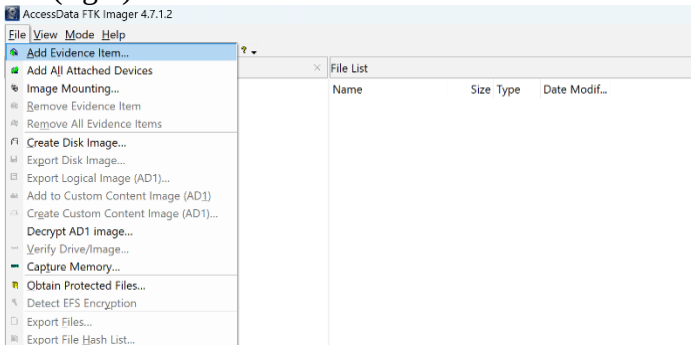
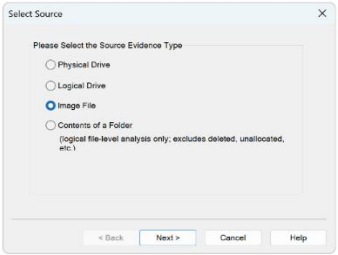
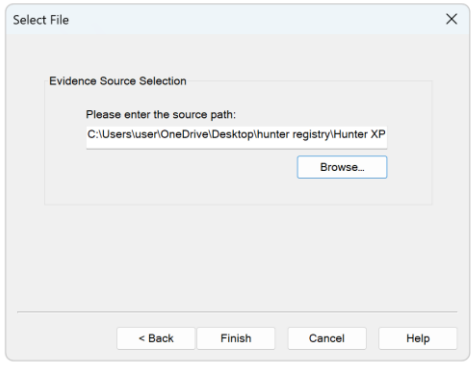
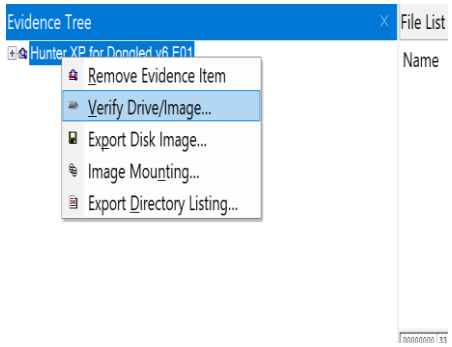
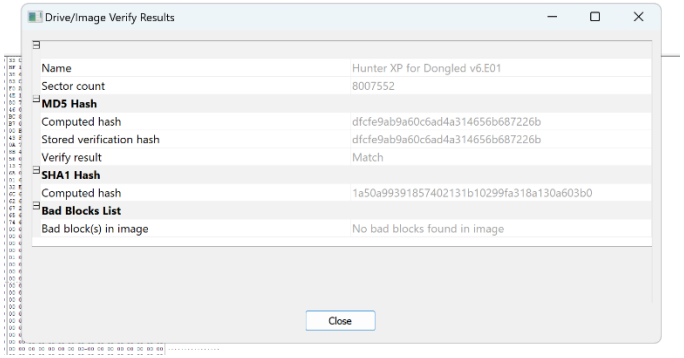
Contemporaneous Notes

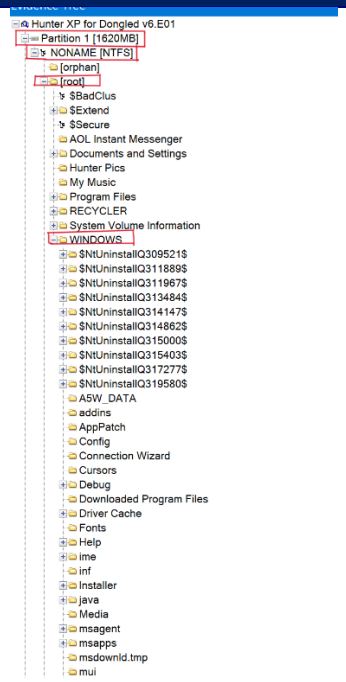
Note: If you decide to omit a process, then you should provide your reasons for doing so. You may add additional rows, as appropriate.

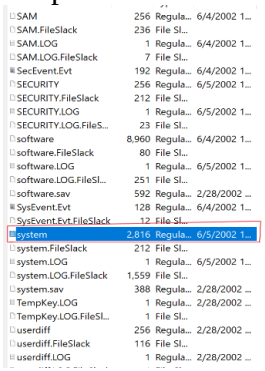
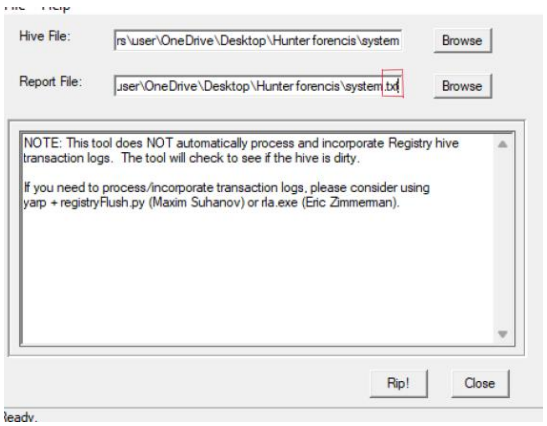
Examiner	Bibek Pandeya	Exam commenced	24th November 2024 12:37 PM
Other relevant information	University ID: 24000863 The whole note is based on Nepali local time (NPT). Path Image/Screenshot	Software used, versions and licensing	All tools are open-sourced 1. Autopsy 4.19.2 2. AccessData FTK Imager 4.7.1.2 3. RegRipper 3.0 4. AccessData Registry Viewer 1.8.0.5 5. Kali Linux 2023.3 6. Ophcrack 3.8.0

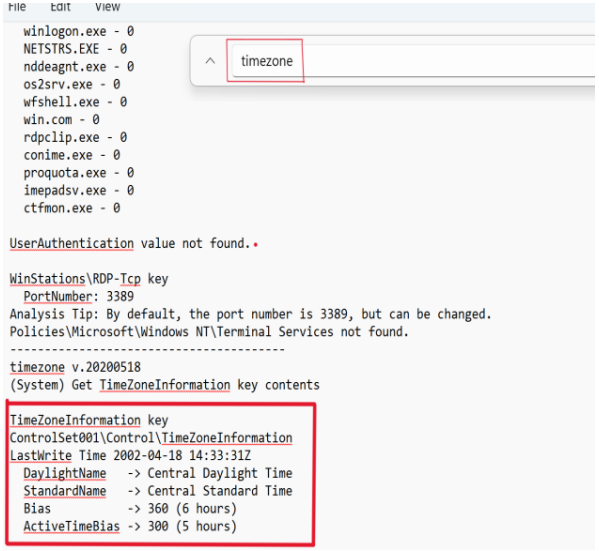
Action	Done?	Date	Time	Notes
Load case and verify image	Yes	24th November 2024	1:26 PM	**1.** To load an image, first open the software **AccessData FTK Imager** and then add the image file you wish to investigate. Shown in the (fig.1):  Fig.1  Fig.2

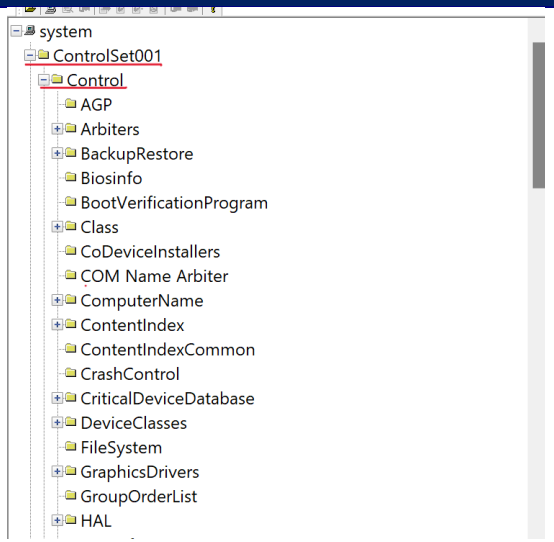
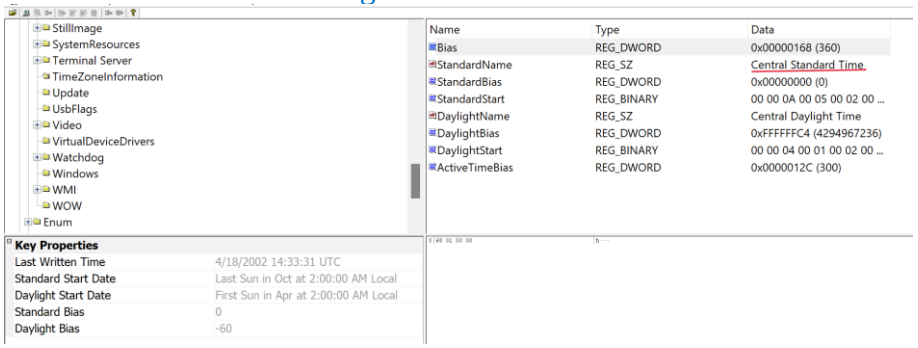
Action	Done?	Date	Time	Notes
				Since I already have an image for investigation, I need to select the image file from its appropriate location. (fig.2&3)  Fig.3 2. After successfully loading the image file, the next step is to verify its hash value. To do this, right-click on the image and select **"Verify Drive/Image". (**fig.4)  Fig.4

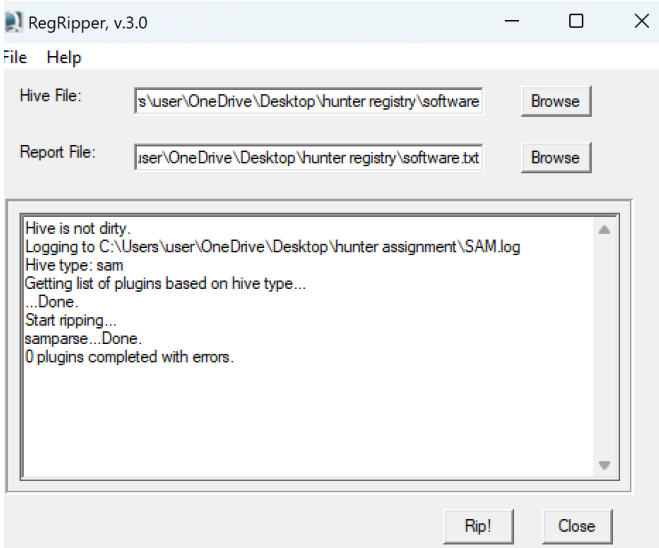
Action	Done?	Date	Time	Notes
				After clicking on the **"Verify"** option, the MD5 and SHA1 hash values of the image file will be displayed. (fig.5)  Fig.5
Load Case into second forensic tool for dual verification of at least 2 key artefacts, evidence items	Yes	24th November 2024	2:45 PM	For this task we will use three tools **AccessData Registry viewer 1.0.8.5**, **Reg ripper 3.0** & **AccessData FTK Imager.** To gather information about **TimeZone** & **Operating system Details** of suspect from the file **SYSTEM** & **SOFTARE.** 1, TimeZone Using **RegRipper 3.0** At first load the hunter xp image file to AccessData FTK Imager. Then, we search for the SAM, SECURITY, SOFTWARE, SYSTEM. LOCATION: Hunterxp/Partion 1/Noname/root/windows/system32/config

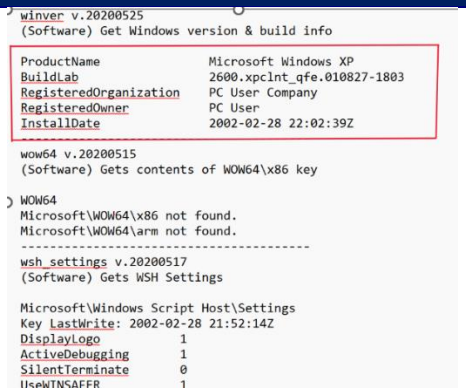
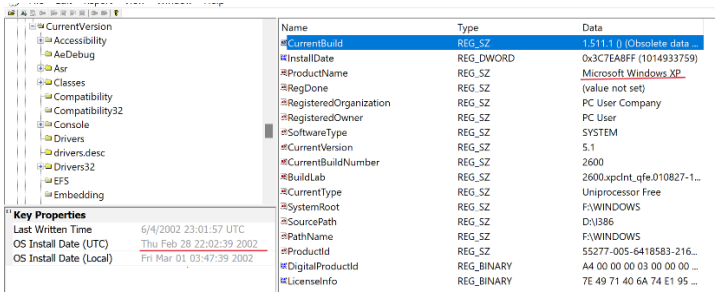
Action	Done?	Date	Time	Notes
				 Fig.6 Fig.7

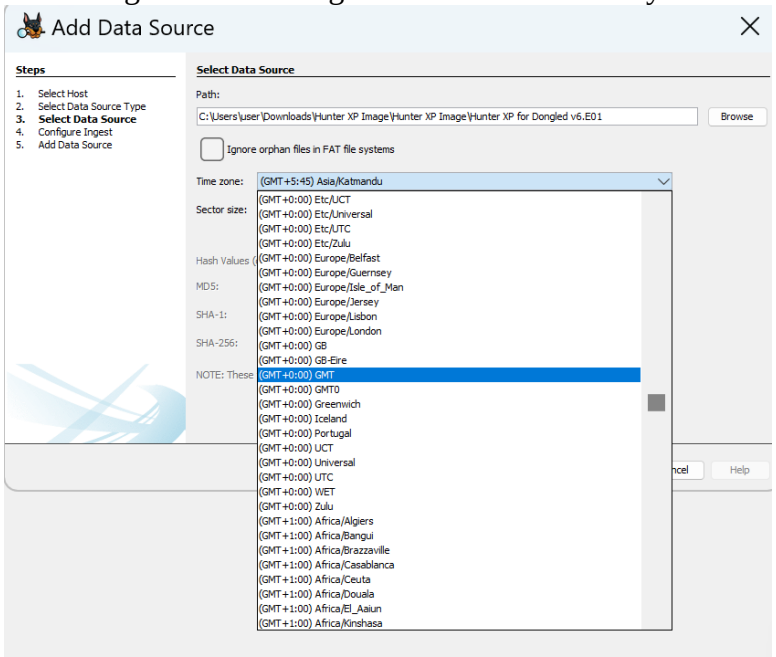
Action	Done?	Date	Time	Notes
				Now, after selecting Config search for SYSTEM because SYSTEM is the place where we can find Time Zone.  Fig.8 Now, after finding the system file export the file by right clicking to the file and giving the appropriate location. After exporting the file, input the file into the “REG RIPPER” software and create a report file in text format.  Fig.9 After clicking the rip option txt file appears in the same folder where TimeZone can be accessed by searching into the text file.

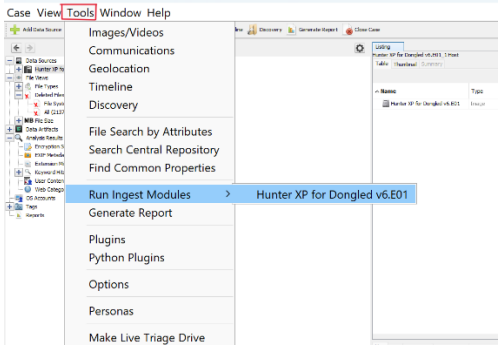
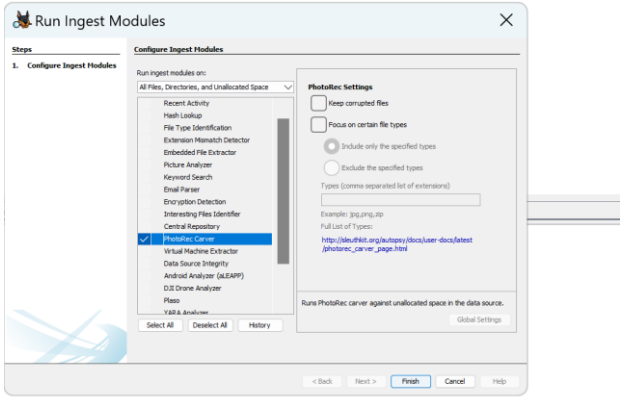
Action	Done?	Date	Time	Notes
				In the txt file we simply search for keyword TimeZone with the key "CTRL+F".  File Edit View winlogon.exe - 0 NETSTRS.EXE - 0 nddeagnt.exe - 0 os2srv.exe - 0 wfshell.exe - 0 win.com - 0 rdpclip.exe - 0 conime.exe - 0 proquota.exe - 0 imepadsv.exe - 0 ctfmon.exe - 0 timezone UserAuthentication value not found. WinStations\RDP-Tcp key PortNumber: 3389 Analysis Tip: By default, the port number is 3389, but can be changed. Policies\Microsoft\Windows NT\Terminal Services not found. ---------- timezone v.20200518 (System) Get TimeZoneInformation key contents TimeZoneInformation key ControlSet001\Control\TimeZoneInformation LastWrite Time 2002-04-18 14:33:31Z DaylightName -> Central Daylight Time StandardName -> Central Standard Time Bias -> 360 (6 hours) ActiveTimeBias -> 300 (5 hours) Fig.10 1.1, TimeZone Using **Registry Viewer 1.0.8.5** To know the TimeZone of The HunterXP file load the system file in registry viewer and navigate through location: System/controlset001/control/

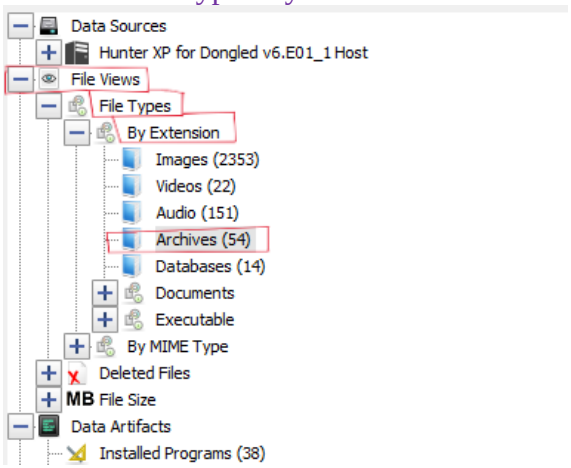
Action	Done?	Date	Time	Notes
				 Fig.11  Fig.12 2, operating System information Using Reg ripper 3.0 For details of the operating system, repeat the process of TimeZone analysis, but the difference is investigating the SOFTWARE file not the SAM or SYSTEM file.

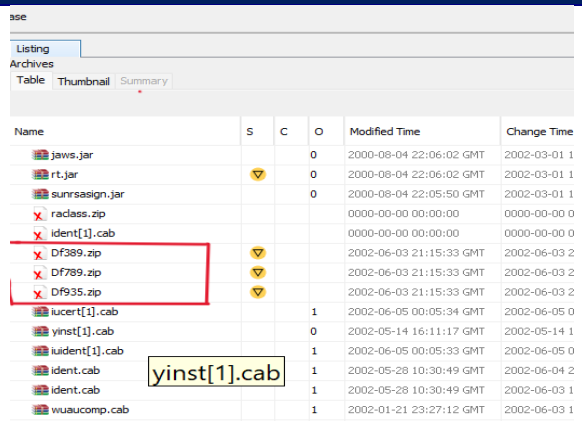
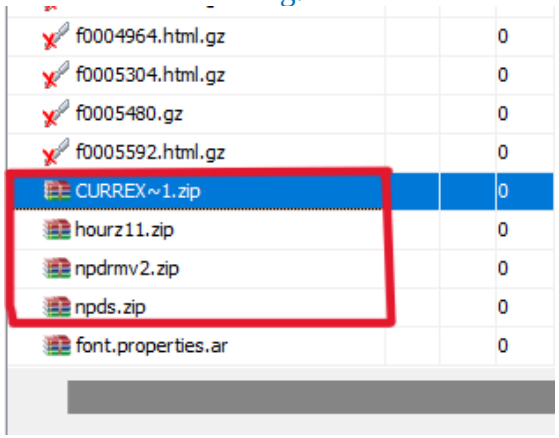
Action	Done?	Date	Time	Notes
				Same as before after exporting the file from autopsy put the SOFTWARE file in the Reg ripper 3.0 tool to get the text file for the required information.  Fig.13 After searching the SOFTWARE file, it will show the details about operating system.

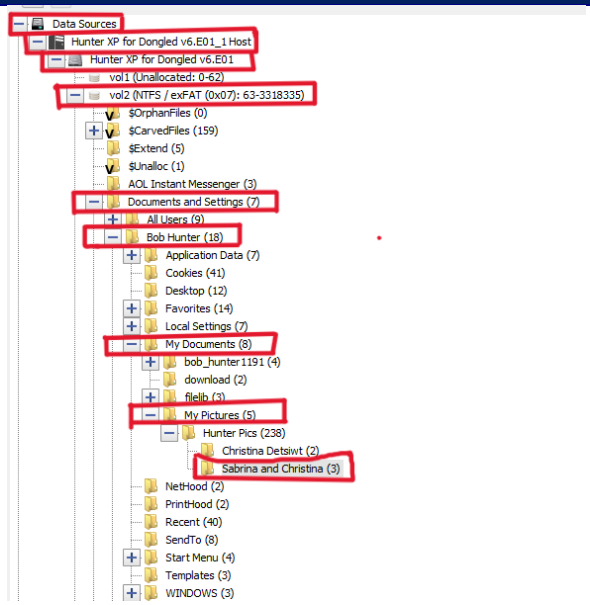
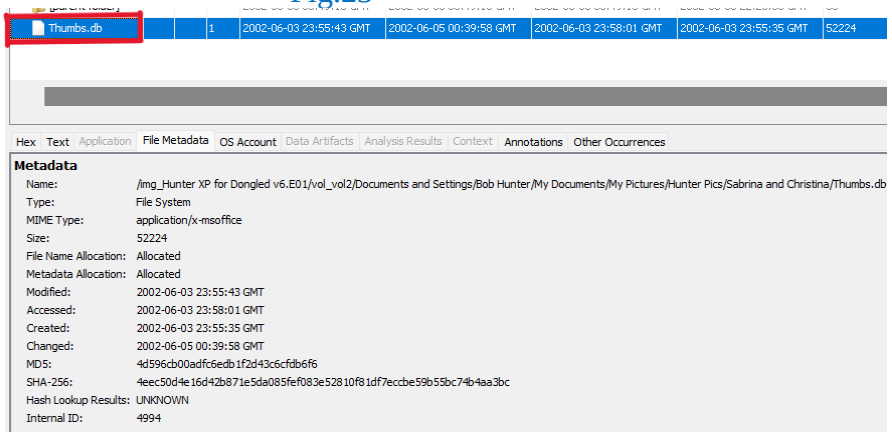
Action	Done?	Date	Time	Notes
				 winver v.20200525 (Software) Get Windows version & build info ProductName Microsoft Windows XP BuildLab 2600.xpclnt_qfe.010827-1803 RegisteredOrganization PC User Company RegisteredOwner PC User InstallDate 2002-02-28 22:02:39Z wow64 v.20200515 (Software) Gets contents 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 Fig.14 2.1, Operating System Information Using **Registry Viewer 1.0.8.5** To get the information first load the Software file exported From AccessData FTK Imager in "Registry Viewer 1.0.8.5", then navigate through the location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion  Fig.15 Therefore, we can see both Artifacts exactly match with each other. We can see Fig (10 & 12) which show the same TimeZone details. Similarly, In the Fig (14 & 15) we can see similar result of operating system.

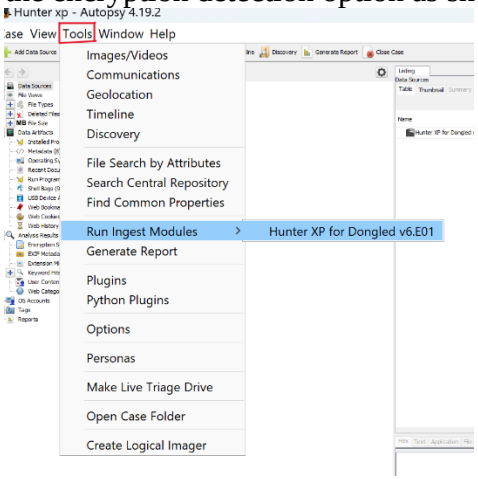
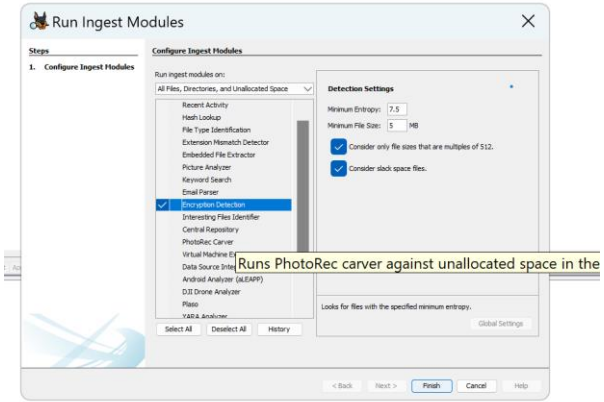
Action	Done?	Date	Time	Notes
Time Zone Adjusted? Report Time Zone used for Analysis.	Yes	24th November 2024	3:35 PM	Yes, we adjusted Time zone of the Hunter Xp image file as per the UK local time which is (GMT +0:00) GMT Because we are examining the file as assignment and the university is at UK. (fig.16)  Fig.16 The Actual Time zone is (GMT +5:45) Asia/Kathmandu but we adjusted the time zone to (GMT +0:00) GMT Because as I mentioned above, we are student at UK university.

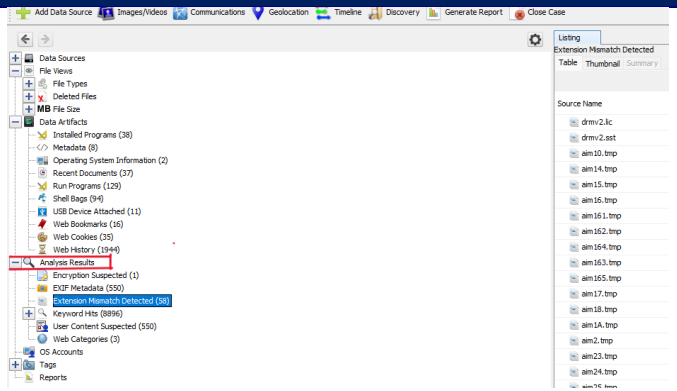
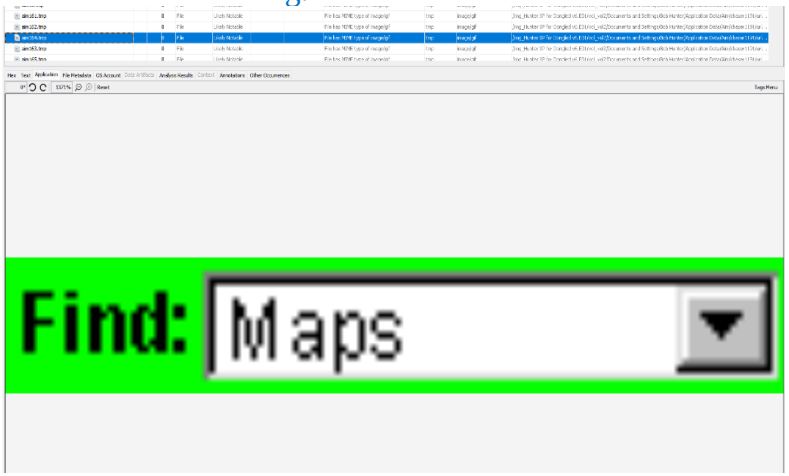
Action	Done?	Date	Time	Notes
Recover lost folders (NTFS, FAT16&32).	Yes	24th November 2024	4:03 Pm	Just after following the directions below, we can easily recover deleted folders. (fig.17) 1. Select the **Ingest Module** for **"PhotoRec Carver"** to recover all deleted files. 2. Navigate to the **Deleted Files** or **Unallocated Space** folder. 3. PATH: **Tool/RunningIngestModule/HunterXP/PhotoRec Carver**.  Fig.17  Fig.18 From here, we can see all deleted files a total of 2137 (fig.19).

Action	Done?	Date	Time	Notes
				 Fig.19
Mount archives; zip, thumbs.db, etc.	Yes	24th November 2024	5:12 Pm	To see the Zip Files, Navigate through the location(fig.20) Fileviews/Filetypes/Byextension/Archives  Fig.20 Here, the file whose name ends with .zip are the Zip files, (fig.21)

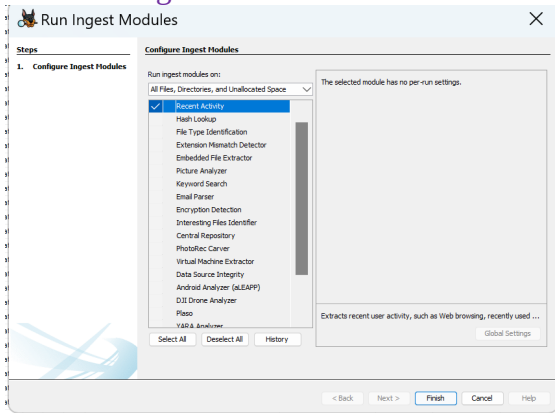
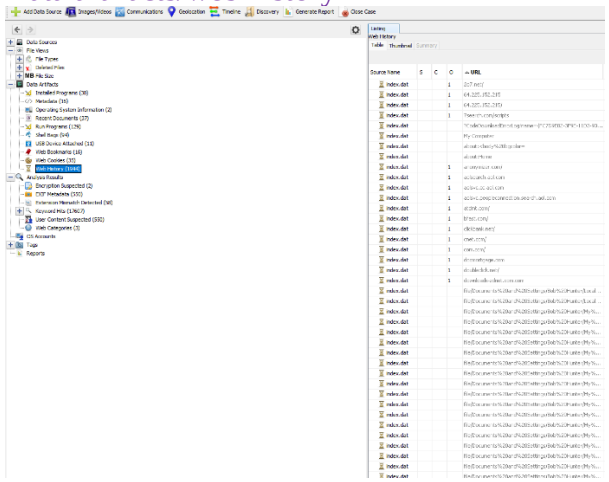
Action	Done?	Date	Time	Notes
				 Fig.21  Fig.22 Now For thumbs. Db Navigate through the location:(fig.23) Hunterxp/volvol2/Documents&setting/bobhunter/mydocuments/mypictures/hunterpics/sabina&christina

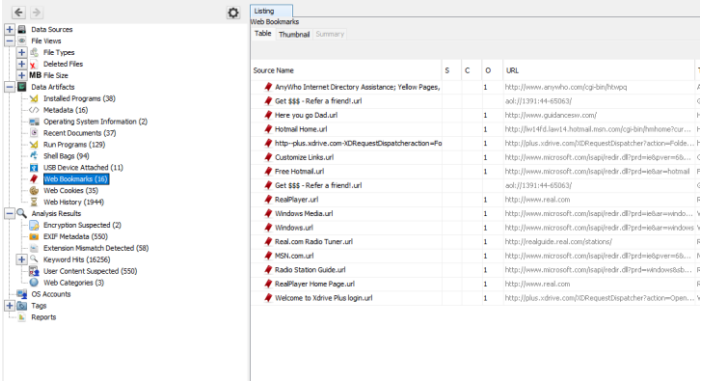
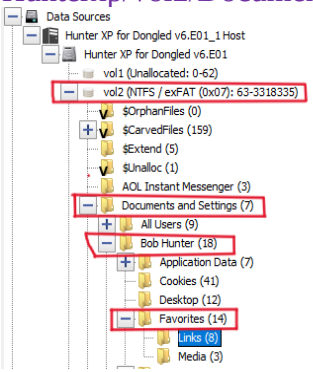
Action	Done?	Date	Time	Notes
				 Fig.23  Fig.24 Here, after reaching the location we can a file name “thumbs. dp” which is the only one file that exists as a db. file.

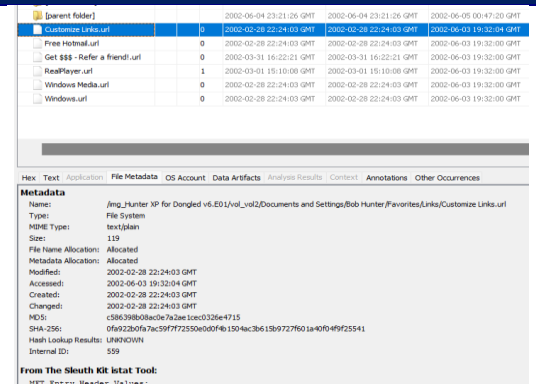
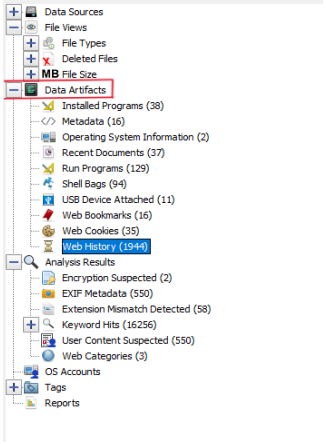
Action	Done?	Date	Time	Notes
File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation)	Yes	25th November 2024	11:48 Am	To see any file mismatch select run ingest module after that execute the encryption detection option as shown below:(fig.25)  Fig.25  Fig.26 After going through ingest module navigate through Analysis result and extension mismatch option.

Action	Done?	Date	Time	Notes
				 Fig.27  Fig.28

Action	Done?	Date	Time	Notes
				 Fig.29 As from the hex number “47 49 46 38” this is the GIF file, but suspect tried to temper the file. (fig.30) • **GIF**: `47 49 46 38` (`GIF87a` or `GIF89a`) • **JPEG/JFIF**: `FF D8 FF E0` (or `FF D8 FF Ex` for various types) • **PNG**: `89 50 4E 47 0D 0A 1A 0A` • **BMP**: `42 4D` • **TIFF**: `49 49 2A 00` (Little-endian) or `4D 4D 00 2A` (Big-endian) • **WebP**: `52 49 46 46` followed by `57 45 42 50` • **ICO**: `00 00 01 00` Fig.30

Action	Done?	Date	Time	Notes
Internet History, favourites, etc. Other browsers?	Yes	25th November 2024	1:08 Pm	(fig.31) First, run the ingest module for information about internet history: Tools/runingestmodule/**recent activities**/  Fig.31 After that we navigate through: Data artifacts/web history  Fig.32

Action	Done?	Date	Time	Notes
				These are the websites or internet history which are accessed by the suspect “bob hunter”. In this Index.dat file we can see a lot of websites visited by the suspect. 2, Bookmarks, Favourites These are the links or URL the suspect has bookmarked(fig.33). Bookmarks:  Fig.33 For the favourites need to go to this location:(fig.34) Hunterxp/vol2/Documents and setting/Bob hunter/favourites  Fig.34

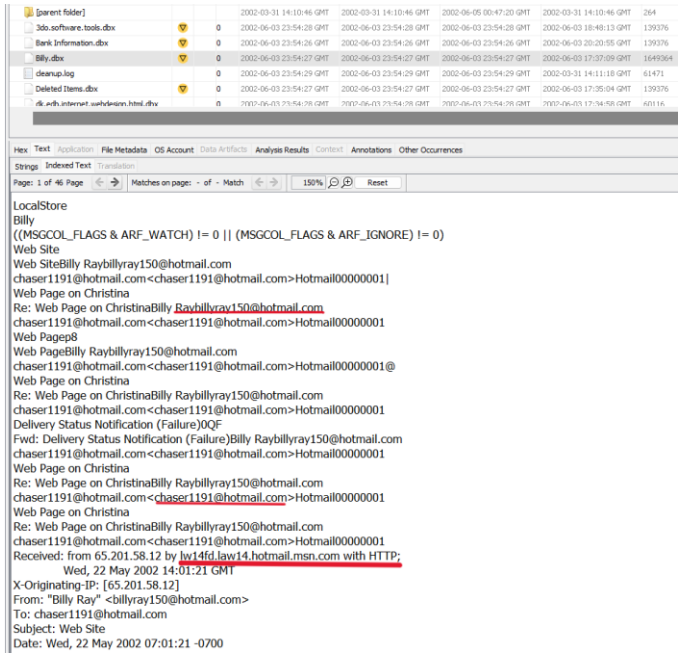
Action	Done?	Date	Time	Notes
				 Fig.35 The browser used by the suspect is Internet Explorer: To see all the websites accessed using the browser navigate through the location: DataArtifacts/webhistory/  Fig.36

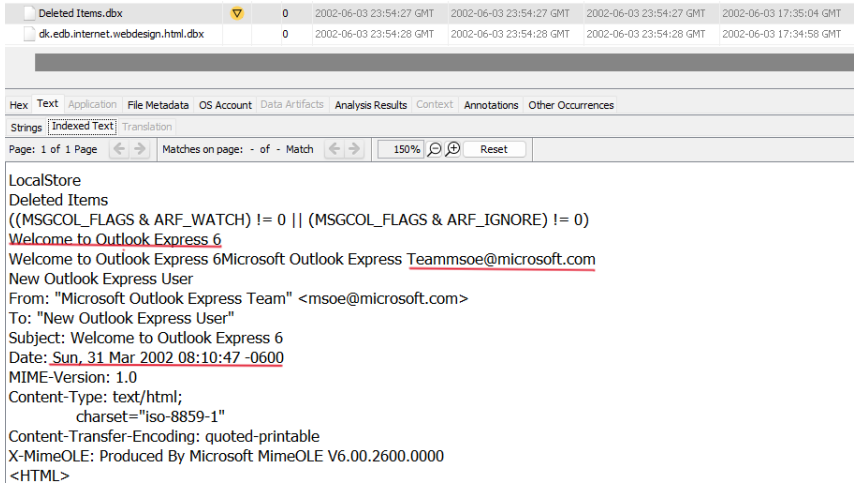
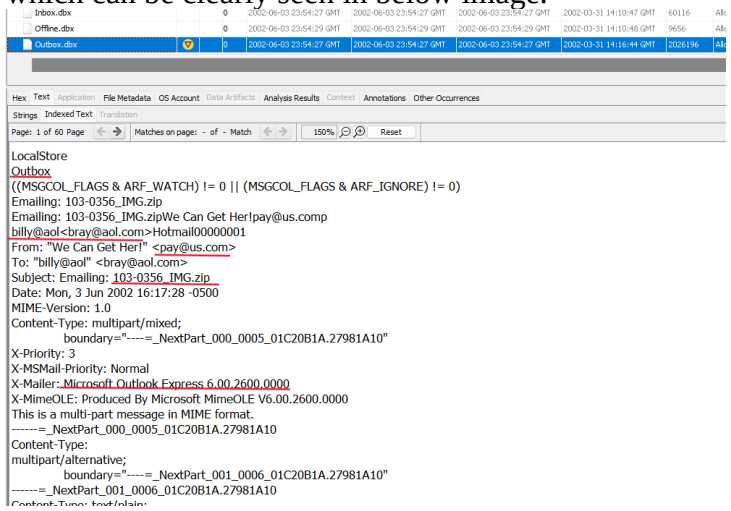
Action	Done?	Date	Time	Notes

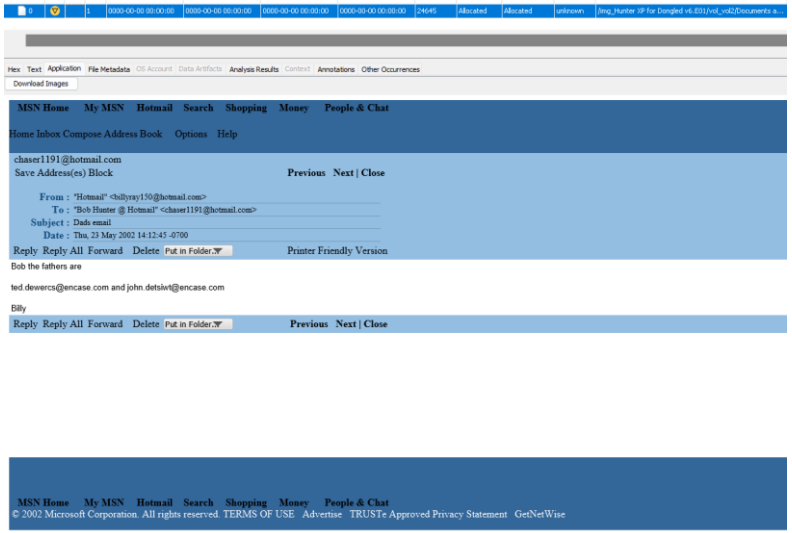
Source Name	S	C	O	URL	Date Accessed	Referrer URL	Program Name	Domain	Username	Data Source
index.dat		1		2o7.net/	2002-06-03 15:26:12 GMT		Internet Explorer	2o7.net	Cookie:bob hunter	Hunter XP for Dongled v6.E01
index.dat		1		64.225.152.215	2002-06-03 13:07:25 GMT		Internet Explorer	64.225.152.215	Bob Hunter	Hunter XP for Dongled v6.E01
index.dat		1		64.225.152.215/	2002-06-03 13:07:22 GMT		Internet Explorer	64.225.152.215	Cookie:bob hunter	Hunter XP for Dongled v6.E01
index.dat		1		7search.com/scripts	2002-06-04 18:49:18 GMT		Internet Explorer	7search.com	Cookie:bob hunter	Hunter XP for Dongled v6.E01
index.dat				7CodeDownloadErrorLog?name={FC7D9E02-3F9E-11D3-93...	2002-05-14 13:01:05 GMT		Internet Explorer			Hunter XP for Dongled v6.E01
index.dat				My Computer	2002-06-03 11:42:45 GMT		Internet Explorer		Bob Hunter	Hunter XP for Dongled v6.E01
index.dat				about:<body%20bgcolor=	2002-06-03 10:57:10 GMT		Internet Explorer		Bob Hunter	Hunter XP for Dongled v6.E01
index.dat				about:Home	2002-02-28 16:37:55 GMT		Internet Explorer		Bob Hunter	Hunter XP for Dongled v6.E01
index.dat		1		anonymizer.com/	2002-06-04 18:56:27 GMT		Internet Explorer	anonymizer.com	Cookie:bob hunter	Hunter XP for Dongled v6.E01
index.dat		1		aolsearch.aol.com	2002-06-04 18:30:27 GMT		Internet Explorer	aol.com	Bob Hunter	Hunter XP for Dongled v6.E01
index.dat		1		aolsvc.cc.aol.com	2002-06-04 18:37:47 GMT		Internet Explorer	aol.com	Bob Hunter	Hunter XP for Dongled v6.E01
index.dat		1		aolsvc.peopleconnection.search.aol.com	2002-06-04 18:29:54 GMT		Internet Explorer	aol.com	Bob Hunter	Hunter XP for Dongled v6.E01
index.dat		1		atdmt.com/	2002-06-03 12:45:17 GMT		Internet Explorer	atdmt.com	Cookie:bob hunter	Hunter XP for Dongled v6.E01
index.dat		1		bfast.com/	2002-06-04 18:49:18 GMT		Internet Explorer	bfast.com	Cookie:bob hunter	Hunter XP for Dongled v6.E01
index.dat		1		clickbank.net/	2002-06-04 18:49:17 GMT		Internet Explorer	clickbank.net	Cookie:bob hunter	Hunter XP for Dongled v6.E01
index.dat		1		cnet.com/	2002-06-04 18:34:30 GMT		Internet Explorer	cnet.com	Cookie:bob hunter	Hunter XP for Dongled v6.E01
index.dat		1		com.com/	2002-06-04 18:31:31 GMT		Internet Explorer	com.com	Cookie:bob hunter	Hunter XP for Dongled v6.E01
index.dat		1		docmortgage.com	2002-06-03 15:27:36 GMT		Internet Explorer	docmortgage.com	Bob Hunter	Hunter XP for Dongled v6.E01
index.dat		1		doubleclick.net/	2002-06-04 18:34:25 GMT		Internet Explorer	doubleclick.net	Cookie:bob hunter	Hunter XP for Dongled v6.E01
index.dat		1		downloads-zdnet.com.com	2002-06-04 18:31:33 GMT		Internet Explorer	com.com	Bob Hunter	Hunter XP for Dongled v6.E01

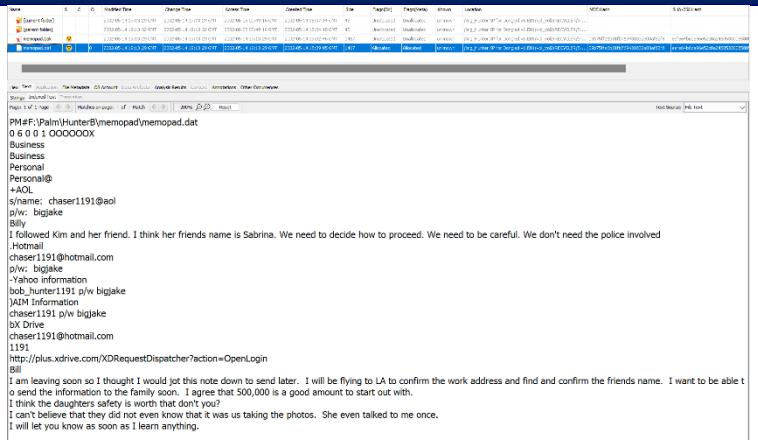
Fig.37

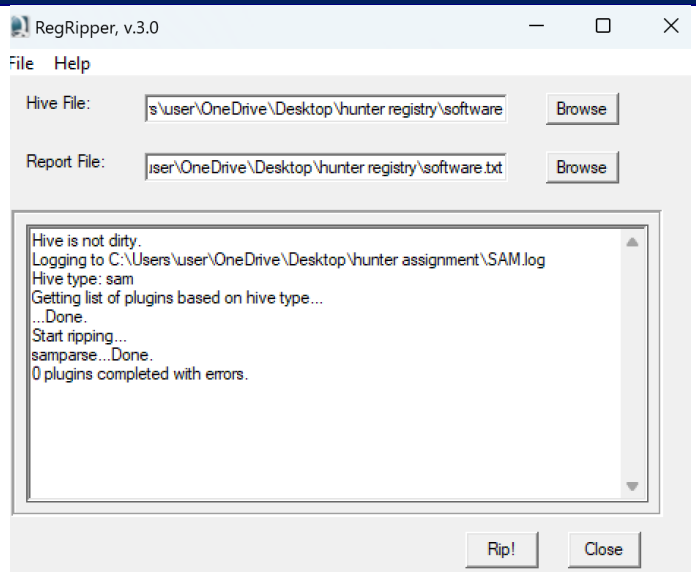
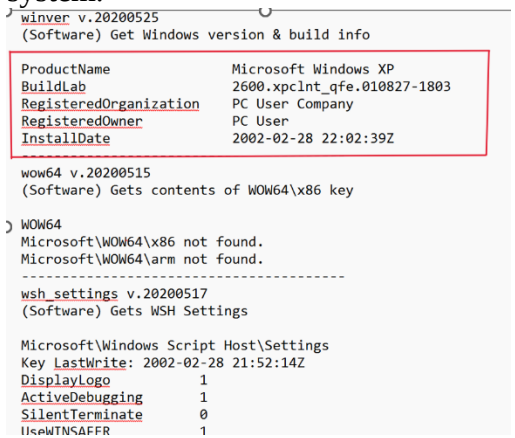
Action	Done?	Date	Time	Notes
Emails, local and web based.	Yes	25th November 2024	2:01 Pm	1, First, the web-based email used by suspect was performed by Hotmail platform. To know where the location of that file is containing that information to go to this location: /Img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Application Data/Identities/{8054E531-ABCC-4D69-A565-3978F75945DF}/Microsoft/Outlook Express/Bank Information.dbx Fig.38 We can see in the below image that suspects are using “Hotmail.msn.com” for sending and receiving emails.

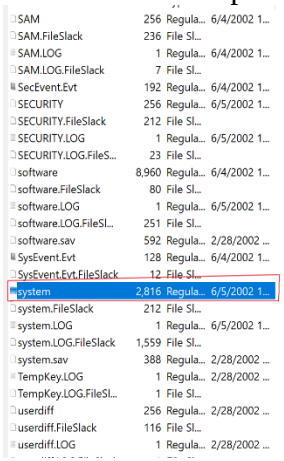
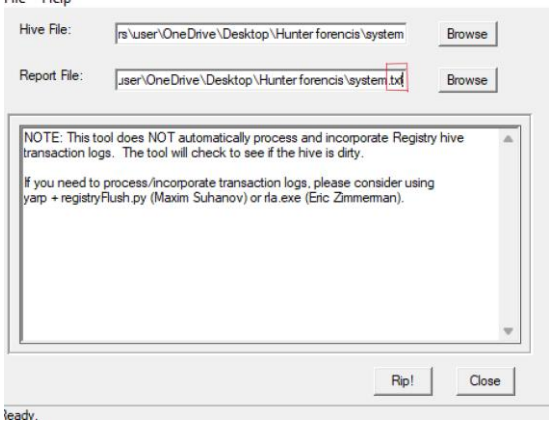
Action	Done?	Date	Time	Notes
				 LocalStore Billy ((MSGCOL_FLAGS & ARF_WATCH) != 0 || (MSGCOL_FLAGS & ARF_IGNORE) != 0) Web Site Web SiteBilly Raybillyray150@hotmail.com chaser1191@hotmail.com<chaser1191@hotmail.com>Hotmail00000001| Web Page on Christina Re: Web Page on ChristinaBilly Raybillyray150@hotmail.com chaser1191@hotmail.com<chaser1191@hotmail.com>Hotmail00000001 Web Pagep8 Web PageBilly Raybillyray150@hotmail.com chaser1191@hotmail.com<chaser1191@hotmail.com>Hotmail00000001@ Web Page on Christina Re: Web Page on ChristinaBilly Raybillyray150@hotmail.com chaser1191@hotmail.com<chaser1191@hotmail.com>Hotmail00000001 Delivery Status Notification (Failure)0QF Fwd: Delivery Status Notification (Failure)Billy Raybillyray150@hotmail.com chaser1191@hotmail.com<chaser1191@hotmail.com>Hotmail00000001 Web Page on Christina Re: Web Page on ChristinaBilly Raybillyray150@hotmail.com chaser1191@hotmail.com<chaser1191@hotmail.com>Hotmail00000001 Web Page on Christina Re: Web Page on ChristinaBilly Raybillyray150@hotmail.com chaser1191@hotmail.com<chaser1191@hotmail.com>Hotmail00000001 Received: from 65.201.58.12 by lw14fd.law14.hotmail.msn.com with HTTP; Wed, 22 May 2002 14:01:21 GMT X-Originating-IP: [65.201.58.12] From: "Billy Ray" <billyray150@hotmail.com> To: chaser1191@hotmail.com Subject: Web Site Date: Wed, 22 May 2002 07:01:21 -0700 Fig.39 2, Again, the suspects also used local email named “outlook express 6”. To go to the location where the file containing information is saved, just go through this location: /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/Deleted Items.dbx After arriving at this location, the suspects used “Microsoft outlook express team”. Furthermore, below is the image where suspect trying to setup or create the outlook express 6 email.

Action	Done?	Date	Time	Notes
				 Fig.40 Using this local mail one suspect had sent an image file to another, which can be clearly seen in below image.  Fig.41

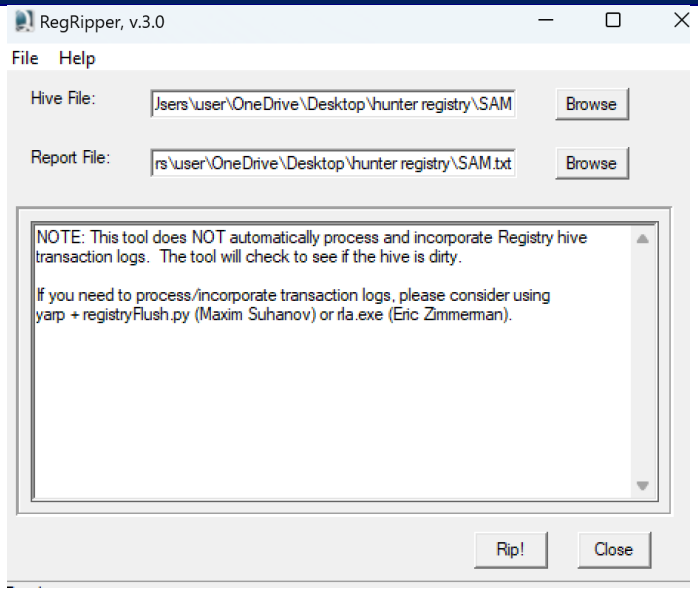
Action	Done?	Date	Time	Notes
				# Suspect's Operating Email to transfer information Below is the image where one suspect is providing the email of victims father email to another suspect.  Fig.42 After this we can see the suspects talking about the amount of money to ask to the father.

Action	Done?	Date	Time	Notes
				 PM#F:\Palm\HunterB\memopad\memopad.dat 0 6 0 0 1 OOOOOOX Business Business Personal Personal@ +AOL s/name: chaser1191@aol p/w: bigjake Billy I followed Kim and her friend. I think her friends name is Sabrina. We need to decide how to proceed. We need to be careful. We don't need the police involved .Hotmail chaser1191@hotmail.com p/w: bigjake -Yahoo information bob_hunter1191 p/w bigjake)AIM Information chaser1191 p/w bigjake bX Drive chaser1191@hotmail.com 1191 http://plus.xdrive.com/XDRequestDispatcher?action=OpenLogin Bill I am leaving soon so I thought I would jot this note down to send later. I will be flying to LA to confirm the work address and find and confirm the friends name. I want to be able t o send the information to the family soon. I agree that 500,000 is a good amount to start out with. I think the daughters safety is worth that don't you? I can't believe that they did not even know that it was us taking the photos. She even talked to me once. I will let you know as soon as I learn anything. Fig.43
Retrieve operating system information, accounts information, software, time zone information etc.).	Yes	25th November 2024	3:47 Pm	First, load the hunter xp image file to AccessData FTK Imager as we had done before. Then, search for the SAM, SECURITY, SOFTWARE, SYSTEM. LOCATION: Hunterxp/Partion 1/Noname/root/windows/system32/config 1, operating System information For details of the operating system, repeat the process of TimeZone analysis, but the difference is examine the SOFTWARE file not the SAM or SYSTEM file. Same as before after exporting the file from autopsy we put the SOFTWARE file in the Reg ripper 3.0 tool to get the text file for the required information.

Action	Done?	Date	Time	Notes
				 Fig.44 After searching the SOFTWARE file, there are details of the operating system.  Fig.45

Action	Done?	Date	Time	Notes
				After that for **TimeZone** Information Choose **SYSTEM** file and execute the same process.  Fig.46  Fig.47 After clicking the rip option, there is a txt file where we need to search for Time Zone. In the txt file simply search for keyword TimeZone with the key "CTRL+F".

Action	Done?	Date	Time	Notes
				File Edit View winlogon.exe - 0 NETSTRS.EXE - 0 nddeagnt.exe - 0 os2srv.exe - 0 wfshell.exe - 0 win.com - 0 rdpclip.exe - 0 conime.exe - 0 proquota.exe - 0 imepadsv.exe - 0 ctfmon.exe - 0 UserAuthentication value not found. WinStations\RDP-Tcp key PortNumber: 3389 Analysis Tip: By default, the port number is 3389, but can be changed. Policies\Microsoft\Windows NT\Terminal Services not found. ---------- timezone v.20200518 (System) Get TimeZoneInformation key contents TimeZoneInformation key ControlSet001\Control\TimeZoneInformation LastWrite Time 2002-04-18 14:33:31Z DaylightName -> Central Daylight Time StandardName -> Central Standard Time Bias -> 360 (6 hours) ActiveTimeBias -> 300 (5 hours) timezone Fig.48 As a result, “Central Daylight Time” found which is the local time of North America. The suspect executed the crime from North America. 2, Account details/User details For user details, copy all the process used for TimeZone analysis, but the difference is for this task investigate the SAM not the SYSTEM.

Action	Done?	Date	Time	Notes
				 Fig.49 Same as before, browse the SAM file and insert it in the Forensics Tool after then text file of SAM is generated where we get the information about the accounts. After searching for the user details, some default information and the suspects information (BOB HUNTER) were clearly seen. Below are the images of Default and the suspect's account information. The first three are default user and the Bob hunter is the suspect.

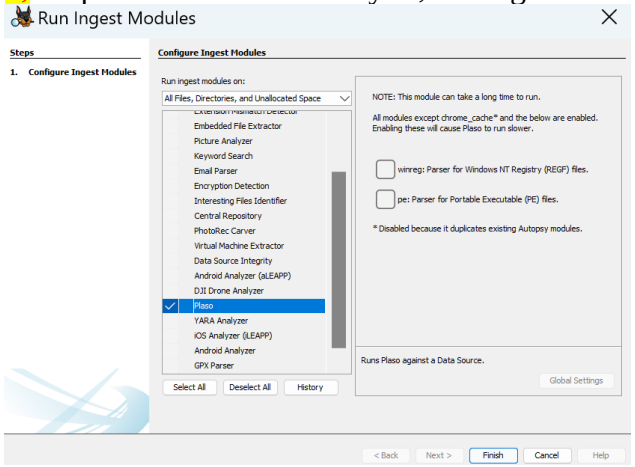
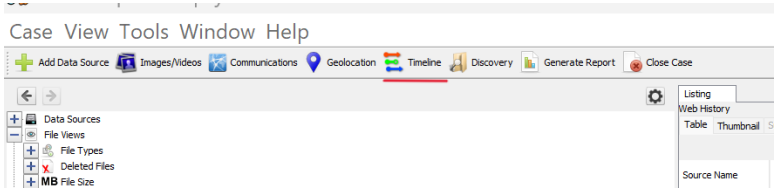
Action	Done?	Date	Time	Notes

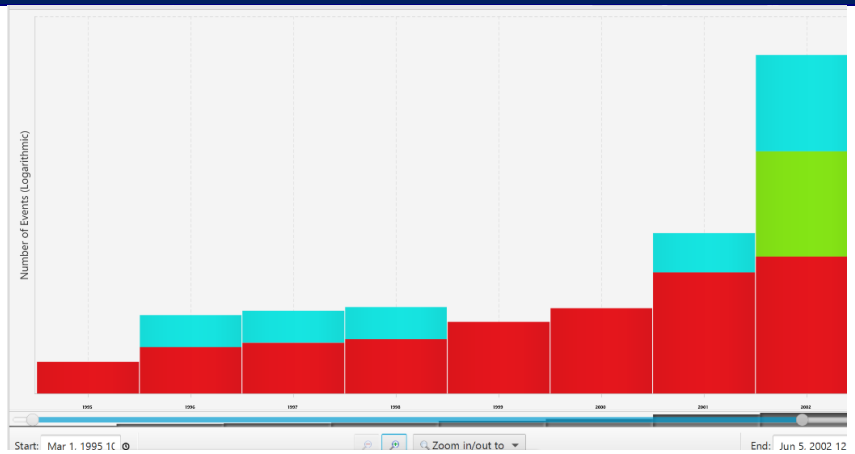
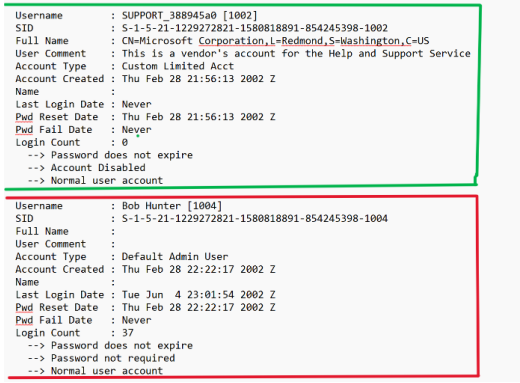
```
Hive (C:\Users\user\OneDrive\Desktop\hunter assignment\SAM) is not dirty.

samparse v.20220921
(SAM) Parse SAM file for user & group mbrshp info

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
```

Fig.50

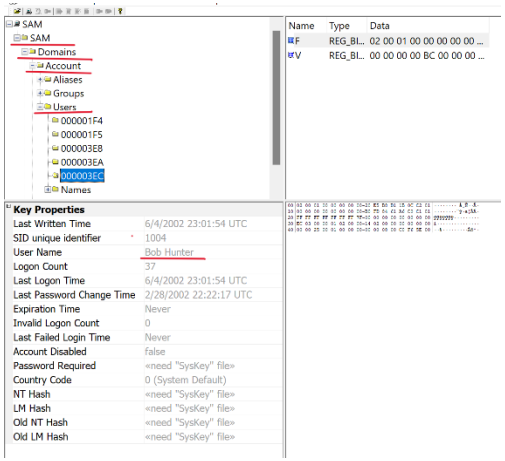
```
Username        : SUPPORT_388945a0 [1002]
SID             : S-1-5-21-1229272821-1580818891-854245398-1002
Full Name       : CN=Microsoft Corporation,L=Redmond,S=Washington,C=US
User Comment    : This is a vendor's account for the Help and Support Service
Account Type    : Custom Limited Acct
Account Created : Thu Feb 28 21:56:13 2002 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Thu Feb 28 21:56:13 2002 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Account Disabled
  --> Normal user account

Username        : Bob Hunter [1004]
SID             : S-1-5-21-1229272821-1580818891-854245398-1004
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Thu Feb 28 22:22:17 2002 Z
Name            :
Last Login Date : Tue Jun  4 23:01:54 2002 Z
Pwd Reset Date  : Thu Feb 28 22:22:17 2002 Z
Pwd Fail Date   : Never
Login Count     : 37
  --> Password does not expire
  --> Password not required
  --> Normal user account
```

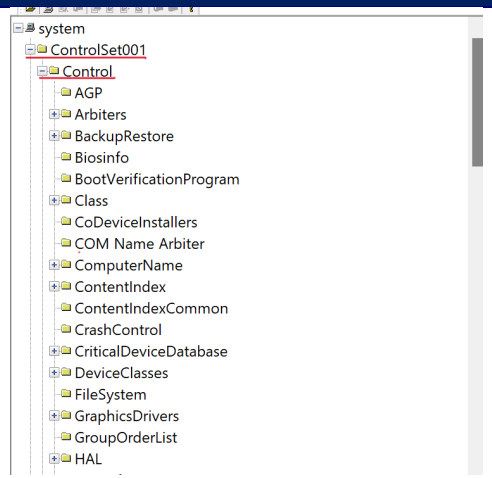
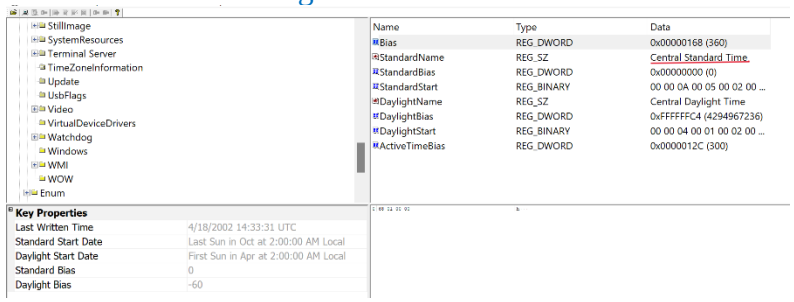
Fig.51

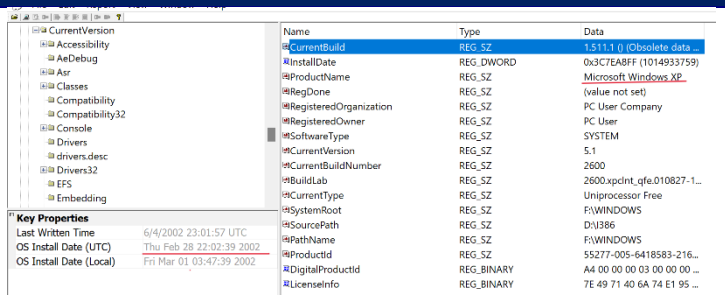
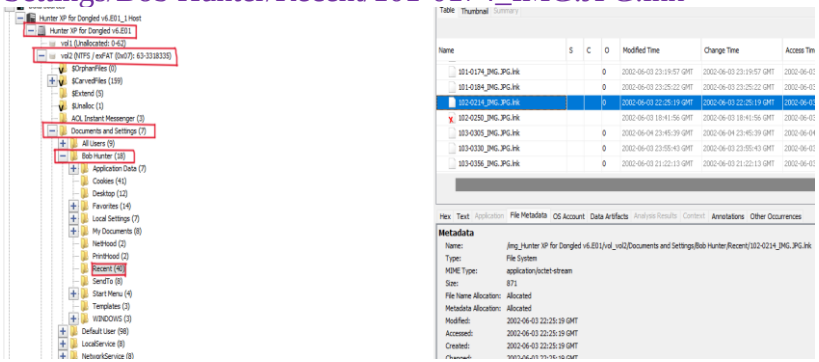
Action	Done?	Date	Time	Notes
Timeline analysis- Note date of last activity on the computer. System profiling.	Yes	26th November 2024	1:19 Pm	1, To perform Timeline analysis, run ingest module and select plaso.  Fig.52 After that timeline section can be seen at the top containing the date and time information.  Fig.53 Finally, after analysing the timeline, we can say that the date of last activity on the computer was Jun 5, 2002, 12:50:12 AM.

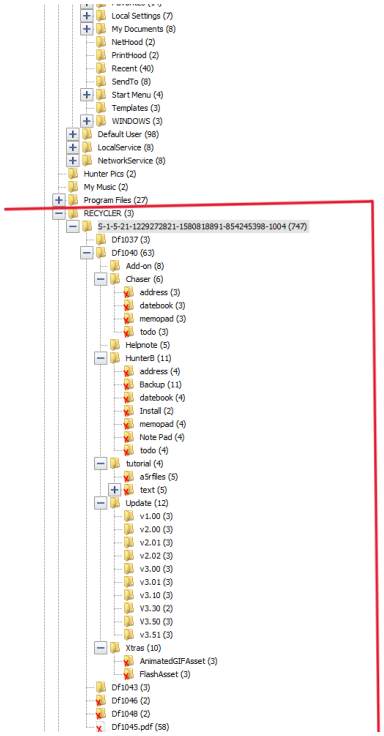
Action	Done?	Date	Time	Notes
				 Fig.54 2, Now, for **System profiling** user details, TimeZone and operating system details play vital role. As, already done this before I will just put the outputs: **1. User Details** We can see below the information about the suspect "bob hunter".  Fig.55

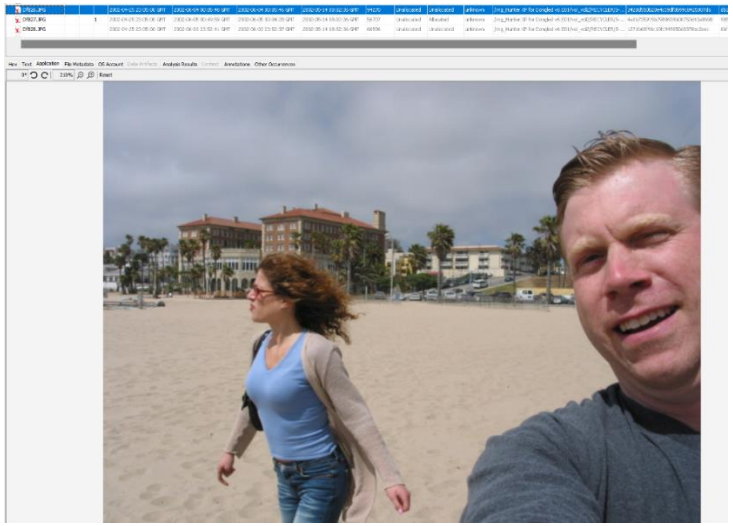
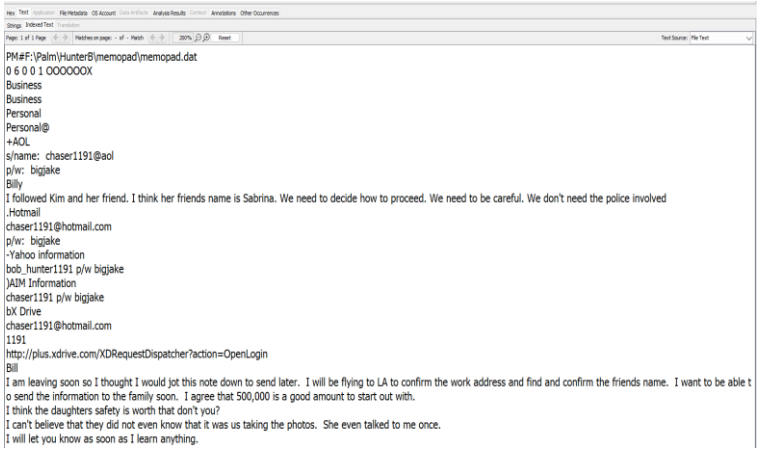
Action	Done?	Date	Time	Notes
				2. TimeZone File Edit View winlogon.exe - 0 NETSTRS.EXE - 0 nddeagnt.exe - 0 os2srv.exe - 0 wfshell.exe - 0 win.com - 0 rdpclip.exe - 0 conime.exe - 0 proquota.exe - 0 imepadsv.exe - 0 ctfmon.exe - 0 timezone UserAuthentication value not found. WinStations\RDP-Tcp key PortNumber: 3389 Analysis Tip: By default, the port number is 3389, but can be changed. Policies\Microsoft\Windows NT\Terminal Services not found. ---------- timezone v.20200518 (System) Get TimeZoneInformation key contents TimeZoneInformation key ControlSet001\Control\TimeZoneInformation LastWrite Time 2002-04-18 14:33:31Z DaylightName -> Central Daylight Time StandardName -> Central Standard Time Bias -> 360 (6 hours) ActiveTimeBias -> 300 (5 hours) Fig.56 **3. Operating system information** winver v.20200525 (Software) Get Windows version & build info ProductName Microsoft Windows XP BuildLab 2600.xpclnt_qfe.010827-1803 RegisteredOrganization PC User Company RegisteredOwner PC User InstallDate 2002-02-28 22:02:39Z ---------- wow64 v.20200515 (Software) Gets contents of WOW64\x86 key 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 Fig.57

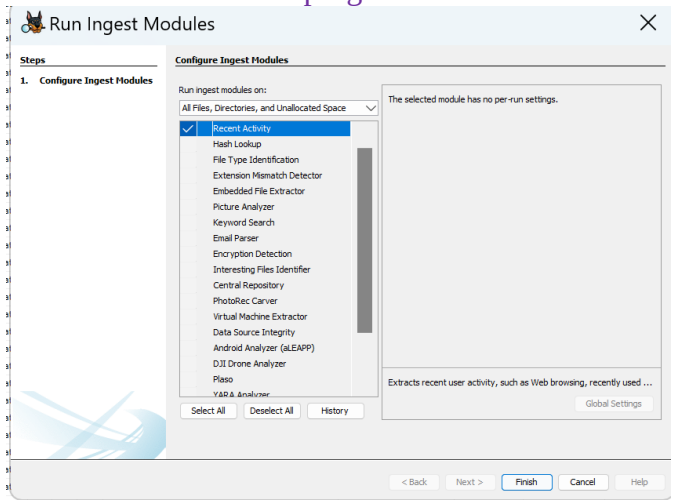
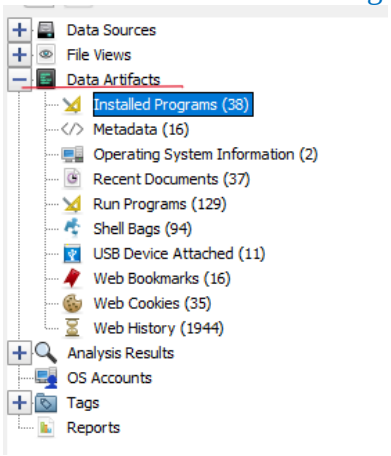
Action	Done?	Date	Time	Notes
Registry analysis and Registry protected area	Yes	26th November 2024	2:10 Pm	To analyse the registry of HunterXP image use registry viewer to see User Details, TimeZone Analysis & Operating System Details. 1. User Details (SAM FILE) First, export the file from autopsy of SAM, SYSTEM, SOFTWARE, SECURITY. Then, load the SAM file in the registry viewer and navigate through the location: Sam/domain/accounts/user  Fig.58 2. TimeZone (SYSTEM FILE): To know the TimeZone of The HunterXP file load the system file in registry viewer and navigate through location: System/controlset001/control/

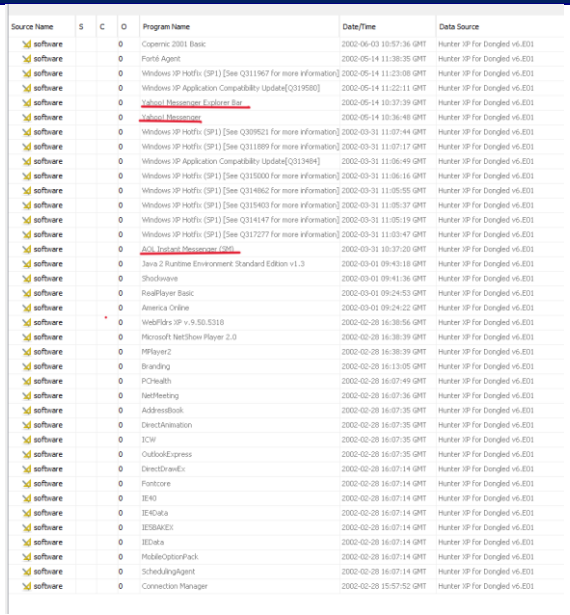
Action	Done?	Date	Time	Notes
				 Fig.59  Fig.60 3. Operating System Information Using **Registry Viewer 1.0.8.5** To get the information first load the Software file exported, then navigate through the location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

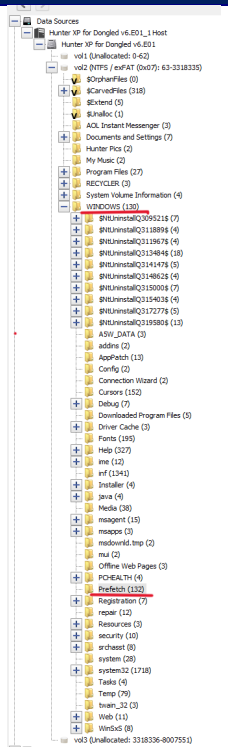
Action	Done?	Date	Time	Notes
				 Fig.61
Link files and Recycle Bin	Yes	26th November 2024	3:08 Pm	1, link files To view the details of link files to go to this location: /Img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Recent/101-0174_IMG.JPG.lnk  Fig.62 Here are all the details of the linked files. .lnk files are used to make shortcuts to a specific location like folder, program. 2, Recycle bin To view all the information of recycle bin to go to this location:

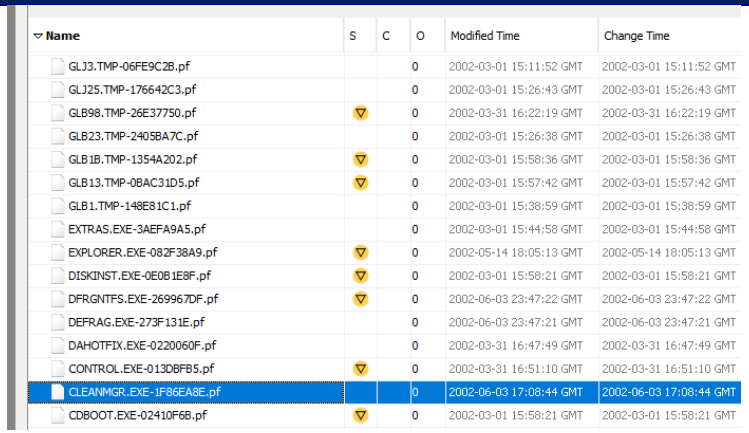
Action	Done?	Date	Time	Notes
				img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1037  Fig.63 In this folder the suspect has deleted a lot of information shown in the screen shot below. 1, The images about the suspects and victims.

Action	Done?	Date	Time	Notes
				 Fig.64 2, The information about the suspect's friend and ransomware.  PM#F:\Palm\HunterB\memopad\memopad.dat 0 6 0 0 1 OOOOOOX Business Business Personal Personal@ +AOL s/name: chaser1191@aol p/w: bigjake Billy I followed Kim and her friend. I think her friends name is Sabrina. We need to decide how to proceed. We need to be careful. We don't need the police involved .Hotmail chaser1191@hotmail.com p/w: bigjake -Yahoo information bob_hunter1191 p/w bigjake)AIM Information chaser1191 p/w bigjake bX Drive chaser1191@hotmail.com 1191 http://plus.xdrive.com/XDRequestDispatcher?action=OpenLogin Bill I am leaving soon so I thought I would jot this note down to send later. I will be flying to LA to confirm the work address and find and confirm the friends name. I want to be able t o send the information to the family soon. I agree that 500,000 is a good amount to start out with. I think the daughters safety is worth that don't you? I can't believe that they did not even know that it was us taking the photos. She even talked to me once. I will let you know as soon as I learn anything. Fig.65

Action	Done?	Date	Time	Notes
Instant Messaging clients	Yes	27th November 2024	12:08 Pm	To know the details of instant messaging clients, First, run ingest module “recent activity” Then navigate through: Data artifacts/installed programs/  Fig.66  Fig.67

Action	Done?	Date	Time	Notes
				 Fig.68 Here, these are the 2 messaging clients: 1. Yahoo messenger 2. AOL Instant Messenger (SM)
Clean-up/Wiping utilities. Check log files. Anything used?	Yes	28th November 2024	2:06 Pm	To see the information regarding the wiping software used navigate through: Prefetch is the location where all the installed application or programs are stored. Hunterxp/windows/prefetch

Action	Done?	Date	Time	Notes
				 Fig.69 After navigating through this location, we can see a software for cleaning data called “cleanmgr.exe”

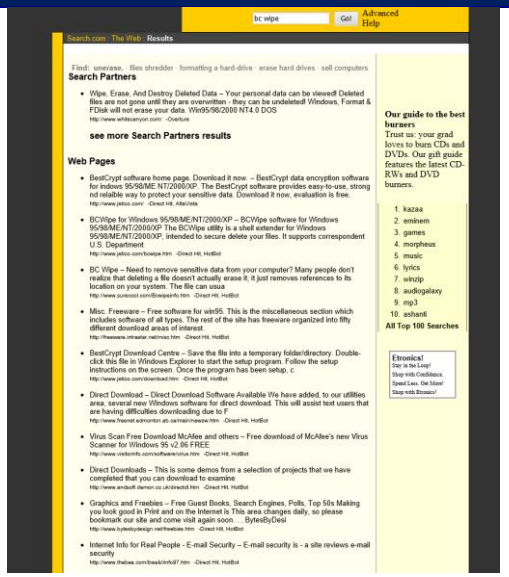
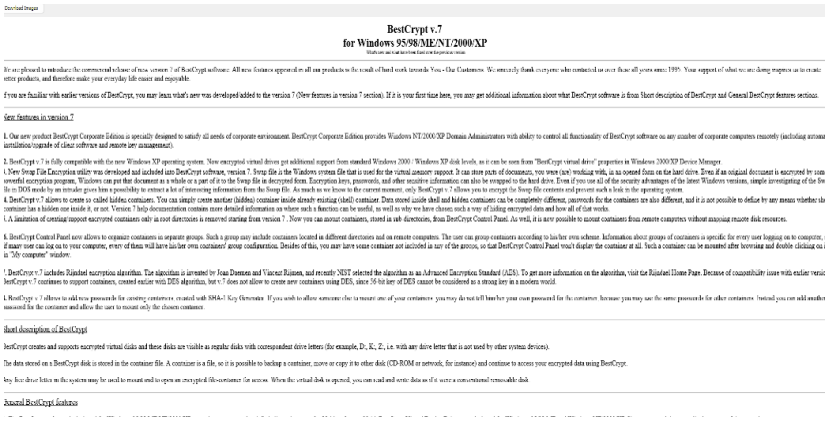
Action	Done?	Date	Time	Notes
				 Fig.70

Name	S	C	O	Modified Time	Change Time
GLJ3.TMP-06FE9C2B.pf			0	2002-03-01 15:11:52 GMT	2002-03-01 15:11:52 GMT
GLJ25.TMP-176642C3.pf			0	2002-03-01 15:26:43 GMT	2002-03-01 15:26:43 GMT
GLB98.TMP-26E37750.pf			0	2002-03-31 16:22:19 GMT	2002-03-31 16:22:19 GMT
GLB23.TMP-2405BA7C.pf			0	2002-03-01 15:26:38 GMT	2002-03-01 15:26:38 GMT
GLB1B.TMP-1354A202.pf			0	2002-03-01 15:58:36 GMT	2002-03-01 15:58:36 GMT
GLB13.TMP-0BAC31D5.pf			0	2002-03-01 15:57:42 GMT	2002-03-01 15:57:42 GMT
GLB1.TMP-148E81C1.pf			0	2002-03-01 15:38:59 GMT	2002-03-01 15:38:59 GMT
EXTRAS.EXE-3AEFA9A5.pf			0	2002-03-01 15:44:58 GMT	2002-03-01 15:44:58 GMT
EXPLORER.EXE-082F38A9.pf			0	2002-05-14 18:05:13 GMT	2002-05-14 18:05:13 GMT
DISKINST.EXE-0E0B1E8F.pf			0	2002-03-01 15:58:21 GMT	2002-03-01 15:58:21 GMT
DFRGNTFS.EXE-269967DF.pf			0	2002-06-03 23:47:22 GMT	2002-06-03 23:47:22 GMT
DEFRAG.EXE-273F131E.pf			0	2002-06-03 23:47:21 GMT	2002-06-03 23:47:21 GMT
DAHOTFIX.EXE-0220060F.pf			0	2002-03-31 16:47:49 GMT	2002-03-31 16:47:49 GMT
CONTROL.EXE-013DBFB5.pf			0	2002-03-31 16:51:10 GMT	2002-03-31 16:51:10 GMT
CLEANMGR.EXE-1F86EA8E.pf			0	2002-06-03 17:08:44 GMT	2002-06-03 17:08:44 GMT
CDBOOT.EXE-02410F6B.pf			0	2002-03-01 15:58:21 GMT	2002-03-01 15:58:21 GMT

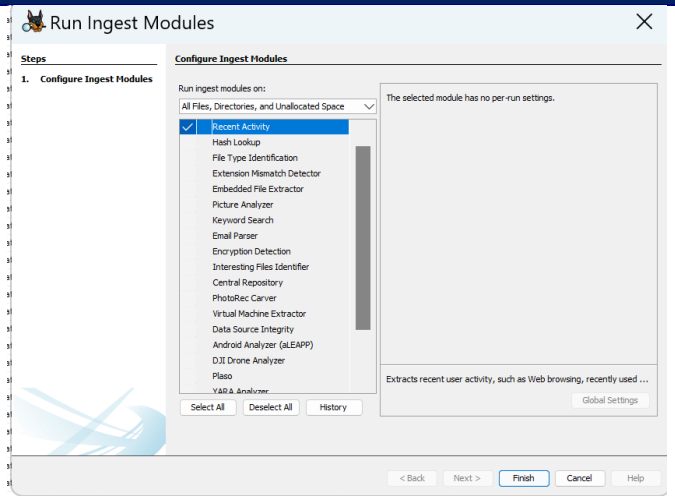
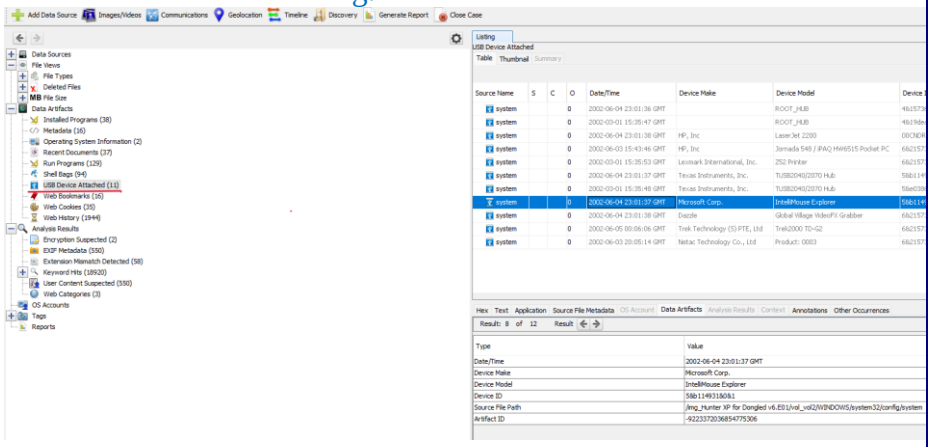
There are also details researched about Clean-up/wiping utilities for this navigate through location:

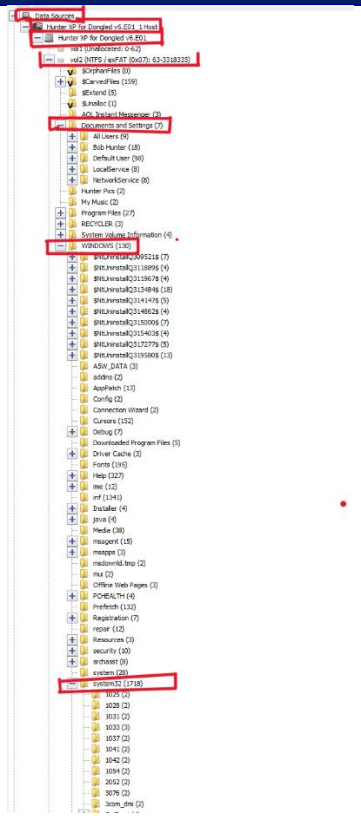
1. Here he researched about BCWIPE tool:

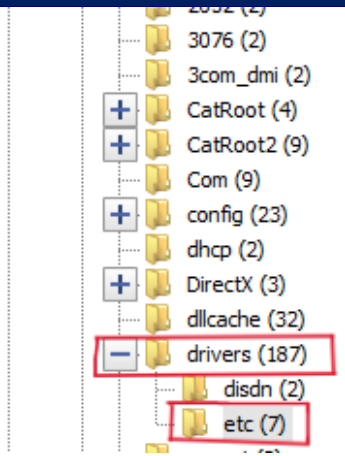
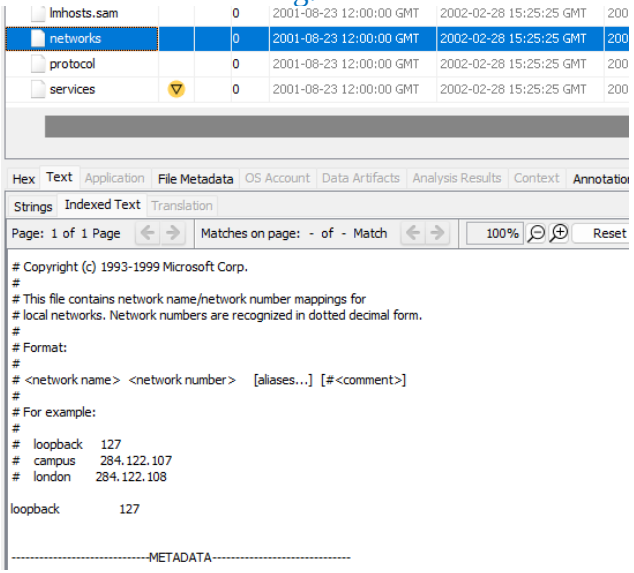
/Img_Hunter XP for Dongled v6.E01/vol_vol2/Document and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/8XGPQD6L/search [3]/search [3]/

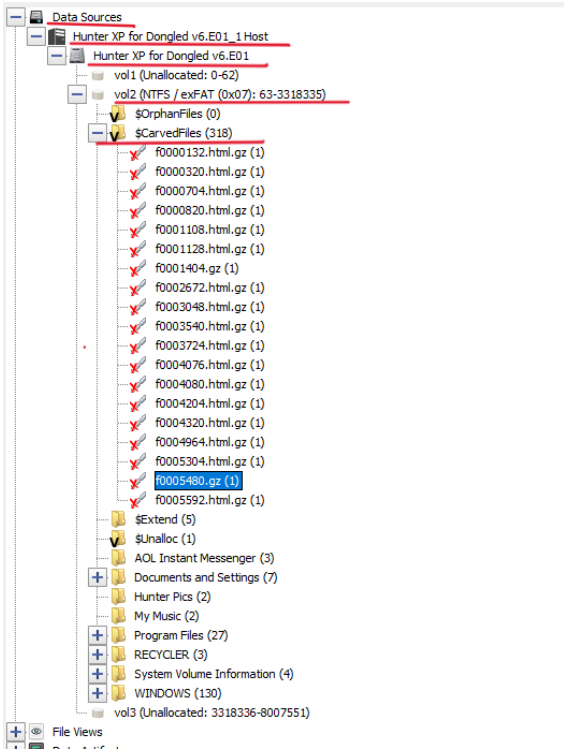
Action	Done?	Date	Time	Notes
				 Fig.71 2. After that we can see the information about BESTCRYPT v7:  Fig.72 We can see he is trying to download the BCWIPE tool:

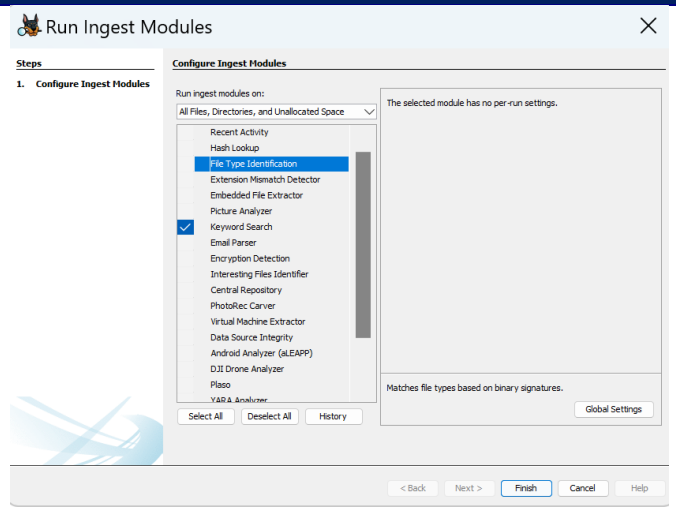
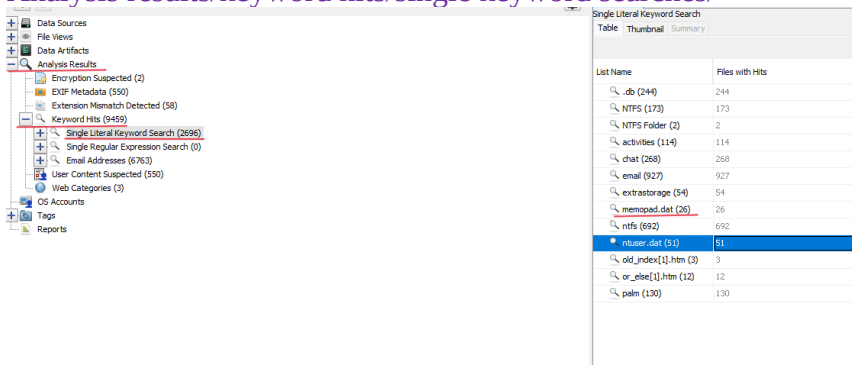
Action	Done?	Date	Time	Notes
				l free space on the specified disk as well as file slacks. Click here to read more and download BCWipe utility **8.** The main commands to control access to encrypted data may be run from Windows Explorer ("My Computer" window) without starting BestCrypt Control Panel. To do it you should use the sar **9.** BestCrypt has been designed as the product with an open architecture: any third-party encryption software and hardware developers are able to insert their own security extensions into the BestC algorithms. To get additional information about the architecture, see the BestCrypt Development Kit for Windows 95/98/ME/NT/2000/XP WWW-page. **10.** The BestCrypt Development Kit (available for downloading from Jetico, Inc. Web site) contains source codes of all BestCrypt modules responsible for security of the software. **11.** BestCrypt automatically saves information about sharing its drives in network. Now user does not need to share the BestCrypt drives every time he/she reboots operating system. **What's new and what have been fixed over the previous version** **1.** New 7.00.b beta version of BestCrypt is announced. (07-September-2001 release, BestCrypt Control Panel v.7.00.b, versions of drivers: v.3.12 for Windows 2000/XP, v.2.41 for Windows 95, v. **2.** Problem with IRQL_NOT_LESS_OR_EQUAL or FILE_SYSTEM error occured when Windows 2000/XP reboots is solved. As well problem of mounting network containers is solved. (02-Oct Windows NT) **3.** Few enhancements were made in low-level BestCrypt driver for Windows XP (28-October-2001 release, BestCrypt Control Panel v.7.03.b, versions of drivers: v.3.15 for Windows 2000/XP, v.2 **4.** Serious problem of reading NTFS formatted containers is fixed in low-level BestCrypt driver for Windows XP (12-November-2001 release, BestCrypt Control Panel v.7.03.b, versions of drivers **5.** Swap File Encryption utility now supports all encryption algorithms available in BestCrypt (Rijndael, Blowfish, Twofish, GOST). Option to remove additional passwords is implemented. (14-N for Windows NT) **6.** Commercial release. (20-November-2001 release, BestCrypt Control Panel v.7.05, versions of drivers: v.3.18 for Windows 2000/XP, v.2.41 for Windows 95, v.2.18 for Windows NT) **7.** In Windows 2000/NT/XP BestCrypt now supports creating and formatting containers by users with ordinary privileges (i.e. not by Administrators only). As well, during "Log off" process BestC of drivers: v.3.21 for Windows 2000/XP, v.2.41 for Windows 95/98/ME, v.2.18 for Windows NT) **8.** In Windows 2000/XP BestCrypt now dismounts virtual drives during restart/shutdown process to perform additional work on flushing cache to NTFS formatted virtual drives. (17-January-2002 Windows NT) **9.** In Windows 2000/XP version of BestCrypt problem of mounting several FAT32 formatted containers is solved. In the Windows 95/98/ME version we could catch and solve occasionally arised Windows 2000/XP, v.2.41 for Windows 95/98/ME, v.2.18 for Windows NT) **10.** In Windows 2000/XP version of BestCrypt problem of saving correct security identificators on NTFS-formatted containers is solved. (13-March-2002 release, BestCrypt Control Panel v.7.07, **11.** Windows 2000/XP now properly reports user if he/she mounts FAT/FAT32 formatted containers in read-only mode. As well we have inserted new recommendation to the "Hidden containers: filesystem if you are going to create hidden part inside it (see more detail in the BestCrypt help file). (06-April-2002 release, BestCrypt Control Panel v.7.07.2, versions of drivers: v.3.27 for Windo If you want to evaluate BestCrypt v.7 for Windows 95/98/ME/NT/2000/XP, visit the Download Centre WWW-page to download the software. **Upgrade policy to version 7.** All registered customers of any of previous versions 4.x, 5.x or 6.x of BestCrypt software are eligible for a special price to upgrade to version 7. To make an order for upgrade, visit Order page. If you have any questions on upgrade procedure, feel free to contact our Sales Department at sales@jetico.com Fig.73
External drives; Network connections	Yes	28th November 2024	11:47 Am	To know the details of External drives, navigate through: Tools/runingestmodule/HunterXP/filetype identification Data artifacts/USB Device attached/

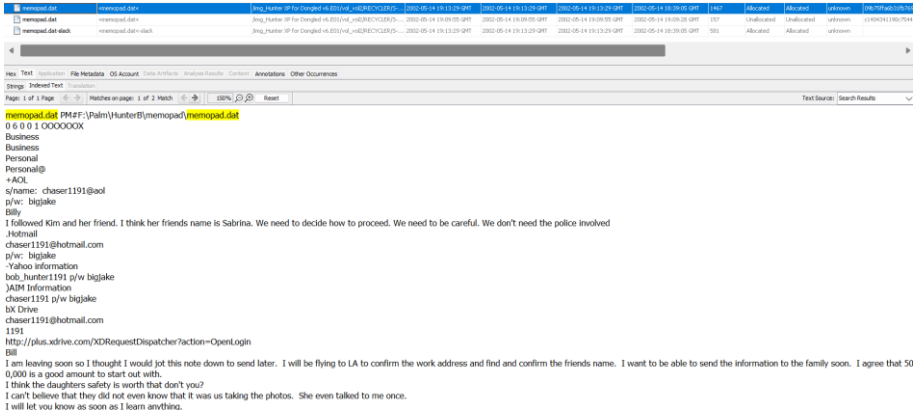
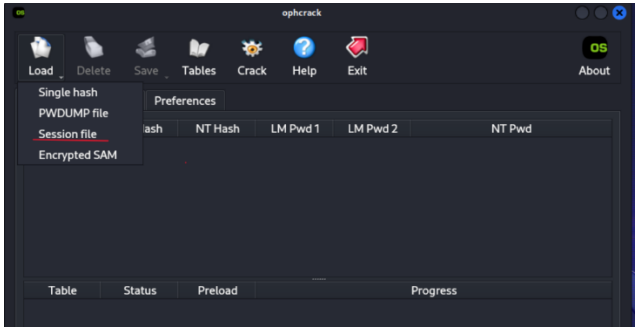
Action	Done?	Date	Time	Notes
				 Fig.74  Fig.75 Here are many details related to external devices attached or USB device attached. 2, To know about the network connections, go to this location: Hunterxp/vol2/windows/system32/drivers/etc/network

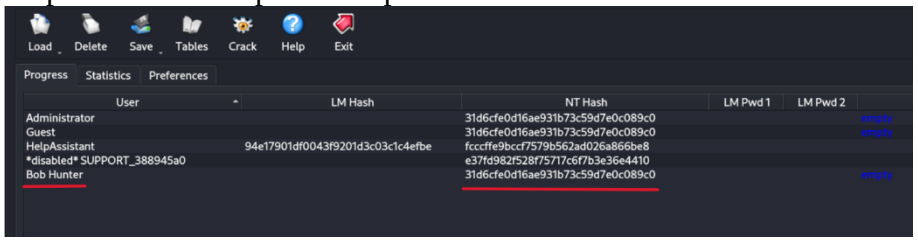
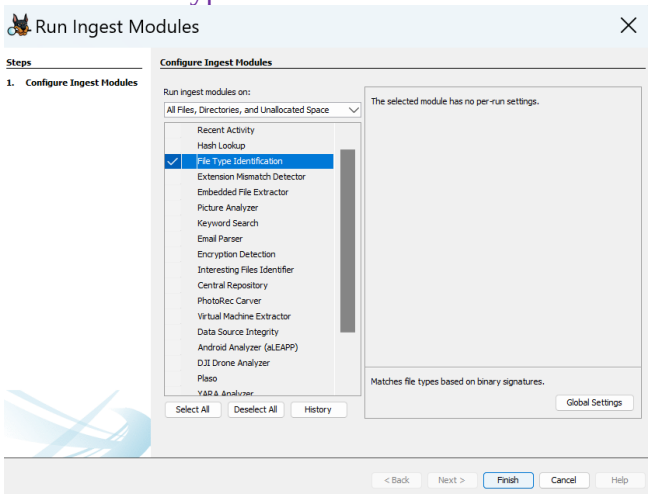
Action	Done?	Date	Time	Notes
				 Fig.76

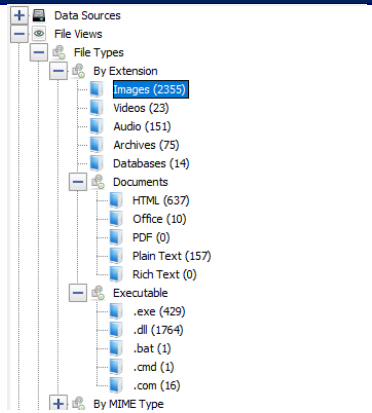
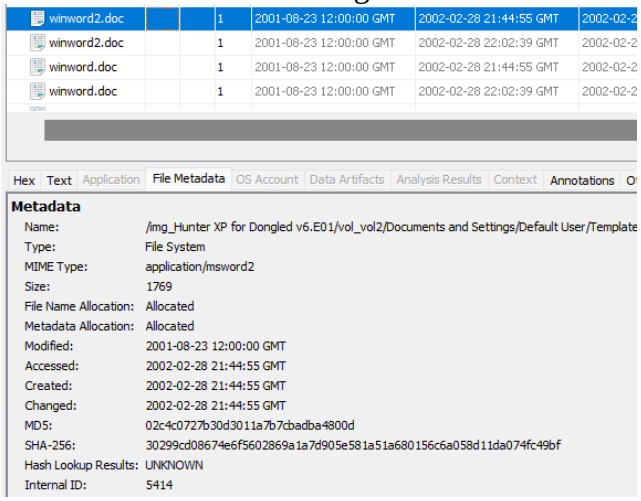
Action	Done?	Date	Time	Notes
				 Fig.77  Fig.78 In this location we can see all the Ip address connected to the pc.

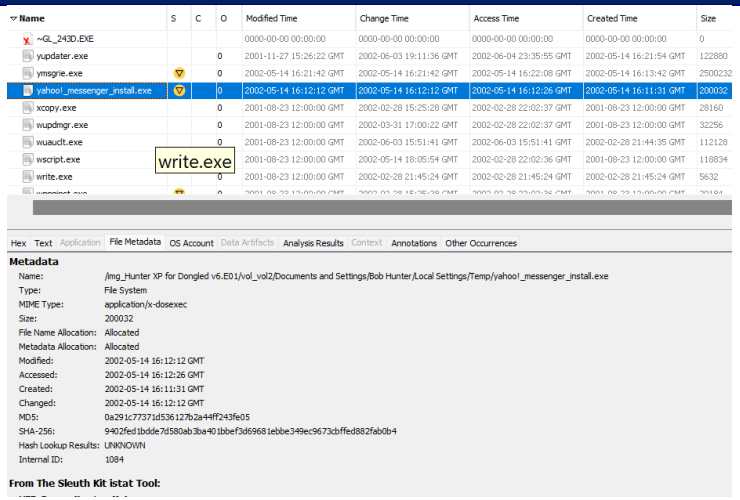
Action	Done?	Date	Time	Notes
Perform data carving				To see the files whose data are carved navigate through: Data source/vol2/carved files  Fig.79 These are the files that are recovered from allocated space or fragment of data.
Run relevant keyword searches. Did you index the evidence file?	Yes	28th November 2024	12:45 Pm	I have searched many activities using keyword to see the exact location where the keywords are: First run the ingest module and select keyword Search.

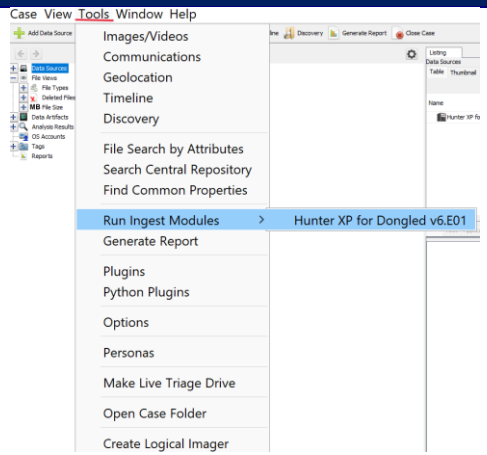
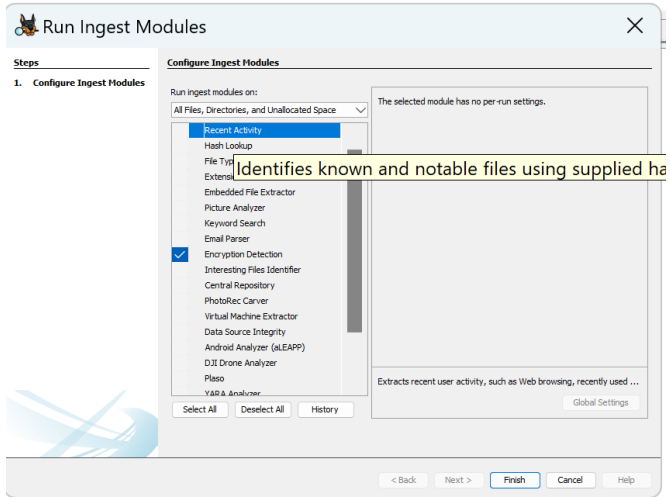
Action	Done?	Date	Time	Notes
				 Fig.80 Then navigate through, Analysis results/keyword hits/single keyword searches/  Fig.81 Through the searches the main keyword is “memopad.dat” in this evidence file there are many details of two suspect talking about the victims.

Action	Done?	Date	Time	Notes
				 memopad.dat PM#F:\Palm\HunterB\memopad\memopad.dat 0 6 0 0 1 OOOOOOX Business Business Personal Personal@ +AOL s/name: chaser1191@aol p/w: bigjake Billy I followed Kim and her friend. I think her friends name is Sabrina. We need to decide how to proceed. We need to be careful. We don't need the police involved .Hotmail chaser1191@hotmail.com p/w: bigjake -Yahoo information bob_hunter1191 p/w bigjake)AIM Information chaser1191 p/w bigjake bX Drive chaser1191@hotmail.com 1191 http://plus.xdrive.com/XDRequestDispatcher?action=OpenLogin Bill I am leaving soon so I thought I would jot this note down to send later. I will be flying to LA to confirm the work address and find and confirm the friends name. I want to be able to send the information to the family soon. I agree that 50 0,000 is a good amount to start out with. I think the daughters safety is worth that don't you? I can't believe that they did not even know that it was us taking the photos. She even talked to me once. I will let you know as soon as I learn anything. Fig.82
Recover Log-on passwords – use SAMInside/Ophcrack/Encase				To know about the password of the user first export the config file from: Hunterxp/windows/system32/config Then run the Linux in Virtual machine and open the software **Ophcrack**. After that just load the config file using the option session file as shown below:  Fig.83

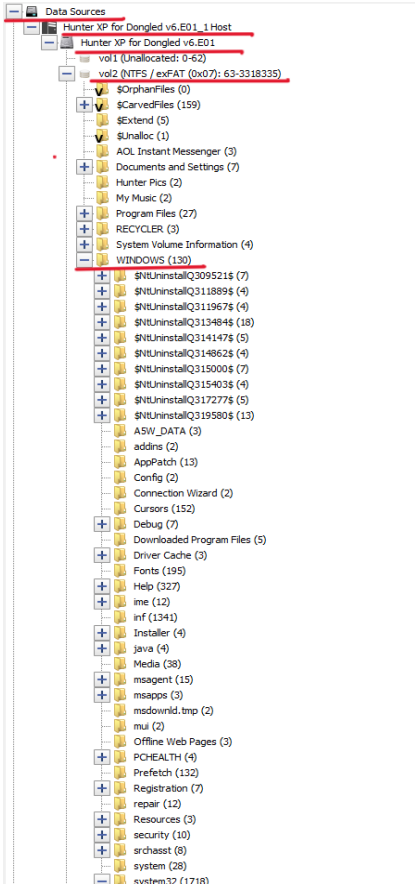
Action	Done?	Date	Time	Notes
				After loading the file, it shows some hash values which gives the output that it is not password protected.  Fig.84
Examine different file types: Export doc/office and exe files; look at Metadata if required	Yes	29th November 2024	3:04 Pm	To see and examine the details of file types first run the ingest module and then select file type identification after then all the information are generated as shown in the image below: Fileviews/filetypes  Fig.85 Here are different types of files:

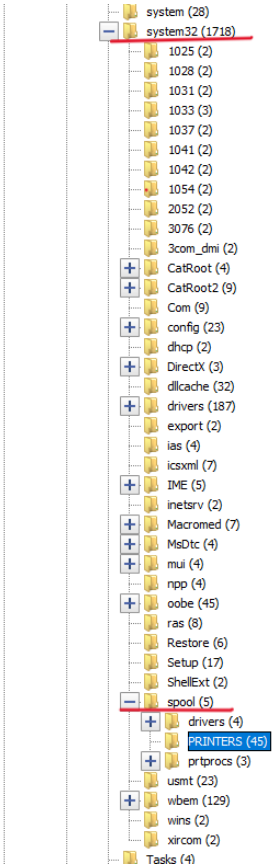
Action	Done?	Date	Time	Notes
				 Fig.86 Details of Doc files: . Doc are the files containing word documents.  Fig.87 Details of Exe files: . Exe are those files which contains program or applications.

Action	Done?	Date	Time	Notes
				 Fig.88
Encryption, Steganalysis (any indications? Entropy or Autopsy can be used)	Yes	29th November 2024	4:02 Pm	To find the encryption detected file first run the ingest module and select “encryption detection” Tools/runingestmodule/HunterXP/encryption detection/ Then navigate through this location: Analysis/encryptions suspected/

Action	Done?	Date	Time	Notes
				 Fig.89  Fig.90 After this the details of encryption with justification (entropy) are seen.

Action	Done?	Date	Time	Notes
				Encryption Suspected Table Thumbnail Summary Source Name | S | C | O | Source Type | Score | Conclusion | Configuration | Justification | Comment oembios.bin | | | 0 | File | Likely Notable | | | Suspected encryption due to high entropy (7.999988). | Suspected encryption due to high entropy (7.999988). Fig.91 Here is the file with high entropy (7.999998) which is almost highest (8).
Print artefacts	Yes	29th November 2024	4:45 Pm	To see the details of print artifacts go to this location: /Img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/spool/PRINTERS/

Action	Done?	Date	Time	Notes
				 Fig.92

Action	Done?	Date	Time	Notes
				 Fig.93 Here we can see all the details related to printers.

Action	Done?	Date	Time	Notes

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2002-06-05 00:41:03 GMT	2002-06-05 00:41:03 GMT	2002-06-05 00:41:03 GMT	2002-02-28 21:42:15 GMT	168
[parent folder]				2002-02-28 21:42:15 GMT	2002-02-28 21:42:15 GMT	2002-06-04 23:01:27 GMT	2002-02-28 15:13:50 GMT	352
00002.SHD			0	2002-06-04 23:32:58 GMT	2002-06-04 23:32:58 GMT	2002-06-04 23:32:58 GMT	2002-06-04 23:32:38 GMT	1332
00002.SPL			0	2002-06-04 23:32:57 GMT	2002-06-04 23:32:57 GMT	2002-06-04 23:32:29 GMT	2002-06-04 23:32:29 GMT	10485760
00003.SHD			0	2002-06-04 23:33:27 GMT	2002-06-04 23:33:27 GMT	2002-06-04 23:33:27 GMT	2002-06-04 23:33:27 GMT	1332
00003.SPL			0	2002-06-04 23:33:27 GMT	2002-06-04 23:33:27 GMT	2002-06-04 23:33:25 GMT	2002-06-04 23:33:25 GMT	723836
00004.SHD			0	2002-06-04 23:34:10 GMT	2002-06-04 23:34:10 GMT	2002-06-04 23:34:10 GMT	2002-06-04 23:34:10 GMT	1332
00004.SPL			0	2002-06-04 23:34:10 GMT	2002-06-04 23:34:10 GMT	2002-06-04 23:33:57 GMT	2002-06-04 23:33:57 GMT	3977148
00005.SHD			0	2002-06-04 23:35:29 GMT	2002-06-04 23:35:29 GMT	2002-06-04 23:35:29 GMT	2002-06-04 23:35:29 GMT	1352
00005.SPL			0	2002-06-04 23:35:29 GMT	2002-06-04 23:35:29 GMT	2002-06-04 23:35:27 GMT	2002-06-04 23:35:27 GMT	8648504
00006.SHD			0	2002-06-04 23:41:49 GMT	2002-06-04 23:41:49 GMT	2002-06-04 23:41:49 GMT	2002-06-04 23:41:49 GMT	1432
00006.SPL			0	2002-06-04 23:41:49 GMT	2002-06-04 23:41:49 GMT	2002-06-04 23:41:49 GMT	2002-06-04 23:41:49 GMT	331308
00007.SHD			0	2002-06-04 23:42:02 GMT	2002-06-04 23:42:02 GMT	2002-06-04 23:42:02 GMT	2002-06-04 23:42:02 GMT	1432
00007.SPL			0	2002-06-04 23:42:02 GMT	2002-06-04 23:42:02 GMT	2002-06-04 23:42:02 GMT	2002-06-04 23:42:02 GMT	92868
00008.SHD			0	2002-06-04 23:42:11 GMT	2002-06-04 23:42:11 GMT	2002-06-04 23:42:11 GMT	2002-06-04 23:42:11 GMT	1432
00008.SPL			0	2002-06-04 23:42:11 GMT	2002-06-04 23:42:11 GMT	2002-06-04 23:42:10 GMT	2002-06-04 23:42:10 GMT	92868
00009.SHD			0	2002-06-04 23:42:49 GMT	2002-06-04 23:42:49 GMT	2002-06-04 23:42:49 GMT	2002-06-04 23:42:49 GMT	1432
00009.SPL			0	2002-06-04 23:42:49 GMT	2002-06-04 23:42:49 GMT	2002-06-04 23:42:49 GMT	2002-06-04 23:42:49 GMT	80792
00010.SHD			0	2002-06-04 23:43:07 GMT	2002-06-04 23:43:07 GMT	2002-06-04 23:43:07 GMT	2002-06-04 23:43:07 GMT	1432
00010.SPL			0	2002-06-04 23:43:07 GMT	2002-06-04 23:43:07 GMT	2002-06-04 23:43:07 GMT	2002-06-04 23:43:07 GMT	302300
00011.SHD			0	2002-06-04 23:58:50 GMT	2002-06-04 23:58:50 GMT	2002-06-04 23:58:50 GMT	2002-06-04 23:58:50 GMT	1368
00011.SPL			0	2002-06-04 23:58:50 GMT	2002-06-04 23:58:50 GMT	2002-06-04 23:58:50 GMT	2002-06-04 23:58:50 GMT	1848
00013.SHD			0	2002-06-05 00:02:52 GMT	2002-06-05 00:02:52 GMT	2002-06-05 00:02:52 GMT	2002-06-05 00:02:52 GMT	1364
00013.SPL			0	2002-06-05 00:02:52 GMT	2002-06-05 00:02:52 GMT	2002-06-05 00:02:43 GMT	2002-06-05 00:02:43 GMT	32291584
00014.SHD			0	2002-06-05 00:04:37 GMT	2002-06-05 00:04:37 GMT	2002-06-05 00:04:37 GMT	2002-06-05 00:04:37 GMT	1368
00014.SPL			0	2002-06-05 00:04:37 GMT	2002-06-05 00:04:37 GMT	2002-06-05 00:04:13 GMT	2002-06-05 00:04:13 GMT	72684
00015.SHD			0	2002-06-05 00:10:56 GMT	2002-06-05 00:10:56 GMT	2002-06-05 00:10:56 GMT	2002-06-05 00:10:56 GMT	1376
00015.SPL			0	2002-06-05 00:10:56 GMT	2002-06-05 00:10:56 GMT	2002-06-05 00:10:56 GMT	2002-06-05 00:10:56 GMT	398772
00016.SHD			0	2002-06-05 00:10:57 GMT	2002-06-05 00:10:57 GMT	2002-06-05 00:10:57 GMT	2002-06-05 00:10:57 GMT	1376
00016.SPL			0	2002-06-05 00:10:57 GMT	2002-06-05 00:10:57 GMT	2002-06-05 00:10:57 GMT	2002-06-05 00:10:57 GMT	365560
00017.SHD			0	2002-06-05 00:10:57 GMT	2002-06-05 00:10:57 GMT	2002-06-05 00:10:57 GMT	2002-06-05 00:10:57 GMT	1376
00017.SPL			0	2002-06-05 00:10:57 GMT	2002-06-05 00:10:57 GMT	2002-06-05 00:10:57 GMT	2002-06-05 00:10:57 GMT	345052
00018.SHD			0	2002-06-05 00:11:37 GMT	2002-06-05 00:11:37 GMT	2002-06-05 00:11:37 GMT	2002-06-05 00:11:37 GMT	1360
00018.SPL			0	2002-06-05 00:11:37 GMT	2002-06-05 00:11:37 GMT	2002-06-05 00:11:37 GMT	2002-06-05 00:11:37 GMT	941248
00019.SHD			0	2002-06-05 00:18:11 GMT	2002-06-05 00:18:11 GMT	2002-06-05 00:18:11 GMT	2002-06-05 00:18:11 GMT	1412
00019.SPL			0	2002-06-05 00:18:11 GMT	2002-06-05 00:18:11 GMT	2002-06-05 00:18:10 GMT	2002-06-05 00:18:10 GMT	394748
00020.SHD			0	2002-06-05 00:18:31 GMT	2002-06-05 00:18:31 GMT	2002-06-05 00:18:31 GMT	2002-06-05 00:18:31 GMT	1372
00020.SPL			0	2002-06-05 00:18:31 GMT	2002-06-05 00:18:31 GMT	2002-06-05 00:18:31 GMT	2002-06-05 00:18:31 GMT	524724
00021.SHD			0	2002-06-05 00:22:25 GMT	2002-06-05 00:22:25 GMT	2002-06-05 00:22:25 GMT	2002-06-05 00:22:25 GMT	1372
00021.SPL			0	2002-06-05 00:22:25 GMT	2002-06-05 00:22:25 GMT	2002-06-05 00:22:24 GMT	2002-06-05 00:22:24 GMT	1216240

Fig.94

In this image there are two types of files:

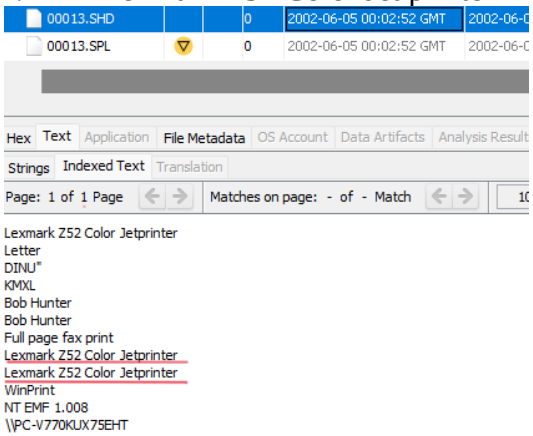
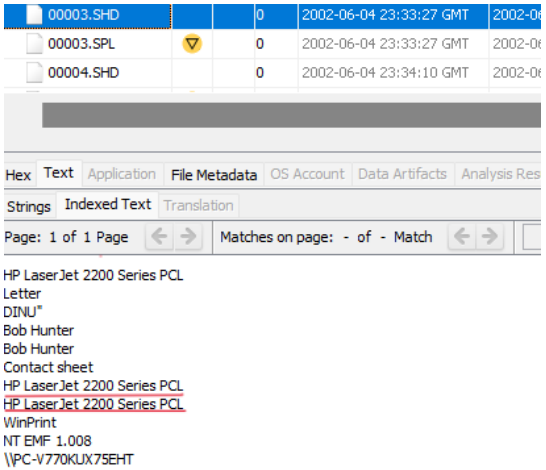
1. . SHD

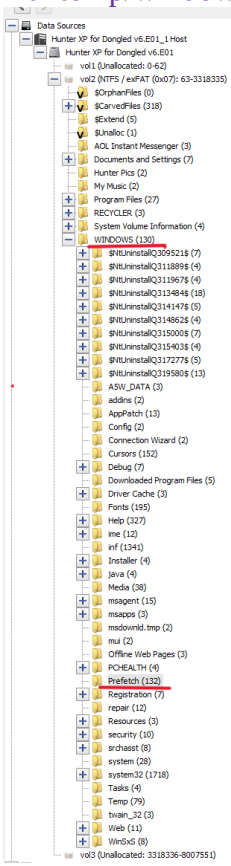
This file contains the details of information the computer sent to printer to execute the process.

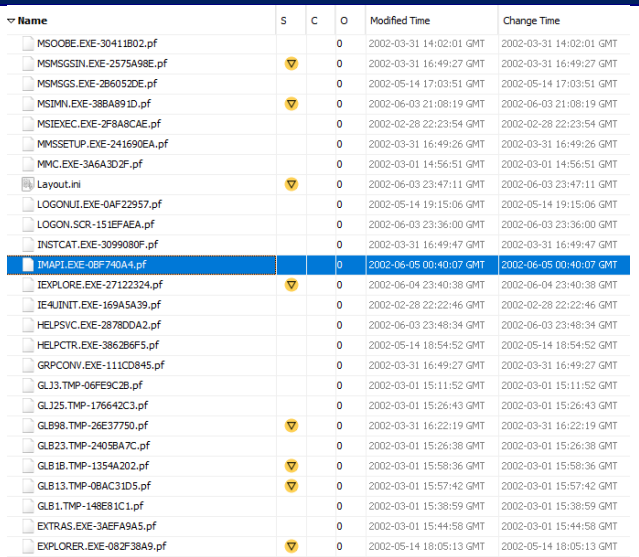
2. SPL

This file contains the name of document, owner name, printer name, etc.

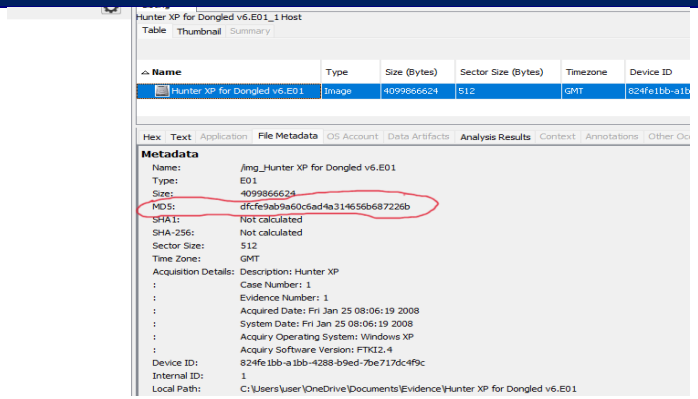
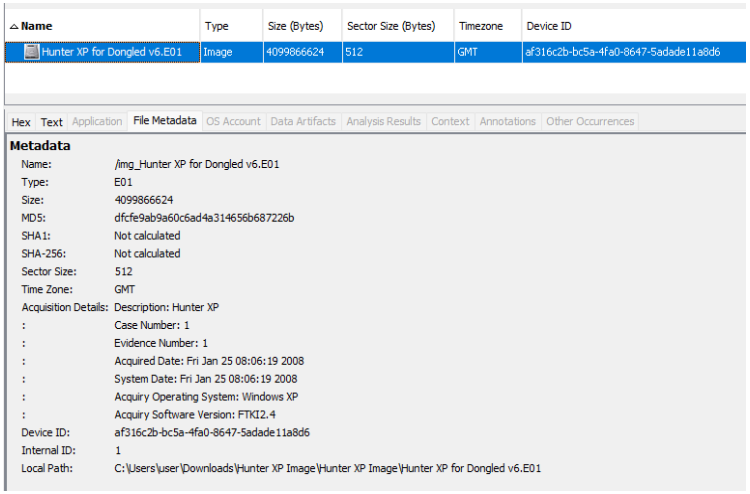
Furthermore, there are 2 printers used for this crime:

Action	Done?	Date	Time	Notes
				I. Lexmark Z52 Color Jet printer  Fig.95 ii, HP LaserJet 2200 Series PCL  Fig.96

Action	Done?	Date	Time	Notes
CD/DVD burning apps; check log files	Yes	30th November 2024	8:00 Pm	To get information about the activity “CD/DVD” burning go through the location: Hunterxp/windows/prefetch  Fig.97 Here is a software “**Imapi.exe**” Imapi is a software used to erase the data from Cd/DVD.

Action	Done?	Date	Time	Notes
				 Fig.98
Validate evidence integrity at the end of the examination	Yes	30th November 2024	8:45 Pm	As I finished the investigation, I need to validate the hash value if the data is altered or not. To validate the hash value, I will use AUTOPSY TOOL after that I will match the initial hash value and ending hash value. INITAIL HASH VALUE FROM AUTOPSY 4.19.2:

Name	S	C	O	Modified Time	Change Time
MSOOBE.EXE-30411B02.pf			0	2002-03-31 14:02:01 GMT	2002-03-31 14:02:01 GMT
MSMSGSIN.EXE-2575A98E.pf			0	2002-03-31 16:49:27 GMT	2002-03-31 16:49:27 GMT
MSMSGS.EXE-2B6052DE.pf			0	2002-05-14 17:03:51 GMT	2002-05-14 17:03:51 GMT
MSIMN.EXE-38BA891D.pf			0	2002-06-03 21:08:19 GMT	2002-06-03 21:08:19 GMT
MSIEXEC.EXE-2F8A8CAE.pf			0	2002-02-28 22:23:54 GMT	2002-02-28 22:23:54 GMT
MMSSETUP.EXE-241690EA.pf			0	2002-03-31 16:49:26 GMT	2002-03-31 16:49:26 GMT
MMC.EXE-3A6A3D2F.pf			0	2002-03-01 14:56:51 GMT	2002-03-01 14:56:51 GMT
Layout.ini			0	2002-06-03 23:47:11 GMT	2002-06-03 23:47:11 GMT
LOGONUI.EXE-0AF22957.pf			0	2002-05-14 19:15:06 GMT	2002-05-14 19:15:06 GMT
LOGON.SCR-151EFAEA.pf			0	2002-06-03 23:36:00 GMT	2002-06-03 23:36:00 GMT
INSTCAT.EXE-3099080F.pf			0	2002-03-31 16:49:47 GMT	2002-03-31 16:49:47 GMT
IMAPI.EXE-0BF740A4.pf			0	2002-06-05 00:40:07 GMT	2002-06-05 00:40:07 GMT
IEXPLORE.EXE-27122324.pf			0	2002-06-04 23:40:38 GMT	2002-06-04 23:40:38 GMT
IE4UINIT.EXE-169A5A39.pf			0	2002-02-28 22:22:46 GMT	2002-02-28 22:22:46 GMT
HELPSVC.EXE-2878DDA2.pf			0	2002-06-03 23:48:34 GMT	2002-06-03 23:48:34 GMT
HELPCTR.EXE-3862B6F5.pf			0	2002-05-14 18:54:52 GMT	2002-05-14 18:54:52 GMT
GRPCONV.EXE-111CD845.pf			0	2002-03-31 16:49:27 GMT	2002-03-31 16:49:27 GMT
GLJ3.TMP-06FE9C2B.pf			0	2002-03-01 15:11:52 GMT	2002-03-01 15:11:52 GMT
GLJ25.TMP-176642C3.pf			0	2002-03-01 15:26:43 GMT	2002-03-01 15:26:43 GMT
GLB98.TMP-26E37750.pf			0	2002-03-31 16:22:19 GMT	2002-03-31 16:22:19 GMT
GLB23.TMP-2405BA7C.pf			0	2002-03-01 15:26:38 GMT	2002-03-01 15:26:38 GMT
GLB1B.TMP-1354A202.pf			0	2002-03-01 15:58:36 GMT	2002-03-01 15:58:36 GMT
GLB13.TMP-08AC31D5.pf			0	2002-03-01 15:57:42 GMT	2002-03-01 15:57:42 GMT
GLB1.TMP-148E81C1.pf			0	2002-03-01 15:38:59 GMT	2002-03-01 15:38:59 GMT
EXTRAS.EXE-3AEFA9A5.pf			0	2002-03-01 15:44:58 GMT	2002-03-01 15:44:58 GMT
EXPLORER.EXE-082F38A9.pf			0	2002-05-14 18:05:13 GMT	2002-05-14 18:05:13 GMT

Action	Done?	Date	Time	Notes
				 Fig.99 FINAL HASH VALUE AFTER ENDING THE INVESTIGATION:  Fig.100 As I can see the hash value of both initial and final is same from autopsy tool. I can say that the evidence is not altered.

Additional Notes/Artefacts Examined:

Colour-coding Legend	Tasks
	Fundamental
	Basic
	Elementary
	Secondary
	Advanced
	Exceptional