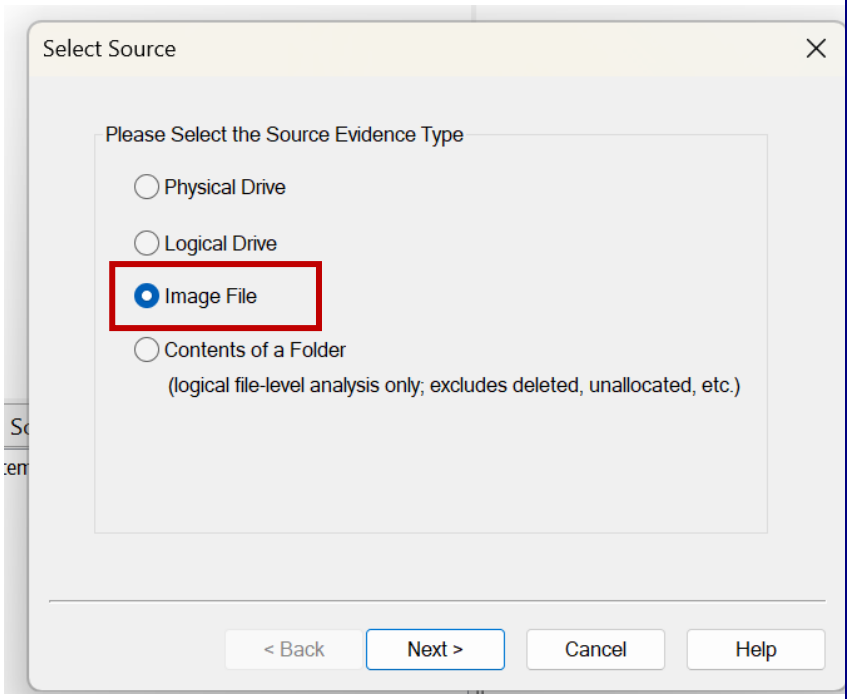
Action	Done?	Date	Time	Notes
Load case and verify image	Yes	19th Dec, 2024	01:00 Pm	**Step1:** • Created Two Folders; named **Case file** and **Evidence file**.

Action	Done?	Date	Time	Notes
				• I kept the evidence image of **Hunter XP for Dongled v6.E01** in the evidence file. And other case-related files in the Case File.  **Step2:** Launched **AccessData FTK Imager**

Action	Done?	Date	Time	Notes
				 **Step3:** • At the left corner I clicked on **file** and selected **add evidence item.**

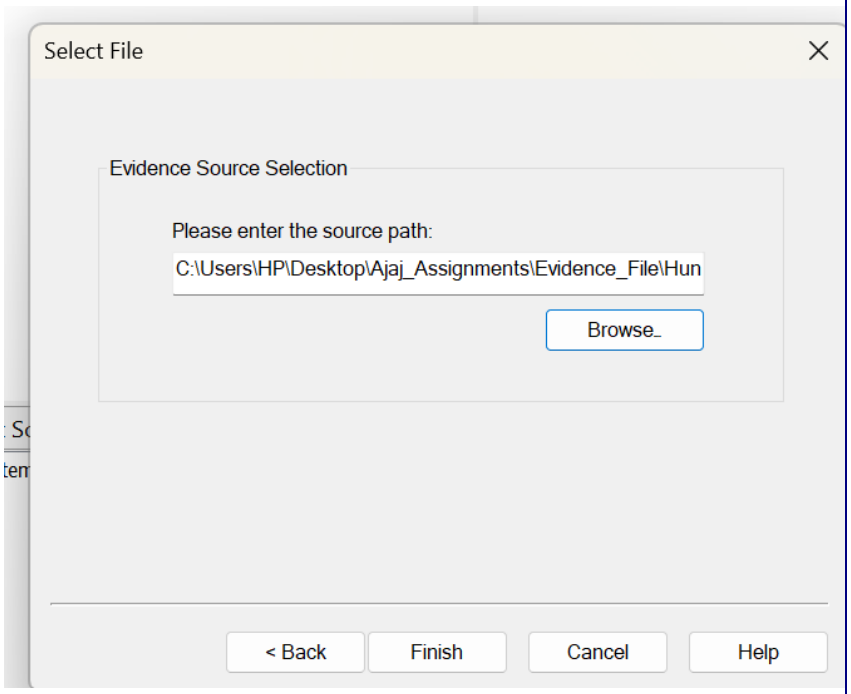
Action	Done?	Date	Time	Notes
				 **Step 4:** • after clicking on the add evidence item we are asked to select different types of files and drives.

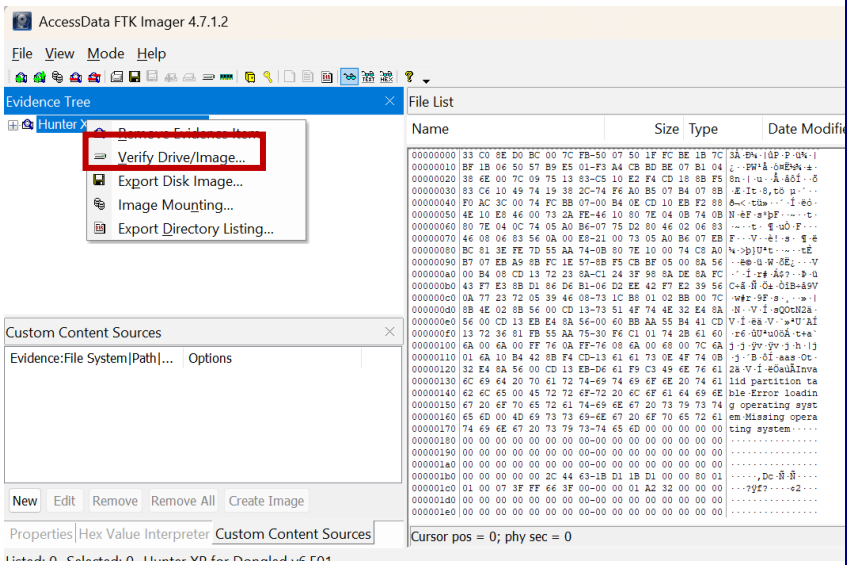
Action	Done?	Date	Time	Notes
				• I selected the **image file** as I have given evidence image of **Hunter XP for Dongled v6.E01**

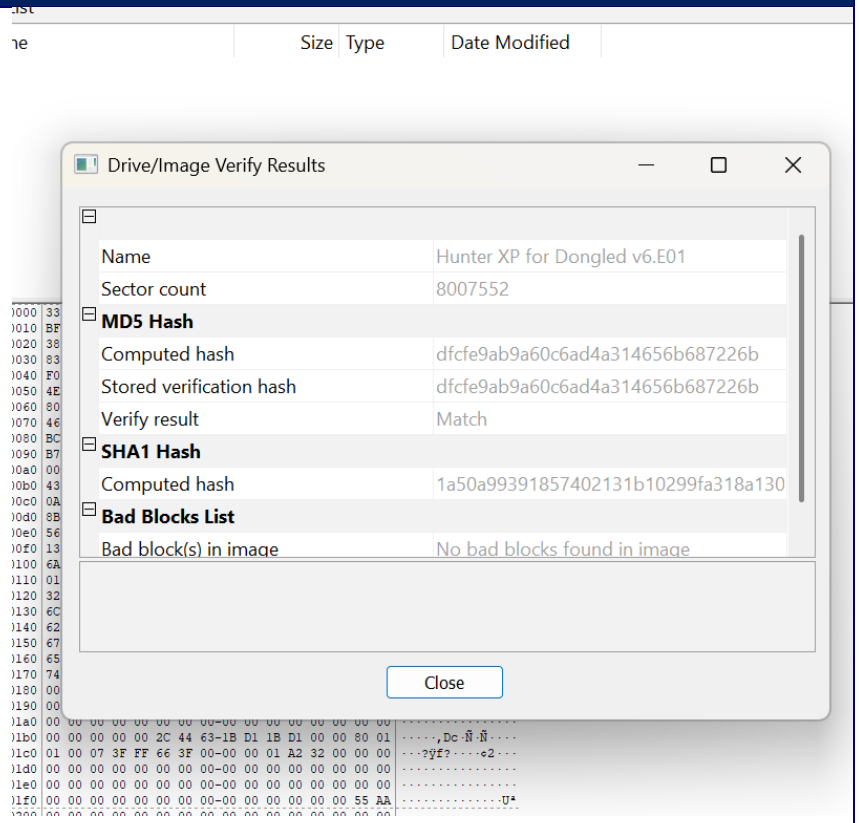


Step 5:

- I browse the path C:\Users\HP\Desktop\Task\Hunter XP Image\Hunter XP Image where we kept the image file

Action	Done?	Date	Time	Notes
				before starting the task and loaded it into **AccessData FTK Imager.**  **Step 6:**

Action	Done?	Date	Time	Notes
				• To Verify the image, I **clicked right on** the image and selected Verify Drive/Image to get MD5 Hash and SHA1 hash. 

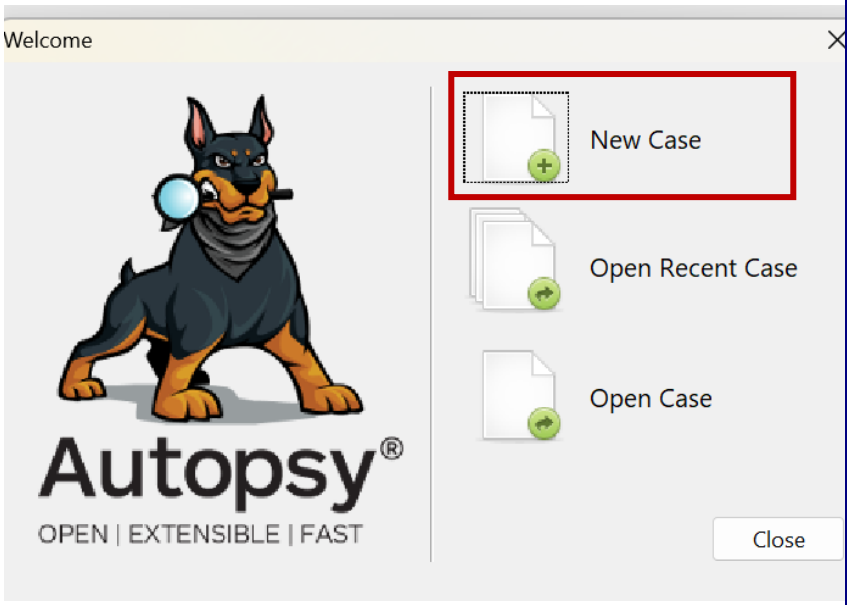
Action	Done?	Date	Time	Notes
				

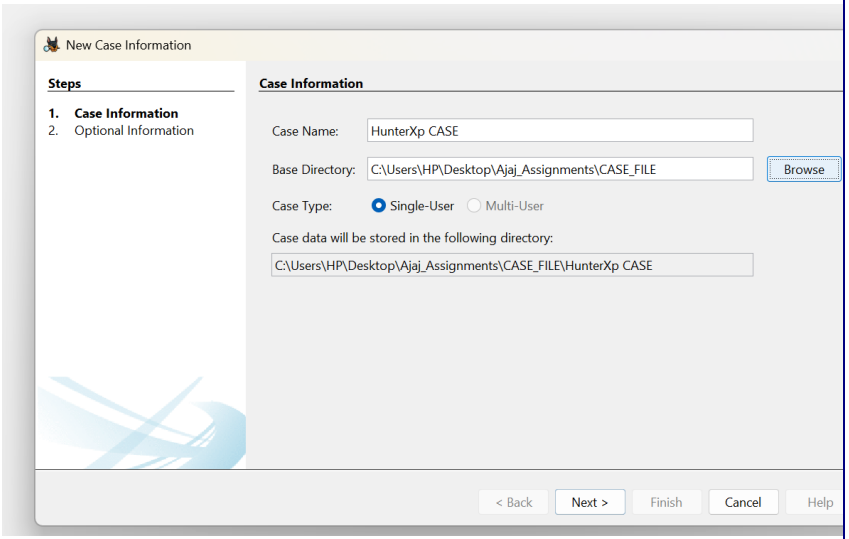
Finally, I got.

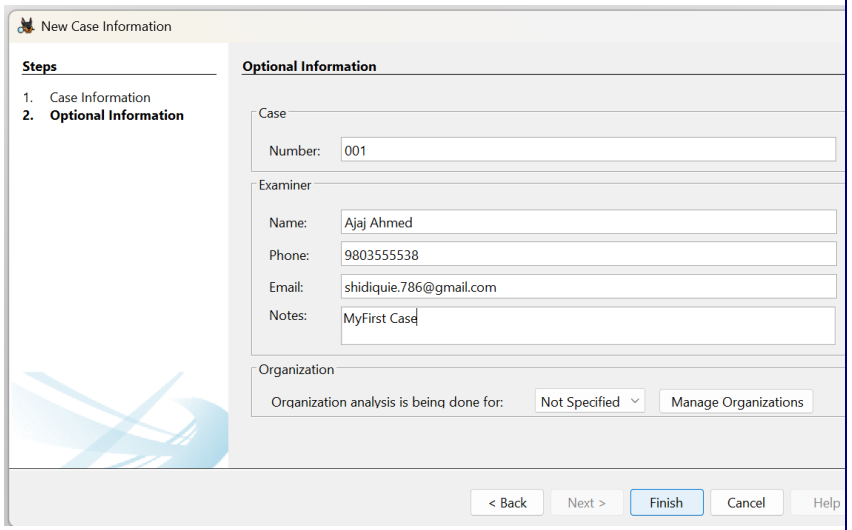
MD5 Hash:

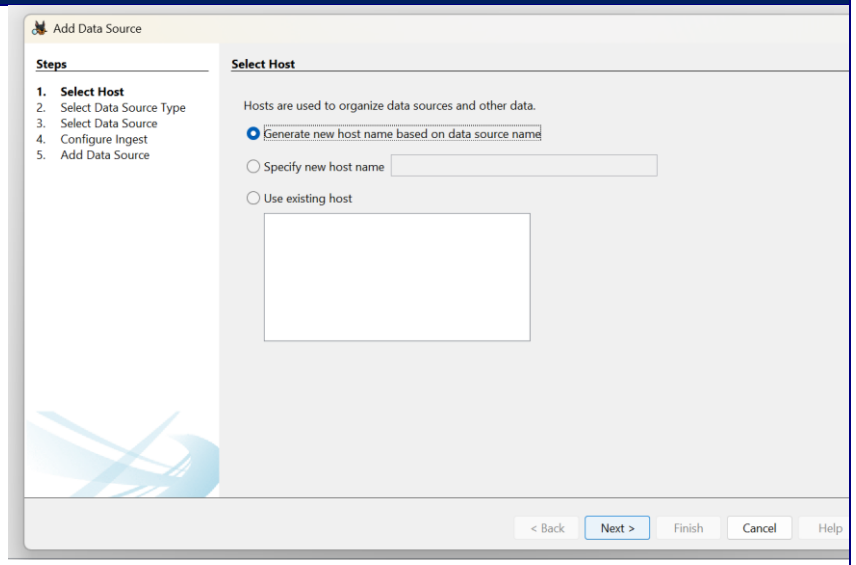
dfcfe9ab9a60c6ad4a314656b687226b

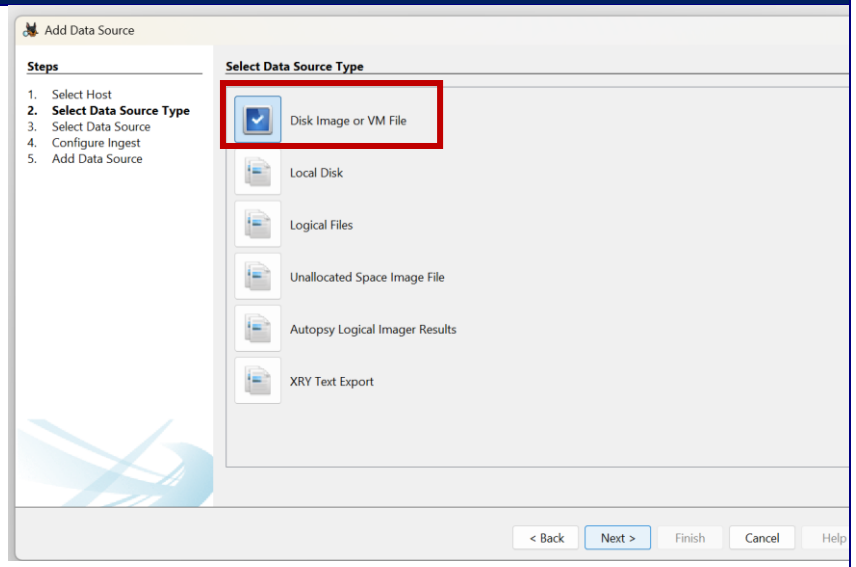
SHA1 Hash:

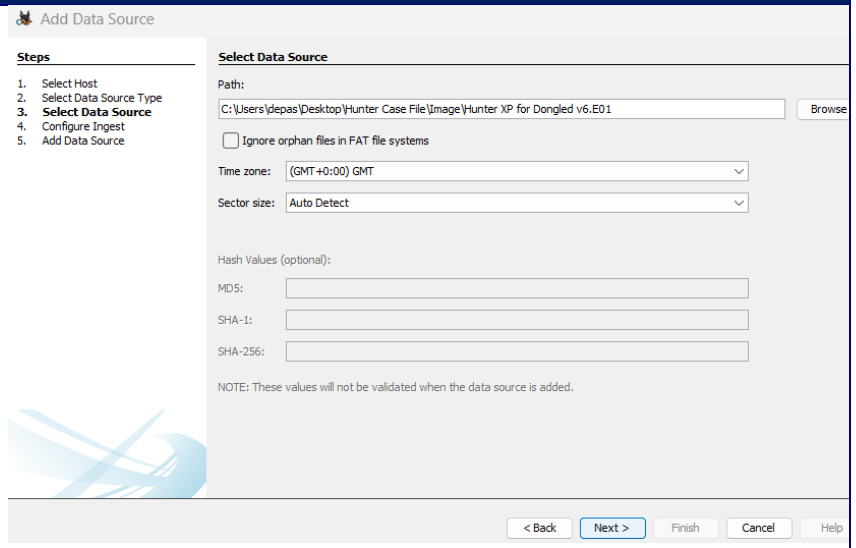
Action	Done?	Date	Time	Notes
				1a50a99391857402131b10299fa318a130a603b0 **VERIFICATION USING AUTOPSY** **Step1:** • Opened second forensic tool **Autopsy**. • Clicked on **New Case**.  **Step2:** • I gave case information.

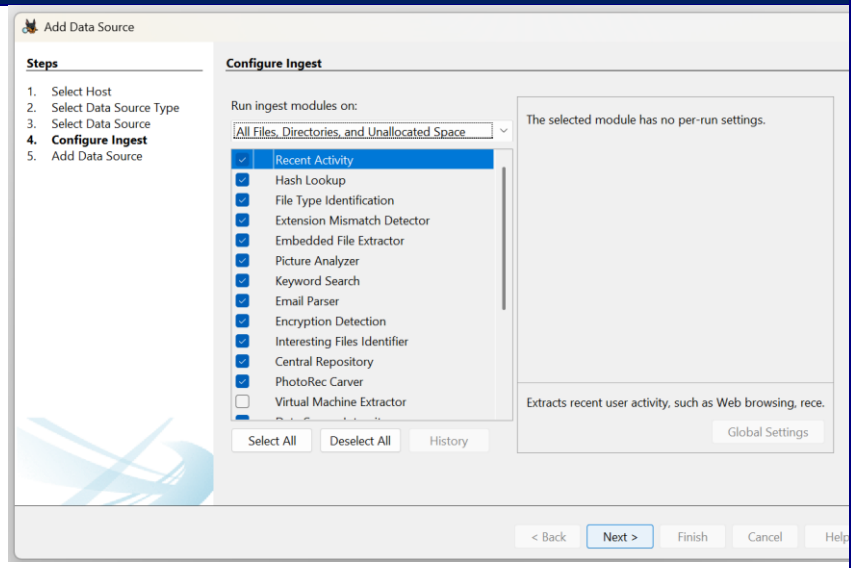
Action	Done?	Date	Time	Notes
				➢ Case Name: **HunterXP Case** ➢ Base Directory: C:\Users\HP\Desktop\Ajaj_Assignments\CASE_FILE  **Step 3:** • I give Optional Information About; ❖ Case: ➢ Case Number: **001**

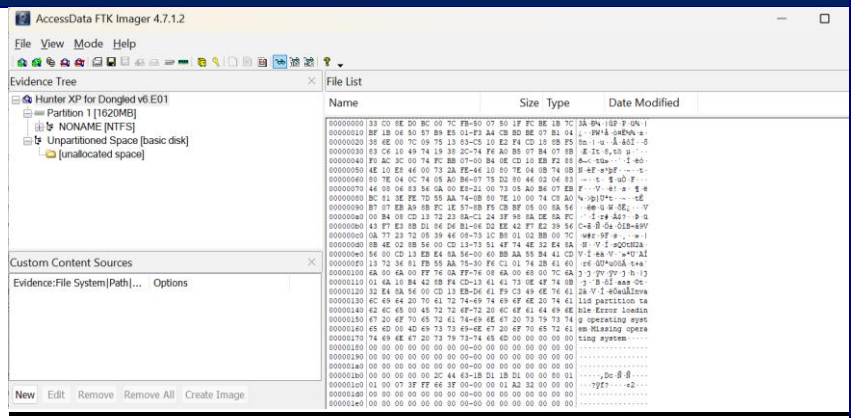
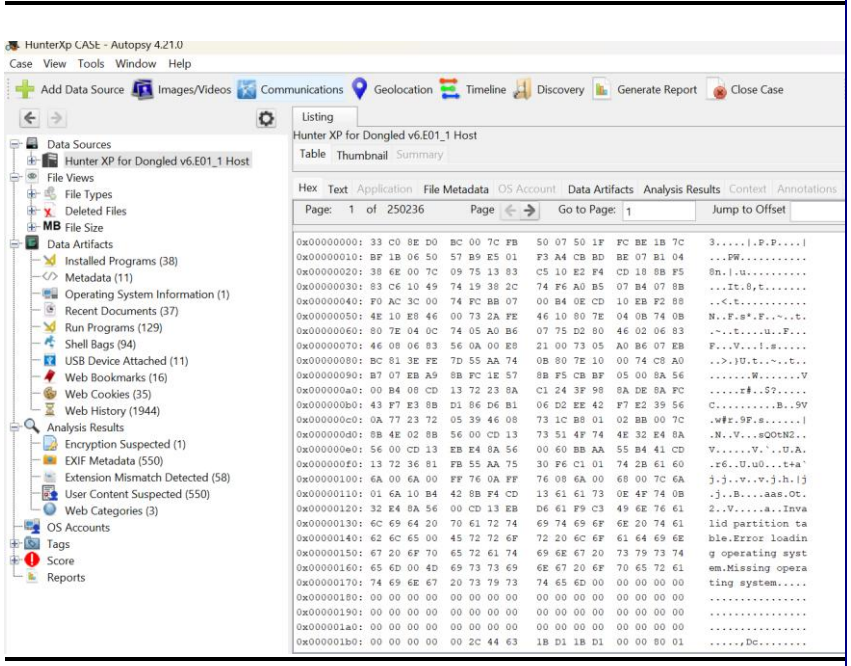
Action	Done?	Date	Time	Notes
				❖ Examiner: ➢ Name: **Ajaj Ahmed** ➢ Phone: **9803555538** ➢ Email: **shidiquie.786@gmail.com** ➢ Note: **MyFirst Case**  **STEP 4:** a. Selected **host**

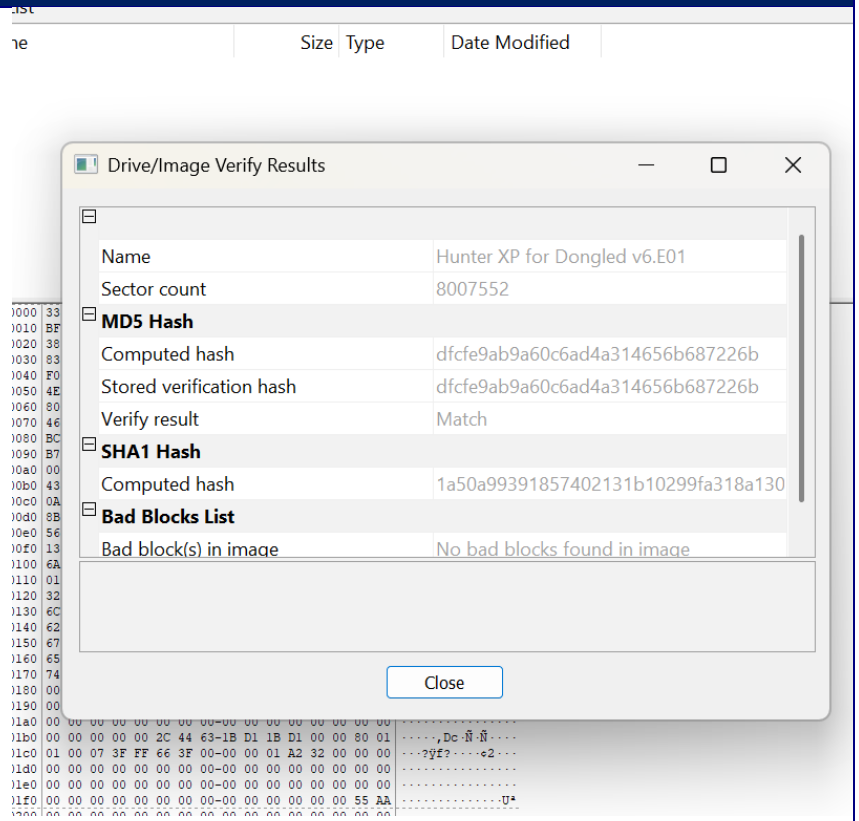
Action	Done?	Date	Time	Notes
				 Selected Data source file **Disk Image or VM File**

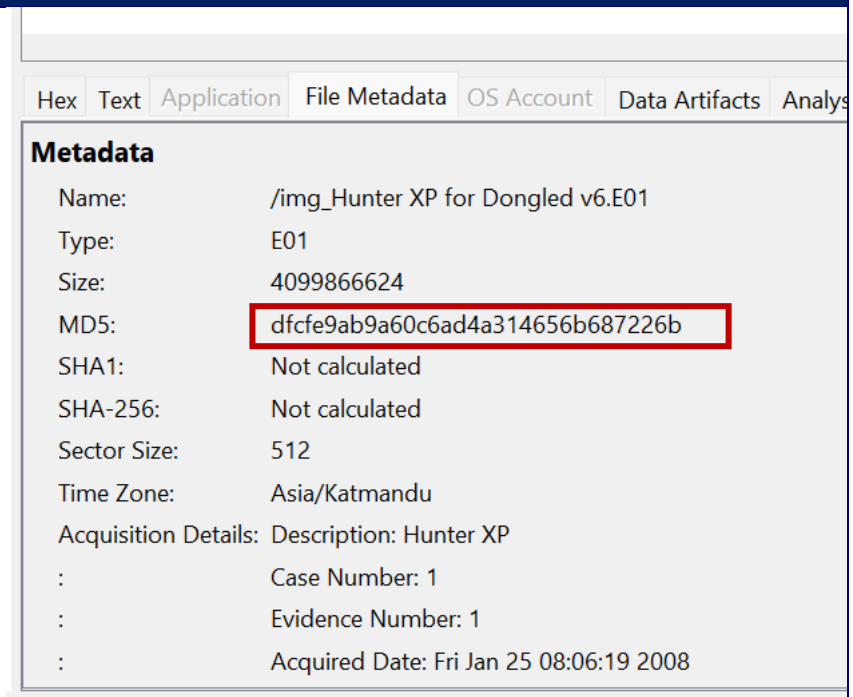
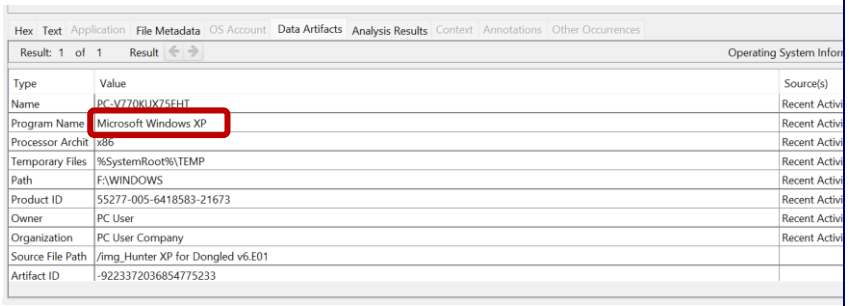
Action	Done?	Date	Time	Notes
				 a. Selected data source by Browsing path C:\Users\HP\Desktop\Task\Hunter XP Image\Hunter XP Image

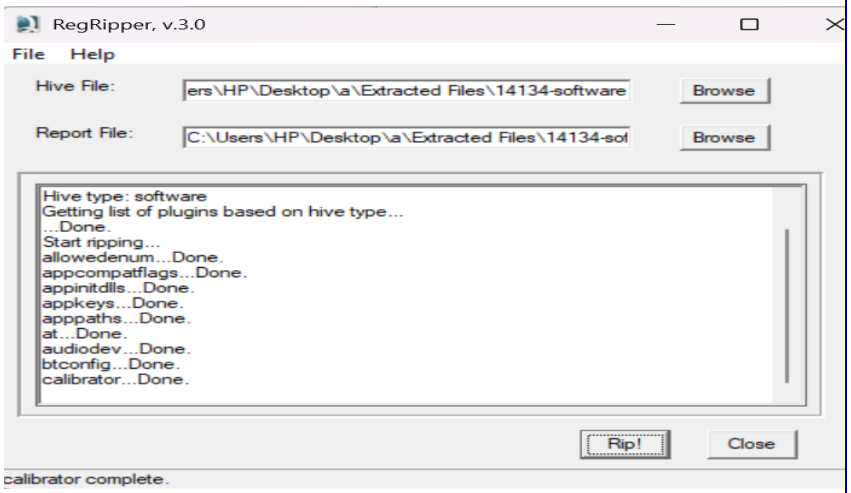
Action	Done?	Date	Time	Notes
				 a. Configured **Ingest Modules**.

Action	Done?	Date	Time	Notes
				 Finally, Data Source has been added to the Autopsy for Further Investigation. **Step 5:** • After loading and analysing the metadata I found the **MD5 hash** value and **hex value** of the image file is same. It gives the dual verification of image artifacts.

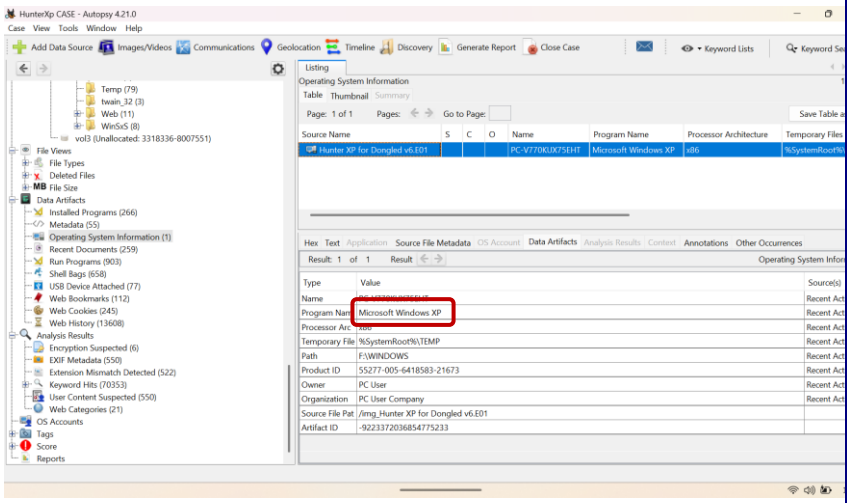
Action	Done?	Date	Time	Notes
				 

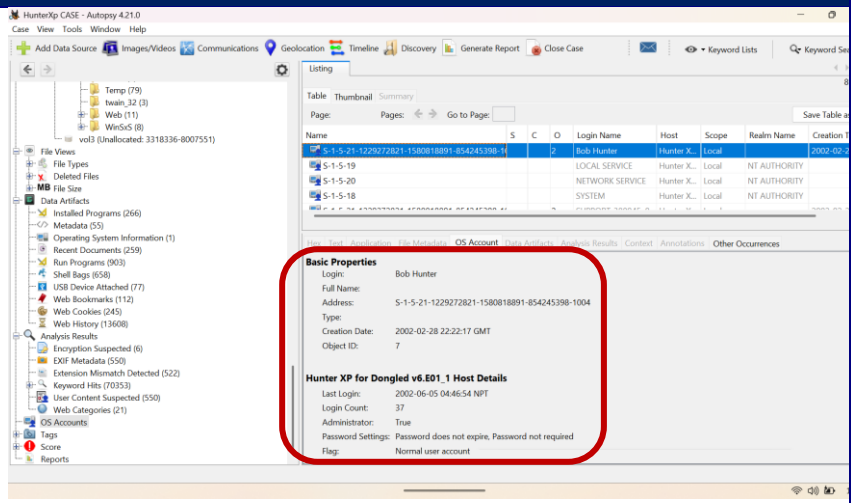
Action	Done?	Date	Time	Notes
				

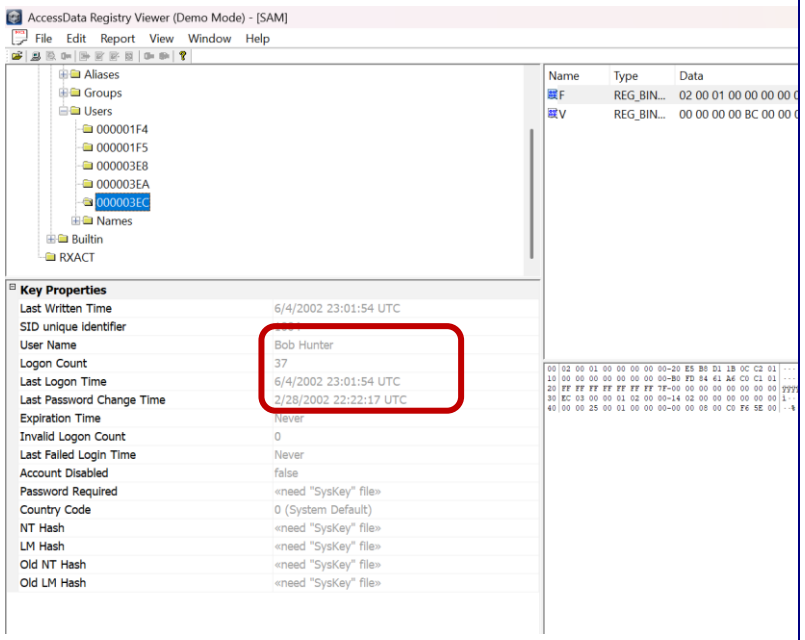
Action	Done?	Date	Time	Notes
				
				

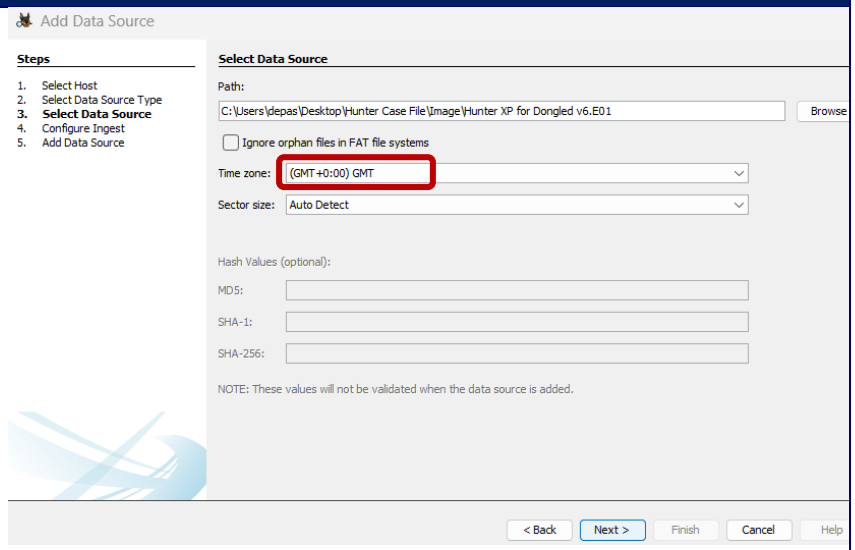
Action	Done?	Date	Time	Notes
Load Case into a second forensic tool for dual verification of at least 2 key artifacts, evidence items	yes	19/12/2024	01/20 pm	**Step1:** Loaded case into Autopsy and followed the path; Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/config • Then extracted software file • The software file is ripped using RegRipper tool to get its txt file. 

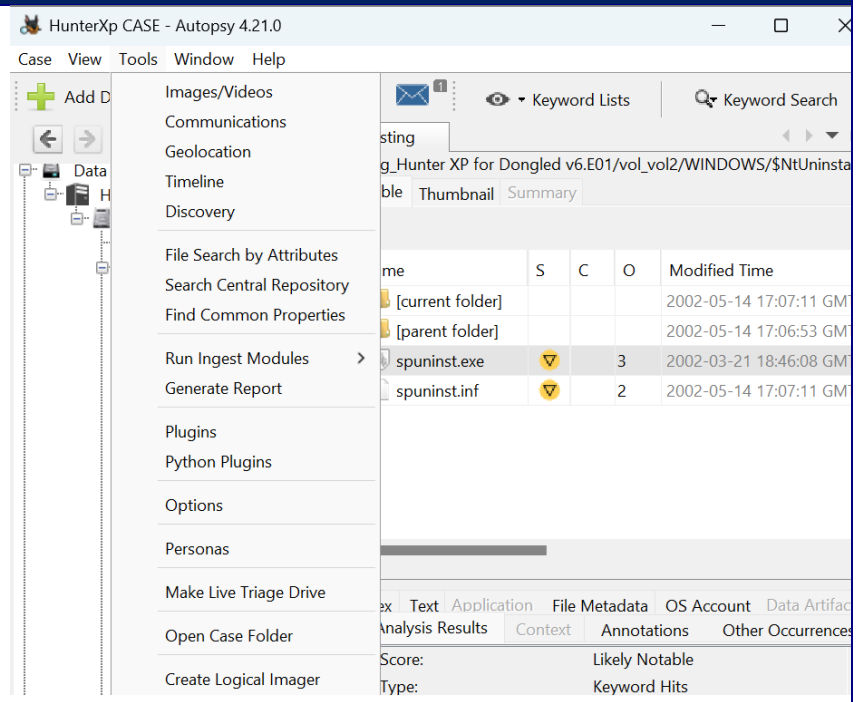
Action	Done?	Date	Time	Notes
				• After making txt file, opened the txt file and searched for product name to get information about operating system. ---------- winver v.20200525 (Software) Get Windows version & build info ProductName Microsoft Windows XP BuildLab 2600.xpclnt_qfe.010827-1803 RegisteredOrganization PC User Company RegisteredOwner PC User InstallDate 2002-02-28 22:02:39Z ---------- wow64 v.20200515 (Software) Gets contents of WOW64\x86 key WOW64 **Step2:** • Now, I have verified the operating system of the image file in **autopsy** by following the given steps: • Selected **Data Artifacts**. • Found **operating system.**

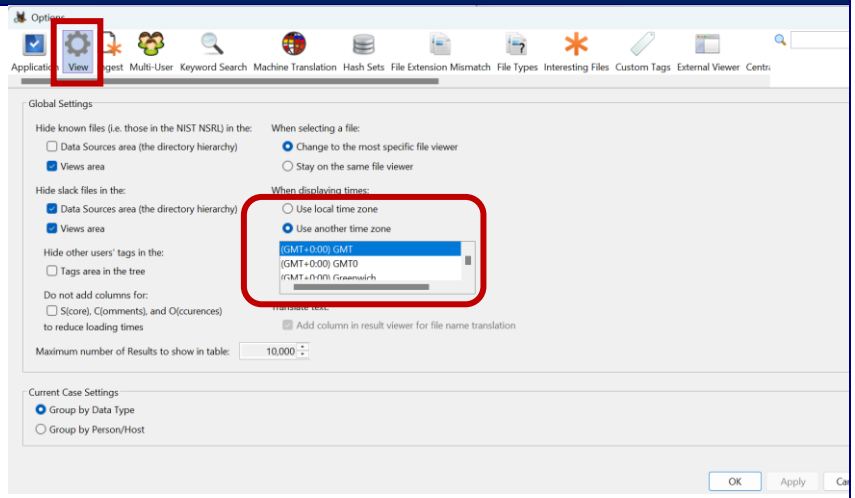
Action	Done?	Date	Time	Notes
				• Then selected **Hunter XP for Dongled v6.E01** After clicking on **Hunter XP for Dongled v6.E01 ,** I got information about the operating system of given evidence file.  Now, the operating system is verified as **Microsoft Windows XP**. **Step3:** • The loaded case in autopsy **OS account** was **accessed**.

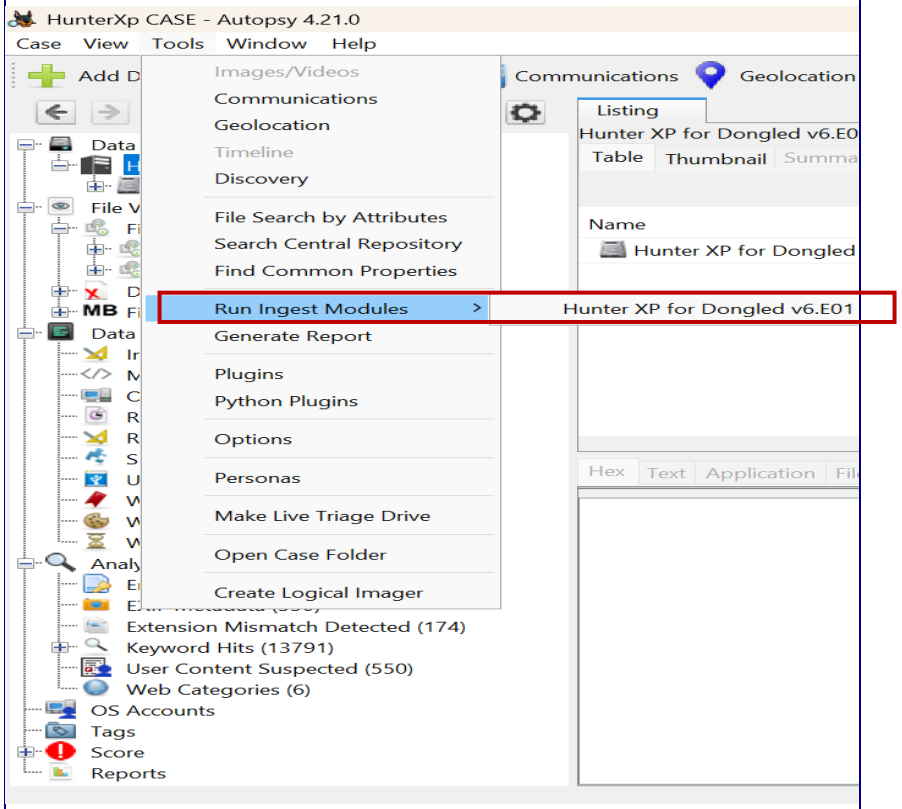
Action	Done?	Date	Time	Notes
				 • In this case I followed the same path as I followed to extract software and extracted **SAM** file. • Then the extracted **SAM** file is loaded in **AccessData Registary Viewer.** • I opened registry viewer as administrator. • Choose file option to load **SAM** in this application and the file was chosen from drop down Menu from the path where I kept **SAM** file. • After Loading the case I followed the path

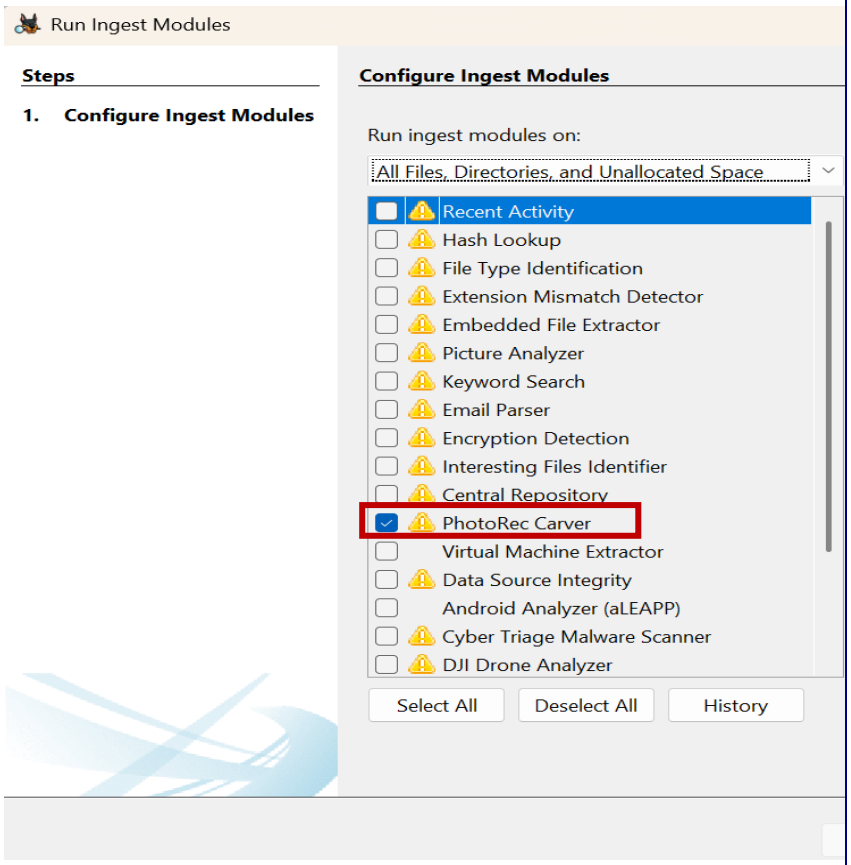
Action	Done?	Date	Time	Notes
				Path: SAM/Domains/Account/Users/000003EC  In both cases the logon count of Bob Hunter is same that is 5.
Time Zone Adjusted? Report Time Zone used for Analysis.	yes	19/12/2024	01/35 pm	**Step1:** The **time zone** is adjusted while loading the case into **Autopsy**.

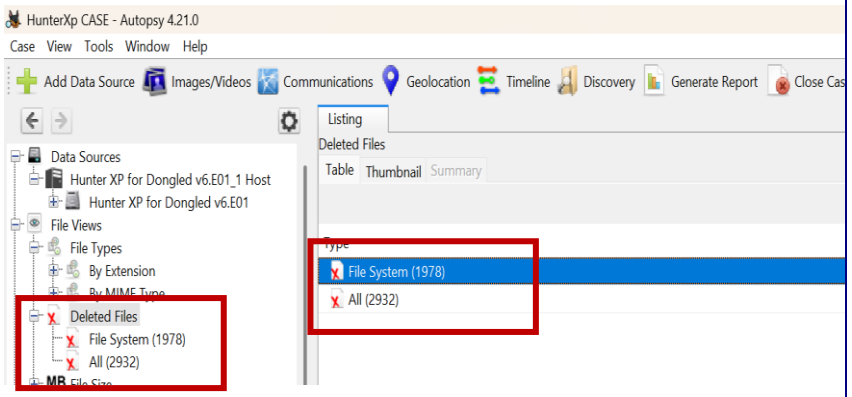
Action	Done?	Date	Time	Notes
				 **Step2:** Time zones can also be adjusted within the **autopsy**, by following the steps below. • Click on **tools** • Selected **options** • Clicked on **View** • Use another Time Zone.

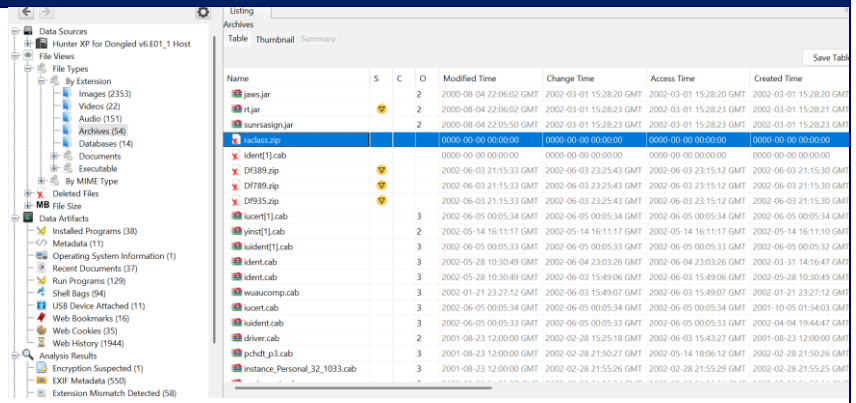
Action	Done?	Date	Time	Notes
				

Action	Done?	Date	Time	Notes
				
Recover lost folders (NTFS, FAT16&32).	yes	20/12/2024	02:30 PM	**Step1:**

Action	Done?	Date	Time	Notes
				• First of all, open **tools** in **Autopsy**.  **<u>Step2:</u>** • And selected **run ingest module** for Hunter XP for Dongled v6.E01.

Action	Done?	Date	Time	Notes
				Step3: • Configured **photoRec carver** to **recover lost folders**. 

Action	Done?	Date	Time	Notes
				Step4: • After running **photoRec Carver** we recovered lost folders as deleted files. We got deleted files containing 1978 files and all files containing 2932 files. 
Mount archives; zip, thumbs.db, etc.	yes	20/12/2024	04:00 PM	**Step1:** • For Mount Archives we follow the Path: Files Views/ FilesTypes / By Extension After following these paths I got the archives folder.

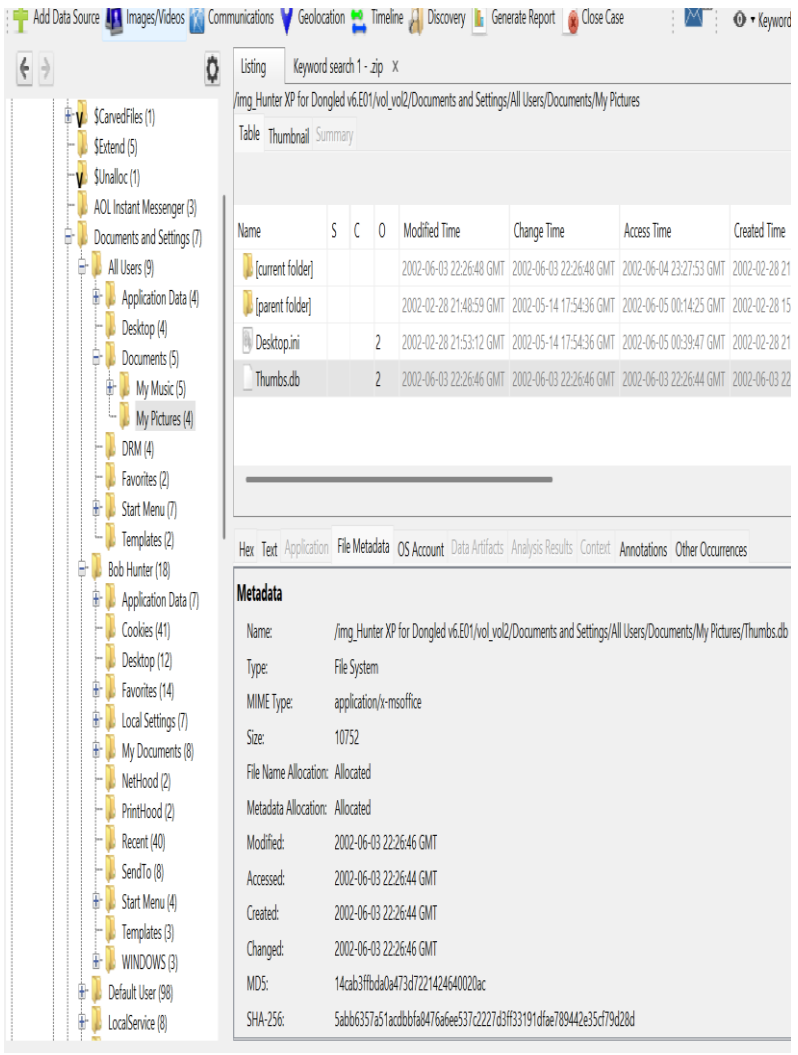
Action	Done?	Date	Time	Notes
				

Step 2:

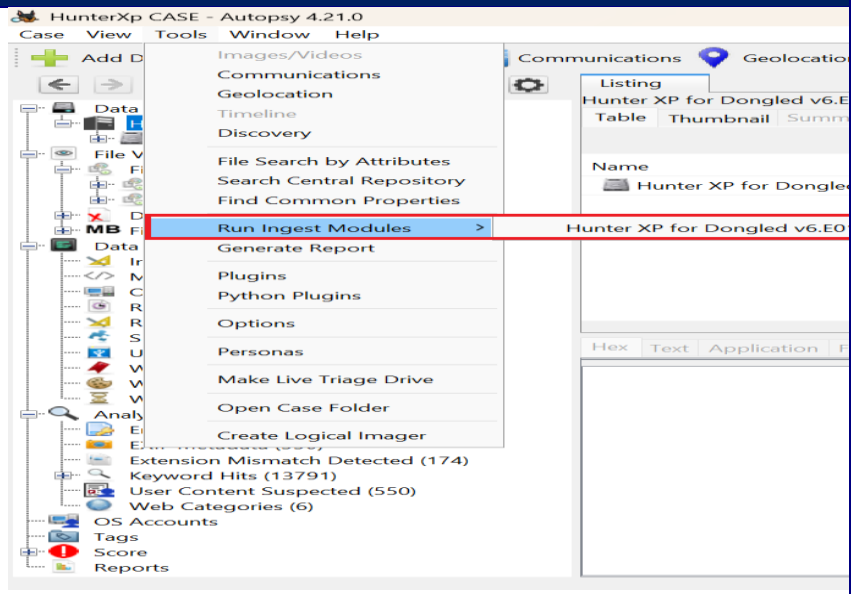
- I found zip files in different path that is.
  - /img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temp/~rnsetup/raclass.zip
  - /img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df389.zip

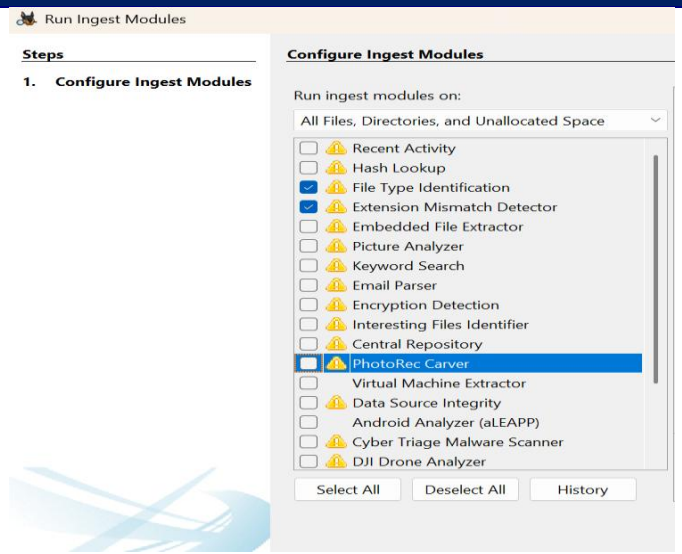
Action	Done?	Date	Time	Notes
				➢ /img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df789.zip ➢ /img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df935.zip ➢ /img_Hunter XP for Dongled v6.E01/vol_vol2/Program Files/America Online 7.0/download/CURREX~1.zip ➢ /img_Hunter XP for Dongled v6.E01/vol_vol2/Program Files/America Online 7.0/download/hourz11.zip

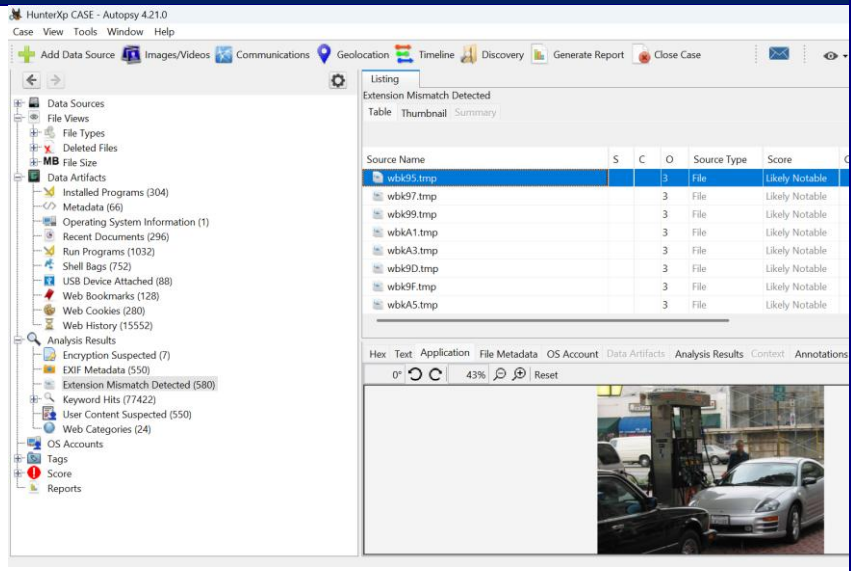
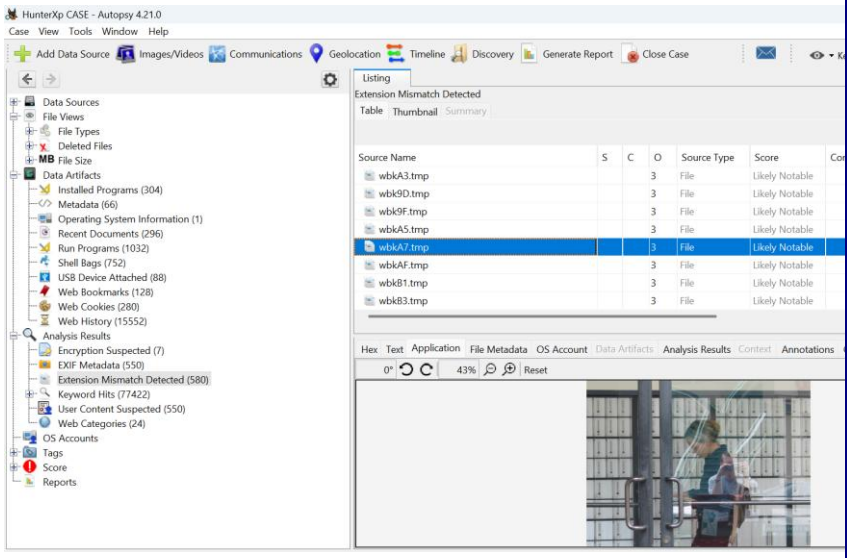
Action	Done?	Date	Time	Notes
				➢ /img_Hunter XP for Dongled v6.E01/vol_vol2/Program Files/Windows Media Player/npdrmv2.zip ➢ /img_Hunter XP for Dongled v6.E01/vol_vol2/Program Files/Windows Media Player/npds.zip **Step 3:** To get thumbs.db i follow the path; 1. /img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/All Users/Documents/My Pictures/Thumbs.db

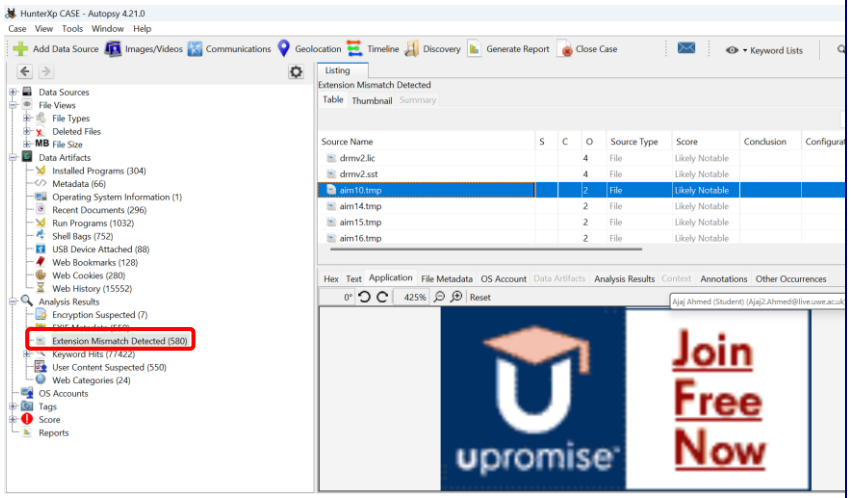
Action	Done?	Date	Time	Notes
				

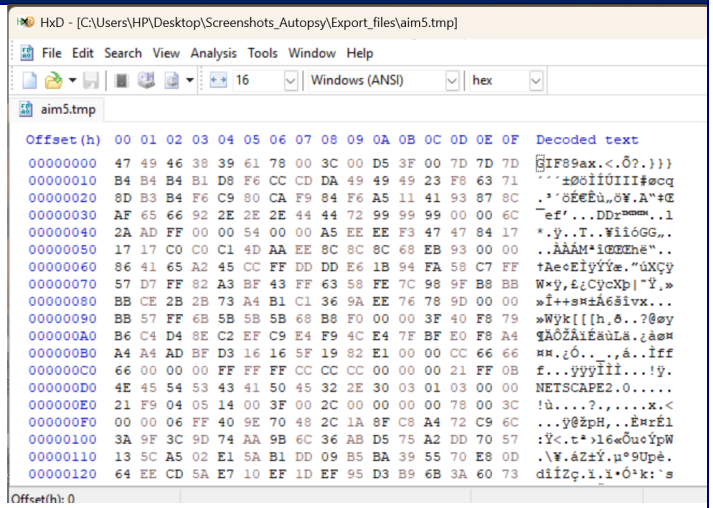
Action	Done?	Date	Time	Notes
				2. /img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Application Data/Microsoft/CD Burning/Hunter Pics/Christina Detsiwt/Thumbs.db 3. We also find thumbs.db on exploring the path file views/ file types/ By Extension/DataBases.
File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation)	yes	20/12/2024	05:00 PM	To Investigate **file signature** and **file mismatch** I followed these steps: **Step1:** • Firstly, I opened **tools** and ran the **ingest module** for the **Hunter XP for Dongled v6.E01**.

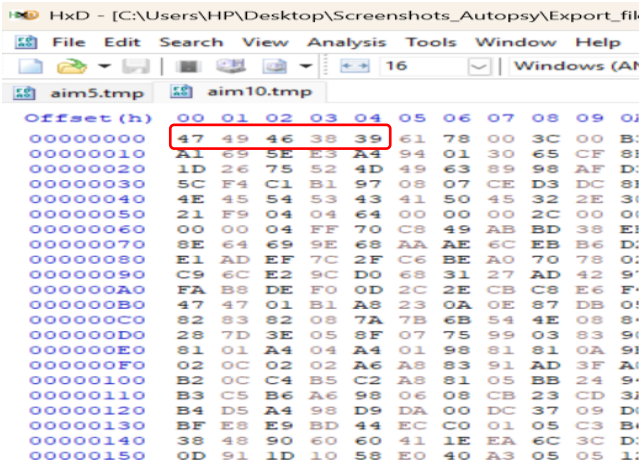
Action	Done?	Date	Time	Notes
				 • The after that I have configured the **File type identification** and **Extension mismatch Detector modules**. • By running the ingest module by clicking on tools in the autopsy.

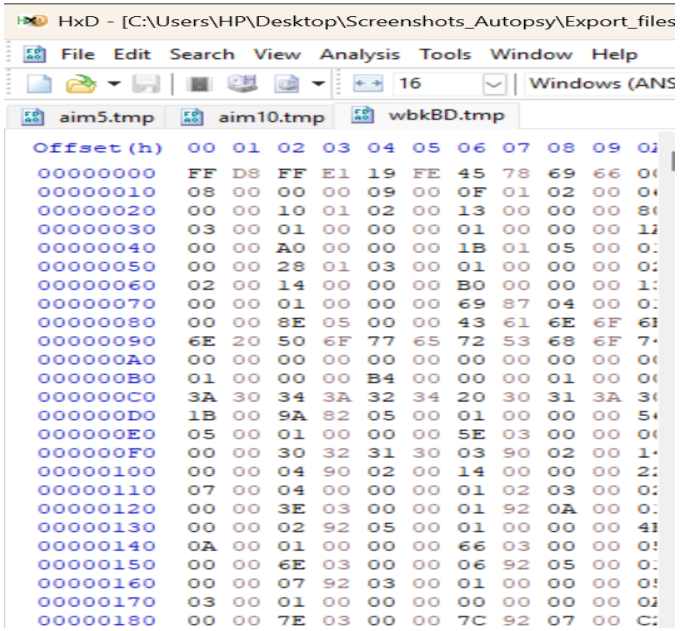
Action	Done?	Date	Time	Notes
				 • After running this module, I found an **Extension mismatch Detected file** in the **Analysis result**.

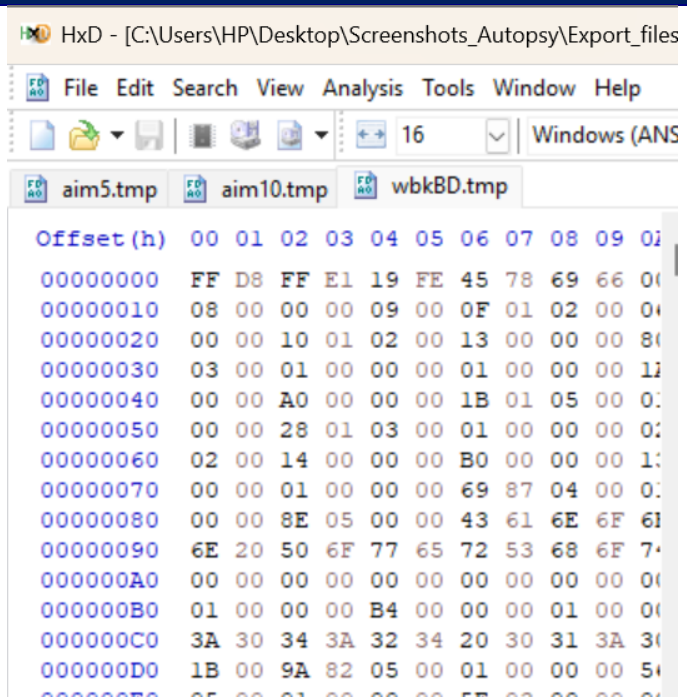
Action	Done?	Date	Time	Notes
				 

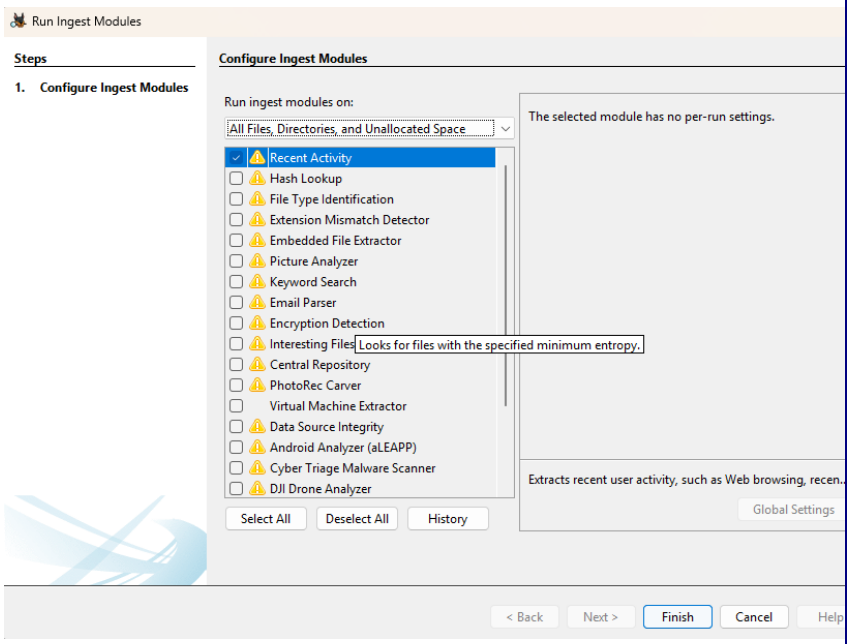
Action	Done?	Date	Time	Notes
				• After performing all these steps, I exported some files to verify whether the extension of these files is correct or not • Now I opened the HXD application for analysis of the hash values of these files, whether these values are correct or not according to the file types. • Now at the top of the righthand side there is the file I have clicked on the file and choose the open file to add the file I have exported for hash values analysis. 

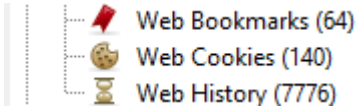
Action	Done?	Date	Time	Notes
				 • At first, I added aim5.tmp for the HEX values analysis I got. In this file, I got hash values 47 49 46 38 39 61. The value I got is not the hash value of the .tmp file the given hash value is for .gif files. So, it seems that there is a mismatch of file extensions. • For aim10.tmp I followed the same step and I got the same result for aim10.tmp file. It is also a .gif file. So, both aim5.tmp and aim10.tmp is .gif file.

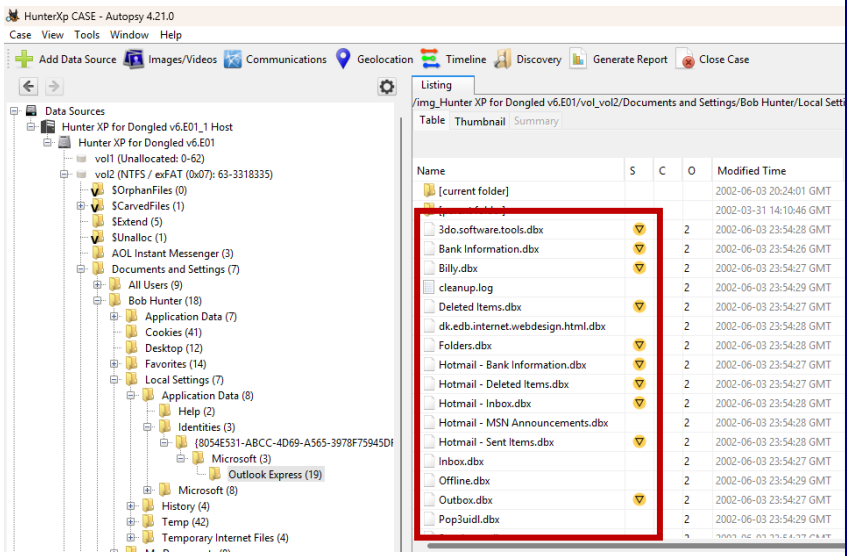
Action	Done?	Date	Time	Notes
				 • Again, performing the same process for verification of wbkBD.tmp and wbkC1.tmp for file extension verification I got there is also file extension mismatch. The hash value I got for these two files is FF D8 FF E1 1B FE. The hash value I got from HXD is the value of the JPEG file. So, it seems that there is a tempering with the files.

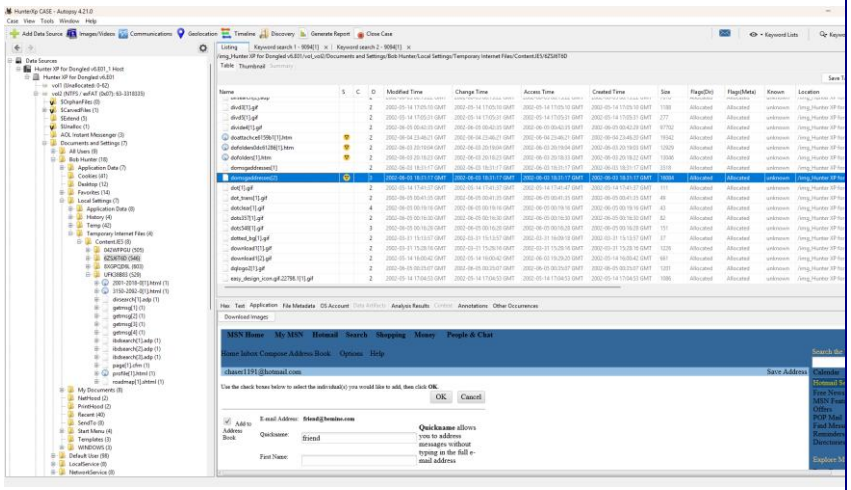
Action	Done?	Date	Time	Notes
				

Action	Done?	Date	Time	Notes
				
Internet History, favourites, etc. Other browsers?	YES	20/12/2024	05:30	**<u>Step1:</u>** I ran the ingest module recent folders to find internet files and followed the following steps. ➢ Clicked on the **tools**.

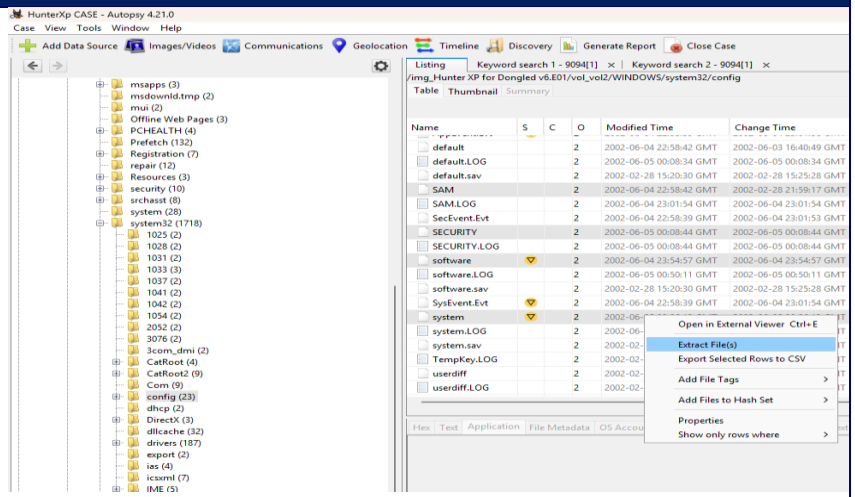
Action	Done?	Date	Time	Notes
				➢ Clicked **run ingest module**. ➢ Select **Hunter XP for Dongled v6.E01**. ➢ And selected **Recent Activities**.  **Step2:** After running this module, I followed the steps given below.

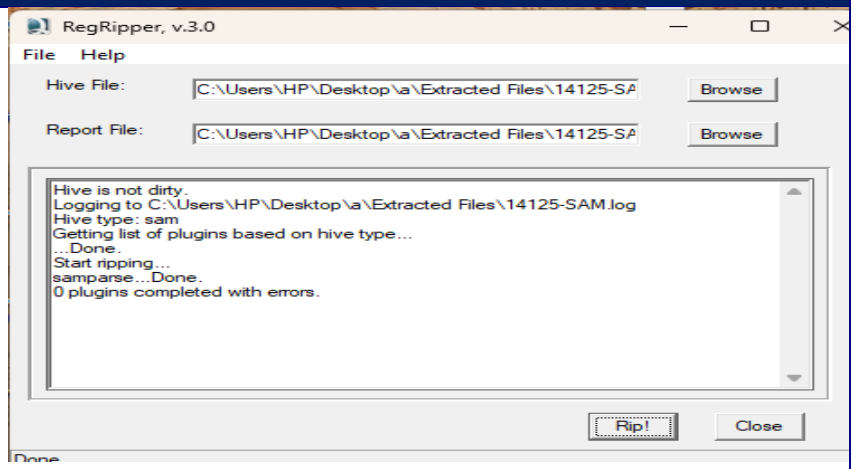
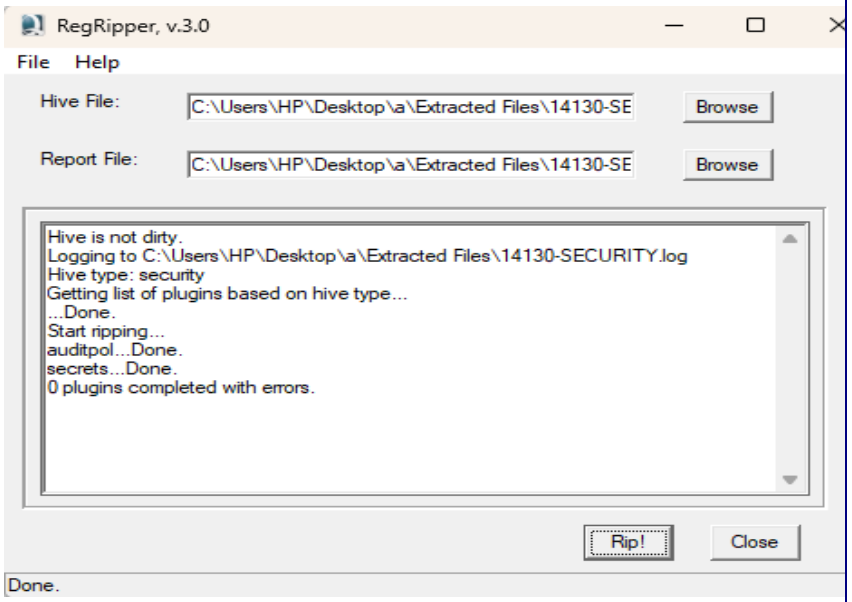
Action	Done?	Date	Time	Notes
				a. Clicked on the data artifacts.  b. In data artifacts I saw three artifacts of a. Web bookmarks. b. Web Cookies c. Web History After investigating the installed programs. I observed that only the Internet Explorer browser was viewed.
Emails, local and web-based.	Yes	20/12/2024	06:15 PM	**Step1:** To find Local emails I have followed the path: /img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Application

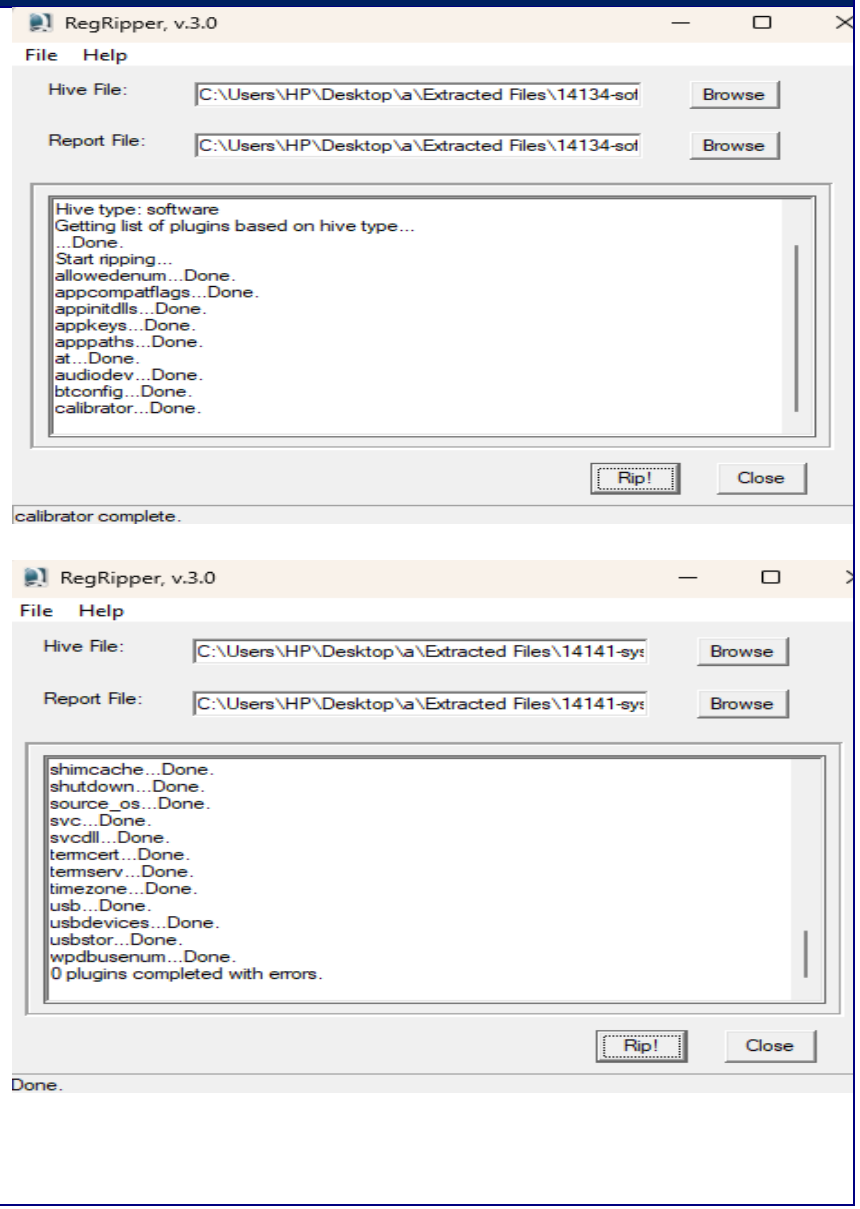
Action	Done?	Date	Time	Notes
				Data/Identities/{8054E531-ABCC-4D69-A565-3978F75945DF}/Microsoft/Outlook Express  **Step2:** To find web-based emails I have followed this path. :/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5

Action	Done?	Date	Time	Notes
				After following this path, I got  Following this path, I learned that many files are used for email purposes.
Retrieve operating system information, accounts information, software, time zone information, etc.).	Yes	20/12/2024	07:15 PM	To retrieve operating system information, account system information, software and time zone information. I have done different task and used different tools like **Autopsy, RegRipper.** I have extracted different types of files that contain

Action	Done?	Date	Time	Notes
				information about these artifacts. The files I have extracted are **SAM, Security, Software and System** **<u>Step1:</u>** To retrieve operating system information, account information, and software time zone information I have extracted SAM, Security, Software, and System files for Analysis. For this task, I have used Rgripper. For analysis and creating CSV and Txt files. c. For extraction of SAM, Security, Software, and System files I have followed the path given below.

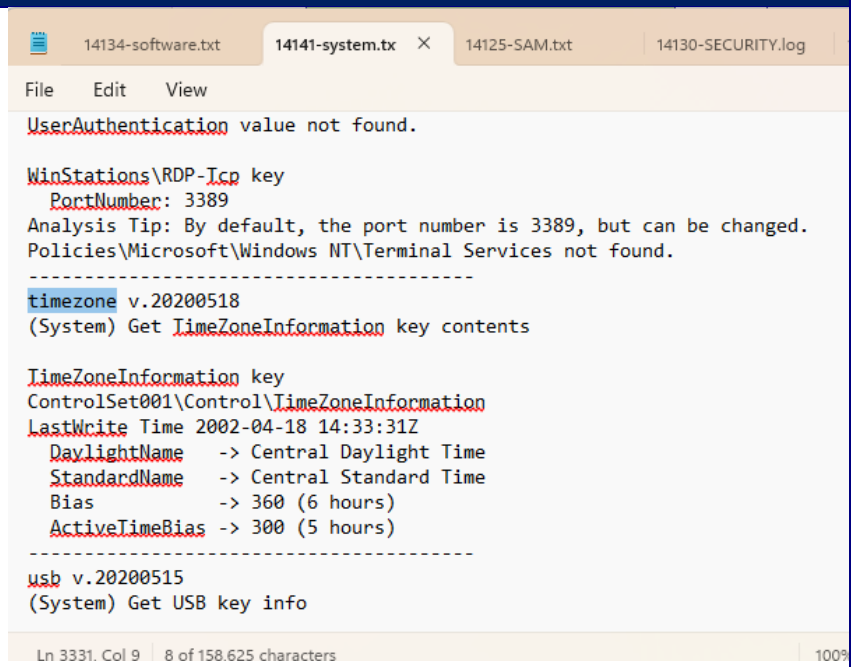
Action	Done?	Date	Time	Notes
				 d. After extracting these files, I have used these files. Now these extracted files are used to retrieve operating system information, account information, software, and time zone information using RegRipper.

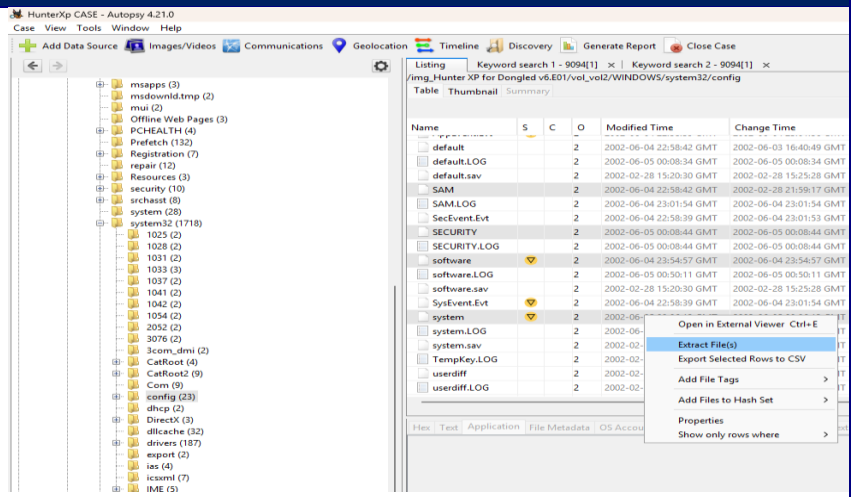
Action	Done?	Date	Time	Notes
				 

Action	Done?	Date	Time	Notes
				

Action	Done?	Date	Time	Notes
				After ripping these all files in the Reg ripper, I watched the .txt files to find Retrieve operating system information, account information, software, time zone information 1. Operating System information: ---------- winver v.20200525 (Software) Get Windows version & build info ProductName Microsoft Windows XP BuildLab 2600.xpclnt_qfe.010827-1803 RegisteredOrganization PC User Company RegisteredOwner PC User InstallDate 2002-02-28 22:02:39Z ---------- wow64 v.20200515 (Software) Gets contents of WOW64\x86 key 2. Accounts Information

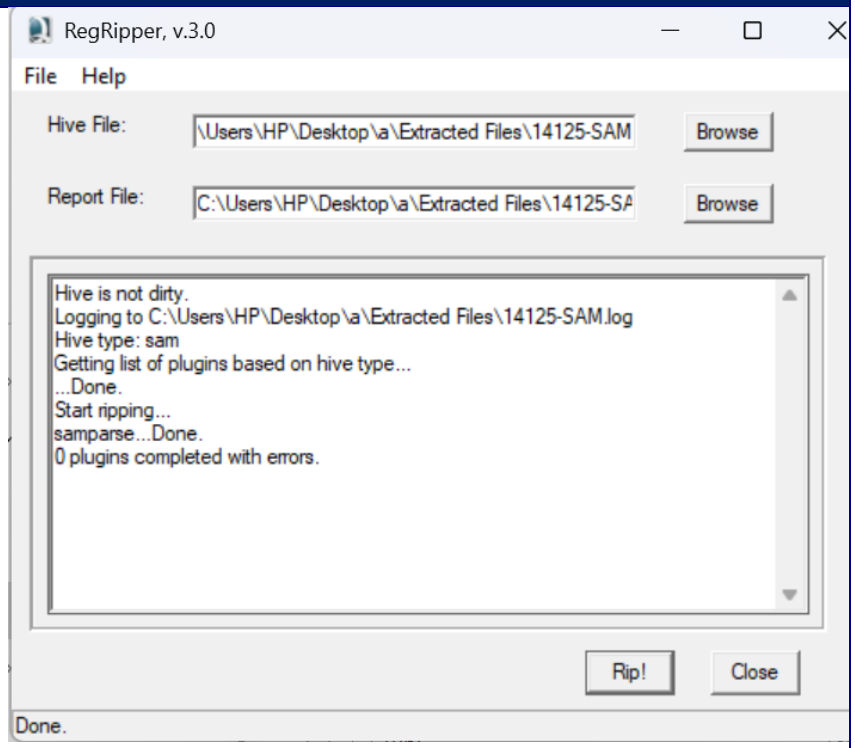
Action	Done?	Date	Time	Notes
				File Edit View --> Account Disabled --> Normal user account Username : Bob Hunter [1004] SID : S-1-5-21-1229272821-1580818891-854245398-1004 Full Name : User Comment : Account Type : Default Admin User Account Created : Thu Feb 28 22:22:17 2002 Z Name : Last Login Date : Tue Jun 4 23:01:54 2002 Z Pwd Reset Date : Thu Feb 28 22:22:17 2002 Z Pwd Fail Date : Never Login Count : 37 --> Password does not expire --> Password not required --> Normal user account 3. Software ---------- winver v.20200525 (Software) Get Windows version & build info ProductName Microsoft Windows XP BuildLab 2600.xpclnt_qfe.010827-1803 RegisteredOrganization PC User Company RegisteredOwner PC User InstallDate 2002-02-28 22:02:39Z ---------- 4. Timezone

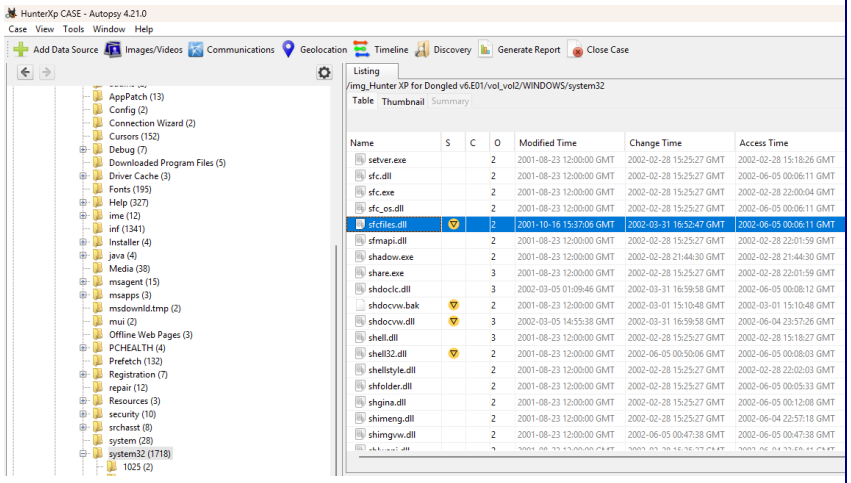
Action	Done?	Date	Time	Notes
				
Timeline analysis- Note date of last activity on the computer. System profiling.	Yes	20/04/2024	08:00 PM	**Step1:** for timeline analysis, I have extracted SAM from the path: Path: \img_Hunter XP forDongledv6.E01/vol_vol2/WINDOWS/system32/config

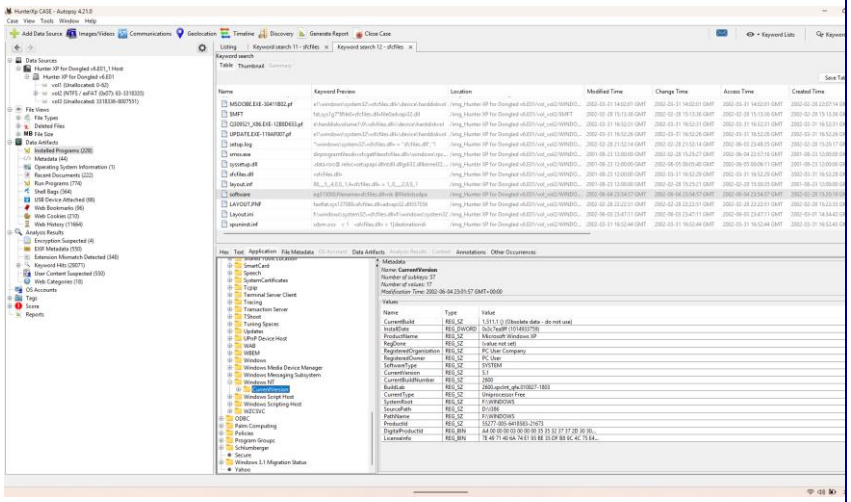
Action	Done?	Date	Time	Notes
				

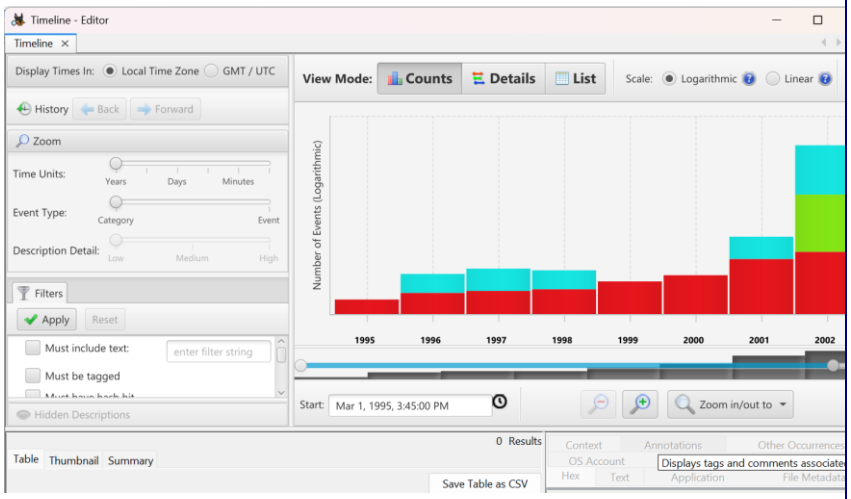
Step2:

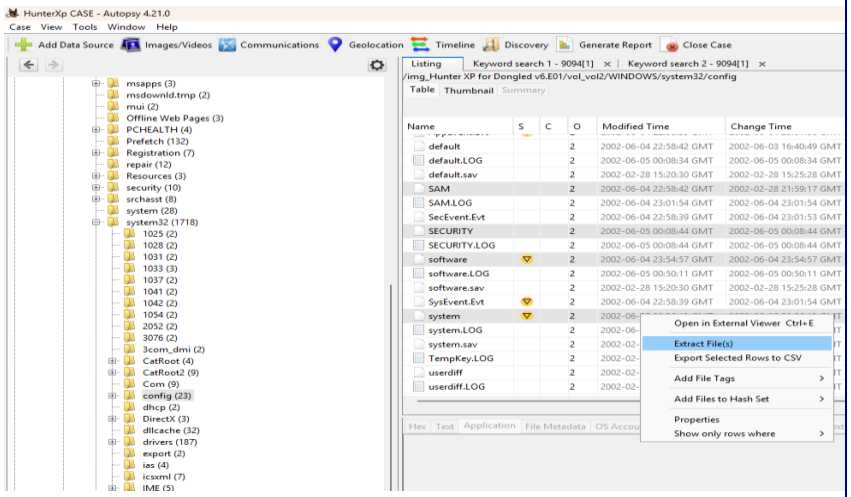
- After extracting **SAM** I ripped SAM in **Reg Ripper** and made **SAM.txt** file.

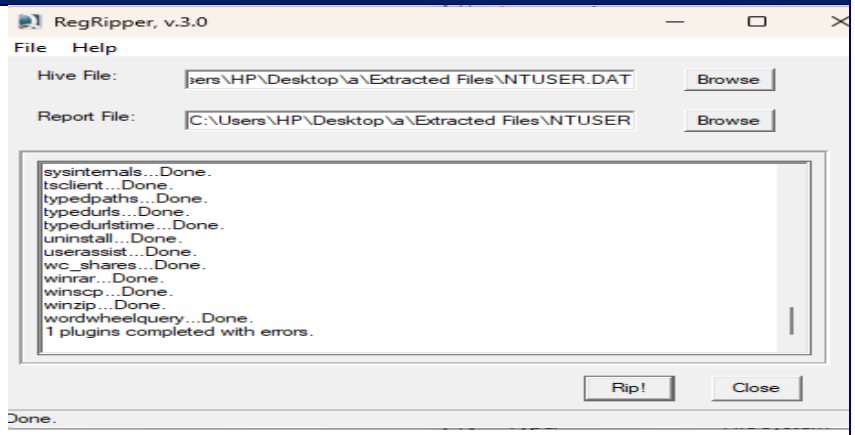
Action	Done?	Date	Time	Notes
				 • From the **SAM.txt** file I got the **last login date** of **Bob Hunter**. Last Login Date : Tue Jun 4 23:01:54 2002 Z Pwd Reset Date : Thu Feb 28 22:22:17 2002 Z Pwd Fail Date : Never Login Count : 37

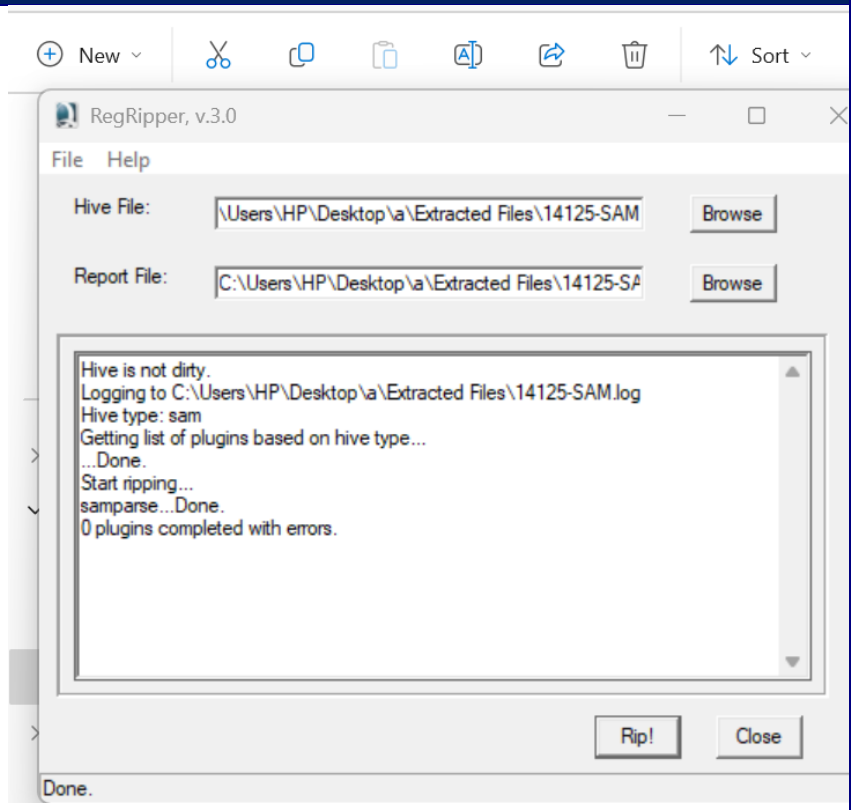
Action	Done?	Date	Time	Notes
				Step3: To find **system profiling** I followed the path **Path**: /img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32 In system32 we found a file name sfcfiles.dll. This sfcfiles.dll contains information about the system.  For extraction of **NUSTER.dat**, I have followed the path. Path:

Action	Done?	Date	Time	Notes
				/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter  **Step4:** for timeline analysis **plaso** ingest module is run. Steps used for running this Module are give below. • Click on **Tools** in the toolbar. • Choose **Run ingest modules.** • Select **Hunter XP for Dongled v6.E01.**

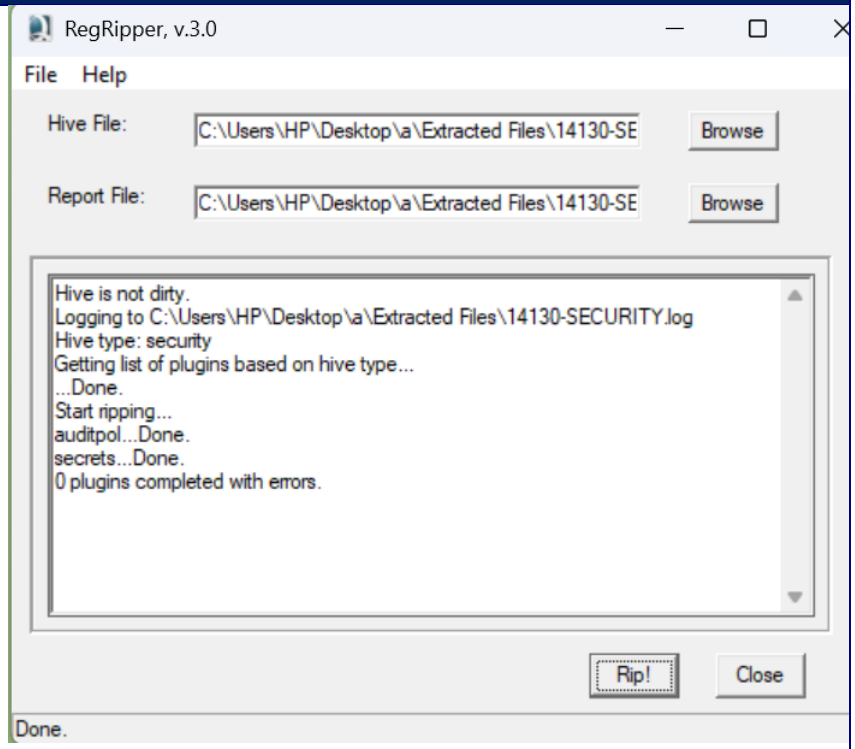
Action	Done?	Date	Time	Notes
				• Picked **Plaso**. • After running **plaso,** clicked on **Timeline** and I got timeline detail. 
Registry analysis and Registry protected area	Yes	21/12/2024	12:00 PM	**<u>Step1:</u>** For registry analysis, I have extracted **SAM**, System, Software, and security. I have also extracted the **NUSTER.dat** file for analysis of information such as: • Recently accessed files • Installed software

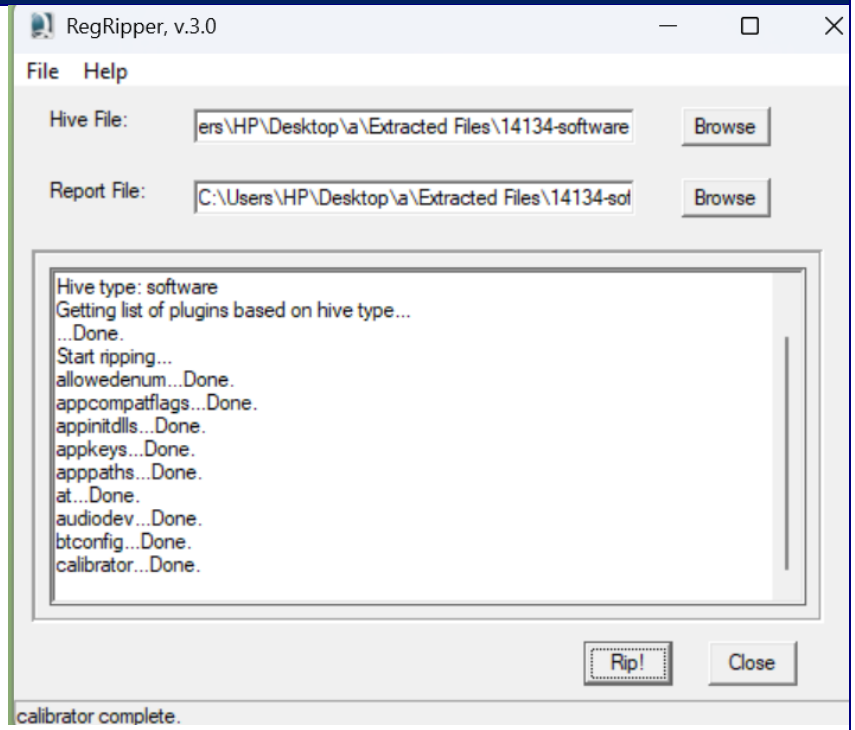
Action	Done?	Date	Time	Notes
				• User preferences • Typed URLs (in Internet Explorer)  **<u>Step2:</u>** After extraction of these files, I made .**txt** files of all files using **Reg Ripper** as I have operated for **Timeline analysis**.

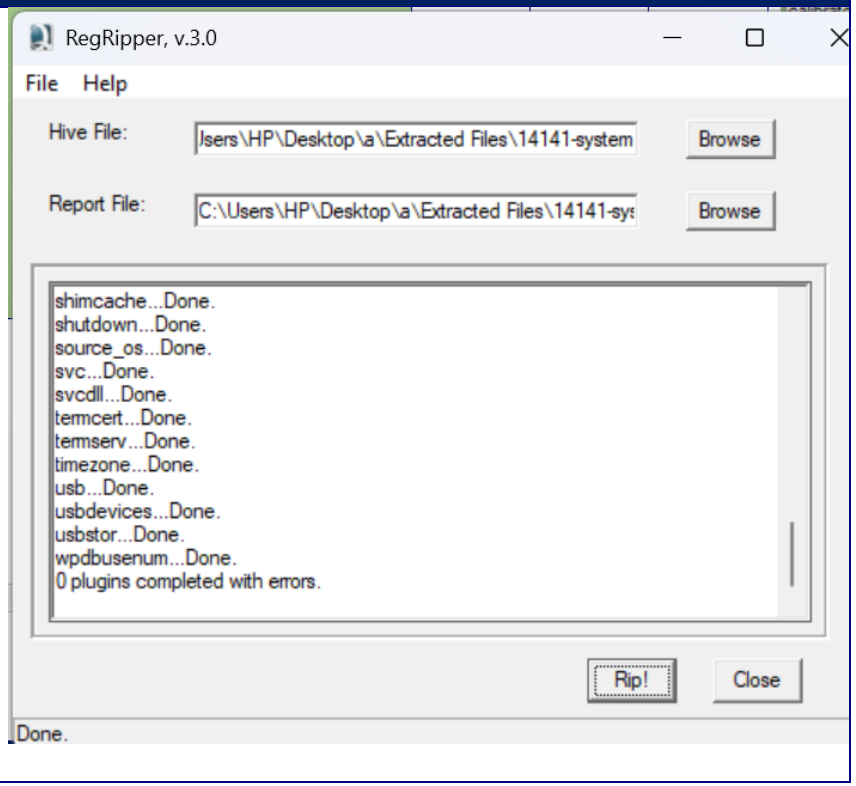
Action	Done?	Date	Time	Notes
				 After **ripping** these all files from **regripper** I have analyzed SAM.txt, System.txt, Software.txt., Security.txt, and Nuster.dat.txt I found the artifacts such as: a. **SAM**.: SAM.txt files contain user details and password hashes.

Action	Done?	Date	Time	Notes
				

Action	Done?	Date	Time	Notes
				--> Normal user account Username : Bob Hunter [1004] SID : S-1-5-21-1229272821-1580818891-854245398-1004 Full Name : User Comment : Account Type : Default Admin User Account Created : Thu Feb 28 22:22:17 2002 Z Name : Last Login Date : Tue Jun 4 23:01:54 2002 Z Pwd Reset Date : Thu Feb 28 22:22:17 2002 Z Pwd Fail Date : Never Login Count : 37 --> Password does not expire --> Password not required --> Normal user account ------------------------ b. **Security**: **Security** is responsible for maintaining the **security** policies of the device.

Action	Done?	Date	Time	Notes
				 c. **Software**: All the installed programs, software settings, and program of versions are recorded by the **Software**.

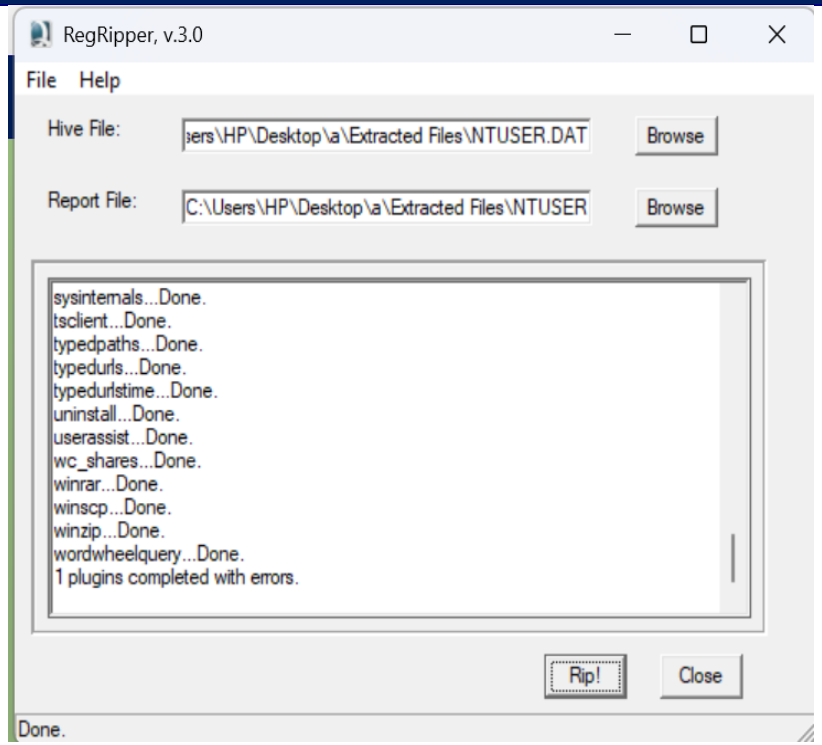
Action	Done?	Date	Time	Notes
				 d. **System**: All information about the hardware and configuration of the device is managed by the system.

Action	Done?	Date	Time	Notes
				

Action	Done?	Date	Time	Notes
				`` ---------- winver v.20200525 (Software) Get Windows version & build info ProductName Microsoft Windows XP BuildLab 2600.xpclnt_qfe.010827- RegisteredOrganization PC User Company RegisteredOwner PC User InstallDate 2002-02-28 22:02:39Z ---------- wow64 v.20200515 (Software) Gets contents of WOW64\x86 key ```

e. NUSTER.dat:

It contains user-specific settings and preferences, including desktop and application configurations. And contains information about installed software and URLs.

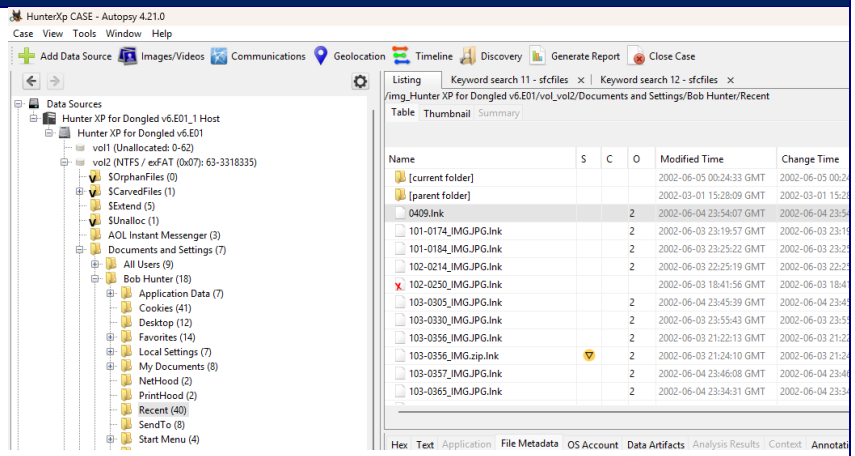
Action	Done?	Date	Time	Notes
				


```
Nation Information Check
Control_Panel\International\Geo
LastWrite time: 2002-02-28 22:22:29Z

The Region value is : 244
The Country Is: United States
For more information please visit the link below:
https://msdn.microsoft.com/en-us/library/aa723531.aspx

---------------------------------------
oisc v.20091125
(NTUSER.DAT) Gets contents of user's Office Internet Server Cache
```

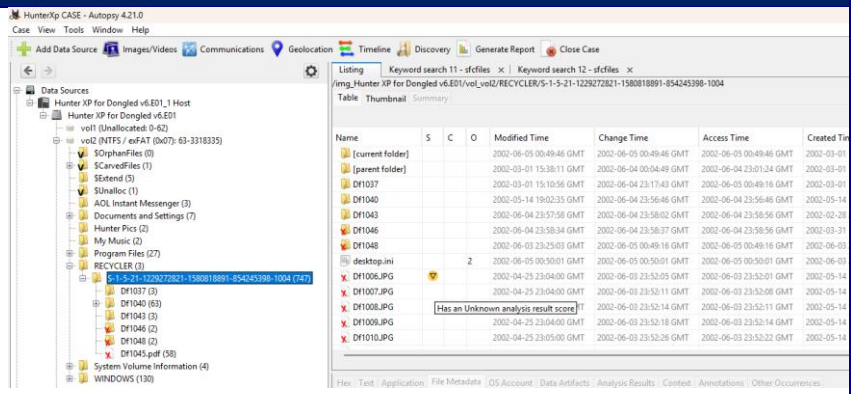
Action	Done?	Date	Time	Notes
Link files and Recycle Bin	YES	21/12/2024	12:25 PM	**Step1:** To find link filesi followed the path; Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Recent I followed the given path for the analysis of linked files. ➢ After following this path, I found that there were **40 link** files with extension .**lnk** which was created by **BOB HUNTER**.

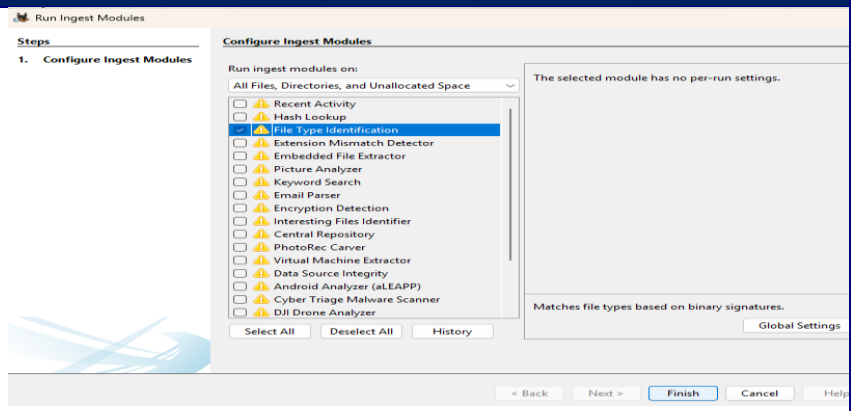
Action	Done?	Date	Time	Notes
				

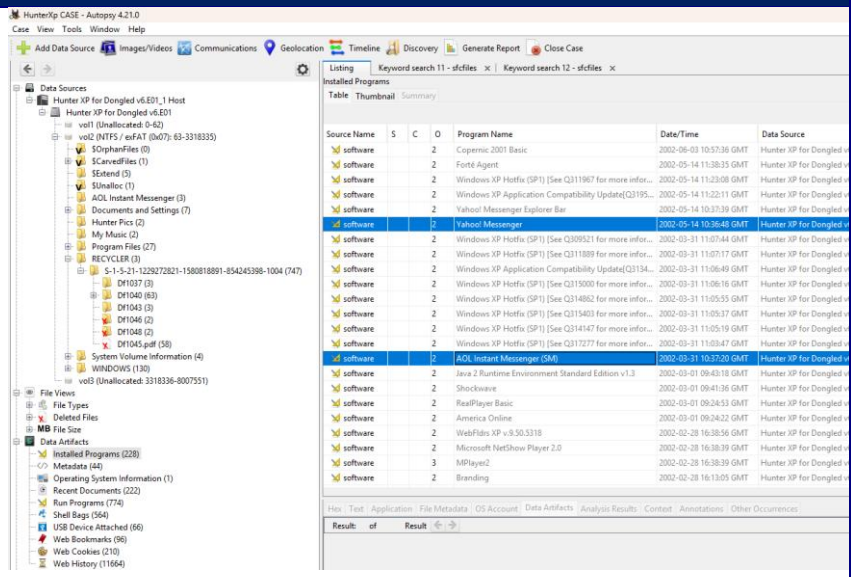
Step2:

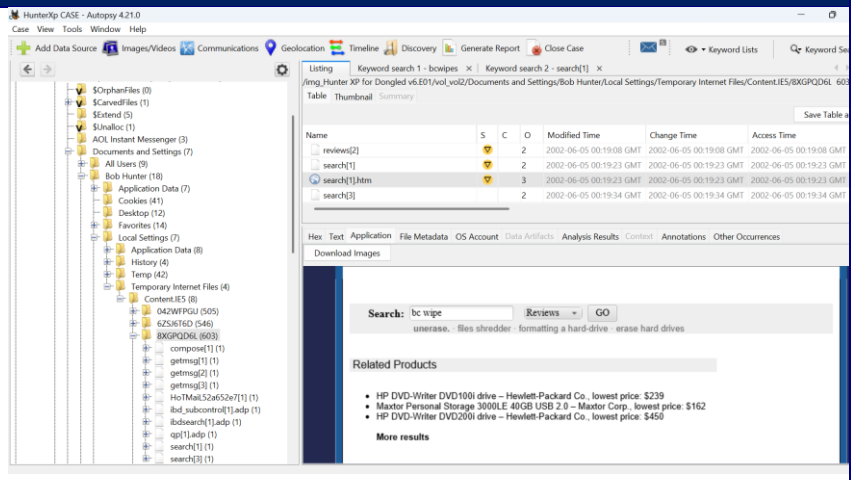
After analysis of the **link files**, I proceed with the analysis of the **Recycle Bin**. To analyze the **recycle** bin I followed the path;

Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004

Action	Done?	Date	Time	Notes
				
Instant Messaging clients	YES	21/12/2024	12:40 PM	**Step1:** To find instant messaging clients I ran the ingest module and followed the steps: ➢ Clicked on **tools** ➢ Chose **Run Ingest Module** ➢ Selected **Hunter XP for Dongled v6.E01**. ➢ Picked **file type identification**.

Action	Done?	Date	Time	Notes
				 **Step2:** After finishing this process. ➢ I clicked on data artifacts and found installed Programs. ➢ I clicked on installed programs and found that there were only two instant messaging apps used. **a. Yahoo messenger** **b. AOL Instant Messenger**

Action	Done?	Date	Time	Notes
				
Clean-up/Wiping utilities. Check log files. Anything used?	YES	21/12/2024	01:00 PM	Clean-up and wiping activities are done in the given evidence file. I found the clean-up and wiping utilities artifacts are found in website search, .exe file and .pf file was executed. **Step1:**

Action	Done?	Date	Time	Notes
				

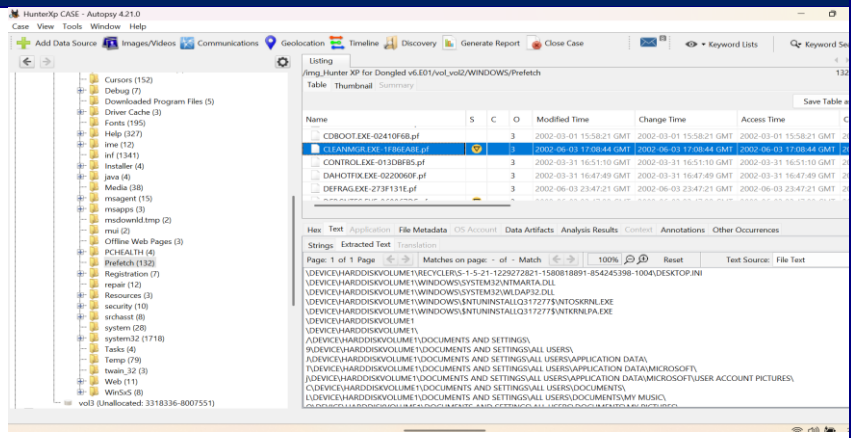
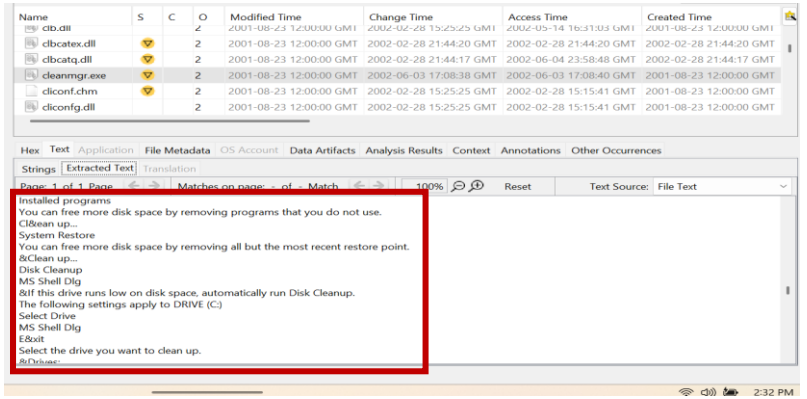
Step2:

I found that cleanmgr.exe file is in the system32 folder and traces of this file execution is also stored in the prefetch folder cleanmgr.exe….pf.

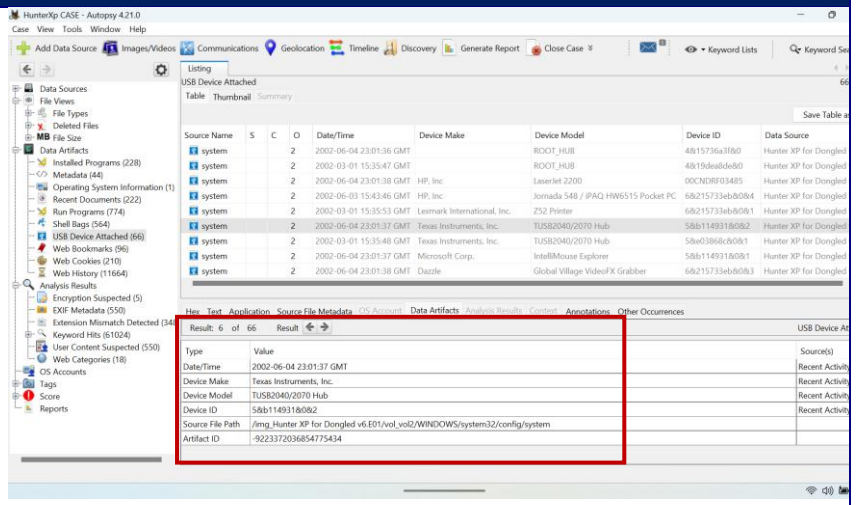
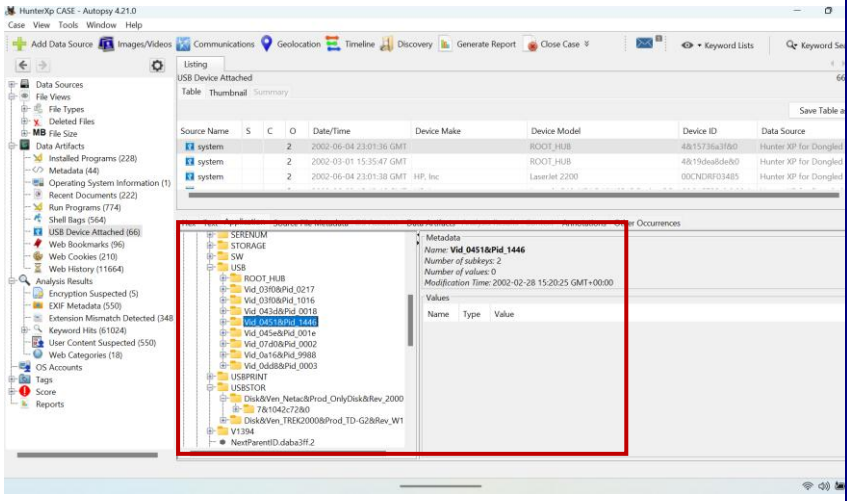
Path browsed to find prefetch file is given below:

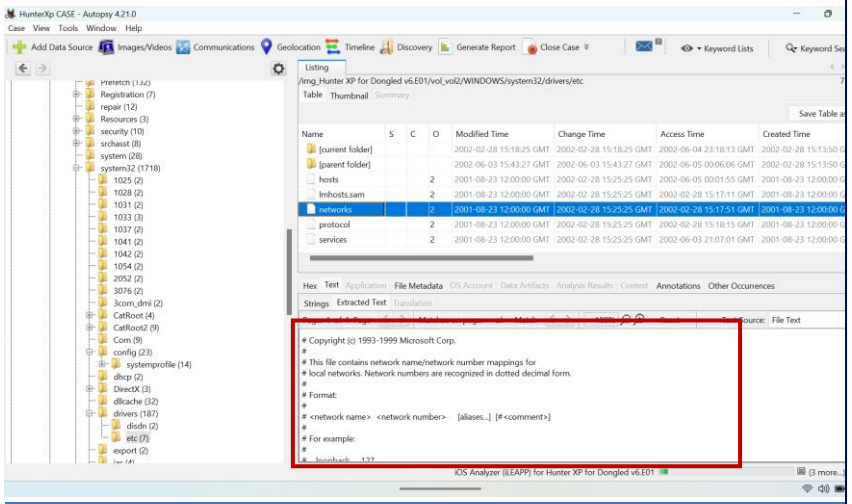
Path:

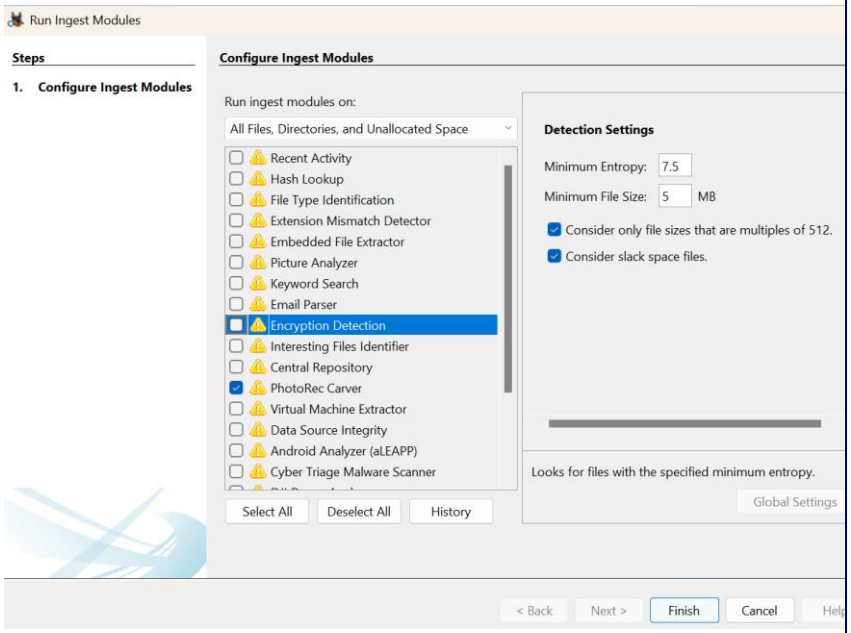
/img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/Prefetch/CLEANMGR.EXE-1F86EA8E.pf

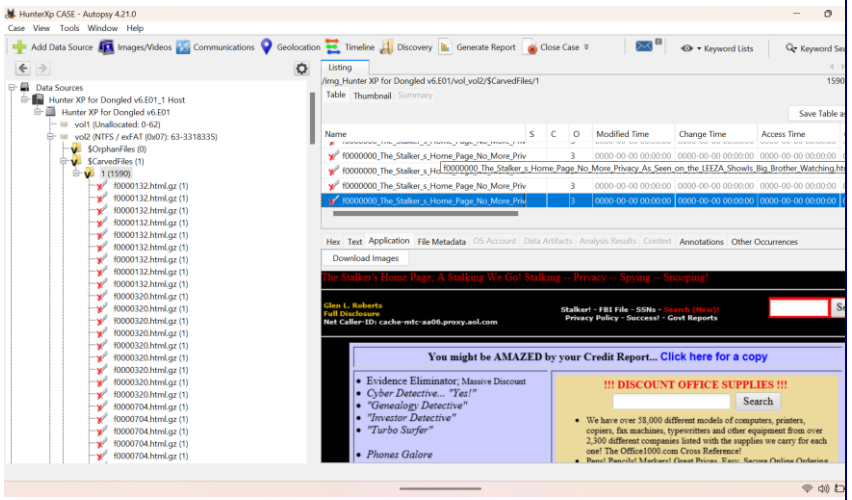
Action	Done?	Date	Time	Notes
				 To find the cleanmgr.exe file I browsed the path: /img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32 

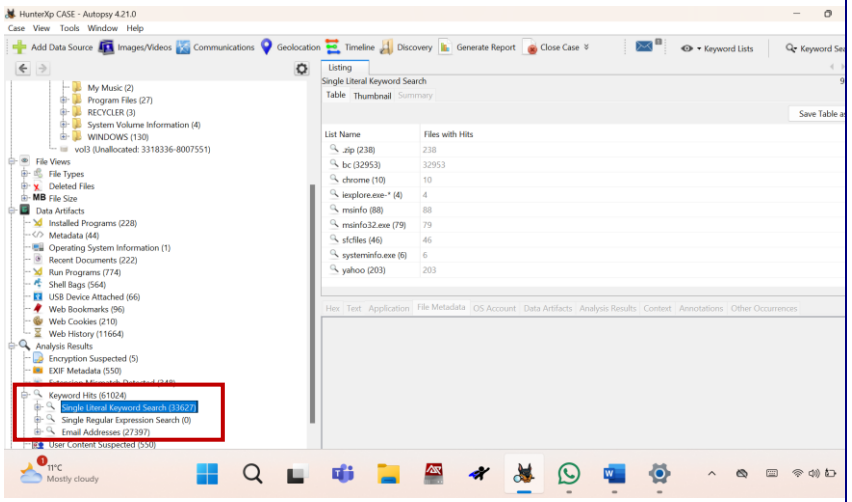
Action	Done?	Date	Time	Notes
External drives; Network connections	Yes	21/12/2024	03:00 PM	To find whether external drives were used in **Hunter XP for Dongled v6.E01**, follow these steps: 1. Open **Hunter XP** and load the **Dongled v6.E01** image. 2. Navigate to **System Artifacts** > **USB Device Attached** 3. Also Analyzed the registry entries under **SYSTEM** > **CurrentControlSet** > **Enum** > **USBSTOR**. **Step2:** I followed the following path to find **External drive artifacts** is; Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/config

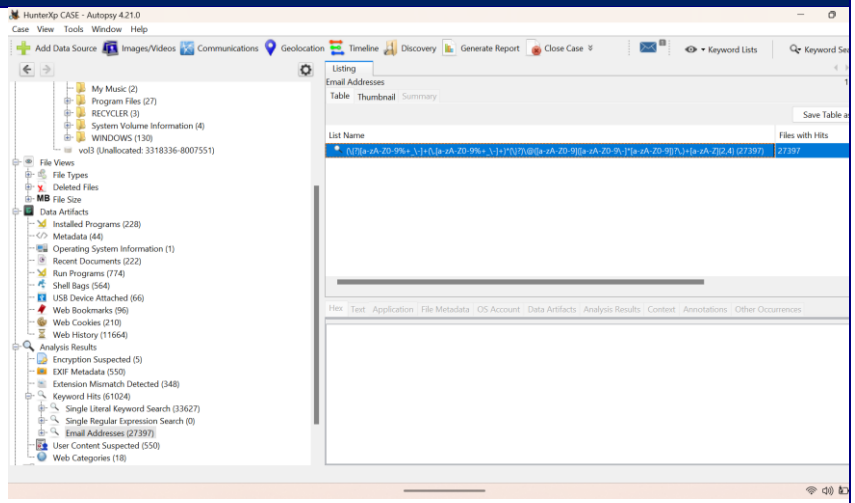
Action	Done?	Date	Time	Notes
				  **For Network Connection:**

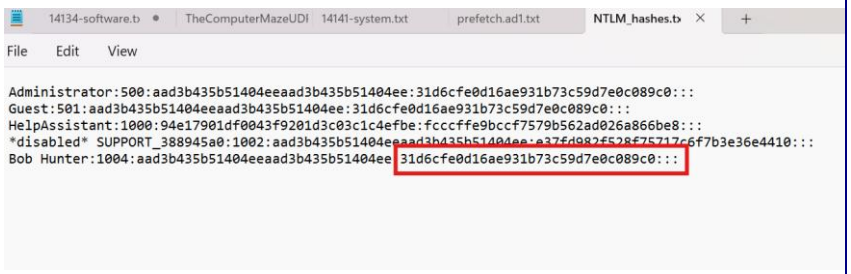
Action	Done?	Date	Time	Notes
				To find the network connection used in **Hunter XP for Dongled v6.E01,** I have followed the path given below; Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/drivers/etc  after analyzing the files etc I found that the user used **TCP/IP** protocol and his file contains the Internet protocols as defined by RFC 1700.

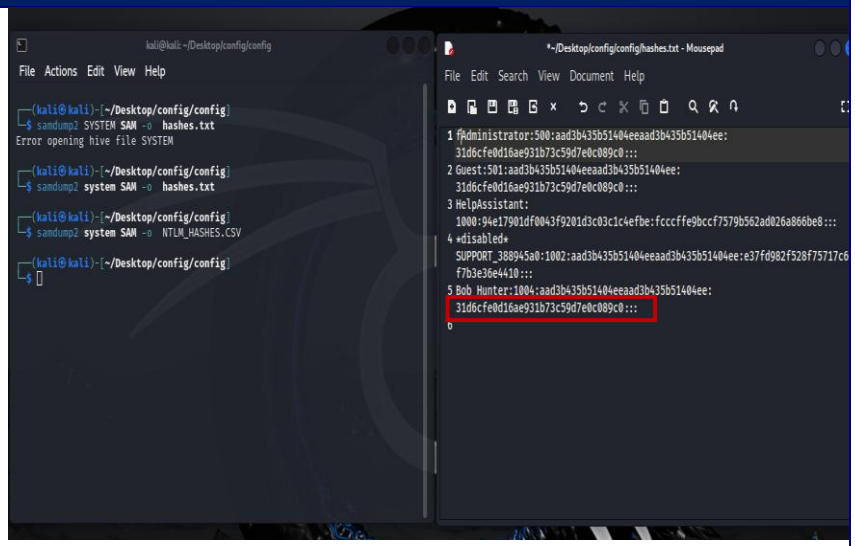
Action	Done?	Date	Time	Notes
Perform data carving	Yes	21/12/2024	03:40 PM	**Step1:** To find instant messaging clients, I used the **run ingest module** and followed the steps such as: ➢ Clicked on **tools** ➢ Chose **Run Ingest Module** ➢ Selected **Hunter XP for Dongled v6.E01.** ➢ Picked **photo rec carver**. 

Action	Done?	Date	Time	Notes
				Step2: After running the **photo rec carver** module, I looked for **carved files** by following the path. Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/$CarvedFiles/1 
Run relevant keyword searches; Did you index the evidence file?	Yes	21/12/2024	04:10 PM	**Step1:**

Action	Done?	Date	Time	Notes
				To find and run relevant keyword searches for single keywords, follow this path: Path: Analysis Results/Keyword Hits/Single Keyword Search.  **Step2:** To find and run relevant keyword searches, follow this corrected path for single keyword searches: Path: Analysis Results/Keyword Hits/Single Keyword Search.

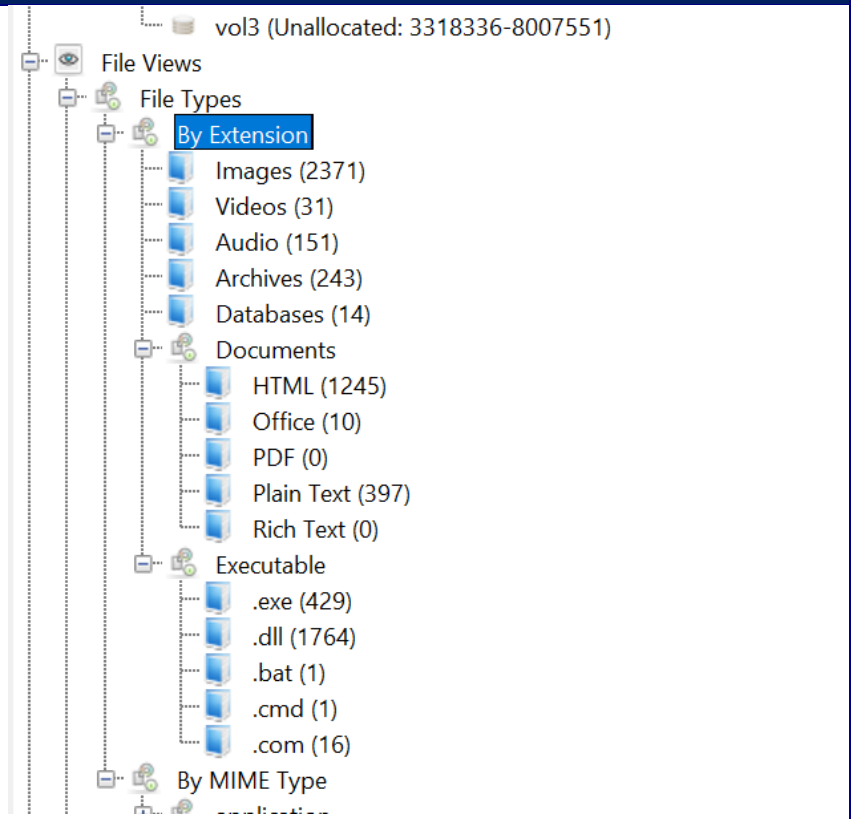
Action	Done?	Date	Time	Notes
				
Recover Log-on passwords – use SAMInside/Ophcrack/Encase	Yes	21/12/2024	04:50 PM	To recover Password **SAM** and **System** is extracted from the Config folder. To explore Config folder I followed the path given below. Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/config **Step2:** After extracting **SAM** and **System** file, it is transferred to linux file.

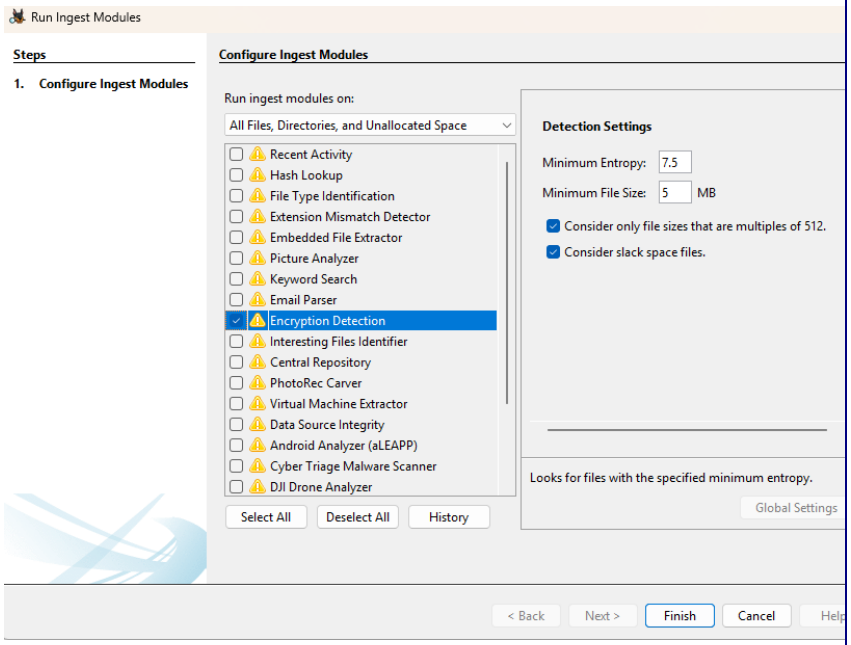
Action	Done?	Date	Time	Notes
				• In linux I used **Samdump2 tool** to extract **NTLM_Hashes** of the **users**. • Then, I Copied **samdum2 tool** source code from **Github.** • **Clonned** the source in the linux terminal • **After cloning** I opened terminal where I kept Sam and system File run the command to get .**txt** file of **NTLM_Hashes.** **Command:** **Samdump2 system SAM -o NTLM_Hashes.txt** **Samdump2 system SAM -o NTLM_Hashes.csv** And got all users **NTLM_Hashes in the text file.** 

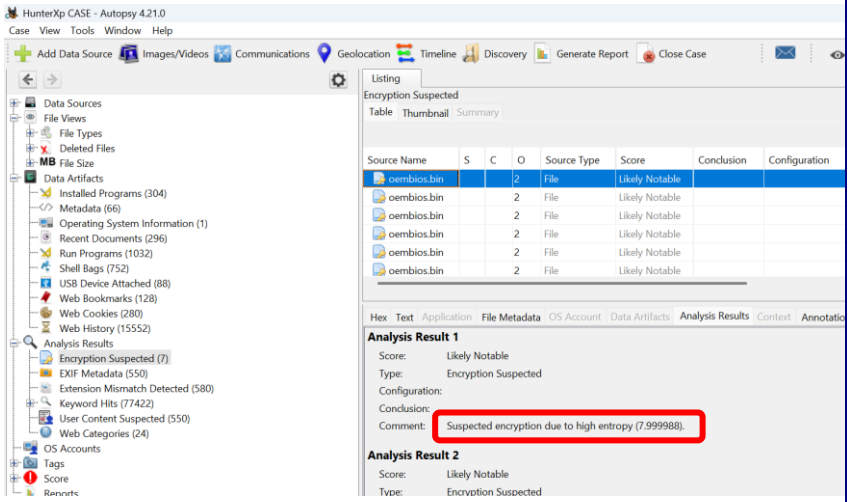
Action	Done?	Date	Time	Notes
				 **The NTLM_hash** value **of BOB Hunte**r is **31d6cfe0d16ae931b73c59d7e0c089c0** It means there is **not any password** Used by **Bob Hunter**.
Examine different file types: Export doc/office and exe files; look at Metadata if required	YES	21/12/2024	06:15 PM	After loading the case, I saw different types of files by following the path such as: Path: /file Views/File Types/ In this path, I found two types of files that are; 1. By Extension

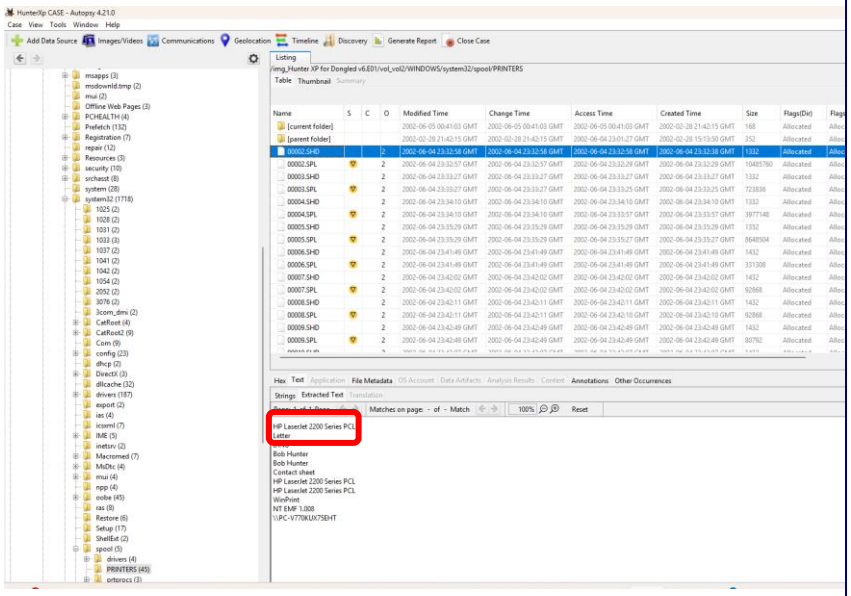
Action	Done?	Date	Time	Notes
				2. By MIME Type When I viewed it by extension, I found that there are different file types such as. • Images (2371) • Videos (31) • Audio (151) • Archives (243) • Databases (14) After examination of these files, I also found that two more modules are: a. Documents • HTML (1245) • Office (10) • Pdf (0) • Plain text (397) • Rich text (0)

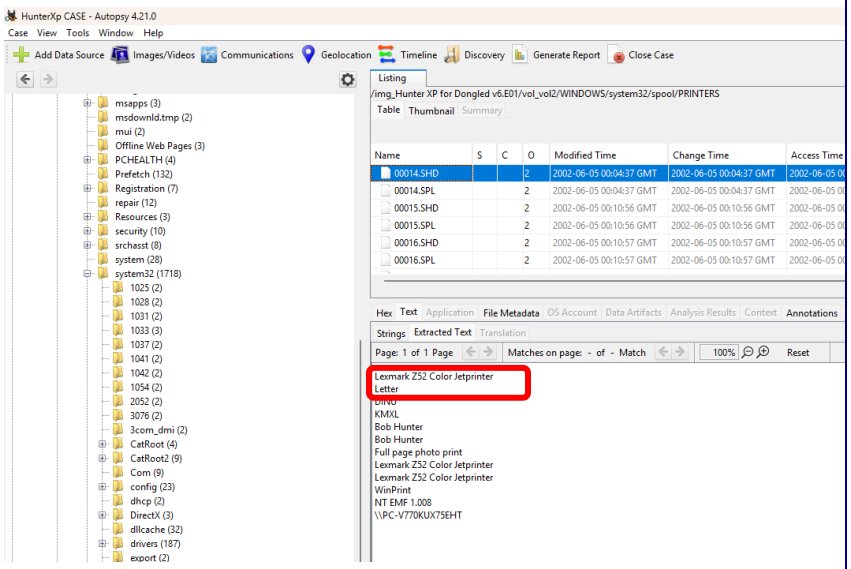
Action	Done?	Date	Time	Notes
				b. Executable • .exe (429) • .dll (1764) • .bat (1) • .cmd (1) • .com (16)

Action	Done?	Date	Time	Notes
				

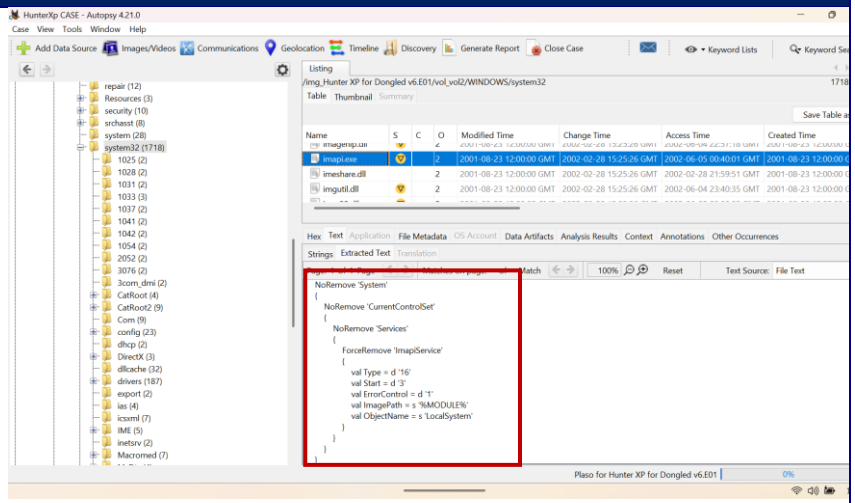
Action	Done?	Date	Time	Notes
Encryption, Steganalysis (any indications? Entropy or Autopsy can be used)	YES	21/12/2024	06:40 PM	For analysis of Encryption, Steganalysis I run Encryption Detection in the ingest module, by following the given steps. ➢ Clicked on **tools.** ➢ Selected **run ingest module** ➢ Clicked **Hunter XP for Dongled v6.E01.** ➢ Picked **Encryption Detection**. 

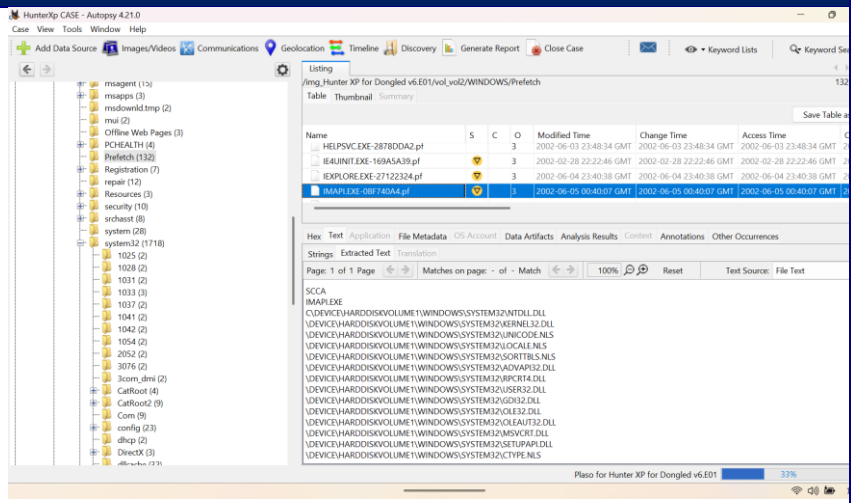
Action	Done?	Date	Time	Notes
				➢ After running this module, I found there was an encryption suspected header when I clicked **Analysis result**. ➢ After analysis, only one encrypted file named '**oembios.bin**' was found. Entropy of **oembios.bin** file = **7.999988** (which is high) 
Print artefacts	YES	21/12/2024	07:05 PM	For analysis of Print artifacts, I found two distinct file extensions with the print spooler to identify: **'.shd' and '.spl**.'

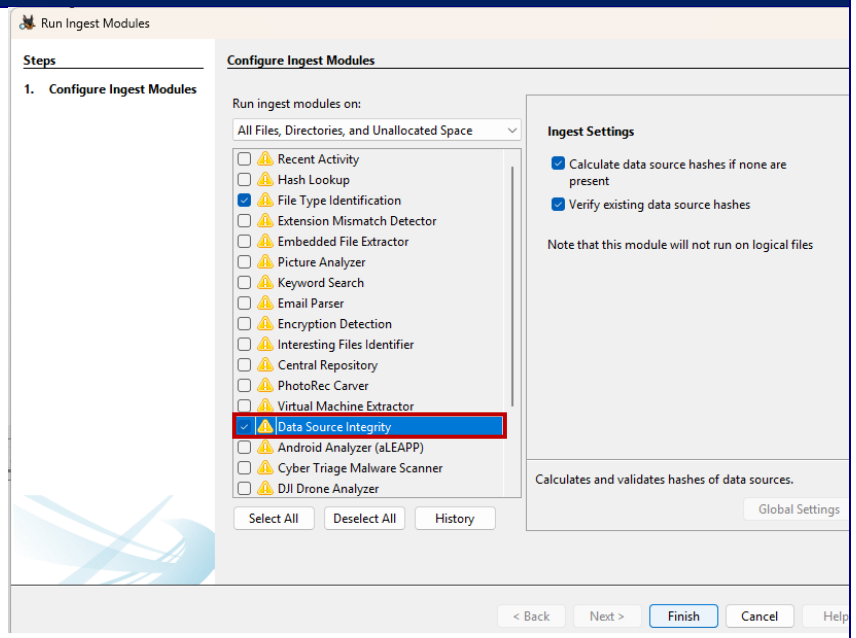
Action	Done?	Date	Time	Notes
				The '.shd' (Shadow) files exclusively contained print job information, while the **'.spl' (Spool)** files housed the content in RAW format as generated during the printing process. For examination of these artifacts, I followed the path; Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/spool/PRINTERS 

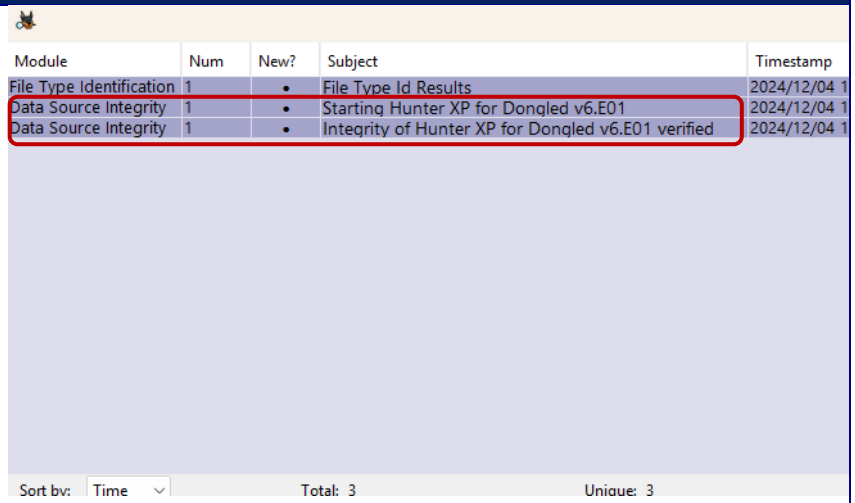
Action	Done?	Date	Time	Notes
				➢ After analyzing the files in the **PRINTERS** folder, I found that the **HP LaserJet 2200 Series PCL Printer** is used for printing. ➢ When I analyzed all the files in the folders, I found that one more printer was used for printing.  I found that the **Lexmark Z52 Color Jetprinter** was also used for printing purposes.

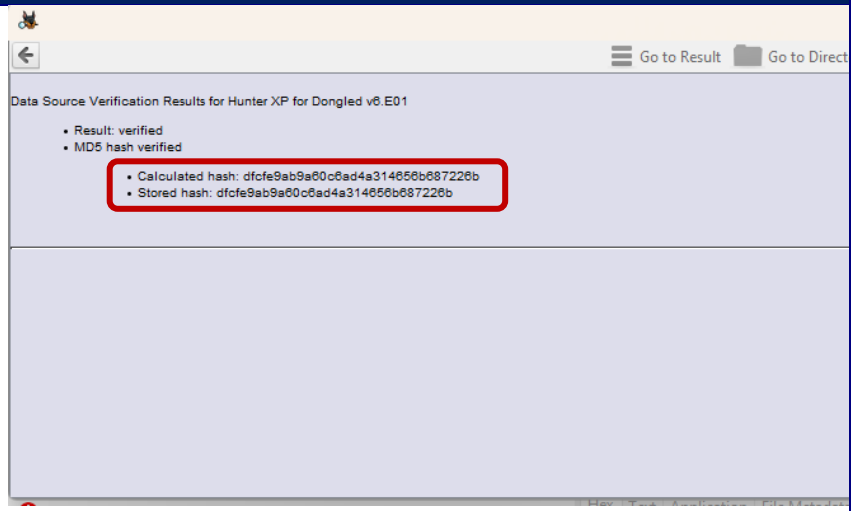
Action	Done?	Date	Time	Notes
				So, the printers used for printing are; 1. **Lexmark Z52 Color Jetprinter** 2. **HP LaserJet 2200 Series PCL Printer**
CD/DVD burning apps; check log files	YES	21/12/2024	07:30 PM	CD/DVD burning app was use by the user. To find the traces of CD/DVD burning I followed the following steps given below: **Step1:** I found the artifacts about the CD/DVD burning in system32 folder where **IMAPI.EXE** details and log is stored. Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32

Action	Done?	Date	Time	Notes
				 **Step2:** **imapi.exe** file is executed by the user. This file data execution details is stored store in prefetch folder. To find **imapi.pf** file I browsed the following path: Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/Prefetch

Action	Done?	Date	Time	Notes
				
Validate evidence integrity at the end of the examination	YES	22/12/2024	12:00 PM	To validate evidence integrity; I go for the ingest module by following the given steps: ➢ First of all, click on **tools.** ➢ Selected **Run Ingest Module.** ➢ Clicked on **Hunter XP for Dongled v6.E01.** ➢ And selected **Data Source Integrity.**

Action	Done?	Date	Time	Notes
				 After finishing these steps. We found that there is a notification shown in the message box.

Action	Done?	Date	Time	Notes
				 When I opened the message box, I found that the Data Source integrity of **Hunter XP for Dongled v6.E01** was verified. When I opened this message, I saw that the result is verified and **MD5 HASH is also verified.**

Action	Done?	Date	Time	Notes
				 So, this information proves that Evidence integrity is not tempered and it is the same as the Starting point.

Additional Notes/Artefacts Examined:

Colour-coding Legend	**Tasks**
	Fundamental
	Basic
	Elementary
	Secondary
	Advanced
	Exceptional