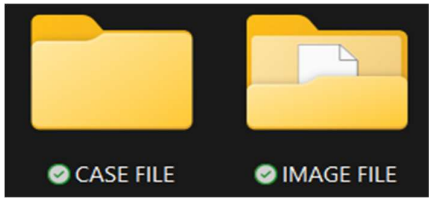
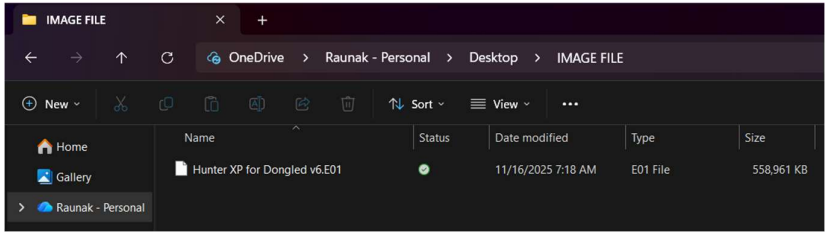
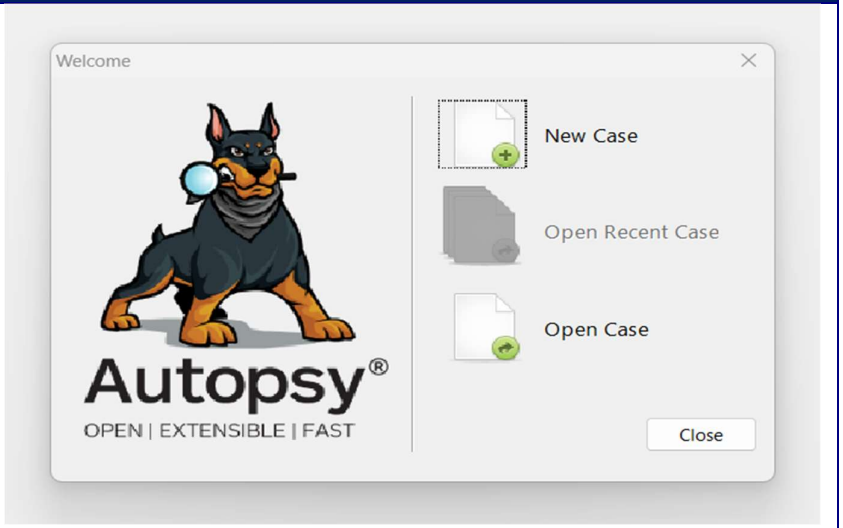
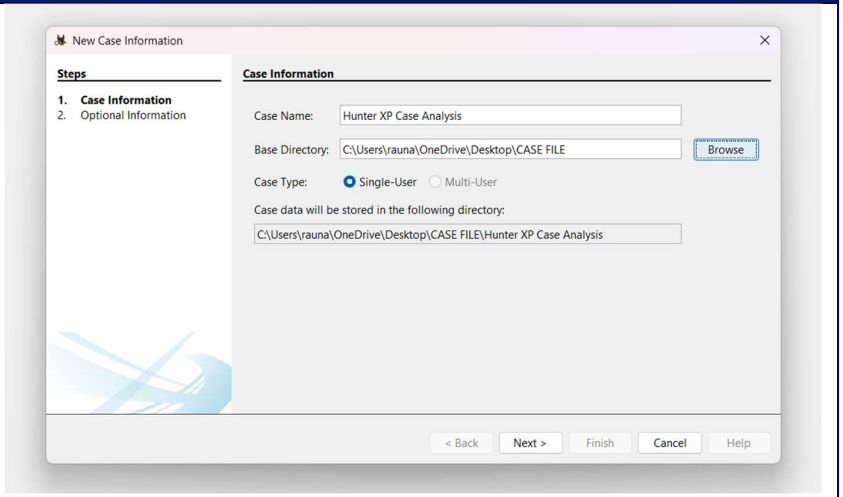
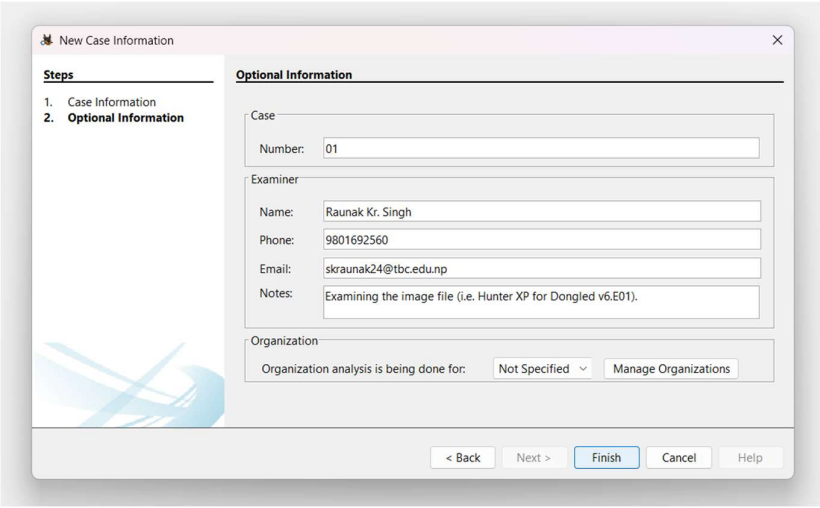
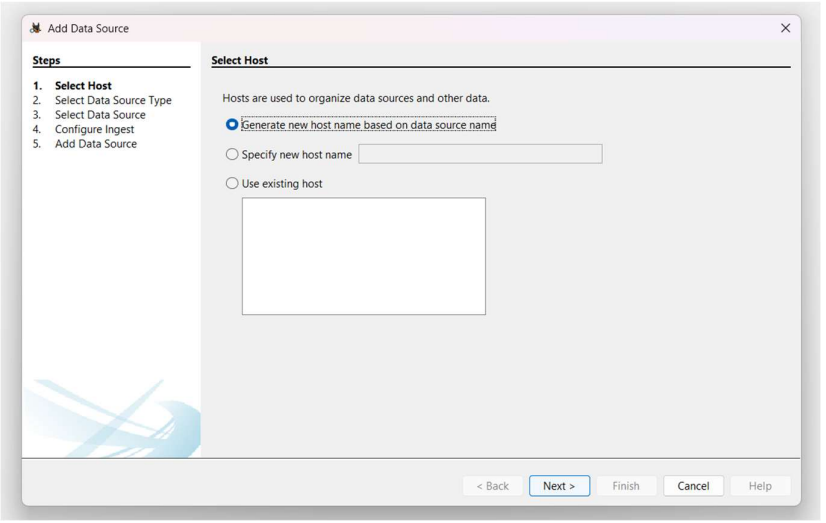
Contemporaneous Notes

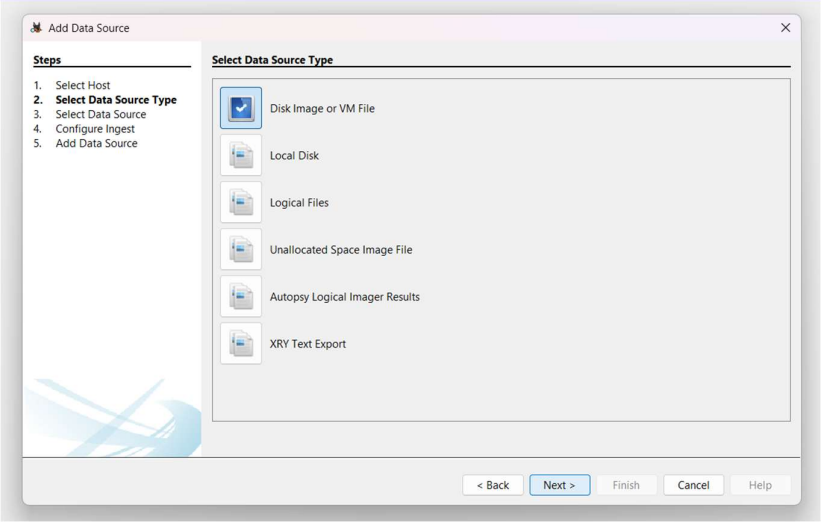
Examiner	Name: **Raunak Kr. Singh** Email: raunak2.singh@live.uwe.ac.uk UWE ID**: 24071246**	Exam commenced	2025/12/8 – 2025/12/16
Other relevant information	1. The given Hunter XP case image file was investigated. The steps are listed below along with the screenshots of each in detail. 2. Additional artefacts studied and analysed.	Software used, versions and licensing	Autopsy v4.22.1 RegRipper v3.0-master AccessData FTK Imager v4.7.1 AccessData Registry Viewer v1.8.0.5 (DEMO) 7-Zip File Manager v25.01 Ophcrack 3.8.0 Hex Editor (HxD) Oracle VirtualBox v7.2.0 -Kali Linux (Debian x64)

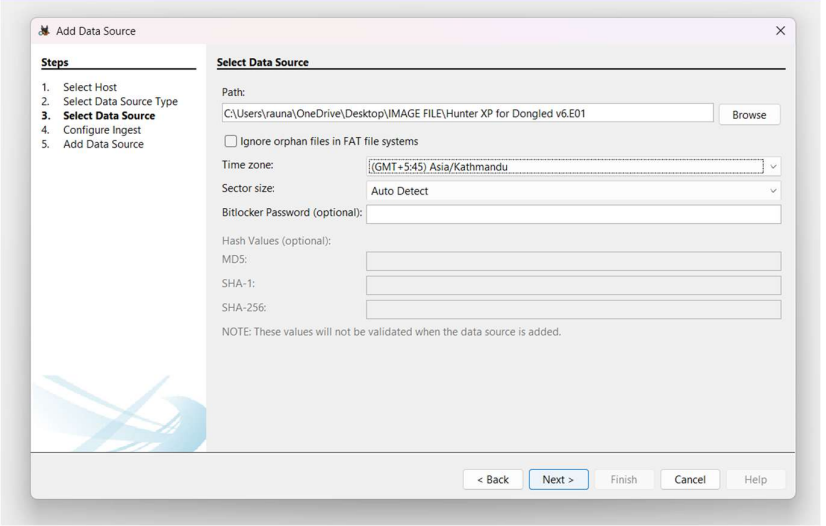
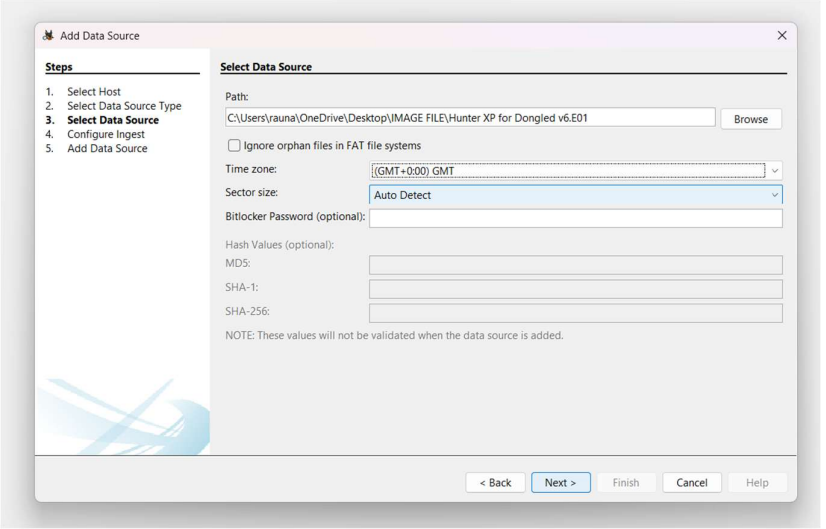
Action	Done?	Date (YY/MM/DD)	Time	Notes
Load case and verify image	Done	2025/12/8	6:00 PM (UTC +5:45)	 Basically, I made 2 folders. **1.Case File – Used for keeping database extracted from Autopsy.** **2.Image File – Used for storing Image file of Hunter XP.**  I opened Autopsy for first time.

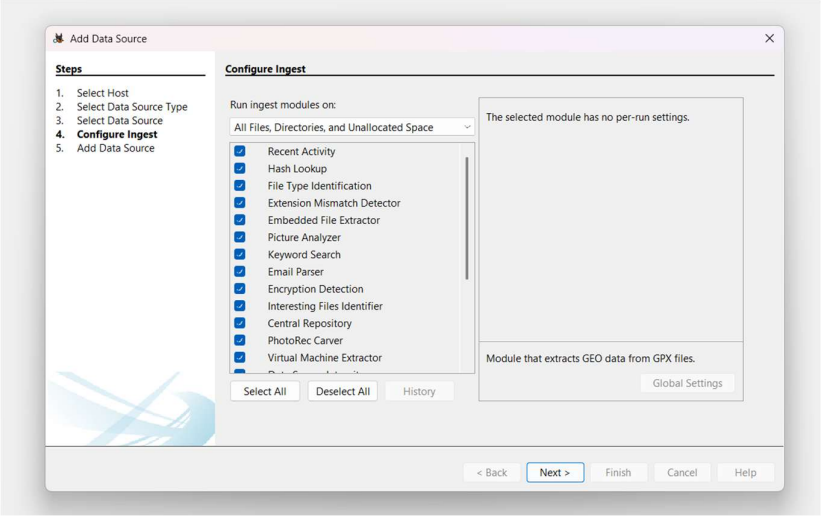
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 I added Case Name and Base Directory. **Case Name: Hunter XP Case Analysis** **Base Directory: Case File (where database is saved)**

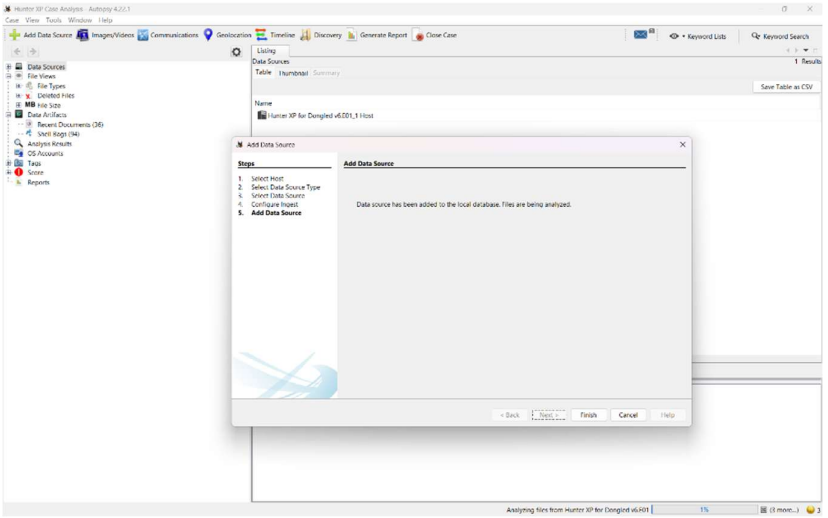
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 I added option information important for the case. 

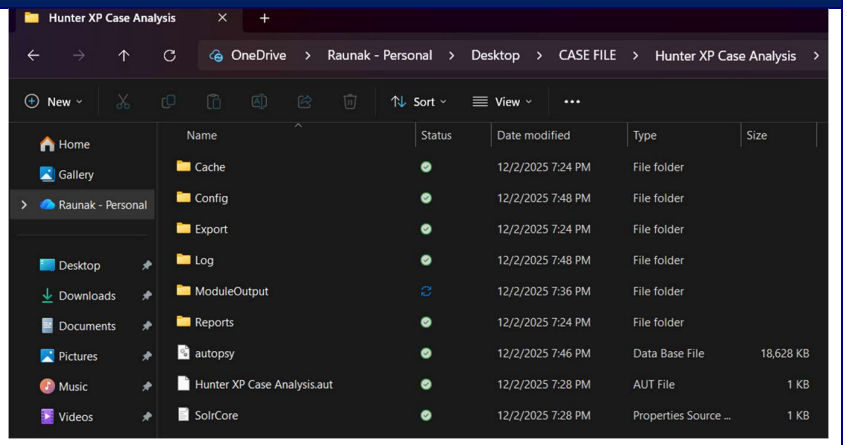
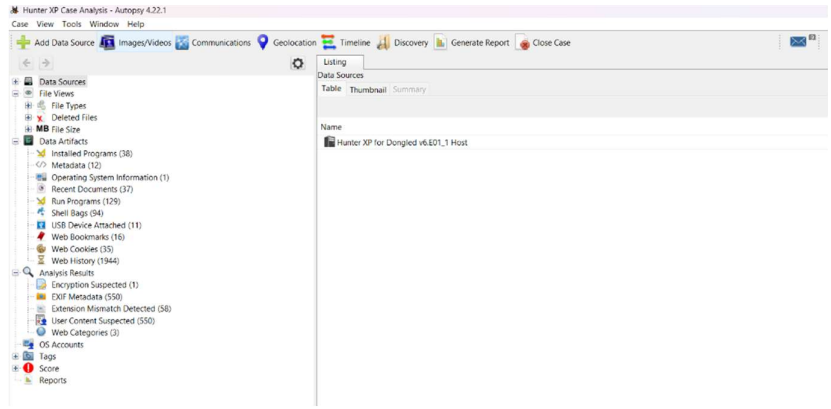
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 I choose disk image because the give file is an image file of Hunter XP.

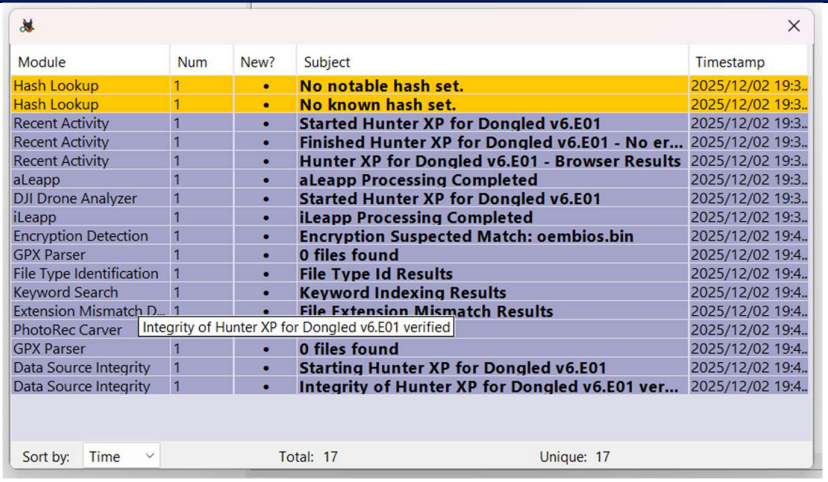
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 I added the data source. **Path: Image File>Hunter XP for Dongled v6. E01** **Time zone: (GMT +0:00) GMT (Adjusted)**

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 

Action	Done?	Date (YY/MM/DD)	Time	Notes
				I configured required ingest module for the case for further investigation. They are: • **Recent Activity** • **Hash Lookup** • **File Type Identification** • **Extension Mismatch Detector** • **Embedded File Extractor** • **Picture Analyzer** • **Keyword search** • **Email Parser** • **Encryption Detection** • **Interesting Files Identifier** • **Central Repository** • **PhotoRec Carver** • **Data Source Integrity** • **GPX Parser** 

Action	Done?	Date (YY/MM/DD)	Time	Notes
				Now, finally I am adding database to Case File Folder.   Here, Finally the database is added to **CASE FILE**.

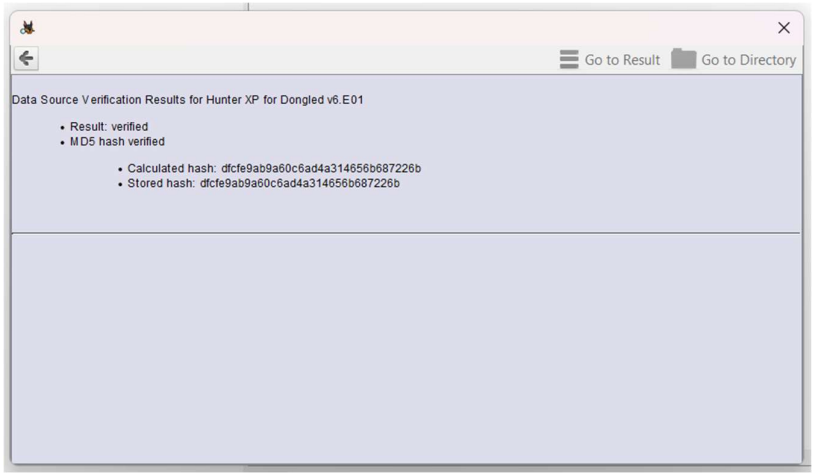
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Now, I clicked on the mail icon for further process.  Required Hash Value for Data Integrity has been obtained.

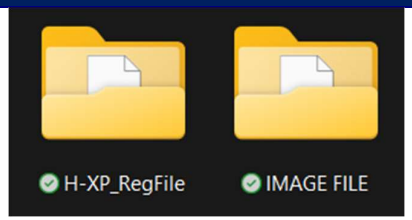
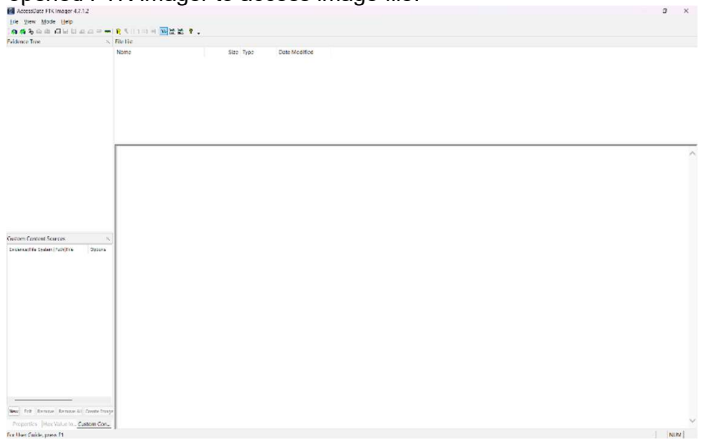
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

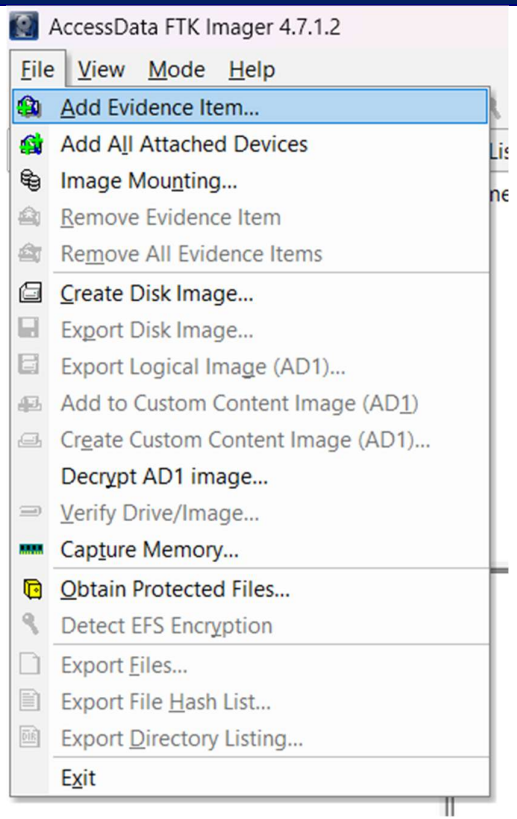
Module	Num	New?	Subject	Timestamp
Hash Lookup	1	•	**No notable hash set.**	2025/12/02 19:3..
Hash Lookup	1	•	**No known hash set.**	2025/12/02 19:3..
Recent Activity	1	•	**Started Hunter XP for Dongled v6.E01**	2025/12/02 19:3..
Recent Activity	1	•	**Finished Hunter XP for Dongled v6.E01 - No er...**	2025/12/02 19:3..
Recent Activity	1	•	**Hunter XP for Dongled v6.E01 - Browser Results**	2025/12/02 19:3..
aLeapp	1	•	**aLeapp Processing Completed**	2025/12/02 19:3..
DJI Drone Analyzer	1	•	**Started Hunter XP for Dongled v6.E01**	2025/12/02 19:3..
iLeapp	1	•	**iLeapp Processing Completed**	2025/12/02 19:3..
Encryption Detection	1	•	**Encryption Suspected Match: oembios.bin**	2025/12/02 19:4..
GPX Parser	1	•	**0 files found**	2025/12/02 19:4..
File Type Identification	1	•	**File Type Id Results**	2025/12/02 19:4..
Keyword Search	1	•	**Keyword Indexing Results**	2025/12/02 19:4..
Extension Mismatch D...	1	•	**File Extension Mismatch Results**	2025/12/02 19:4..
PhotoRec Carver			Integrity of Hunter XP for Dongled v6.E01 verified	2025/12/02 19:4..
GPX Parser	1	•	**0 files found**	2025/12/02 19:4..
Data Source Integrity	1	•	**Starting Hunter XP for Dongled v6.E01**	2025/12/02 19:4..
Data Source Integrity	1	•	**Integrity of Hunter XP for Dongled v6.E01 ver...**	2025/12/02 19:4..

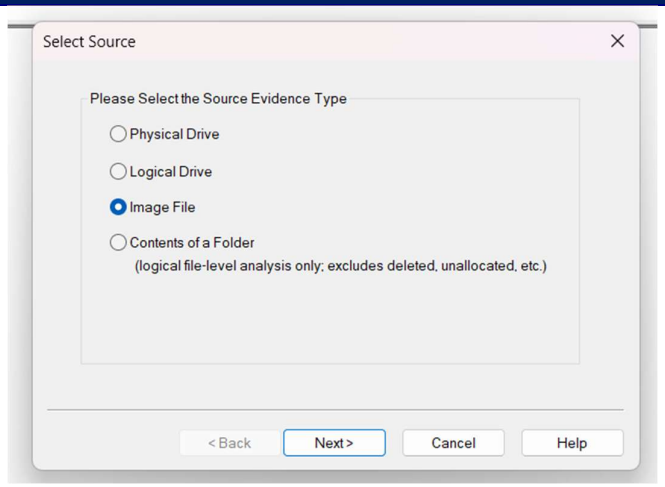
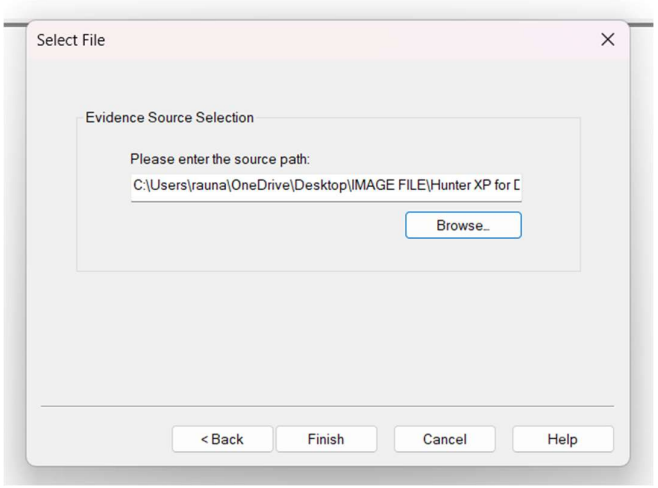
Sort by: Time Total: 17 Unique: 17

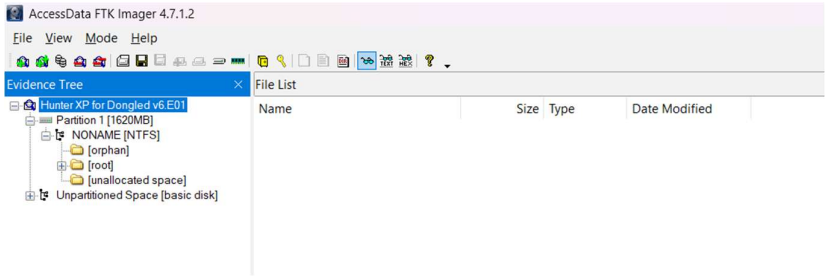
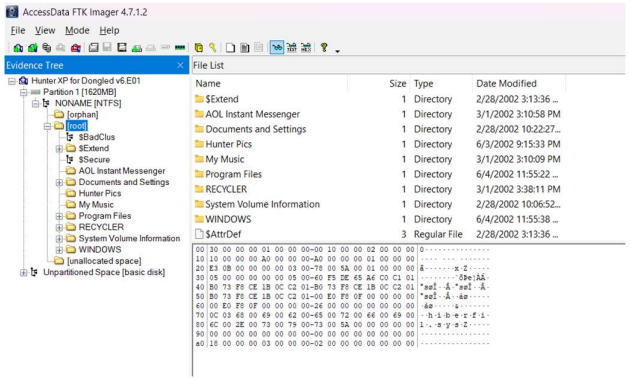
Here is the required hash value which will show the integrity throughout the investigation.

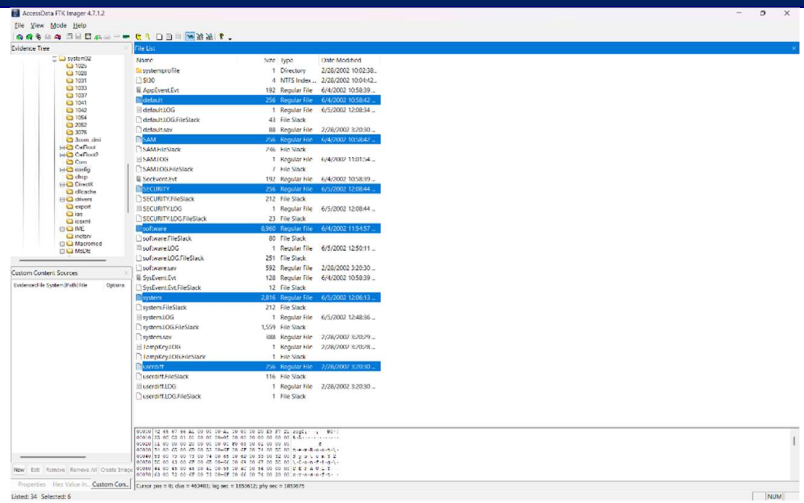
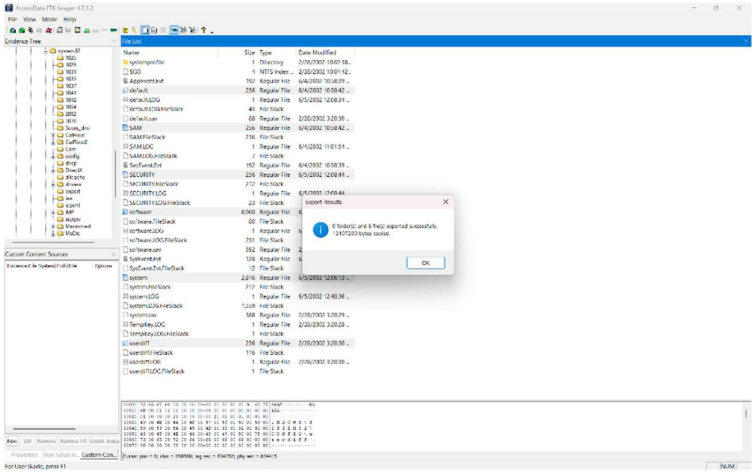


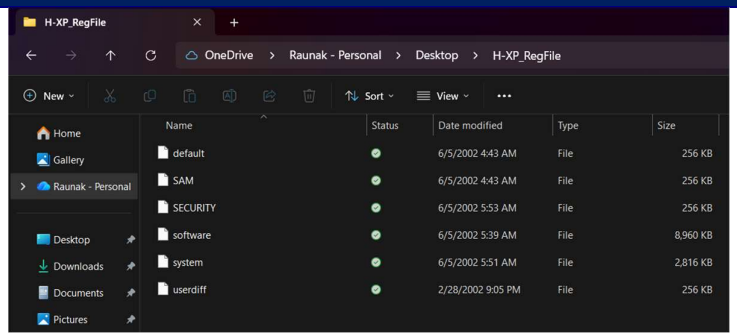
Action	Done?	Date (YY/MM/DD)	Time	Notes
Load Case into second forensic tool for dual verification of at least 2 key artefacts, evidence items	Done	2025/12/8	7:00 PM (UTC +5:45)	 Basically, Here I Created 2 folders. **1.H-XP_RegFile – Used for storing extracted Registry from the image.** **2.Image File – Used for storing Hunter XP Image file.** Now, I opened FTK Imager to access image file.  I added evidence item here.

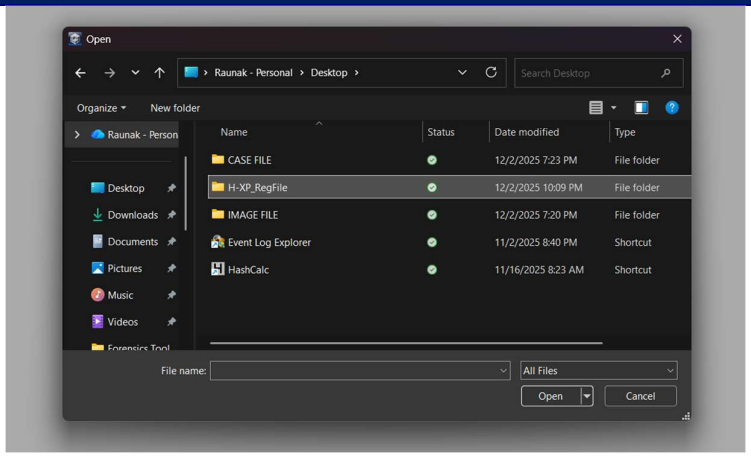
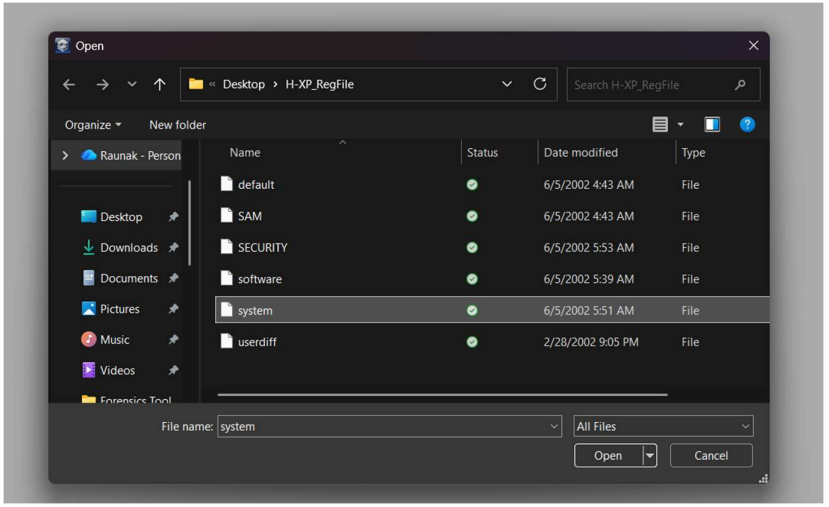
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 As Hunter XP being an image file so while adding evidence item I selected Image file.

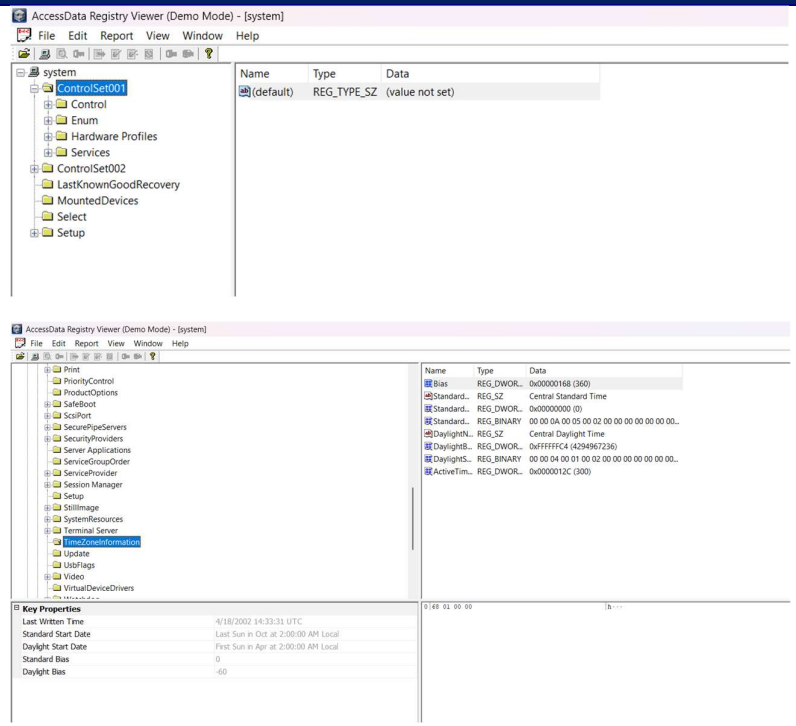
Action	Done?	Date (YY/MM/DD)	Time	Notes
				  Process to access Registry File from this image. **Partition 1>ROOT>WINDOWS>SYSTEM32>CONFIG**

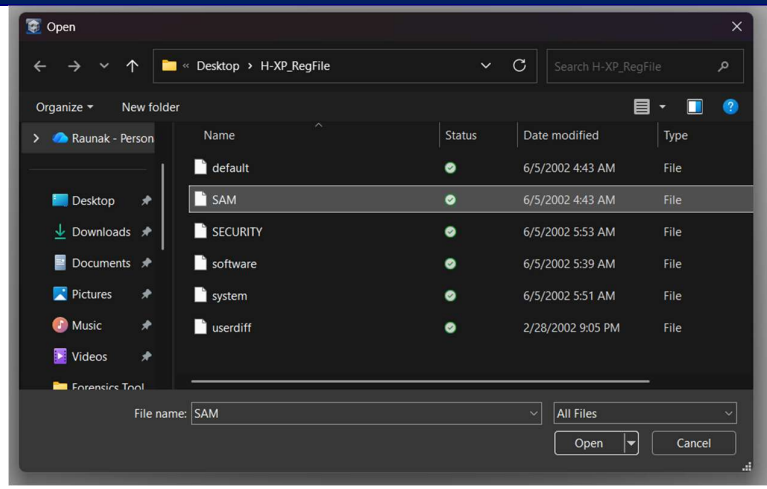
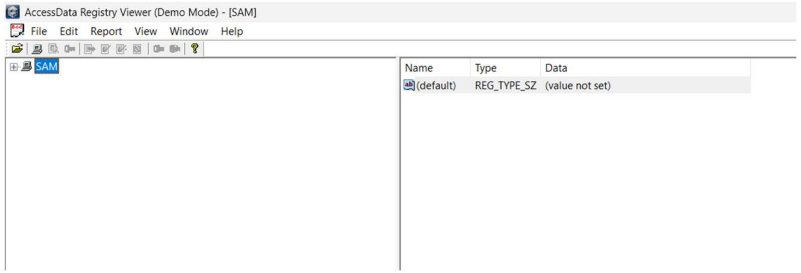
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 

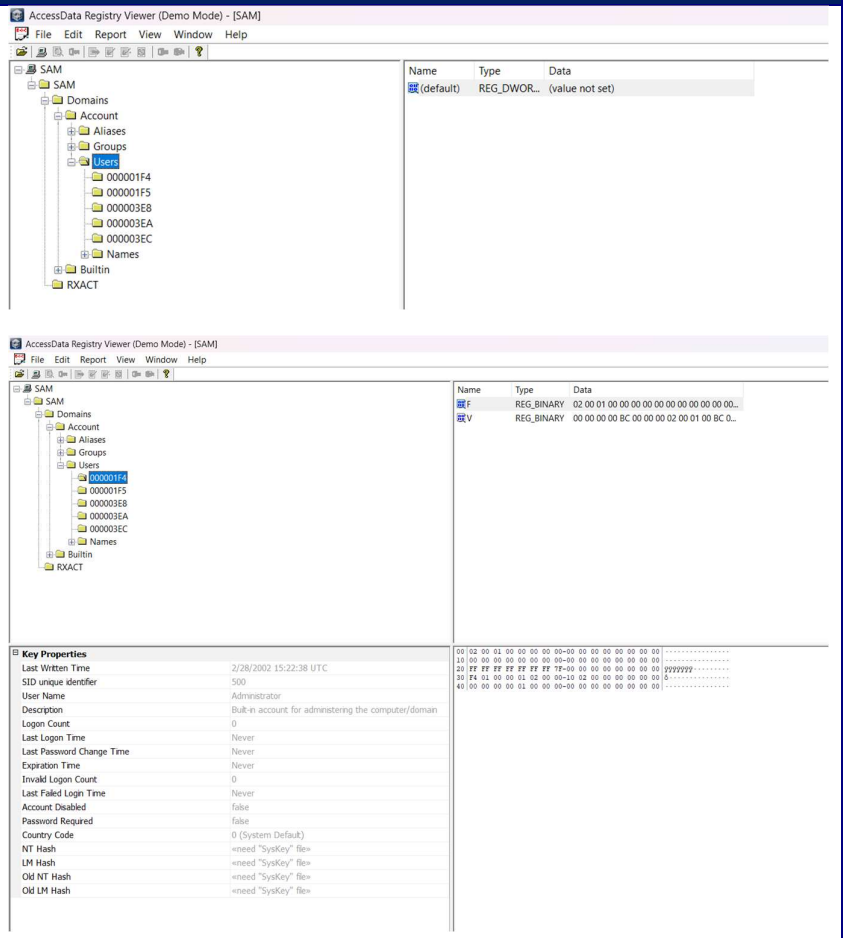
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Finally, I exported these registry files.  Location of the exported Registry file: **Desktop>H-XP_RegFile**

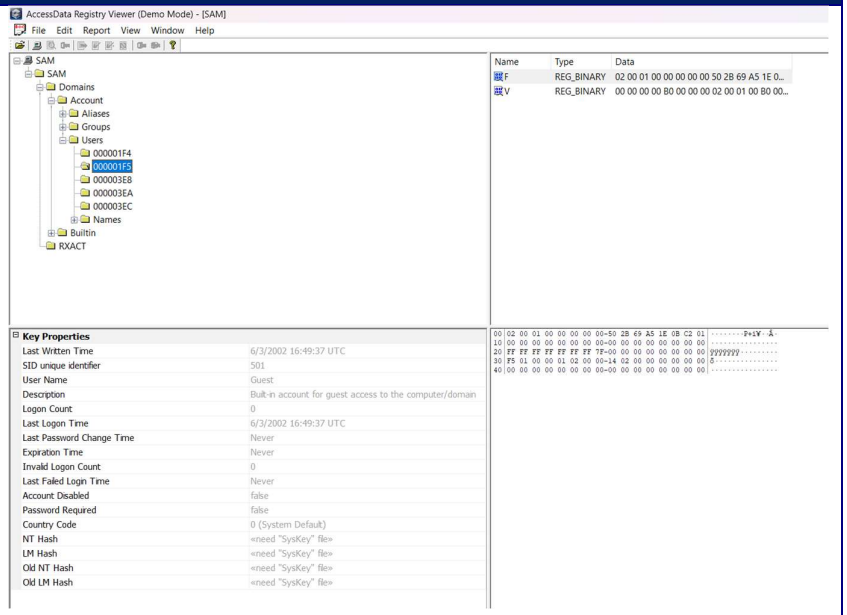
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Now, I opened Registry Viewer. 

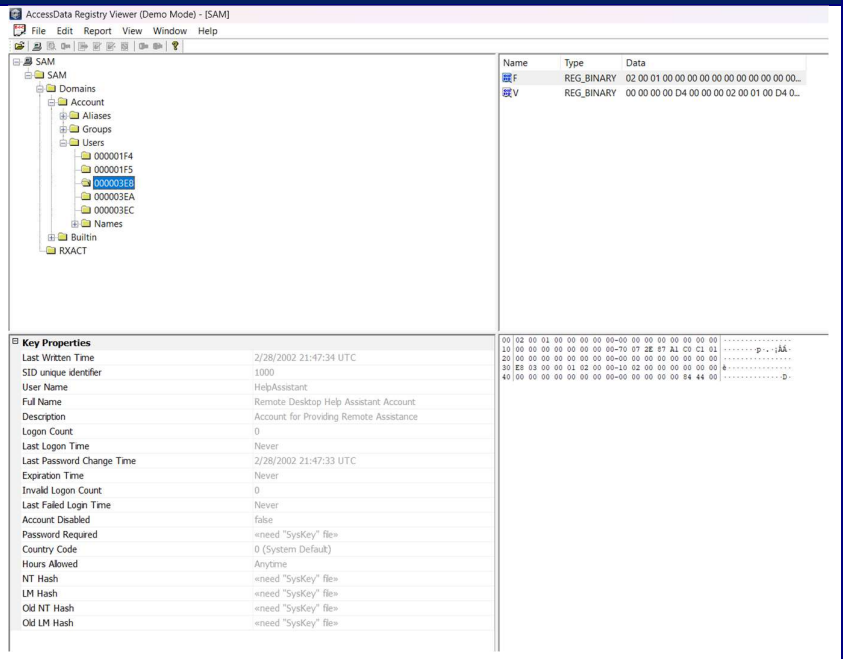
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 I loaded System Registry file to view information about Time Zone.  Process to reach till Time Zone: **System>ControlSet001>Control>TimeZoneInformation**

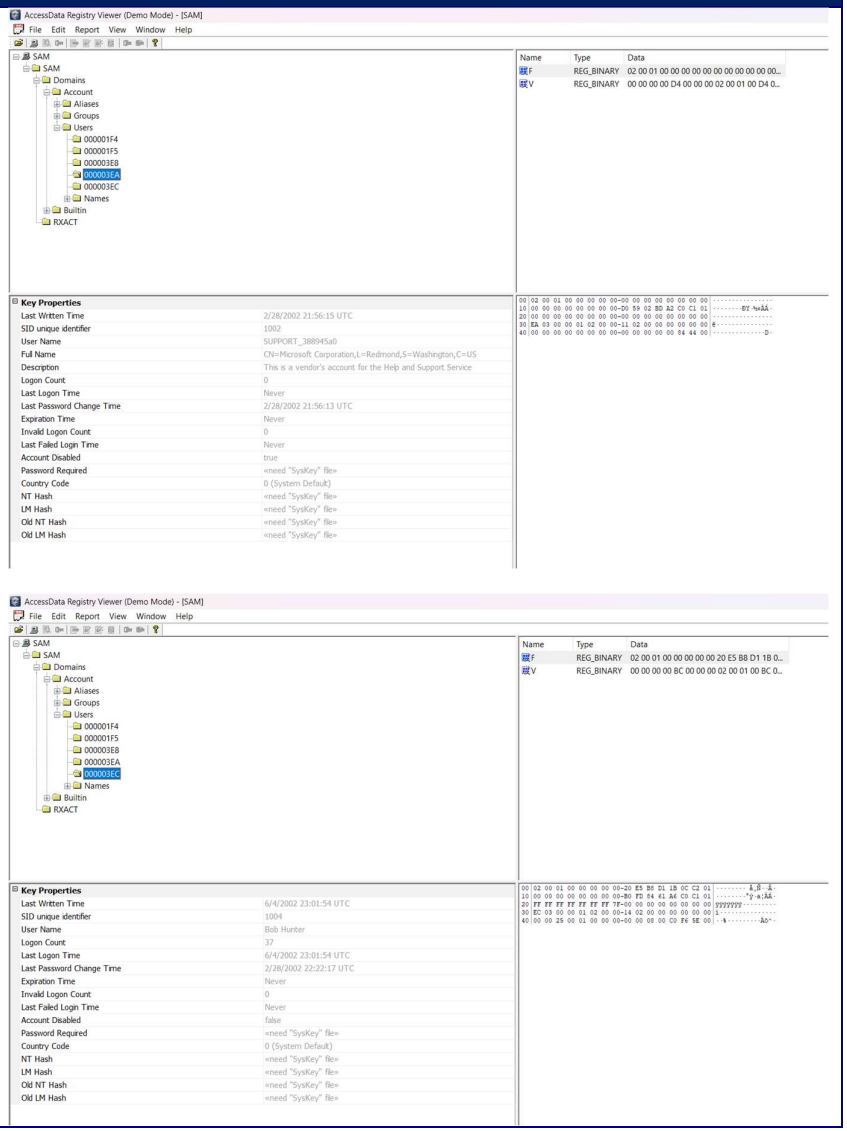
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Now, I loaded Sam Registry File in the registry viewer to access information about users.

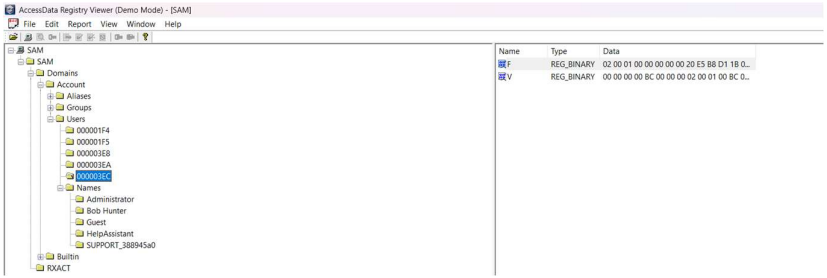
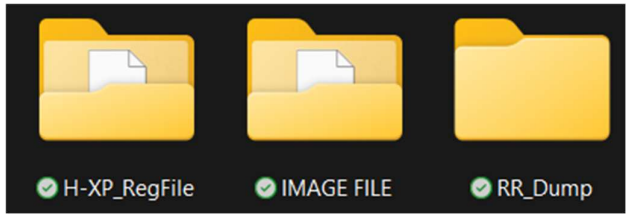
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Process to access Users: **Sam>Domains>Users** 

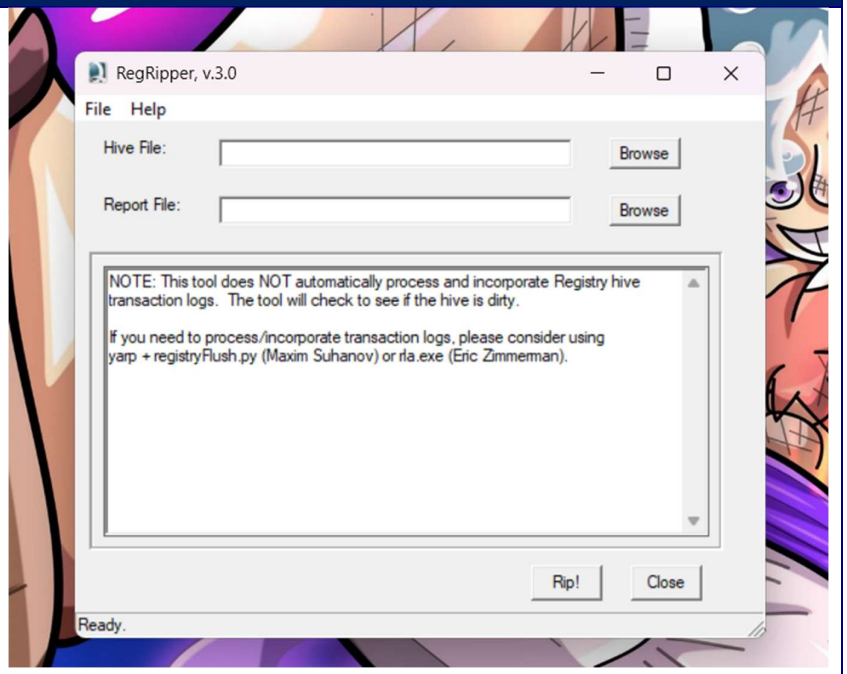
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

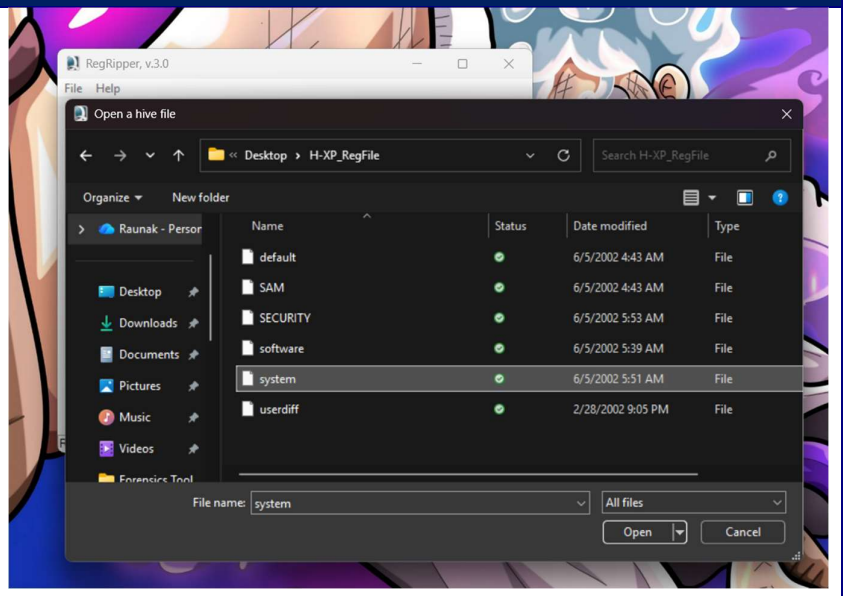
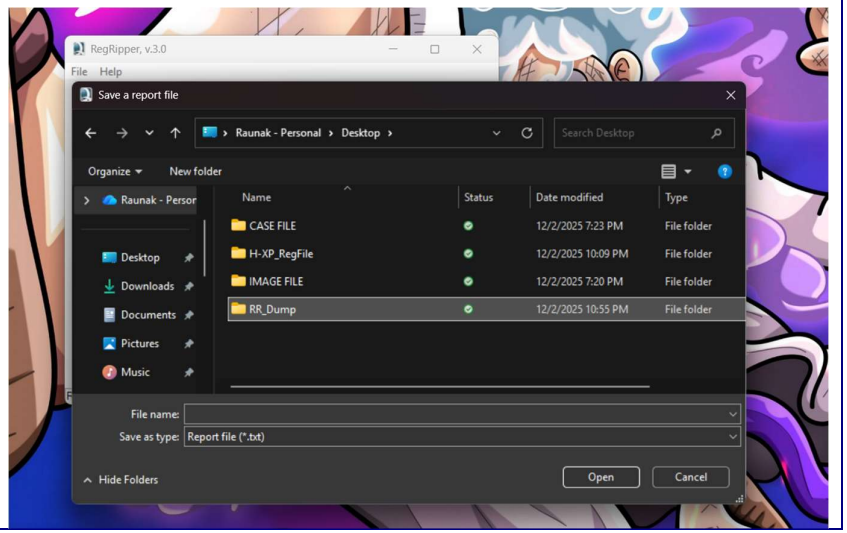
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

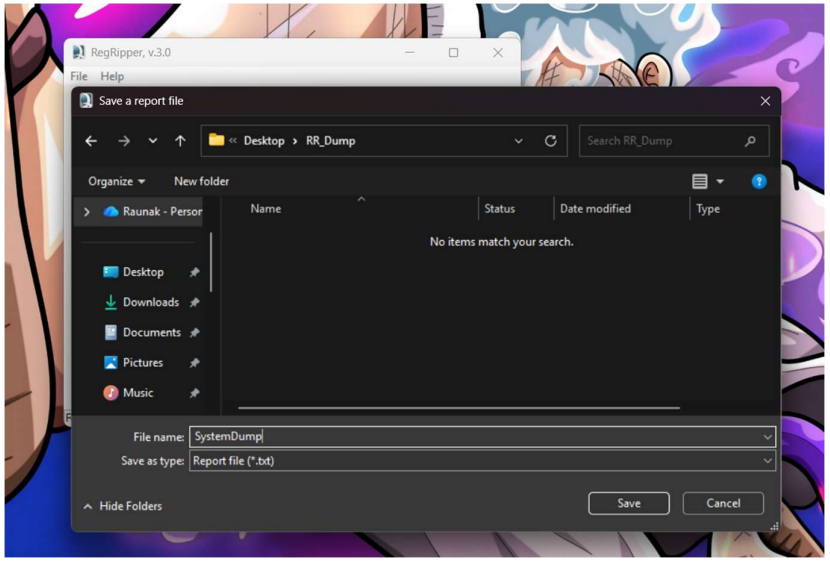
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

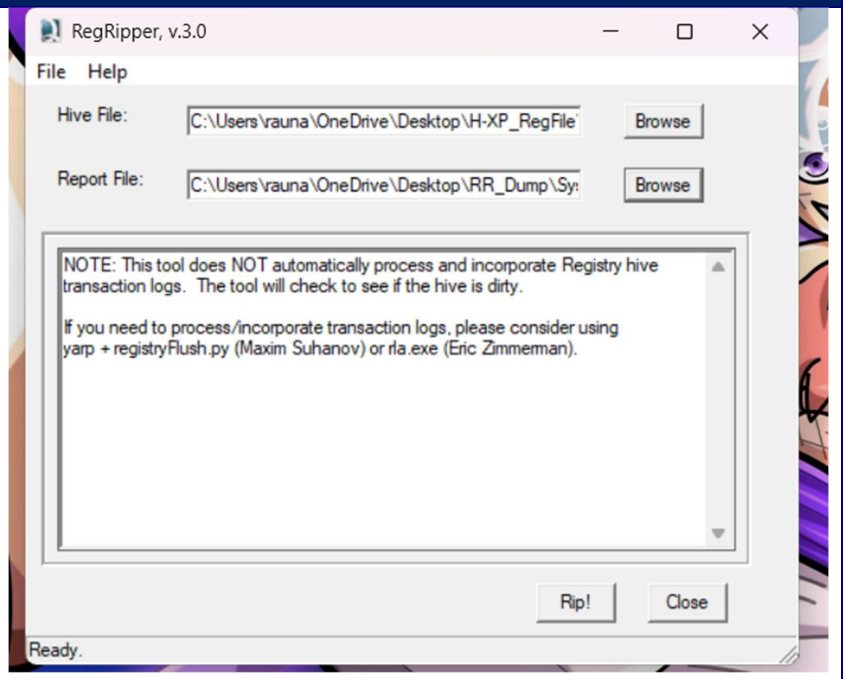
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

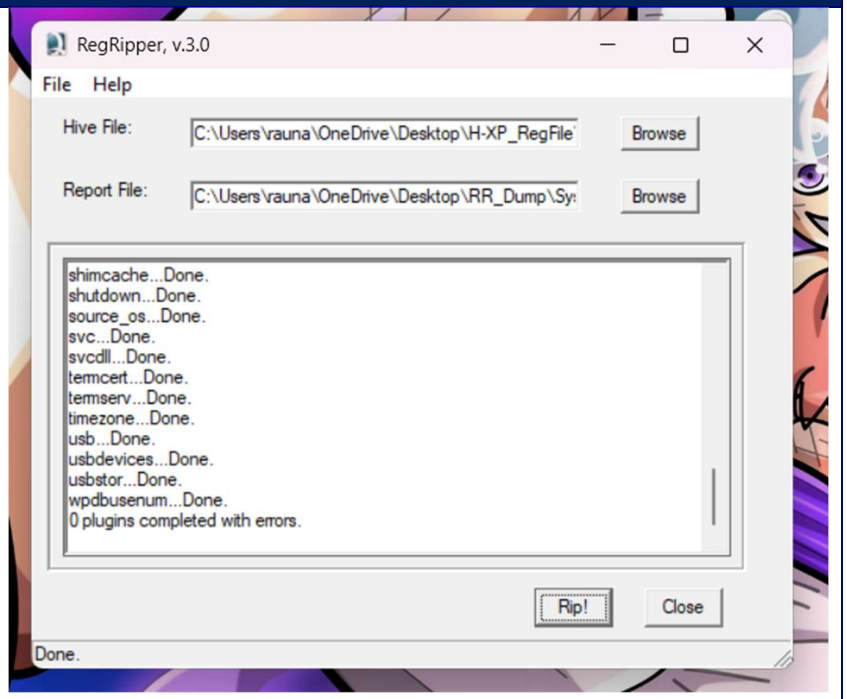
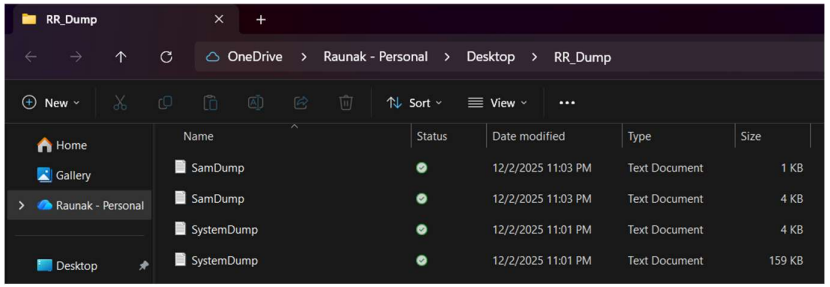
Action	Done?	Date (YY/MM/DD)	Time	Notes
				  Additionally, I made one more folder. **RR_Dump – Used for saving dump file from Reg Ripper.** Now, I opened Reg Ripper to get information about time zone.

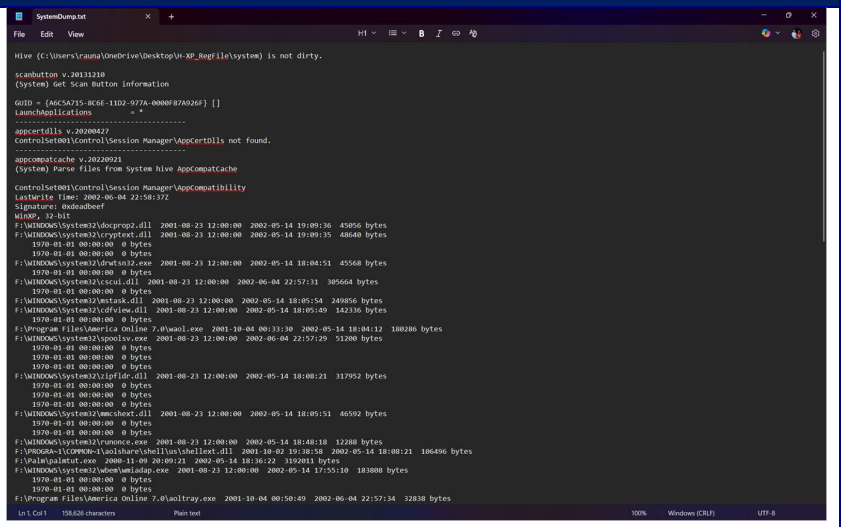
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Now, I loaded System Registry to reg ripper to get detailed information about system in form of .txt.

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 

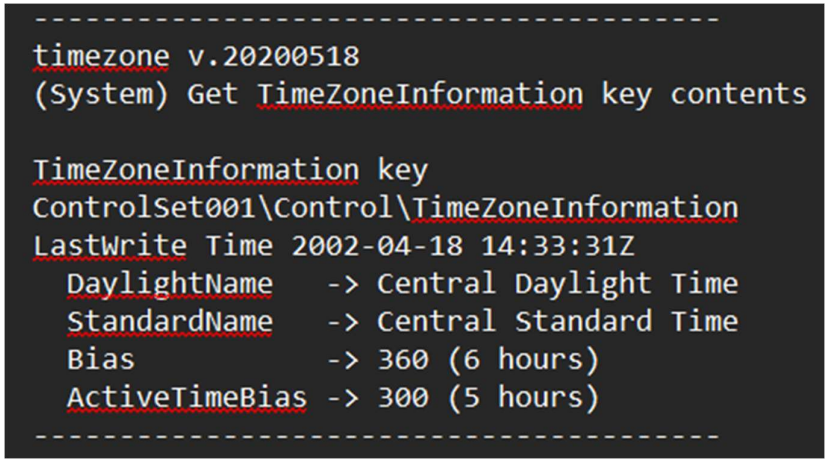
Action	Done?	Date (YY/MM/DD)	Time	Notes
				I saved the dump as SystemDump.txt. 

Action	Done?	Date (YY/MM/DD)	Time	Notes
				

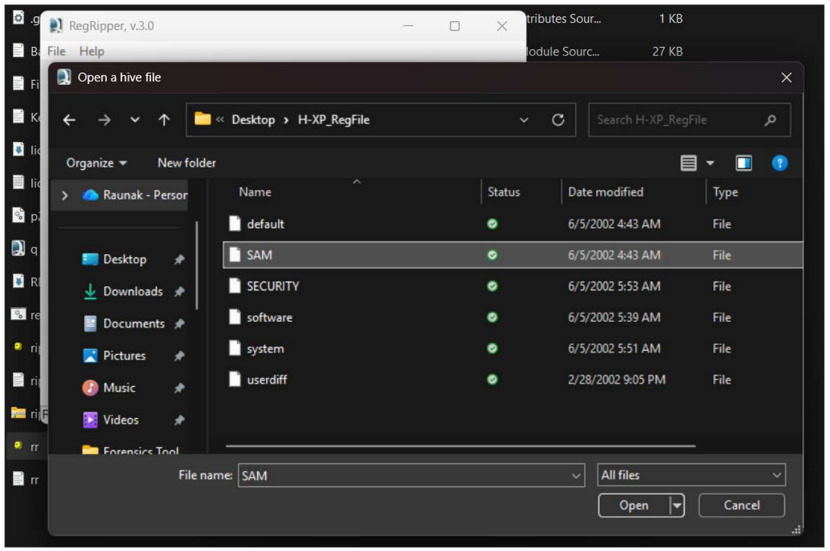
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Finally, System was ripped and we got the .txt file.  I opened SystemDump.txt to get information about Time Zone.

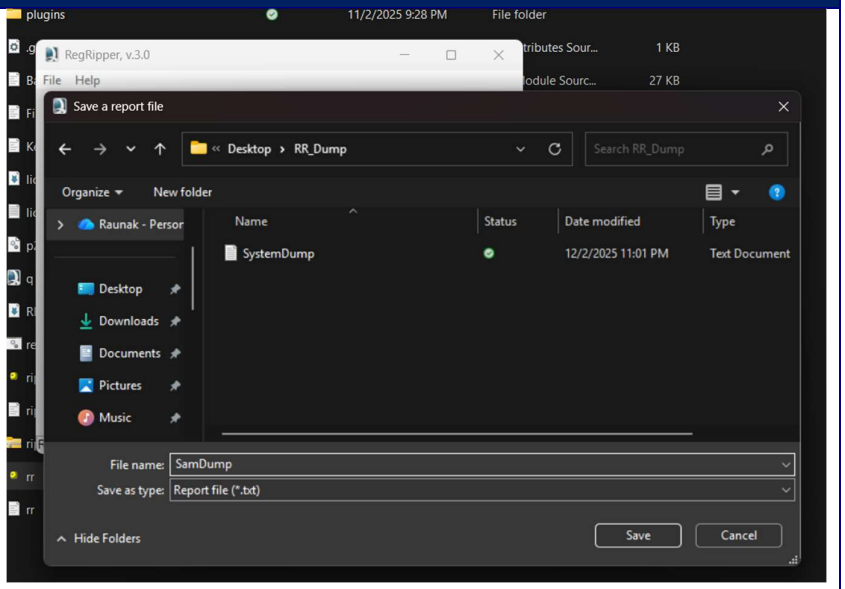
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

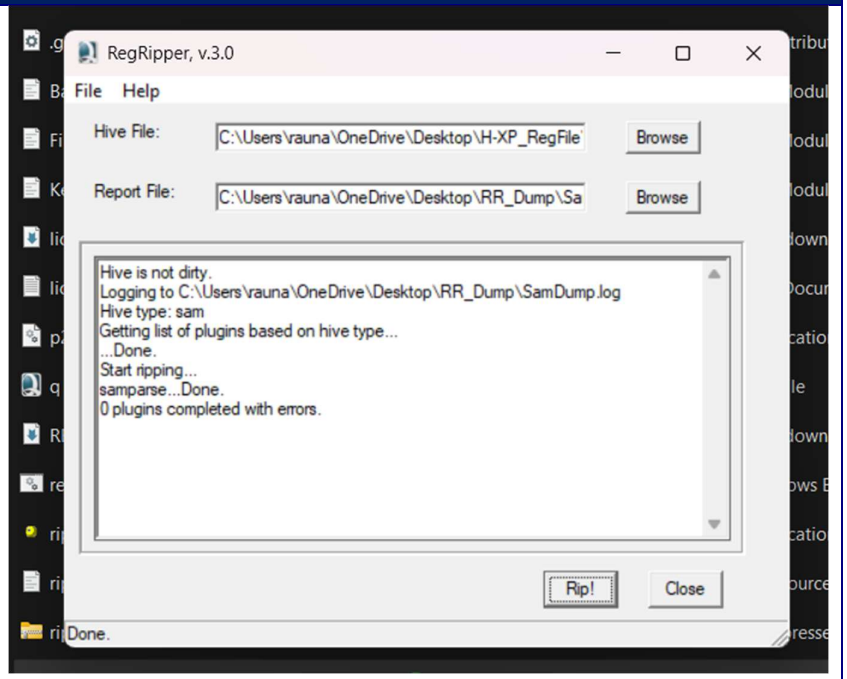
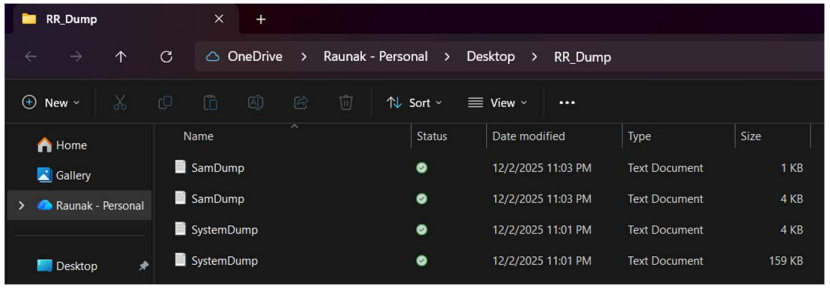
After Scrolling down, I got time zone information.

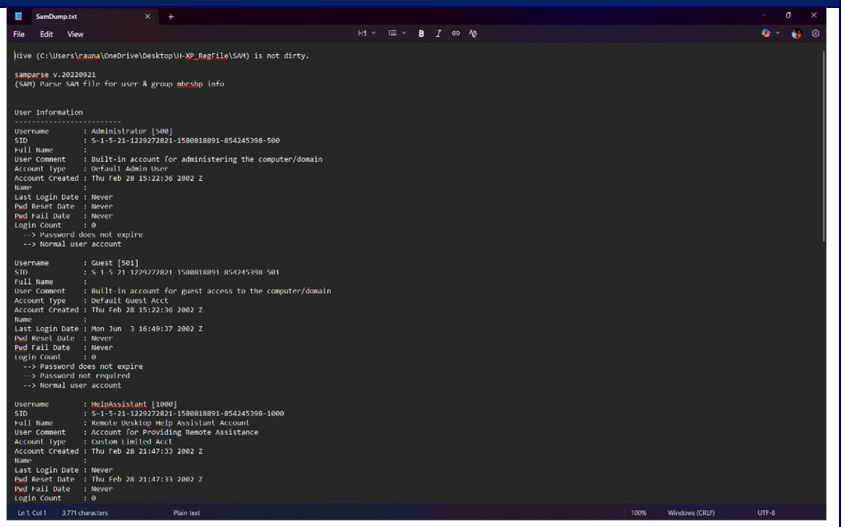


Similarly,
For Sam Registry, I loaded it on reg ripper.

Action	Done?	Date (YY/MM/DD)	Time	Notes
				.  I saved it as SamDump.txt to get information about users.

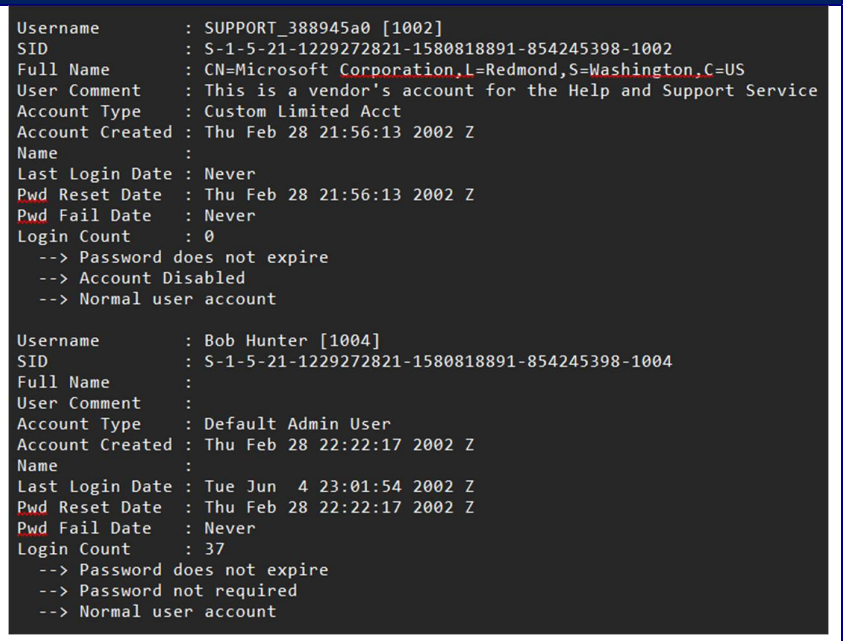
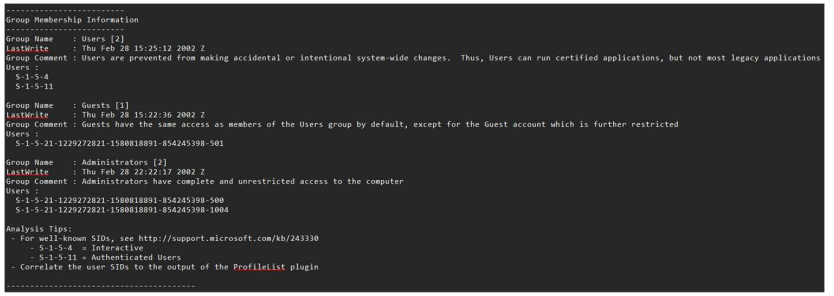
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

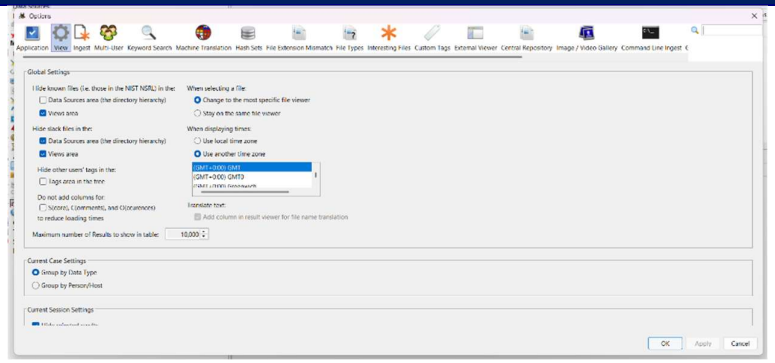
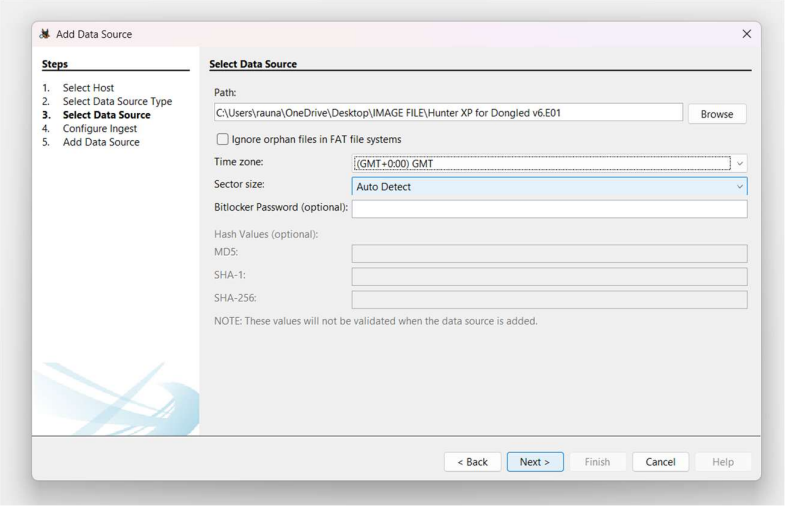
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 I ripped SAM in reg ripper and got detailed information in .txt format.  I opened SamDump.txt and got information about Users.

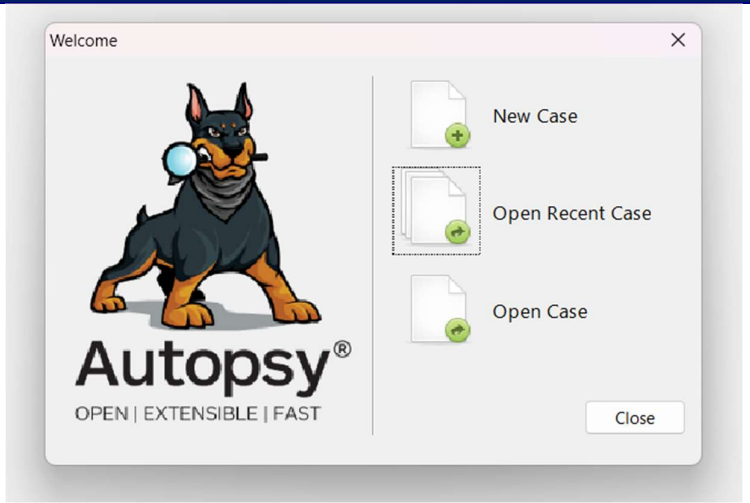
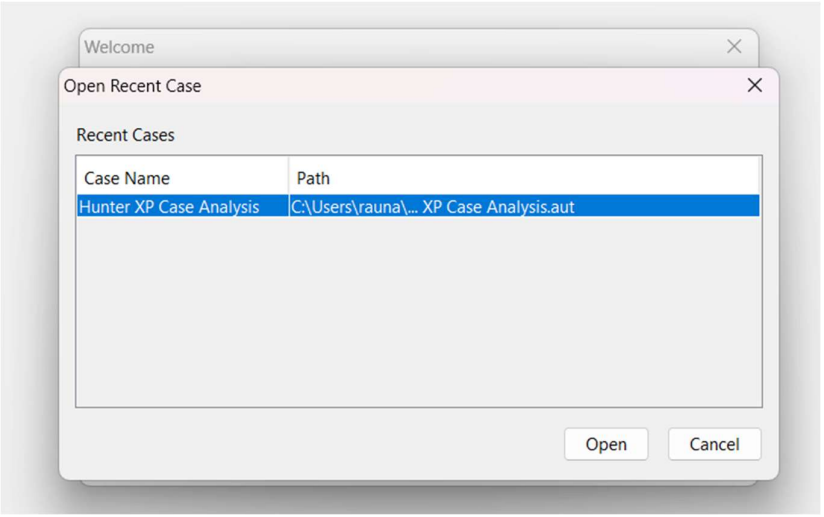
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

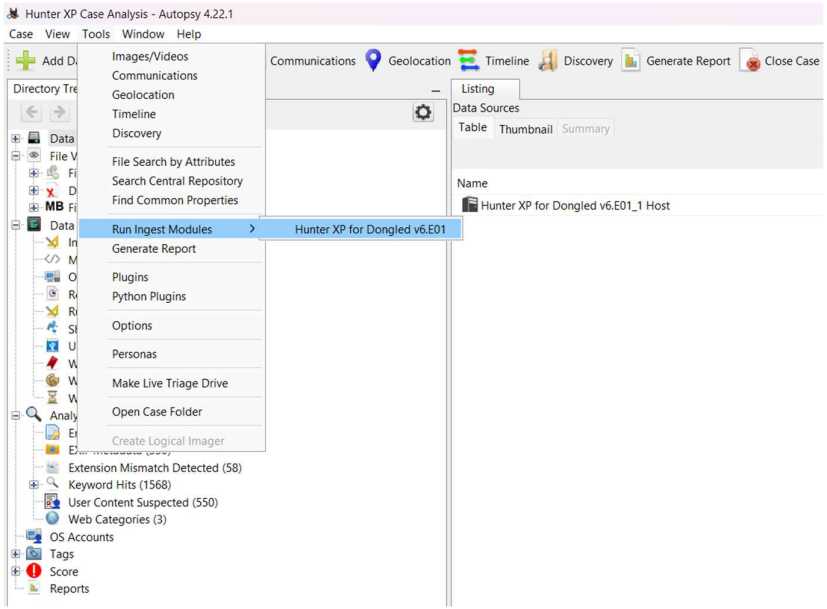
Action	Done?	Date (YY/MM/DD)	Time	Notes

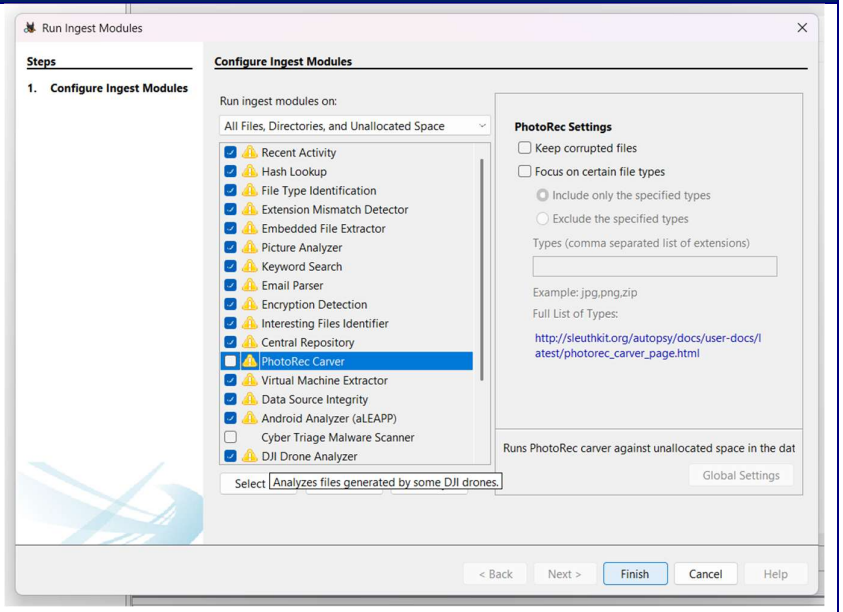
```
User Information
------------------------
Username        : Administrator [500]
SID             : S-1-5-21-1229272821-1580818891-854245398-500
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Thu Feb 28 15:22:36 2002 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account

Username        : Guest [501]
SID             : S-1-5-21-1229272821-1580818891-854245398-501
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Thu Feb 28 15:22:36 2002 Z
Name            :
Last Login Date : Mon Jun  3 16:49:37 2002 Z
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Password not required
  --> Normal user account

Username        : HelpAssistant [1000]
SID             : S-1-5-21-1229272821-1580818891-854245398-1000
Full Name       : Remote Desktop Help Assistant Account
User Comment    : Account for Providing Remote Assistance
Account Type    : Custom Limited Acct
Account Created : Thu Feb 28 21:47:33 2002 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Thu Feb 28 21:47:33 2002 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account
```

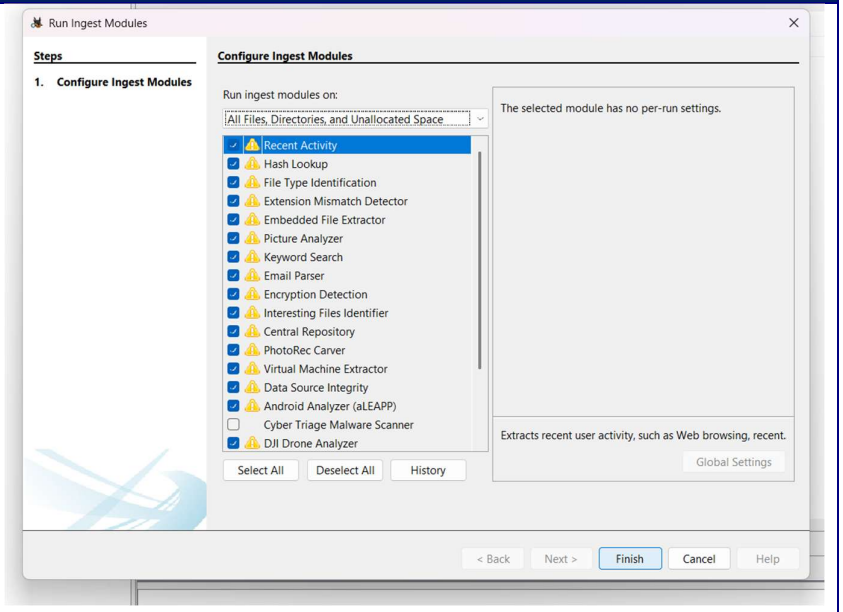
Action	Done?	Date (YY/MM/DD)	Time	Notes
				  Here, I got all information about the users.
Time Zone Adjusted? Report Time Zone used for Analysis.	Done	2025/12/8	6:10 PM (UTC +5:45)	For this we can adjust the time zone at the start of loading the case as shown here. We can adjust time zone as follows: **TOOLS>OPTIONS>VIEW>While Displaying Times**

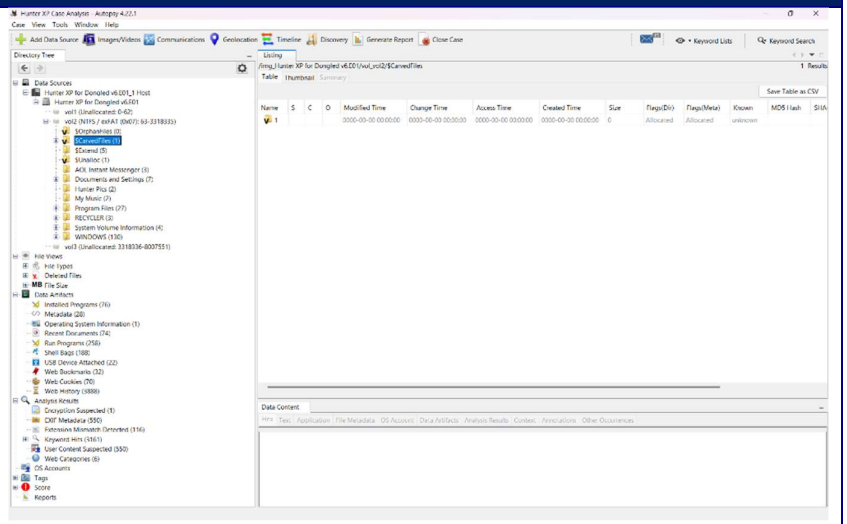
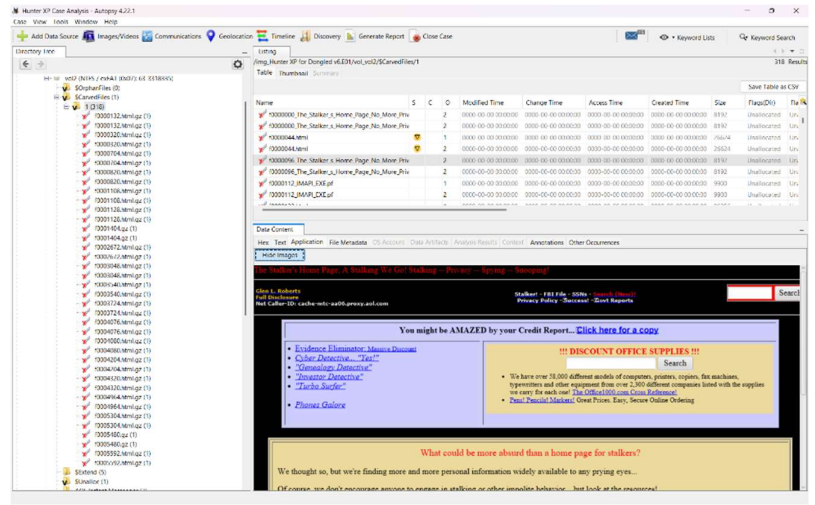
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 While adding the case, we can set it normally by: Process: **Select Data Source>Time Zone**  Time zone used for analysis is **(GMT +0:00) GMT.**

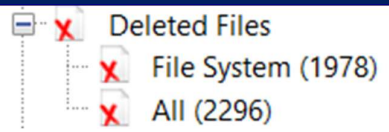
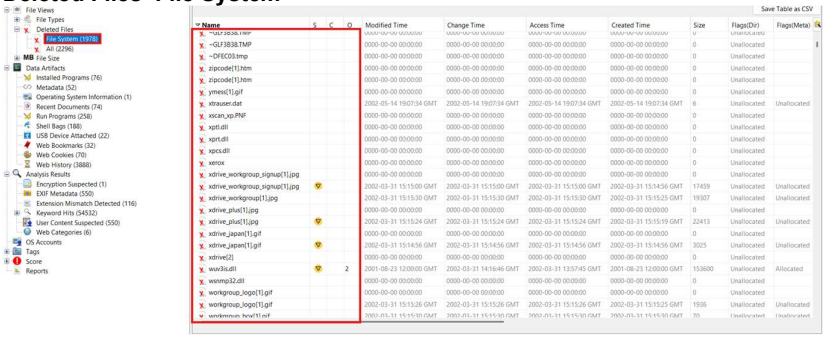
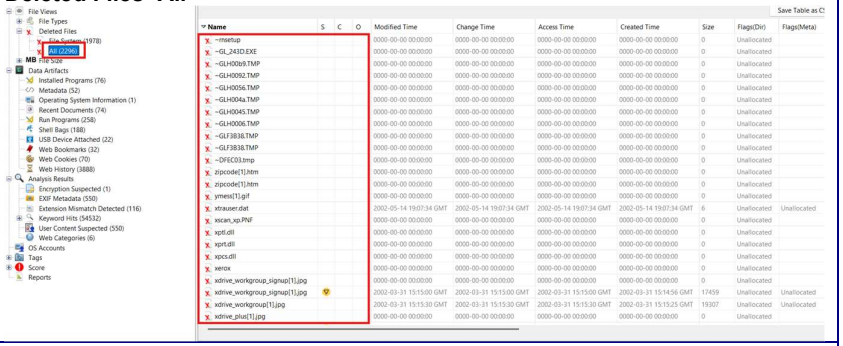
Action	Done?	Date (YY/MM/DD)	Time	Notes
Recover lost folders (NTFS, FAT16&32).	Done	2025/12/9	6:10 PM (UTC +5:45)	 I re-opened the case in Autopsy and did the following actions as shown below. 

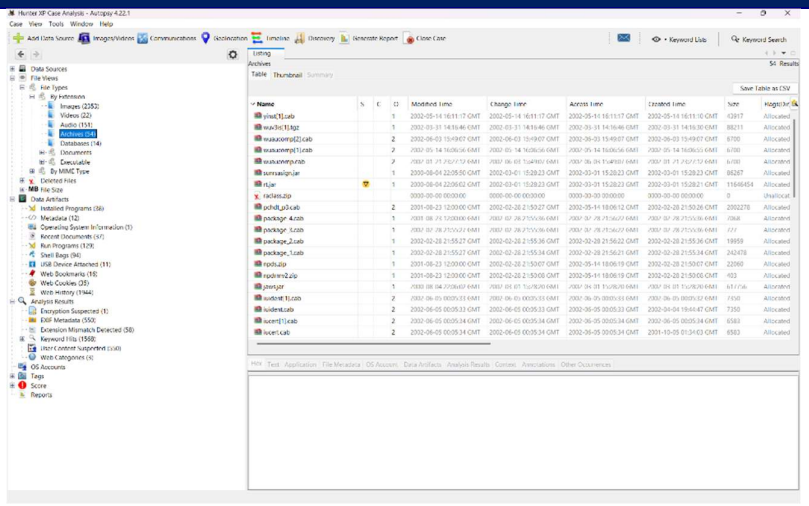
Action	Done?	Date (YY/MM/DD)	Time	Notes
				To recover the lost folders, we go through the procedure of getting access of the lost files in the image. We do that by; **Tools>Run Ingest Modules>PhotoRec Carver** 

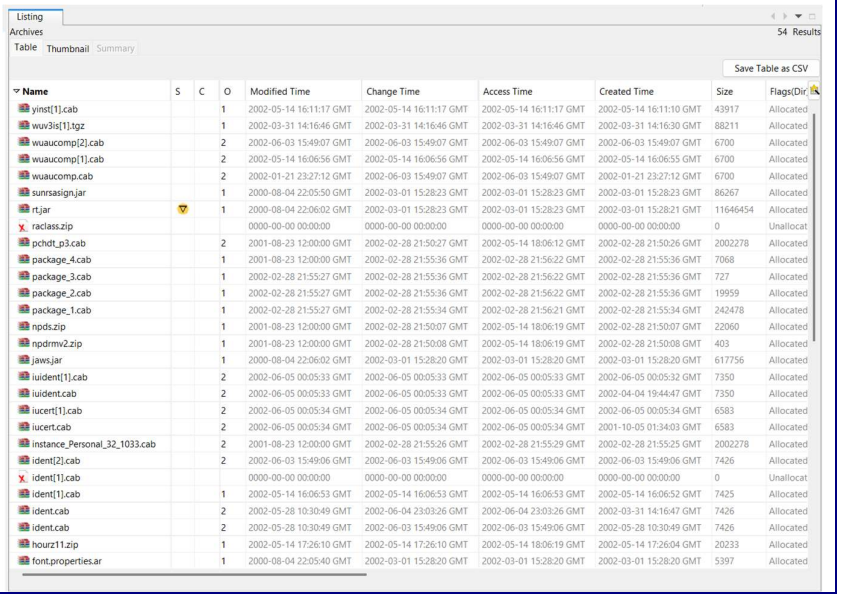
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

Action	Done?	Date (YY/MM/DD)	Time	Notes
				  After selecting PhotoRec Caver Module we click finish and proceed. By selecting PhotoRec Caver we get access to these: Process: **Vol-Vol2>CarvedFiles>1** **Here we have File System with 318 items:**

Action	Done?	Date (YY/MM/DD)	Time	Notes
				  Here, we have File System with 1978 items. And All Files with 2296 items:

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Process to reach File System: **Deleted Files>File System**  Process to reach All Files: **Deleted Files>All** 
Mount archives; zip, thumbs.db, etc.	Done	2025/12/9	8:25 PM (UTC +5:45)	For this investigation we navigated to **Files Views>File Types>By Extension>Archives**

Action	Done?	Date (YY/MM/DD)	Time	Notes
				



Listing

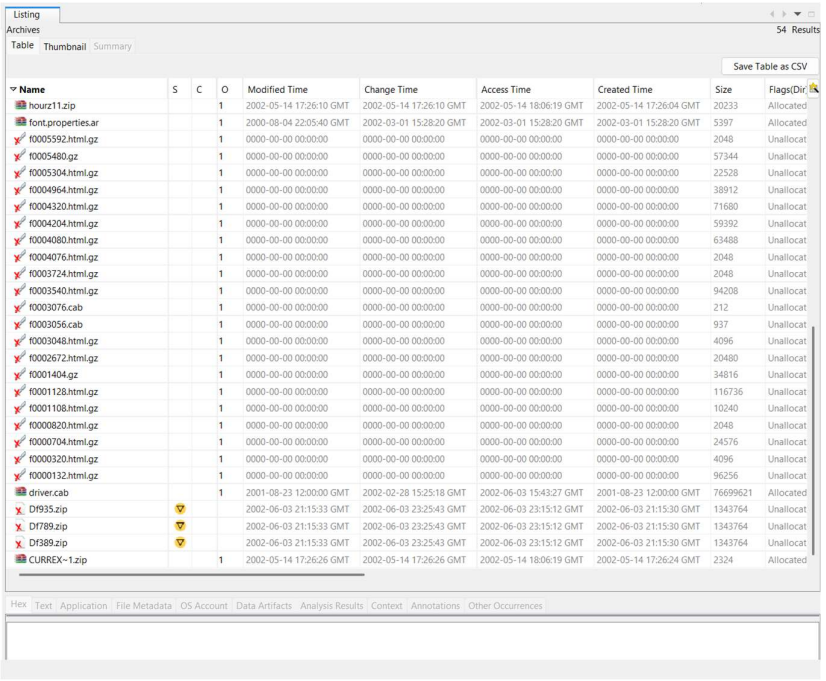
Archives

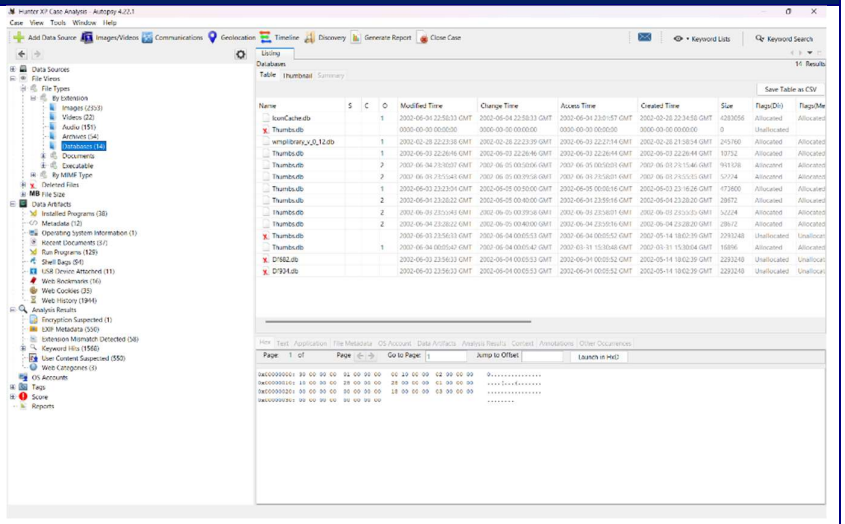
54 Results

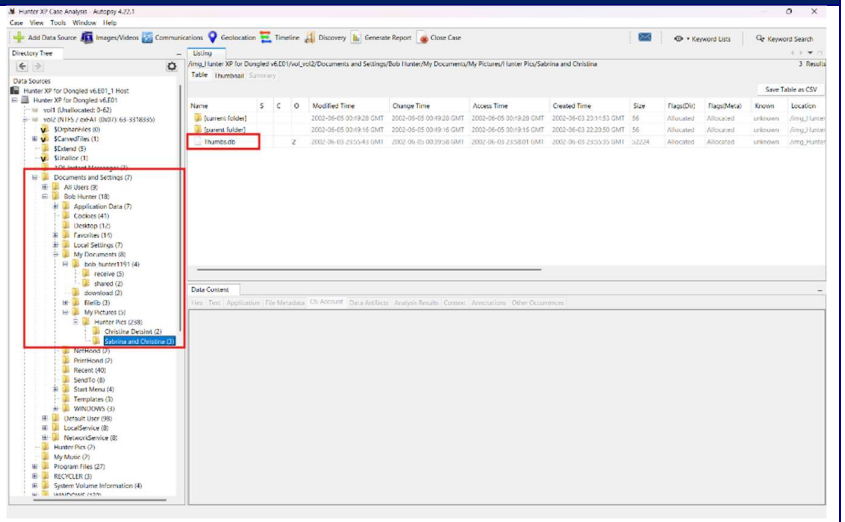
Table | Thumbnail | Summary

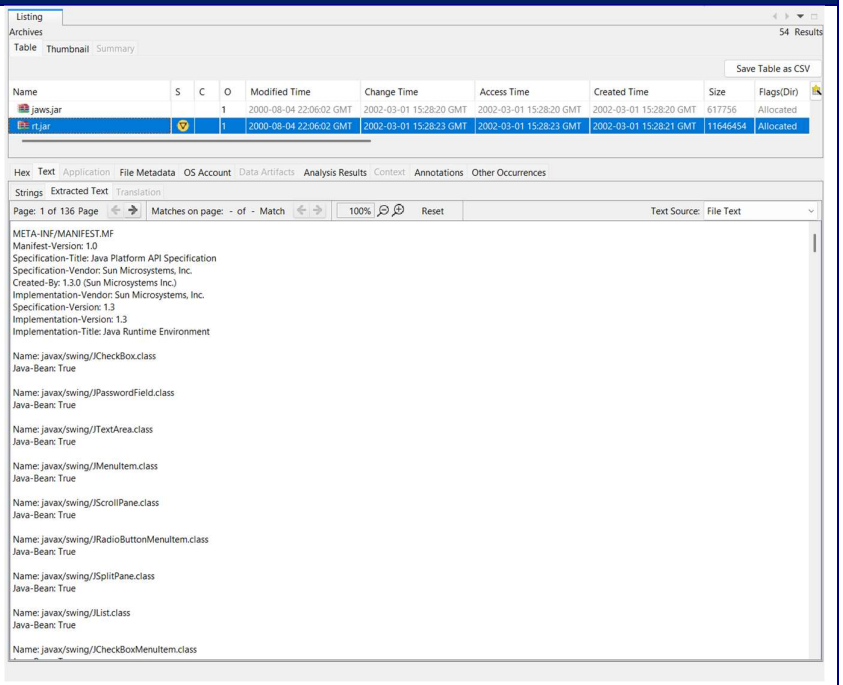
Save Table as CSV

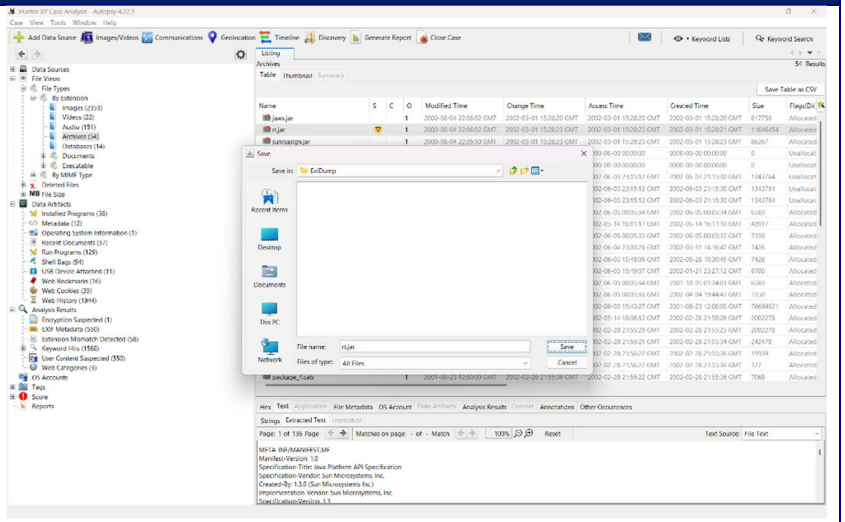
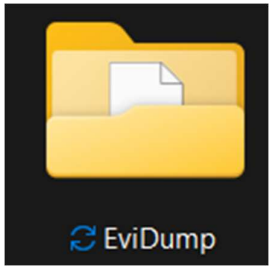
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir
yinst[1].cab			1	2002-05-14 16:11:17 GMT	2002-05-14 16:11:17 GMT	2002-05-14 16:11:17 GMT	2002-05-14 16:11:10 GMT	43917	Allocated
wuv3is[1].tgz			1	2002-03-31 14:16:46 GMT	2002-03-31 14:16:46 GMT	2002-03-31 14:16:46 GMT	2002-03-31 14:16:30 GMT	88211	Allocated
wuaucomp[2].cab			2	2002-06-03 15:49:07 GMT	2002-06-03 15:49:07 GMT	2002-06-03 15:49:07 GMT	2002-06-03 15:49:07 GMT	6700	Allocated
wuaucomp[1].cab			2	2002-05-14 16:06:56 GMT	2002-05-14 16:06:56 GMT	2002-05-14 16:06:56 GMT	2002-05-14 16:06:55 GMT	6700	Allocated
wuaucomp.cab			2	2002-01-21 23:27:12 GMT	2002-06-03 15:49:07 GMT	2002-06-03 15:49:07 GMT	2002-01-21 23:27:12 GMT	6700	Allocated
sunrsasign.jar			1	2000-08-04 22:05:50 GMT	2002-03-01 15:28:23 GMT	2002-03-01 15:28:23 GMT	2002-03-01 15:28:23 GMT	86267	Allocated
rt.jar			1	2000-08-04 22:06:02 GMT	2002-03-01 15:28:23 GMT	2002-03-01 15:28:23 GMT	2002-03-01 15:28:21 GMT	11646454	Allocated
raclass.zip				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocat
pchdt_p3.cab			2	2001-08-23 12:00:00 GMT	2002-02-28 21:50:27 GMT	2002-05-14 18:06:12 GMT	2002-02-28 21:50:26 GMT	2002278	Allocated
package_4.cab			1	2001-08-23 12:00:00 GMT	2002-02-28 21:55:36 GMT	2002-02-28 21:56:22 GMT	2002-02-28 21:55:36 GMT	7068	Allocated
package_3.cab			1	2002-02-28 21:55:27 GMT	2002-02-28 21:55:36 GMT	2002-02-28 21:56:22 GMT	2002-02-28 21:55:36 GMT	727	Allocated
package_2.cab			1	2002-02-28 21:55:27 GMT	2002-02-28 21:55:36 GMT	2002-02-28 21:56:22 GMT	2002-02-28 21:55:36 GMT	19959	Allocated
package_1.cab			1	2002-02-28 21:55:27 GMT	2002-02-28 21:55:34 GMT	2002-02-28 21:56:21 GMT	2002-02-28 21:55:34 GMT	242478	Allocated
npds.zip			1	2001-08-23 12:00:00 GMT	2002-02-28 21:50:07 GMT	2002-05-14 18:06:19 GMT	2002-02-28 21:50:07 GMT	22060	Allocated
npdrmv2.zip			1	2001-08-23 12:00:00 GMT	2002-02-28 21:50:08 GMT	2002-05-14 18:06:19 GMT	2002-02-28 21:50:08 GMT	403	Allocated
jaws.jar			1	2000-08-04 22:06:02 GMT	2002-03-01 15:28:20 GMT	2002-03-01 15:28:20 GMT	2002-03-01 15:28:20 GMT	617756	Allocated
iuident[1].cab			2	2002-06-05 00:05:33 GMT	2002-06-05 00:05:33 GMT	2002-06-05 00:05:33 GMT	2002-06-05 00:05:32 GMT	7350	Allocated
iuident.cab			2	2002-06-05 00:05:33 GMT	2002-06-05 00:05:33 GMT	2002-06-05 00:05:33 GMT	2002-04-04 19:44:47 GMT	7350	Allocated
iucert[1].cab			2	2002-06-05 00:05:34 GMT	2002-06-05 00:05:34 GMT	2002-06-05 00:05:34 GMT	2002-06-05 00:05:34 GMT	6583	Allocated
iucert.cab			2	2002-06-05 00:05:34 GMT	2002-06-05 00:05:34 GMT	2002-06-05 00:05:34 GMT	2001-10-05 01:34:03 GMT	6583	Allocated
instance_Personal_32_1033.cab			2	2001-08-23 12:00:00 GMT	2002-02-28 21:55:26 GMT	2002-02-28 21:55:29 GMT	2002-02-28 21:55:25 GMT	2002278	Allocated
ident[2].cab			2	2002-06-03 15:49:06 GMT	2002-06-03 15:49:06 GMT	2002-06-03 15:49:06 GMT	2002-06-03 15:49:06 GMT	7426	Allocated
ident[1].cab				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocat
ident[1].cab			1	2002-05-14 16:06:53 GMT	2002-05-14 16:06:53 GMT	2002-05-14 16:06:53 GMT	2002-05-14 16:06:52 GMT	7425	Allocated
ident.cab			2	2002-05-28 10:30:49 GMT	2002-06-04 23:03:26 GMT	2002-06-04 23:03:26 GMT	2002-03-31 14:16:47 GMT	7426	Allocated
ident.cab			2	2002-05-28 10:30:49 GMT	2002-06-03 15:49:06 GMT	2002-06-03 15:49:06 GMT	2002-05-28 10:30:49 GMT	7426	Allocated
hourz11.zip			1	2002-05-14 17:26:10 GMT	2002-05-14 17:26:10 GMT	2002-05-14 18:06:19 GMT	2002-05-14 17:26:04 GMT	20233	Allocated
font.properties.ar			1	2000-08-04 22:05:40 GMT	2002-03-01 15:28:20 GMT	2002-03-01 15:28:20 GMT	2002-03-01 15:28:20 GMT	5397	Allocated

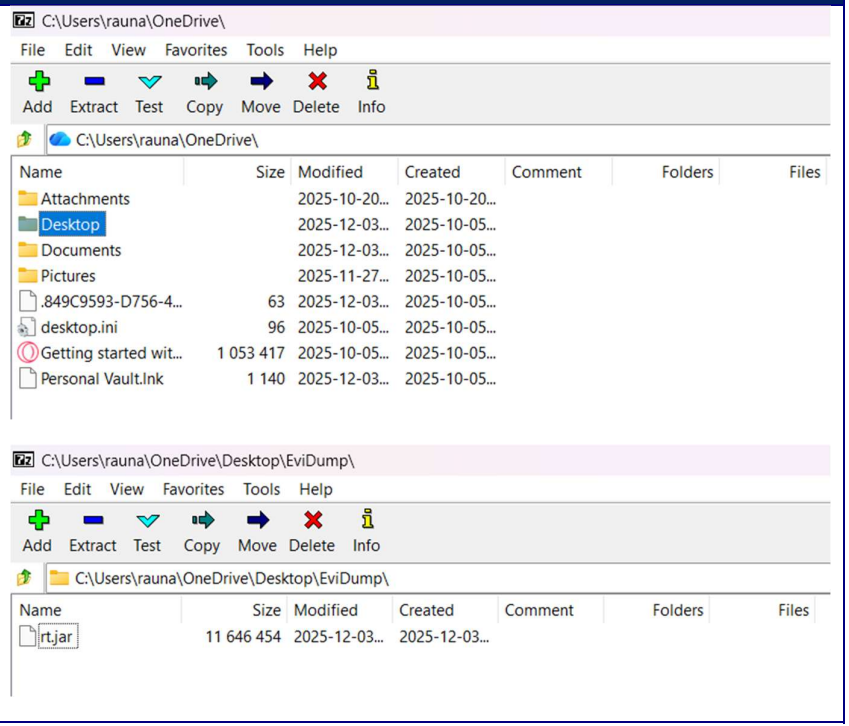
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 The zip files are located here. As for thumbs.db we go to this location Firstly, Location: **Files Views>File Types>By Extension>Databases**

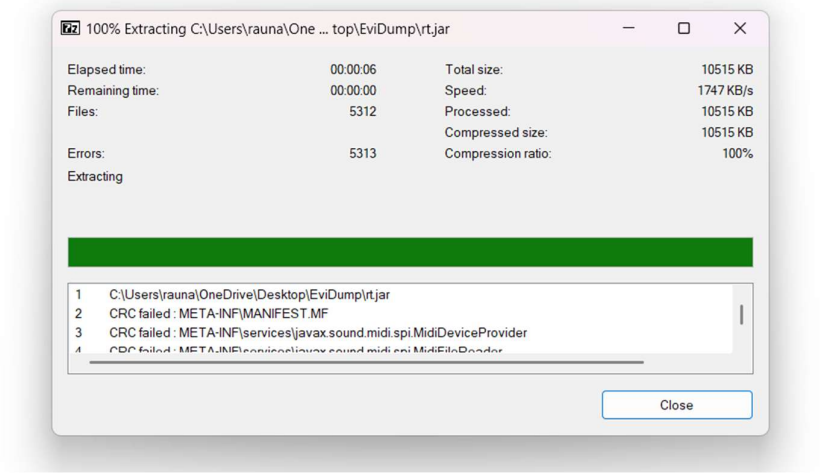
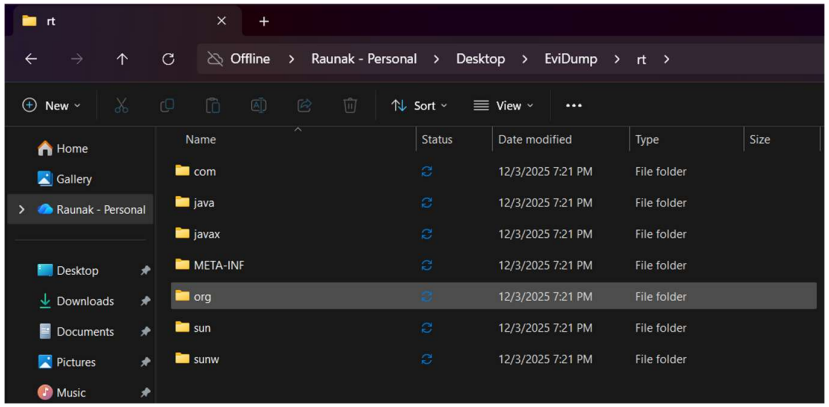
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Secondly, Location: **Vol-vol2>Documents and setting>bob hunter>my documents>my pictures>hunter pics>Sabrina and Christina**

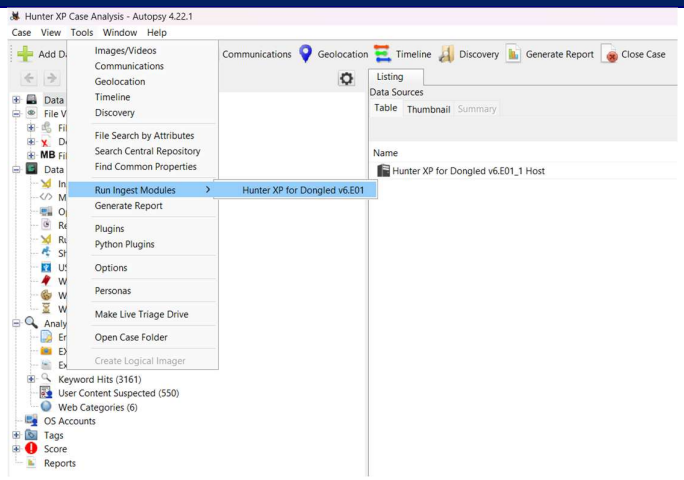
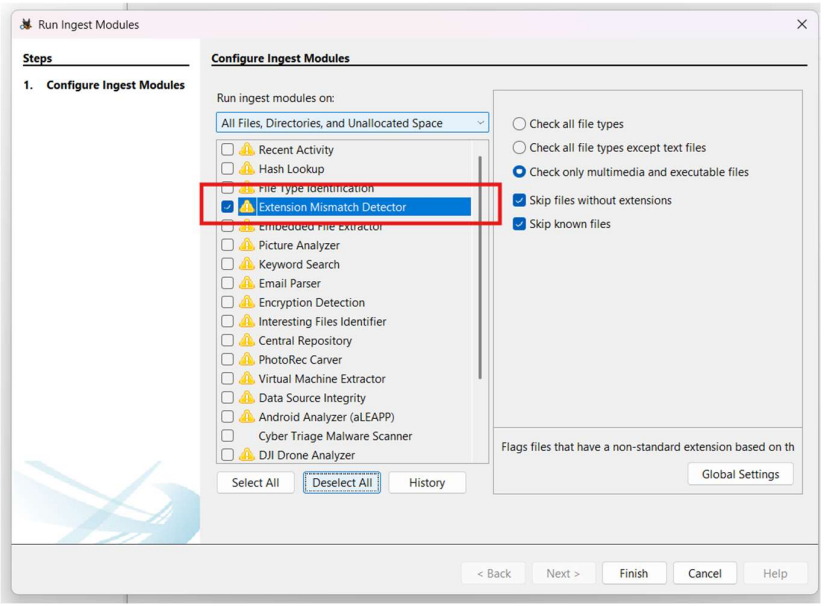
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Here we can find database file i.e. **Thumbs.db**. To mount it further, I extracted **rt.jar** zip file in my pc.

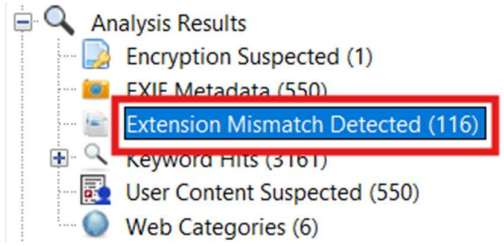
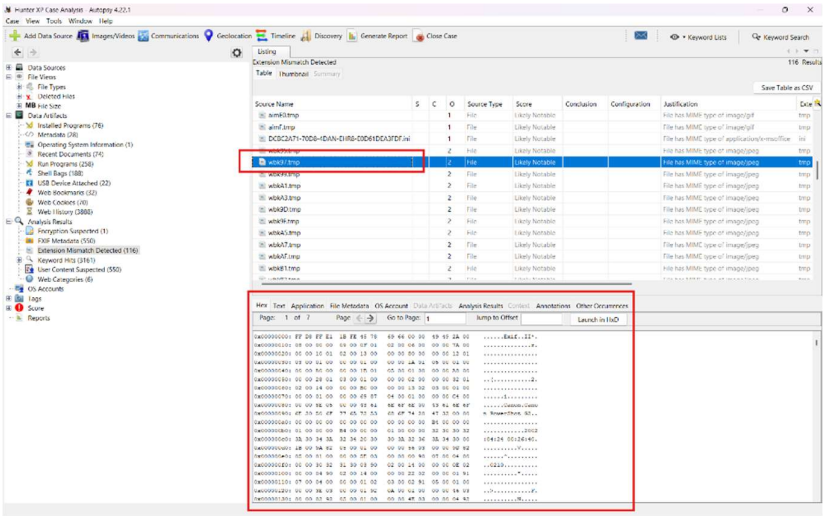
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

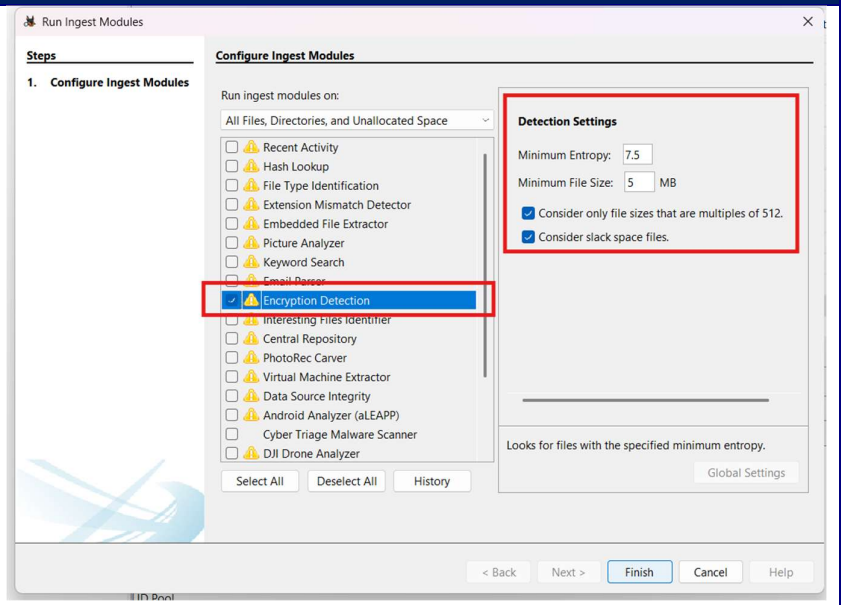
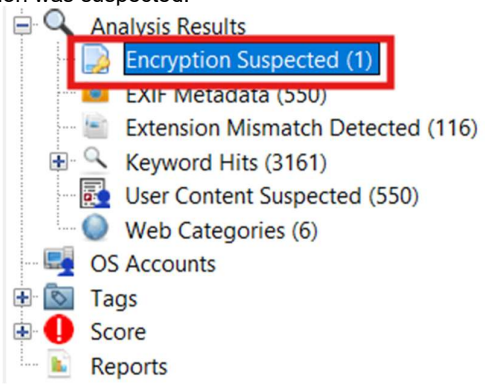
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Location of the extracted file: **Desktop>EviDump**  Then, I extracted it using **7-Zip** Software.

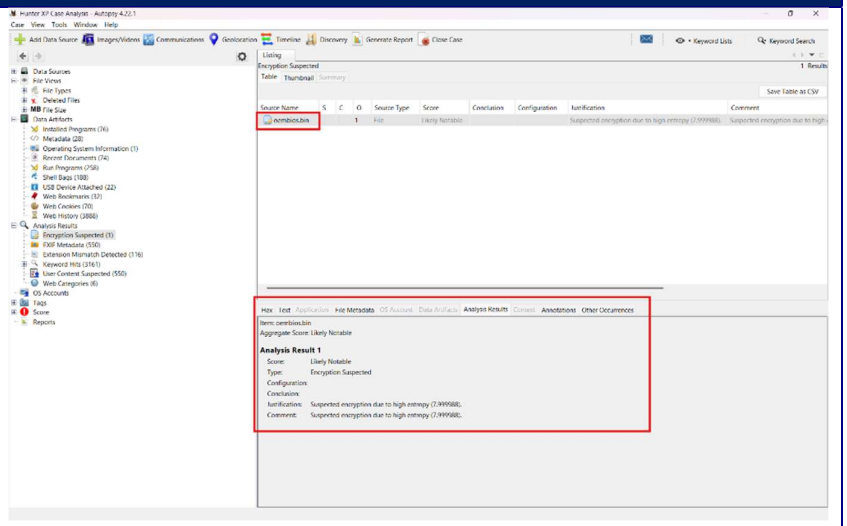
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

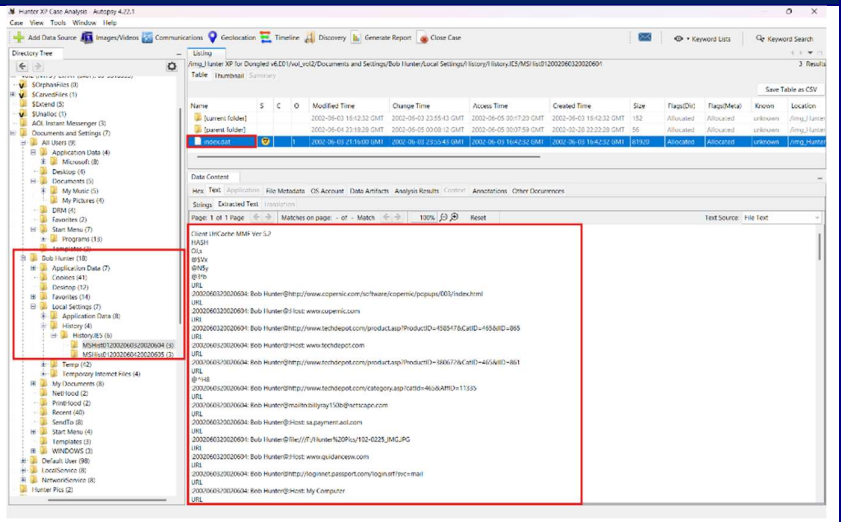
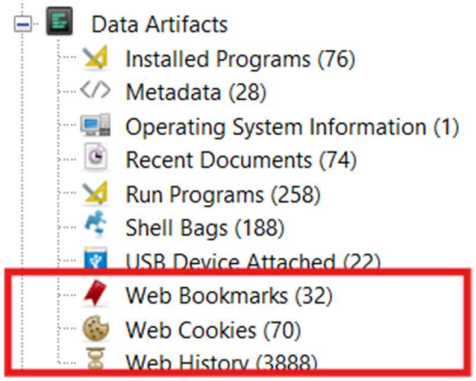
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Lastly, I mounted all of them and maximum were html-oriented files. 
File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation)	Done	2025/12/10	6:30 PM (UTC +5:45)	For this we run a ingest module called “**Extension Mismatch**”. First of all, we need to open the Run Ingest Modules from tools window and select Hunter XP for Dongled v6.E01

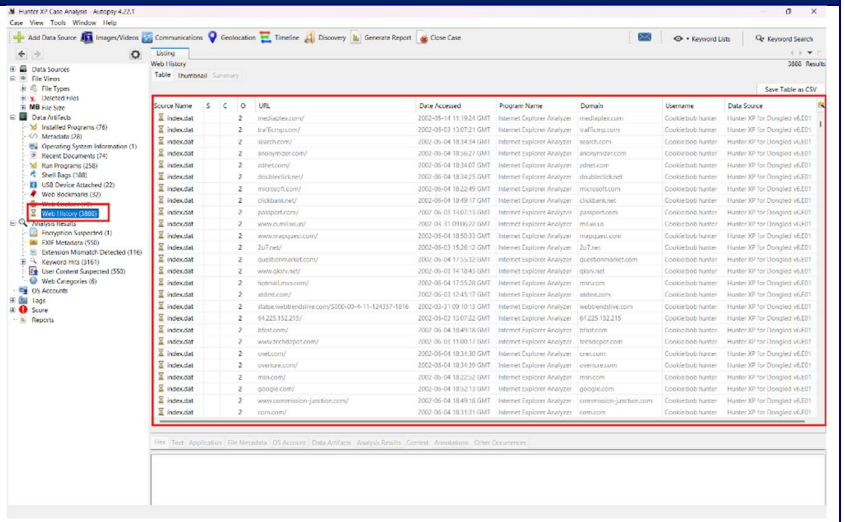
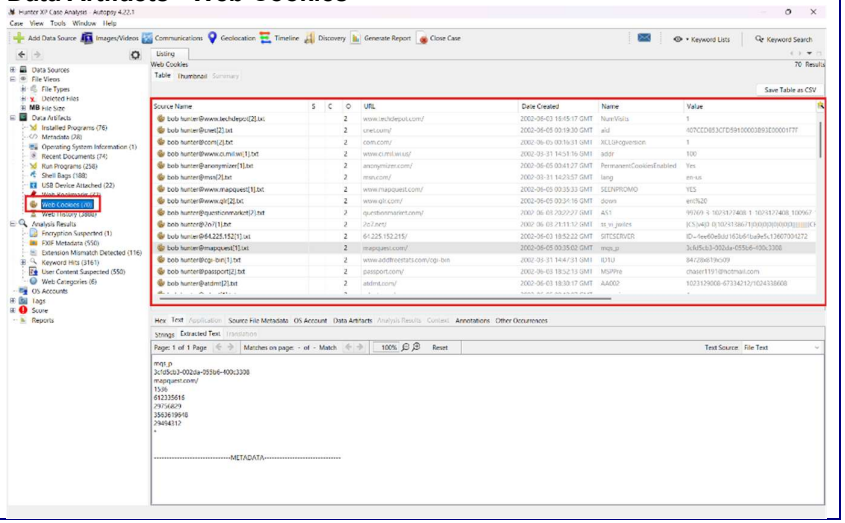
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 

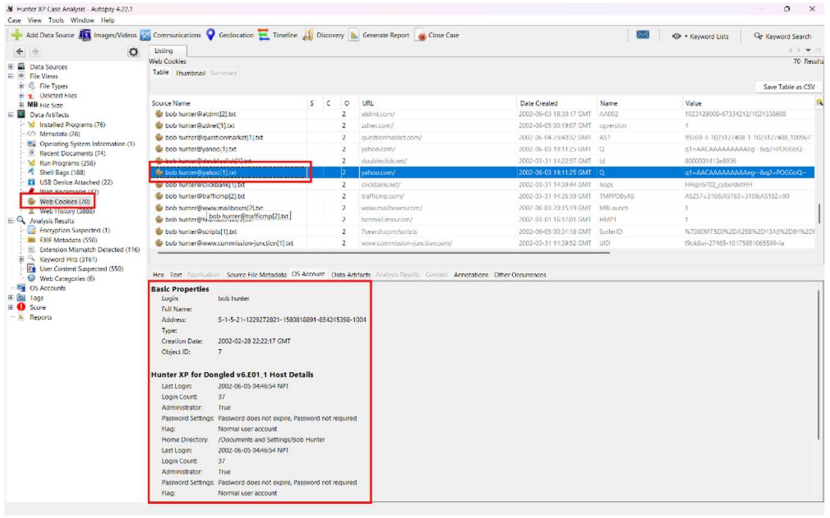
Action	Done?	Date (YY/MM/DD)	Time	Notes
				Then we can find mismatch under Analysis Results.  Here 116 files suspected to have extension mismatch has been found.  Here the hash shows that this is a .JPEG file. For Encryption Detection, I used ingest module. Process: **TOOLS>RUN INGEST MODULES>ENCRYPTION DETECTION**

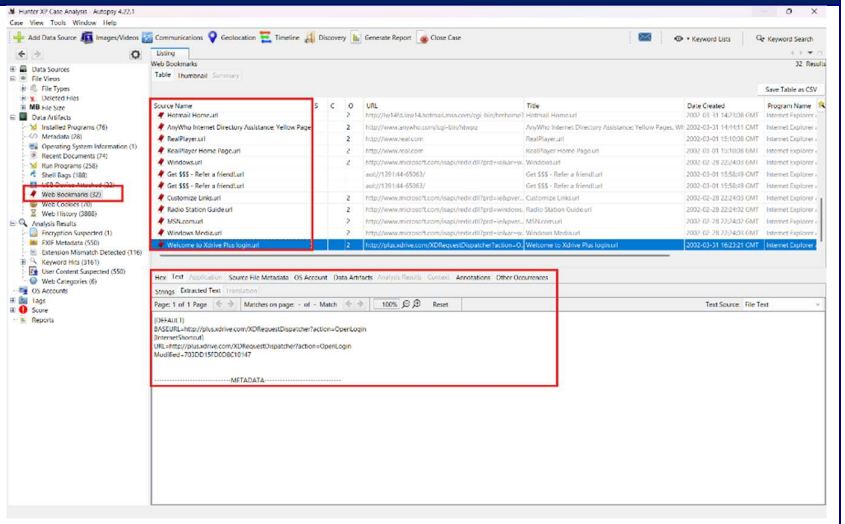
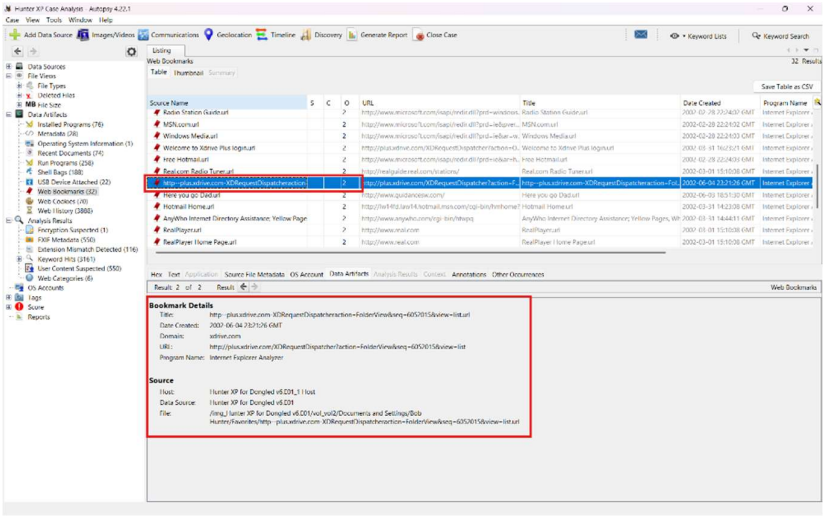
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Here, 1 Encryption was suspected. 

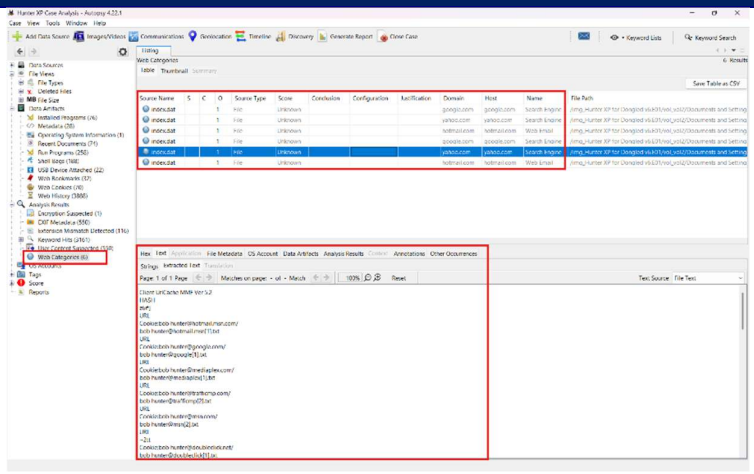
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 **Oembios.bin** was encrypted.
Internet History, favourites, etc. Other browsers?	Done	2025/12/10	8:00 PM (UTC +5:45)	For this we Navigate to **vol_vol2>Documents and Settings>Bob Hunter>Local Settings>History>History.IE5>MSHist012002060320020604> index.dat**

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Here, History can be seen.  Likewise, we can also find web history from **Data Artifacts> Web History**

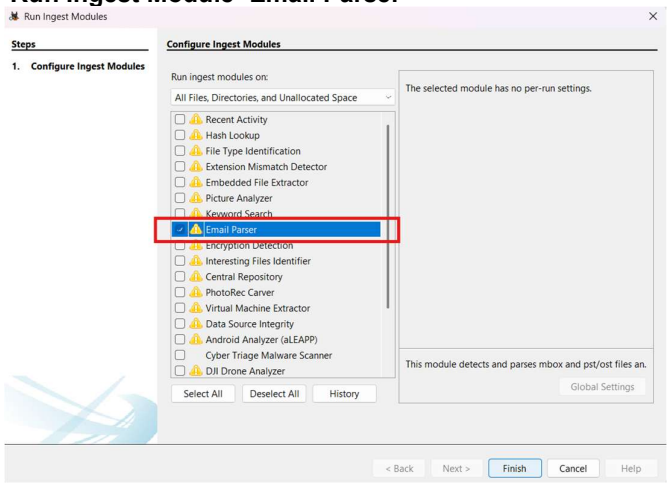
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Likewise, we can also find web cookies from **Data Artifacts> Web Cookies** 

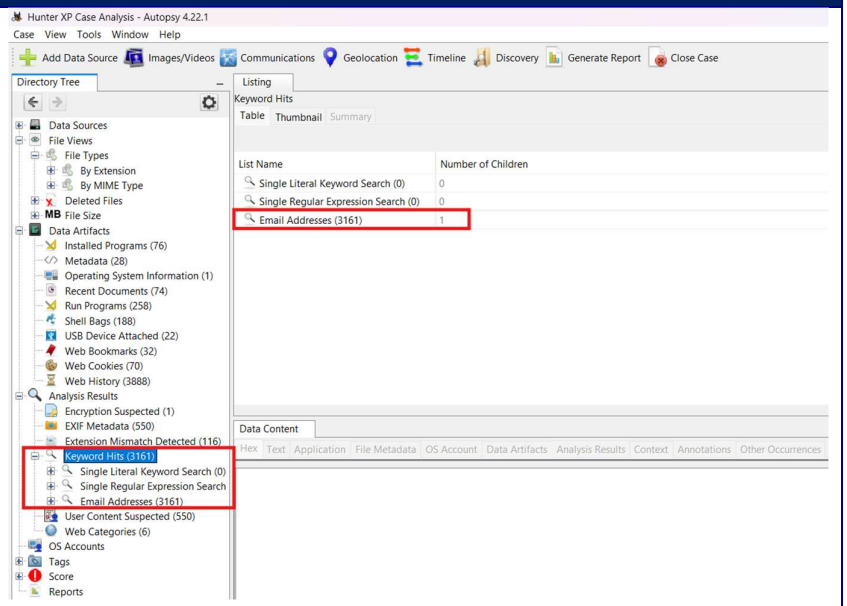
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Likewise, we can also find web bookmarks from **Data Artifacts> Web Bookmarks**

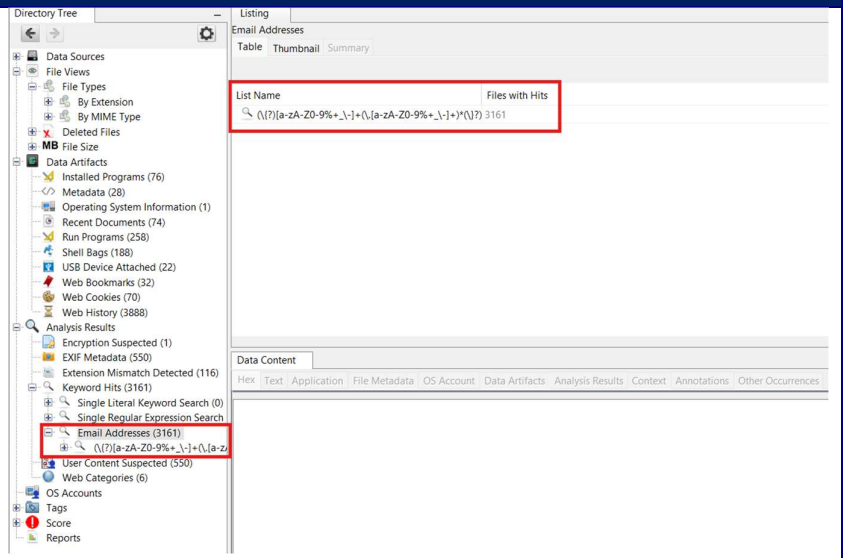
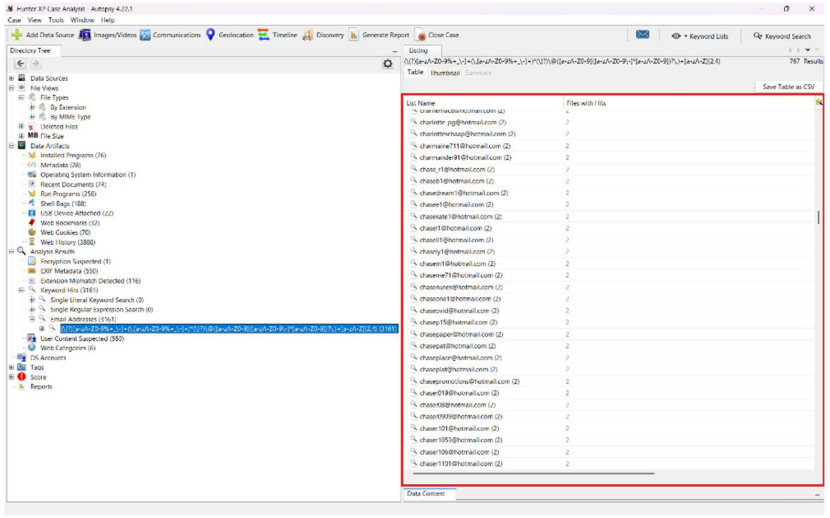
Action	Done?	Date (YY/MM/DD)	Time	Notes
				  Likewise, we can also find web categories from **Data Artifacts> Web Categories**

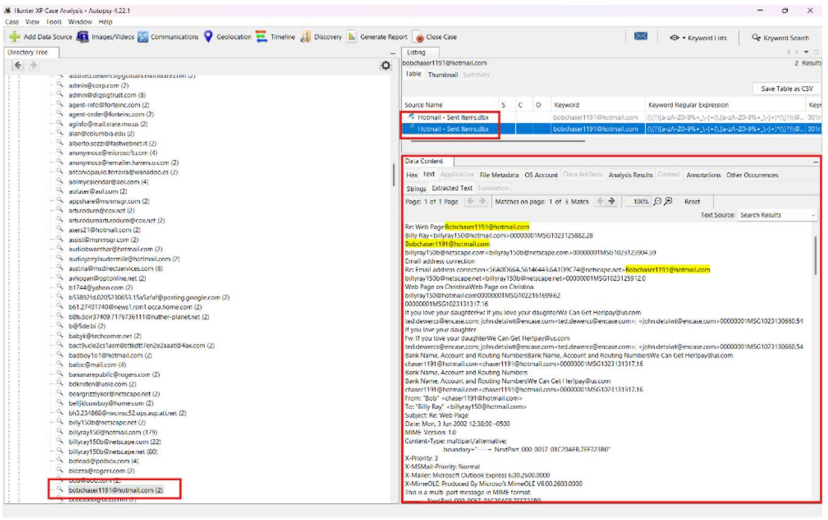
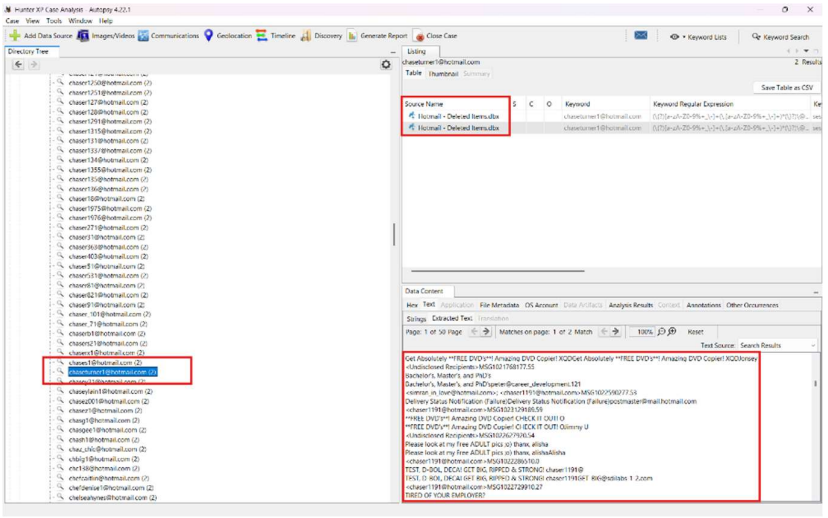
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

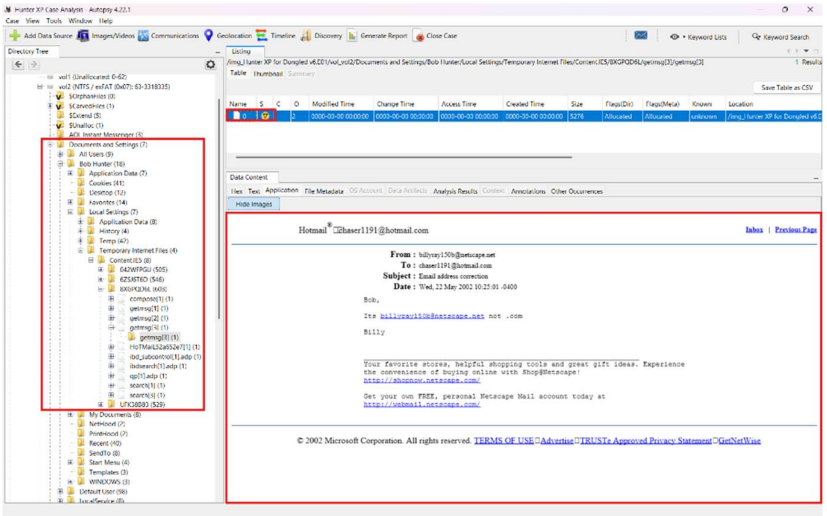
Client UrlCache MMF Ver 5.2
HASH
z6#]
URL
Cookie:bob hunter@hotmail.msn.com/
bob hunter@hotmail.msn[1].txt
URL
Cookie:bob hunter@google.com/
bob hunter@google[1].txt
URL
Cookie:bob hunter@mediaplex.com/
bob hunter@mediaplex[1].txt
URL
Cookie:bob hunter@trafficmp.com/
bob hunter@trafficmp[2].txt
URL
Cookie:bob hunter@msn.com/
bob hunter@msn[2].txt
URL
~2tt
Cookie:bob hunter@doubleclick.net/
bob hunter@doubleclick[1].txt
URL
Cookie:bob hunter@7search.com/scripts
bob hunter@scripts[1].txt
URL
Cookie:bob hunter@clickbank.net/
bob hunter@clickbank[1].txt
URL
Cookie:bob hunter@www.addfreestats.com/cgi-bin
bob hunter@cgi-bin[1].txt
URL
Cookie:bob hunter@www.commission-junction.com/
bob hunter@www.commission-junction[1].txt
URL
Cookie:bob hunter@bfast.com/
bob hunter@bfast[2].txt
URL
Cookie:bob hunter@www.ci.mil.wi.us/bob hunter@www.ci.mil.wi[1].txt
URL
Cookie:bob hunter@statse.webtrendslive.com/S000-00-4-11-124357-1816bob hunter@S000-00-4-11-124357-1816[1].txt
URL
Cookie:bob hunter@mapquest.com/bob hunter@mapquest[1].txt

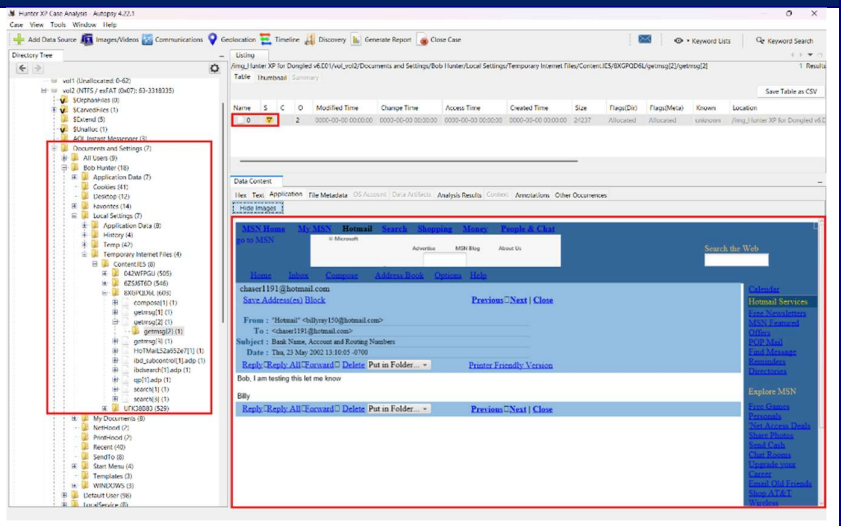
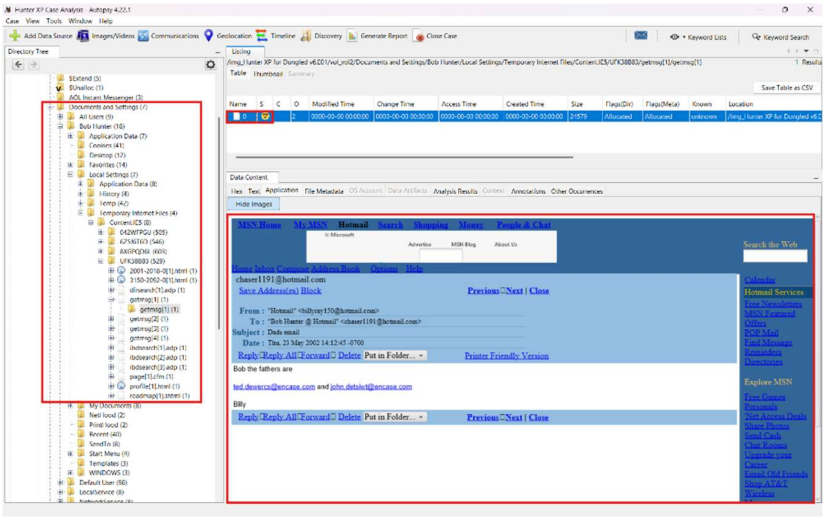
Action	Done?	Date (YY/MM/DD)	Time	Notes
Emails, local and web-based.	Done	2025/12/11	7:00 PM (UTC +5:45)	For this, I used “**Email Parser”** ingest module. Process: **Tools>Run Ingest Module>Email Parser**  Then, I basically went to keyword search and choose Email Addresses. Process: **Analysis Results>Keyword Hits>Email Addresses**

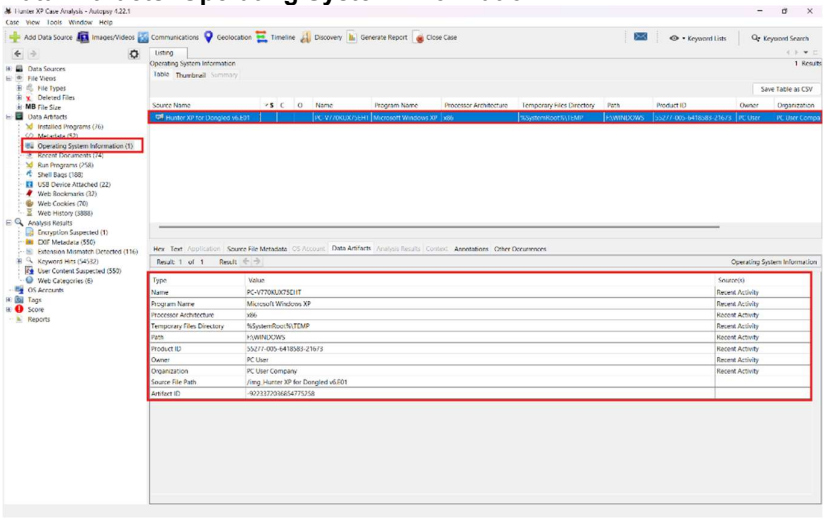
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 

Action	Done?	Date (YY/MM/DD)	Time	Notes
				For specific mails we go to different locations. Here in this location **vol_vol2>Documents and Settings>Bob Hunter>Local Settings>Temporary Internet Files>Content.IE5/8XGPQD6L>getmsg[3]** Here, we can see Billray sending mail to Chaser .  Likewise at the location **vol_vol2>Documents and Settings>Bob Hunter>Local Settings>Temporary Internet Files>Content.IE5>8XGPQD6L** Here,we can find other mails there from **getmsg[1]** and **getmsg[2].**

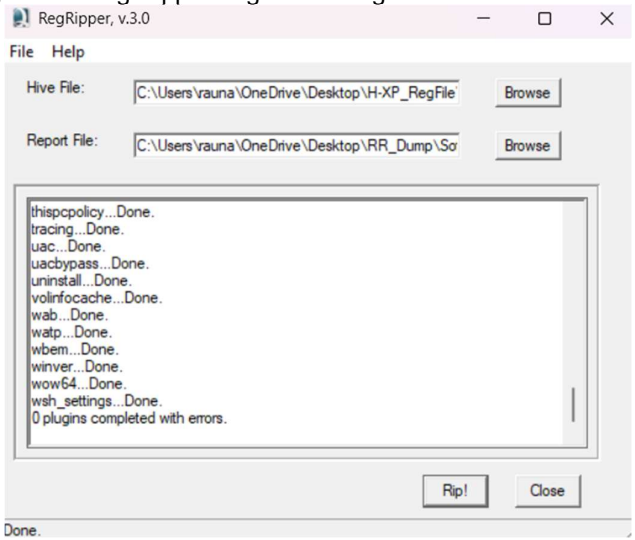
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 

Action	Done?	Date (YY/MM/DD)	Time	Notes
				Here are few notable email addresses: billyray150@hotmail.com chaser1191@hotmail.com billyray150b@netscape.net ted.dewercs@encase.com john.detsiwt@encase.com Others were also found asking for ransom and giving death threat.
Retrieve operating system information, accounts information, software, time zone information etc.).	Done	2025/12/11	10:00 PM (UTC +5:45)	For this we navigate to **Data Artifacts>Operating System Information** 

Action	Done?	Date (YY/MM/DD)	Time	Notes

Type	Value
Name	PC-V770KUX75EHT
Program Name	Microsoft Windows XP
Processor Architecture	x86
Temporary Files Directory	%SystemRoot%\TEMP
Path	F:\WINDOWS
Product ID	55277-005-6418583-21673
Owner	PC User
Organization	PC User Company
Source File Path	/img_Hunter XP for Dongled v6.E01
Artifact ID	-9223372036854775258

Similarly, I used Reg Ripper to get following information:

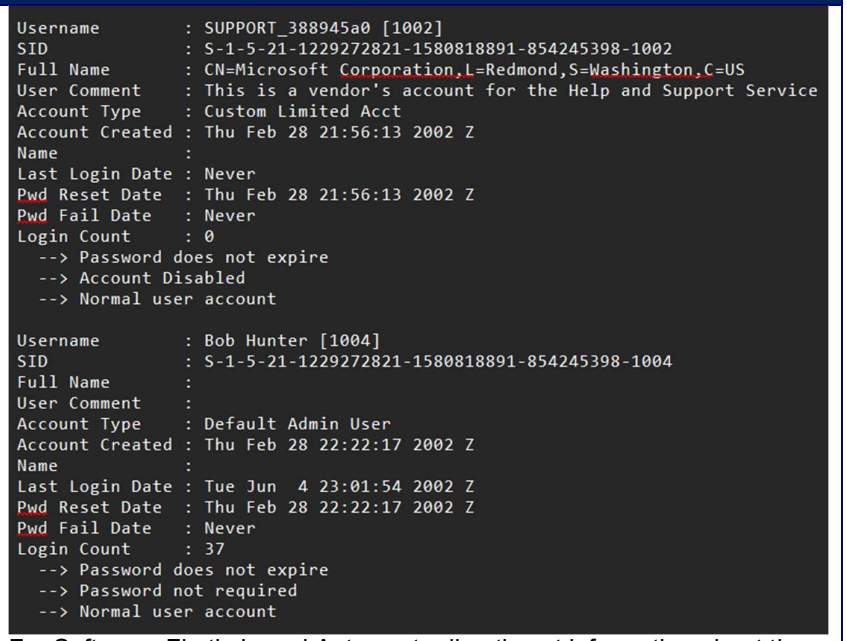


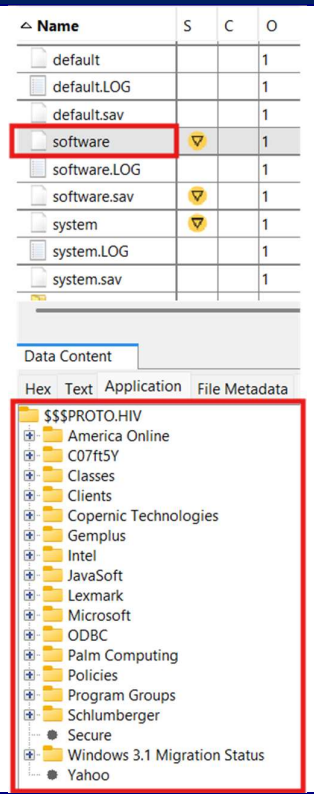
For OS, I checked SoftwareDump.txt:

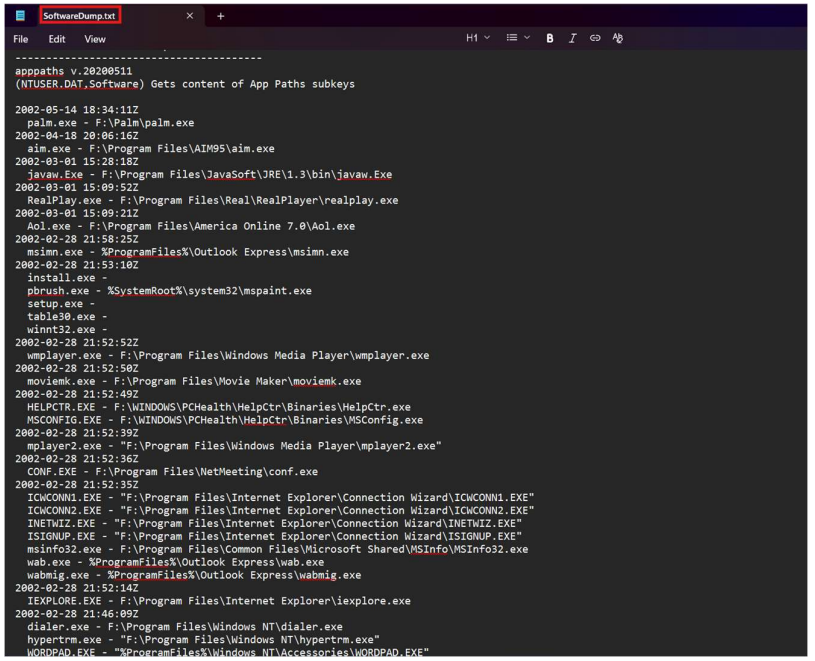
Action	Done?	Date (YY/MM/DD)	Time	Notes
				winver v.20200525 (Software) Get Windows version & build info ProductName Microsoft Windows XP BuildLab 2600.xpclnt_qfe.010827-1803 RegisteredOrganization PC User Company RegisteredOwner PC User InstallDate 2002-02-28 22:02:39Z ---------- wow64 v.20200515 (Software) Gets contents of WOW64\x86 key WOW64 Microsoft\WOW64\x86 not found. Microsoft\WOW64\arm not found. ---------- wsh_settings v.20200517 (Software) Gets WSH Settings Microsoft\Windows Script Host\Settings Key LastWrite: 2002-02-28 21:52:14Z DisplayLogo 1 ActiveDebugging 1 SilentTerminate 0 UseWINSAFER 1 For Accounts Information, I checked SamDump.txt:

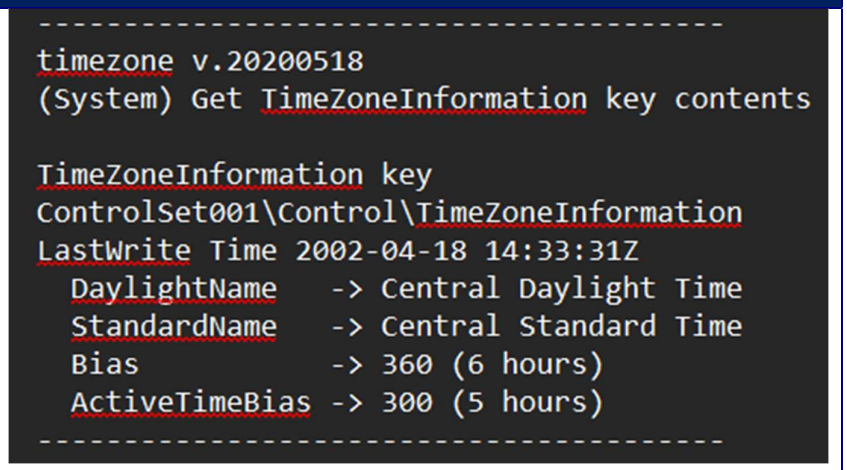
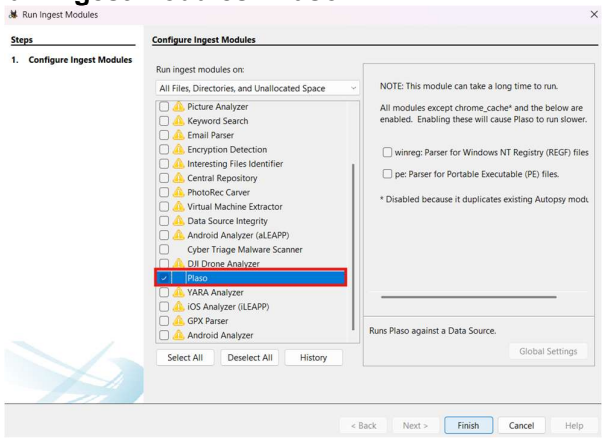
Action	Done?	Date (YY/MM/DD)	Time	Notes

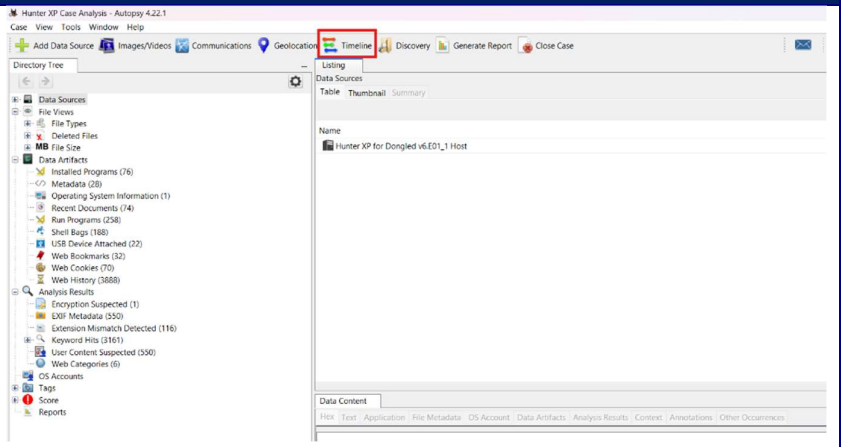
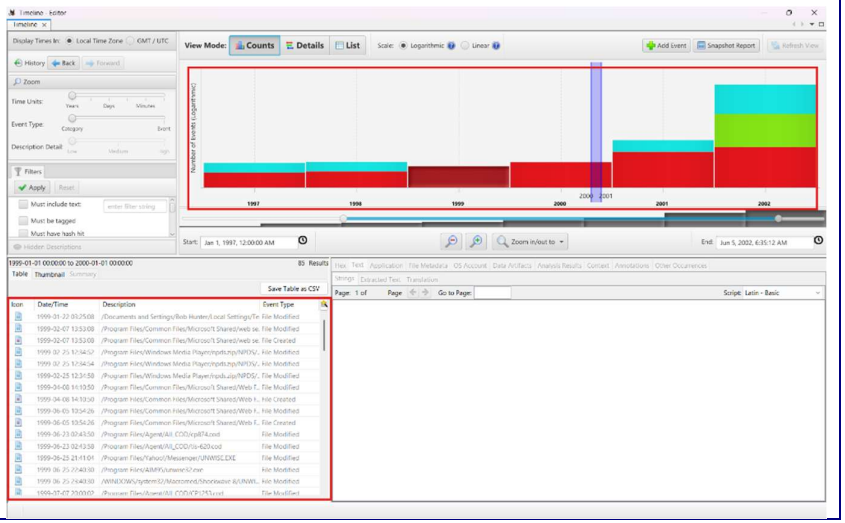
```
User Information
------------------------
Username        : Administrator [500]
SID             : S-1-5-21-1229272821-1580818891-854245398-500
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Thu Feb 28 15:22:36 2002 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account

Username        : Guest [501]
SID             : S-1-5-21-1229272821-1580818891-854245398-501
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Thu Feb 28 15:22:36 2002 Z
Name            :
Last Login Date : Mon Jun  3 16:49:37 2002 Z
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Password not required
  --> Normal user account

Username        : HelpAssistant [1000]
SID             : S-1-5-21-1229272821-1580818891-854245398-1000
Full Name       : Remote Desktop Help Assistant Account
User Comment    : Account for Providing Remote Assistance
Account Type    : Custom Limited Acct
Account Created : Thu Feb 28 21:47:33 2002 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Thu Feb 28 21:47:33 2002 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account
```

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 For Software, Firstly I used Autopsy to directly get information about the software. Location: **Windows>System32>Config>Software**

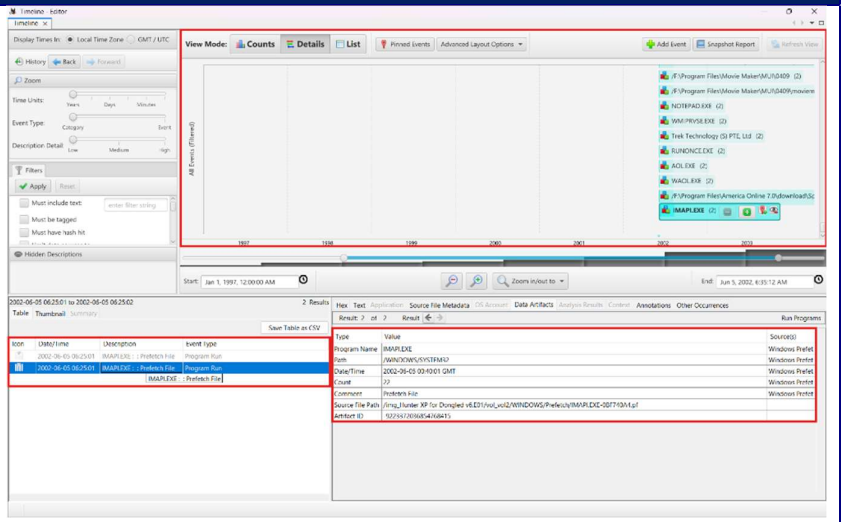
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

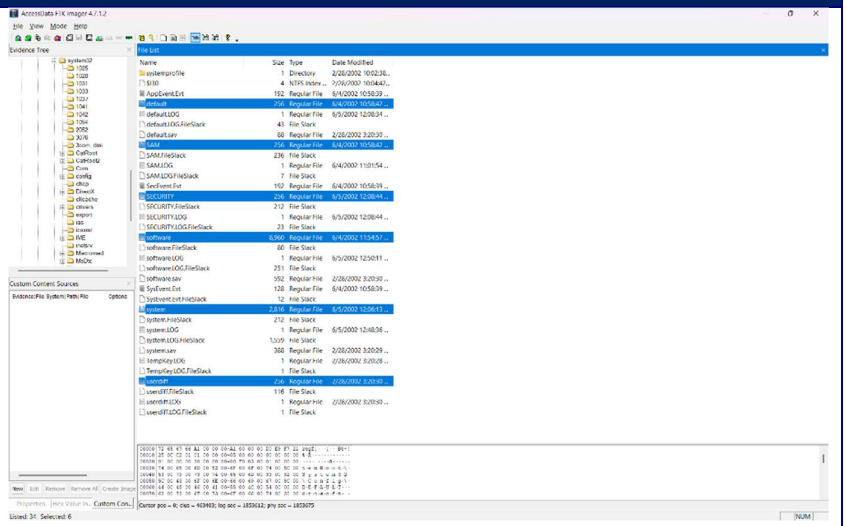
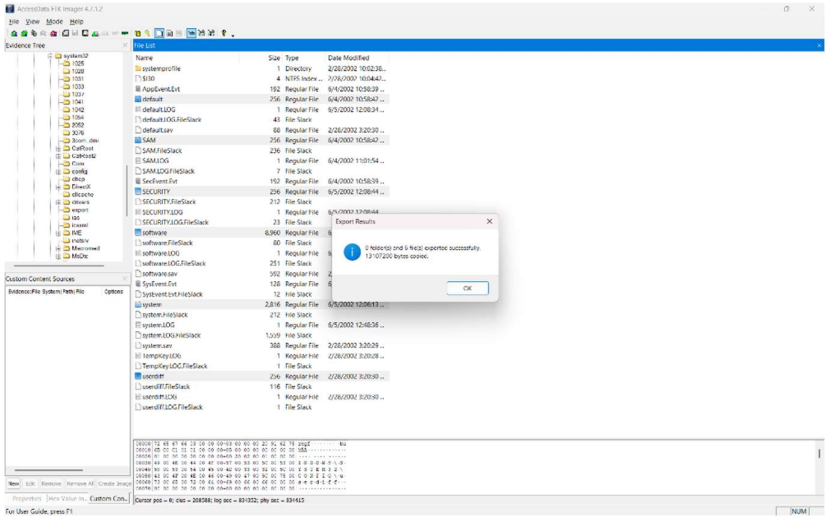
Action	Done?	Date (YY/MM/DD)	Time	Notes
				Secondly, I checked SoftwareDump.txt to check about the software information.  For Time Zone, I checked SystemDump.txt.

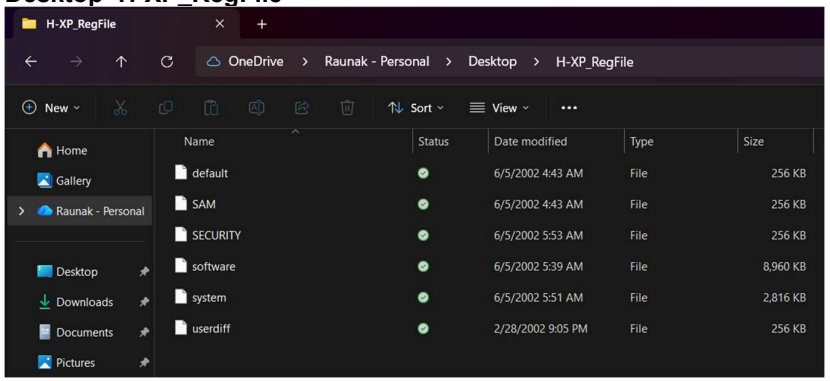
Action	Done?	Date (YY/MM/DD)	Time	Notes
				
Timeline analysis- Note date of last activity on the computer. System profiling.	Done	2025/12/12	07:00 PM (UTC +5:45)	For this we run **Tools>Run Ingest Modules>Plaso**  With this we can access the timeline page at the top.

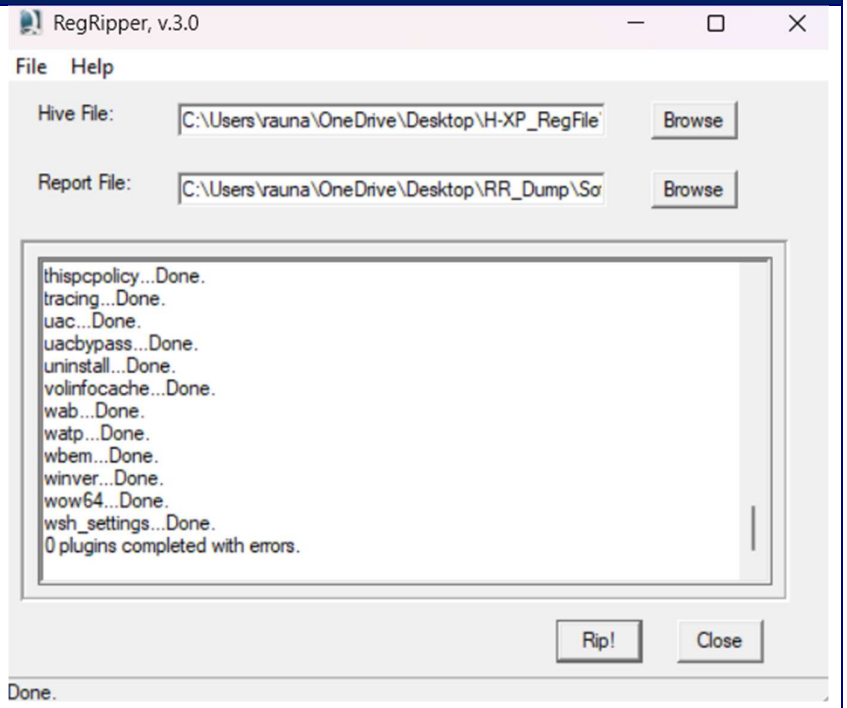
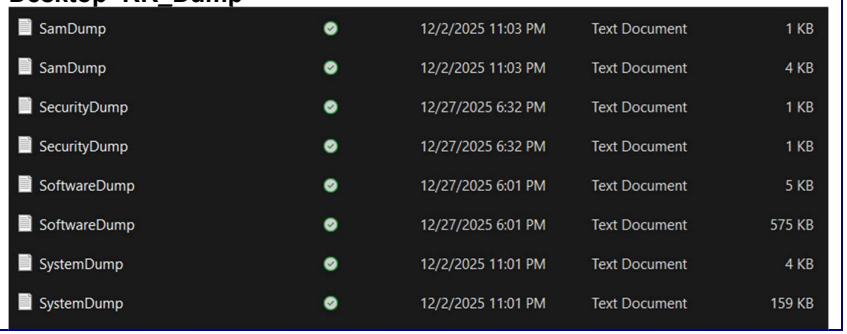
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Here we can analyse, when different events happened. For the last activity we can select the bar graph to show the latest activities at the end of the computer. 

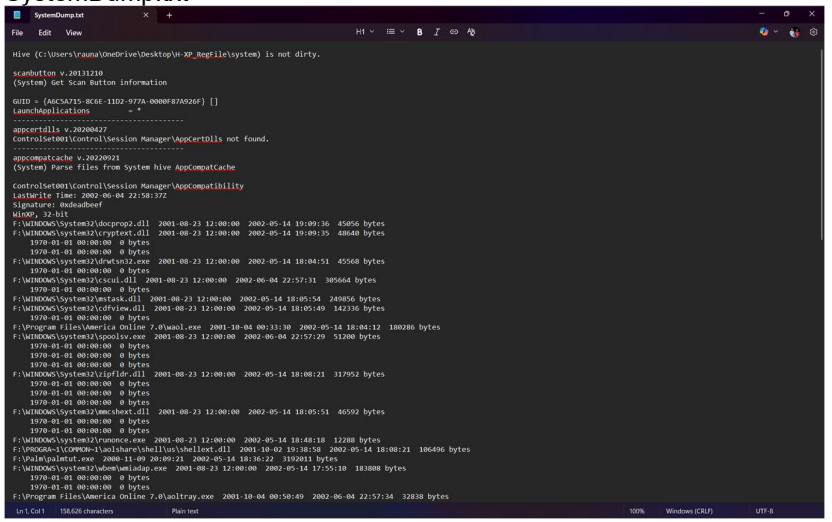
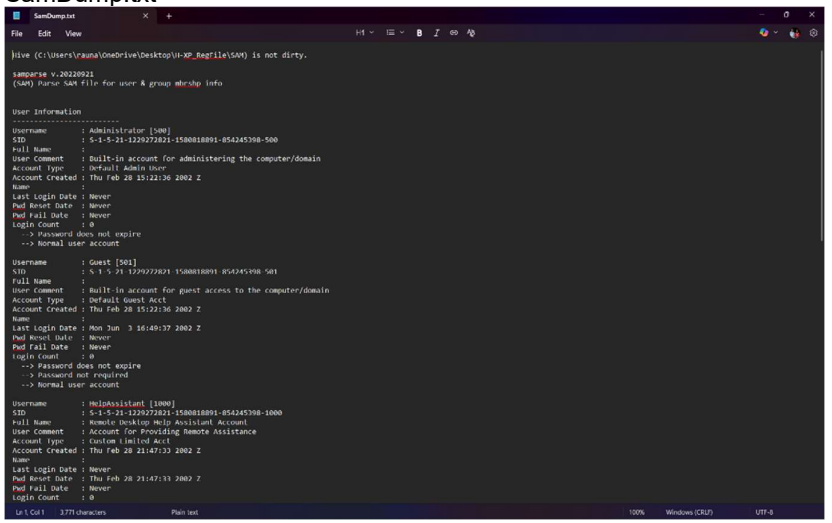
Here we can analyse, when different events happened.
For the last activity we can select the bar graph to show the latest activities at the end of the computer.

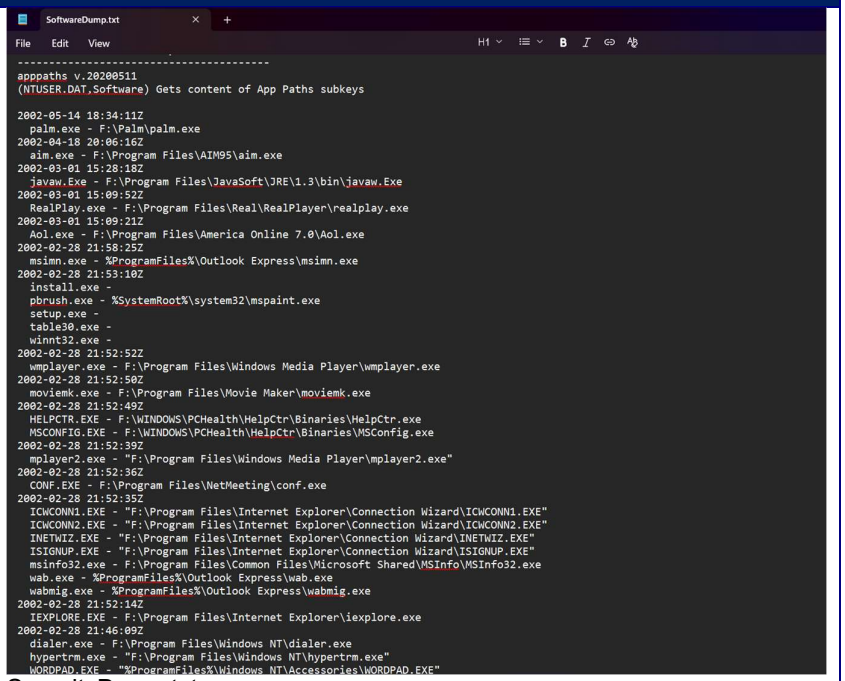
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Now we can see that at the end CD-burning tool IMAPI.exe was run.
Registry analysis and Registry protected area	Done	2025/12/12	09:00 PM (UTC +5:45)	We used ftk to access the image file and go to this location **Windows>System32>Config**

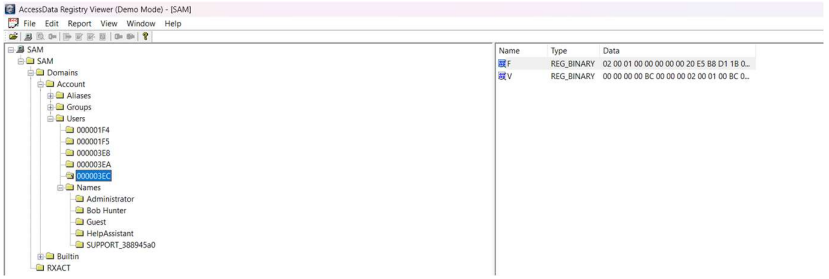
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 

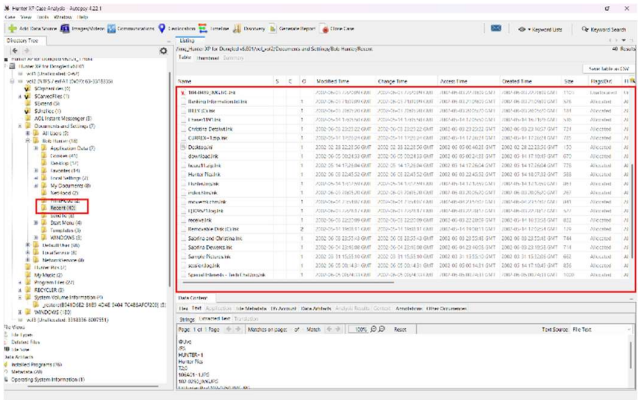
Action	Done?	Date (YY/MM/DD)	Time	Notes
				For this we extracted SAM, SECURITY, SYSTEM, SOFTWARE, and etc. Which is located at: **Desktop>H-XP_RegFile**  Now, I used Reg Ripper to RIP all the extracted registry files.

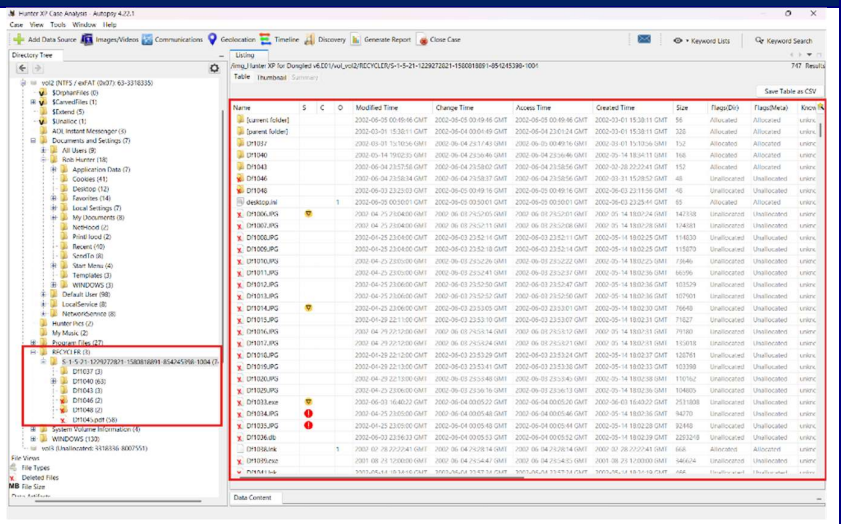
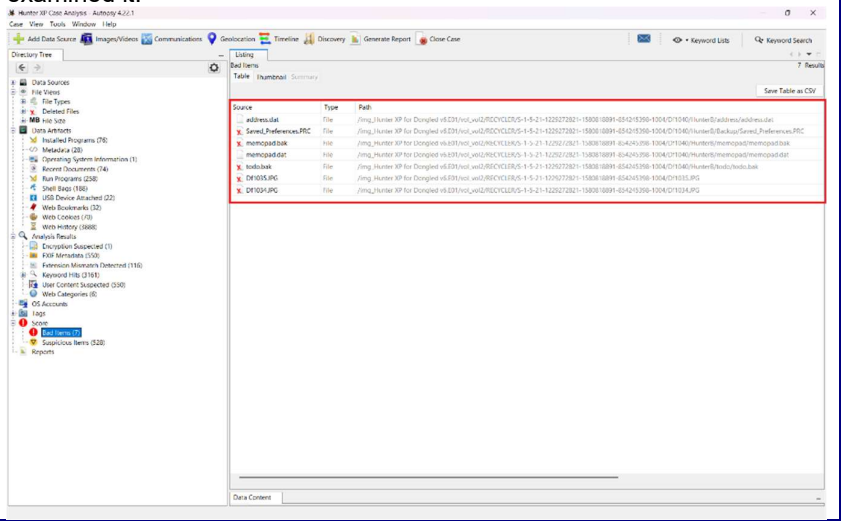
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Dump of Ripped Files is at: **Desktop>RR_Dump** 

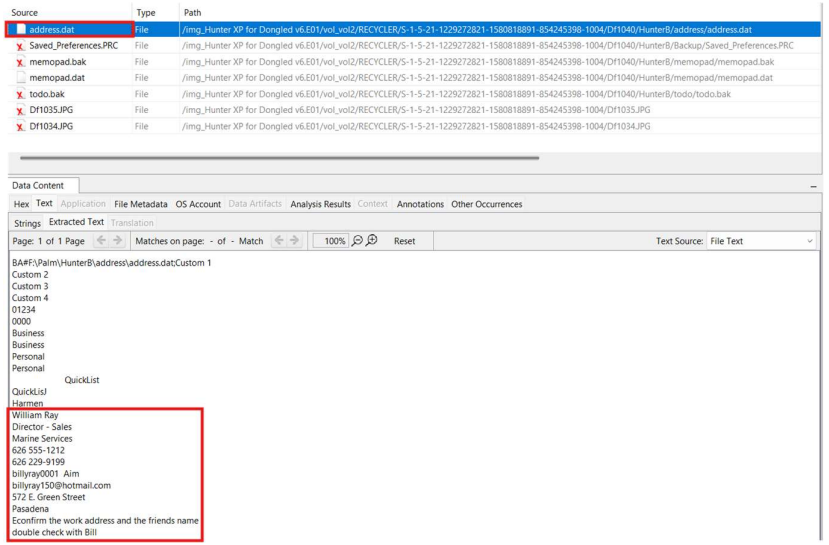
Action	Done?	Date (YY/MM/DD)	Time	Notes
				SystemDump.txt  SamDump.txt  SoftwareDump.txt

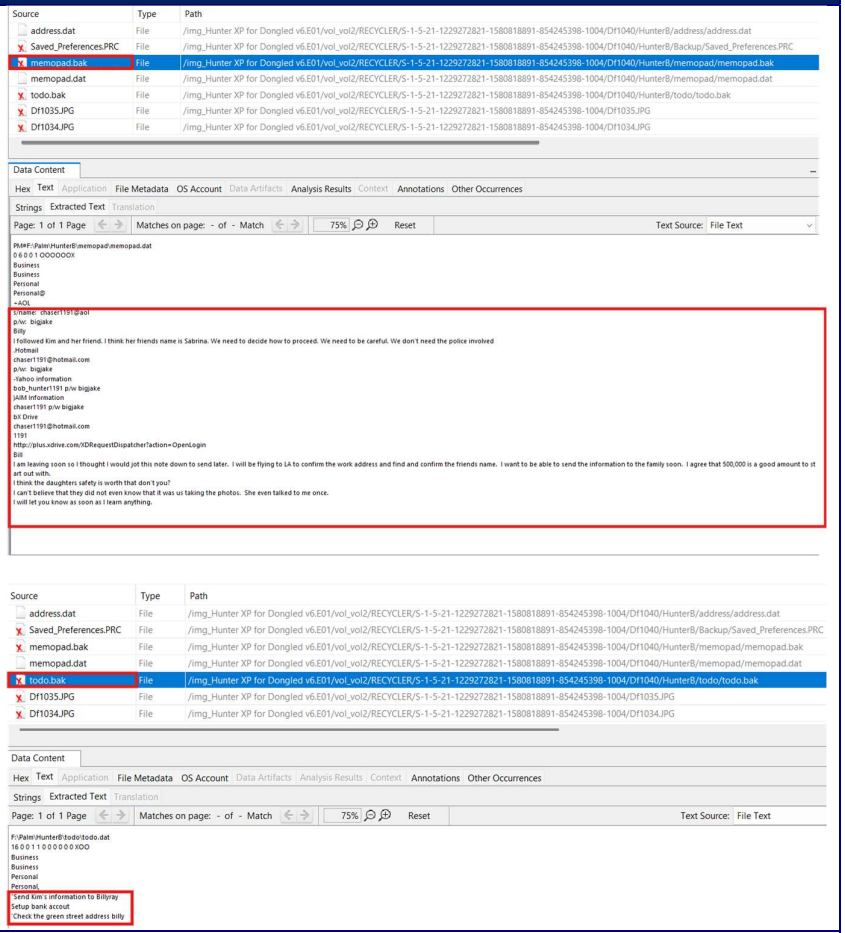
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 SecurityDump.txt

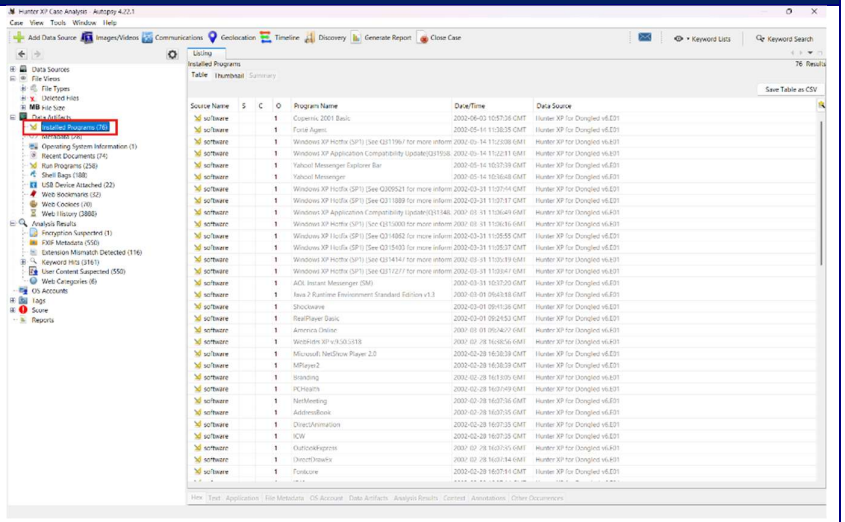
Action	Done?	Date (YY/MM/DD)	Time	Notes
				SecurityDump.txt File Edit View Hive (C:\Users\rauna\OneDrive\Desktop\H-XP_RegFile\SECURITY) is not dirty. auditpol v.20200515 (Security) Get audit policy from the Security hive file auditpol Policy\PolAdtEv LastWrite Time 2002-02-28 15:25:30Z Data Length: 0x2c 0x00000000: 01 00 07 00 03 00 00 00 03 00 00 00 00 00 00 00 .... 0x00000010: 00 00 00 00 00 00 00 00 03 00 00 00 03 00 00 00 .... 0x00000020: 00 00 00 00 03 00 00 00 09 00 00 00 .... ---------- secrets v.20200517 (Security) Get the last write time for the Policy\Secrets key Policy\Secrets LastWrite Time 2002-03-31 14:27:32Z ---------- We can also use Registry Viewer to see this information. For E.g. SAM: Location: **SAM>Domains>Account>Users>Names**  Here, I viewed information about the users.

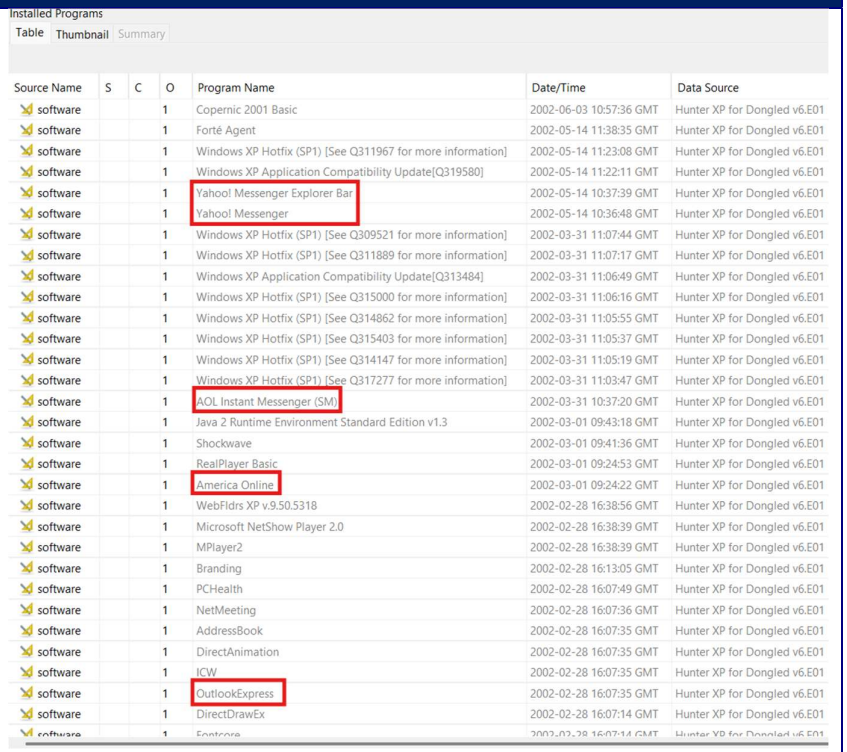
Action	Done?	Date (YY/MM/DD)	Time	Notes
Link files and Recycle Bin	Done	2025/12/13	08:00 PM (UTC +5:45)	For this procedure, we navigate to **img_Hunter XP for Dongled v6.E01 > vol_vol2>Documents and Settings > Bob Hunter > Recent** Here, we can see various .lnk files, which were links frequently visited by the user, as well as, a txt file labelled as “Banking Information”. A lot of the links were named after the victims (Sabrina and Christina) which further contained various images of the victims, as evidenced by the image below:  For deleted files in the recycler located in **Hunter XP for Dongled v6.E01 > vol_vol2/Documents and Settings > RECYCLER** Which are mostly images of the victims, address of the suspect, information about the bank, and etc that was deleted in order to get rid of the evidence of stalking.

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 I added like notable tag on suspicious file from the recycle bin and examined it. 

Action	Done?	Date (YY/MM/DD)	Time	Notes
				

Action	Done?	Date (YY/MM/DD)	Time	Notes
				
Instant Messaging clients	Done	2025/12/13	10:00 PM (UTC +5:45)	For this we navigate to **Data Artifacts>Installed Programs**

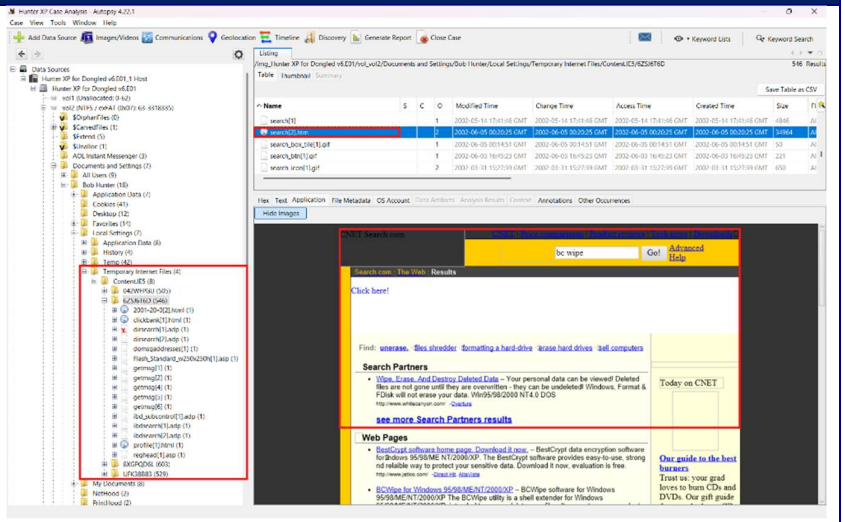
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Here we can find different installed messaging clients like **Yahoo Messenger**, **American Online**, **Outlook Express** and **AOL instant Messenger**.

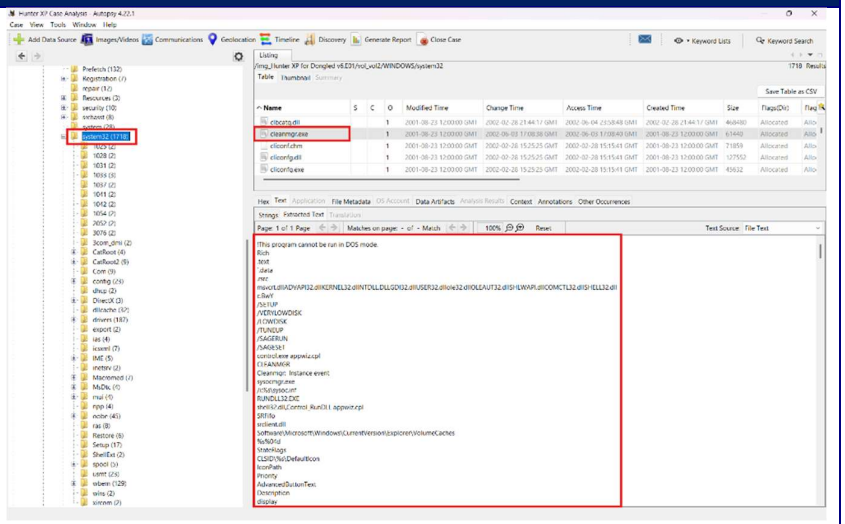
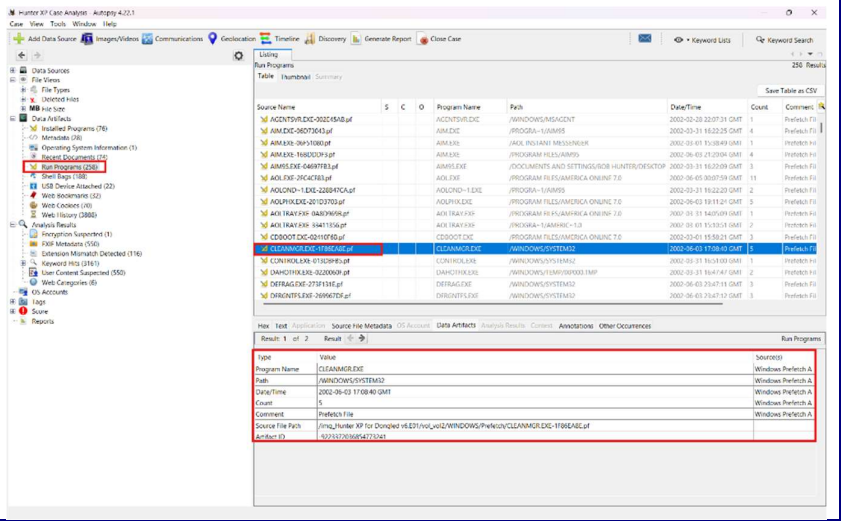
Action	Done?	Date (YY/MM/DD)	Time	Notes
				
Clean-up/Wiping utilities. Check log files. Anything used?	Done	2025/12/13	10:45 PM (UTC +5:45)	Info related to disk wiping was found in this location: **vol_vol2>Documents and Settings>Bob Hunter>Local Settings>Temporary Internet Files>Content.IE5>6ZSJ6T6D>Search [2].htm.**

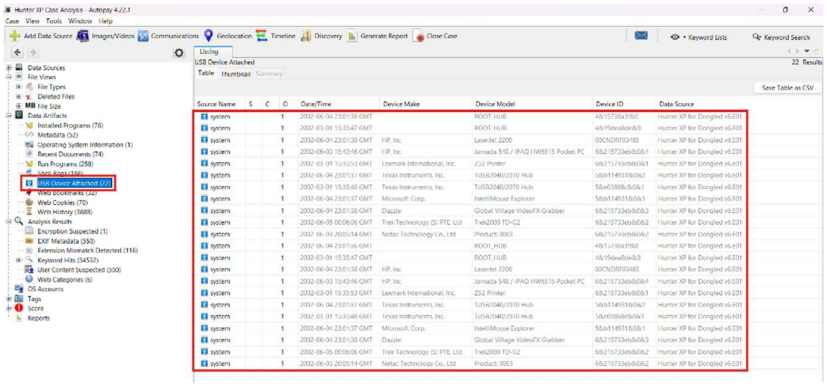
Installed Programs

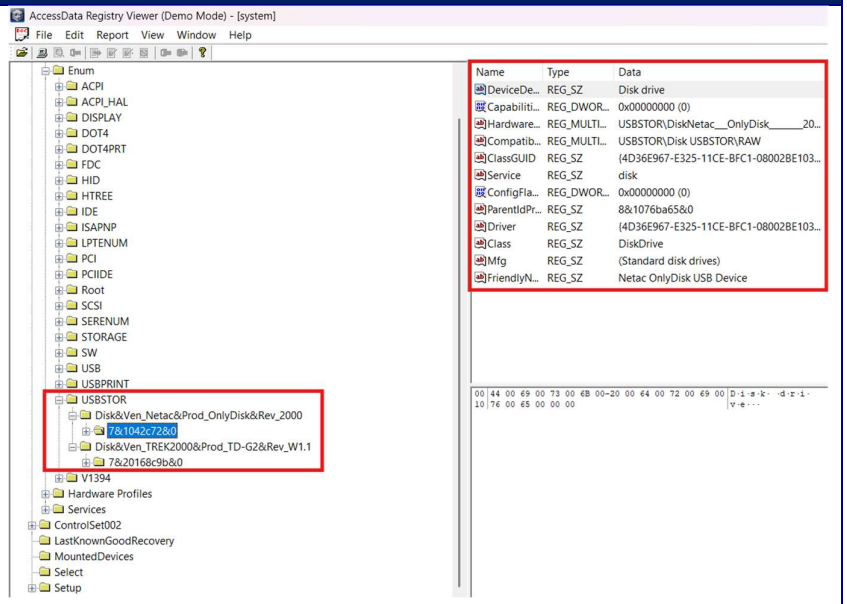
Table | Thumbnail | Summary

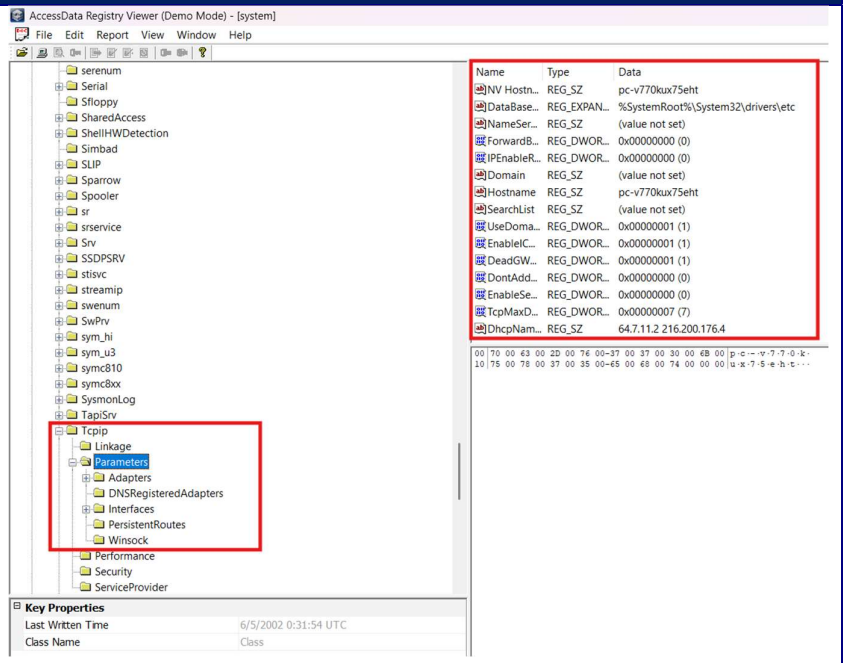
Source Name	S	C	O	Program Name	Date/Time	Data Source
software			1	Copernic 2001 Basic	2002-06-03 10:57:36 GMT	Hunter XP for Dongled v6.E01
software			1	Forté Agent	2002-05-14 11:38:35 GMT	Hunter XP for Dongled v6.E01
software			1	Windows XP Hotfix (SP1) [See Q311967 for more information]	2002-05-14 11:23:08 GMT	Hunter XP for Dongled v6.E01
software			1	Windows XP Application Compatibility Update[Q319580]	2002-05-14 11:22:11 GMT	Hunter XP for Dongled v6.E01
software			1	Yahoo! Messenger Explorer Bar	2002-05-14 10:37:39 GMT	Hunter XP for Dongled v6.E01
software			1	Yahoo! Messenger	2002-05-14 10:36:48 GMT	Hunter XP for Dongled v6.E01
software			1	Windows XP Hotfix (SP1) [See Q309521 for more information]	2002-03-31 11:07:44 GMT	Hunter XP for Dongled v6.E01
software			1	Windows XP Hotfix (SP1) [See Q311889 for more information]	2002-03-31 11:07:17 GMT	Hunter XP for Dongled v6.E01
software			1	Windows XP Application Compatibility Update[Q313484]	2002-03-31 11:06:49 GMT	Hunter XP for Dongled v6.E01
software			1	Windows XP Hotfix (SP1) [See Q315000 for more information]	2002-03-31 11:06:16 GMT	Hunter XP for Dongled v6.E01
software			1	Windows XP Hotfix (SP1) [See Q314862 for more information]	2002-03-31 11:05:55 GMT	Hunter XP for Dongled v6.E01
software			1	Windows XP Hotfix (SP1) [See Q315403 for more information]	2002-03-31 11:05:37 GMT	Hunter XP for Dongled v6.E01
software			1	Windows XP Hotfix (SP1) [See Q314147 for more information]	2002-03-31 11:05:19 GMT	Hunter XP for Dongled v6.E01
software			1	Windows XP Hotfix (SP1) [See Q317277 for more information]	2002-03-31 11:03:47 GMT	Hunter XP for Dongled v6.E01
software			1	AOL Instant Messenger (SM)	2002-03-31 10:37:20 GMT	Hunter XP for Dongled v6.E01
software			1	Java 2 Runtime Environment Standard Edition v1.3	2002-03-01 09:43:18 GMT	Hunter XP for Dongled v6.E01
software			1	Shockwave	2002-03-01 09:41:36 GMT	Hunter XP for Dongled v6.E01
software			1	RealPlayer Basic	2002-03-01 09:24:53 GMT	Hunter XP for Dongled v6.E01
software			1	America Online	2002-03-01 09:24:22 GMT	Hunter XP for Dongled v6.E01
software			1	WebFldrs XP v.9.50.5318	2002-02-28 16:38:56 GMT	Hunter XP for Dongled v6.E01
software			1	Microsoft NetShow Player 2.0	2002-02-28 16:38:39 GMT	Hunter XP for Dongled v6.E01
software			1	MPlayer2	2002-02-28 16:38:39 GMT	Hunter XP for Dongled v6.E01
software			1	Branding	2002-02-28 16:13:05 GMT	Hunter XP for Dongled v6.E01
software			1	PCHealth	2002-02-28 16:07:49 GMT	Hunter XP for Dongled v6.E01
software			1	NetMeeting	2002-02-28 16:07:36 GMT	Hunter XP for Dongled v6.E01
software			1	AddressBook	2002-02-28 16:07:35 GMT	Hunter XP for Dongled v6.E01
software			1	DirectAnimation	2002-02-28 16:07:35 GMT	Hunter XP for Dongled v6.E01
software			1	ICW	2002-02-28 16:07:35 GMT	Hunter XP for Dongled v6.E01
software			1	OutlookExpress	2002-02-28 16:07:35 GMT	Hunter XP for Dongled v6.E01
software			1	DirectDrawEx	2002-02-28 16:07:14 GMT	Hunter XP for Dongled v6.E01
software			1	Fontcore	2002-02-28 16:07:14 GMT	Hunter XP for Dongled v6.E01

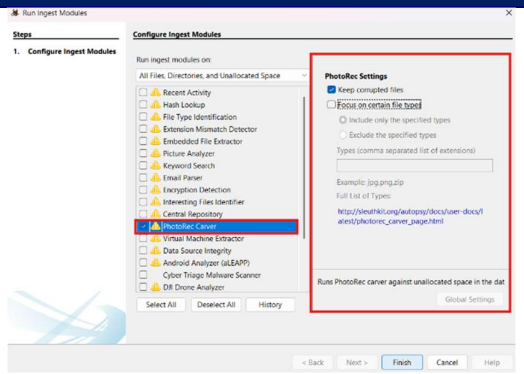
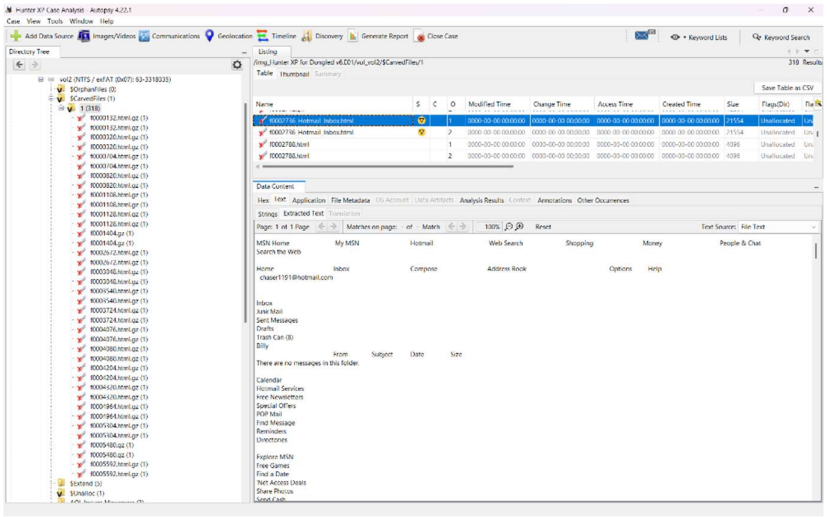
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 BC Wipe is a secure file deletion tool used to remove data beyond recovery. In system32 folder we can see that cleanmgr.exe was found.

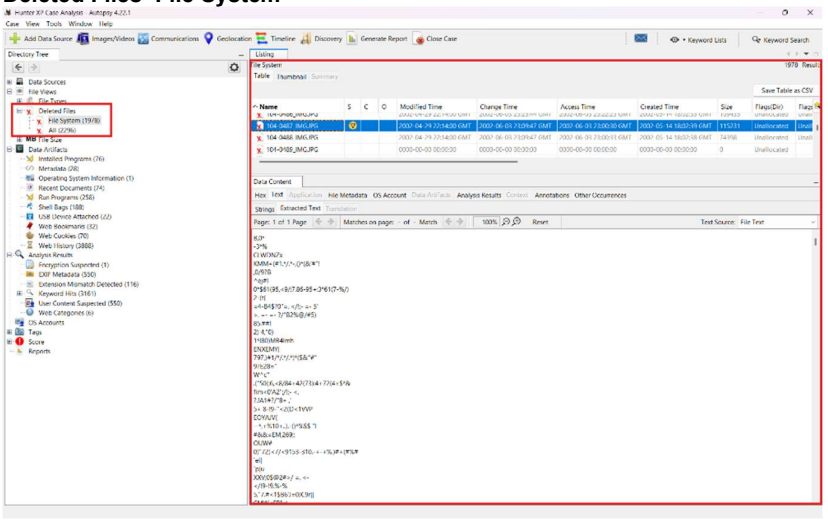
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Cleanmgr.exe is the Windows Disk Cleanup utility. 

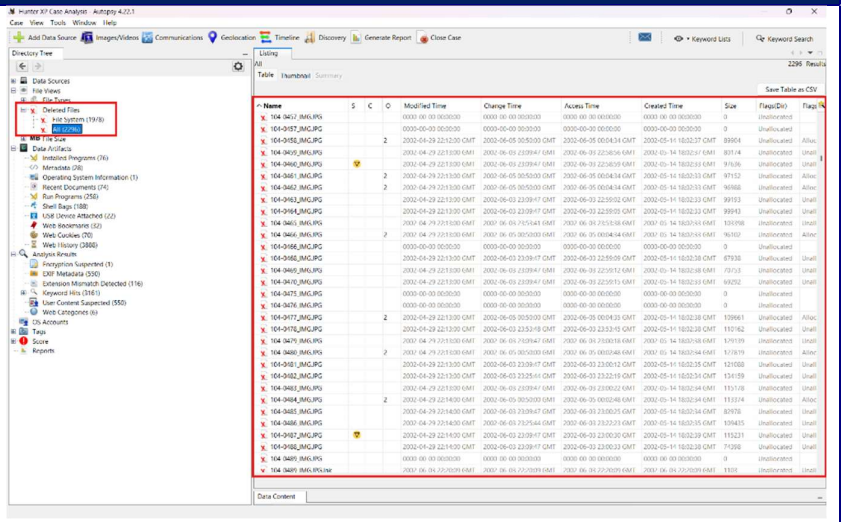
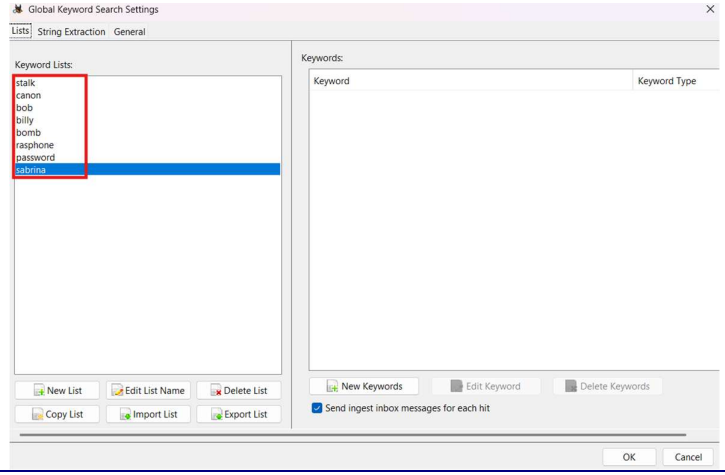
Action	Done?	Date (YY/MM/DD)	Time	Notes
External drives; Network connections	Done	2025/12/14	6:00 PM (UTC +5:45)	We can get the attached USB devices by navigating to Process: **Data Artifacts>USB Device Attached**  We can also get info by extracting and going to this location using "**Registry Viewer**". Process: **SYSTEM>CurrentControlSet>Enum>USBSTOR** Here info on external devices is available:

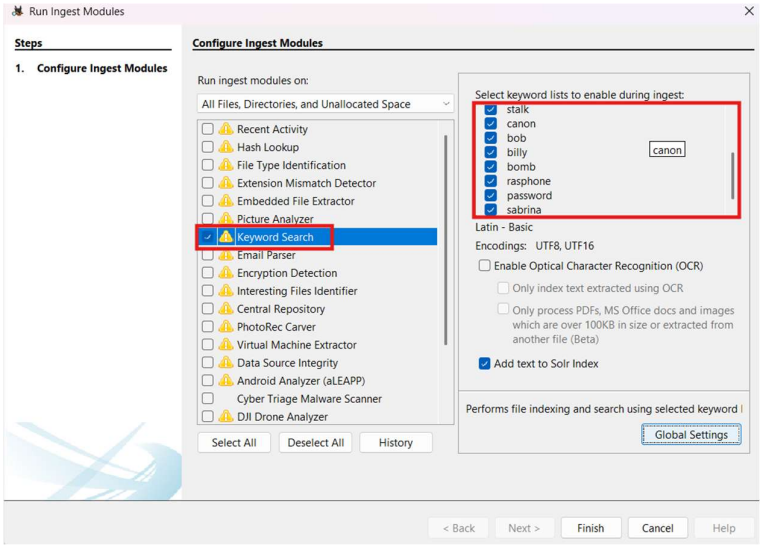
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Likewise for network connections we go to Process: **SYSTEM>CurrentControlSet>Services>Tcpip>Parameters**

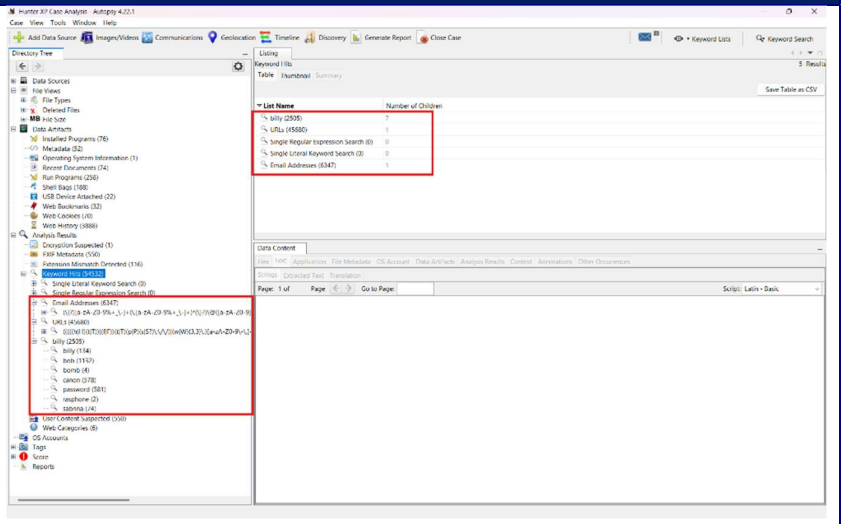
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 From this location we can get network connections.
Perform data carving	Done	2025/12/14	8:00 PM (UTC +5:45)	For this we run a ingest module called "**PhotoRec Caver**". Process: **Tools>Run Ingest Modules>PhotoRec Caver**

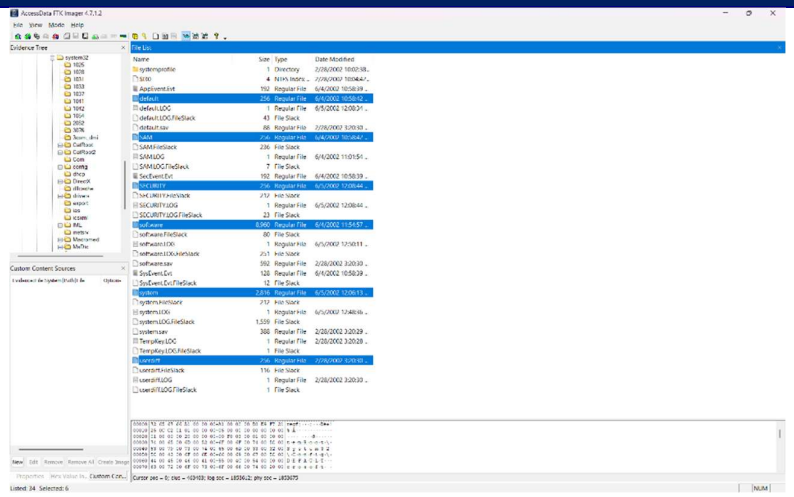
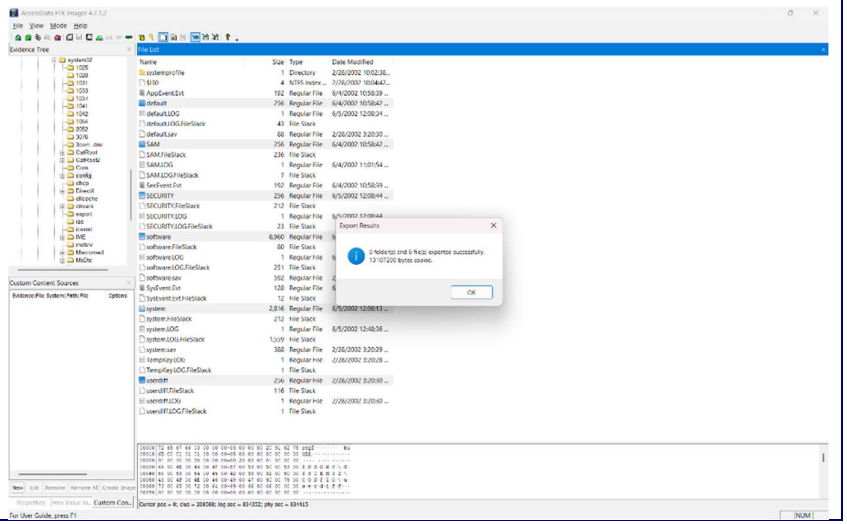
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 After selecting "**PhotoRec Caver Module**" we click finish and proceed. By selecting PhotoRec Caver we get access to these: Process: **Data Source > Hunter XP Dongled > VOL2 > CarvedFiles > 1** 

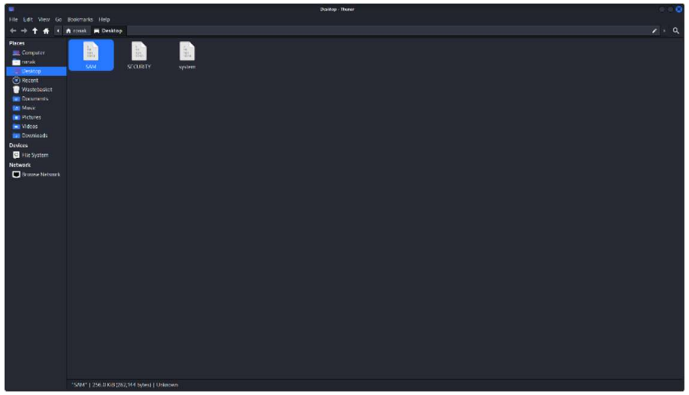
Action	Done?	Date (YY/MM/DD)	Time	Notes
				Process: **Deleted Files>File System**  Process: **Deleted Files>All**

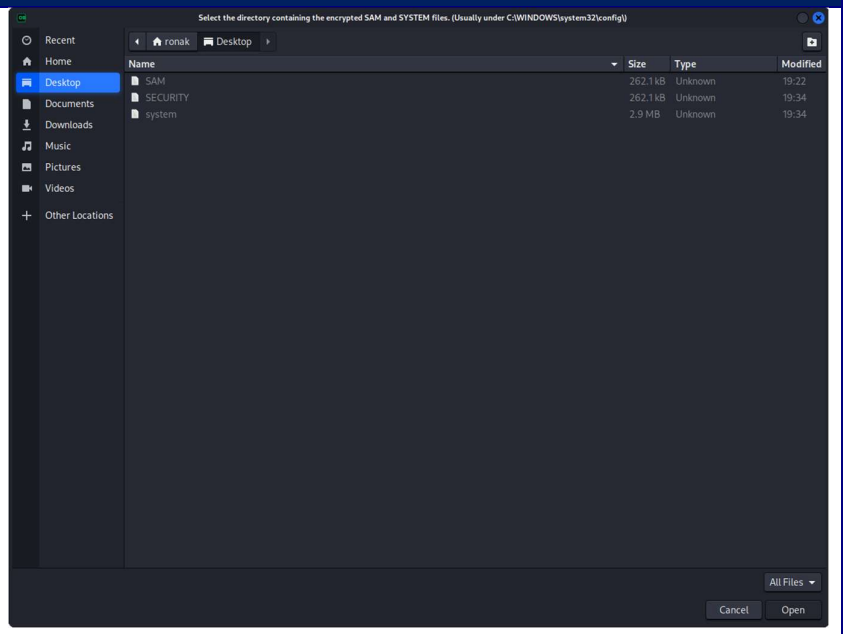
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 With this we are able to recover lost filed and the deleted files were carved.
Run relevant keyword searches; Did you index the evidence file?	Done	2025/12/14	10:00 PM (UTC +5:45)	I mentioned few single-word keywords in the module “**Keyword Search**”. 

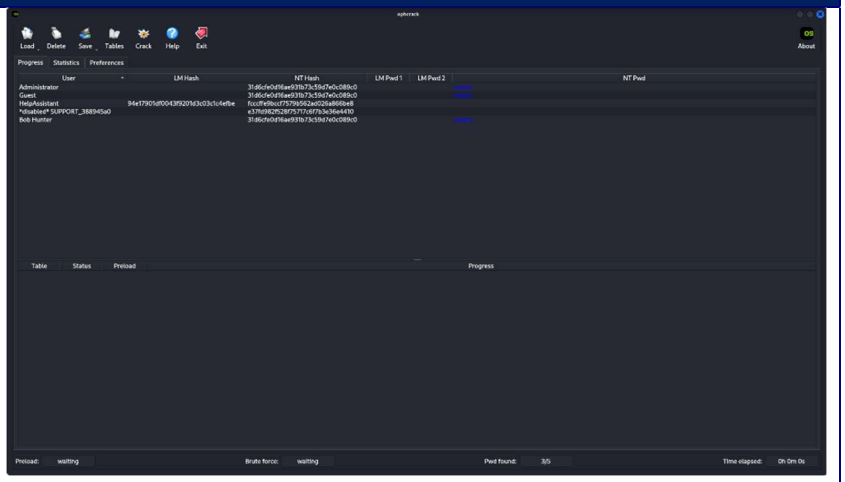
Action	Done?	Date (YY/MM/DD)	Time	Notes
				For this a ingest module was run called “**keyword search**”.  As shown below relevant search has been done:

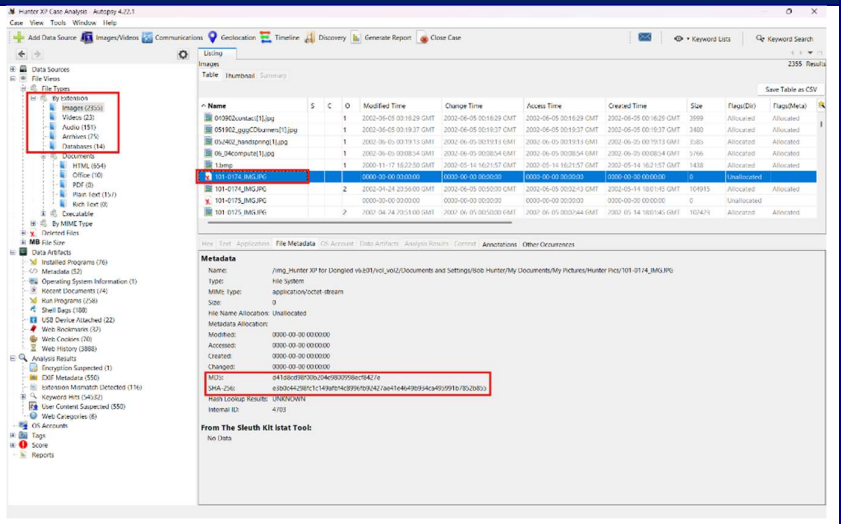
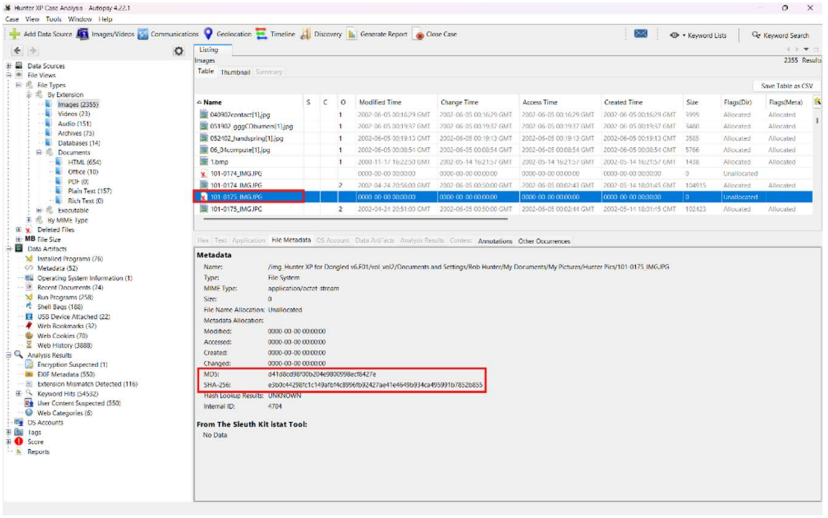
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Under the Single-Keyword Search (**Billy**), I found information about: 1.Billy 2.Bob 3.Bomb 4.Canon 5.Password 6.Rasphone 7.Sabrina
Recover Log-on passwords – use SAMInside/Ophcrack/Encase	Done	2025/12/15	6:00 PM (UTC +5:45)	For this we extract the **SAM**, **SECURITY**, and **SYSTEM** files using ftk imager.

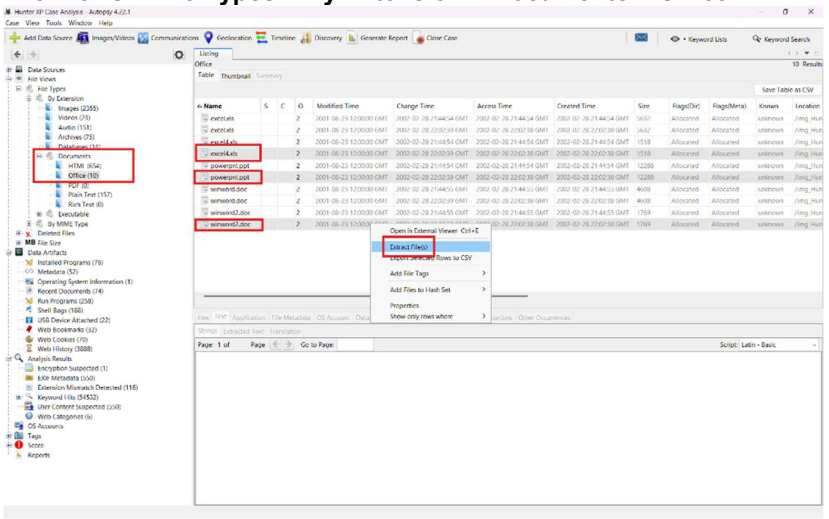
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 We used ftk to access the image file and go to this location **Windows>System32>Config** 

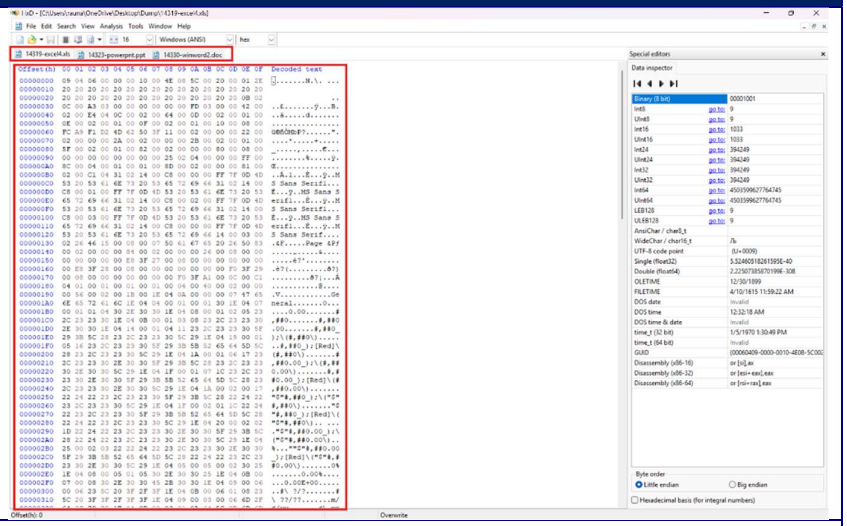
Action	Done?	Date (YY/MM/DD)	Time	Notes
				Here, I extracted the Registry files. **Location: Extract Files>Desktop>H-XP_RegFiles** I used Kali Linux to run **OPHCRACK**. So, I moved these 3 (**Sam, Security, and System**) in Kali Linux.  Now we load up **ophcrack** and load the folder where the needed items are kept at.

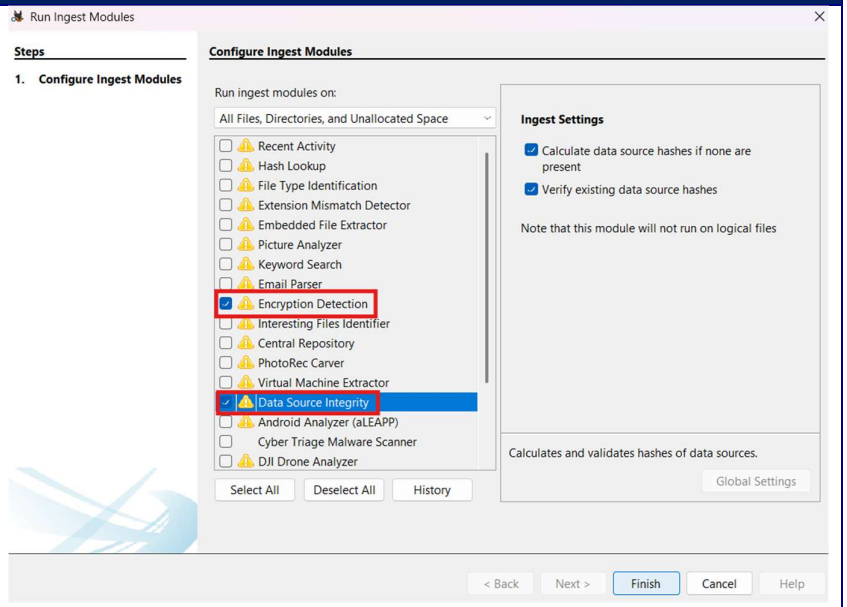
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 With this we are able to get the info we need.

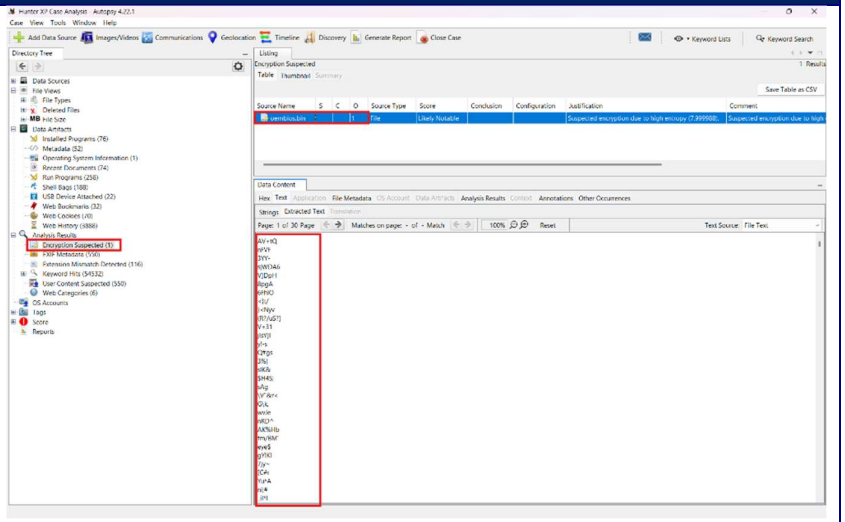
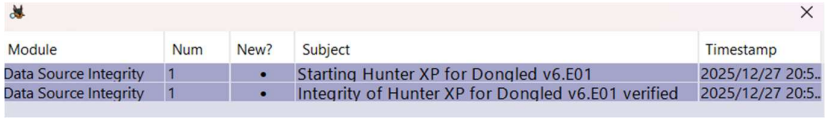
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 We get the following hash which means that there is no password in the system.
Examine different file types: Export doc/office and exe files; look at Metadata if required	Done	2025/12/15	9:00 PM (UTC +5:45)	Here, we analysed the file types in autopsy. We found out that the files in deleted files of different internal ID, apparently, have the same hashes. We go through this procedure by going to **File Views / File Types / By Extension** **File Views > File Types > By Extension** Here, we inspected the image files:

Action	Done?	Date (YY/MM/DD)	Time	Notes
				  The **MD5** and **SHA -256** of all the image files have the same hash values.

Action	Done?	Date (YY/MM/DD)	Time	Notes
				Similarly, For the purpose of inspection, we extracted the doc files. In order to do this, we go to **File Views > File Types > By Extension > Documents > Office**  Then we extract the doc files. **Location: Extract files>Desktop>Dump (Folder)**  And put it through **HxD**. Through which we are able to take a look at the binary data of the doc files.

Action	Done?	Date (YY/MM/DD)	Time	Notes
				
Encryption, Steganalysis (any indications? Entropy or Autopsy can be used)	Done	2025/12/15	11:30 PM (UTC +5:45)	For this process, we run a ingest module called “**Encryption Detection**". Also, if you want to check the integrity of the file, you can run “**Data Source Integrity**”.

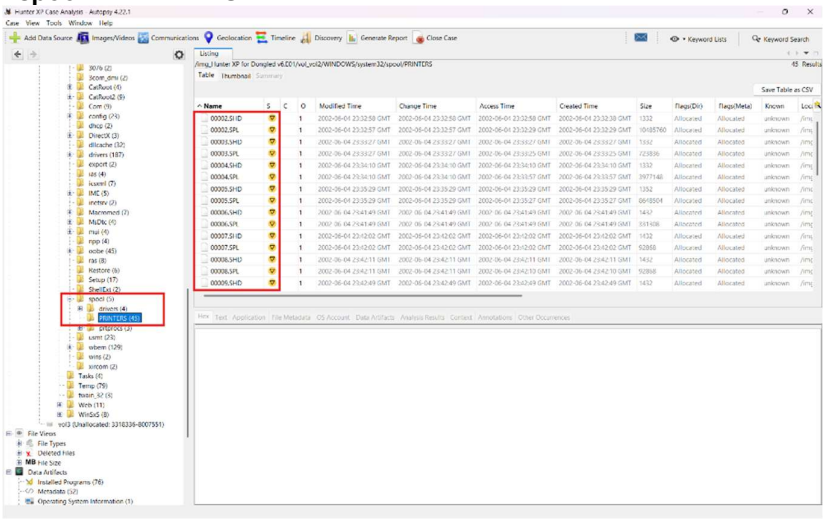
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 With this we can find the Encryption Suspected tab under Analysis Result.

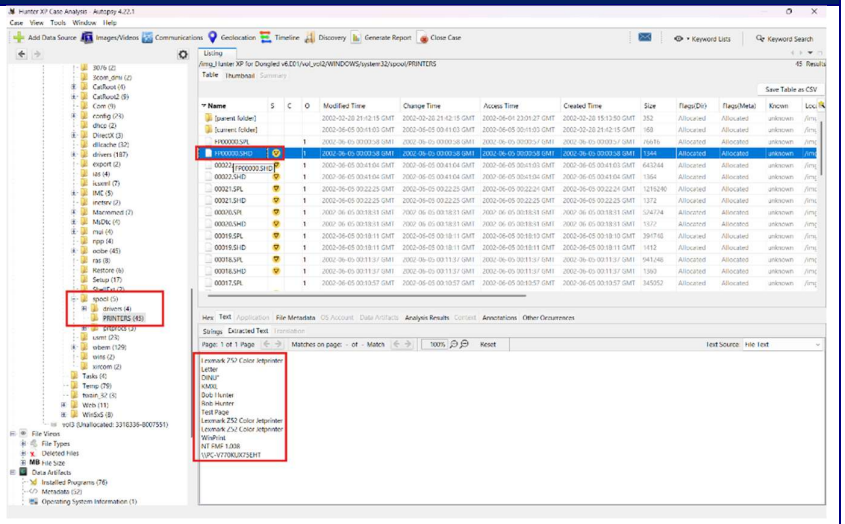
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Here the file **oembios.bin** are suspected to be encrypted. I performed this module to check if the file was tempered or not while performing any task which shows if the file was encrypted or not.  Here is the hash value of the image.  All the forensic task was carried out without any tempering.

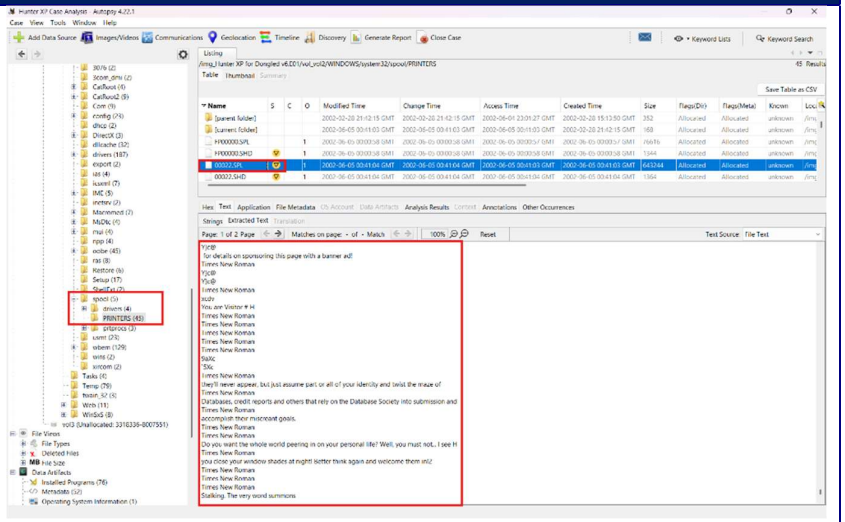
Module	Num	New?	Subject	Timestamp
Data Source Integrity	1	•	Starting Hunter XP for Dongled v6.E01	2025/12/27 20:5..
Data Source Integrity	1	•	Integrity of Hunter XP for Dongled v6.E01 verified	2025/12/27 20:5..

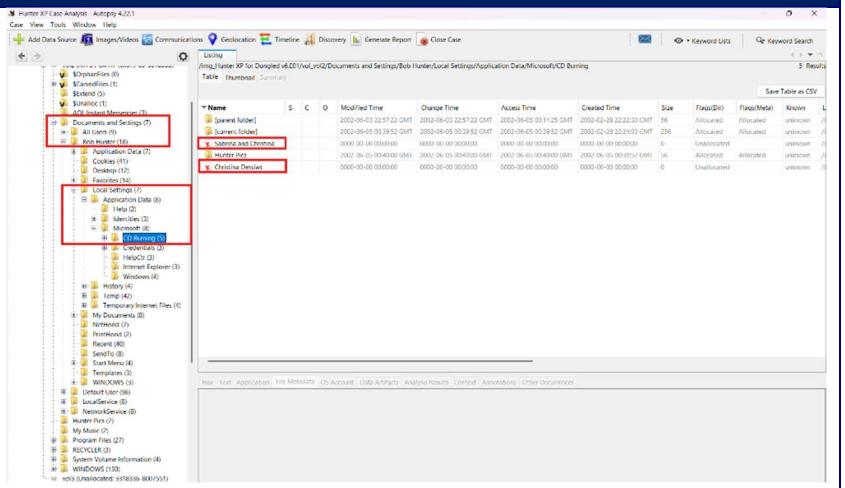
Go to Result Go to Directory

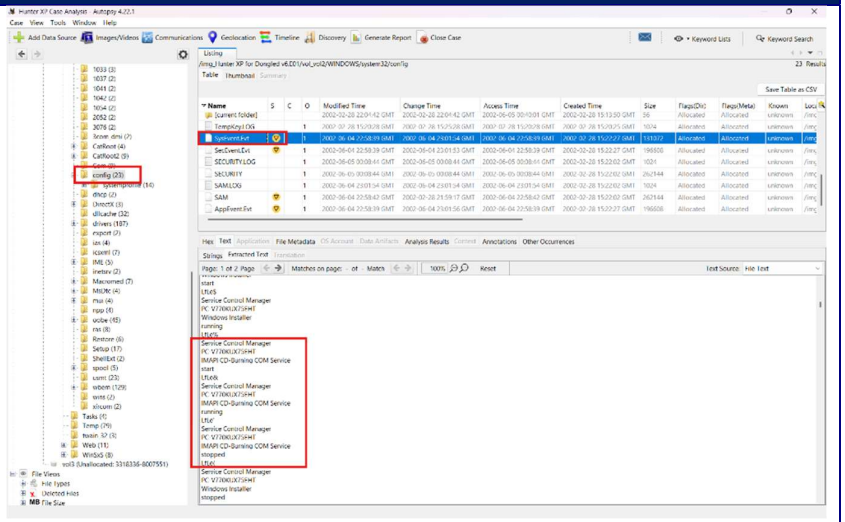
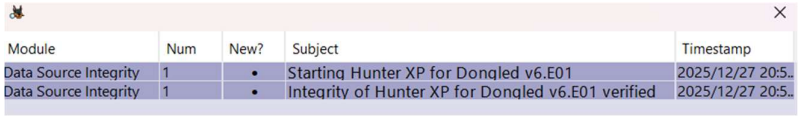
Data Source Verification Results for Hunter XP for Dongled v6.E01
Result: verified
MD5 hash verified
Calculated hash: dfcfe9ab9a60c6ad4a314656b687226b
Stored hash: dfcfe9ab9a60c6ad4a314656b687226b

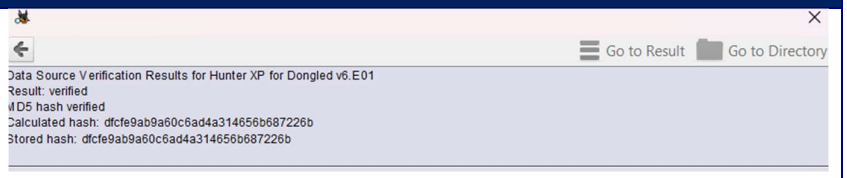
Action	Done?	Date (YY/MM/DD)	Time	Notes
Print artefacts	Done	2025/12/16	8:00 PM (UTC +5:45)	To find the print artifacts we first navigate to Process: **Data Source > Hunter XP Dongled > VOL2 > WINDOWS > system32 >spool > PRINTERS**  Here, we check the .SHD and .SPL files which are likely to be the print artifacts.

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 For .**SHD** Here we can see the print artifacts named 1.HP LaserJet 2200 Series PCL 2.Lexmark Z52 Color Jetprinter

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 For .**SPL** We got information about fonts, databases, etc.
CD/DVD burning apps; check log files	Done	2025/12/16	9:00 PM (UTC +5:45)	We first navigate to, img_Hunter XP for Dongled v6.E01 Process: **vol_vol2 > Documents and Settings > Bob Hunter > Local Settings > Application Data > Microsoft > CD Burning**

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 We can see in the image above, that the two victim's folder **1.Sabrina and Christina** **2.Christina Detsiwt** that contain their pictures, obtained through stalking, have been burned onto an external device. We can find the log through, img_Hunter XP for Dongled v6.E01 Process: **vol_vol2 > WINDOWS > system32 > config > SysEventEvt**

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Here we can see that the suspect used “**IMAPI CD BURNING COM Service**” and the log was stored.
Validate evidence integrity at the end of the examination	Done	2025/12/16	10:00 PM (UTC +5:45)	To validate evidence integrity, we must run a ingest module called Data source integrity. Process: **Tools>Run Ingest Modules>Data Source Integrity>Mail Icon.**  Among them the 2nd has the hash value that we are looking for.

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 Comparing with initial Hash Value.  Data Source Verification Results for Hunter XP for Dongled v6.E01: 1.Result: verified 2.MD5 hash verified 3.Calculated hash: **dfcfe9ab9a60c6ad4a314656b687226b** 4.Stored hash: **dfcfe9ab9a60c6ad4a314656b687226b** The hash value remains the same (i.e. dfcfe9ab9a60c6ad4a314656b687226b) which signifies that no alterations were made.

Additional Notes/Artefacts Examined:

Colour-coding Legend	Tasks
	Fundamental
	Basic
	Elementary
	Secondary
	Advanced
	Exceptional