**Hunter XP Report**

**Computer Crime and Digital Evidence**

A logo with blue and red text

Description automatically generated

**Submitted by**

Name: Ajaj Ahmed

Cyber Security and Digital Forensics

Kathmandu, Nepal

Dec 24, 2024

**Hunter XP Image Report**

**Table of Content:**

1. **Scope of Investigation 3**
   1. Evidence file overview 3
   2. Hash verification 3
2. **System profiling 5**
   1. Operating system and timeline 7
   2. Time zone Information 9
   3. User Accounts 10
3. **Data Recovery 10**
   1. Lost Folders (NTFS, FAT16 & FAT32) 10
   2. File signature analysis 11
4. **Internet Activity 14**
   1. Browsing and Email Analysis 15
5. **Artifacts and Application Analysis 17**
   1. Link Files Recycle Bin 18
   2. Instant Messaging Clients 19
6. **Hardware and Network Usage 20**
   1. External Drives 20
   2. Network Connections 22
7. **Password Recovery 23**
   1. Log-on Password 23
   2. SAMinside/Ophcrack Analysis 23
8. **Encryption and steganalysis 25**
   1. Encryption Detection and Entropy Computation
9. **Print Artifacts 26**

10.1 CD/DVD Burning Application  **28**

1. **Miscellaneous Findings 29**
2. **Conclusion 31**
3. **Appendix 32**
4. **Scope of Investigation:**

On December 5, 2024, I received an evidence file in .E01 format, which is in encase evidence format. My task is to examine the image for any signs of criminal activity. This image is forensic image of a digital device, which is a type of windows computer. I used different forensics tools for investigation of this evidence file. The tools used for investigation are given below.

1. Access Data FTK Imager
2. Autopsy
3. Reg Ripper
4. Registry Viewer
5. Event Log Explorer
   1. **Evidence file overview:**

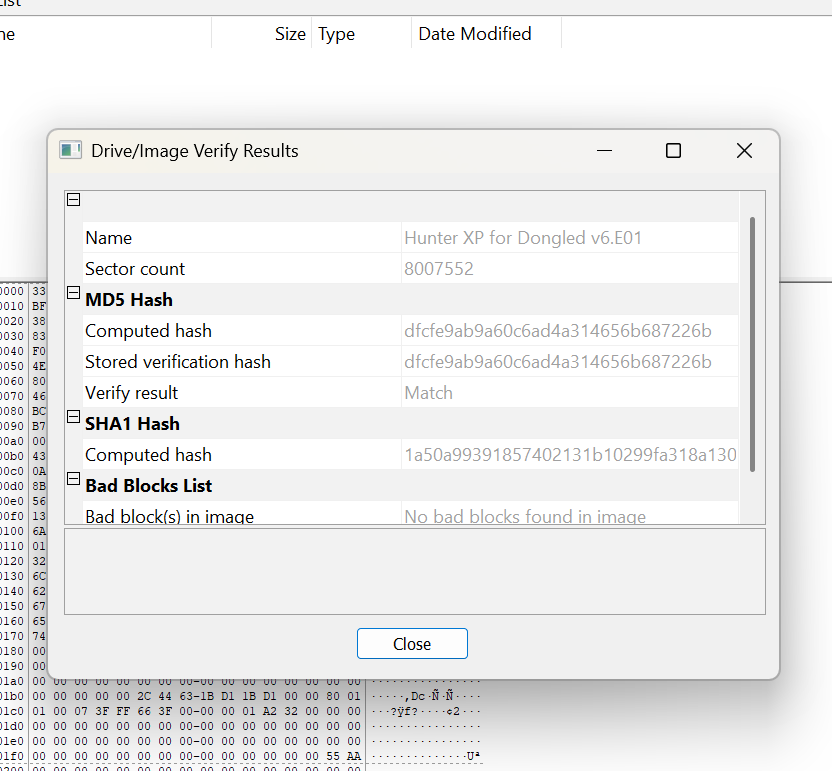
**Hunter XP for Dongled v6.E01** is the evidence file which is investigated. It is an evidence file in image file format related to the case. Firstly, the given image file is loaded into Access data FTK Imager for Further Investigation. The given image files contain many digital Artifacts and deleted files, details and all the malicious and illegal activity done by the user.

* 1. **Hash Verification**

To verify the hash of the given evidence image, it is loaded into both autopsy and AccessData FTK Imager forensics Tool.

1. AccessData FTK Imager:

First of all, I have opened FTK Imager application and added evidence item Hunter XP for Dongled v6.E01 Image file, to ensure that the file has not been altered during Examination Process.



After Verifying in Access Data FTK Imager I Got the hash values of this image.

**MD5 Hash: dfcfe9ab9a60c6ad4a314656b687226b**

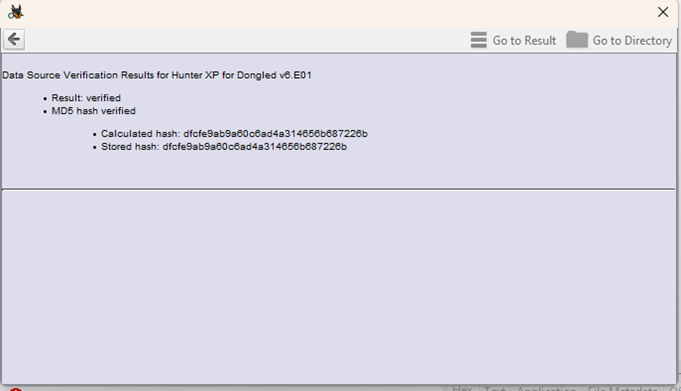
**SHA1 Hash: 1a50a99391857402131b10299fa318a130a603b0**

After verifying the hash values of image in Access Data FTK Imager, the evidence file is loaded into the Autopsy for double Verification. To verify the integrity of the Evidence file I have followed the following steps after loading this image file into the autopsy.

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.

After performing these steps I found that there is on message at the right side of message notification bar. I clicked and after seeing that message, it is confirmed that there is not any mismatch of files integrity both hashes values are same.



Hence, the integrity of evidence file is not tempered. The hash values were identical across both tools, ensuring the authenticity and integrity of the evidence during the investigation.

1. **System Proofing**

System proofing is the process examining various aspect of a system, such as operating system, hardware installed, installed software, user accounts, time zone setting, and other system level attributes

**Findings:**

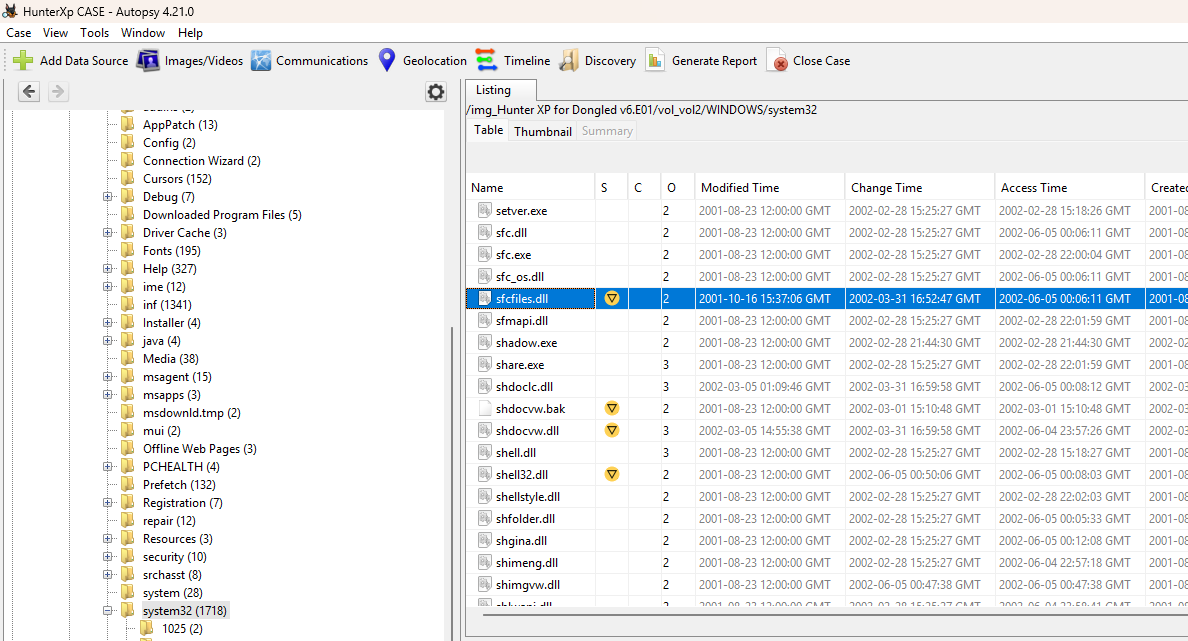
I collect information about system configuration from sfcfiles.dll files by following path;

**img\_Hunter XP for Dongled v6.E01**

**vol\_vol2**

**WINDOWS**

**system32**



sfcfiles.dll contains the information about the system.

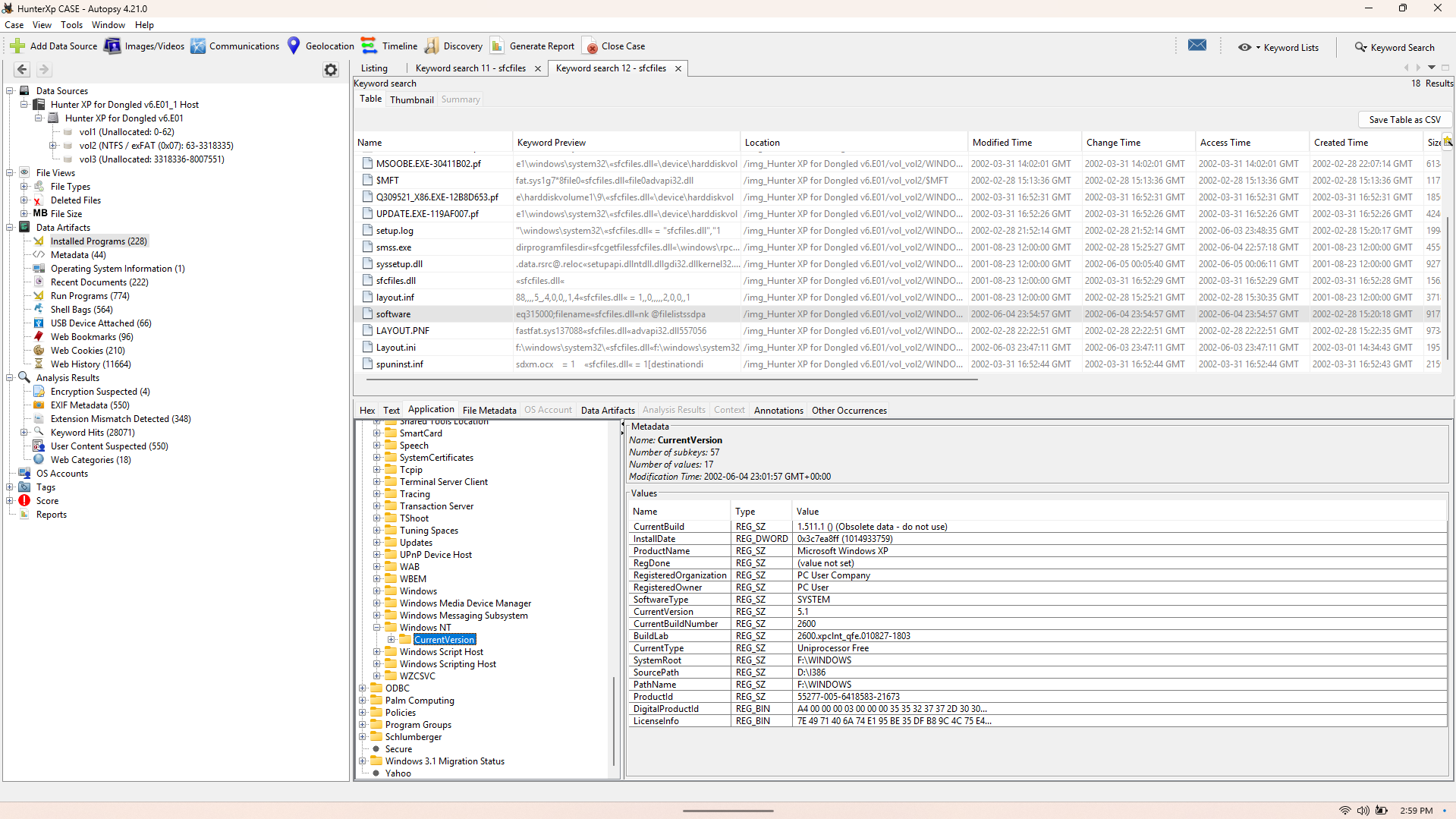
Again, I also found **NUSTER.dat** files which help to find and identify the user specific setting and application preferences, also help to understand about the operating system state and user information. I found NUSTER.dat in the path given below.

**img\_Hunter XP for Dongled v6.E01**

**vol\_vol2**

**Documents and Settings**

**Bob Hunter**



* 1. **Operating System and Timeline:**

Operating system details are obtained by extracting **SAM (Security Account Manager),** I got the SAM file from the config folder. I found **SAM** by following path such as.

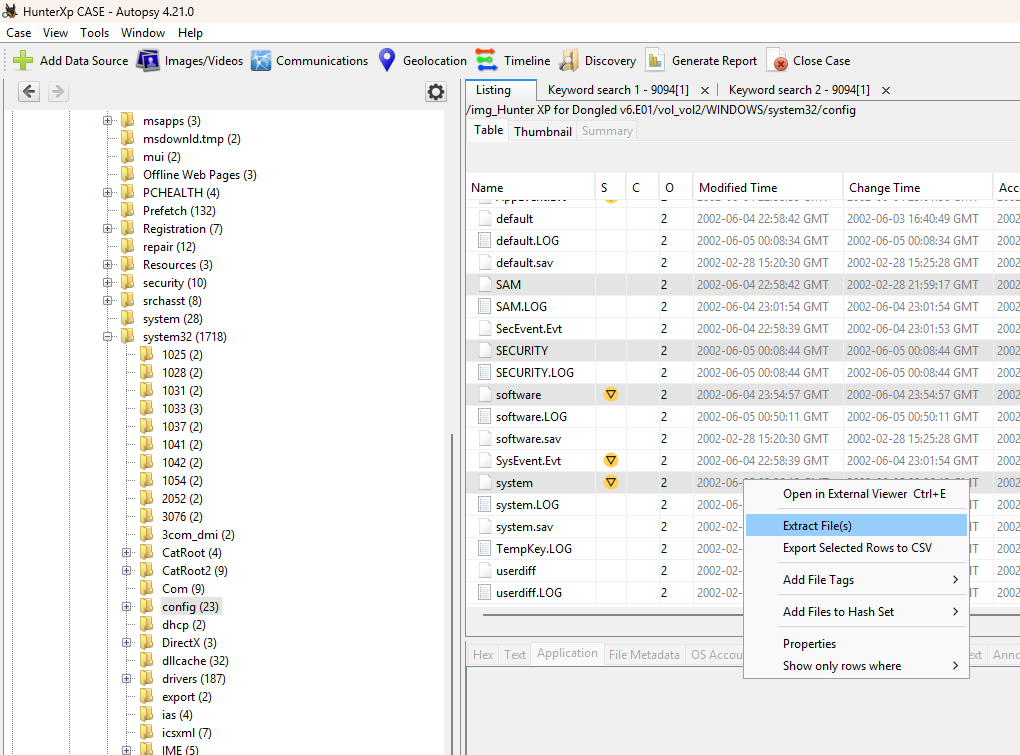
**img\_Hunter XP for Dongled v6.E01**

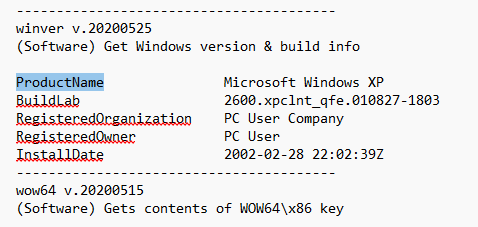
**vol\_vol2**

**WINDOWS**

**system32**

**config**

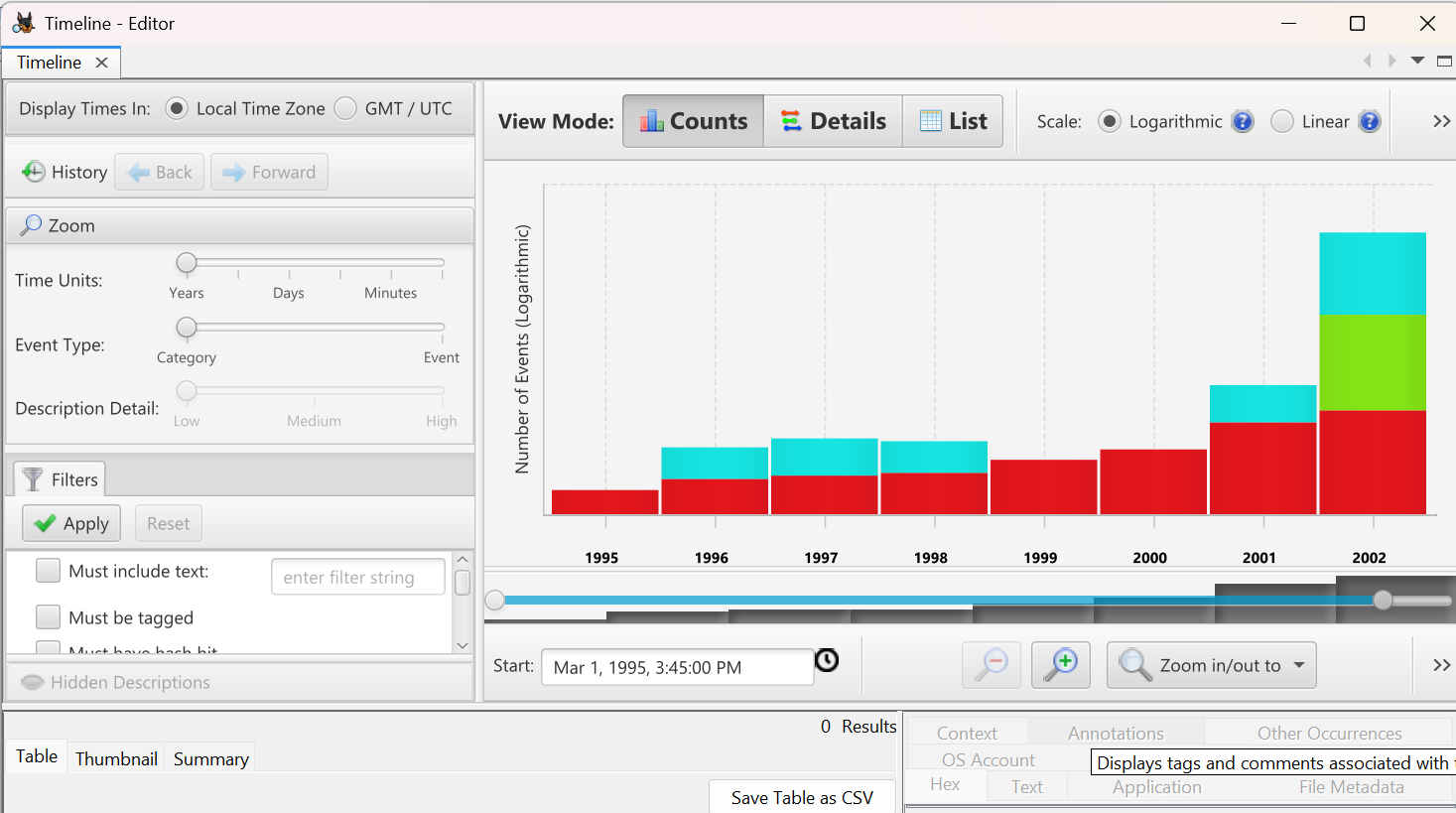




After ripping SAM file into RegRipper I found **Microsoft Windows XP** Version is the operating system is used in the evidence system, and it is installed on **2002-02-28 22:02:39Z.**

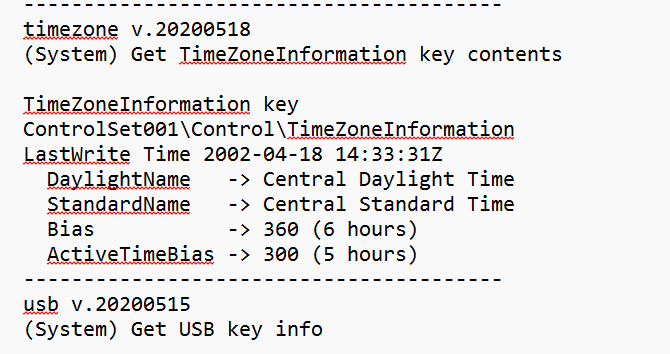
for **timeline** analysis **plaso** ingest module is run. Steps used for running this Module are give below.

* Click on **Tools** in the toolbar.
* Choose **Run ingest modules.**
* Select **Hunter XP for Dongled v6.E01.**
* Picked **Plaso**.
* After running **plaso,** clicked on **Timeline** and I got timeline detail.



* 1. **Time Zone Information:**

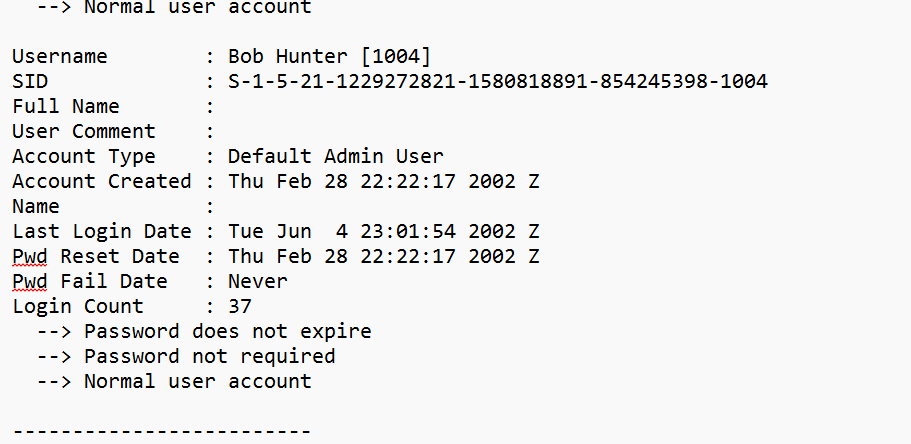
Time zone information was obtained by extracting **SAM, SYSTEM, and Software** files using **Autopsy**. After extracting these files information is retrieved in .txt files using **Reg Ripper Tool.** The extracted txt files analyzed, and I got information about the Time Zone. Time zone information is stored in the system hive file. I opened **System.txt** file and found **Time Zone information**.



* 1. **User Accounts**

The user account information is also extracted from **SAM, System, and Security** files. The **SAM** file contains critical information about the user accounts. It also consists of password hashes and user details. In this case also I followed the same steps extraction and ripping, as I did for time zone and operating system analysis. When analyzed the txt file of SAM I found the user is **Bob Hunter,** the primary user of the system.

In this file I also got information about status of user accounts such as last login details and password policies. This provides detailed information about user accounts.



1. **Data Recovery**

Data recovery is the process of retrieving lost, deleted or inaccessible data from a storage medium.

* 1. **Lost Folders (NTFS, FAT16 & FAT32)**

When the folders are deleted or file system gets corrupted, accidentally or by malicious activity, they can be recovered by analyzing the metadata structures of file system. NTFS uses **MFT (Master file table)** to store files and folders. It provides maps for the stored data by maintaining file allocation table. Deleted files and folders can be found by scanning the table for files that are marked as “Deleted” but not overwritten.

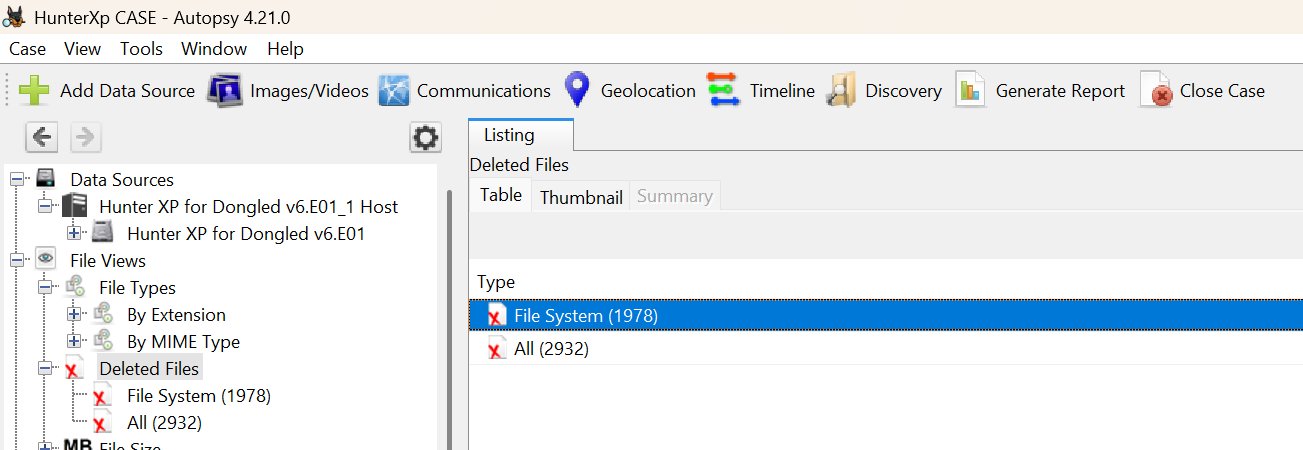
**Findings:**

To obtain Lost folders I run the ingest module called photorec Carver by following the steps given below:

* Clicked on tools
* Selected RunIngest Module
* Clicked Hunter XP Dongled V6.E01.
* Selected Photorec Carver.

After finishing these steps, I see for Deleted file by following path.

**File Views Deleted Files**I found that there are 2932 files are deleted in folder all and 1978 files are stored in the file system.



* 1. **File signature Analysis**

File signature analysis is a technique used to identify and validate files based on their unique **hex values or binary patterns**, which remain intact even if the file extension is altered or tempered.

file that **uniquely** **identify** its type, such as

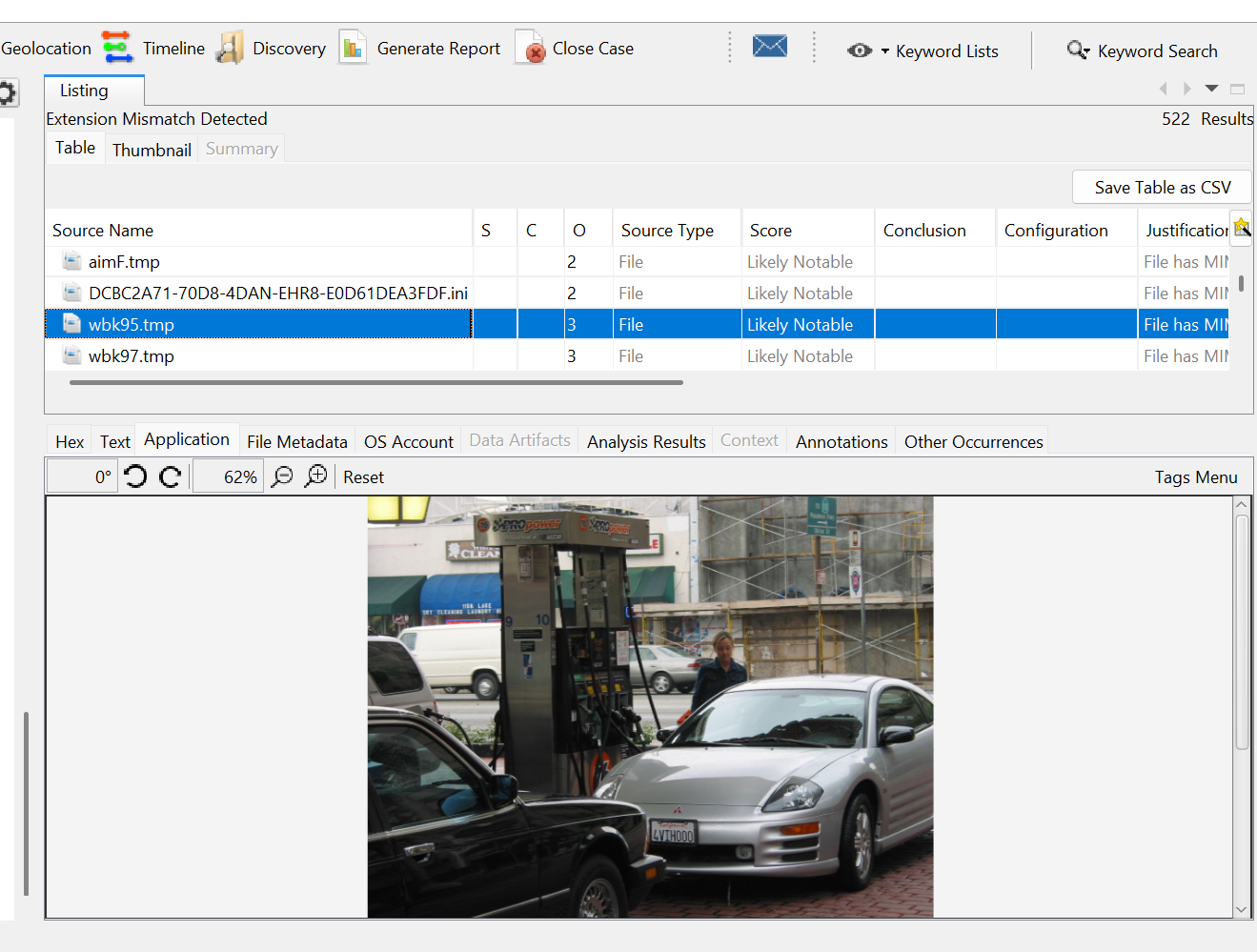
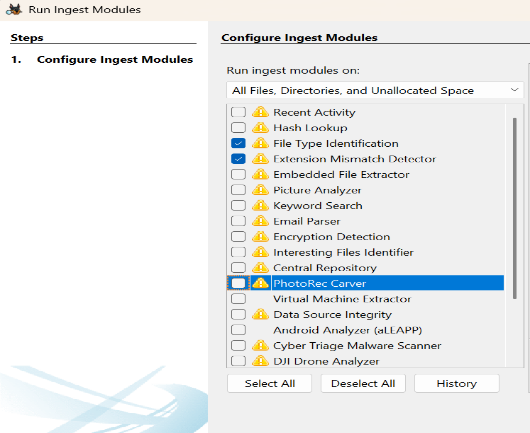
* For **JPEG**: **FF D8 FF EO**
* For **PDF: 25 50 44 46**

**Findings:**

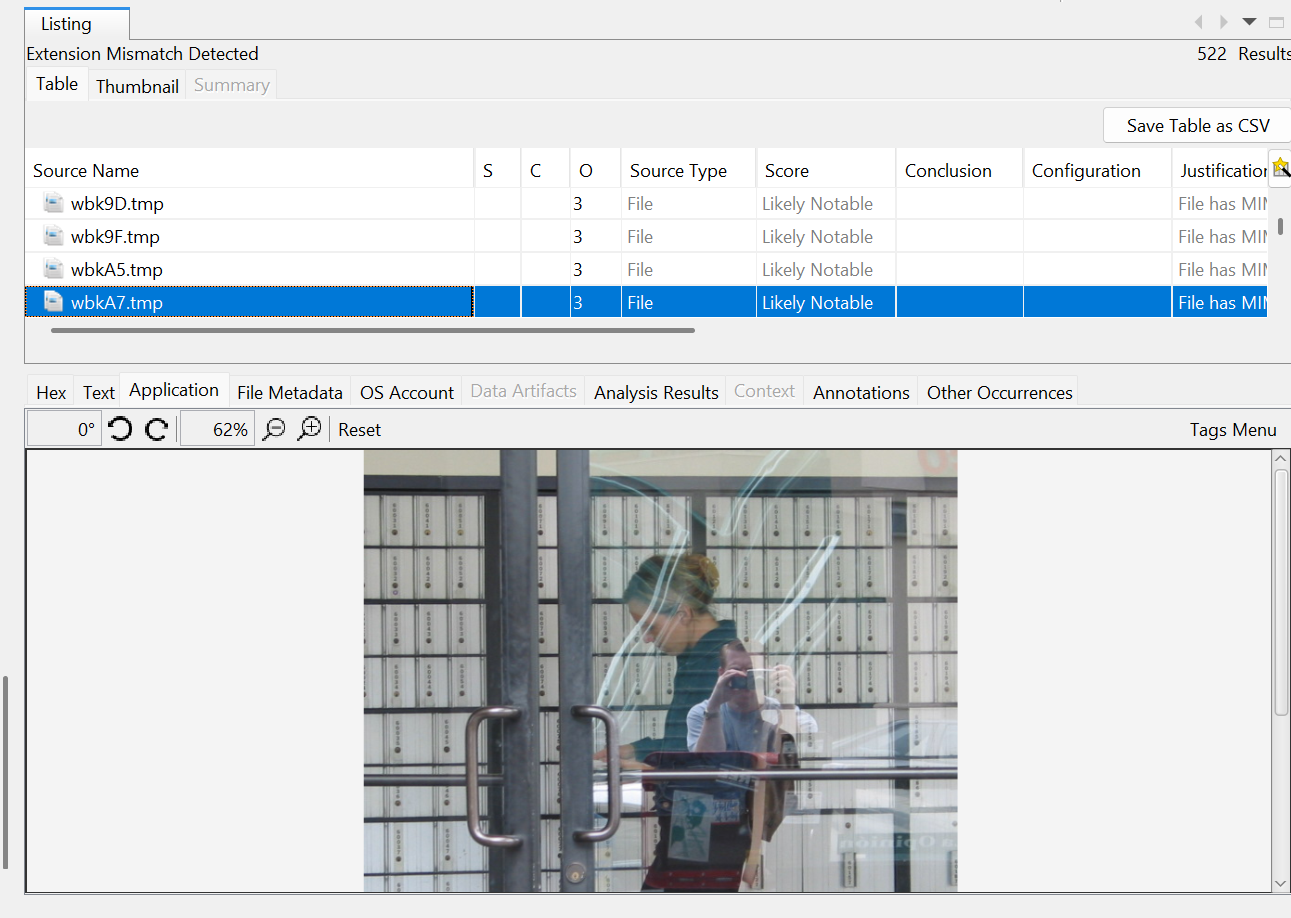
For analysis file signature and file mismatch analysis, I proceed to the **run ingest** module for the **Hunter XP for Dongled v6.E01**. I followed the steps given below.

* + First, click on **tools**.
  + Selected **Run Ingest Module.**
  + Clicked on **Hunter XP for Dongled v6.E01.**
  + And selected **File type identification** and **Extension mismatch Detector modules**.
  + After running this module, I got the 232-extension mismatch Detected files in path.

**Analysis Result Extension Mismatch Detector (232)**



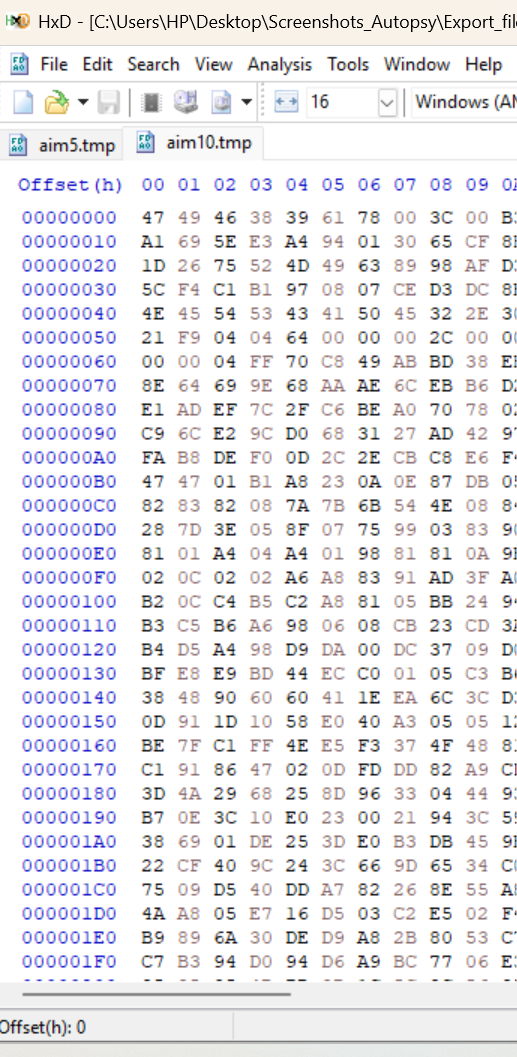
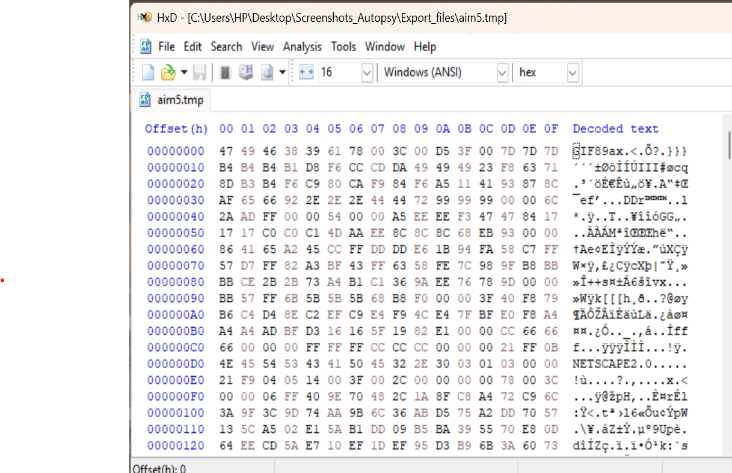
**MD5 Hash of image: 5ead9d1c32a5deb91600b0783b7b4699**



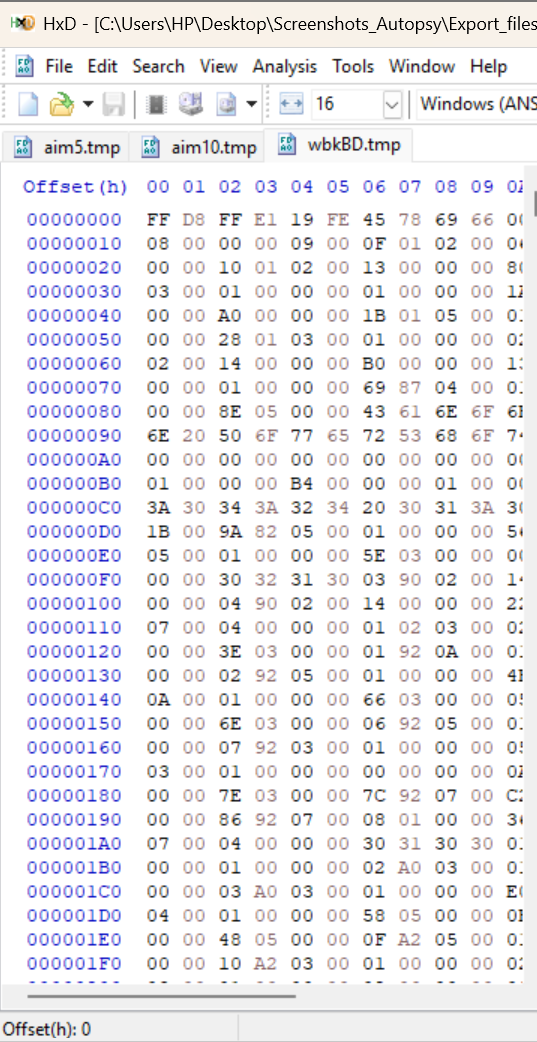
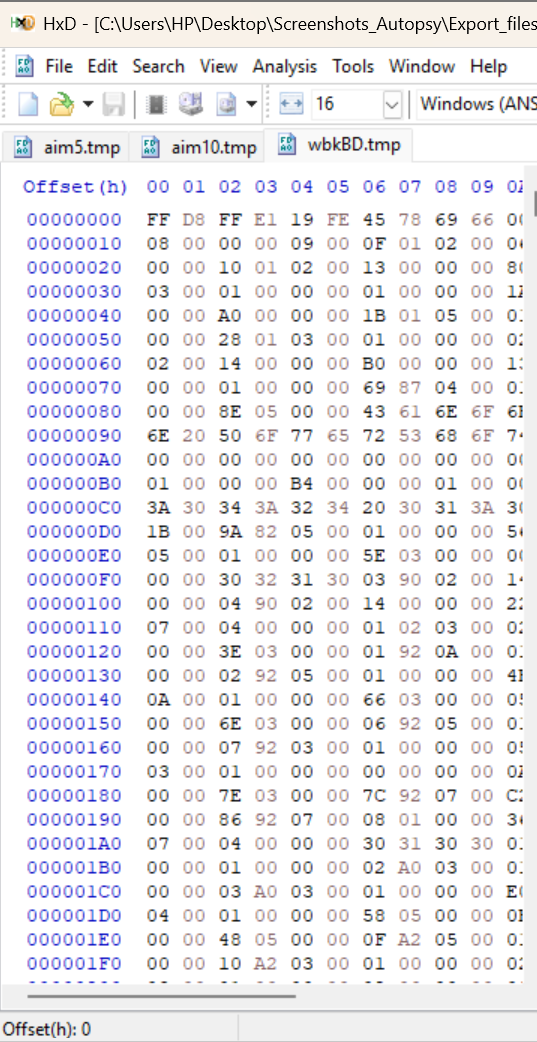
**MD5 of Image: cec6f1262f2563db19574238c959d5f7**

I opened the extension mismatch detected folder and extracted some files. After extracting these files, I opened **HXD** application for analysis of hex values of the extracted files, weather the extracted files are tempered or not according to file extension given in the file.

When aim5.tmp, aim10.tmp are the files I have extracted and are kept in the HXD application I found that the hex value of these two files is **47 49 46 38 39 31.** The given hex value is the value of .gif file. So, it seems that there is mismatch of file extension.



Again, I followed the same steps to check the integrity of wbkBD.tmp and wbkC1.tmp for file extension verification. After keeping it into HXD I got hex value that is **FF D8 FF E1 1B FE.** The hash value I got from the HXD is the value of **.JPEG** file. So, it seems that the user has changed the extension of **.JPEG** is suspicious activity.

1. **Internet Activity**

Internet Activity provides uncovering traces of online behavior to identify browsing patterns, email communication, and any digital footprints left behind by the user.  **Browsing and Email Analysis**

Data can be recovered from **History Files, Cache file, Cookies, Bookmarks and favorites, Session and tab Data.**

**Findings:**

Local emails footprints are stored in the outlook Express folder which is in path

**img\_Hunter XP for Dongled v6.E01**

**vol\_vol2/Documents and Settings**

**Bob Hunter**

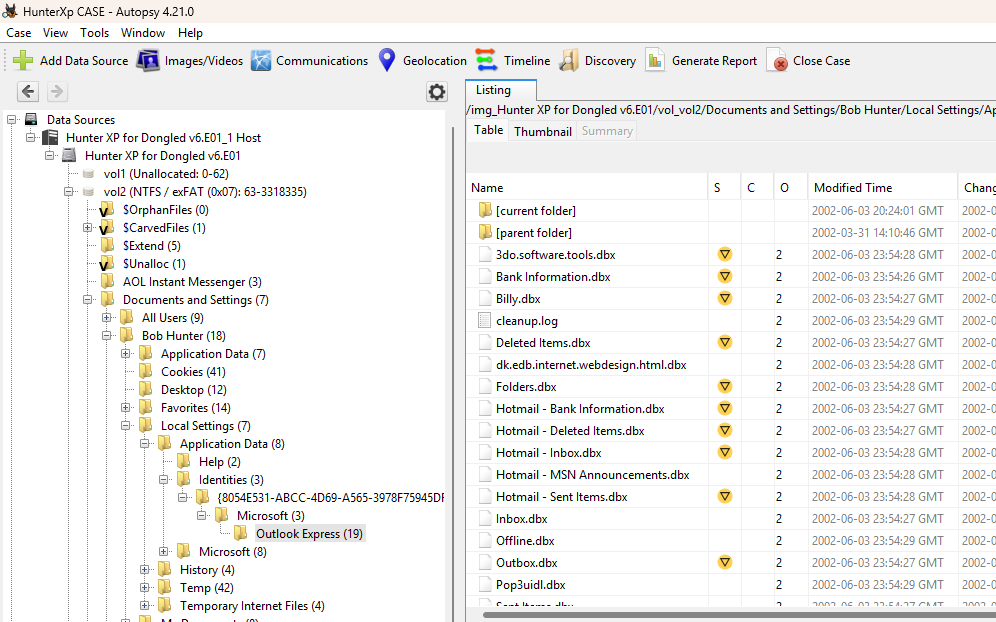
**Local Settings**

**Application Data**

**Identities/{8054E531-ABCC-4D69-A565-3978F75945DF}**

**Microsoft**

**Outlook Express**



In this evidence file, I also found that there are footprints and data of web based emails traces. I found this evidence by following these paths:

**img\_Hunter XP for Dongled v6.E01**

**vol\_vol2**

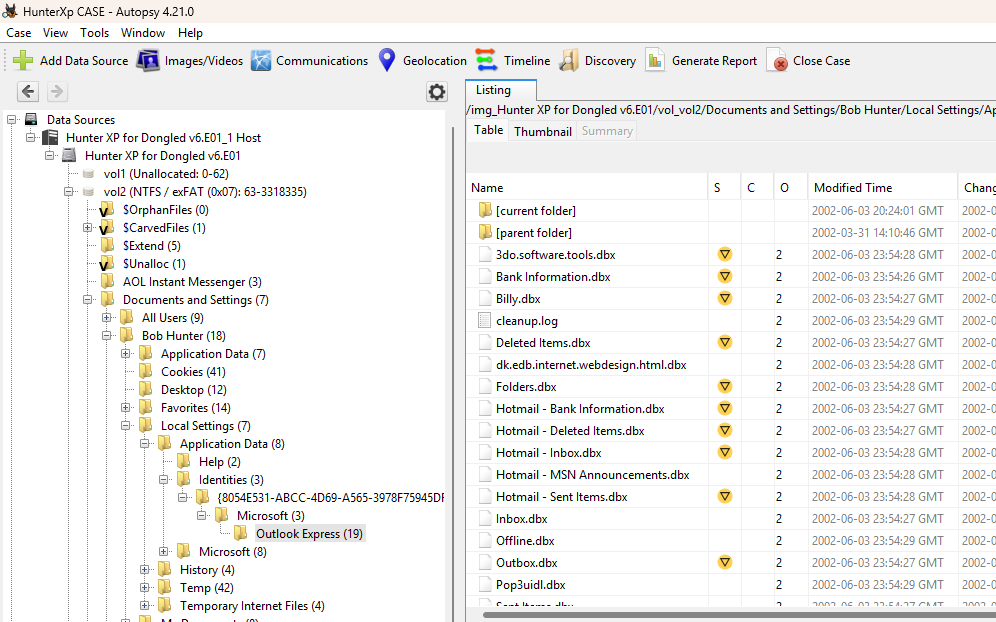
**Documents and Settings**

**Bob Hunter**

**Local Settings**

**Temporary Internet Files**

**Content.IE5**



After following these paths, I found the traces of emails sent are stored in this folder. In this folder I got that the user have done criminal activities like email creation, Extorsion money demand, Bank details exchanged etc. I found the following **email** **addresses** used to **exchange** emails between **14th may to 20th may**.

|  |  |
| --- | --- |
| **Victim Email address** | **Criminal Email Address** |
| 1. [Ted.deweres@encase.com](mailto:Ted.deweres@encase.com) 2. [John.dewist@encase.com](mailto:John.dewist@encase.com) | 1. [Friend@bemine.com](mailto:Friend@bemine.com) 2. [Chase1191@hotmail.com](mailto:Chase1191@hotmail.com) 3. [Billyray150b@netscape.com](mailto:Billyray150b@netscape.com) 4. [Mailer-Demon@ywing.netscape.com](mailto:Mailer-Demon@ywing.netscape.com) |

There are some messages that show the criminal activities or user.

A screenshot of a computer

Description automatically generatedA close up of numbers

Description automatically generated

1. **Artifacts and Application Analysis**

Artifacts and application analysis focus on identifying and interpreting data traces left by system and user activities. This provides information about user actions, deleted files, and usage of specific applications.

**Link Files and Recycle Bin**

Link files are automatically created by the windows operating system of the device with .lnk extension.

**Findings**

Link files are stored in the Recent Folder, I browsed the path given below to get .lnk file;

**img\_Hunter XP for Dongled v6.E01**

**vol\_vol2**

**Documents and Settings**

**Bob Hunter**

**Recent**

Recycle Bin stores temporarily deleted files before permanent removal. Each deleted file and folder are renamed with unique prefixes such as $R and $I file. Original file name, location, and deleted timestamp are stored in the $I file. Files can be restored if not overwritten by new data.

**Findings:**

Recycle bin files are stored in the location given below.

**img\_Hunter XP for Dongled v6.E01**

**vol\_vol2**

**RECYCLER**

**S-1-5-21-1229272821-1580818891-854245398-1004**

* 1. **Instant Messaging Clients**

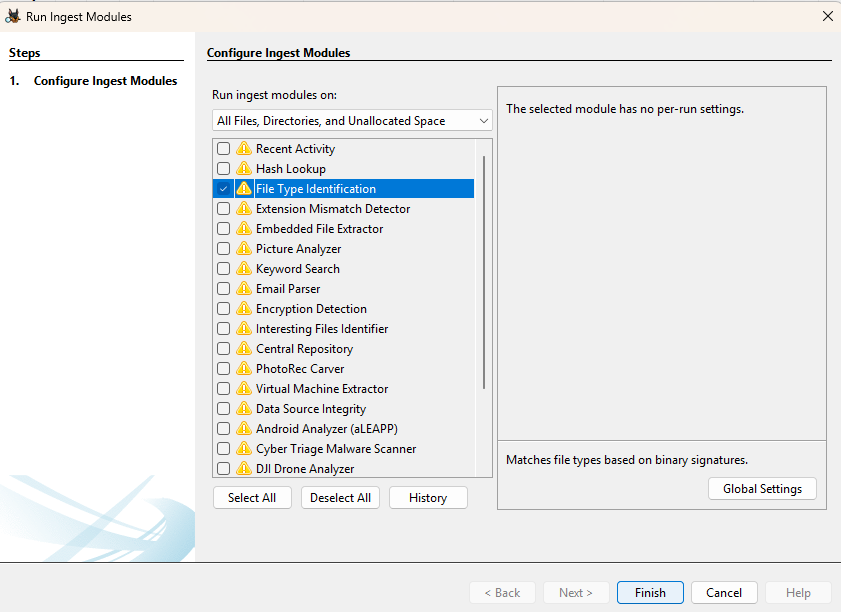
Instant messaging clients such as yahoo, whatsapp, skype, snapchat are the common platforms for communication. Specifically, it stores data with the extension .db.

**Findings:**

For investigation of instant messaging clients, File identification type ingest module was run.

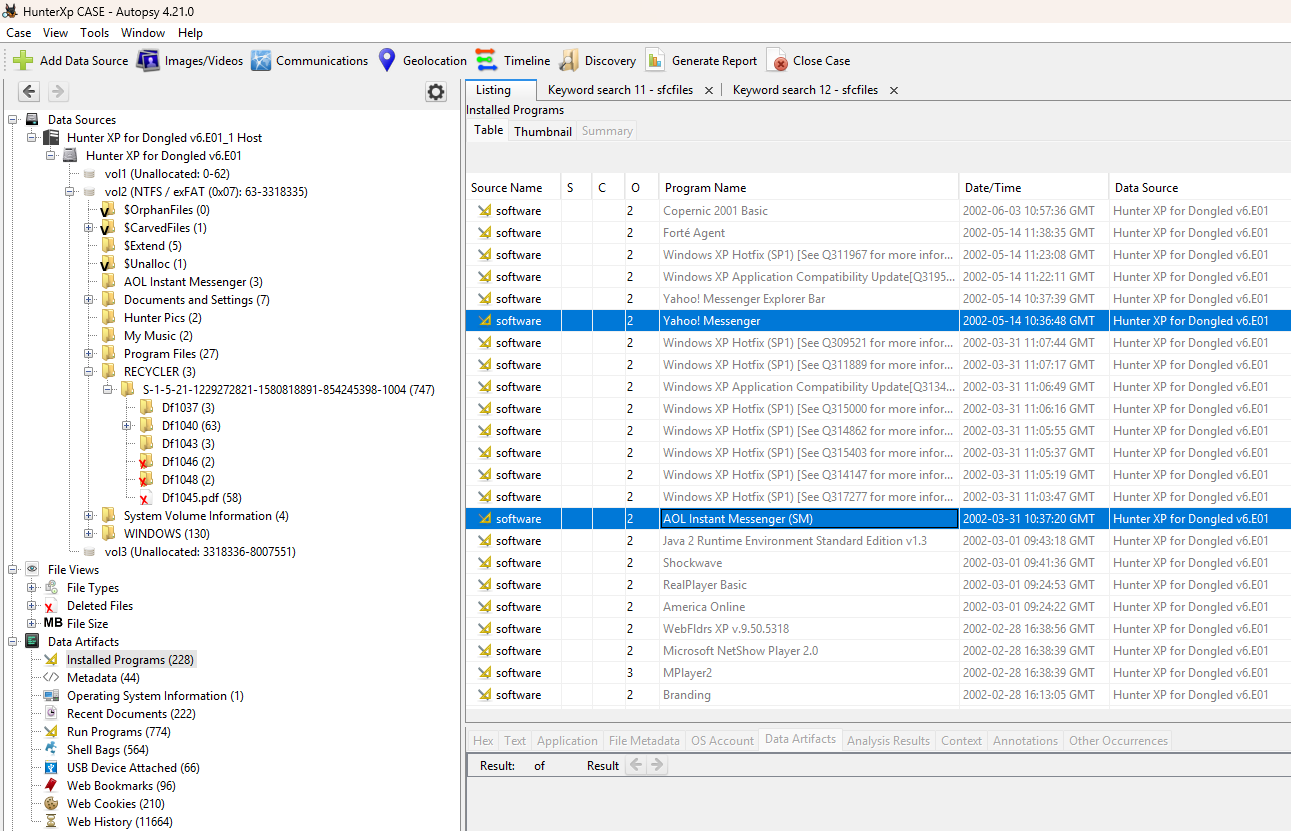
**Steps followed to Run Ingest Module:**

**Tools Run Ingest Module Hunter XP for Dongled v6.E01. file** **type** **identification**



After running ingest module I found that there were two messaging apps that are used for messaging purposes. It is located at the location  
**Data Artifact**

**Installed Programs**



**MD5 yahoo Massenger: dbda9a624d0ca6c78f2a76dfe4e17f30**

**MD5 AOL: dbda9a624d0ca6c78f2a76dfe4e17f30**

1. **Hardware and Network Usage**

Investigation of external drives and network connections can provide critical information about data transfers, manipulation of data and unauthorized access.

* 1. **External Drives**

External drives, like USB flash drives, External hard drives, and SD cards, leave their artifacts when they are ingested or connected to the system.

**Findings:**

Hardware usages are stored in system artifacts in autopsy. The path to location of Hardware usage is.

**System Artifacts USB Device Attached**

It is also located in the location

**CurrentcontrolSet > Enum > USBTOR**

I have also followed the steps given to find system

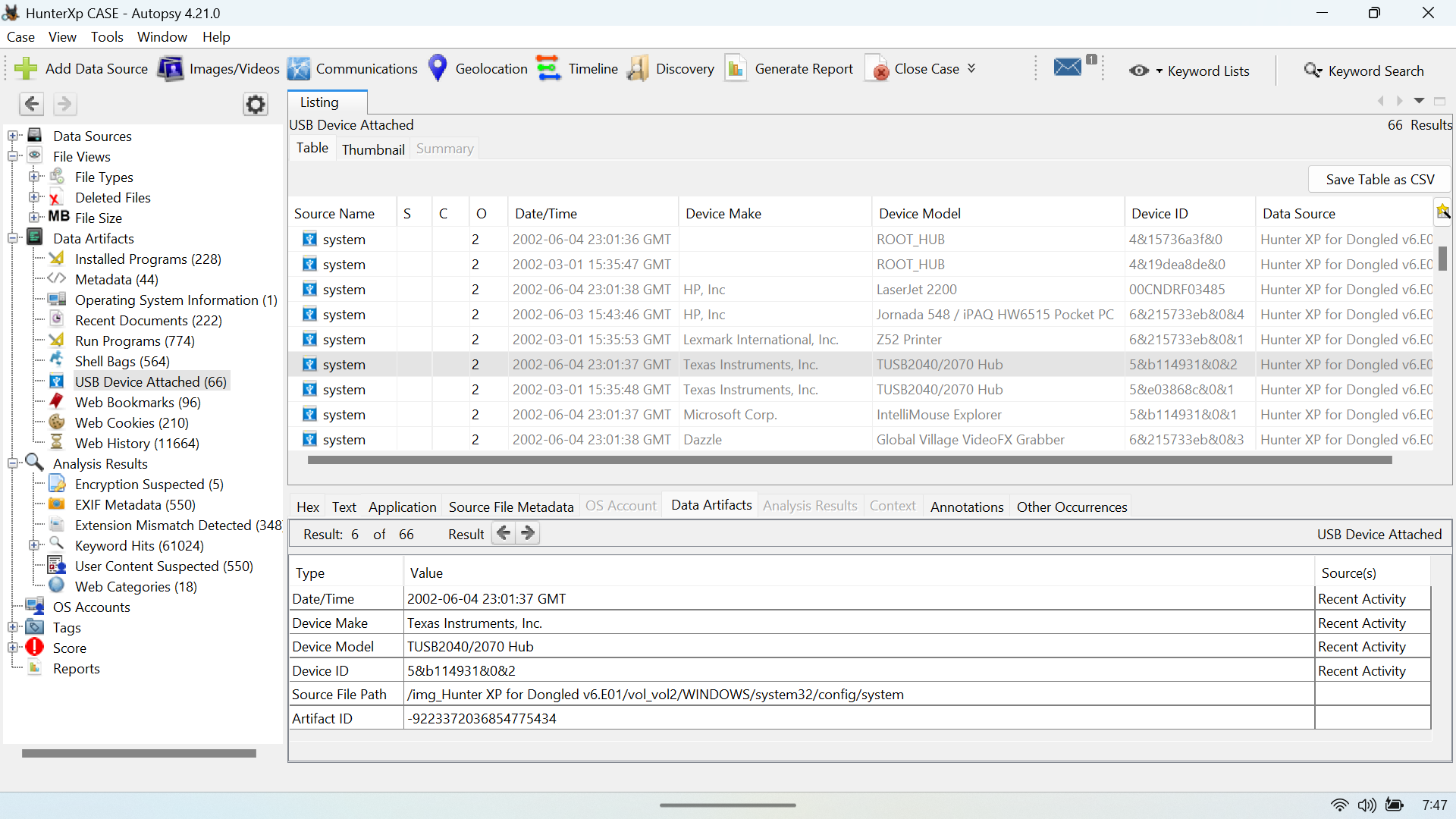
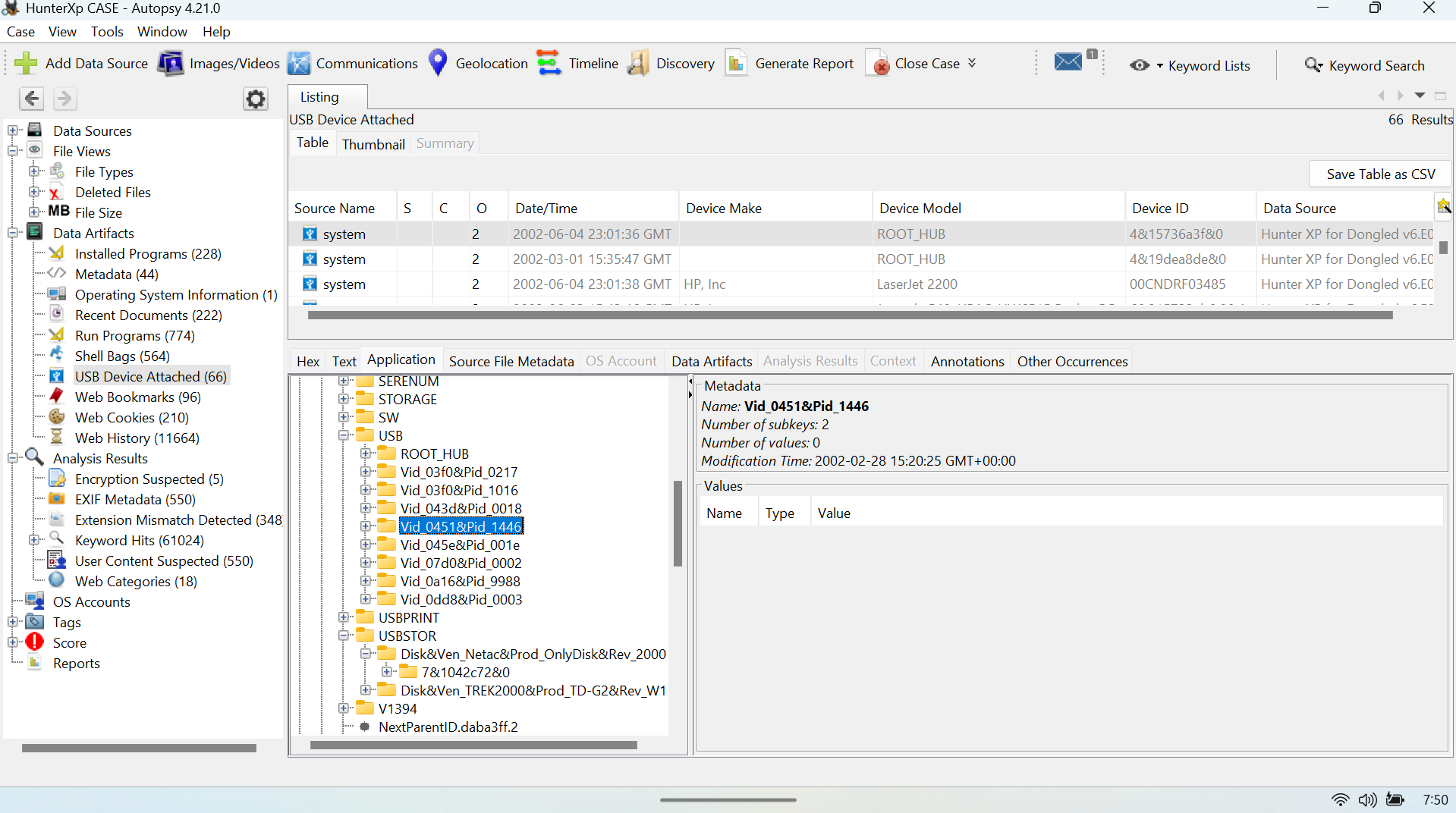
**img\_Hunter XP for Dongled v6.E01**

**vol\_vol2**

**WINDOWS**

**system32**

**config**

****

**MD5: e481dace1baf5277c9934f9912e41f65**

* 1. **Network Connections**

Investigation of network connection is examination of system’s interaction with the devices over the network. It stores local (LAN) and internet-based communications.

**Findings:**

Network connection traces were found in etc. folder of drivers which is in SYSTEM32.

The path where I found Network connection artifacts is.

**img\_Hunter XP for Dongled v6.E01**

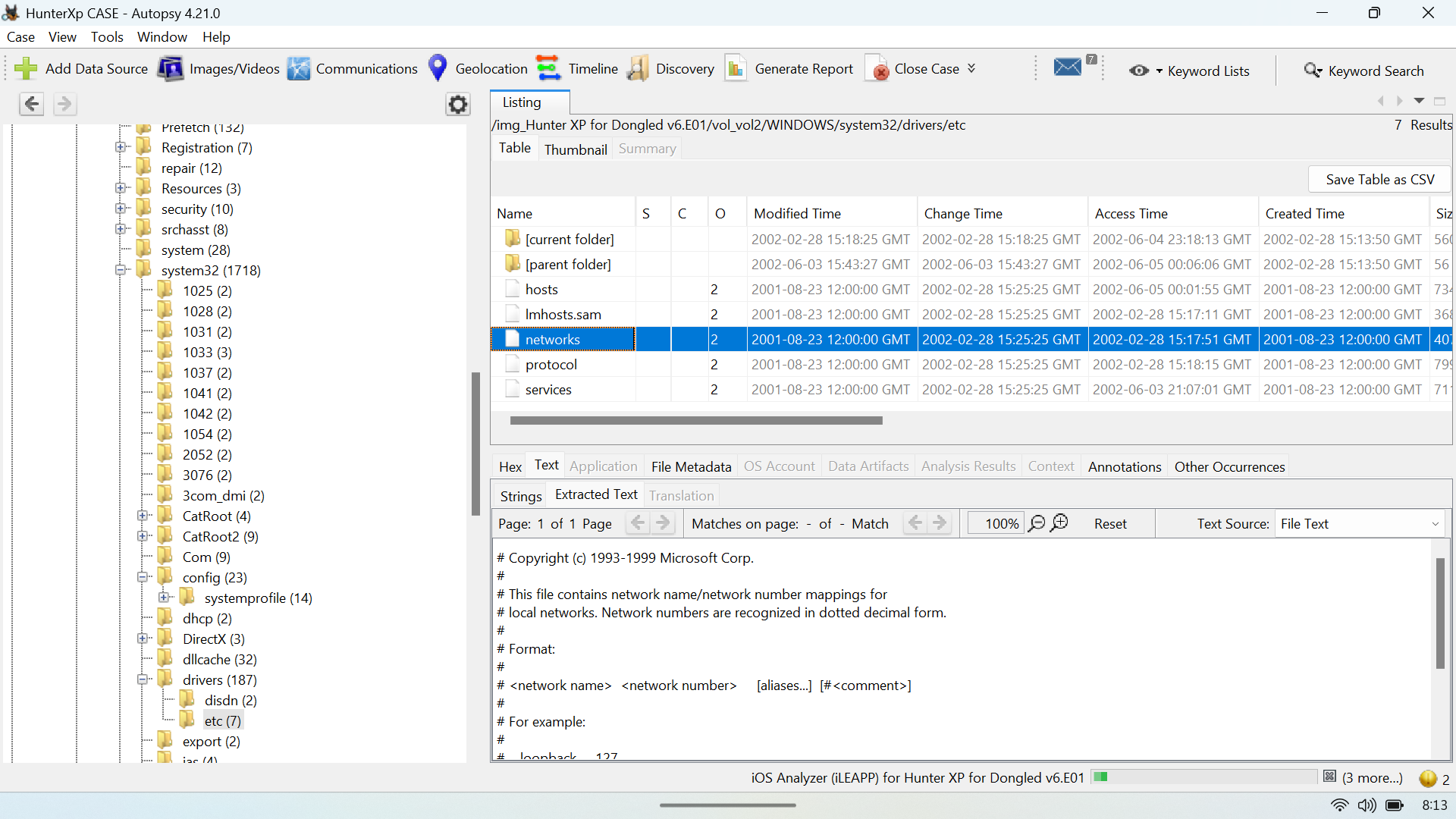
**vol\_vol2**

**WINDOWS**

**system32**

**drivers**

**etc**

****

**MD5: 6165c3e83c1e16469715e7c28d115699**

1. **Password Recovery**

Password recovery is one of the critical tasks of digital forensics, specifically in cases of protected data or where password is encrypted should be accessed to gather evidence.

* 1. **Log-on Password**

Any system password is stored in the hashes format to maintain security in the system. Log-on user password hashes are stored in the **Security Account Manager (SAM)** file.

* 1. **SAMinside / Ophcrack Analysis**

**SAMinside and ophcrack** are the specialized tools which are used for recovering windows log-on password from the **SAM** file of system.

**Findings**

The password of user Bob hunter was recovered by extracting SAM and System. For finding this I have extracted these artifacts from path.

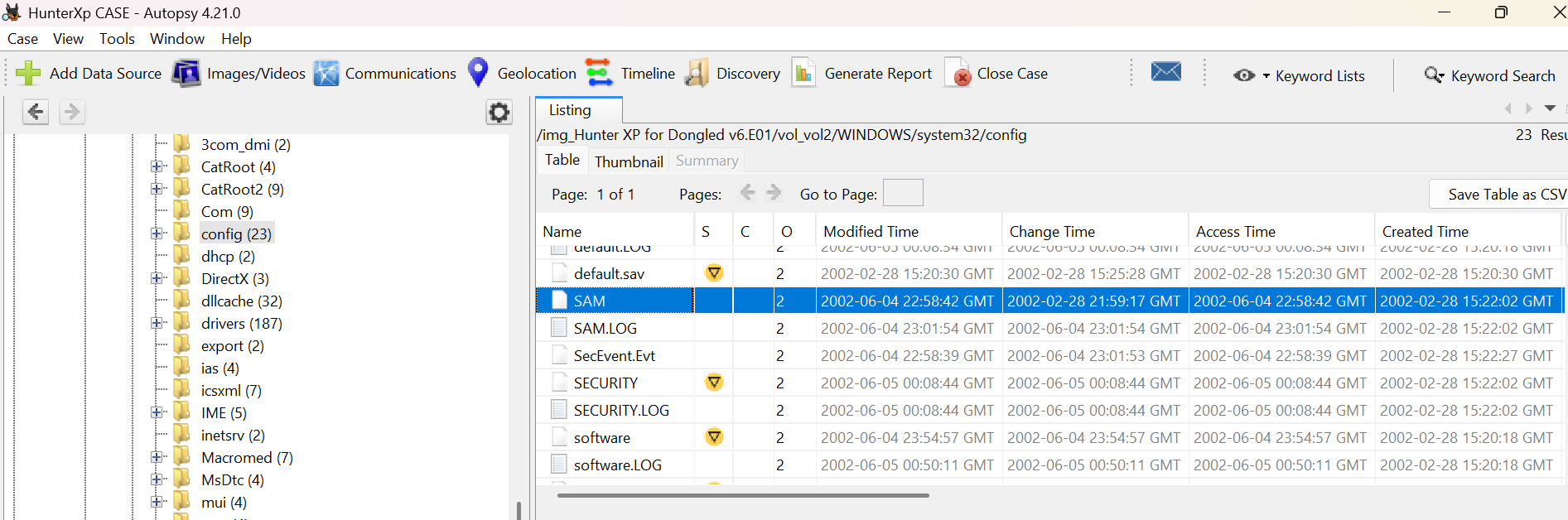
**img\_Hunter XP for Dongled v6.E01**

**vol\_vol2**

**WINDOWS**

**system32**

**config**



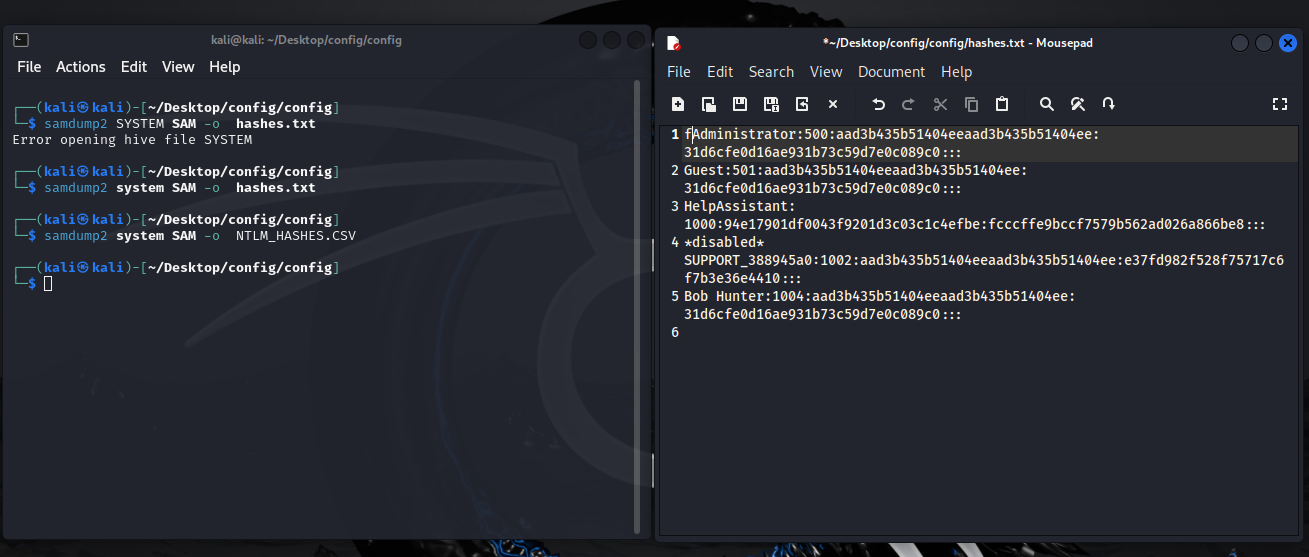
**MD5 of SAM: 6165c3e83c1e16469715e7c28d115699**

After extracting SAM I proceed for extraction of NTLM\_hashes. I have transferred sam and security files in linux. First, I copied the samdump2 source code and cloned it in my linux terminal by giving command.

**Git clone** [**https://github.com/foreni-packages/Samdump2.git**](https://github.com/foreni-packages/Samdump2.git)

After cloning **samdump2** tool in my terminal I proceed for extraction of user **NTLM\_hash** value by giving command.

**Samdump2 system SAM -o <filename>.txt**

After running this command, it generated txt and csv file of hashes values of all the users of system.

1. **Encryption and Steganalysis**

Encryption and steganalysis is one of the essential components of digital forensics. It is the factor that protects and hides data.

**Findings**

For encryption type of file identification, I run encryption detection ingest Module by following the steps given below.

* Clicked on **tools.**
* Selected **runs ingest module**
* Clicked **Hunter XP for Dongled v6.E01.**
* Picked **Encryption Detection**.
* 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)

A screenshot of a computer

Description automatically generated

**MD5:6d0bd10dd99ae61ba6e8a1a3e697dfcd**

1. **Print Artifacts**

print artifacts show the traces of how many external devices are used in the system. In this case I investigate for. shdand. splto know how many printers are used for printing purposes. I found these artifacts in spool folder in system32. The path followed for this investigation is.

img\_Hunter XP for Dongled v6.E01

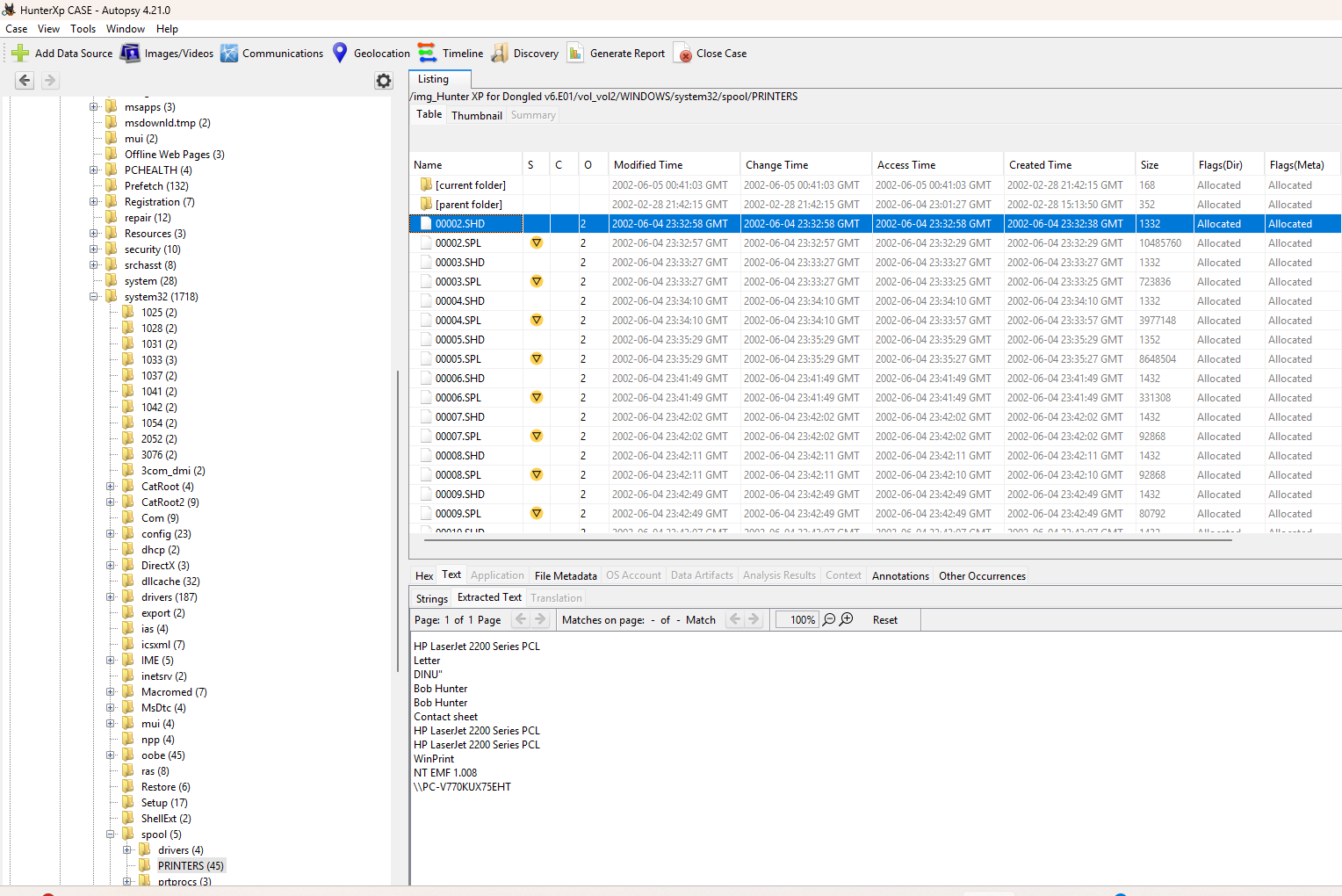
vol\_vol2

WINDOWS

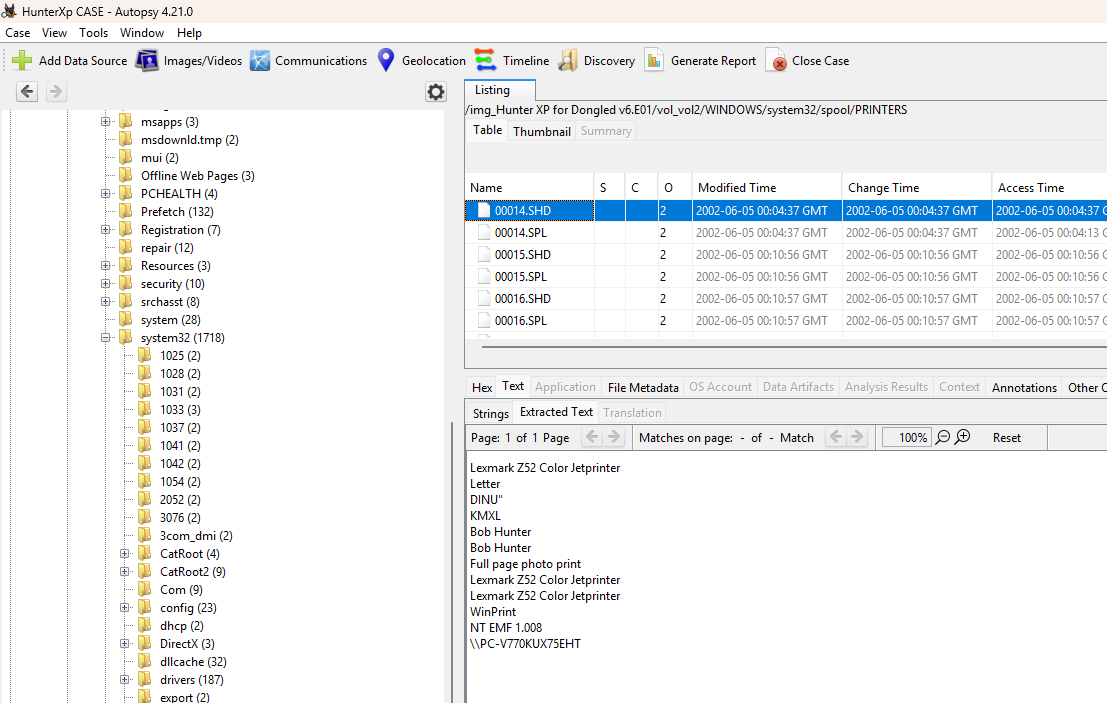
system32

spool

PRINTERS



**MD5: fffa8a311f7c26dd5adf9c17f5ba000a**



**Md5: 9e178a42cf4232139187a2a794a5899**

After investigating this folder, I found that there is two types of printer is used that is;

1. **HP LaserJet 2200 Series PCL Printer**
2. **Lexmark Z52 Color Jetprinter**
   1. **CD/DVD Burning application**

**IMAPI** application is used for CD/DVD burning. The artifacts of CD/DVD burning is stored in System32 file and prefetch folders.

**img\_Hunter XP for Dongled v6.E01**

**vol\_vol2**

**WINDOWS**

**system32**

path for prefetch Files:

**img\_Hunter XP for Dongled v6.E01**

**vol\_vol2**

**WINDOWS**

**Prefetch**



fig1

Fig2

**MD5:f6069827b0a39dc75d251cfb37c4e9c9** (fig1) **Md5:0b4a4eb2c3ae3bf4c6503d0d52185b91 (**fig2**)**

1. **Miscellaneous**
2. **Ransom Artifacts:**

**A screenshot of a computer

Description automatically generatedA screenshot of a computer

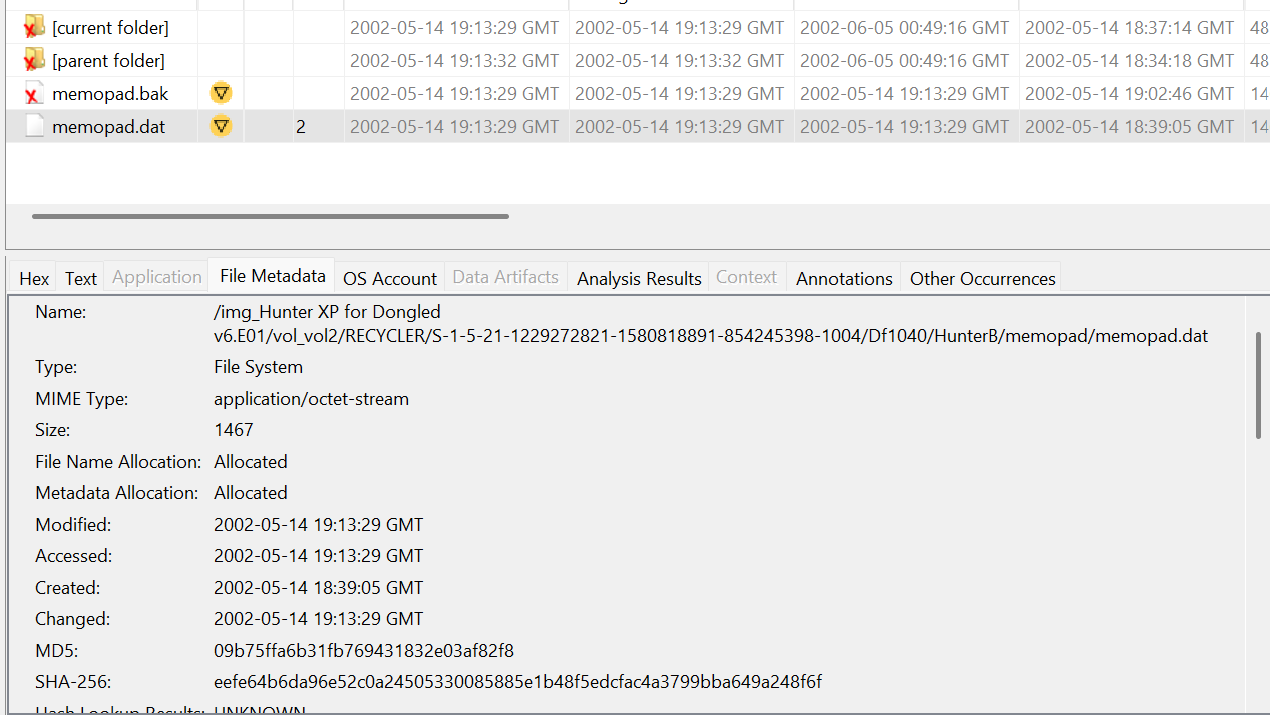
Description automatically generated**

This message shows the demand of $1 million of extorsion money by the criminals.

1. **Ransom Bargaining**

A screenshot of a computer

Description automatically generated



This information shows the bargaining of ransom money.

1. **Conclusion**

Investigation on the provided image **Hunter XP for Dongled v6.E01** provides the activities and evidence stored on the system to find illegal and malicious activities done by the users. The investigation is done by using different forensics tools and its integrity was established by analyzing its hashes by using ‘Autopsy’ and ‘Access Data FTK Imager’.

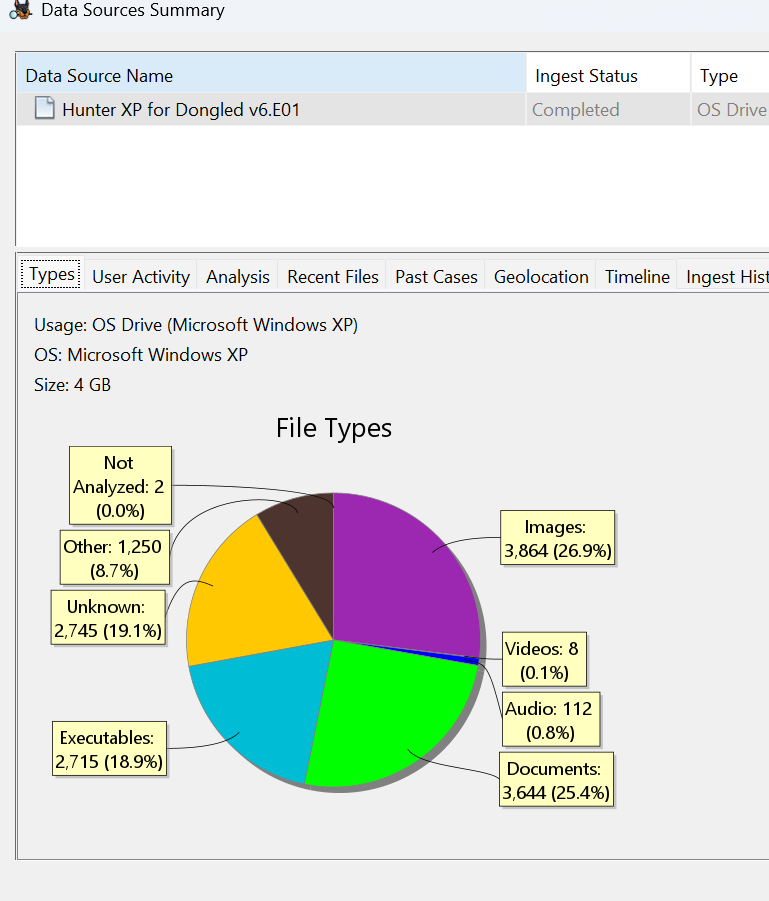
Investigation of this evidence file provides critical information about the operating system (Windows XP), User accounts (Bob Hunter), evidence of 2932 deleted files, many extensions mismatched files, and so on.

The investigation of this file also provides information about the stocking, and also detailed information about demand of $1 million, along with the details of bargaining between victim and criminals.

In conclusion, the investigation of the evidence file provides the suspicious activities of the users on the system. Investigation of the evidence file **Hunter XP for Dongled v6.E01** states that the users have performed extorsion, stocking, CD/DVD burning, disk wiping which shows the suspicious and criminal activities.

1. **Appendix**

These are the artifacts that are extracted from autopsy Data Source Summary.

****

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**