

# Contemporaneous Notes

## Cyber Crime and Digital Evidence



### Submitted by

Name: Sidhant Kumar Chaurasiya

Student ID:10487

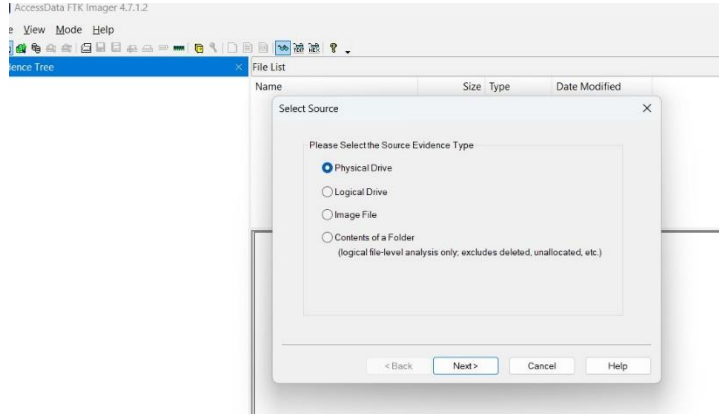
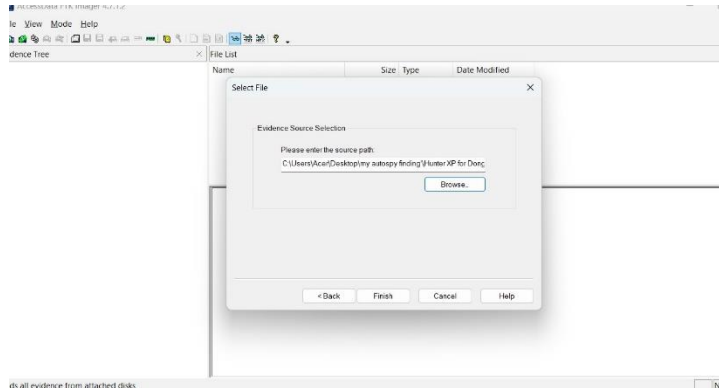
Cyber Security and digital forensics

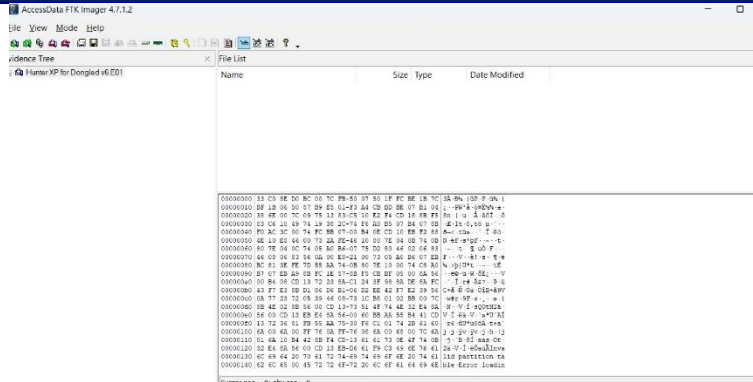
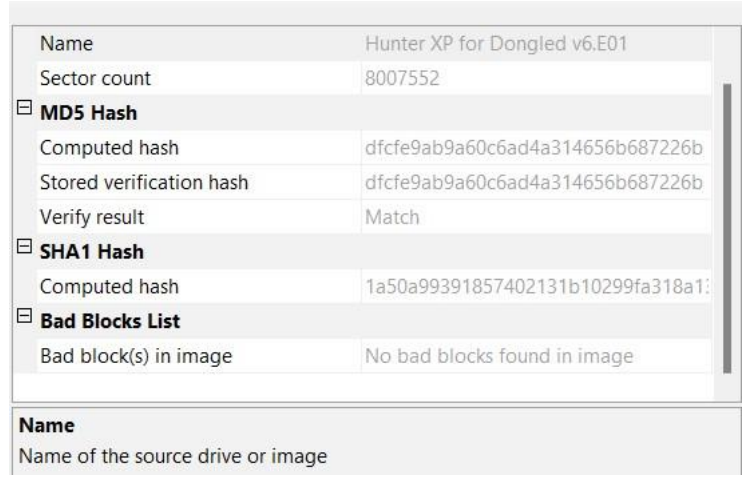
Kathmandu, Nepal

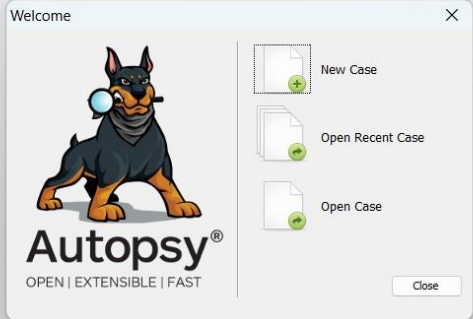
## Contemporaneous Notes

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

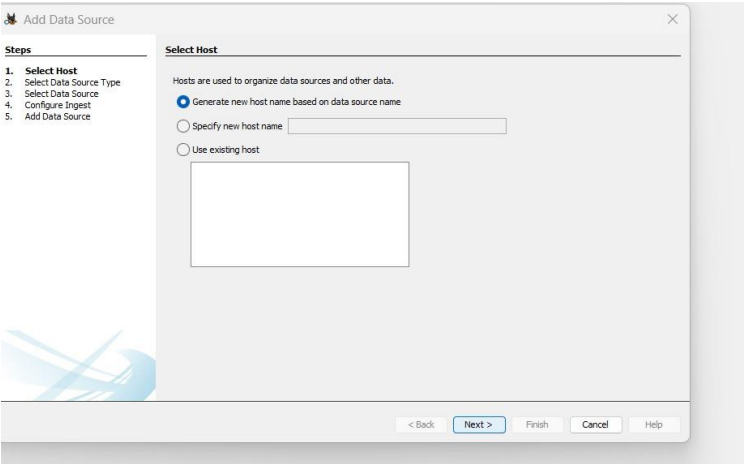
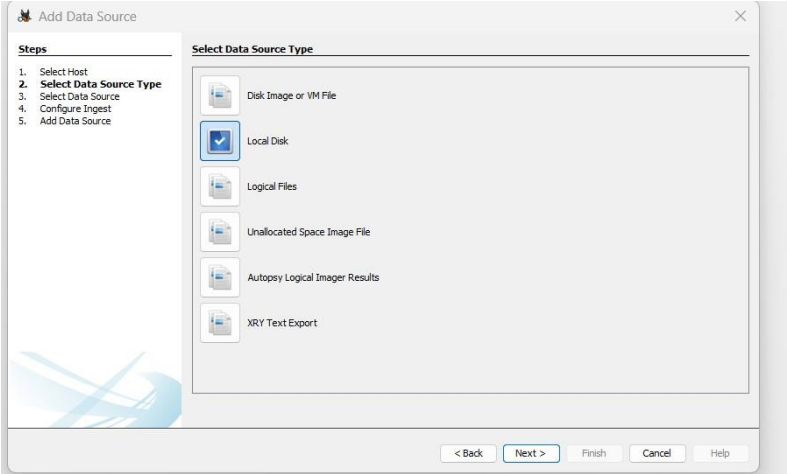
Examiner	Sidhant Kumar Chaurasiya	Exam commenced	November 26 <sup>th</sup> 2024
Other relevant information	Student number:- 24000865	Software used, versions, and licensing	FTK Imager 4.7.12 Registry viewer 1.8.0.5 Autopsy 4.19.2 Event Log Explorer 4.8 Reg ripper 3.0 Is the software used in the investigation

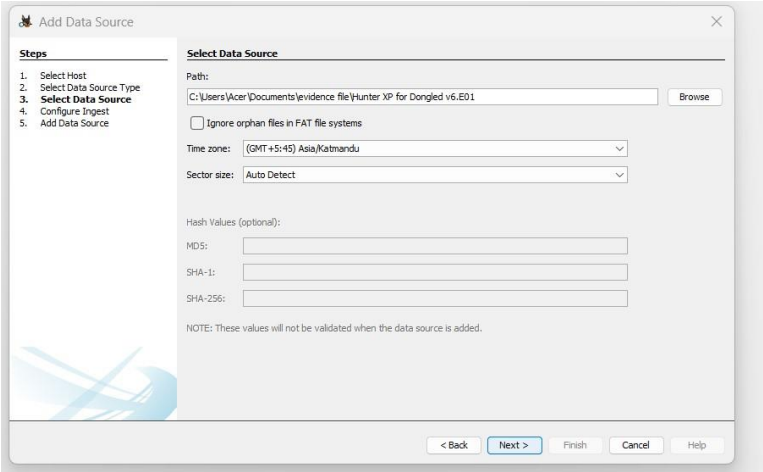
Action	Done?	Date	Time	Notes
Load case and verify image	yes	Nov 26th 2024	12 A.M	<p>For loading the image I use the FTK imager.</p> <ol style="list-style-type: none"> <li>1. go to add evidence item. click on it to open.</li> <li>2. select the sources evidence types as "image file" .select next</li> </ol>  <ol style="list-style-type: none"> <li>3. select the image sources path. Click on finish</li> </ol>  <ol style="list-style-type: none"> <li>4. after clicking to finish we see the file like the screenshot given below.</li> </ol>

Action	Done?	Date	Time	Notes
				 <p>5. after the image is successfully loaded. Left-click on the image and select the “verify drive image”.it takes some time to give the value after clicking on it.</p> <p>6. after some time values are seen where there is the hash value of the file “ Hunter XP” which we are going to analyse</p> 

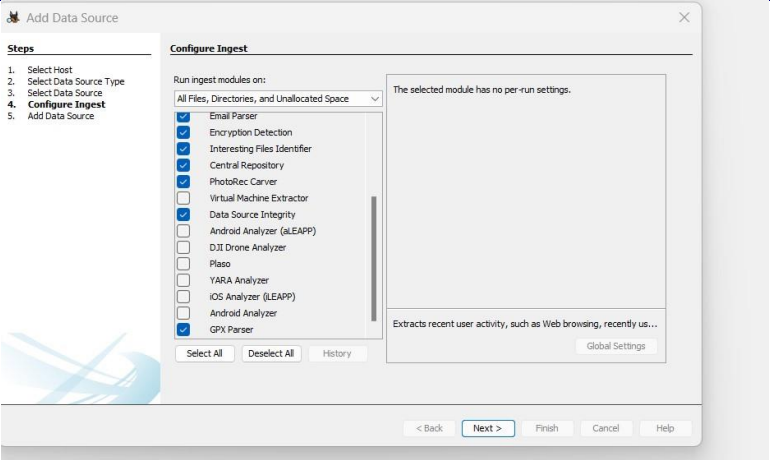
Action	Done?	Date	Time	Notes
Load Case into a second forensic tool for dual verification of at least 2 key artifacts, evidence items	yes	Nov 26th 2024	12:20 P.M	<p>The second tool I use to check the dual verification of at least 2 key artifacts in the autopsy</p> <ol style="list-style-type: none"> <li>1. Double-click the autopsy tool to open it.</li> <li>2. after opening the autopsy it looks like this.</li> </ol>  <ol style="list-style-type: none"> <li>3. to load a Case Select the new case. and give the case name and the path of the base directory. And check the case type (if you are doing it alone select single-user or if you are doing it in the group then choose multi-user)</li> </ol>

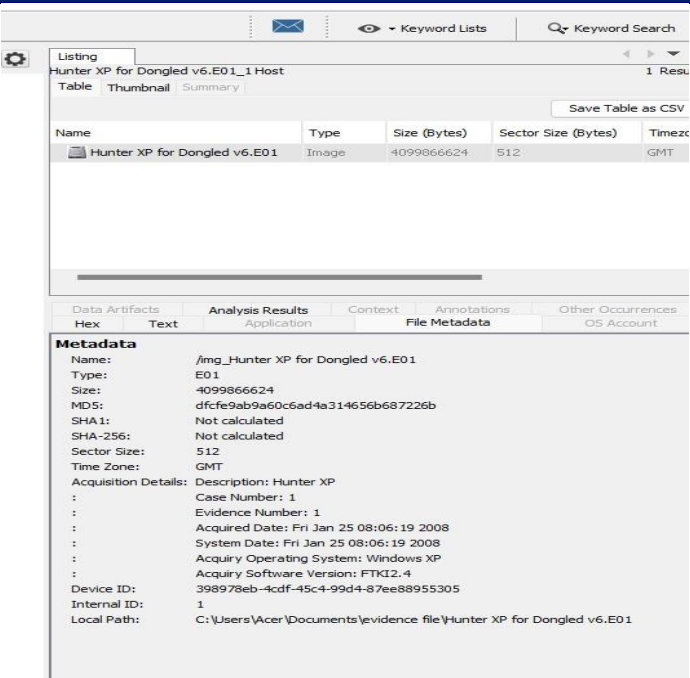


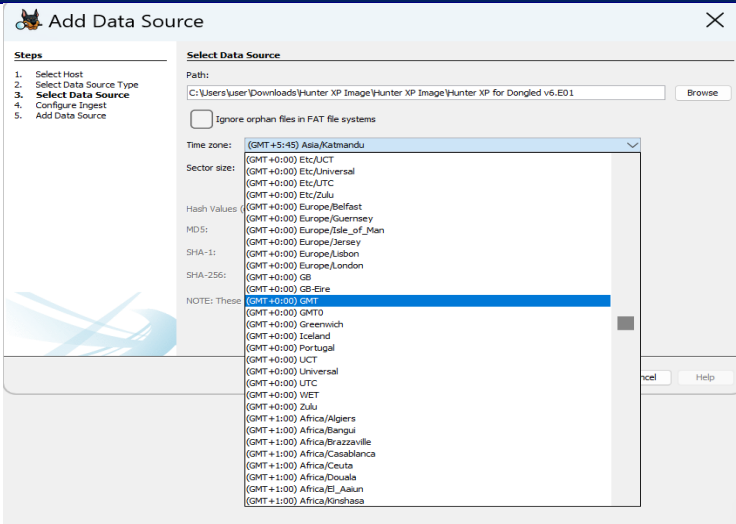
Action	Done?	Date	Time	Notes
				<p>5.select host and click next</p> 
				<p>6. then select the disk image or VM file and click next</p> 

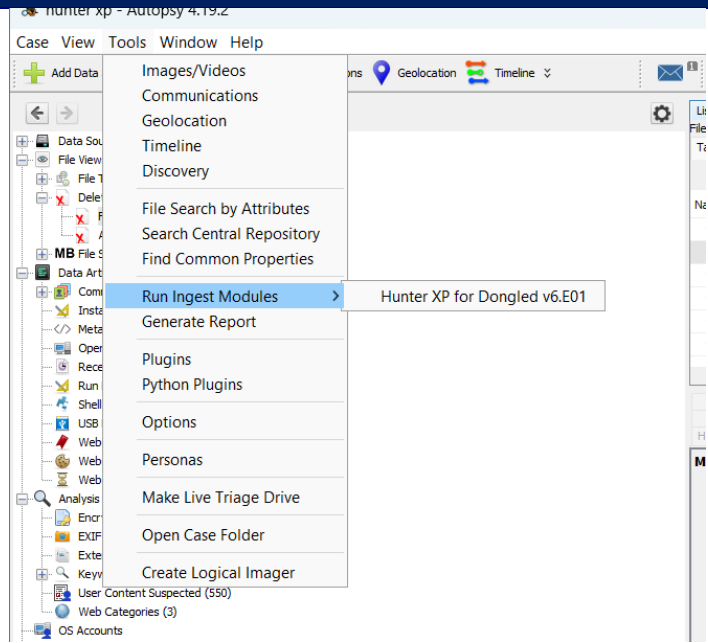
Action	Done?	Date	Time	Notes
				<p>7. select data sources and give the local disk location where there is a file for the image. Then select the time zone to the country where you are for easy understanding of file details</p>  <p>8. then select the configuration to ingest and click next</p>

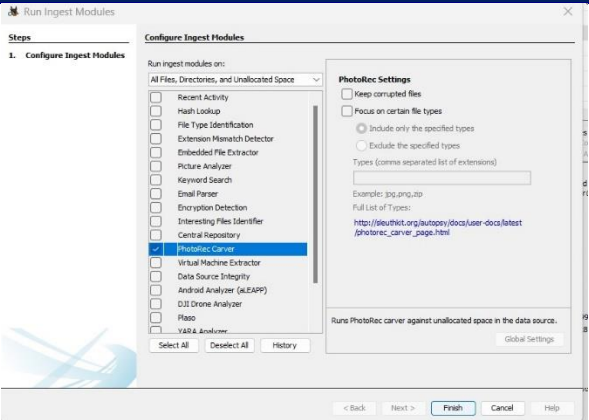
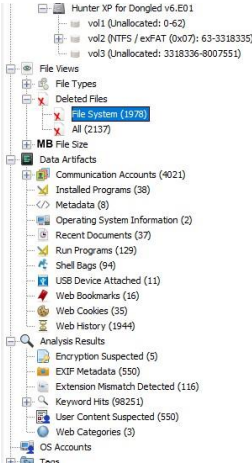


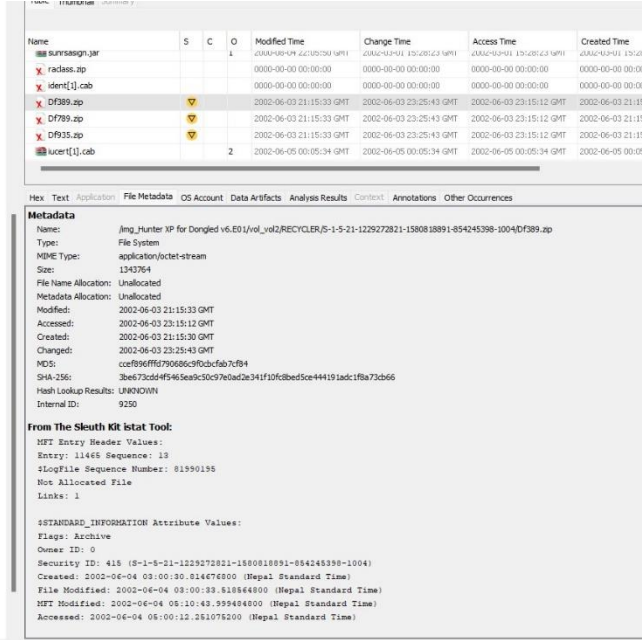
Action	Done?	Date	Time	Notes
				<div data-bbox="1128 239 1895 700"></div> <p>9. click on Hunter XP and go to the metadata. Check the hash value and verify it from the above imaging file of the FTK image if both are the same then the file is not changed/written by anyone</p>

Action	Done?	Date	Time	Notes
				
Time Zone Adjusted? Report Time Zone used for Analysis.	yes	Nov 26 <sup>th</sup> 2024	1 P.M	I adjusted the Time zone of the Hunter XP image file as per the UK local time which is (GMT +0:00) GMT Because the case is executed from the UK but we are doing forensics from Nepal. So for a better understanding of the case, we analysed the case in the UK time zone

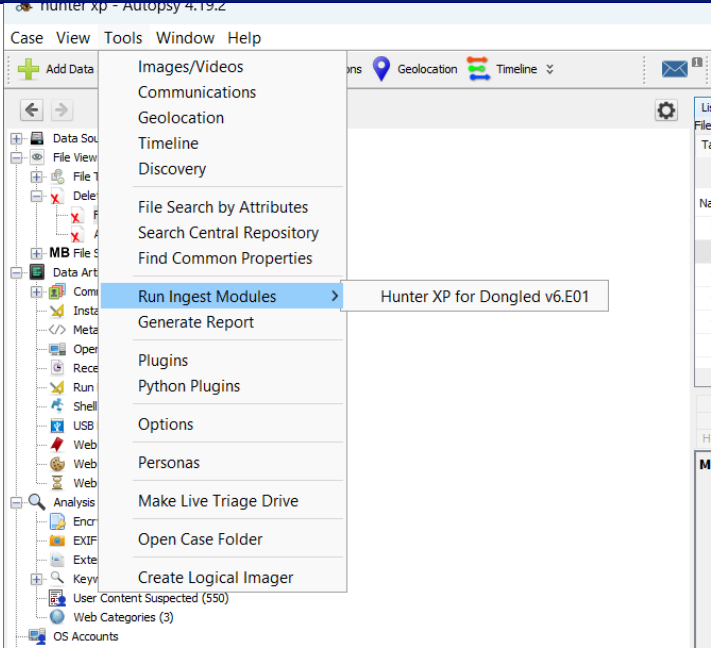
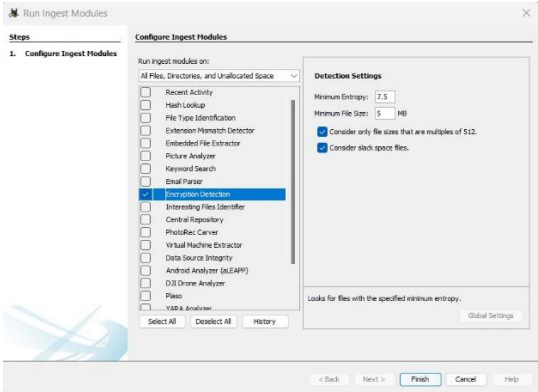
Action	Done?	Date	Time	Notes
				
Recover lost folders (NTFS, FAT16&32).	yes	Nov 26 <sup>th</sup> 2024	1:30 P.M	1. The NTFS file can be found when we go to the <b>tools</b> and then go to the <b>Run ingest Modules</b> and select <b>Hunter xp for dongled v6 E01</b>

Action	Done?	Date	Time	Notes
				<div></div> <p>2. after that go to the <b>photoRec Carver</b> select it and click on the finished</p>


Action	Done?	Date	Time	Notes
				<div></div> <p>3. after that go</p> <p>Files Type→Deleted Files → Files System</p> <div></div>

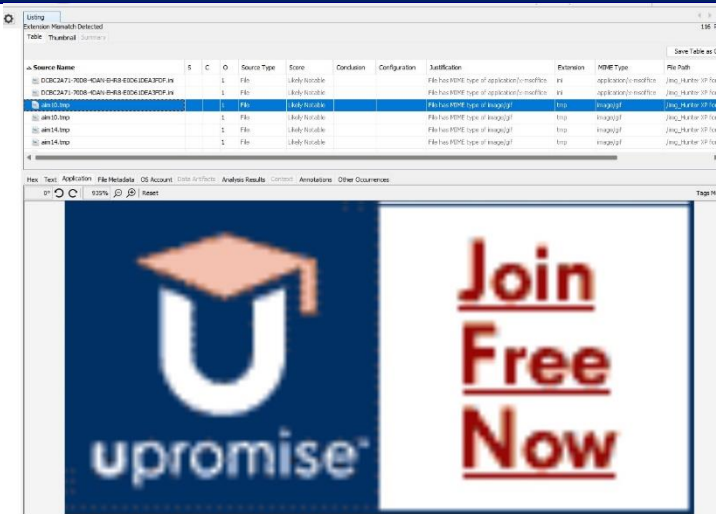
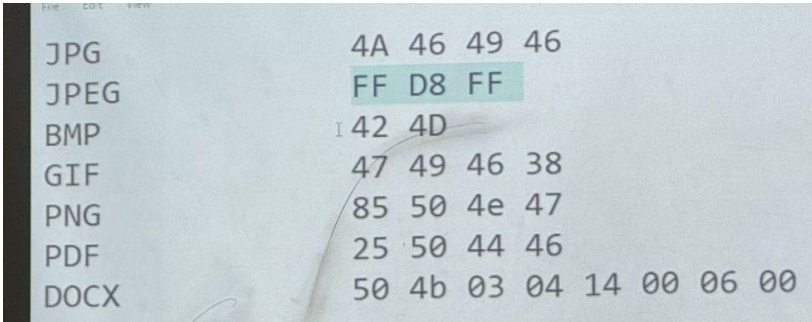
Action	Done?	Date	Time	Notes
Mount archives; zip, thumbs.db, etc.	yes	Nov 26 <sup>th</sup> 2024	2 P.M	<p>1. To find the Mount archived Zip file we must go to the file view go to file types, and then select by extension where we can see the archived files</p> <p>Link:- /img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df389.zip</p>  <p>2. to find the thumbs.db file we must go to HunterXP\volvol2\Documents &amp; Settings\bobhunter\My Documents\My Pictures\HunterPics\Sabina &amp; Christina location where we can find the file thumbs. DB</p>

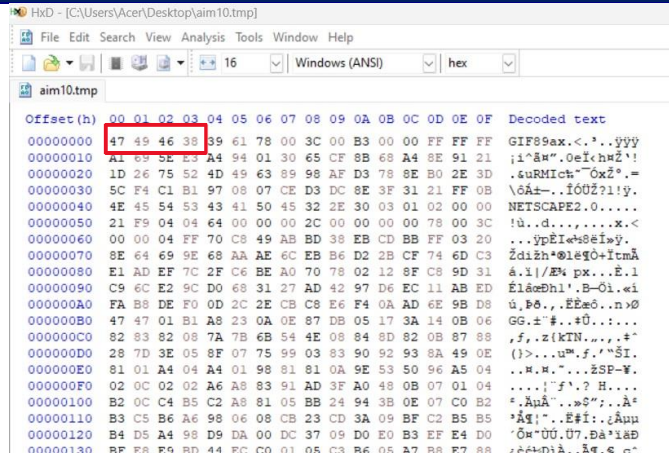
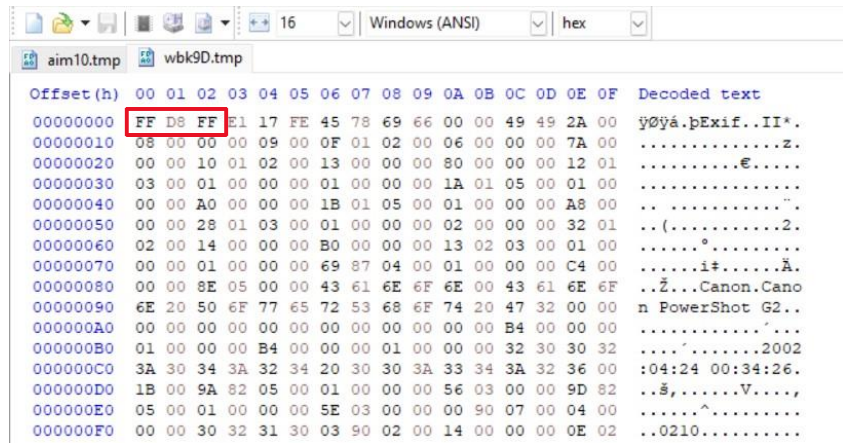
Action	Done?	Date	Time	Notes																																																				
				<div><div><div>Save Table as CSV</div><table><tr><th>Name</th><th>S</th><th>C</th><th>O</th><th>Modified Time</th><th>Change Time</th><th>Access Time</th><th>Created Time</th><th>Size</th><th>Flags(Dr)</th><th>Flags(Meta)</th><th>Known</th><th>Location</th></tr><tr><td> [current folder]</td><td></td><td></td><td></td><td>2002-06-05 00:49:28 GMT</td><td>2002-06-05 00:49:28 GMT</td><td>2002-06-05 00:49:28 GMT</td><td>2002-06-03 23:14:53 GMT</td><td>56</td><td>Allocated</td><td>Allocated</td><td>unknown</td><td>/img_hunter XP for Dongled v6.EC</td></tr><tr><td> [parent folder]</td><td></td><td></td><td></td><td>2002-06-05 00:49:16 GMT</td><td>2002-06-05 00:49:16 GMT</td><td>2002-06-05 00:49:16 GMT</td><td>2002-06-03 22:39:50 GMT</td><td>56</td><td>Allocated</td><td>Allocated</td><td>unknown</td><td>/img_hunter XP for Dongled v6.EC</td></tr><tr><td> Thumbnail.db</td><td>2</td><td></td><td></td><td>2002-06-03 23:55:43 GMT</td><td>2002-06-05 00:39:58 GMT</td><td>2002-06-03 23:58:01 GMT</td><td>2002-06-03 23:55:35 GMT</td><td>52224</td><td>Allocated</td><td>Allocated</td><td>unknown</td><td>/img_hunter XP for Dongled v6.EC</td></tr></table></div><div><div></div><div>Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences</div><div>Type: File System</div><div>MIME Type: application/x-msoffice</div><div>Size: 52224</div><div>File Name Allocation: Allocated</div><div>Metadata Allocation: Allocated</div><div>Modfied: 2002-06-03 23:55:43 GMT</div><div>Accessed: 2002-06-03 23:58:01 GMT</div><div>Created: 2002-06-03 23:55:35 GMT</div><div>Changed: 2002-06-05 00:39:58 GMT</div><div>MD5: 4d596cd0a0f0c5eb1f5d43dc0fba06</div><div>SHA-256: 4ee5d4e16442b67a5d4a019ef083e5281d81d77ecbe98b58c74b4aa3c</div><div>Hash Lookup Results: L989C20N</div><div>Internal ID: 4994</div><div>From The Sleuth Kit Instat Tool:<div><div>NFT Entry Header Values:<div>Entry: 9144 Sequence: 10</div><div>StlogFile Sequence Number: 88285526</div><div>Allocated File</div><div>Links: 2</div></div><div>STANDARD_INFORMATION Attribute Values:<div>Flags: Hidden, System, Archive</div><div>Owner ID: 0</div><div>Security ID: 361 (B-1-5-01-1229272821-1800818991-054248398-1004)</div><div>Created: 2002-04-04 08:40:38.448774400 (Hpal Standard Time)</div><div>File Modified: 2002-06-04 05:40:43.286000000 (Hpal Standard Time)</div><div>NFT Modified: 2002-06-08 04:24:58.390871200 (Hpal Standard Time)</div><div>Accessed: 2002-06-04 05:43:01.255164800 (Hpal Standard Time)</div></div><div>2FILE_NAME Attribute Values:<div>Filename: Thumbnail.db</div></div></div></div></div></div>	Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location	[current folder]				2002-06-05 00:49:28 GMT	2002-06-05 00:49:28 GMT	2002-06-05 00:49:28 GMT	2002-06-03 23:14:53 GMT	56	Allocated	Allocated	unknown	/img_hunter XP for Dongled v6.EC	[parent folder]				2002-06-05 00:49:16 GMT	2002-06-05 00:49:16 GMT	2002-06-05 00:49:16 GMT	2002-06-03 22:39:50 GMT	56	Allocated	Allocated	unknown	/img_hunter XP for Dongled v6.EC	Thumbnail.db	2			2002-06-03 23:55:43 GMT	2002-06-05 00:39:58 GMT	2002-06-03 23:58:01 GMT	2002-06-03 23:55:35 GMT	52224	Allocated	Allocated	unknown	/img_hunter XP for Dongled v6.EC
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location																																												
[current folder]				2002-06-05 00:49:28 GMT	2002-06-05 00:49:28 GMT	2002-06-05 00:49:28 GMT	2002-06-03 23:14:53 GMT	56	Allocated	Allocated	unknown	/img_hunter XP for Dongled v6.EC																																												
[parent folder]				2002-06-05 00:49:16 GMT	2002-06-05 00:49:16 GMT	2002-06-05 00:49:16 GMT	2002-06-03 22:39:50 GMT	56	Allocated	Allocated	unknown	/img_hunter XP for Dongled v6.EC																																												
Thumbnail.db	2			2002-06-03 23:55:43 GMT	2002-06-05 00:39:58 GMT	2002-06-03 23:58:01 GMT	2002-06-03 23:55:35 GMT	52224	Allocated	Allocated	unknown	/img_hunter XP for Dongled v6.EC																																												
File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation)	yes	Nov 26 <sup>th</sup> 2024	3 P.M	1. files signature analysis (any interesting mismatch) can be found when we go to the <b>tools</b> and then go to the <b>Run ingest Modules</b> and select <b>Hunter xp for dongled v6 E01</b>																																																				

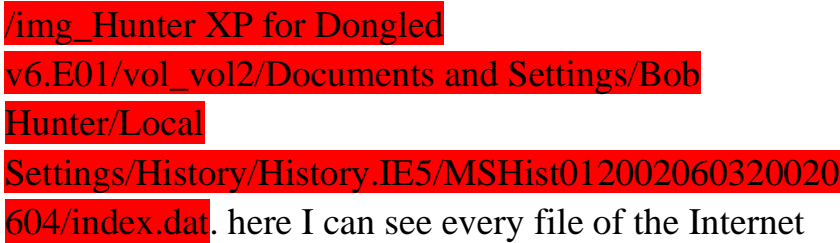
Action	Done?	Date	Time	Notes
				<div></div> <p>2. then select encryption detection and then select finish.</p> <div></div>

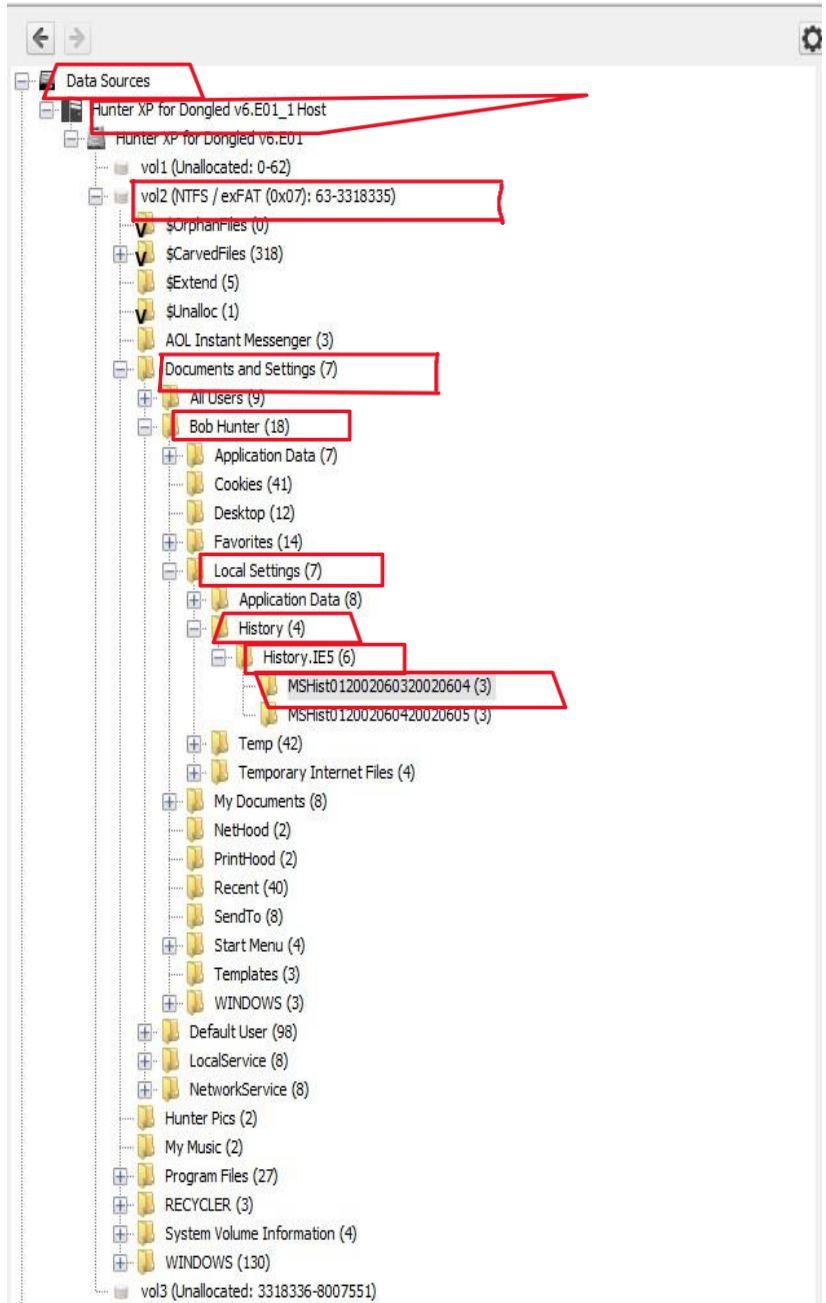


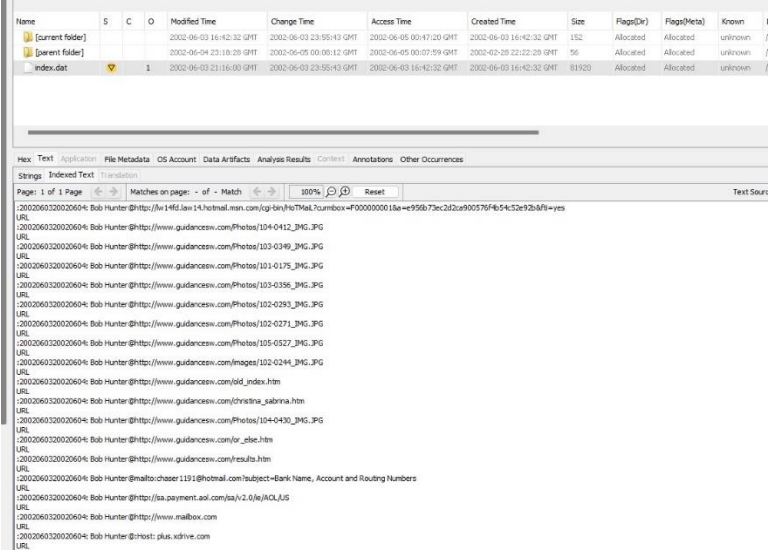
Action	Done?	Date	Time	Notes
				<p>3. Go to the Analysis Result→ Extension Mismatch Detected</p>  <p>4. here we can find the different file's signature mismatch we analyzed one file from extension mismatch detection by finding the hash value of that file from it</p>


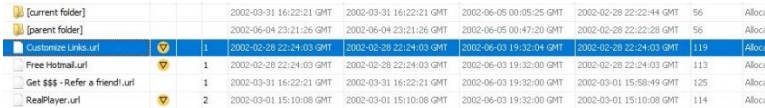
Action	Done?	Date	Time	Notes
				 <p>5. analysis the hash value of this file in HDX setup where we can hash value of the file where the first 4 values define the file types</p>  <p>6. then we check the hash value of aim10.tmp to verify that the file signature of that files is changed or not</p>




Action	Done?	Date	Time	Notes
				 <p>From here we can say that the file signature is changed the file name is aim10.tmp which is a GIF file</p> <p>7. also check the other to know how many file signatures are changed here we analyze an image</p> 

Action	Done?	Date	Time	Notes
				Here I see that these files we can see are actually JPEG and the files/evidence is tempering
Internet History, favorites, etc. Other browsers?	yes	NOV 27 <sup>TH</sup> 2024	10A.M	1.here to find internet history I go to the  here I can see every file of the Internet history

				 <p>The screenshot displays a file explorer window showing a directory tree. The tree structure is as follows:</p> <ul style="list-style-type: none"><li>Data Sources<ul style="list-style-type: none"><li>Hunter XP for Dongled v6.E01_1 Host</li><li>Hunter XP for Dongled v6.E01<ul style="list-style-type: none"><li>vol1 (Unallocated: 0-62)</li><li>vol2 (NTFS / exFAT (0x07): 63-3318335)<ul style="list-style-type: none"><li>\$orphanFiles (0)</li><li>\$CarvedFiles (318)</li><li>\$Extend (5)</li><li>\$Unalloc (1)</li><li>AOL Instant Messenger (3)</li><li>Documents and Settings (7)<ul style="list-style-type: none"><li>All Users (9)</li><li>Bob Hunter (18)<ul style="list-style-type: none"><li>Application Data (7)</li><li>Cookies (41)</li><li>Desktop (12)</li><li>Favorites (14)</li><li>Local Settings (7)<ul style="list-style-type: none"><li>Application Data (8)</li><li>History (4)<ul style="list-style-type: none"><li>History.IE5 (6)<ul style="list-style-type: none"><li>MSHist012002060320020604 (3)</li><li>MSHist012002060420020605 (3)</li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul> <li>Temp (42)</li> <li>Temporary Internet Files (4)</li> <li>My Documents (8)</li> <li>NetHood (2)</li> <li>PrintHood (2)</li> <li>Recent (40)</li> <li>SendTo (8)</li> <li>Start Menu (4)</li> <li>Templates (3)</li> <li>WINDOWS (3)</li> <li>Default User (98)</li> <li>LocalService (8)</li> <li>NetworkService (8)</li> <li>Hunter Pics (2)</li> <li>My Music (2)</li> <li>Program Files (27)</li> <li>RECYCLER (3)</li> <li>System Volume Information (4)</li> <li>WINDOWS (130)</li> <li>vol3 (Unallocated: 3318336-8007551)</li>
--	--	--	--	---


Action	Done?	Date	Time	Notes
				<p>2. here I can see all the internet history of Bob Hunter</p>  <p>These all are the websites visited by suspected “bob hunter”. In this index.dat file, we can see here that there are a lot of alleged app</p> <p>3. for favourites I must go</p> <p>/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Favorites</p>

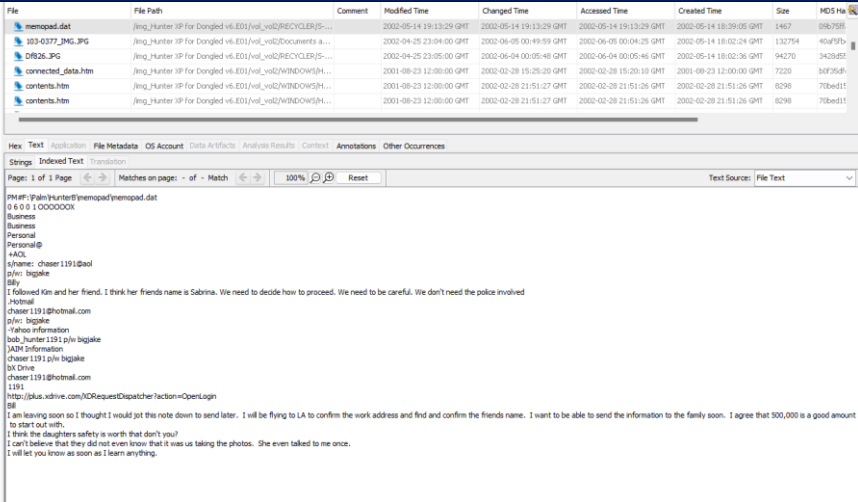
Action	Done?	Date	Time	Notes
				 <p>All the favourite files are</p>  <p>3. to find another browser I go to web history and check all file program names and find that there is only one browser used which is Internet Explorer</p>

Action	Done?	Date	Time	Notes																																																																								
				<div><div><table><tr><th>Source Name</th><th>S</th><th>C</th><th>O</th><th>URL</th><th>Date Accessed</th><th>Referrer URL</th><th>Program Name</th><th>Domain</th></tr><tr><td>index.dat</td><td></td><td></td><td>2</td><td>http://plus.xdrive.com/latin/moz/xdrv/no_LOCALE/media/...</td><td>2002-06-04 17:36:28 GMT</td><td></td><td>Internet Explorer</td><td>xdrive.com</td></tr><tr><td>index.dat</td><td></td><td></td><td>2</td><td>http://lw14fd.law14.hotmail.msn.com/cgi-bin/dasp/EN/hot...</td><td>2002-06-04 18:02:37 GMT</td><td></td><td>Internet Explorer</td><td>msn.com</td></tr><tr><td>index.dat</td><td></td><td></td><td>2</td><td>http://lw14fd.law14.hotmail.msn.com/cgi-bin/HotMail?cur...</td><td>2002-05-14 11:18:47 GMT</td><td></td><td>Internet Explorer</td><td>msn.com</td></tr><tr><td>index.dat</td><td></td><td></td><td>2</td><td>http://ads.web.aol.com/content/B0/0H7pTL2Luf0_jw3xml...</td><td>2002-05-14 11:47:40 GMT</td><td></td><td>Internet Explorer</td><td>aol.com</td></tr><tr><td>index.dat</td><td></td><td></td><td>2</td><td>https://plus.xdrive.com/latin/moz/xdrv/no_LOCALE/media/...</td><td>2002-03-31 10:39:51 GMT</td><td></td><td>Internet Explorer</td><td>xdrive.com</td></tr><tr><td>index.dat</td><td></td><td></td><td>2</td><td>https://plus.xdrive.com/latin/moz/xdrv/no_LOCALE/media/...</td><td>2002-03-31 10:40:41 GMT</td><td></td><td>Internet Explorer</td><td>xdrive.com</td></tr><tr><td>index.dat</td><td></td><td></td><td>2</td><td>http://plus.xdrive.com/latin/moz/xdrv/no_LOCALE/media/...</td><td>2002-06-04 17:34:34 GMT</td><td></td><td>Internet Explorer</td><td>xdrive.com</td></tr></table></div><p>Another method to find Internet History, favorites, etc. Other browsers are simply go to the Data Artifacts→Web Bookmarks/Web Cookies/Web History</p><div><div><div> Web Bookmarks (64)</div><div> Web Cookies (140)</div><div> Web History (7776)</div></div></div><p>1. to find the email I go to the files <div>/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/6ZSJ6T6D/getmsg[2]/getmsg[2]/0</div></p></div>	Source Name	S	C	O	URL	Date Accessed	Referrer URL	Program Name	Domain	index.dat			2	http://plus.xdrive.com/latin/moz/xdrv/no_LOCALE/media/...	2002-06-04 17:36:28 GMT		Internet Explorer	xdrive.com	index.dat			2	http://lw14fd.law14.hotmail.msn.com/cgi-bin/dasp/EN/hot...	2002-06-04 18:02:37 GMT		Internet Explorer	msn.com	index.dat			2	http://lw14fd.law14.hotmail.msn.com/cgi-bin/HotMail?cur...	2002-05-14 11:18:47 GMT		Internet Explorer	msn.com	index.dat			2	http://ads.web.aol.com/content/B0/0H7pTL2Luf0_jw3xml...	2002-05-14 11:47:40 GMT		Internet Explorer	aol.com	index.dat			2	https://plus.xdrive.com/latin/moz/xdrv/no_LOCALE/media/...	2002-03-31 10:39:51 GMT		Internet Explorer	xdrive.com	index.dat			2	https://plus.xdrive.com/latin/moz/xdrv/no_LOCALE/media/...	2002-03-31 10:40:41 GMT		Internet Explorer	xdrive.com	index.dat			2	http://plus.xdrive.com/latin/moz/xdrv/no_LOCALE/media/...	2002-06-04 17:34:34 GMT		Internet Explorer	xdrive.com
Source Name	S	C	O	URL	Date Accessed	Referrer URL	Program Name	Domain																																																																				
index.dat			2	http://plus.xdrive.com/latin/moz/xdrv/no_LOCALE/media/...	2002-06-04 17:36:28 GMT		Internet Explorer	xdrive.com																																																																				
index.dat			2	http://lw14fd.law14.hotmail.msn.com/cgi-bin/dasp/EN/hot...	2002-06-04 18:02:37 GMT		Internet Explorer	msn.com																																																																				
index.dat			2	http://lw14fd.law14.hotmail.msn.com/cgi-bin/HotMail?cur...	2002-05-14 11:18:47 GMT		Internet Explorer	msn.com																																																																				
index.dat			2	http://ads.web.aol.com/content/B0/0H7pTL2Luf0_jw3xml...	2002-05-14 11:47:40 GMT		Internet Explorer	aol.com																																																																				
index.dat			2	https://plus.xdrive.com/latin/moz/xdrv/no_LOCALE/media/...	2002-03-31 10:39:51 GMT		Internet Explorer	xdrive.com																																																																				
index.dat			2	https://plus.xdrive.com/latin/moz/xdrv/no_LOCALE/media/...	2002-03-31 10:40:41 GMT		Internet Explorer	xdrive.com																																																																				
index.dat			2	http://plus.xdrive.com/latin/moz/xdrv/no_LOCALE/media/...	2002-06-04 17:34:34 GMT		Internet Explorer	xdrive.com																																																																				
Emails, local and web-based.	yes	NOV 27 <sup>TH</sup> 2024	11:20 A.M																																																																									



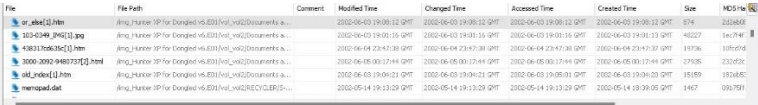
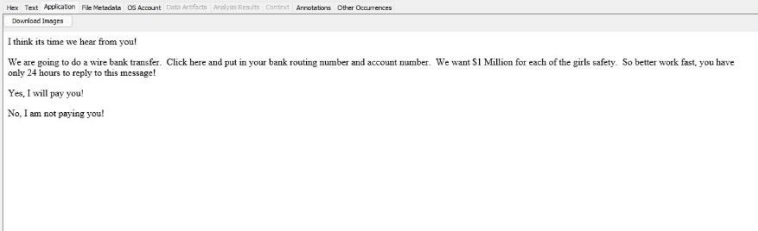

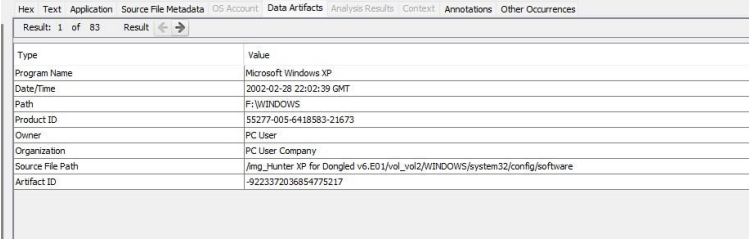
Action	Done?	Date	Time	Notes
				<p>Here I can see that there is an email ID of <a href="mailto:friend@bemine.com">friend@bemine.com</a> and <a href="mailto:chaser1191@hotmail.com">chaser1191@hotmail.com</a> also the email of chaser friend <a href="mailto:billyray150b@netscape.com">billyray150b@netscape.com</a> here from the given screenshot I can also find out that Billyray was also involved in the case and share the email of father.</p>  

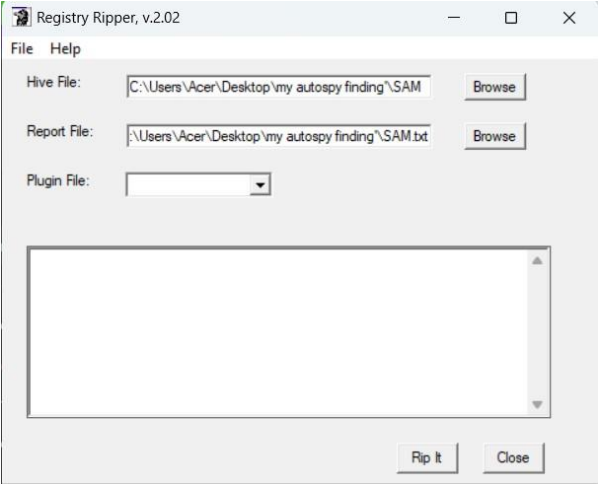
Action	Done?	Date	Time	Notes
				 <p>3. also I found more details of the case by analysing the email where I see the details of the discussion for ransomware and the file path of the image is</p> <p><b>/img_Hunter XP for Dongled</b>  <b>v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-</b>  <b>1580818891-854245398-</b>  <b>1004/Df1040/HunterB/memopad/memopad.dat</b></p>

Action	Done?	Date	Time	Notes
				
				<p>4. by analyzing deeply I can find the conversation on the case and bargaining of the ransomware for the crime. The location of the file</p> <p><b>/img_Hunter XP for Dongled</b></p> <p><b>v6.E01/vol_vol2/Documents and Settings/Bob</b></p> <p><b>Hunter/Local Settings/Temporary Internet</b></p> <p><b>Files/Content.IE5/6ZSJ6T6D/or_else[1].htm</b></p>

4. by analyzing deeply I can find the conversation on the case and bargaining of the ransomware for the crime. The location of the file

/img\_Hunter XP for Dongled  
v6.E01/vol\_vol2/Documents and Settings/Bob  
Hunter/Local Settings/Temporary Internet  
Files/Content.IE5/6ZSJ6T6D/or\_else[1].htm

Action	Done?	Date	Time	Notes
				 
Retrieve operating system information, accounts information, software, time zone information etc.).	yes	NOV 27 <sup>TH</sup> 2024	12 A.M	<p>1. I can found the information on the operation system of Hunter XP on the <b>file data artifacts</b> after that I go to the <b>operating system information</b> where I can see the whole details of OS and the source's path for the file is <b>img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/config/software</b></p>   <p>2. I can find the account information by go to <b>the LOCATION: Hunterxp/Partition 1/Noname/root/windows/system32/config</b> and then</p>

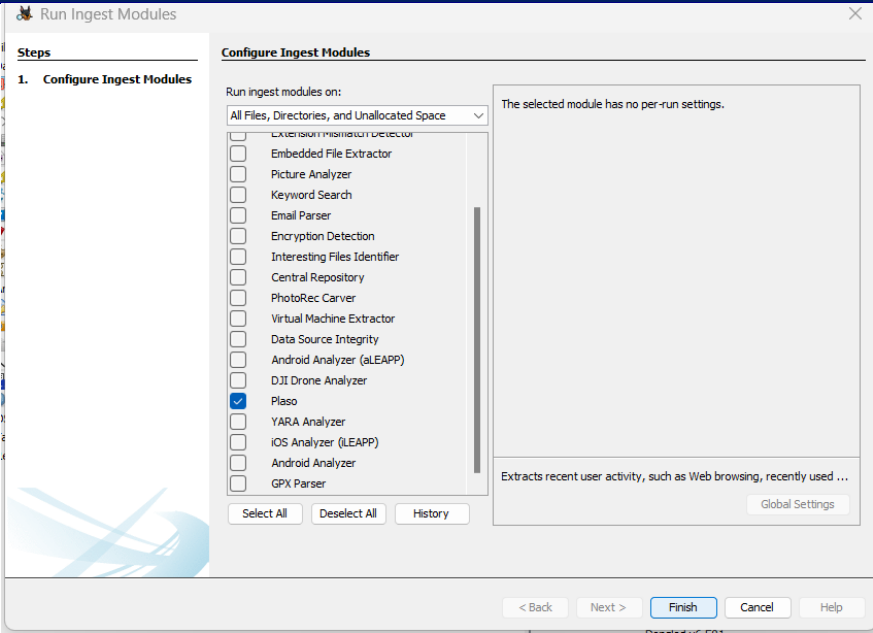
Action	Done?	Date	Time	Notes
				<p>left click it and <b>export files</b> after that I analyze the file name <b>SAM</b> by putting it into the reg ripper and convert that files into SAM.txt</p>  <p>Here we find the details about all the account user information where there is only one active user “Bob Hunter” and others are the system generated user</p> <pre>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 --&gt; Password does not expire --&gt; Password not required --&gt; Normal user account</pre> <p>The other system generated users are</p>

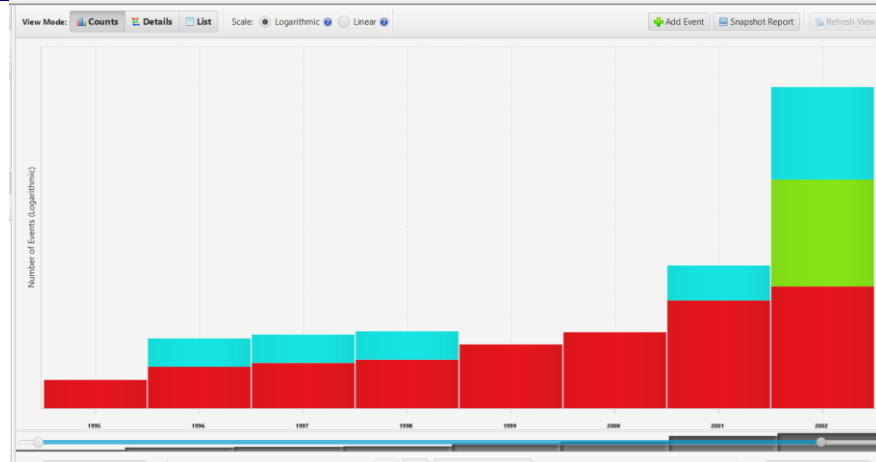


Action	Done?	Date	Time	Notes
				<pre> User Information ----- Username       : Administrator [500] SID            : S-1-5-21-1229272821-1580818891-854245398-500 Full Name      : User Comment    : Built-in account for administering the computer/domain Account Type    : Default Admin User Account Created : Thu Feb 28 15:22:36 2002 Z Name           : Last Login Date : Never Pwd Reset Date  : Never Pwd Fail Date   : Never Login Count     : 0 --&gt; Password does not expire --&gt; 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 --&gt; Password does not expire --&gt; Password not required --&gt; Normal user account  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 --&gt; Password does not expire --&gt; Account Disabled --&gt; Normal user account </pre> <p>3. I can also find the time zone information from the above-exported files <b>config</b> where there is a file name <b>system</b>. where I can find the time zone information by analyzing the <b>system file in reg ripper</b></p>

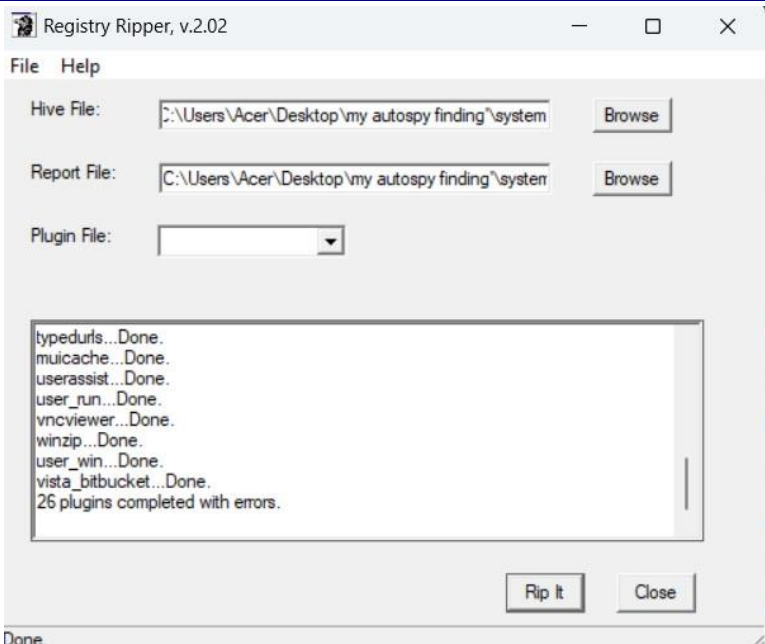
Action	Done?	Date	Time	Notes
				<pre> timezone v.20200518 (System) Get TimeZoneInformation key contents  TimeZoneInformation key ControlSet001\Control\TimeZoneInformation LastWrite Time 2002-04-18 14:33:31Z DaylightName -&gt; Central Daylight Time StandardName -&gt; Central Standard Time Bias -&gt; 360 (6 hours) ActiveTimeBias -&gt; 300 (5 hours) ----- usb v.20200515 </pre> <p>From the daylight name which is Central Daylight Time, I can find out that the time zone is North America so the crime must be happening in North America</p>
<p>Timeline analysis-</p> <p>Note date of last activity on the computer.system profiling</p>	yes	NOV 27 <sup>TH</sup> 2024	12:35 P.M	<p>1. I can find the time analysis at the same file location at the SAM.txt whose converting process has been done on the above, here data of the last activity on the computer are found inside the SAM</p> <p>Last Login Date : Tue Jun 4 23:01:54 2002 Z</p> <pre> 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 --&gt; Password does not expire --&gt; Password not required --&gt; Normal user account </pre>

Action	Done?	Date	Time	Notes
				<p>I also found the last login date of the guest Last Login Date: Mon Jun 3 16:49:37 2002 Z</p> <pre> 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 --&gt; Password does not expire --&gt; Password not required --&gt; Normal user account           </pre> <p>For timeline analysis</p> <p>I can also go through the tool → Run ingest Modules → Hunter Xp → Plaso</p>

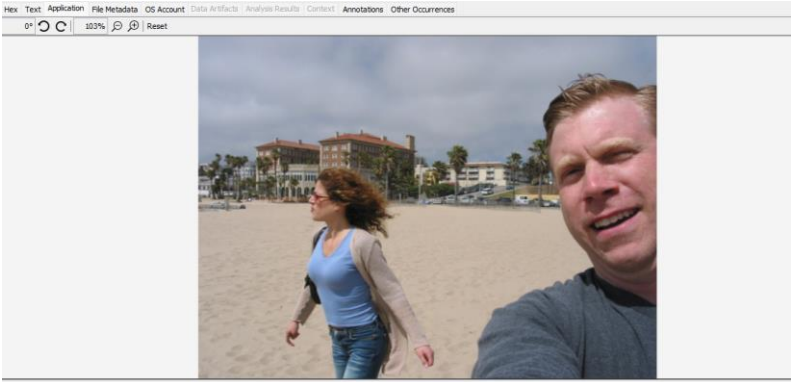


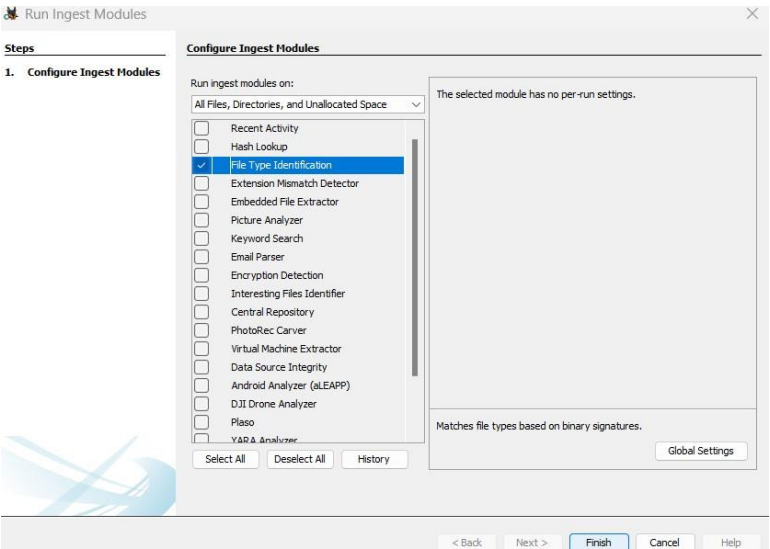
Action	Done?	Date	Time	Notes
				<div></div> <p>After that click on the timeline</p>

Action	Done?	Date	Time	Notes
				 <p>Here I get the details of File System, Web Activity and other at the yearly use</p>
Registry analysis and Registry protected area	yes	NOV 27 <sup>TH</sup> 2024	12:50 P.M	<p>I find the registry analysis and registry-protected area at the location    </p> <p>Here I analyze the file that cannot be opened and copied by the system but can be exported by FTK Imager here I analyze file SAM, System, and others in the reg ripper</p>

Action	Done?	Date	Time	Notes
				
Link files and Recycle Bin	yes	NOV 27 <sup>TH</sup> 2024	1 P.M	<p>1. I found the link files at the location</p> <p>/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Recent/ where I can see all 40 files link</p>

Action	Done?	Date	Time	Notes																																																																																	
				<div><table><tr><td></td><td>0409.Link</td><td></td><td>1</td><td>2002-06-04 23:54:07 GMT</td><td>2002-06-04 23:54:07 GMT</td><td>2002-06-04 23:54:07 GMT</td><td>2002-06-04 23:54:07 GMT</td><td>657</td></tr><tr><td></td><td>101-0174_IMG.JPG.Link</td><td></td><td>1</td><td>2002-06-03 23:19:57 GMT</td><td>2002-06-03 23:19:57 GMT</td><td>2002-06-03 22:45:52 GMT</td><td></td><td>1029</td></tr><tr><td></td><td>101-0184_IMG.JPG.Link</td><td></td><td>1</td><td>2002-06-03 23:25:22 GMT</td><td>2002-06-03 23:25:22 GMT</td><td>2002-06-03 23:25:22 GMT</td><td>2002-06-03 23:25:22 GMT</td><td>1043</td></tr><tr><td></td><td>102-0214_IMG.JPG.Link</td><td></td><td>1</td><td>2002-06-03 22:25:19 GMT</td><td>2002-06-03 22:25:19 GMT</td><td>2002-06-03 22:25:19 GMT</td><td>2002-06-03 22:25:19 GMT</td><td>871</td></tr><tr><td></td><td>102-0250_IMG.JPG.Link</td><td></td><td></td><td>2002-06-03 18:41:56 GMT</td><td>2002-06-03 18:41:56 GMT</td><td>2002-06-03 18:41:56 GMT</td><td>2002-06-03 18:41:56 GMT</td><td>563</td></tr><tr><td></td><td>103-0305_IMG.JPG.Link</td><td></td><td>1</td><td>2002-06-04 23:45:39 GMT</td><td>2002-06-04 23:45:39 GMT</td><td>2002-06-04 23:45:39 GMT</td><td>2002-06-04 23:45:39 GMT</td><td>1029</td></tr><tr><td></td><td>103-0330_IMG.JPG.Link</td><td></td><td>1</td><td>2002-06-03 23:55:43 GMT</td><td>2002-06-03 23:55:43 GMT</td><td>2002-06-03 23:55:43 GMT</td><td>2002-06-03 23:55:43 GMT</td><td>1071</td></tr><tr><td></td><td>103-0356_IMG.JPG.Link</td><td></td><td>1</td><td>2002-06-03 21:22:13 GMT</td><td>2002-06-03 21:22:13 GMT</td><td>2002-06-03 21:22:13 GMT</td><td>2002-06-03 21:22:13 GMT</td><td>563</td></tr><tr><td></td><td>103-0356_IMG.ap.Link</td><td></td><td>1</td><td>2002-06-03 21:24:10 GMT</td><td>2002-06-03 21:24:10 GMT</td><td>2002-06-03 21:24:10 GMT</td><td>2002-06-03 21:24:10 GMT</td><td>533</td></tr></table></div> <div><div>HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences</div><div>StringsIndexed TextTranslation</div><div>Page: 1 of 1 PageMatches on page: - of - Match100%Reset</div><div>MVPIC1-1 My Pictures Bob Hunter HUNTER-1 Hunter Pic CHRIST-1 Christina Detawit 101-01-1.JPG 101-0184_IMG.JPG F:\Documents and Settings\Bob Hunter\My Documents\My Pictures\Hunter Pic\Christina Detawit\101-0184_IMG.JPG J:\My Documents\My Pictures\Hunter Pic\Christina Detawit\101-0184_IMG.JPG[F:\Documents and Settings\Bob Hunter\My Documents\My Pictures\Hunter Pic\Christina Detawit pc&lt;v770kuw75elt</div></div>		0409.Link		1	2002-06-04 23:54:07 GMT	2002-06-04 23:54:07 GMT	2002-06-04 23:54:07 GMT	2002-06-04 23:54:07 GMT	657		101-0174_IMG.JPG.Link		1	2002-06-03 23:19:57 GMT	2002-06-03 23:19:57 GMT	2002-06-03 22:45:52 GMT		1029		101-0184_IMG.JPG.Link		1	2002-06-03 23:25:22 GMT	2002-06-03 23:25:22 GMT	2002-06-03 23:25:22 GMT	2002-06-03 23:25:22 GMT	1043		102-0214_IMG.JPG.Link		1	2002-06-03 22:25:19 GMT	2002-06-03 22:25:19 GMT	2002-06-03 22:25:19 GMT	2002-06-03 22:25:19 GMT	871		102-0250_IMG.JPG.Link			2002-06-03 18:41:56 GMT	2002-06-03 18:41:56 GMT	2002-06-03 18:41:56 GMT	2002-06-03 18:41:56 GMT	563		103-0305_IMG.JPG.Link		1	2002-06-04 23:45:39 GMT	2002-06-04 23:45:39 GMT	2002-06-04 23:45:39 GMT	2002-06-04 23:45:39 GMT	1029		103-0330_IMG.JPG.Link		1	2002-06-03 23:55:43 GMT	2002-06-03 23:55:43 GMT	2002-06-03 23:55:43 GMT	2002-06-03 23:55:43 GMT	1071		103-0356_IMG.JPG.Link		1	2002-06-03 21:22:13 GMT	2002-06-03 21:22:13 GMT	2002-06-03 21:22:13 GMT	2002-06-03 21:22:13 GMT	563		103-0356_IMG.ap.Link		1	2002-06-03 21:24:10 GMT	2002-06-03 21:24:10 GMT	2002-06-03 21:24:10 GMT	2002-06-03 21:24:10 GMT	533
	0409.Link		1	2002-06-04 23:54:07 GMT	2002-06-04 23:54:07 GMT	2002-06-04 23:54:07 GMT	2002-06-04 23:54:07 GMT	657																																																																													
	101-0174_IMG.JPG.Link		1	2002-06-03 23:19:57 GMT	2002-06-03 23:19:57 GMT	2002-06-03 22:45:52 GMT		1029																																																																													
	101-0184_IMG.JPG.Link		1	2002-06-03 23:25:22 GMT	2002-06-03 23:25:22 GMT	2002-06-03 23:25:22 GMT	2002-06-03 23:25:22 GMT	1043																																																																													
	102-0214_IMG.JPG.Link		1	2002-06-03 22:25:19 GMT	2002-06-03 22:25:19 GMT	2002-06-03 22:25:19 GMT	2002-06-03 22:25:19 GMT	871																																																																													
	102-0250_IMG.JPG.Link			2002-06-03 18:41:56 GMT	2002-06-03 18:41:56 GMT	2002-06-03 18:41:56 GMT	2002-06-03 18:41:56 GMT	563																																																																													
	103-0305_IMG.JPG.Link		1	2002-06-04 23:45:39 GMT	2002-06-04 23:45:39 GMT	2002-06-04 23:45:39 GMT	2002-06-04 23:45:39 GMT	1029																																																																													
	103-0330_IMG.JPG.Link		1	2002-06-03 23:55:43 GMT	2002-06-03 23:55:43 GMT	2002-06-03 23:55:43 GMT	2002-06-03 23:55:43 GMT	1071																																																																													
	103-0356_IMG.JPG.Link		1	2002-06-03 21:22:13 GMT	2002-06-03 21:22:13 GMT	2002-06-03 21:22:13 GMT	2002-06-03 21:22:13 GMT	563																																																																													
	103-0356_IMG.ap.Link		1	2002-06-03 21:24:10 GMT	2002-06-03 21:24:10 GMT	2002-06-03 21:24:10 GMT	2002-06-03 21:24:10 GMT	533																																																																													
				<p>2. I found 747 deleted files/images in the recycle bin where there is also an image suspected image captured in the recycle bin</p> <p>At the location:</p> <p>/img_Hunter XP for Dongled</p> <p>v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df826.JPG</p>																																																																																	

Action	Done?	Date	Time	Notes
				<div data-bbox="1142 244 1930 627"></div> <p>As dived deep into the recycle bin I found the conversation between Chaser and Billy at the location:</p> <p><code>/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821- 1580818891-854245398- 1004/Df1040/HunterB/memopad/memopad.bak</code> where they discuss about the family information and discuss about money</p>

Action	Done?	Date	Time	Notes
				<pre> PM#F:Pain\HunterB\memopad\memopad.dat 0 6 0 0 1 000000X Business Business Personal Personal@ +ACL s/name: chaser 1191@aol p/vr: 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 chaser 1191@hotmail.com p/vr: bigjake -Yahoo information bob_hunter 1191 p/vr bigjake JAM Information chaser 1191 p/vr bigjake bX Drive chaser 1191@hotmail.com 1191 http://plus.xdrive.com/IDRequestsDispatcher?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 so d 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. </pre>
Instant Messaging clients	yes	NOV 27 <sup>TH</sup> 22024	1:20 P.M	<p>I found the instant massaging clients by opening the <b>tool</b> and selecting run to <b>ingest module</b> then selecting <b>the file type identification</b> and clicking on finished</p> 

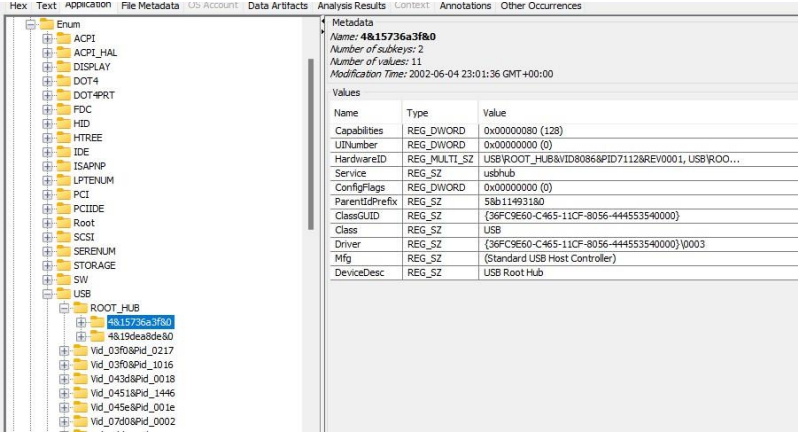
Action	Done?	Date	Time	Notes																																																																																																														
				<p>After that I go to the location</p> <p>/img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/config/software</p> <p>Here I found the two massaging apps used that are</p> <ol style="list-style-type: none"><li>1. Yahoo messenger</li><li>2. AOL instant messenger</li></ol> <div><table><tr><td>software</td><td>1</td><td>Windows XP Home [SP1] [See Q314727 for more information]</td><td>2002-03-31 11:00:17 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>AOL Instant Messenger (SP1)</td><td>2002-03-31 10:37:20 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Java 2 Runtime Environment Standard Edition v1.3</td><td>2002-03-01 09:43:18 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Shockwave</td><td>2002-03-01 09:41:36 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>RealPlayer Basic</td><td>2002-03-01 09:24:53 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>America Online</td><td>2002-03-01 09:24:02 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>WebFlds XP v.9.50.5318</td><td>2002-02-28 16:38:56 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Microsoft NetShow Player 2.0</td><td>2002-02-28 16:38:39 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>MPayer2</td><td>2002-02-28 16:38:39 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Branding</td><td>2002-02-28 16:13:05 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>PCHealth</td><td>2002-02-28 16:07:49 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr></table><div><div>Hex</div><div>Text</div><div>Application</div><div>Source File Metadata</div><div>OS Account</div><div>Data Artifacts</div><div>Analysis Results</div><div>Context</div><div>Annotations</div><div>Other Occurrences</div></div><div>Result: 98 of 121</div><div>Result</div><div>Type</div><div>Value</div><div>Program Name</div><div>AOL Instant Messenger (SP1)</div><div>Date/Time</div><div>2002-03-31 10:37:20 GMT</div><div>Source File Path</div><div>/img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/config/software</div><div>Artifact ID</div><div>-9223372036854669707</div></div> <div><table><tr><td>software</td><td>4</td><td>Windows XP Home [SP1] [See Q314727 for more information]</td><td>2002-03-31 11:00:17 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Yahoo! Messenger Explorer Bar</td><td>2002-05-14 10:37:39 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Yahoo! Messenger</td><td>2002-05-14 10:36:48 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Windows XP Hotfix (SP1) [See Q309521 for more information]</td><td>2002-03-31 11:07:44 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Windows XP Hotfix (SP1) [See Q311889 for more information]</td><td>2002-03-31 11:07:17 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Windows XP Application Compatibility Update[Q313494]</td><td>2002-03-31 11:06:49 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Windows XP Hotfix (SP1) [See Q315000 for more information]</td><td>2002-03-31 11:06:16 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Windows XP Hotfix (SP1) [See Q314862 for more information]</td><td>2002-03-31 11:05:55 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Windows XP Hotfix (SP1) [See Q315403 for more information]</td><td>2002-03-31 11:05:37 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Windows XP Hotfix (SP1) [See Q314147 for more information]</td><td>2002-03-31 11:05:19 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr><tr><td>software</td><td>1</td><td>Windows XP Hotfix (SP1) [See Q317277 for more information]</td><td>2002-03-31 11:03:47 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr></table><div><div>Hex</div><div>Text</div><div>Application</div><div>Source File Metadata</div><div>OS Account</div><div>Data Artifacts</div><div>Analysis Results</div><div>Context</div><div>Annotations</div><div>Other Occurrences</div></div><div>Result: 89 of 121</div><div>Result</div><div>Type</div><div>Value</div><div>Program Name</div><div>Yahoo! Messenger</div><div>Date/Time</div><div>2002-05-14 10:36:48 GMT</div><div>Source File Path</div><div>/img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/config/software</div><div>Artifact ID</div><div>-9223372036854669716</div></div>	software	1	Windows XP Home [SP1] [See Q314727 for more information]	2002-03-31 11:00:17 GMT	Hunter XP for Dongled v6.E01	software	1	AOL Instant Messenger (SP1)	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 09:24:02 GMT	Hunter XP for Dongled v6.E01	software	1	WebFlds 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	MPayer2	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	4	Windows XP Home [SP1] [See Q314727 for more information]	2002-03-31 11:00:17 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[Q313494]	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	Windows XP Home [SP1] [See Q314727 for more information]	2002-03-31 11:00:17 GMT	Hunter XP for Dongled v6.E01																																																																																																														
software	1	AOL Instant Messenger (SP1)	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 09:24:02 GMT	Hunter XP for Dongled v6.E01																																																																																																														
software	1	WebFlds 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	MPayer2	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	4	Windows XP Home [SP1] [See Q314727 for more information]	2002-03-31 11:00:17 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[Q313494]	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																																																																																																														

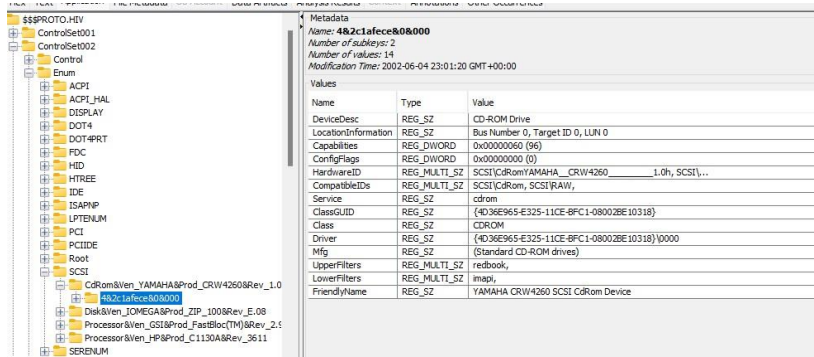
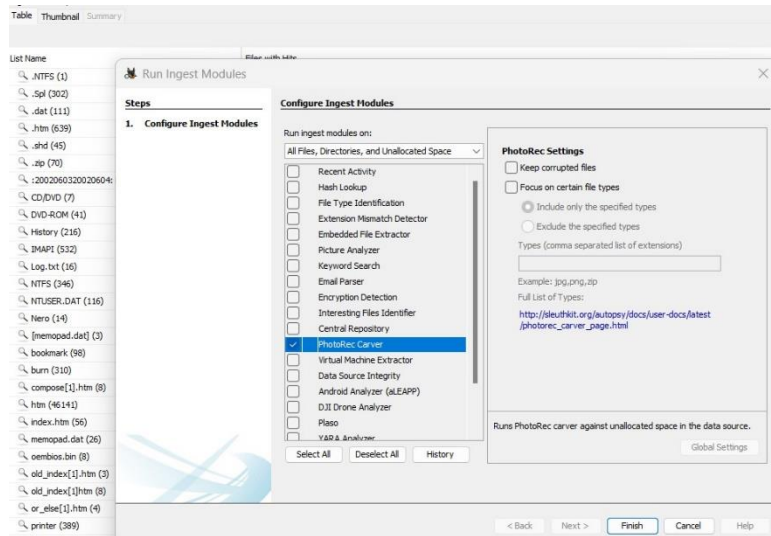
Action	Done?	Date	Time	Notes
Clean-up/Wiping utilities. Check log files. Anything used?	yes	NOV 27 <sup>TH</sup> 2024	1:40P.M	<p>I can find the clean-up/wiping utilities at the location</p> <p><a href="#">/img_Hunter XP for Dongled v6.E01/vol_vol2//\$CarvedFiles/f0003340_BestCrypt_v_7_for_Windows_95_98_ME_NT_2000_XP.html</a></p> <p>Here I found BCWipe software and BestCrypt software and these both software is used for cleaning and wiping the disk</p> <div><div>Listing   Keyword search 1 - erase   Keyword search 2 - BCWipe   X</div><div>Keyword search</div><div>Table   Thumbnail   Summary</div><div><div>Name</div><div>Keyword Preview</div><div>Location</div><div>Modified Time</div><div>Change Time</div><div>Access Time</div><div>Created Time</div><div>Save Table</div></div><div>Hex   Text   Application   File Metadata   OS Account   Data Artifact   Analysis Results   Context   Annotations   Other Occurrences</div><div>Download Images</div><div><div>BCWipe software for Windows 95/98/ME/NT/2000/XP</div><div>Thank you and please have time that view the previous version</div></div><div><p>The BCWipe utility is a shell extender for Windows 95/98/ME/NT/2000/XP, intended to secure delete your files. It supports correspondent U.S. Department of Defense recommendations (DoD 5200.28-STD). The Bt utility provides several ways to shred file's contents from the disk:</p><ul style="list-style-type: none"><li>a. Delete with wiping. Using 'Delete with wiping' command you can delete and wipe your files and folders using pop-up context menus in Windows Shell (Explorer program).</li><li>b. Wipe free disk space. If you have previously deleted sensitive files using a standard operating system command, you may wipe free space on the disk where these files were stored - all previously deleted files' contents will be erased.</li><li>c. Swap file wiping. BCWipe utility automatically wipes Windows Swap file contents when you run 'Wipe free disk space' command.</li><li>d. Recycle Bin wiping. You can wipe contents of Windows Recycle Bin by pointing on the Bin icon by mouse and running the 'Wipe Recycle Bin' command from context pop-up menu.</li><li>e. Windows ME specific: allows to wipe contents of special folders, created by Windows ME 'System Restore' function.</li></ul></div><div><div>What's new and what have been fixed over the previous version</div><div><div>1). 1.07 version is released (30 October, 1997).</div><div>2). 2.0 beta version is released (12 June, 1998).</div></div><div><div>What's new in this beta release:</div><div>a) wiping of file slack is included;</div><div>b) it is possible to look at a content of a file before and after deletion;</div><div>c) the option to turn on/off the wiping procedure is included.</div></div><div><div>3). 2.08b version (4 August, 1998). The problem previously appeared while working with large (over 2 Gb) partitions is solved.</div><div>4). 2.13 version (7 October, 1998). It becomes possible to set a variable number of passes for wiping of data. Beginning from 2.13 release the 2-ad version becomes a standard version of BCWipe.</div><div>5). ZDNet Software Library placed BCWipe v.2.16 to the list of Top Rated Utilities. The 2.16 version of BCWipe (as well as the v.1.07 earlier) is ranked as a 5 stars software. Click here to read review of BCWipe public by ZDNet Software Library. (30 October, 1998)</div><div>6). 2.28 version (28 October, 1999). Problems of hanging BCWipe on NTFS volumes and incorrect wiping of directory entries on compressed volumes are fixed.</div></div></div></div>

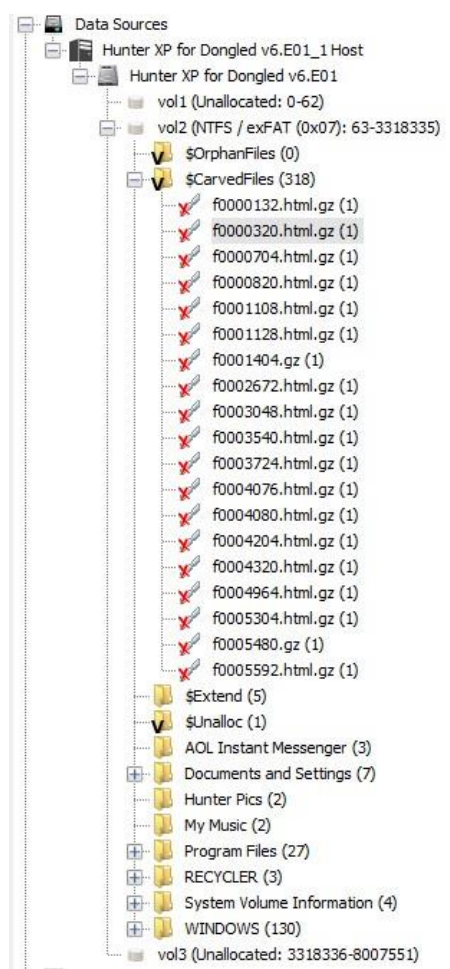


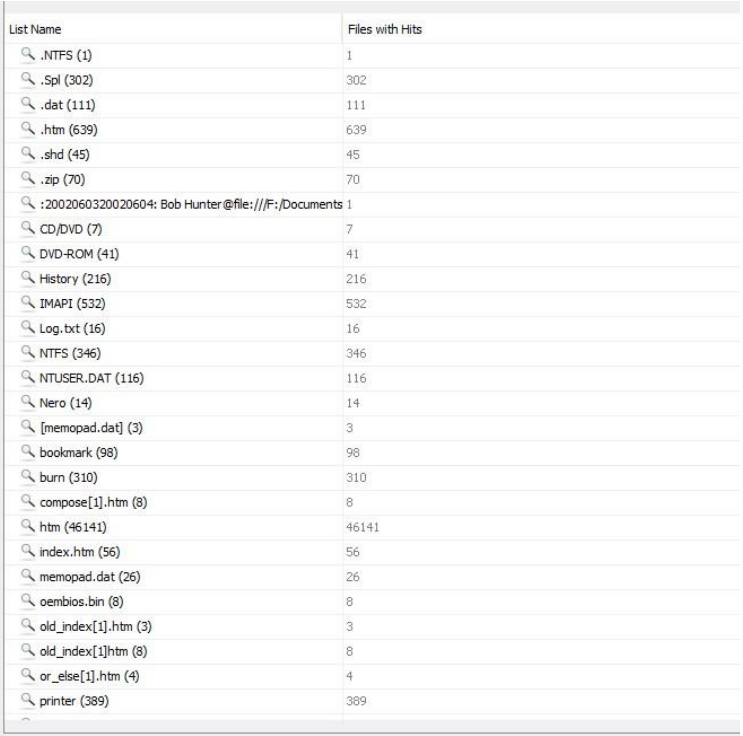
Action	Done?	Date	Time	Notes
				<div><div>HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences</div><div><div>Metadata</div><div><div>Name:/img_Hunter XP for Dongled v6.E01/vol_vol2//%CarvedFiles/R0000568_BCWipe_for_Windows_95_98_ME_NT_2000_XP.html</div><div>Type:Carved</div><div>MIME Type:text/html</div><div>Size:6672</div><div>File Name Allocation:Unallocated</div><div>Metadata Allocation:Unallocated</div><div>Modified:0000-00-00 00:00:00</div><div>Accessed:0000-00-00 00:00:00</div><div>Created:0000-00-00 00:00:00</div><div>Changed:0000-00-00 00:00:00</div><div>MD5:7bd4d1650d3b527c6f98cfd370b4062a</div><div>SHA-256:9f2a1b4eb2331b47761387e37c438ac34830336bdc2617605dc579e926dab19d</div><div>Hash Lookup Results:UNKNOWN</div><div>Internal ID:27701</div></div></div></div>
External drives; Network connections	yes	NOV 27 <sup>TH</sup> 2024	2 P.M	<p>1.i can find out the network connection details/information at the location:</p> <div><div>/img_Hunter XP for Dongled</div><div>v6.E01/vol_vol2/WINDOWS/system32/drivers/etc/net</div><div>works</div></div>

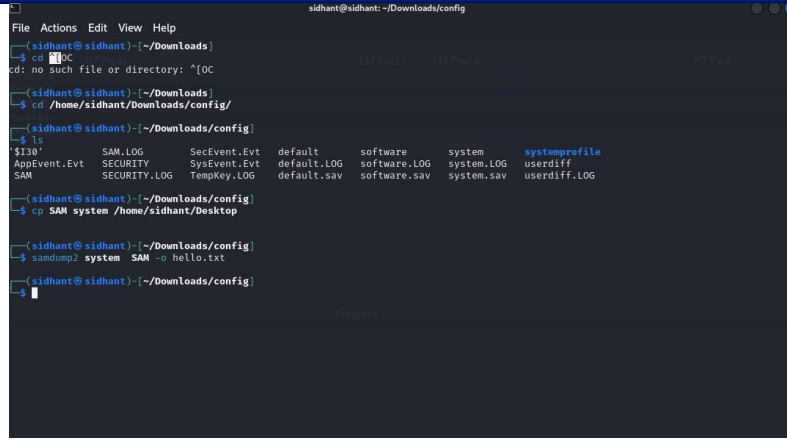
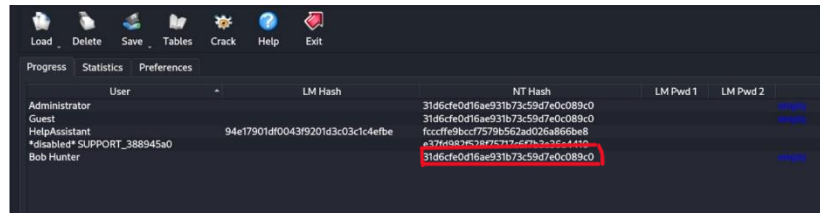
Action	Done?	Date	Time	Notes																																	
				<div><div><div>HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences</div><div>StringsIndexed TextTranslation</div><div>Page: 1 of 1 PageMatches on page: - of - Match100%Reset</div><div># Copyright (c) 1993-1999 Microsoft Corp. # # This file contains network name/network number mappings for # local networks. Network numbers are recognized in dotted decimal form. # # Format: # # &lt;network name&gt; &lt;network number&gt; [aliases...] [#&lt;comment&gt;] # # For example: # # loopback 127 # campus 284.122.107 # london 284.122.108  loopback 127  -----METADATA-----</div></div></div> <p>I can find the information about the external drives at the location</p> <p>Hunterxp/Partion1/Noname/root/windows/system32/control2set/enum/Scsi , in this image Microsoft USB IntelliMouse Explorer is connected externally.</p> <div><div><div>HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences</div><div><div>Drum</div><div>ACPI</div><div>ACPI_HAL</div><div>DISPLAY</div><div>DOT4</div><div>DOT4PRINT</div><div>PDC</div><div>HID</div><div>Vol_04fe5bPd_001e</div><div>045c73c7f7808000</div><div>Device Parameters</div><div>LogConf</div><div>Capabilities</div><div>HardwareID</div><div>CompatibleIDs</div><div>Service</div><div>ClassGUID</div><div>ConfigFlags</div><div>Driver</div><div>Class</div><div>MFg</div><div>DeviceDesc</div><div>HTREE</div><div>IDE</div><div>ISAPNP</div><div>LPTENUM</div><div>PCI</div><div>PCIDE</div><div>Root</div><div>Scsi</div></div><div><div>Metadata</div><div>Name: 045c73c7f7808000</div><div>Number of subkeys: 2</div><div>Number of values: 10</div><div>Modification Time: 2002-06-04 23:01:37 GMT+00:00</div><div>Values</div><div><table><tr><th>Name</th><th>Type</th><th>Value</th></tr><tr><td>Capabilities</td><td>REG_DWORD</td><td>0x000000a0 (160)</td></tr><tr><td>HardwareID</td><td>REG_MULTI_SZ</td><td>HID/Vid_045e8Pd_001e8Rev_0114_HID/Vid_045e8...</td></tr><tr><td>CompatibleIDs</td><td>REG_MULTI_SZ</td><td>.</td></tr><tr><td>Service</td><td>REG_SZ</td><td>mousehid</td></tr><tr><td>ClassGUID</td><td>REG_SZ</td><td>{4D36E96F-E325-11CE-BFC1-08002BE10318}</td></tr><tr><td>ConfigFlags</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td>Driver</td><td>REG_SZ</td><td>{4D36E96F-E325-11CE-BFC1-08002BE10318}0000</td></tr><tr><td>Class</td><td>REG_SZ</td><td>Mouse</td></tr><tr><td>Mfg</td><td>REG_SZ</td><td>Microsoft</td></tr><tr><td>DeviceDesc</td><td>REG_SZ</td><td>Microsoft USB IntelliMouse Explorer</td></tr></table></div></div></div></div>	Name	Type	Value	Capabilities	REG_DWORD	0x000000a0 (160)	HardwareID	REG_MULTI_SZ	HID/Vid_045e8Pd_001e8Rev_0114_HID/Vid_045e8...	CompatibleIDs	REG_MULTI_SZ	.	Service	REG_SZ	mousehid	ClassGUID	REG_SZ	{4D36E96F-E325-11CE-BFC1-08002BE10318}	ConfigFlags	REG_DWORD	0x00000000 (0)	Driver	REG_SZ	{4D36E96F-E325-11CE-BFC1-08002BE10318}0000	Class	REG_SZ	Mouse	Mfg	REG_SZ	Microsoft	DeviceDesc	REG_SZ	Microsoft USB IntelliMouse Explorer
	Name	Type	Value																																		
Capabilities	REG_DWORD	0x000000a0 (160)																																			
HardwareID	REG_MULTI_SZ	HID/Vid_045e8Pd_001e8Rev_0114_HID/Vid_045e8...																																			
CompatibleIDs	REG_MULTI_SZ	.																																			
Service	REG_SZ	mousehid																																			
ClassGUID	REG_SZ	{4D36E96F-E325-11CE-BFC1-08002BE10318}																																			
ConfigFlags	REG_DWORD	0x00000000 (0)																																			
Driver	REG_SZ	{4D36E96F-E325-11CE-BFC1-08002BE10318}0000																																			
Class	REG_SZ	Mouse																																			
Mfg	REG_SZ	Microsoft																																			
DeviceDesc	REG_SZ	Microsoft USB IntelliMouse Explorer																																			

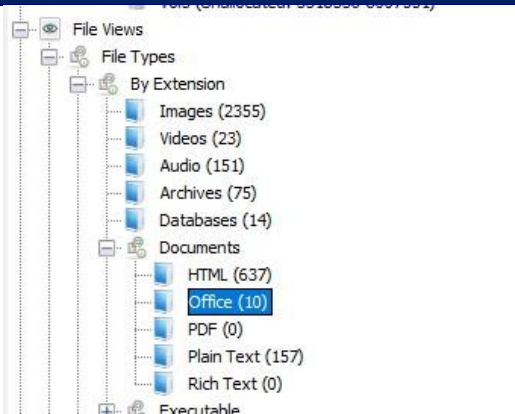
Action	Done?	Date	Time	Notes
				<p>I also found other external drives connected at the LOCATION: <b>Hunterxp/Partion1/Noname/root/windows/system32/control2set/enum/HID</b> which is USB root Hub</p>  <p>I also found the other external drives at the LOCATION: <b>Hunterxp/Partion1/Noname/root/windows/system32/control2set/enum/USB</b> which is a CD-ROM Drive</p>

Action	Done?	Date	Time	Notes
				
Perform data carving	yes	NOV 27 <sup>TH</sup> 2024	2:20P.M	<p>1. perform data carving to find deleted files that need to be recovered and also unallocated space needs to be analyzed for hidden or residual data. I find it by going to the tool opening run ingest module and then selecting Photorec carver</p>  <p>Then go to the location</p>

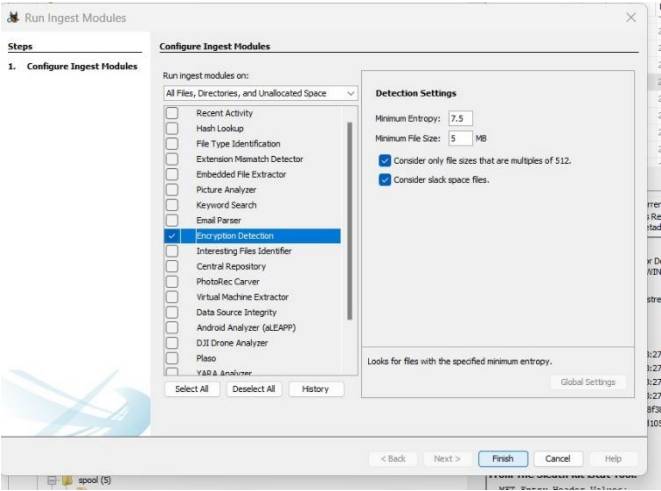
Action	Done?	Date	Time	Notes
				 <p>Here I can see all the deleted files</p>






















Action	Done?	Date	Time	Notes
Run relevant keyword searches; Did you index the evidence file?	yes	NOV 27 <sup>TH</sup> 2024	2:40 P.M	<p>I searched for relevant keywords to find the exact evidence file for Hunter that is mention in the screenshot</p>  <p>From this search, I found the details of the conversation between the father and chaser in the file “old_index[1].htm”</p>
Recover Log-on passwords – use SAMInside/Ophcrack/Encase	yes	NOV 27 <sup>TH</sup> 2024	3:10 P.M	<p>To recover the log-on password I used the tool ophcrack in Linux. For this, I exported the config file from Windows to Linux where I used samdump2 to analyze it.</p>

Action	Done?	Date	Time	Notes
				 <p>After doing this I put the output file which I get by using the command <b>samdump2 system SAM -o</b> and save it by name hello.txt and put the file hello.txt in ophcrack where the file analyzed and I get the result</p>  <p>From this hash value of Bob Hunter its proved that there is no login password</p>
<p>Examine different file types:</p> <p>Export doc/office and exe files; look at Metadata if required</p>	yes	NOV 27 <sup>TH</sup> 2024	3:30 P.M	<p>I found doc/office files by going to <b>files views</b> and opening it and then selecting <b>files types</b> after that select by <b>extension</b> here you will see a <b>document</b> folder open it and click on <b>office</b> here we see all the doc/office files</p>

Action	Done?	Date	Time	Notes																																																																						
				<div></div> <p>Here I can see all the file types used that are doc, ppt, xls and the</p> <p>File Metadata</p> <div><table><tr><th>Name</th><th>S</th><th>C</th><th>O</th><th>Modified Time</th><th>Change Time</th><th>Access Time</th><th>Created Time</th><th>Size</th><th>Flags/D</th></tr><tr><td>winword.doc</td><td></td><td></td><td>2</td><td>2001-08-23 12:00:00 GMT</td><td>2002-02-28 21:44:55 GMT</td><td>2002-02-28 21:44:55 GMT</td><td>2002-02-28 21:44:55 GMT</td><td>4608</td><td>Allocates</td></tr><tr><td>winword.doc</td><td></td><td></td><td>2</td><td>2001-08-23 12:00:00 GMT</td><td>2002-02-28 22:02:39 GMT</td><td>2002-02-28 22:02:39 GMT</td><td>2002-02-28 22:02:39 GMT</td><td>4608</td><td>Allocates</td></tr><tr><td>winword2.doc</td><td></td><td></td><td>2</td><td>2001-08-23 12:00:00 GMT</td><td>2002-02-28 21:44:55 GMT</td><td>2002-02-28 21:44:55 GMT</td><td>2002-02-28 21:44:55 GMT</td><td>1769</td><td>Allocates</td></tr><tr><td>winword2.doc</td><td></td><td></td><td>2</td><td>2001-08-23 12:00:00 GMT</td><td>2002-02-28 22:02:39 GMT</td><td>2002-02-28 22:02:39 GMT</td><td>2002-02-28 22:02:39 GMT</td><td>1769</td><td>Allocates</td></tr><tr><td>excel.xls</td><td></td><td></td><td>2</td><td>2001-08-23 12:00:00 GMT</td><td>2002-02-28 21:44:54 GMT</td><td>2002-02-28 21:44:54 GMT</td><td>2002-02-28 21:44:54 GMT</td><td>5632</td><td>Allocates</td></tr><tr><td>excel.xls</td><td></td><td></td><td>2</td><td>2001-08-23 12:00:00 GMT</td><td>2002-02-28 22:02:39 GMT</td><td>2002-02-28 22:02:39 GMT</td><td>2002-02-28 22:02:39 GMT</td><td>5632</td><td>Allocates</td></tr></table><div><div>Hex</div><div>Text</div><div>Application</div><div>File Metadata</div><div>OS Account</div><div>Data Artifacts</div><div>Analysis Results</div><div>Context</div><div>Annotations</div><div>Other Occurrences</div></div><div><b>Metadata</b> Name: /img_hunter XP for Dongled v6.ED1/vol2/WINDOWS/system32/config/systemprofile/Template/excel.xls Type: File System MIME Type: application/vnd.ms-excel Size: 5632 File Name Allocation: Allocated Metadata Allocation: Allocated Modified: 2001-08-23 12:00:00 GMT Accessed: 2002-02-28 22:02:38 GMT Created: 2002-02-28 22:02:38 GMT Changed: 2002-02-28 22:02:39 GMT MD5: 8c485fa7aae7091b4c720079bee3088 SHA-256: 3ee03bc99613c157c8b561c0f0e6f308d965b0be047294d45c37740452b76d Hash Lookup Results: UNKNOWN Internal ID: 14517  <b>From The Sleuth Kit Istat Tool:</b> NTFS Entry Header Values: Entry: 6115 Sequence: 1 LogFile Sequence Number: 18996176 Allocated File Links: 1  STANDARD_INFORMATION Attribute Values: Flags: Archive Owner ID: 0 Security ID: 307 (S-1-5-32-544) Created: 2002-03-01 03:47:39.721100000 (Nepal Standard Time) File Modified: 2001-08-23 17:46:00.000000000 (Nepal Standard Time) File Modified: 2002-03-01 03:47:39.472348800 (Nepal Standard Time) Accessed: 2002-03-01 03:47:39.991412000 (Nepal Standard Time)</div></div>	Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags/D	winword.doc			2	2001-08-23 12:00:00 GMT	2002-02-28 21:44:55 GMT	2002-02-28 21:44:55 GMT	2002-02-28 21:44:55 GMT	4608	Allocates	winword.doc			2	2001-08-23 12:00:00 GMT	2002-02-28 22:02:39 GMT	2002-02-28 22:02:39 GMT	2002-02-28 22:02:39 GMT	4608	Allocates	winword2.doc			2	2001-08-23 12:00:00 GMT	2002-02-28 21:44:55 GMT	2002-02-28 21:44:55 GMT	2002-02-28 21:44:55 GMT	1769	Allocates	winword2.doc			2	2001-08-23 12:00:00 GMT	2002-02-28 22:02:39 GMT	2002-02-28 22:02:39 GMT	2002-02-28 22:02:39 GMT	1769	Allocates	excel.xls			2	2001-08-23 12:00:00 GMT	2002-02-28 21:44:54 GMT	2002-02-28 21:44:54 GMT	2002-02-28 21:44:54 GMT	5632	Allocates	excel.xls			2	2001-08-23 12:00:00 GMT	2002-02-28 22:02:39 GMT	2002-02-28 22:02:39 GMT	2002-02-28 22:02:39 GMT	5632	Allocates
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags/D																																																																	
winword.doc			2	2001-08-23 12:00:00 GMT	2002-02-28 21:44:55 GMT	2002-02-28 21:44:55 GMT	2002-02-28 21:44:55 GMT	4608	Allocates																																																																	
winword.doc			2	2001-08-23 12:00:00 GMT	2002-02-28 22:02:39 GMT	2002-02-28 22:02:39 GMT	2002-02-28 22:02:39 GMT	4608	Allocates																																																																	
winword2.doc			2	2001-08-23 12:00:00 GMT	2002-02-28 21:44:55 GMT	2002-02-28 21:44:55 GMT	2002-02-28 21:44:55 GMT	1769	Allocates																																																																	
winword2.doc			2	2001-08-23 12:00:00 GMT	2002-02-28 22:02:39 GMT	2002-02-28 22:02:39 GMT	2002-02-28 22:02:39 GMT	1769	Allocates																																																																	
excel.xls			2	2001-08-23 12:00:00 GMT	2002-02-28 21:44:54 GMT	2002-02-28 21:44:54 GMT	2002-02-28 21:44:54 GMT	5632	Allocates																																																																	
excel.xls			2	2001-08-23 12:00:00 GMT	2002-02-28 22:02:39 GMT	2002-02-28 22:02:39 GMT	2002-02-28 22:02:39 GMT	5632	Allocates																																																																	



Action	Done?	Date	Time	Notes
Encryption, Steganalysis (any indications? Entropy or Autopsy can be used)	yes	NOV 27 <sup>TH</sup> 2024	4:10 P.M	<p>1 I can find the encryption by going to the <b>tool</b> and then <b>selecting run ingest modules</b> and then selecting <b>Encryption detection</b> and then select <b>Finished</b></p>  <p>After that I go to the location <b>/img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/oembios.bin</b> where I can found the Files with <b>suspected encryption due to high entropy</b></p>

Action	Done?	Date	Time	Notes																																																																																
				<div><table><tr><th>Source Name</th><th>S</th><th>C</th><th>O</th><th>Source Type</th><th>Score</th><th>Conclusion</th><th>Configuration</th><th>Justification</th><th>Comment</th></tr><tr><td> sembios.bin</td><td>1</td><td></td><td></td><td>File</td><td>Likely Notable</td><td></td><td></td><td>Suspected encryption due to high entropy (7.999980).</td><td>Suspected encryption due to high entropy (7.999980).</td></tr><tr><td> sembios.bin</td><td>1</td><td></td><td></td><td>File</td><td>Likely Notable</td><td></td><td></td><td>Suspected encryption due to high entropy (7.999980).</td><td>Suspected encryption due to high entropy (7.999980).</td></tr><tr><td> sembios.bin</td><td>1</td><td></td><td></td><td>File</td><td>Likely Notable</td><td></td><td></td><td>Suspected encryption due to high entropy (7.999980).</td><td>Suspected encryption due to high entropy (7.999980).</td></tr><tr><td> sembios.bin</td><td>1</td><td></td><td></td><td>File</td><td>Likely Notable</td><td></td><td></td><td>Suspected encryption due to high entropy (7.999980).</td><td>Suspected encryption due to high entropy (7.999980).</td></tr><tr><td> sembios.bin</td><td>1</td><td></td><td></td><td>File</td><td>Likely Notable</td><td></td><td></td><td>Suspected encryption due to high entropy (7.999980).</td><td>Suspected encryption due to high entropy (7.999980).</td></tr><tr><td> sembios.bin</td><td>1</td><td></td><td></td><td>File</td><td>Likely Notable</td><td></td><td></td><td>Suspected encryption due to high entropy (7.999980).</td><td>Suspected encryption due to high entropy (7.999980).</td></tr><tr><td> sembios.bin</td><td>1</td><td></td><td></td><td>File</td><td>Likely Notable</td><td></td><td></td><td>Suspected encryption due to high entropy (7.999980).</td><td>Suspected encryption due to high entropy (7.999980).</td></tr></table></div> <div><div>HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences</div><div><div>Metadata</div><div><div>Name:</div><div>/img_hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/sembios.bin</div></div><div><div>Type:</div><div>File System</div></div><div><div>MIME Type:</div><div>application/octet-stream</div></div><div><div>Size:</div><div>1107200</div></div><div><div>File Name Allocation:</div><div>Allocated</div></div><div><div>Metadata Allocation:</div><div>Allocated</div></div><div><div>Modified:</div><div>2001-08-23 12:00:00 GMT</div></div><div><div>Accessed:</div><div>2002-02-28 22:00:00 GMT</div></div><div><div>Created:</div><div>2001-08-23 12:00:00 GMT</div></div><div><div>Changed:</div><div>2002-02-28 18:28:27 GMT</div></div><div><div>NDS:</div><div>6d3dd10d899aed5daf6a1a3ef978fd</div></div><div><div>SHA-256:</div><div>f6347aec3e072c46f92a2c537401c2a63c2d39fcb2ae405c45f25008474</div></div><div><div>Hash Lookup Results:</div><div>UNMATCHED</div></div><div><div>Internal ID:</div><div>17136</div></div></div><div><div>From The Sleuth Kit Inet Tool:</div><div><div>MFT Entry Header Values:</div><div><div>Entry:</div><div>1514 Sequence: 1</div></div><div><div>\$logFile Sequence Number:</div><div>18063499</div></div><div><div>Allocated File</div></div><div><div>Links:</div><div>1</div></div></div><div><div>STANDARD_INFORMATION Attribute Values:</div><div><div>Flags:</div><div>Archive</div></div><div><div>Owner ID:</div><div>0</div></div><div><div>Security ID:</div><div>273 (8-1-6-32-444)</div></div><div><div>Created:</div><div>2001-08-23 17:48:00.000000000 (Regal Standard Time)</div></div><div><div>File Modified:</div><div>2001-08-23 17:48:00.000000000 (Regal Standard Time)</div></div></div></div></div>	Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment	 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).	 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).	 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).	 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).	 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).	 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).	 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).
Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment																																																																											
 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).																																																																											
 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).																																																																											
 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).																																																																											
 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).																																																																											
 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).																																																																											
 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).																																																																											
 sembios.bin	1			File	Likely Notable			Suspected encryption due to high entropy (7.999980).	Suspected encryption due to high entropy (7.999980).																																																																											
Print artefacts	yes	NOV 27 <sup>TH</sup> 2024	4:35 P.M	<p>1. I find the print artifacts at the location</p> <p><b>/img_hunter XP for Dongled</b> <b>v6.E01/vol_vol2/WINDOWS/system32/spool/PRINTERS/</b></p> <p>Here I can see that there is two types of printer used. The name of the printer is <b>Lexmark Z52 Color Jetprinter</b> and the <b>HP LaserJet 2200 Series PCL</b></p>																																																																																

Action	Done?	Date	Time	Notes																																																																																
				<div><div><div>TableThumbnailSummary</div><table><tr><th>Name</th><th>S</th><th>C</th><th>O</th><th>Modified Time</th><th>Change Time</th><th>Access Time</th><th>Created</th></tr><tr><td>[parent folder]</td><td></td><td></td><td></td><td>2002-02-28 21:42:15 GMT</td><td>2002-02-28 21:42:15 GMT</td><td>2002-06-04 23:01:27 GMT</td><td>2002-02-28 21:42:15 GMT</td></tr><tr><td>00002.SHD</td><td>▼</td><td></td><td>1</td><td>2002-06-04 23:32:58 GMT</td><td>2002-06-04 23:32:58 GMT</td><td>2002-06-04 23:32:58 GMT</td><td>2002-06-04 23:32:58 GMT</td></tr><tr><td>00002.SPL</td><td>▼</td><td></td><td>1</td><td>2002-06-04 23:32:57 GMT</td><td>2002-06-04 23:32:57 GMT</td><td>2002-06-04 23:32:29 GMT</td><td>2002-06-04 23:32:57 GMT</td></tr><tr><td>00003.SHD</td><td>▼</td><td></td><td>1</td><td>2002-06-04 23:33:27 GMT</td><td>2002-06-04 23:33:27 GMT</td><td>2002-06-04 23:33:27 GMT</td><td>2002-06-04 23:33:27 GMT</td></tr><tr><td>00003.SPL</td><td>▼</td><td></td><td>1</td><td>2002-06-04 23:33:27 GMT</td><td>2002-06-04 23:33:27 GMT</td><td>2002-06-04 23:33:25 GMT</td><td>2002-06-04 23:33:27 GMT</td></tr><tr><td>00004.SHD</td><td>▼</td><td></td><td>1</td><td>2002-06-04 23:34:10 GMT</td><td>2002-06-04 23:34:10 GMT</td><td>2002-06-04 23:34:10 GMT</td><td>2002-06-04 23:34:10 GMT</td></tr><tr><td>00004.SPL</td><td>▼</td><td></td><td>1</td><td>2002-06-04 23:34:10 GMT</td><td>2002-06-04 23:34:10 GMT</td><td>2002-06-04 23:33:57 GMT</td><td>2002-06-04 23:34:10 GMT</td></tr><tr><td>00005.SHD</td><td>▼</td><td></td><td>1</td><td>2002-06-04 23:35:29 GMT</td><td>2002-06-04 23:35:29 GMT</td><td>2002-06-04 23:35:29 GMT</td><td>2002-06-04 23:35:29 GMT</td></tr><tr><td>00005.SPL</td><td>▼</td><td></td><td>1</td><td>2002-06-04 23:35:29 GMT</td><td>2002-06-04 23:35:29 GMT</td><td>2002-06-04 23:35:27 GMT</td><td>2002-06-04 23:35:29 GMT</td></tr></table></div><div><div>HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences</div><div><div>Metadata</div><div><div>Name:</div><div>/img_Hunter XP for Dongled v6.E01\vol2\WINDOWS\system32\spool\PRINTERS\00003.SHD</div></div><div><div>Type:</div><div>File System</div></div><div><div>MIME Type:</div><div>application/octet-stream</div></div><div><div>Size:</div><div>1332</div></div><div><div>File Name Allocation:</div><div>Allocated</div></div><div><div>Metadata Allocation:</div><div>Allocated</div></div><div><div>Modified:</div><div>2002-06-04 23:33:27 GMT</div></div><div><div>Accessed:</div><div>2002-06-04 23:33:27 GMT</div></div><div><div>Created:</div><div>2002-06-04 23:33:27 GMT</div></div><div><div>Changed:</div><div>2002-06-04 23:33:27 GMT</div></div><div><div>MD5:</div><div>0bdd8a093e6d978f387c2be6054992e6</div></div><div><div>SHA-256:</div><div>11b622f256abc7d105baf29e4f467561b6e7f107d2f17b72a829f30b7e403a1</div></div><div><div>Hash Lookup Results:</div><div>UNKNOWN</div></div><div><div>Internal ID:</div><div>17476</div></div></div><div><div>From The Sleuth Kit istat Tool:</div><div><div>MFT Entry Header Values:</div><div>Entry: 9925 Sequence: 13</div><div>\$LogFile Sequence Number: 84583383</div><div>Allocated File</div><div>Links: 1</div><div>\$STANDARD_INFORMATION Attribute Values:</div><div>Flags: Archive</div><div>Owner ID: 0</div><div>Security ID: 367 (S-1-5-32-544)</div><div>Created: 2002-06-05 05:18:27.722360000 (Nepal Standard Time)</div><div>\$File Modified: 2002-06-05 05:18:27.722360000 (Nepal Standard Time)</div></div></div></div></div>	Name	S	C	O	Modified Time	Change Time	Access Time	Created	[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 21:42:15 GMT	00002.SHD	▼		1	2002-06-04 23:32:58 GMT	2002-06-04 23:32:58 GMT	2002-06-04 23:32:58 GMT	2002-06-04 23:32:58 GMT	00002.SPL	▼		1	2002-06-04 23:32:57 GMT	2002-06-04 23:32:57 GMT	2002-06-04 23:32:29 GMT	2002-06-04 23:32:57 GMT	00003.SHD	▼		1	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	00003.SPL	▼		1	2002-06-04 23:33:27 GMT	2002-06-04 23:33:27 GMT	2002-06-04 23:33:25 GMT	2002-06-04 23:33:27 GMT	00004.SHD	▼		1	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	00004.SPL	▼		1	2002-06-04 23:34:10 GMT	2002-06-04 23:34:10 GMT	2002-06-04 23:33:57 GMT	2002-06-04 23:34:10 GMT	00005.SHD	▼		1	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	00005.SPL	▼		1	2002-06-04 23:35:29 GMT	2002-06-04 23:35:29 GMT	2002-06-04 23:35:27 GMT	2002-06-04 23:35:29 GMT
Name	S	C	O	Modified Time	Change Time	Access Time	Created																																																																													
[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 21:42:15 GMT																																																																													
00002.SHD	▼		1	2002-06-04 23:32:58 GMT	2002-06-04 23:32:58 GMT	2002-06-04 23:32:58 GMT	2002-06-04 23:32:58 GMT																																																																													
00002.SPL	▼		1	2002-06-04 23:32:57 GMT	2002-06-04 23:32:57 GMT	2002-06-04 23:32:29 GMT	2002-06-04 23:32:57 GMT																																																																													
00003.SHD	▼		1	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																																																																													
00003.SPL	▼		1	2002-06-04 23:33:27 GMT	2002-06-04 23:33:27 GMT	2002-06-04 23:33:25 GMT	2002-06-04 23:33:27 GMT																																																																													
00004.SHD	▼		1	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																																																																													
00004.SPL	▼		1	2002-06-04 23:34:10 GMT	2002-06-04 23:34:10 GMT	2002-06-04 23:33:57 GMT	2002-06-04 23:34:10 GMT																																																																													
00005.SHD	▼		1	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																																																																													
00005.SPL	▼		1	2002-06-04 23:35:29 GMT	2002-06-04 23:35:29 GMT	2002-06-04 23:35:27 GMT	2002-06-04 23:35:29 GMT																																																																													

Here I can also see that there is two types of files SHD and SPL.

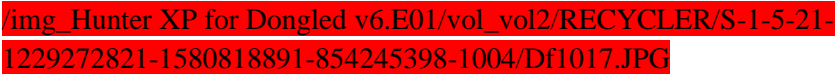
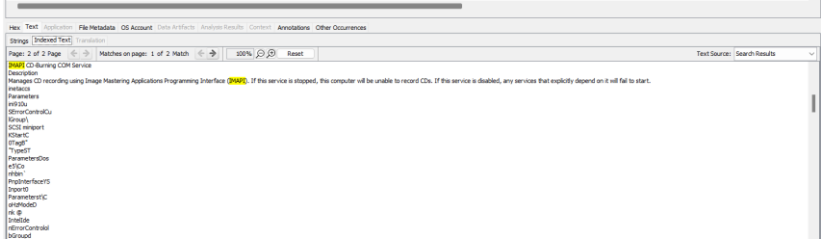
SPL files Contain the raw print job data, including text, images, and formatting.

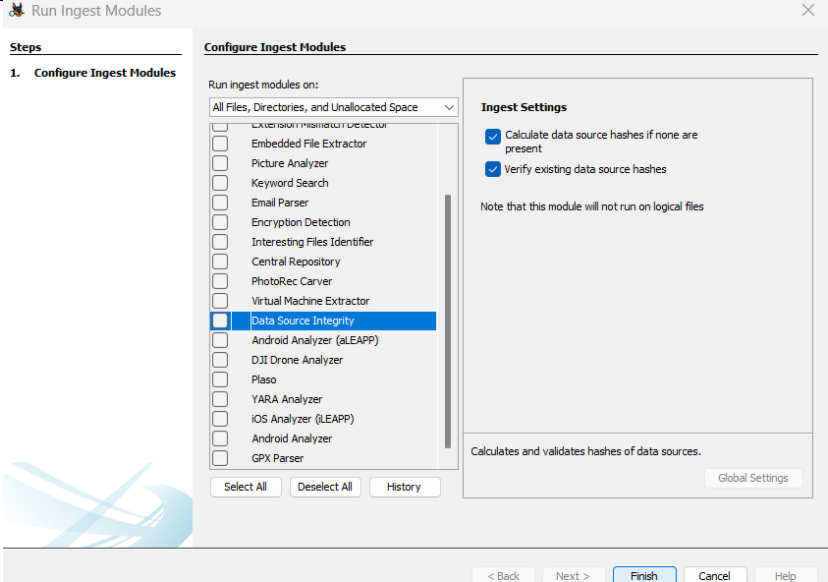
SHD files store metadata about the print job, such as job details and user information.

Here I can also see that there is two types of files SHD and SPL.

SPL files Contain the raw print job data, including text, images, and formatting.

SHD files store metadata about the print job, such as job details and user information.

Action	Done?	Date	Time	Notes
CD/DVD burning apps; check log files	yes	NOV 27 <sup>TH</sup> 2024	4:45 P.M	<p>I found the information and the app of CD/DVD burning at the location  </p> <p>Here I found the IMAPI It is a Microsoft API that provides developers with the ability to create applications capable of writing data to optical discs such as CDs, DVDs, and Blu-rays. It is not specifically designed for forensics but can be used to create accurate disc images or burn data for preservation or analysis.</p> 
Validate evidence integrity at the end of the examination	yes	NOV 27 <sup>TH</sup> 2024	5:20 P.M	<p>1.for the validation of evidence integrity.</p> <p>Tools→ Run ingest modules → Hunter Xp→Data Sources integrity</p>

Action	Done?	Date	Time	Notes
				 <p>Here I find the details on email box which is located at the right sside corner</p>

Action	Done?	Date	Time	Notes												
				<div><div><div><div>DiscoveryGenerate ReportClose Case</div><div><div>19</div></div></div><div>Listing</div><div>Hunter XP for Dongled v6.E01 Host</div><div>TableThumbnailSummary</div><div>Save Table as CSV</div><table><tr><th>Name</th><th>Type</th><th>Size (Bytes)</th><th>Sector Size (Bytes)</th><th>Timezone</th><th>Device ID</th></tr><tr><td>Hunter XP for Dongled v6.E01</td><td>Image</td><td>409900624</td><td>512</td><td>GMT</td><td>306970db-4c8f-45c4-99d4-07ee68955305</td></tr></table><div><div>Module</div><div>Num</div><div>Hex?</div><div>Subject</div><div>Timestamp</div></div><div><div>Data Source Integrity</div><div>1</div><div></div><div>Starting Hunter XP for Dongled v6.E01</div><div>2024/12/16 17:...</div></div><div><div>Data Source Integrity</div><div>1</div><div></div><div>Integrity of Hunter XP for Dongled v6.E01 verified.</div><div>2024/12/16 17:...</div></div><div>Here</div><div>Meta</div><div>Hex</div><div>Tag</div><div>Size</div><div>MD5</div><div>SHA</div><div>Sec</div><div>Time</div><div>Acc</div><div>Sort By: Time</div><div>Total: 2</div><div>Unique: 2</div><div>Acquire Operating System: Windows XP</div><div>Acquire Software Version: FPG2.4</div><div>Path: W:\...</div></div></div> <div>By clicking in it I can verify that my data integrity is maintained by checking the hash</div> <div><div><div>Go to ResultGo to Directory</div><div>Data Source Verification Results for Hunter XP for Dongled v6.E01</div><div>Result: verified</div><div>MD5 hash verified</div><div>Calculated hash: dfcfe9ab9a60c6ad4a314656b687226b</div><div>Stored hash: dfcfe9ab9a60c6ad4a314656b687226b</div></div></div>	Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID	Hunter XP for Dongled v6.E01	Image	409900624	512	GMT	306970db-4c8f-45c4-99d4-07ee68955305
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID											
Hunter XP for Dongled v6.E01	Image	409900624	512	GMT	306970db-4c8f-45c4-99d4-07ee68955305											

**Additional Notes/Artefacts Examined:**


Colour-coding Legend	Tasks
	Fundamental
	Basic
	Elementary
	Secondary
	Advanced
	Exceptional