

## **Contemporaneous Notes**

### **Computer Crime and Digital Evidence**



#### **Submitted by**

Name: Ajaj Ahmed

Cyber Security and Digital Forensics

Kathmandu, Nepal

Dec 24, 2024

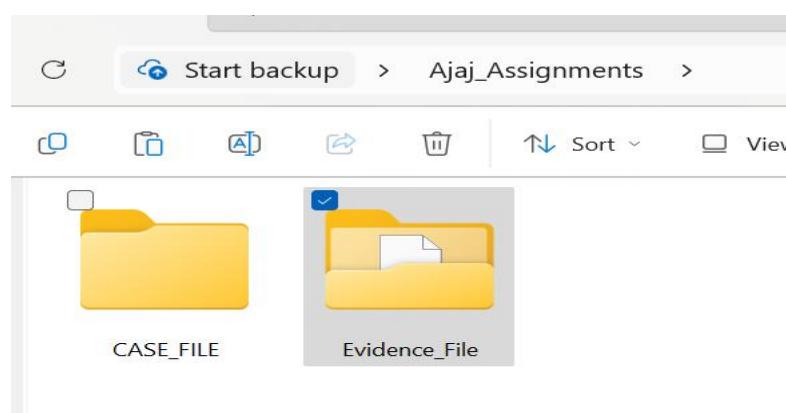
## **Contemporaneous Notes**

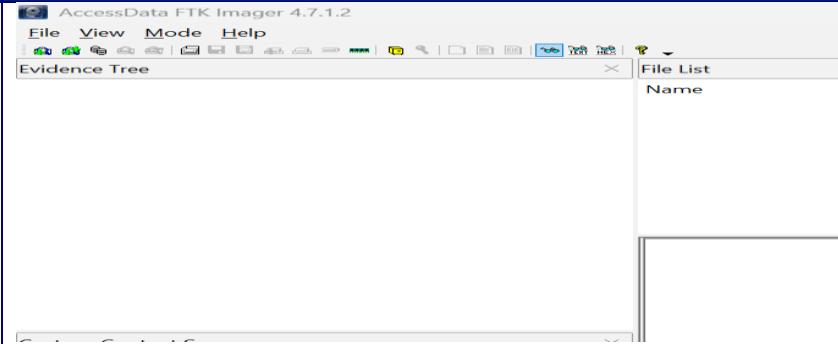
Examiner	AJAJ AHMED	Exam commenced	26 <sup>th</sup> November, 2024
Other relevant information	UWE ID: 24000864	Software used, versions, and licensing.	<ol style="list-style-type: none"><li>1. AccessData FTK Imager 4.7.1.2</li><li>2. Autopsy 4.21.0</li><li>3. Event Log Explorer 4.8</li><li>4. Registry Viewer 6.0</li><li>5. RegRipper 3.0</li><li>6. HXD 2.5</li><li>7. SAMDUMP2 (used in Linux)</li></ol>

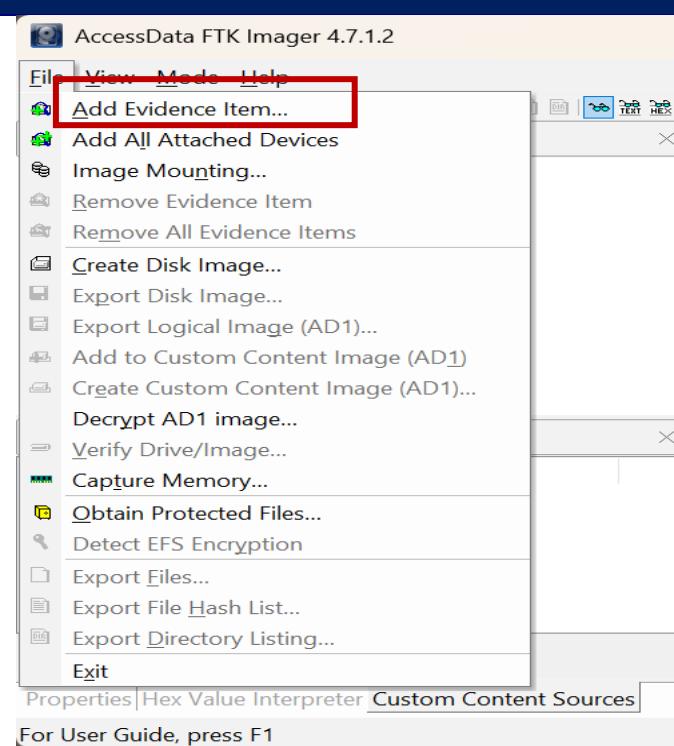


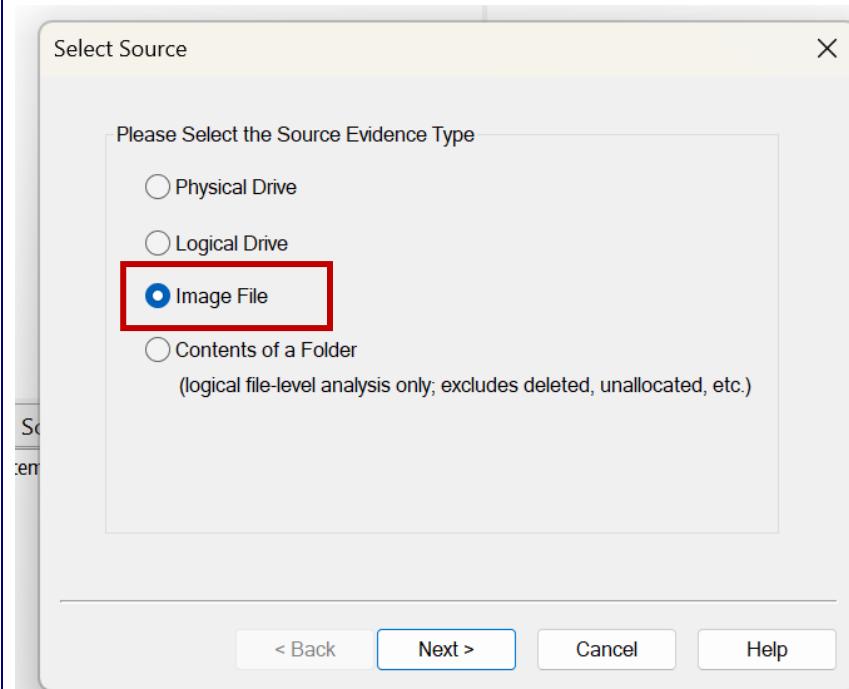
Note: If you decide to omit a process, you should provide your reasons. You may add additional rows, as appropriate.

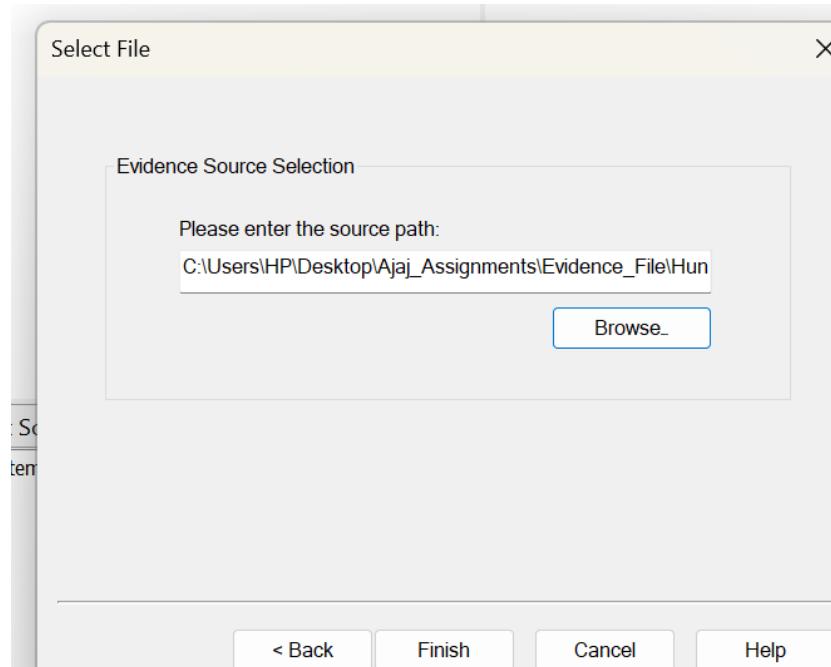
Action	Done?	Date	Time	Notes
Load case and verify image	Yes	19 <sup>th</sup> Dec, 2024	01:00 Pm	<b><u>Step1:</u></b> <ul style="list-style-type: none"><li>• Created Two Folders; named <b>Case file</b> and <b>Evidence file</b>.</li></ul>

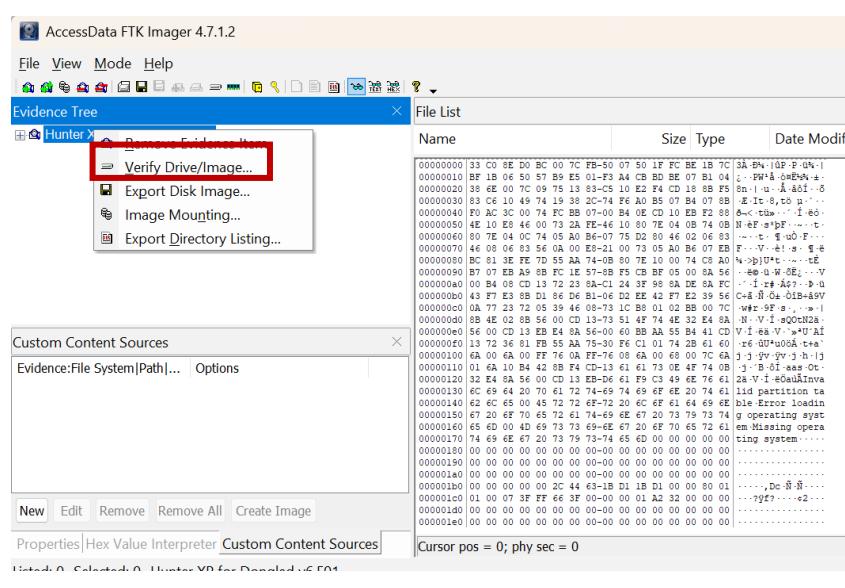
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>I kept the evidence image of <b>Hunter XP for Dongled v6.E01</b> in the evidence file. And other case-related files in the Case File.</li> </ul>  <p><b>Step2:</b> Launched AccessData FTK Imager</p>

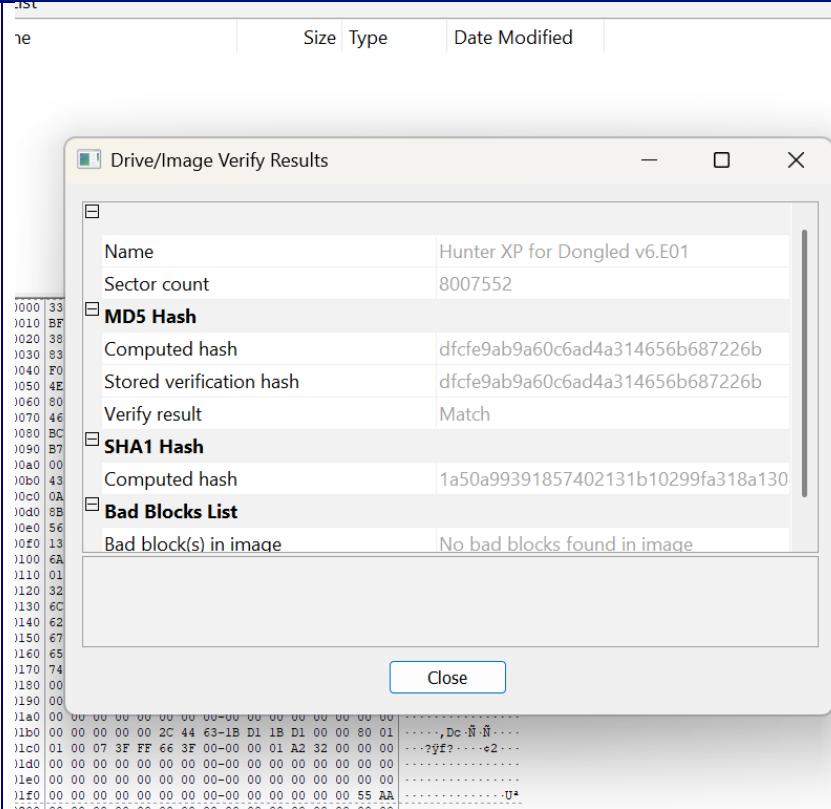
Action	Done?	Date	Time	Notes
				 <p><b>Step3:</b></p> <ul style="list-style-type: none"><li>• At the left corner I clicked on <b>file</b> and selected <b>add evidence item</b>.</li></ul>

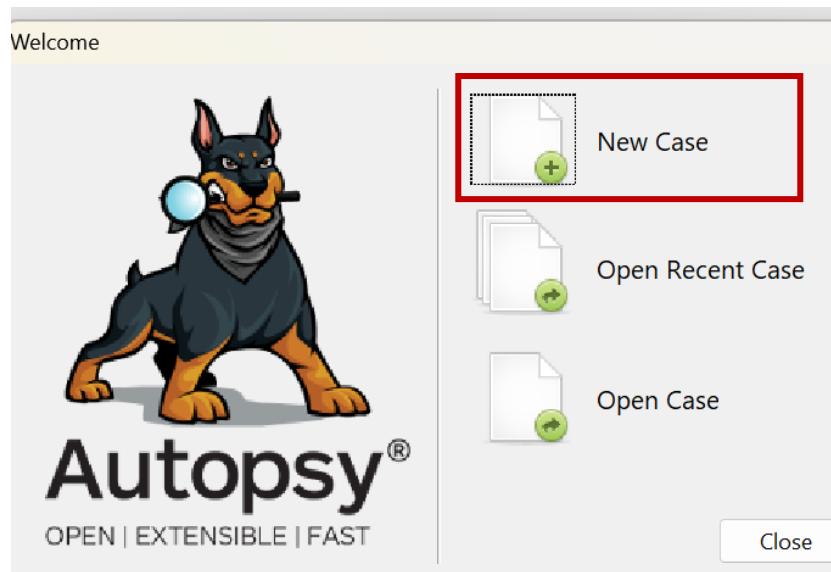
Action	Done?	Date	Time	Notes
				 <p><b>Step 4:</b></p> <ul style="list-style-type: none"> <li>• after clicking on the add evidence item we are asked to select different types of files and drives.</li> </ul>

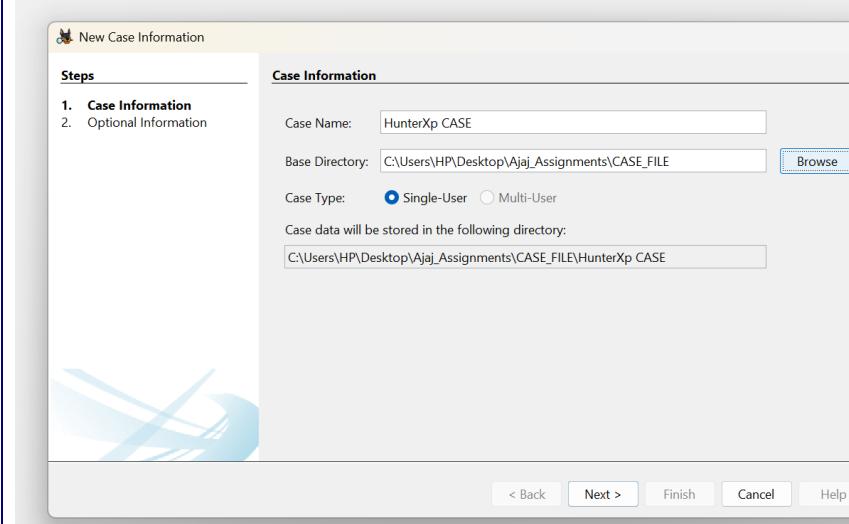
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>I selected the <b>image file</b> as I have given evidence image of <b>Hunter XP for Dongled v6.E01</b></li> </ul>  <p><b>Step 5:</b></p> <ul style="list-style-type: none"> <li>I browse the path <a href="C:\Users\HP\Desktop\Task\Hunter%20XP%20Image\Hunter%20XP%20Image">C:\Users\HP\Desktop\Task\Hunter XP Image\Hunter XP Image</a> where we kept the image file</li> </ul>

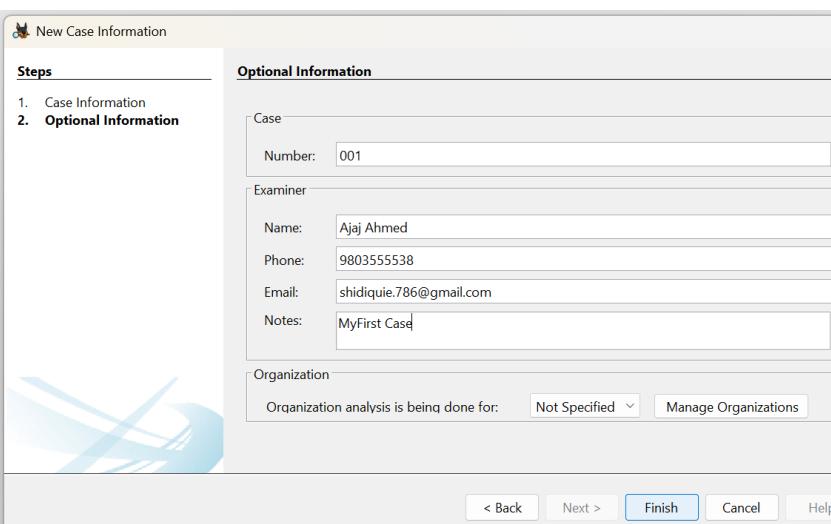
Action	Done?	Date	Time	Notes
				<p>before starting the task and loaded it into <b>AccessData</b></p> <p><b>FTK Imager.</b></p>  <p><b>Step 6:</b></p>

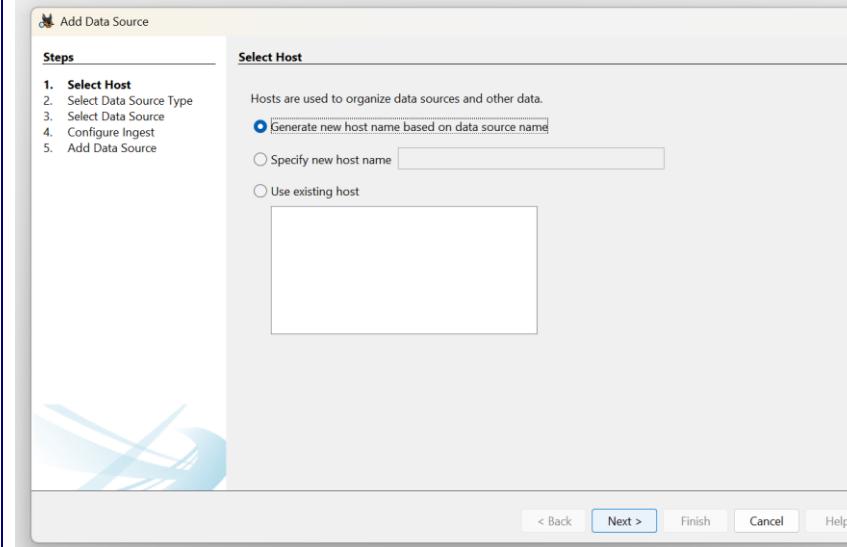
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>To Verify the image, I clicked right on the image and selected Verify Drive/Image to get MD5 Hash and SHA1 hash.</li> </ul> 

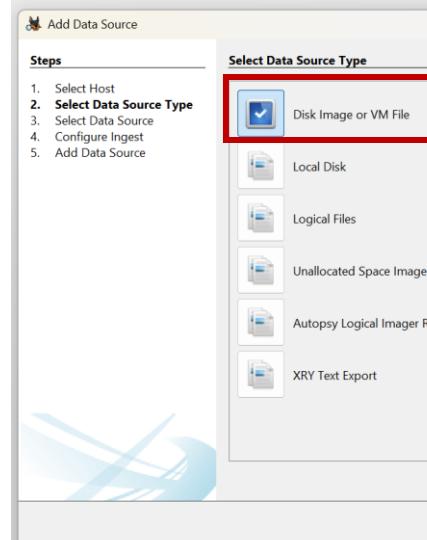
Action	Done?	Date	Time	Notes																				
				 <p>The screenshot shows a 'Drive/Image Verify Results' dialog box. It displays the following information:</p> <table border="1"> <tr> <td>Name</td> <td>Hunter XP for Dongled v6.E01</td> </tr> <tr> <td>Sector count</td> <td>8007552</td> </tr> <tr> <td colspan="2"><b>MD5 Hash</b></td> </tr> <tr> <td>Computed hash</td> <td>dfcfe9ab9a60c6ad4a314656b687226b</td> </tr> <tr> <td>Stored verification hash</td> <td>dfcfe9ab9a60c6ad4a314656b687226b</td> </tr> <tr> <td>Verify result</td> <td>Match</td> </tr> <tr> <td colspan="2"><b>SHA1 Hash</b></td> </tr> <tr> <td>Computed hash</td> <td>1a50a99391857402131b10299fa318a130</td> </tr> <tr> <td colspan="2"><b>Bad Blocks List</b></td> </tr> <tr> <td>Bad block(s) in image</td> <td>No bad blocks found in image</td> </tr> </table> <p>Finally, I got.</p> <p><b>MD5 Hash:</b></p> <p style="color: red;">dfcfe9ab9a60c6ad4a314656b687226b</p> <p><b>SHA1 Hash:</b></p>	Name	Hunter XP for Dongled v6.E01	Sector count	8007552	<b>MD5 Hash</b>		Computed hash	dfcfe9ab9a60c6ad4a314656b687226b	Stored verification hash	dfcfe9ab9a60c6ad4a314656b687226b	Verify result	Match	<b>SHA1 Hash</b>		Computed hash	1a50a99391857402131b10299fa318a130	<b>Bad Blocks List</b>		Bad block(s) in image	No bad blocks found in image
Name	Hunter XP for Dongled v6.E01																							
Sector count	8007552																							
<b>MD5 Hash</b>																								
Computed hash	dfcfe9ab9a60c6ad4a314656b687226b																							
Stored verification hash	dfcfe9ab9a60c6ad4a314656b687226b																							
Verify result	Match																							
<b>SHA1 Hash</b>																								
Computed hash	1a50a99391857402131b10299fa318a130																							
<b>Bad Blocks List</b>																								
Bad block(s) in image	No bad blocks found in image																							

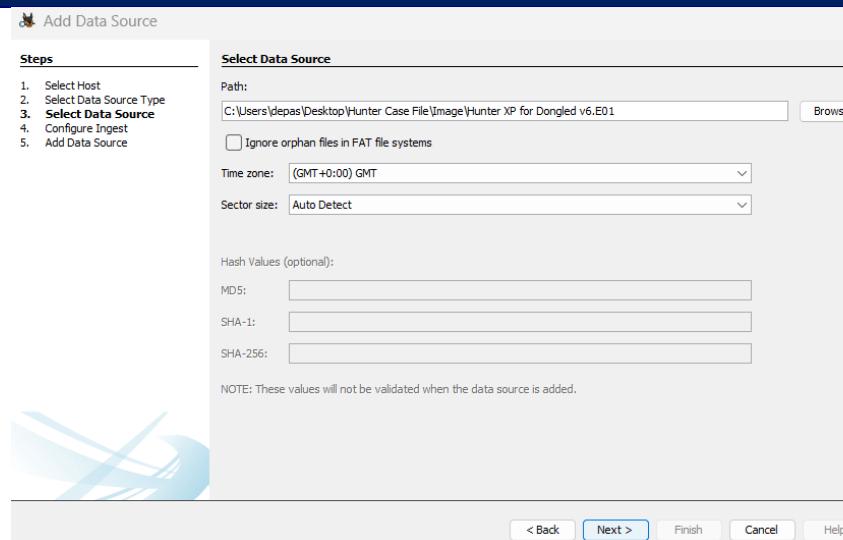
Action	Done?	Date	Time	Notes
				<p>1a50a99391857402131b10299fa318a130a603b0</p> <p><b><u>VERIFICATION USING AUTOPSY</u></b></p> <p><b><u>Step1:</u></b></p> <ul style="list-style-type: none"> <li>• Opened second forensic tool <b>Autopsy</b>.</li> <li>• Clicked on <b>New Case</b>.</li> </ul>  <p><b><u>Step2:</u></b></p> <ul style="list-style-type: none"> <li>• I gave case information.</li> </ul>

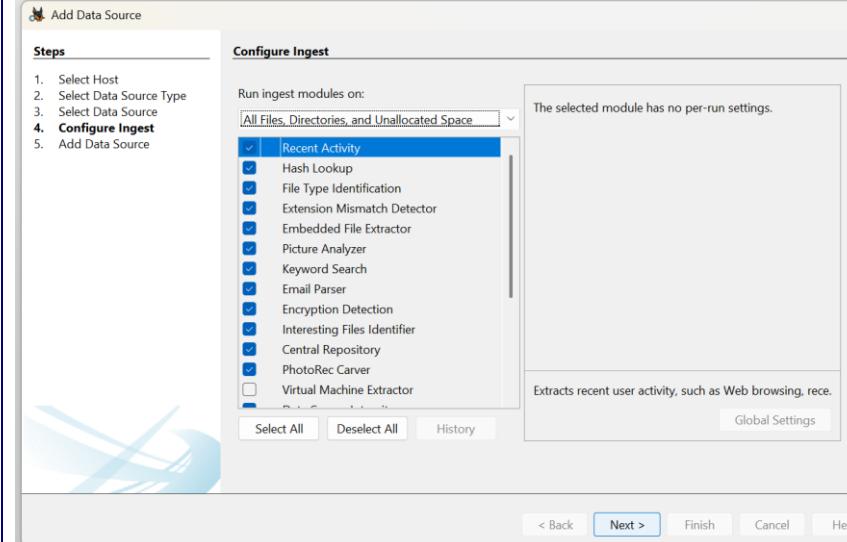
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>➤ Case Name: <b>HunterXP Case</b></li> <li>➤ Base Directory: <a href="C:\Users\HP\Desktop\Ajaj_Assignments\CASE_FILE">C:\Users\HP\Desktop\Ajaj_Assignments\CASE_FILE</a></li> </ul>  <p><b>Step 3:</b></p> <ul style="list-style-type: none"> <li>• I give Optional Information About;</li> <li>❖ Case: <ul style="list-style-type: none"> <li>➤ Case Number: <b>001</b></li> </ul> </li> </ul>

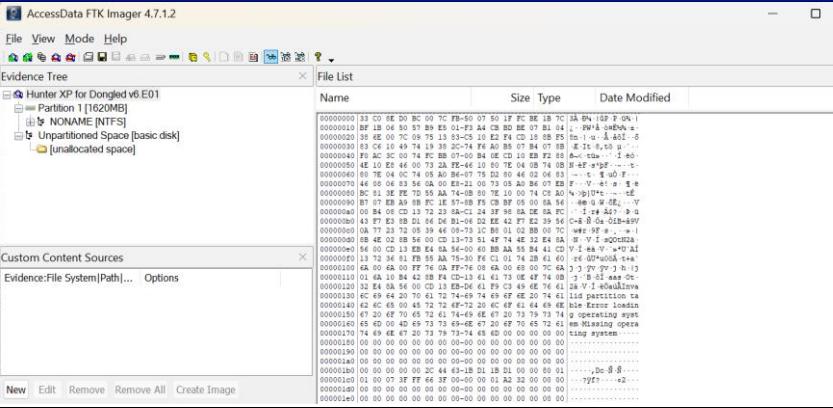
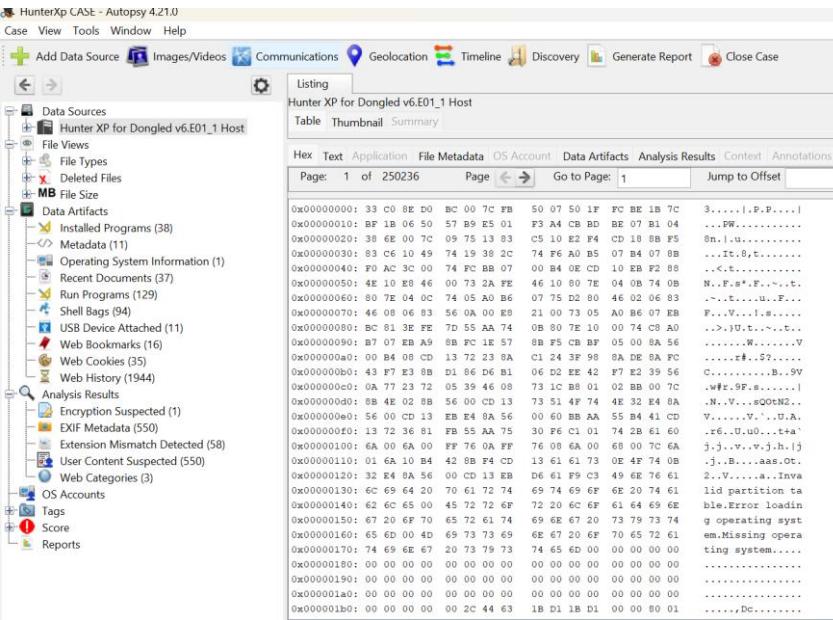
Action	Done?	Date	Time	Notes
				<p>❖ Examiner:</p> <ul style="list-style-type: none"> <li>➤ Name: <b>Ajaj Ahmed</b></li> <li>➤ Phone: <b>9803555538</b></li> <li>➤ Email: <a href="mailto:shidique.786@gmail.com"><u>shidique.786@gmail.com</u></a></li> <li>➤ Note: <b>MyFirst Case</b></li> </ul>  <p><b>STEP 4:</b></p> <p>a. Selected host</p>

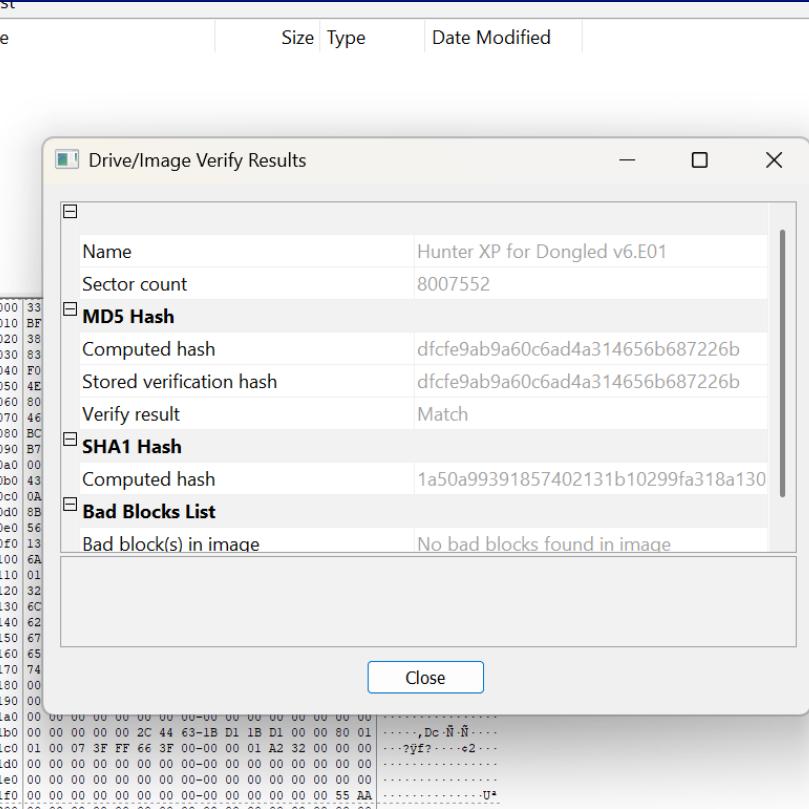
Action	Done?	Date	Time	Notes
				 <p>Selected Data source file <b>Disk Image or VM File</b></p>

Action	Done?	Date	Time	Notes
				 <p>a. Selected data source by Browsing path <a href="C:\Users\HP\Desktop\Task\Hunter XP Image\Hunter XP Image">C:\Users\HP\Desktop\Task\Hunter XP Image\Hunter XP Image</a></p>

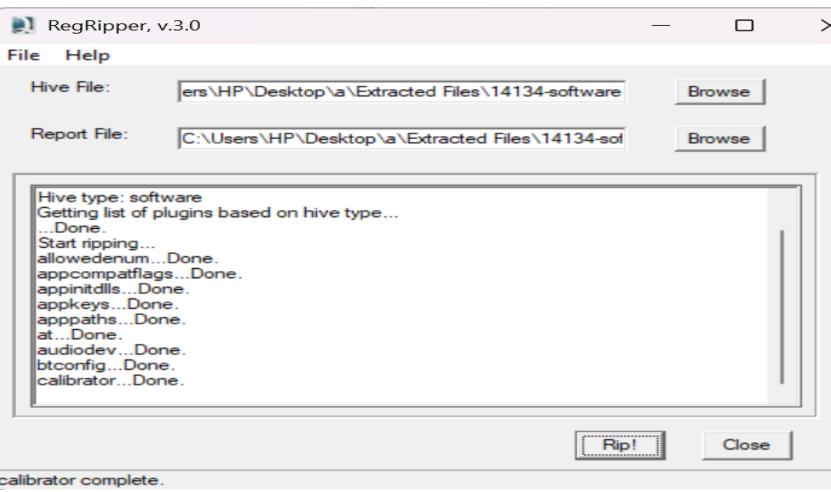
Action	Done?	Date	Time	Notes
				 <p><b>Steps</b></p> <ol style="list-style-type: none"> <li>1. Select Host</li> <li>2. Select Data Source Type</li> <li><b>3. Select Data Source</b></li> <li>4. Configure Ingest</li> <li>5. Add Data Source</li> </ol> <p><b>Select Data Source</b></p> <p>Path: C:\Users\depas\Desktop\Hunter Case File\Image\Hunter XP for Dongled v6.E01 <input type="button" value="Browse"/></p> <p><input type="checkbox"/> Ignore orphan files in FAT file systems</p> <p>Time zone: (GMT+0:00) GMT</p> <p>Sector size: Auto Detect</p> <p>Hash Values (optional):</p> <p>MD5: <input type="text"/></p> <p>SHA-1: <input type="text"/></p> <p>SHA-256: <input type="text"/></p> <p>NOTE: These values will not be validated when the data source is added.</p> <p>&lt; Back <input type="button" value="Next &gt;"/> <input type="button" value="Finish"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/></p> <p>a. Configured Ingest Modules.</p>

Action	Done?	Date	Time	Notes
				 <p>Finally, Data Source has been added to the Autopsy for Further Investigation.</p> <p><b>Step 5:</b></p> <ul style="list-style-type: none"> <li>• After loading and analysing the metadata I found the <b>MD5 hash</b> value and <b>hex value</b> of the image file is same. It gives the dual verification of image artifacts.</li> </ul>

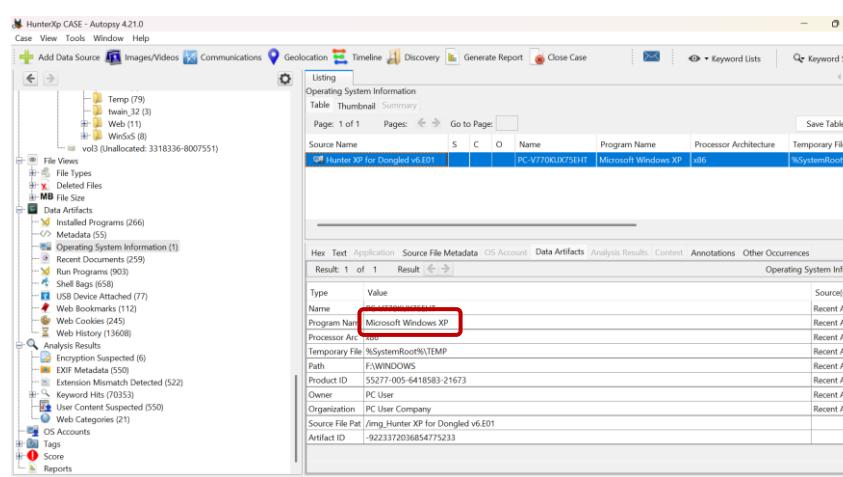
Action	Done?	Date	Time	Notes
				 

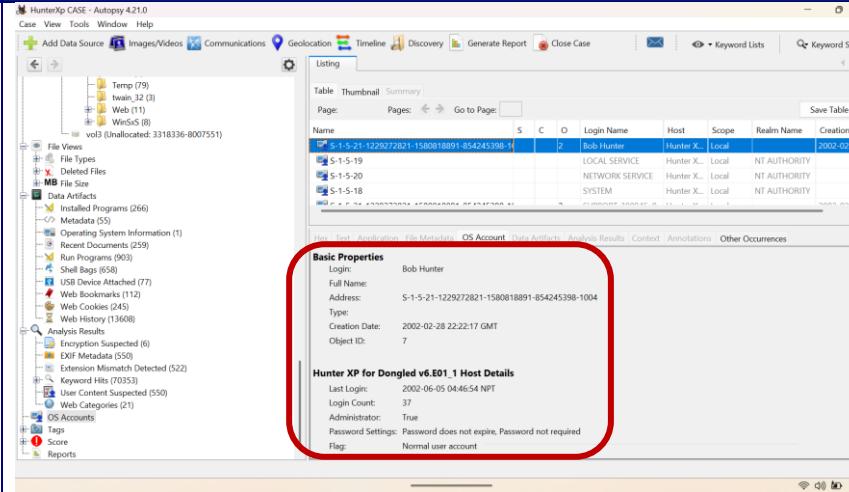
Action	Done?	Date	Time	Notes
				 <p>The screenshot shows a 'Drive/Image Verify Results' dialog box. It displays the following information:</p> <ul style="list-style-type: none"> <li><b>Name:</b> Hunter XP for Dongled v6.E01</li> <li><b>Sector count:</b> 8007552</li> <li><b>MD5 Hash:</b> <ul style="list-style-type: none"> <li>Computed hash: dfcfe9ab9a60c6ad4a314656b687226b</li> <li>Stored verification hash: dfcfe9ab9a60c6ad4a314656b687226b</li> <li>Verify result: Match</li> </ul> </li> <li><b>SHA1 Hash:</b> <ul style="list-style-type: none"> <li>Computed hash: 1a50a99391857402131b10299fa318a130</li> </ul> </li> <li><b>Bad Blocks List:</b> No bad blocks found in image.</li> </ul> <p>At the bottom right of the dialog box is a 'Close' button.</p>

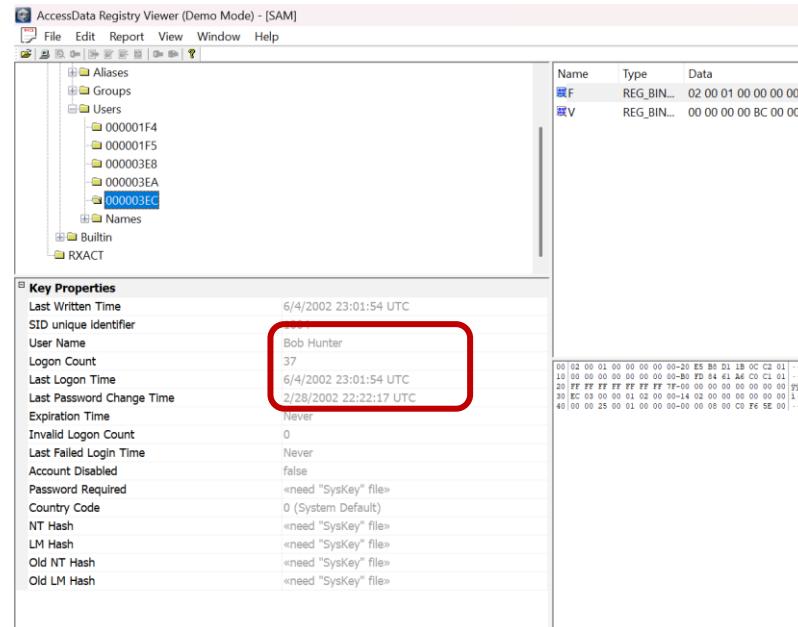
Action	Done?	Date	Time	Notes																																																			
				<div style="border: 1px solid #ccc; padding: 10px;"> <p style="margin: 0;">Hex Text Application File Metadata OS Account Data Artifacts Analysis</p> <h3>Metadata</h3> <table border="0" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Name:</td> <td>/img_Hunter XP for Dongled v6.E01</td> </tr> <tr> <td>Type:</td> <td>E01</td> </tr> <tr> <td>Size:</td> <td>4099866624</td> </tr> <tr> <td>MD5:</td> <td style="background-color: #f0f0f0;">dfcfe9ab9a60c6ad4a314656b687226b</td> </tr> <tr> <td>SHA1:</td> <td>Not calculated</td> </tr> <tr> <td>SHA-256:</td> <td>Not calculated</td> </tr> <tr> <td>Sector Size:</td> <td>512</td> </tr> <tr> <td>Time Zone:</td> <td>Asia/Katmandu</td> </tr> <tr> <td>Acquisition Details:</td> <td>Description: Hunter XP Case Number: 1 Evidence Number: 1 Acquired Date: Fri Jan 25 08:06:19 2008</td> </tr> </table> <p style="margin-top: 20px;">Operating System Information</p> <table border="0" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Type</td> <td style="width: 85%;">Value</td> <td style="width: 10%;">Source(s)</td> </tr> <tr> <td>Name</td> <td>DC-V770KUX75FHT</td> <td>Recent Activity</td> </tr> <tr> <td>Program Name</td> <td style="background-color: #f0f0f0;">Microsoft Windows XP</td> <td>Recent Activity</td> </tr> <tr> <td>Processor Archit</td> <td>x86</td> <td>Recent Activity</td> </tr> <tr> <td>Temporary Files</td> <td>%SystemRoot%\TEMP</td> <td>Recent Activity</td> </tr> <tr> <td>Path</td> <td>F:\WINDOWS</td> <td>Recent Activity</td> </tr> <tr> <td>Product ID</td> <td>55277-005-6418583-21673</td> <td>Recent Activity</td> </tr> <tr> <td>Owner</td> <td>PC User</td> <td>Recent Activity</td> </tr> <tr> <td>Organization</td> <td>PC User Company</td> <td>Recent Activity</td> </tr> <tr> <td>Source File Path</td> <td>/img_Hunter XP for Dongled v6.E01</td> <td></td> </tr> <tr> <td>Artifact ID</td> <td>-9223372036854775233</td> <td></td> </tr> </table> </div>	Name:	/img_Hunter XP for Dongled v6.E01	Type:	E01	Size:	4099866624	MD5:	dfcfe9ab9a60c6ad4a314656b687226b	SHA1:	Not calculated	SHA-256:	Not calculated	Sector Size:	512	Time Zone:	Asia/Katmandu	Acquisition Details:	Description: Hunter XP Case Number: 1 Evidence Number: 1 Acquired Date: Fri Jan 25 08:06:19 2008	Type	Value	Source(s)	Name	DC-V770KUX75FHT	Recent Activity	Program Name	Microsoft Windows XP	Recent Activity	Processor Archit	x86	Recent Activity	Temporary Files	%SystemRoot%\TEMP	Recent Activity	Path	F:\WINDOWS	Recent Activity	Product ID	55277-005-6418583-21673	Recent Activity	Owner	PC User	Recent Activity	Organization	PC User Company	Recent Activity	Source File Path	/img_Hunter XP for Dongled v6.E01		Artifact ID	-9223372036854775233	
Name:	/img_Hunter XP for Dongled v6.E01																																																						
Type:	E01																																																						
Size:	4099866624																																																						
MD5:	dfcfe9ab9a60c6ad4a314656b687226b																																																						
SHA1:	Not calculated																																																						
SHA-256:	Not calculated																																																						
Sector Size:	512																																																						
Time Zone:	Asia/Katmandu																																																						
Acquisition Details:	Description: Hunter XP Case Number: 1 Evidence Number: 1 Acquired Date: Fri Jan 25 08:06:19 2008																																																						
Type	Value	Source(s)																																																					
Name	DC-V770KUX75FHT	Recent Activity																																																					
Program Name	Microsoft Windows XP	Recent Activity																																																					
Processor Archit	x86	Recent Activity																																																					
Temporary Files	%SystemRoot%\TEMP	Recent Activity																																																					
Path	F:\WINDOWS	Recent Activity																																																					
Product ID	55277-005-6418583-21673	Recent Activity																																																					
Owner	PC User	Recent Activity																																																					
Organization	PC User Company	Recent Activity																																																					
Source File Path	/img_Hunter XP for Dongled v6.E01																																																						
Artifact ID	-9223372036854775233																																																						

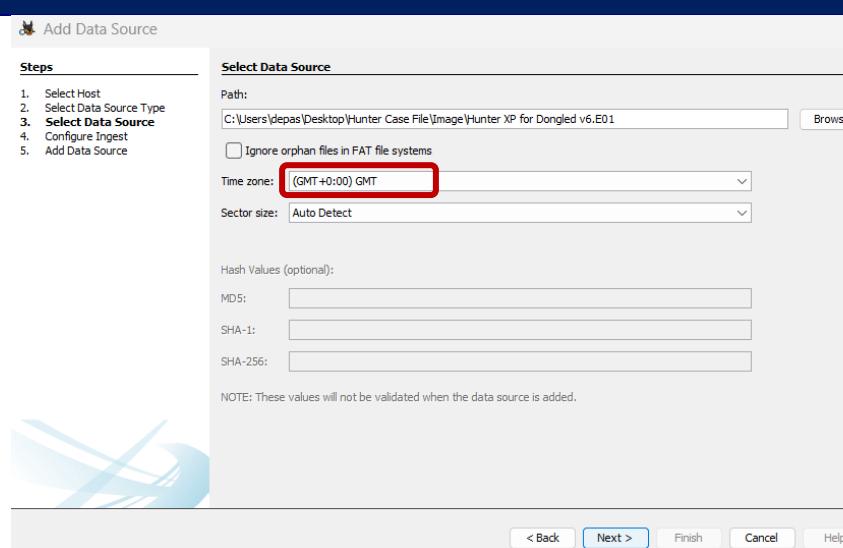
Action	Done?	Date	Time	Notes
Load Case into a second forensic tool for dual verification of at least 2 key artifacts, evidence items	yes	19/12/2024	01/20 pm	<p><b>Step1:</b></p> <p>Loaded case into Autopsy and followed the path;</p> <p>Path:</p> <p>/img_Hunter XP for Dongled</p> <p>v6.E01/vol_vo2/WINDOWS/system32/config</p> <ul style="list-style-type: none"> <li>• Then extracted software file</li> <li>• The software file is ripped using RegRipper tool to get its txt file.</li> </ul>  <p>The screenshot shows the RegRipper v.3.0 application window. The 'Hive File:' field contains 'ers\HP\Desktop\1\Extracted Files\14134-software' and the 'Report File:' field contains 'C:\Users\HP\Desktop\1\Extracted Files\14134-sof'. The main pane displays the output of the rippling process for a 'software' hive, listing various registry keys and their status as 'Done'. The bottom right of the window has 'Rip!' and 'Close' buttons.</p>

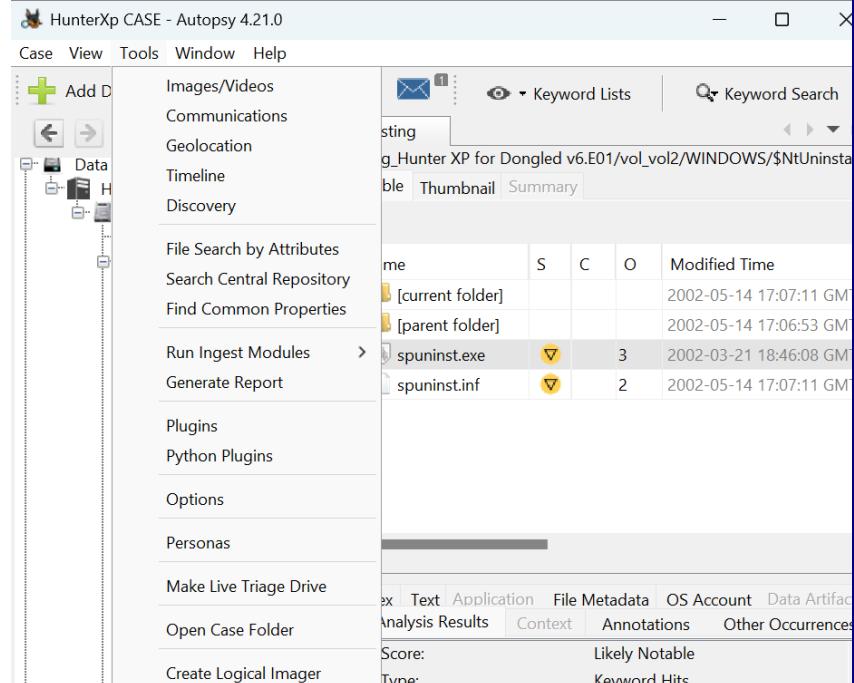
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>After making txt file, opened the txt file and searched for product name to get information about operating system.</li> </ul> <pre> -----  winver v.20200525  (Software) Get Windows version &amp; build info    ProductName Microsoft Windows XP  BuildLab 2600.xpcIntl_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 </pre> <p><b>Step2:</b></p> <ul style="list-style-type: none"> <li>Now, I have verified the operating system of the image file in <b>autopsy</b> by following the given steps:</li> <li>Selected <b>Data Artifacts</b>.</li> <li>Found <b>operating system</b>.</li> </ul>

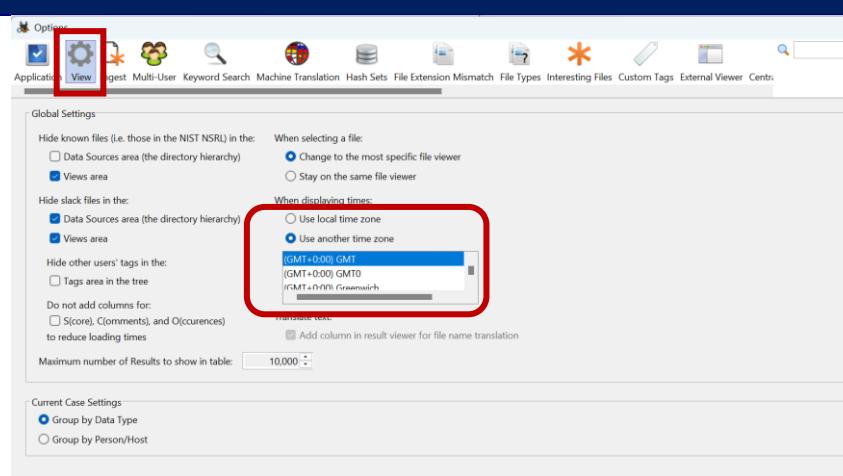
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>Then selected <b>Hunter XP for Dongled v6.E01</b></li> </ul> <p>After clicking on <b>Hunter XP for Dongled v6.E01</b> , I got information about the operating system of given evidence file.</p>  <p>The screenshot shows the Autopsy interface with the 'Operating System Information' table open. The 'Program Name' row is highlighted with a red box, showing 'Microsoft Windows XP'. Other columns include Source Name (PC_V770KUXT5EHT), Processor Architecture (x86), and Temporary File (%SystemRoot%).</p> <p>Now, the operating system is verified as <b>Microsoft Windows XP</b>.</p> <p><b>Step3:</b></p> <ul style="list-style-type: none"> <li>The loaded case in autopsy <b>OS account</b> was accessed.</li> </ul>

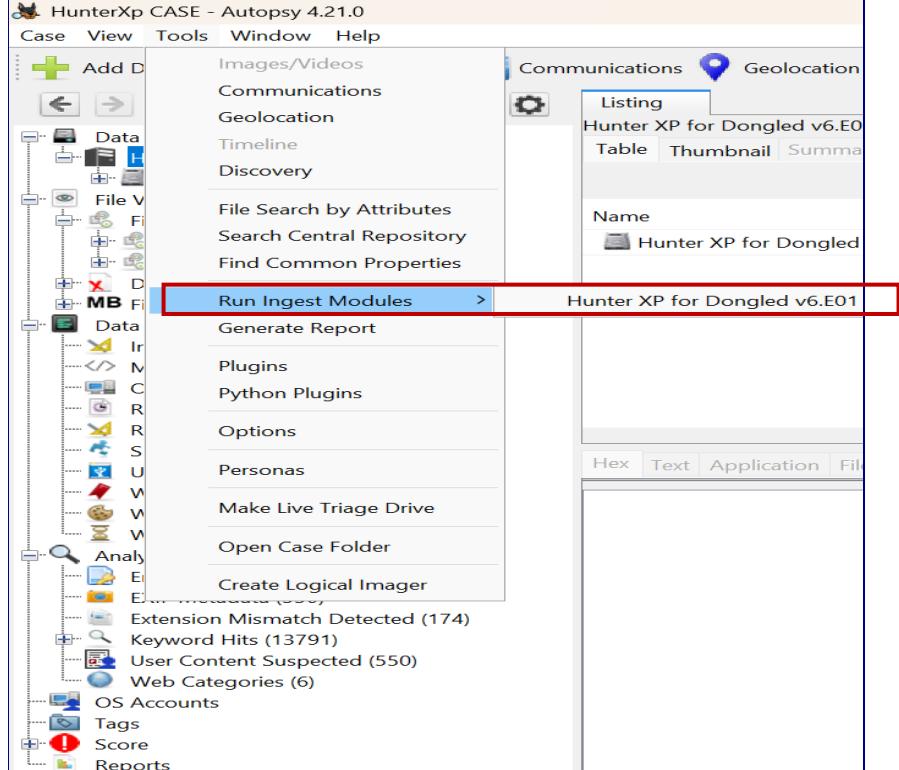
Action	Done?	Date	Time	Notes
				 <ul style="list-style-type: none"> <li>In this case I followed the same path as I followed to extract software and extracted <b>SAM</b> file.</li> <li>Then the extracted <b>SAM</b> file is loaded in <b>AccessData Registry Viewer</b>.</li> <li>I opened registry viewer as administrator.</li> <li>Choose file option to load <b>SAM</b> in this application and the file was chosen from drop down Menu from the path where I kept <b>SAM</b> file.</li> <li>After Loading the case I followed the path</li> </ul>

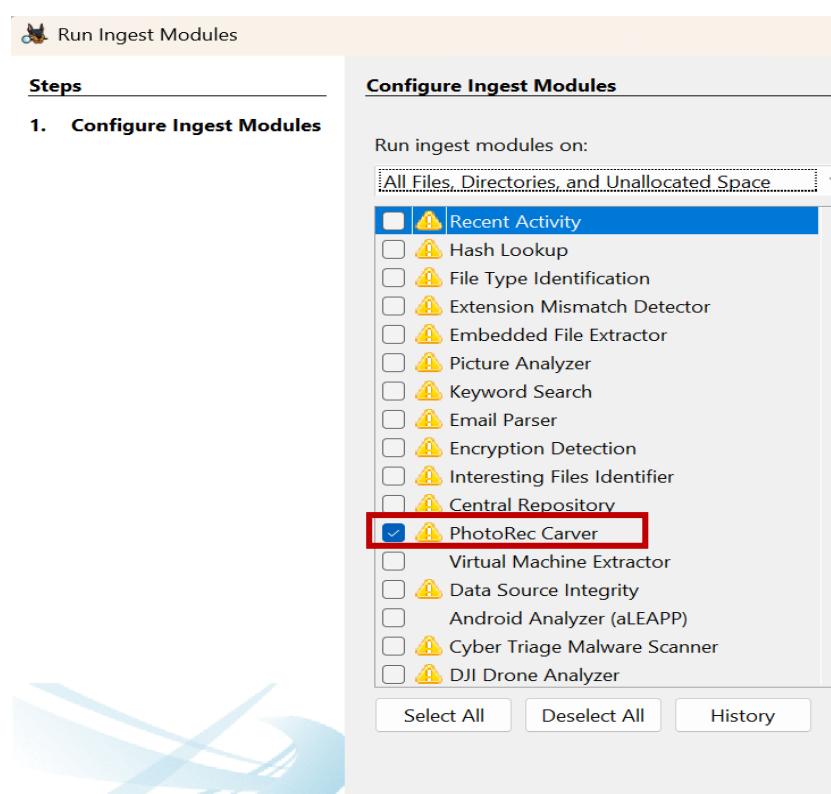
Action	Done?	Date	Time	Notes
				<p>Path:</p> <p><a href="#">SAM/Domains/Account/Users/000003EC</a></p>  <p>In both cases the logon count of Bob Hunter is same that is 5.</p>
Time Zone Adjusted? Report Time Zone used for Analysis.	yes	19/12/2024	01/35 pm	<p><b>Step1:</b></p> <p>The <b>time zone</b> is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

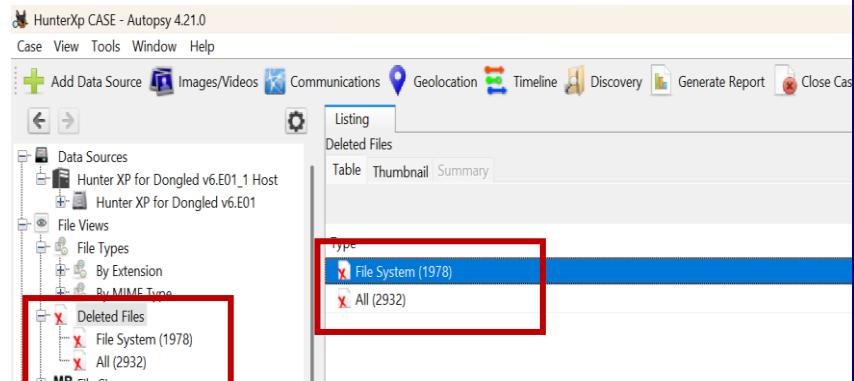
Action	Done?	Date	Time	Notes
				 <p><b>Step2:</b></p> <p>Time zones can also be adjusted within the <b>autopsy</b>, by following the steps below.</p> <ul style="list-style-type: none"> <li>• Click on <b>tools</b></li> <li>• Selected <b>options</b></li> <li>• Clicked on <b>View</b></li> <li>• Use another Time Zone.</li> </ul>

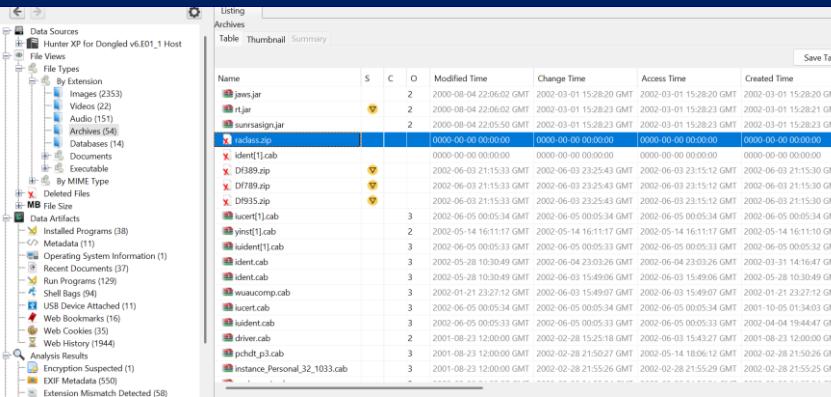
Action	Done?	Date	Time	Notes																									
				 <p>The screenshot shows the HunterXp CASE - Autopsy 4.21.0 interface. The main window displays a file search results table. The table has columns for Name, S, C, O, and Modified Time. The results show two files: 'spuninst.exe' and 'spuninst.inf'. Both files have a score of 3 and were modified on 2002-05-14 at 17:07:11 GMT.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>S</th> <th>C</th> <th>O</th> <th>Modified Time</th> </tr> </thead> <tbody> <tr> <td>[current folder]</td> <td></td> <td></td> <td></td> <td>2002-05-14 17:07:11 GMT</td> </tr> <tr> <td>[parent folder]</td> <td></td> <td></td> <td></td> <td>2002-05-14 17:06:53 GMT</td> </tr> <tr> <td>spuninst.exe</td> <td>3</td> <td></td> <td></td> <td>2002-03-21 18:46:08 GMT</td> </tr> <tr> <td>spuninst.inf</td> <td>2</td> <td></td> <td></td> <td>2002-05-14 17:07:11 GMT</td> </tr> </tbody> </table>	Name	S	C	O	Modified Time	[current folder]				2002-05-14 17:07:11 GMT	[parent folder]				2002-05-14 17:06:53 GMT	spuninst.exe	3			2002-03-21 18:46:08 GMT	spuninst.inf	2			2002-05-14 17:07:11 GMT
Name	S	C	O	Modified Time																									
[current folder]				2002-05-14 17:07:11 GMT																									
[parent folder]				2002-05-14 17:06:53 GMT																									
spuninst.exe	3			2002-03-21 18:46:08 GMT																									
spuninst.inf	2			2002-05-14 17:07:11 GMT																									

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

Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>• First of all, open <b>tools</b> in Autopsy.</li> </ul>  <p><b>Step2:</b></p> <ul style="list-style-type: none"> <li>• And selected <b>run ingest module</b> for Hunter XP for Dongled v6.E01.</li> </ul>

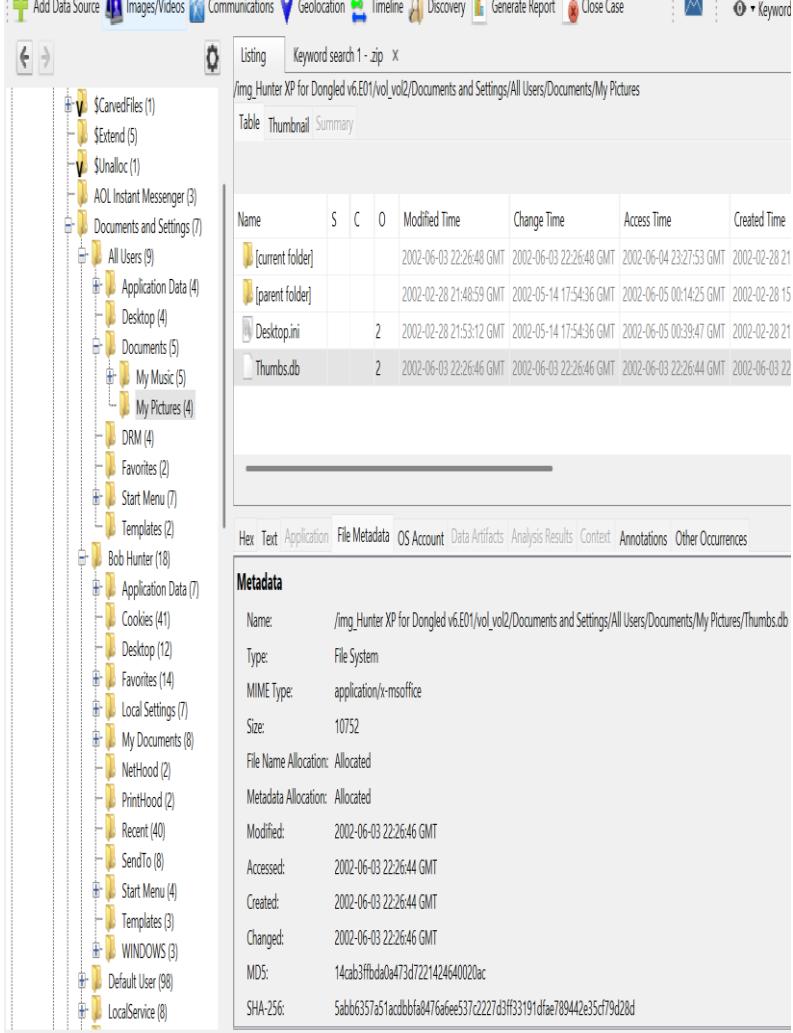
Action	Done?	Date	Time	Notes
				<p><b><u>Step3:</u></b></p> <ul style="list-style-type: none"> <li>Configured <b>photoRec carver</b> to recover lost folders.</li> </ul> 

Action	Done?	Date	Time	Notes
				<p><b>Step4:</b></p> <ul style="list-style-type: none"> <li>After running <b>photoRec Carver</b> we recovered lost folders as deleted files. We got deleted files containing 1978 files and all files containing 2932 files.</li> </ul> 
Mount archives; zip, thumbs.db, etc.	yes	20/12/2024	04:00 PM	<p><b>Step1:</b></p> <ul style="list-style-type: none"> <li>For Mount Archives we follow the Path: Files Views/ FileTypes / By Extension</li> </ul> <p>After following these paths I got the archives folder.</p>

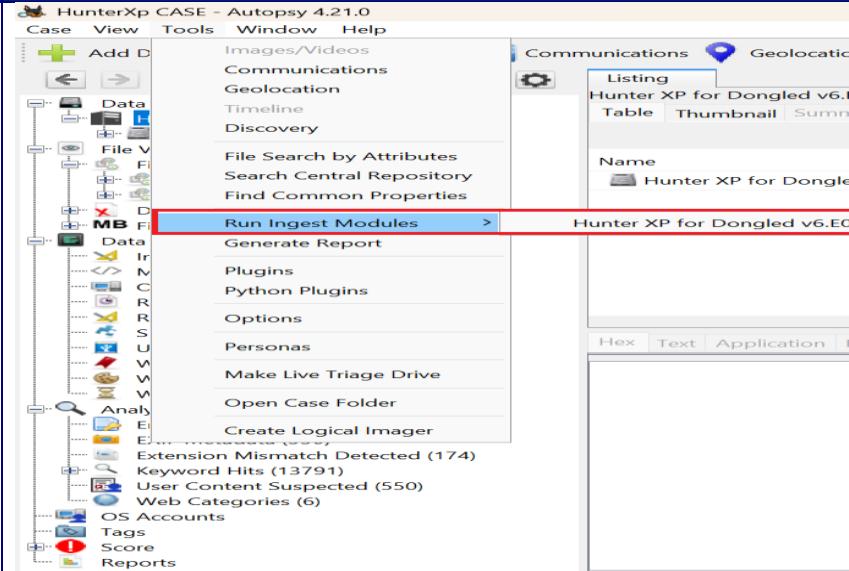
Action	Done?	Date	Time	Notes
				 <p><b>Step 2:</b></p> <ul style="list-style-type: none"> <li>I found zip files in different path that is.       <ul style="list-style-type: none"> <li>➤ <a href="#">/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temp/~rnsetup/raclass.zip</a></li> <li>➤ <a href="#">/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df389.zip</a></li> </ul> </li> </ul>

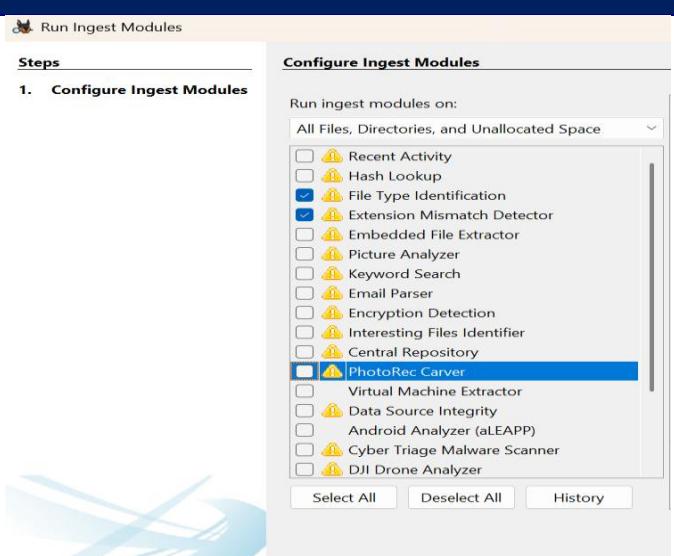
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>➤ <a href="#">/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df789.zip</a></li>   <li>➤ <a href="#">/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df935.zip</a></li>   <li>➤ <a href="#">/img_Hunter XP for Dongled v6.E01/vol_vol2/Program Files/America Online 7.0/download/CURREX~1.zip</a></li>   <li>➤ <a href="#">/img_Hunter XP for Dongled v6.E01/vol_vol2/Program Files/America Online 7.0/download/hourz11.zip</a></li> </ul>

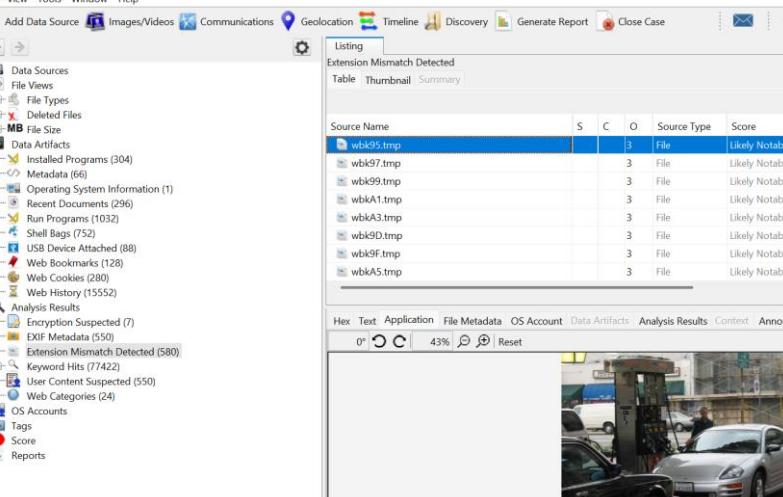
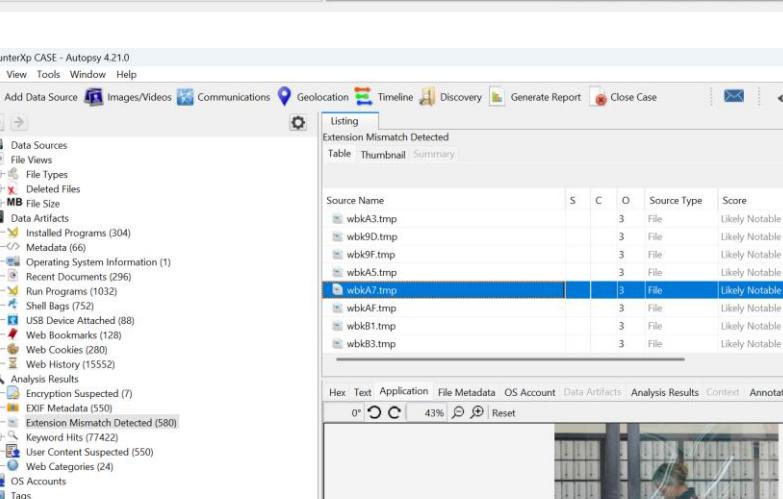
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>➤ /img_Hunter XP for Dongled</li> <li>v6.E01/vol_vol2/Program Files/Windows Media</li> <li>Player/npdrmv2.zip</li>   <li>➤ /img_Hunter XP for Dongled</li> <li>v6.E01/vol_vol2/Program Files/Windows Media</li> <li>Player/npds.zip</li> </ul> <p><b><u>Step 3:</u></b></p> <p>To get thumbs.db i follow the path;</p> <ol style="list-style-type: none"> <li>1. /img_Hunter XP for Dongled</li> <li>v6.E01/vol_vol2/Documents and Settings/All</li> <li>Users/Documents/My Pictures/Thumbs.db</li> </ol>

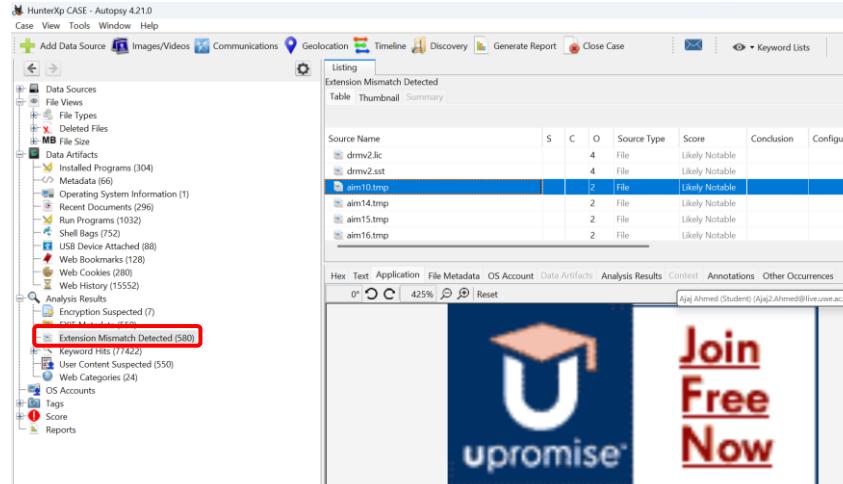
Action	Done?	Date	Time	Notes																																								
				 <p>The screenshot shows a digital forensic analysis interface. At the top, there's a toolbar with various icons: Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, Close Case, and a Keyword search field. Below the toolbar is a navigation bar with tabs: Listing (selected), Keyword search 1 - zip, and X. The main area displays a file tree on the left and a detailed table on the right.</p> <p><b>File Tree:</b></p> <ul style="list-style-type: none"> <li>\$CarvedFiles (1)</li> <li>\$Extend (5)</li> <li>\$Jalloc (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>Application Data (4)</li> <li>Desktop (4)</li> <li>Documents (5)           <ul style="list-style-type: none"> <li>My Music (5)</li> <li>My Pictures (4)</li> </ul> </li> <li>DRM (4)</li> <li>Favorites (2)</li> <li>Start Menu (7)</li> <li>Templates (2)</li> </ul> </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)</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> </ul> </li> <li>Default User (98)</li> <li>LocalService (8)</li> </ul> <p><b>Table:</b></p> <p>/img_Hunter XP for Dongled v6.E01/vol.vol2/Documents and Settings/All Users/Documents/My Pictures</p> <table border="1"> <thead> <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> </tr> </thead> <tbody> <tr> <td>[current folder]</td> <td></td> <td></td> <td></td> <td>2002-06-03 22:26:48 GMT</td> <td>2002-06-03 22:26:48 GMT</td> <td>2002-06-04 23:27:53 GMT</td> <td>2002-02-28 21</td> </tr> <tr> <td>[parent folder]</td> <td></td> <td></td> <td></td> <td>2002-02-28 21:48:59 GMT</td> <td>2002-05-14 17:54:36 GMT</td> <td>2002-06-05 00:14:25 GMT</td> <td>2002-02-28 15</td> </tr> <tr> <td>Desktop.ini</td> <td>2</td> <td></td> <td></td> <td>2002-02-28 21:53:12 GMT</td> <td>2002-05-14 17:54:36 GMT</td> <td>2002-06-05 00:39:47 GMT</td> <td>2002-02-28 21</td> </tr> <tr> <td>Thumbs.db</td> <td>2</td> <td></td> <td></td> <td>2002-06-03 22:26:46 GMT</td> <td>2002-06-03 22:26:46 GMT</td> <td>2002-06-03 22:26:44 GMT</td> <td>2002-06-03 22</td> </tr> </tbody> </table> <p><b>Metadata:</b></p> <p>Name: /img_Hunter XP for Dongled v6.E01/vol.vol2/Documents and Settings/All Users/Documents/My Pictures/Thumbs.db    Type: File System    MIME Type: application/x-msoffice    Size: 10752    File Name Allocation: Allocated    Metadata Allocation: Allocated    Modified: 2002-06-03 22:26:46 GMT    Accessed: 2002-06-03 22:26:44 GMT    Created: 2002-06-03 22:26:44 GMT    Changed: 2002-06-03 22:26:46 GMT    MD5: 14cab3fbda0a473d721424640020ac    SHA-256: 5abb6357a51acd0bbfa8476a6ee537c2227d3ff33191dfa78944e35cf79d28d</p>	Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	[current folder]				2002-06-03 22:26:48 GMT	2002-06-03 22:26:48 GMT	2002-06-04 23:27:53 GMT	2002-02-28 21	[parent folder]				2002-02-28 21:48:59 GMT	2002-05-14 17:54:36 GMT	2002-06-05 00:14:25 GMT	2002-02-28 15	Desktop.ini	2			2002-02-28 21:53:12 GMT	2002-05-14 17:54:36 GMT	2002-06-05 00:39:47 GMT	2002-02-28 21	Thumbs.db	2			2002-06-03 22:26:46 GMT	2002-06-03 22:26:46 GMT	2002-06-03 22:26:44 GMT	2002-06-03 22
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time																																					
[current folder]				2002-06-03 22:26:48 GMT	2002-06-03 22:26:48 GMT	2002-06-04 23:27:53 GMT	2002-02-28 21																																					
[parent folder]				2002-02-28 21:48:59 GMT	2002-05-14 17:54:36 GMT	2002-06-05 00:14:25 GMT	2002-02-28 15																																					
Desktop.ini	2			2002-02-28 21:53:12 GMT	2002-05-14 17:54:36 GMT	2002-06-05 00:39:47 GMT	2002-02-28 21																																					
Thumbs.db	2			2002-06-03 22:26:46 GMT	2002-06-03 22:26:46 GMT	2002-06-03 22:26:44 GMT	2002-06-03 22																																					

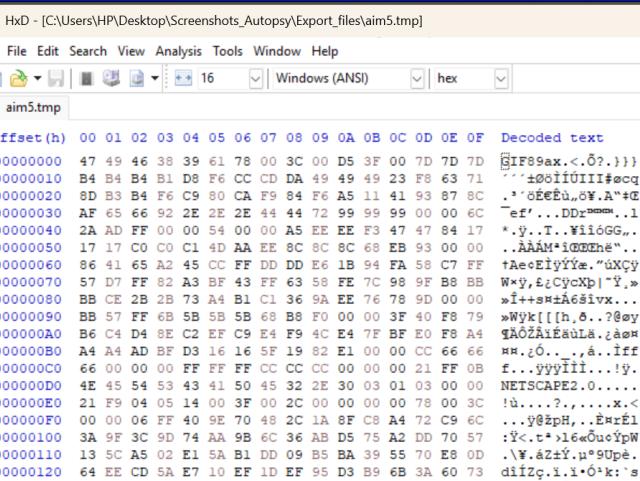
Action	Done?	Date	Time	Notes
				<p>2. /img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Application Data/Microsoft/CD Burning/Hunter Pics/Christina Detsiwt/Thumbs.db</p> <p>3. We also find thumbs.db on exploring the path file views/ file types/ By Extension/DataBases.</p>
File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation)	yes	20/12/2024	05:00 PM	<p>To Investigate <b>file signature</b> and <b>file mismatch</b> I followed these steps:</p> <p><b>Step1:</b></p> <ul style="list-style-type: none"> <li>Firstly, I opened <b>tools</b> and ran the <b>ingest module</b> for the <b>Hunter XP for Dongled v6.E01</b>.</li> </ul>

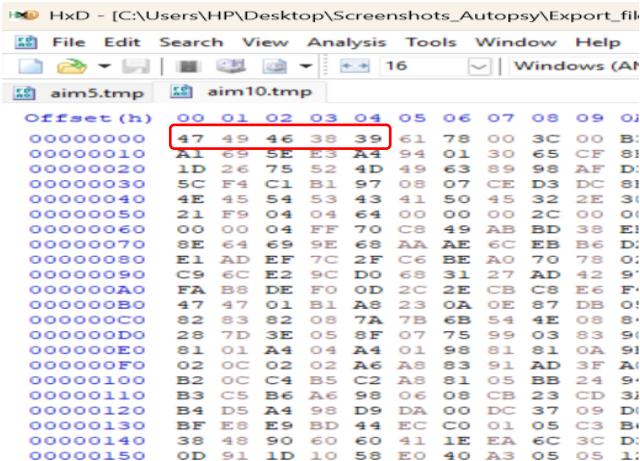
Action	Done?	Date	Time	Notes
				 <ul style="list-style-type: none"> <li>• The after that I have configured the <b>File type identification</b> and <b>Extension mismatch Detector modules.</b></li> <li>• By running the ingest module by clicking on tools in the autopsy.</li> </ul>

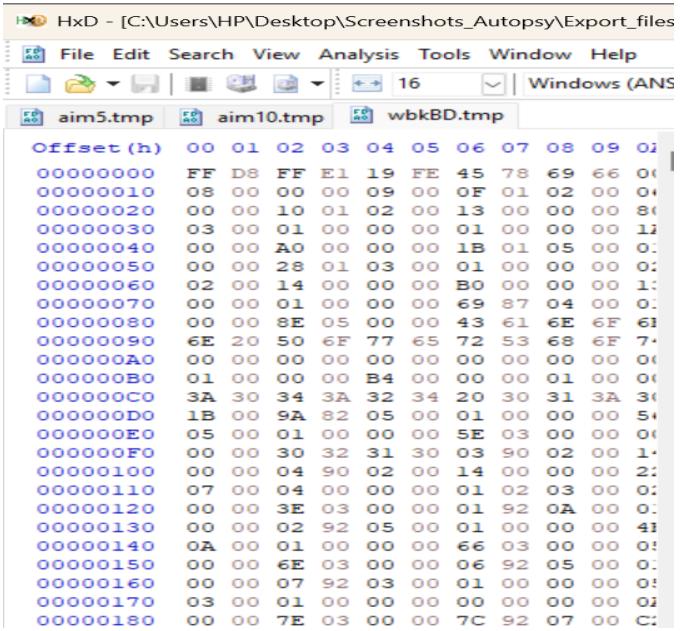
Action	Done?	Date	Time	Notes
				 <ul style="list-style-type: none"> <li>• After running this module, I found an <b>Extension mismatch Detected</b> file in the <b>Analysis result</b>.</li> </ul>

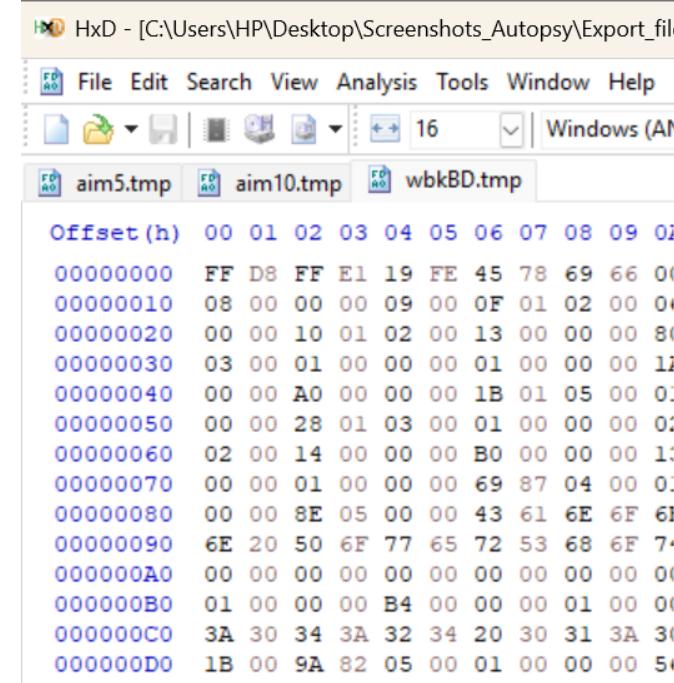
Action	Done?	Date	Time	Notes
				
				

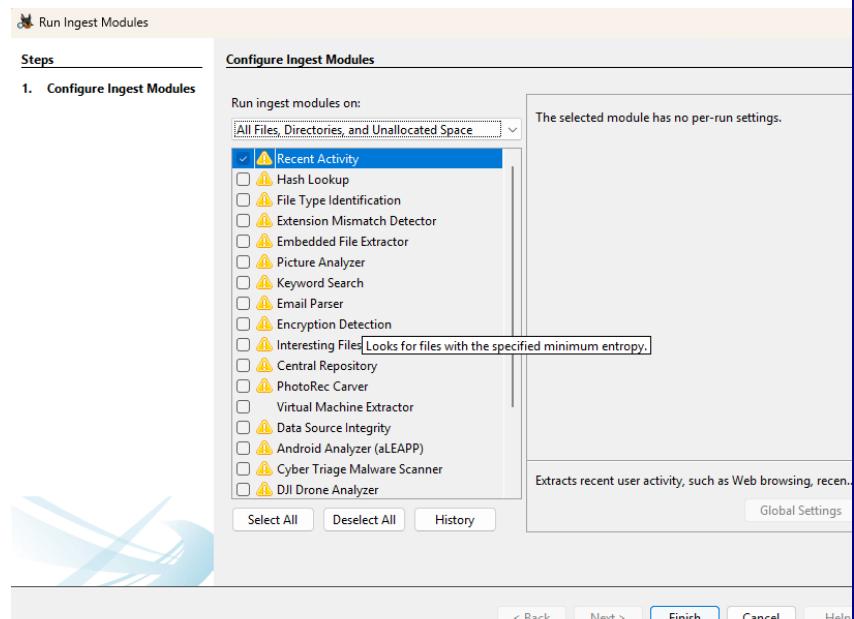
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>After performing all these steps, I exported some files to verify whether the extension of these files is correct or not</li> <li>Now I opened the HXD application for analysis of the hash values of these files, whether these values are correct or not according to the file types.</li> <li>Now at the top of the righthand side there is the file I have clicked on the file and choose the open file to add the file I have exported for hash values analysis.</li> </ul> 

Action	Done?	Date	Time	Notes
				 <ul style="list-style-type: none"> <li>At first, I added aim5.tmp for the HEX values analysis I got.</li> <p>In this file, I got hash values <b>47 49 46 38 39 61</b>. The value I got is not the hash value of the .tmp file the given hash value is for .gif files. So, it seems that there is a mismatch of file extensions.</p> <li>For aim10.tmp I followed the same step and I got the same result for aim10.tmp file. It is also a .gif file. So, both aim5.tmp and aim10.tmp is .gif file.</li> </ul>

Action	Done?	Date	Time	Notes
				 <ul style="list-style-type: none"> <li>Again, performing the same process for verification of wbkBD.tmp and wbkC1.tmp for file extension verification I got there is also file extension mismatch. The hash value I got for these two files is <b>FF D8 FF E1 1B FE</b>. The hash value I got from HXD is the value of the <b>JPEG</b> file. So, it seems that there is a tempering with the files.</li> </ul>

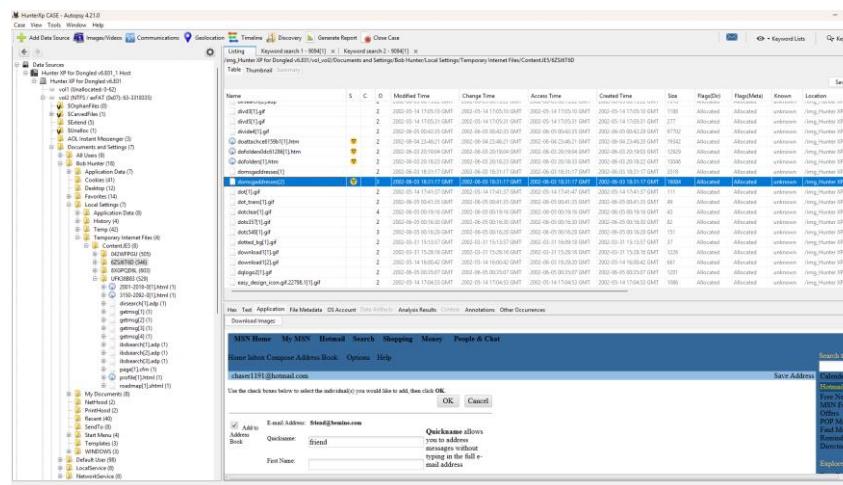
Action	Done?	Date	Time	Notes
				 <pre> HxD - [C:\Users\HP\Desktop\Screenshots_Autopsy\Export_files] File Edit Search View Analysis Tools Window Help aim5.tmp aim10.tmp wbkBD.tmp Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 00000000 FF D8 FF E1 19 FE 45 78 69 66 01 00000010 08 00 00 00 09 00 0F 01 02 00 04 00000020 00 00 10 01 02 00 13 00 00 00 80 00000030 03 00 01 00 00 00 01 00 00 00 11 00000040 00 00 A0 00 00 00 1B 01 05 00 00 00000050 00 00 28 01 03 00 01 00 00 00 01 00000060 02 00 14 00 00 00 B0 00 00 00 11 00000070 00 00 01 00 00 00 69 87 04 00 00 00000080 00 00 8E 05 00 00 43 61 6E 6F 61 00000090 6E 20 50 6F 77 65 72 53 68 6F 74 000000A0 00 00 00 00 00 00 00 00 00 00 00 000000B0 01 00 00 00 B4 00 00 00 01 00 00 000000C0 3A 30 34 3A 32 34 20 30 31 3A 30 000000D0 1B 00 9A 82 05 00 01 00 00 00 54 000000E0 05 00 01 00 00 00 5E 03 00 00 00 000000F0 00 00 30 32 31 30 03 90 02 00 14 00000100 00 00 04 90 02 00 14 00 00 00 21 00000110 07 00 04 00 00 00 01 02 03 00 00 00000120 00 00 3E 03 00 00 01 92 0A 00 00 00000130 00 00 02 92 05 00 01 00 00 00 41 00000140 0A 00 01 00 00 00 66 03 00 00 00 00000150 00 00 6E 03 00 00 06 92 05 00 00 00000160 00 00 07 92 03 00 01 00 00 00 00 00000170 03 00 01 00 00 00 00 00 00 00 01 00000180 00 00 7E 03 00 00 7C 92 07 00 C1 </pre>

Action	Done?	Date	Time	Notes
				 <pre> HxD - [C:\Users\HP\Desktop\Screenshots_Autopsy\Export_files] File Edit Search View Analysis Tools Window Help Windows (ANS) aim5.tmp aim10.tmp wbkBD.tmp  Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 00000000 FF D8 FF E1 19 FE 45 78 69 66 00 00000010 08 00 00 00 09 00 0F 01 02 00 00 00 00000020 00 00 10 01 02 00 13 00 00 00 00 80 00000030 03 00 01 00 00 00 01 00 00 00 00 12 00000040 00 00 A0 00 00 00 1B 01 05 00 00 00 00000050 00 00 28 01 03 00 01 00 00 00 00 02 00000060 02 00 14 00 00 00 B0 00 00 00 00 1E 00000070 00 00 01 00 00 00 69 87 04 00 00 00 00000080 00 00 8E 05 00 00 43 61 6E 6F 61 00000090 6E 20 50 6F 77 65 72 53 68 6F 74 000000A0 00 00 00 00 00 00 00 00 00 00 00 00 000000B0 01 00 00 00 B4 00 00 00 01 00 00 00 000000C0 3A 30 34 3A 32 34 20 30 31 3A 30 000000D0 1B 00 9A 82 05 00 01 00 00 00 00 51 ..... 00 00 00 00 00 00 00 00 00 00 00 00 </pre>
Internet History, favourites, etc. Other browsers?	YES	20/12/2024	05:30	<p><b><u>Step1:</u></b></p> <p>I ran the ingest module recent folders to find internet files and followed the following steps.</p> <ul style="list-style-type: none"> <li>➤ Clicked on the <b>tools</b>.</li> </ul>

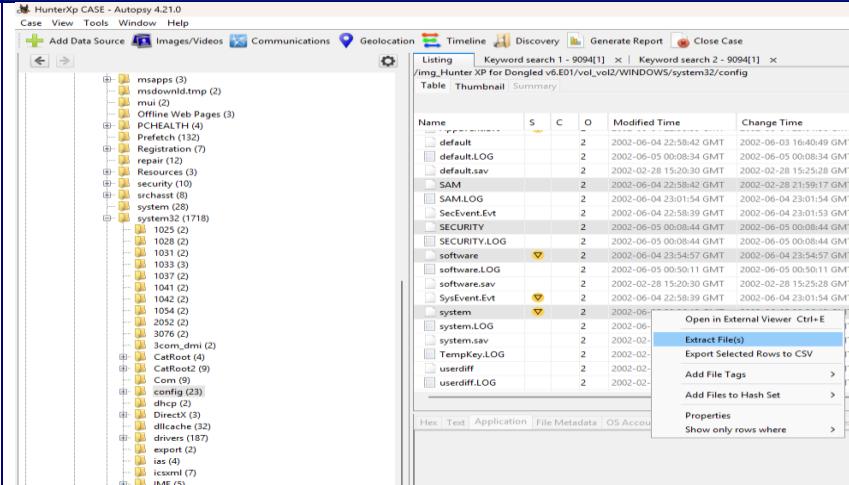
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>➤ Clicked <b>run ingest module</b>.</li> <li>➤ Select <b>Hunter XP for Dongled v6.E01</b>.</li> <li>➤ And selected <b>Recent Activities</b>.</li> </ul>  <p><b>Step2:</b></p> <p>After running this module, I followed the steps given below.</p>

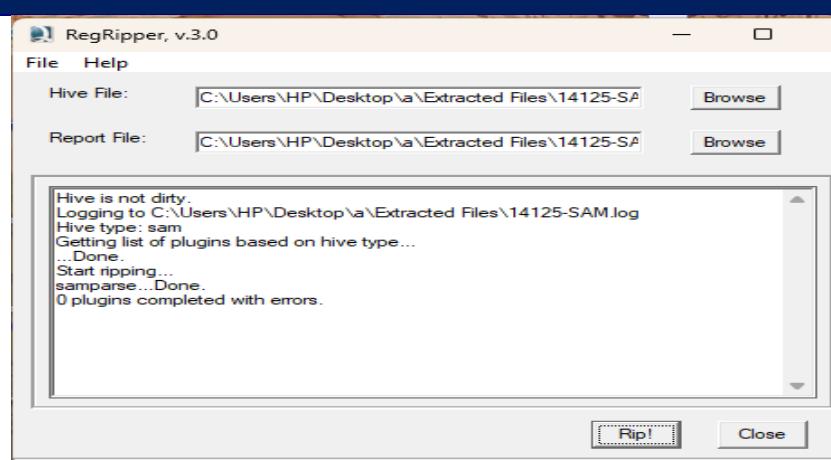
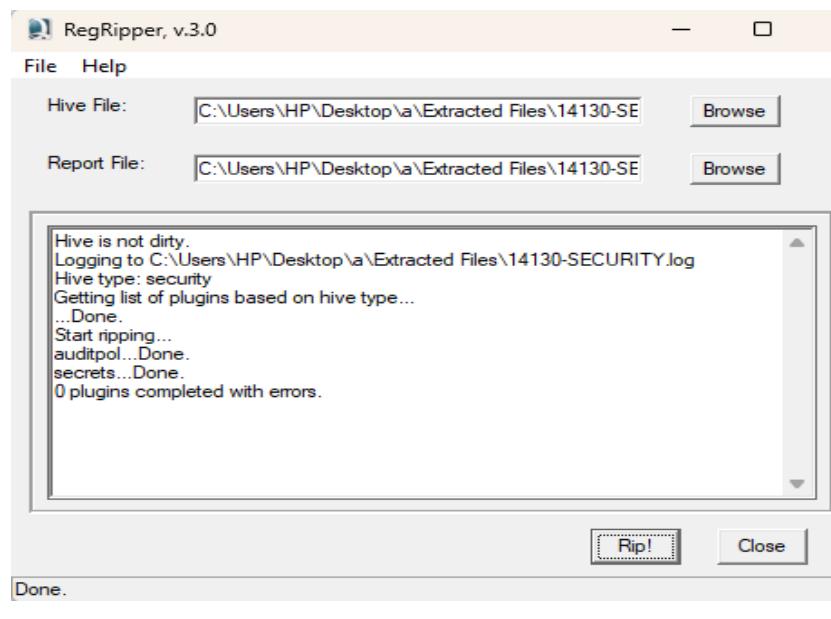
Action	Done?	Date	Time	Notes
				<p>a. Clicked on the data artifacts.</p> <p>b. In data artifacts I saw three artifacts of</p> <ul style="list-style-type: none"> <li>a. Web bookmarks.</li> <li>b. Web Cookies</li> <li>c. Web History</li> </ul> <p>After investigating the installed programs. I observed that only the Internet Explorer browser was viewed.</p>
Emails, local and web-based.	Yes	20/12/2024	06:15 PM	<p><b><u>Step1:</u></b></p> <p>To find Local emails I have followed the path:  <a href="/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Application">/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Application</a></p>

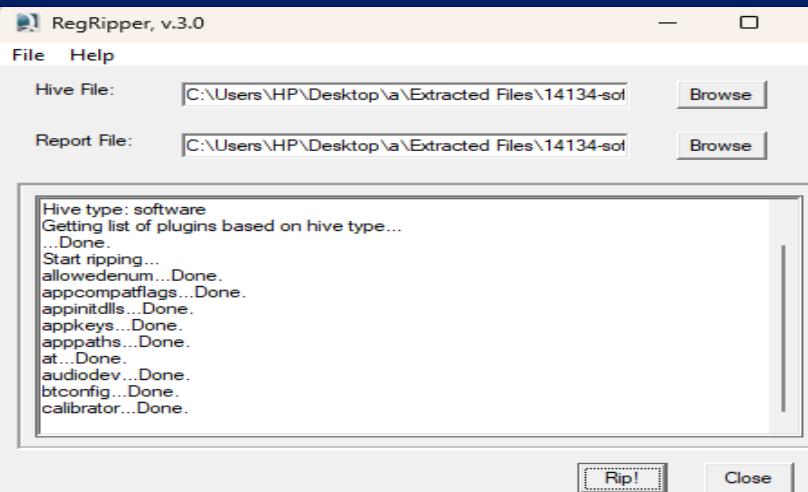
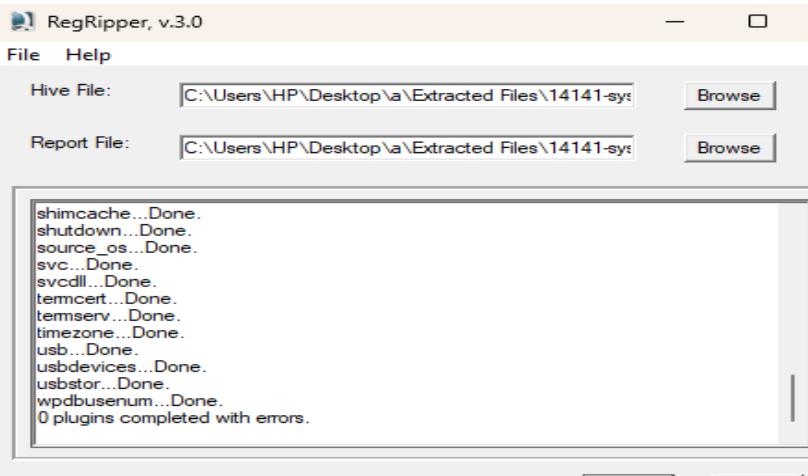
Action	Done?	Date	Time	Notes
				<p>Data/Identities/{8054E531-ABCC-4D69-A565-3978F75945DF}/Microsoft/Outlook Express</p> <p><b>Step2:</b></p> <p>To find web-based emails I have followed this path.</p> <p><a href="#">:/img_Hunter XP for Dongled v6.E01/vol.vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5</a></p>

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

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

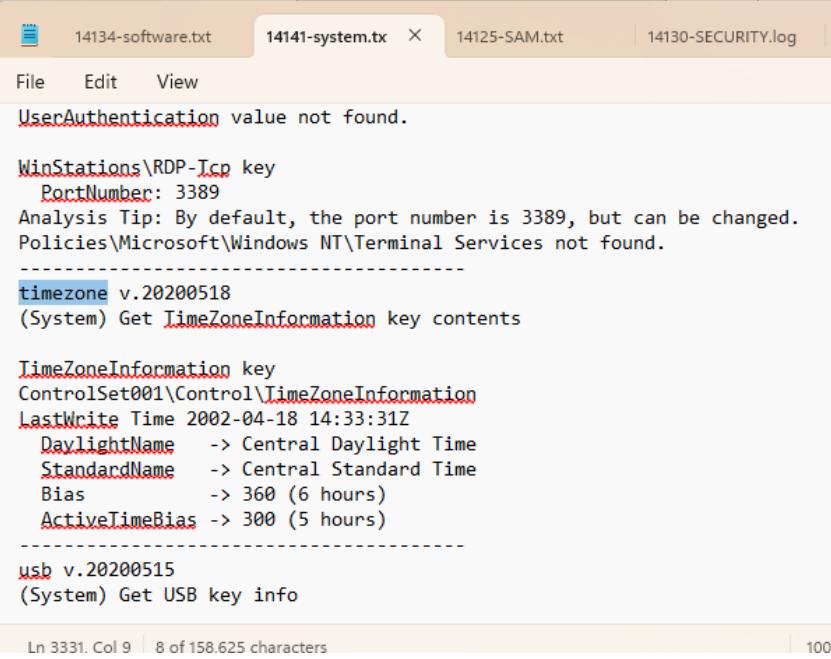
Action	Done?	Date	Time	Notes
				 <p>d. After extracting these files, I have used these files. Now these extracted files are used to retrieve operating system information, account information, software, and time zone information using RegRipper.</p>

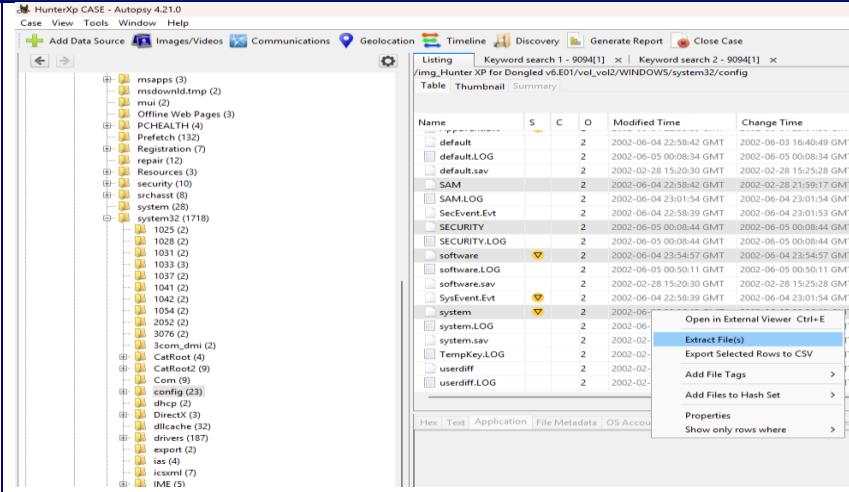
Action	Done?	Date	Time	Notes
				 <p>RegRipper, v.3.0</p> <p>Hive File: C:\Users\HP\Desktop\va\Extracted Files\14125-SAM</p> <p>Report File: C:\Users\HP\Desktop\va\Extracted Files\14125-SAM.log</p> <pre>Hive is not dirty. Logging to C:\Users\HP\Desktop\va\Extracted Files\14125-SAM.log Hive type: sam Getting list of plugins based on hive type... ...Done. Start ripping... samparse...Done. 0 plugins completed with errors.</pre> <p>Rip! Close Done</p>
				 <p>RegRipper, v.3.0</p> <p>Hive File: C:\Users\HP\Desktop\va\Extracted Files\14130-SECURITY</p> <p>Report File: C:\Users\HP\Desktop\va\Extracted Files\14130-SECURITY.log</p> <pre>Hive is not dirty. Logging to C:\Users\HP\Desktop\va\Extracted Files\14130-SECURITY.log Hive type: security Getting list of plugins based on hive type... ...Done. Start ripping... auditpol...Done. secrets...Done. 0 plugins completed with errors.</pre> <p>Rip! Close Done</p>

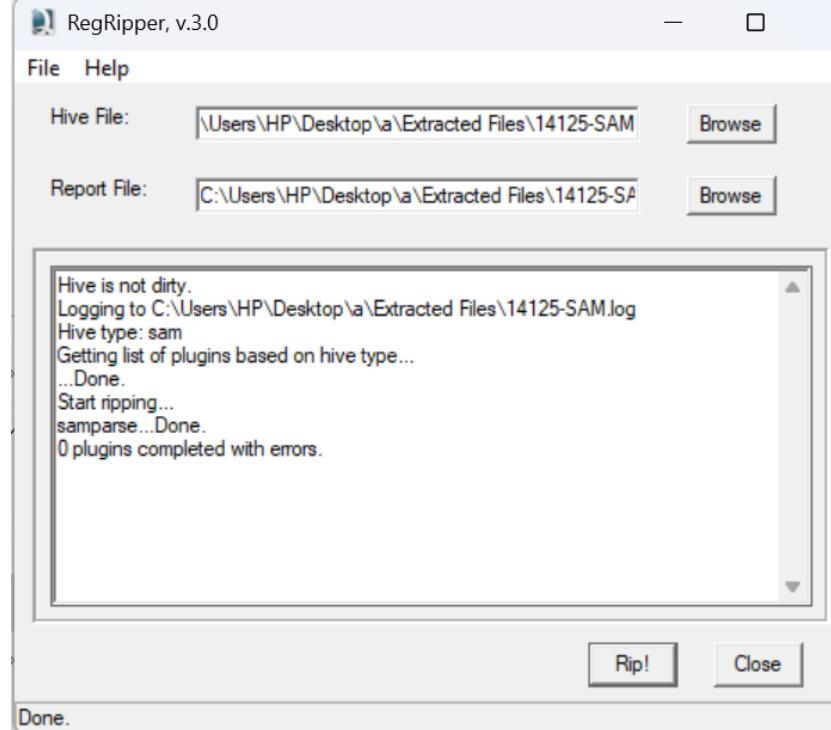
Action	Done?	Date	Time	Notes
				 <p>RegRipper, v.3.0</p> <p>Hive File: C:\Users\HP\Desktop\va\Extracted Files\14134-sot <input type="button" value="Browse"/></p> <p>Report File: C:\Users\HP\Desktop\va\Extracted Files\14134-sot <input type="button" value="Browse"/></p> <pre>Hive type: software Getting list of plugins based on hive type... ...Done. Start ripping... allowedenum...Done. appcompatflags...Done. appinitdlls...Done. appkeys...Done. apppaths...Done. at...Done. audiodev...Done. btconfig...Done. calibrator...Done.</pre> <p><input type="button" value="Rip!"/> <input type="button" value="Close"/></p> <p>calibrator complete.</p>
				 <p>RegRipper, v.3.0</p> <p>Hive File: C:\Users\HP\Desktop\va\Extracted Files\14141-sys <input type="button" value="Browse"/></p> <p>Report File: C:\Users\HP\Desktop\va\Extracted Files\14141-sys <input type="button" value="Browse"/></p> <pre>shimcache...Done. shutdown...Done. source_os...Done. svc...Done. svcdll...Done. temcert...Done. termserv...Done. timezone...Done. usb...Done. usbdevices...Done. usbstor...Done. wpdbusenum...Done. 0 plugins completed with errors.</pre> <p><input type="button" value="Rip!"/> <input type="button" value="Close"/></p> <p>Done.</p>

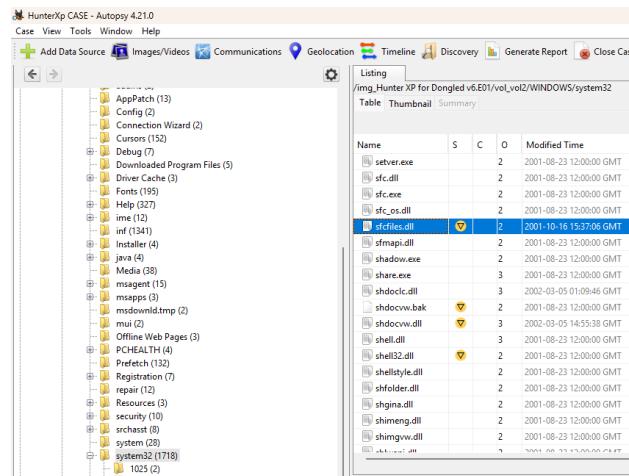
Action	Done?	Date	Time	Notes
				<p>After ripping these all files in the Reg ripper, I watched the .txt files to find Retrieve operating system information, account information, software, time zone information</p> <p>1. Operating System information:</p> <pre>----- winver v.20200525 (Software) Get Windows version &amp; 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</pre> <p>2. Accounts Information</p>

Action	Done?	Date	Time	Notes
				<pre> File   Edit   View --&gt; Account Disabled --&gt; 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 --&gt; Password does not expire --&gt; Password not required --&gt; Normal user account  3. Software  ----- winver v.20200525 (Software) Get Windows version &amp; build info  ProductName      Microsoft Windows XP BuildLab        2600.xpcnt_qfe.010827-1803 RegisteredOrganization PC User Company RegisteredOwner   PC User InstallDate     2002-02-28 22:02:39Z -----   4. Timezone </pre>

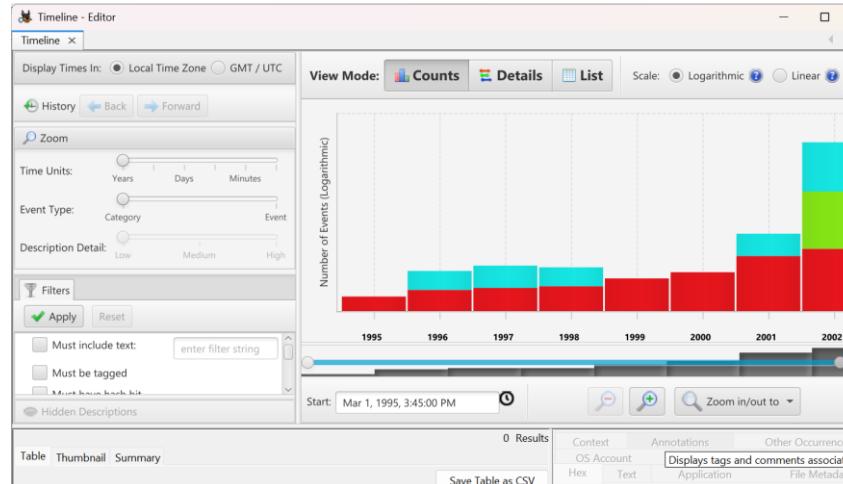
Action	Done?	Date	Time	Notes
				 <pre> 14134-software.txt 14141-system.tx X 14125-SAM.txt 14130-SECURITY.log  File Edit View UserAuthentication value not found.  WinStations\RDP-Tcp key PortNumber: 3389 Analysis Tip: By default, the port number is 3389, but can be changed. Policies\Microsoft\Windows 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 -&gt; Central Daylight Time StandardName -&gt; Central Standard Time Bias -&gt; 360 (6 hours) ActiveTimeBias -&gt; 300 (5 hours)  ----- usb v.20200515 (System) Get USB key info  Ln 3331. Col 9   8 of 158.625 characters   100% </pre>
Timeline analysis- Note date of last activity on the computer. System profiling.	Yes	20/04/2024	08:00 PM	<p><b>Step1:</b></p> <p>for timeline analysis, I have extracted SAM from the path:  <b>Path:</b>  <a href="#">\img_Hunter XP</a>  <a href="#">forDongledv6.E01/vol_vo2/WINDOWS/system32/config</a></p>

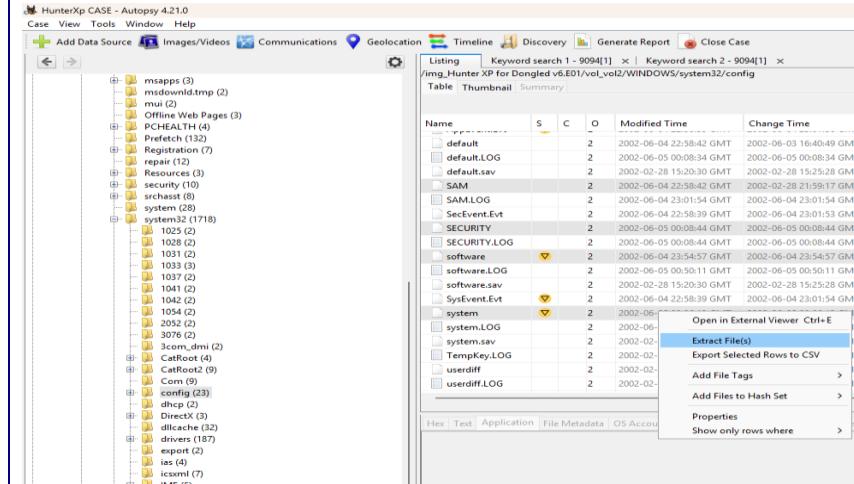
Action	Done?	Date	Time	Notes
				 <p>Step2:</p> <ul style="list-style-type: none"> <li>• After extracting SAM I ripped SAM in Reg Ripper and made <b>SAM.txt</b> file.</li> </ul>

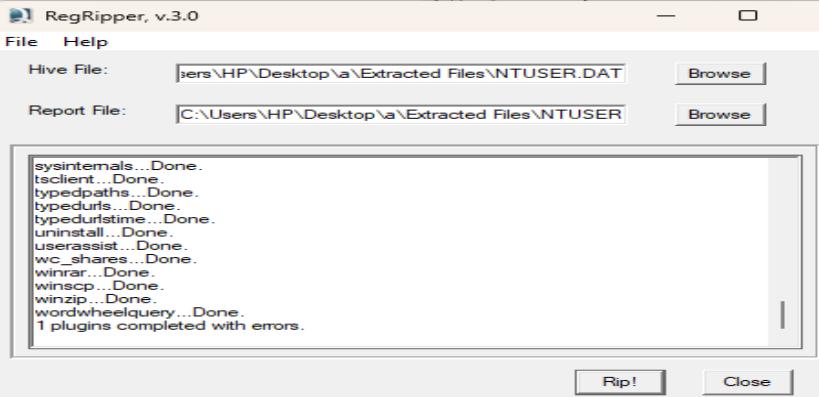
Action	Done?	Date	Time	Notes
				 <p>The screenshot shows the RegRipper v.3.0 application window. The 'File' menu is open, and the 'Hive File' field contains the path to a SAM file. The 'Report File' field is also visible. The main pane displays log messages indicating the extraction process: 'Hive is not dirty.', 'Logging to C:\Users\HP\Desktop\...\SAM.log', 'Hive type: sam', 'Getting list of plugins based on hive type...', '...Done.', 'Start ripping...', 'sampsarse...Done.', and '0 plugins completed with errors.' At the bottom, there are 'Rip!' and 'Close' buttons, and a status message 'Done.'</p> <ul style="list-style-type: none"> <li>From the SAM.txt file I got the <b>last login date of Bob Hunter.</b></li> </ul> <pre> <b>Name</b> 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 </pre>

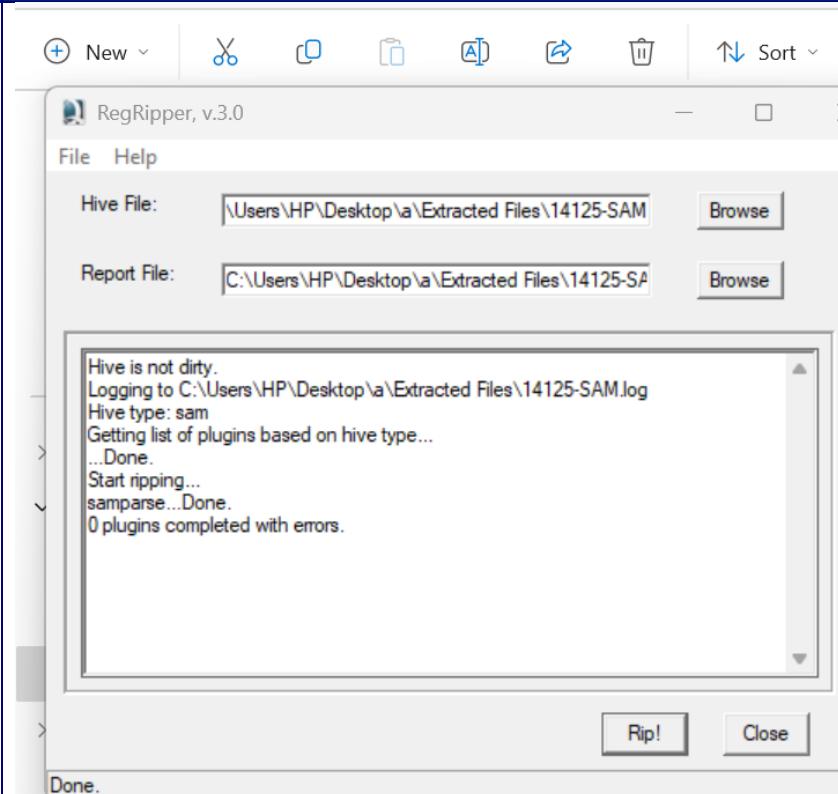
Action	Done?	Date	Time	Notes																																																																																																																																												
				<p><b>Step3:</b></p> <p>To find <b>system profiling</b> I followed the path</p> <p><b>Path:</b></p> <p><a href="#">/img_Hunter XP for Dongled</a></p> <p><a href="#">v6.E01/vol_vo12/WINDOWS/system32</a></p> <p>In system32 we found a file name sfcfiles.dll. This sfcfiles.dll contains information about the system.</p>  <table border="1"> <caption>/img_Hunter XP for Dongled v6.E01/vol_vo12/WINDOWS/system32</caption> <thead> <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> </tr> </thead> <tbody> <tr> <td>sever.exe</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-02-28 15:18:26 GMT</td> </tr> <tr> <td>sfc.dll</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-02-05 00:06:11 GMT</td> </tr> <tr> <td>sfc.exe</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-02-28 22:00:04 GMT</td> </tr> <tr> <td>sfc.os.dll</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-02-05 00:06:11 GMT</td> </tr> <tr> <td><b>sfcfiles.dll</b></td> <td>2</td> <td></td> <td></td> <td>2001-10-16 15:57:06 GMT</td> <td>2002-03-31 16:52:47 GMT</td> <td>2002-06-05 00:06:11 GMT</td> </tr> <tr> <td>sfmapi.dll</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-02-28 22:01:59 GMT</td> </tr> <tr> <td>shadow.exe</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 21:44:30 GMT</td> <td>2002-02-28 21:44:30 GMT</td> </tr> <tr> <td>shdcl.dll</td> <td>3</td> <td></td> <td></td> <td>2002-03-05 01:09:46 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-02-05 00:08:12 GMT</td> </tr> <tr> <td>share.exe</td> <td>3</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-02-28 22:01:59 GMT</td> </tr> <tr> <td>shdocvw.bak</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-03-31 16:59:58 GMT</td> <td>2002-02-05 00:08:12 GMT</td> </tr> <tr> <td>shdocvw.dll</td> <td>3</td> <td></td> <td></td> <td>2002-03-05 14:55:38 GMT</td> <td>2002-03-31 16:59:58 GMT</td> <td>2002-06-04 23:57:26 GMT</td> </tr> <tr> <td>shell.dll</td> <td>3</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-02-28 15:18:27 GMT</td> </tr> <tr> <td>shell32.dll</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-06-05 00:50:06 GMT</td> <td>2002-06-05 00:08:03 GMT</td> </tr> <tr> <td>shellstyle.dll</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-02-28 22:02:03 GMT</td> </tr> <tr> <td>shfilder.dll</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-02-05 00:05:33 GMT</td> </tr> <tr> <td>shgina.dll</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-06-04 00:12:08 GMT</td> </tr> <tr> <td>shimeng.dll</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-06-04 22:57:18 GMT</td> </tr> <tr> <td>shimgvw.dll</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-06-05 00:04:38 GMT</td> <td>2002-06-05 00:47:38 GMT</td> </tr> <tr> <td>shobj.dll</td> <td>2</td> <td></td> <td></td> <td>2001-08-23 12:00:00 GMT</td> <td>2002-02-28 15:25:27 GMT</td> <td>2002-02-05 00:08:03 GMT</td> </tr> </tbody> </table> <p>For extraction of <b>NUSTER.dat</b>, I have followed the path.</p> <p><b>Path:</b></p>	Name	S	C	O	Modified Time	Change Time	Access Time	sever.exe	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-28 15:18:26 GMT	sfc.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-05 00:06:11 GMT	sfc.exe	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-28 22:00:04 GMT	sfc.os.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-05 00:06:11 GMT	<b>sfcfiles.dll</b>	2			2001-10-16 15:57:06 GMT	2002-03-31 16:52:47 GMT	2002-06-05 00:06:11 GMT	sfmapi.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-28 22:01:59 GMT	shadow.exe	2			2001-08-23 12:00:00 GMT	2002-02-28 21:44:30 GMT	2002-02-28 21:44:30 GMT	shdcl.dll	3			2002-03-05 01:09:46 GMT	2002-02-28 15:25:27 GMT	2002-02-05 00:08:12 GMT	share.exe	3			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-28 22:01:59 GMT	shdocvw.bak	2			2001-08-23 12:00:00 GMT	2002-03-31 16:59:58 GMT	2002-02-05 00:08:12 GMT	shdocvw.dll	3			2002-03-05 14:55:38 GMT	2002-03-31 16:59:58 GMT	2002-06-04 23:57:26 GMT	shell.dll	3			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-28 15:18:27 GMT	shell32.dll	2			2001-08-23 12:00:00 GMT	2002-06-05 00:50:06 GMT	2002-06-05 00:08:03 GMT	shellstyle.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-28 22:02:03 GMT	shfilder.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-05 00:05:33 GMT	shgina.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-06-04 00:12:08 GMT	shimeng.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-06-04 22:57:18 GMT	shimgvw.dll	2			2001-08-23 12:00:00 GMT	2002-06-05 00:04:38 GMT	2002-06-05 00:47:38 GMT	shobj.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-05 00:08:03 GMT
Name	S	C	O	Modified Time	Change Time	Access Time																																																																																																																																										
sever.exe	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-28 15:18:26 GMT																																																																																																																																										
sfc.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-05 00:06:11 GMT																																																																																																																																										
sfc.exe	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-28 22:00:04 GMT																																																																																																																																										
sfc.os.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-05 00:06:11 GMT																																																																																																																																										
<b>sfcfiles.dll</b>	2			2001-10-16 15:57:06 GMT	2002-03-31 16:52:47 GMT	2002-06-05 00:06:11 GMT																																																																																																																																										
sfmapi.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-28 22:01:59 GMT																																																																																																																																										
shadow.exe	2			2001-08-23 12:00:00 GMT	2002-02-28 21:44:30 GMT	2002-02-28 21:44:30 GMT																																																																																																																																										
shdcl.dll	3			2002-03-05 01:09:46 GMT	2002-02-28 15:25:27 GMT	2002-02-05 00:08:12 GMT																																																																																																																																										
share.exe	3			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-28 22:01:59 GMT																																																																																																																																										
shdocvw.bak	2			2001-08-23 12:00:00 GMT	2002-03-31 16:59:58 GMT	2002-02-05 00:08:12 GMT																																																																																																																																										
shdocvw.dll	3			2002-03-05 14:55:38 GMT	2002-03-31 16:59:58 GMT	2002-06-04 23:57:26 GMT																																																																																																																																										
shell.dll	3			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-28 15:18:27 GMT																																																																																																																																										
shell32.dll	2			2001-08-23 12:00:00 GMT	2002-06-05 00:50:06 GMT	2002-06-05 00:08:03 GMT																																																																																																																																										
shellstyle.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-28 22:02:03 GMT																																																																																																																																										
shfilder.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-05 00:05:33 GMT																																																																																																																																										
shgina.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-06-04 00:12:08 GMT																																																																																																																																										
shimeng.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-06-04 22:57:18 GMT																																																																																																																																										
shimgvw.dll	2			2001-08-23 12:00:00 GMT	2002-06-05 00:04:38 GMT	2002-06-05 00:47:38 GMT																																																																																																																																										
shobj.dll	2			2001-08-23 12:00:00 GMT	2002-02-28 15:25:27 GMT	2002-02-05 00:08:03 GMT																																																																																																																																										

Action	Done?	Date	Time	Notes
				<p>/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter</p> <p>Step4:</p> <p>for timeline analysis <b>plaso</b> ingest module is run. Steps used for running this Module are give below.</p> <ul style="list-style-type: none"> <li>• Click on <b>Tools</b> in the toolbar.</li> <li>• Choose <b>Run ingest modules</b>.</li> <li>• Select <b>Hunter XP for Dongled v6.E01</b>.</li> </ul>

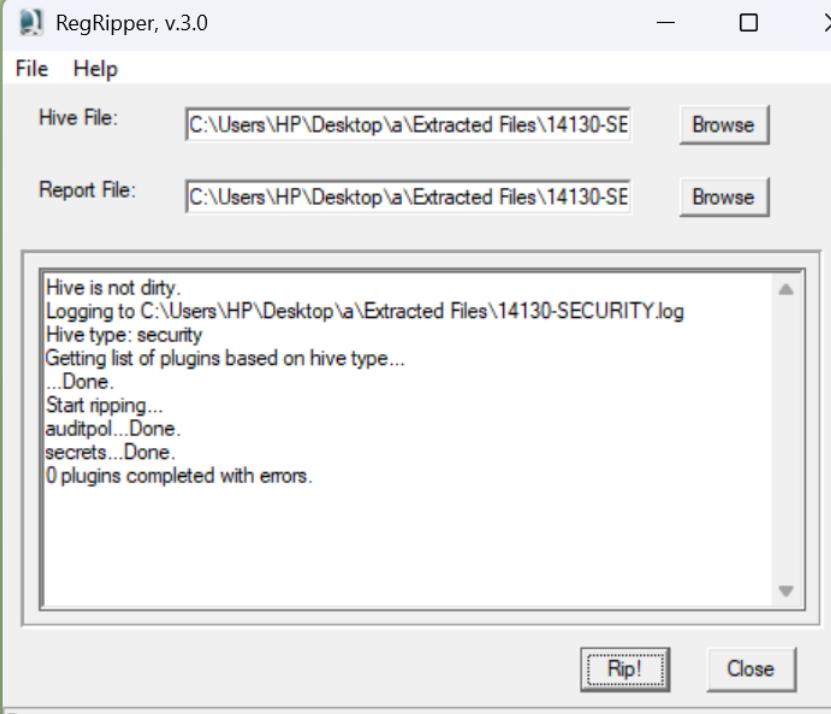
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>Picked <b>Plaso</b>.</li> <li>After running <b>plaso</b>, clicked on <b>Timeline</b> and I got timeline detail.</li> </ul> 
Registry analysis and Registry protected area	Yes	21/12/2024	12:00 PM	<p><b>Step1:</b></p> <p>For registry analysis, I have extracted <b>SAM</b>, <b>System</b>, <b>Software</b>, and security. I have also extracted the <b>NUSTER.dat</b> file for analysis of information such as:</p> <ul style="list-style-type: none"> <li>Recently accessed files</li> <li>Installed software</li> </ul>

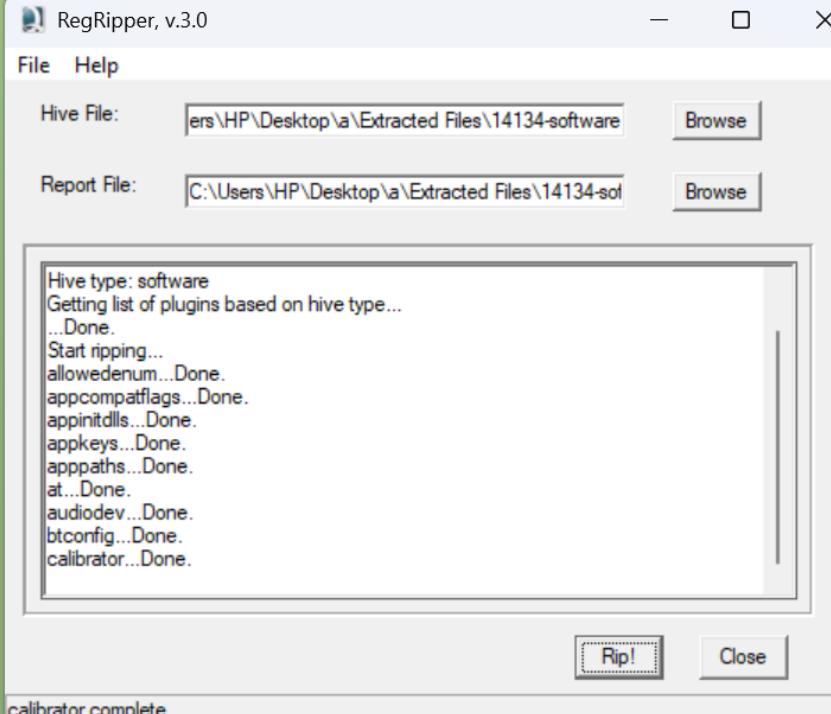
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>• User preferences</li> <li>• Typed URLs (in Internet Explorer)</li> </ul>  <p><b>Step2:</b></p> <p>After extraction of these files, I made .txt files of all files using <b>Reg Ripper</b> as I have operated for <b>Timeline analysis</b>.</p>

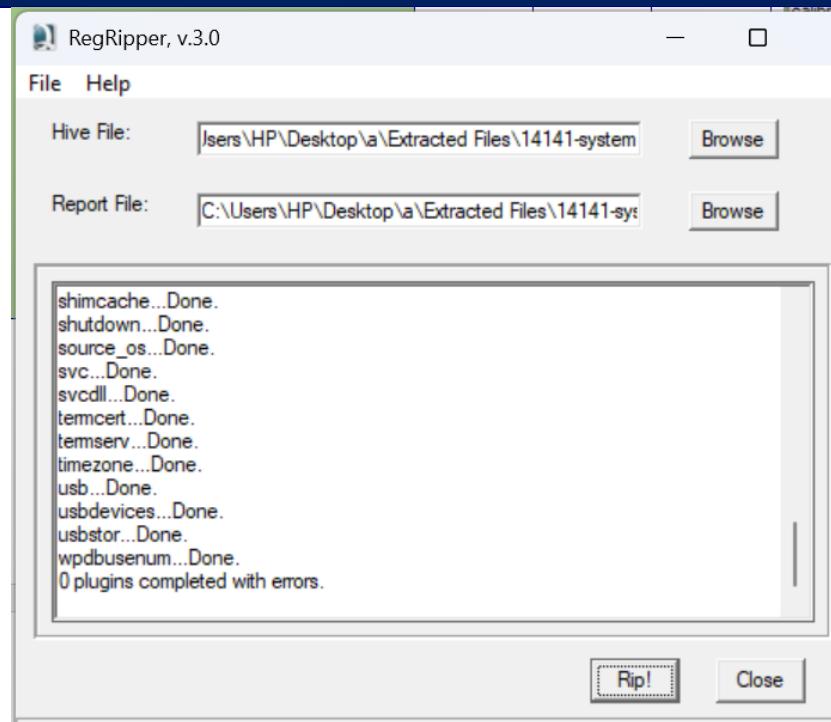
Action	Done?	Date	Time	Notes
				 <p>After ripping these all files from regripper I have analyzed SAM.txt, System.txt, Software.txt., Security.txt, and Nuster.dat.txt I found the artifacts such as:</p> <p>a. <b>SAM.:</b></p> <p>SAM.txt files contain user details and password hashes.</p>

Action	Done?	Date	Time	Notes
				 <p>The screenshot shows the RegRipper v.3.0 application window. The 'File' menu is open, showing 'RegRipper, v.3.0', 'File', and 'Help'. Below the menu, there are two input fields: 'Hive File:' containing the path '\Users\HP\Desktop\...\Extracted Files\14125-SAM' with a 'Browse' button, and 'Report File:' containing the path 'C:\Users\HP\Desktop\...\Extracted Files\14125-SA' with a 'Browse' button. A large text area displays the following log output:</p> <pre>Hive is not dirty. Logging to C:\Users\HP\Desktop\...\Extracted Files\14125-SAM.log Hive type: sam Getting list of plugins based on hive type... ...Done. Start ripping... samparse...Done. 0 plugins completed with errors.</pre> <p>At the bottom right of the window are 'Rip!' and 'Close' buttons. The status bar at the bottom shows the word 'Done.'</p>

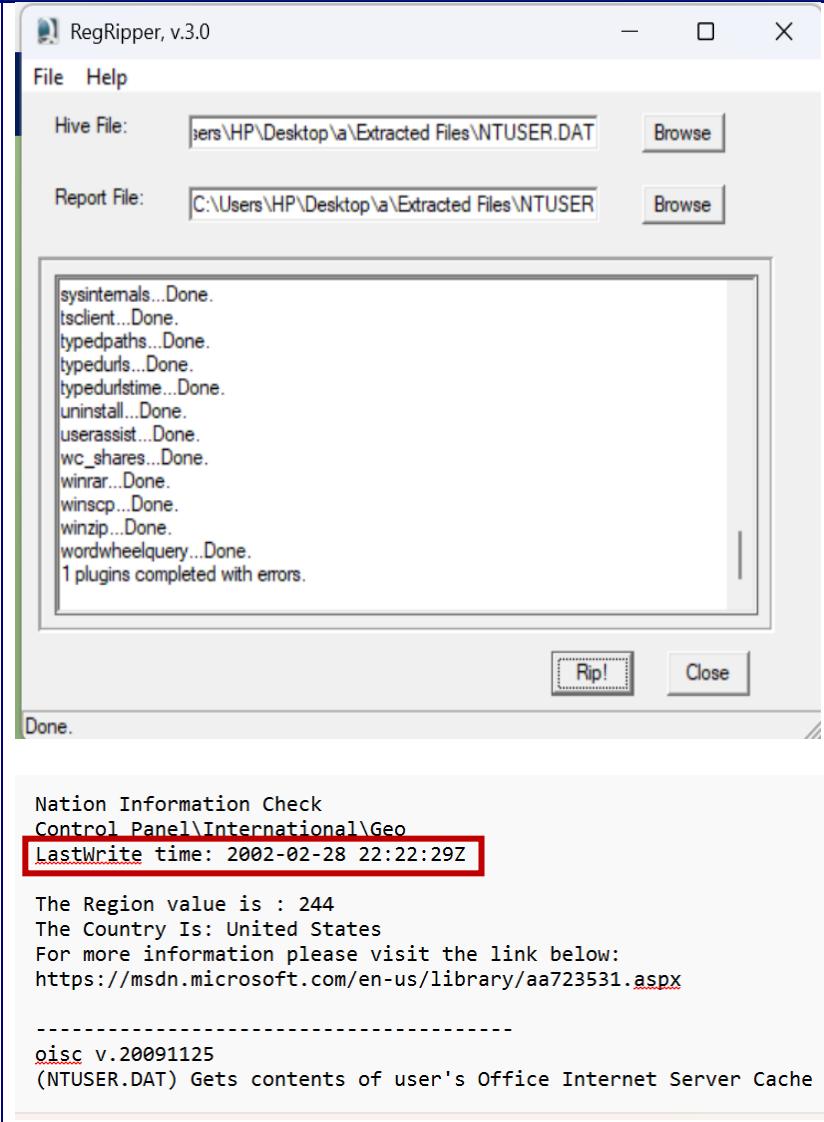
Action	Done?	Date	Time	Notes
				<pre>--&gt; Normal user account  Username      : Bob Hunter [1004] SID          : S-1-5-21-1229272821-1580818891-854245398-1004 Full Name    : User Comment  : Account Type : Default Admin User Account Created : Thu Feb 28 22:22:17 2002 Z Name         : Last Login Date : 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     --&gt; Password does not expire     --&gt; Password not required     --&gt; Normal user account  ----- b. <b>Security:</b>  <b>Security</b> is responsible for maintaining the <b>security</b> policies of the device.</pre>

Action	Done?	Date	Time	Notes
				 <p>RegRipper, v.3.0</p> <p>Hive File: C:\Users\HP\Desktop\va\Extracted Files\14130-SE <input type="button" value="Browse"/></p> <p>Report File: C:\Users\HP\Desktop\va\Extracted Files\14130-SE <input type="button" value="Browse"/></p> <pre>Hive is not dirty. Logging to C:\Users\HP\Desktop\va\Extracted Files\14130-SECURITY.log Hive type: security Getting list of plugins based on hive type... ...Done. Start ripping... auditpol...Done. secrets...Done. 0 plugins completed with errors.</pre> <p>Rip! <input type="button" value="Close"/></p> <p>Done.</p> <p>c. <b>Software:</b></p> <p>All the installed programs, software settings, and program of versions are recorded by the <b>Software</b>.</p>

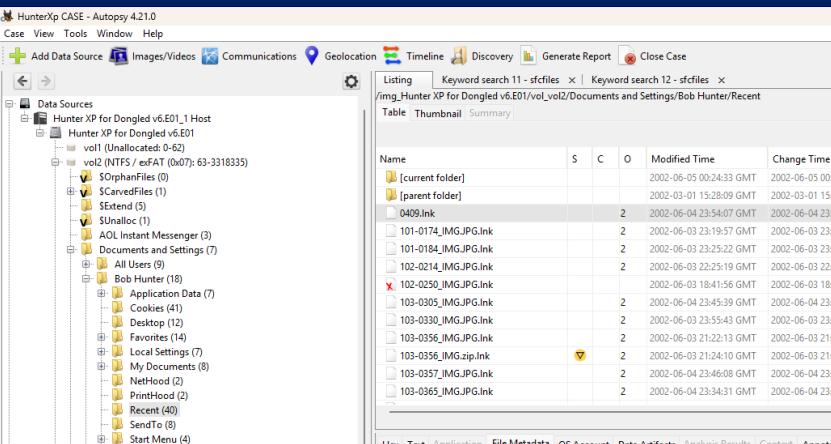
Action	Done?	Date	Time	Notes
				 <p>RegRipper, v.3.0</p> <p>Hive File: C:\Users\HP\Desktop\...\Extracted Files\14134-software</p> <p>Report File: C:\Users\HP\Desktop\...\Extracted Files\14134-software</p> <p>Hive type: software      Getting list of plugins based on hive type...      ...Done.      Start ripping...      allowedenum...Done.      appcompatflags...Done.      appinitdlls...Done.      appkeys...Done.      apppaths...Done.      at...Done.      audiodev...Done.      btconfig...Done.      calibrator...Done.</p> <p>Rip! Close</p> <p>calibrator complete.</p> <p>d. System:      All information about the hardware and configuration of the device is managed by the system.</p>

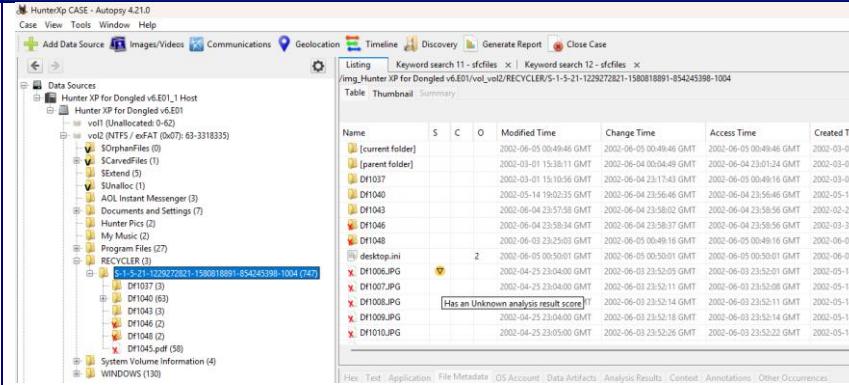
Action	Done?	Date	Time	Notes
				 <p>RegRipper, v.3.0</p> <p>File Help</p> <p>Hive File: Isers\HP\Desktop\...\Extracted Files\14141-system <input type="button" value="Browse"/></p> <p>Report File: C:\Users\HP\Desktop\...\Extracted Files\14141-sy... <input type="button" value="Browse"/></p> <pre>shimcache...Done. shutdown...Done. source_os...Done. svc...Done. svcdll...Done. termcert...Done. termserv...Done. timezone...Done. usb...Done. usbdevices...Done. usbstor...Done. wpdbusenum...Done. 0 plugins completed with errors.</pre> <p>Rip! <input type="button" value="Close"/></p> <p>Done.</p>

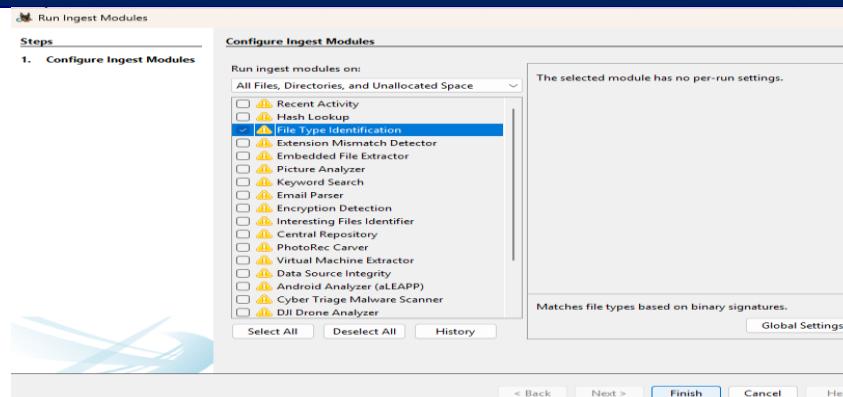
Action	Done?	Date	Time	Notes
				<pre> -----  winver v.20200525  (Software) Get Windows version &amp; build info    ProductName Microsoft Windows XP  BuildLab 2600.xpclnt_qfe.010827-  RegisteredOrganization PC User Company  RegisteredOwner PC User  InstallDate 2002-02-28 22:02:39Z  -----  wow64 v.20200515  (Software) Gets contents of WOW64\x86 key </pre> <p>e. <b>NUSTER.dat:</b></p> <p>It contains user-specific settings and preferences, including desktop and application configurations. And contains information about installed software and URLs.</p>

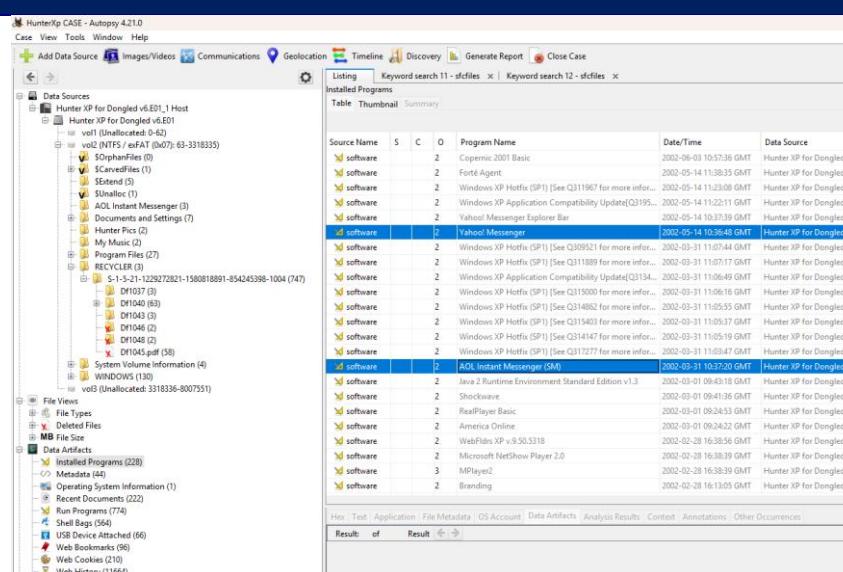
Action	Done?	Date	Time	Notes
				 <p>RegRipper, v.3.0</p> <p>Hive File: C:\Users\HP\Desktop\...\Extracted Files\NTUSER.DAT Browse</p> <p>Report File: C:\Users\HP\Desktop\...\Extracted Files\NTUSER Browse</p> <pre>sysinternals...Done. tsclient...Done. typedpaths...Done. typedurls...Done. typedurstime...Done. uninstall...Done. userassist...Done. wc_shares...Done. winrar...Done. winscp...Done. winzip...Done. wordwheelquery...Done. 1 plugins completed with errors.</pre> <p>Rip! Close</p> <p>Done.</p> <p>Nation Information Check Control Panel\International\Geo LastWrite time: 2002-02-28 22:22:29Z</p> <p>The Region value is : 244 The Country Is: United States For more information please visit the link below: <a href="https://msdn.microsoft.com/en-us/library/aa723531.aspx">https://msdn.microsoft.com/en-us/library/aa723531.aspx</a></p> <p>----- oisc v.20091125 (NTUSER.DAT) Gets contents of user's Office Internet Server Cache</p>

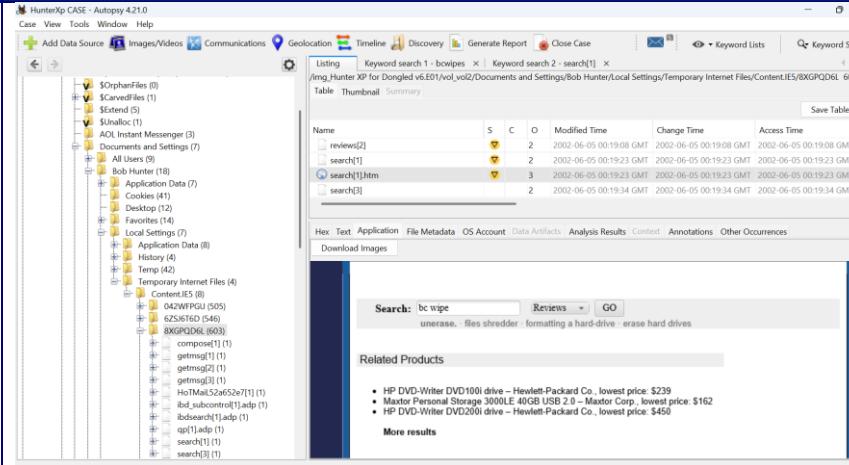
Action	Done?	Date	Time	Notes
Link files and Recycle Bin	YES	21/12/2024	12:25 PM	<p><b><u>Step1:</u></b></p> <p>To find link files i followed the path;</p> <p>Path:</p> <p><a href="/img_Hunter XP for Dongled v6.E01/vol_vo2/Documents and Settings/Bob Hunter/Recent">/img_Hunter XP for Dongled v6.E01/vol_vo2/Documents and Settings/Bob Hunter/Recent</a></p> <p>I followed the given path for the analysis of linked files.</p> <p>➤ After following this path, I found that there were <b>40 link</b> files with extension <b>.lnk</b> which was created by <b>BOB HUNTER.</b></p>

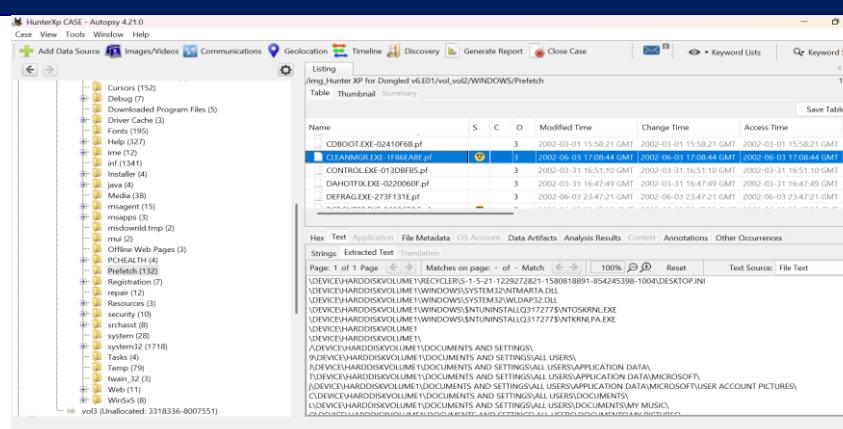
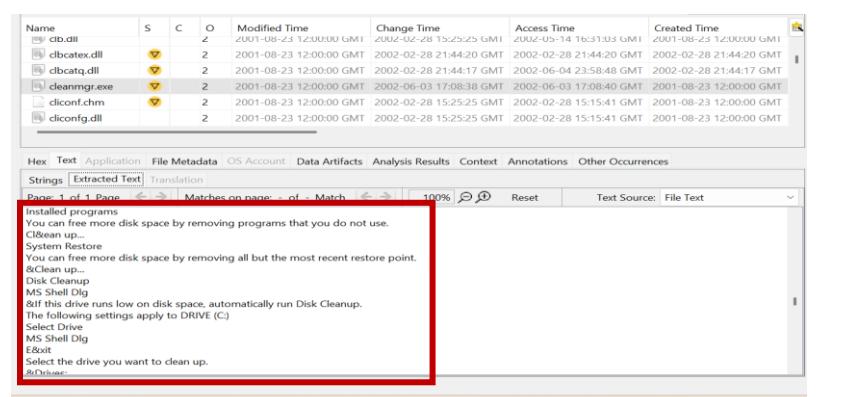
Action	Done?	Date	Time	Notes
				 <p><b>Step2:</b></p> <p>After analysis of the <b>link files</b>, I proceed with the analysis of the <b>Recycle Bin</b>. To analyze the <b>recycle bin</b> I followed the path;</p> <p>Path: <a href="#">/img_Hunter XP for Dongled/v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004</a></p>

Action	Done?	Date	Time	Notes
				
Instant Messaging clients	YES	21/12/2024	12:40 PM	<p><b>Step1:</b></p> <p>To find instant messaging clients I ran the ingest module and followed the steps:</p> <ul style="list-style-type: none"> <li>➤ Clicked on <b>tools</b></li> <li>➤ Chose <b>Run Ingest Module</b></li> <li>➤ Selected <b>Hunter XP for Dongled v6.E01</b>.</li> <li>➤ Picked <b>file type identification</b>.</li> </ul>

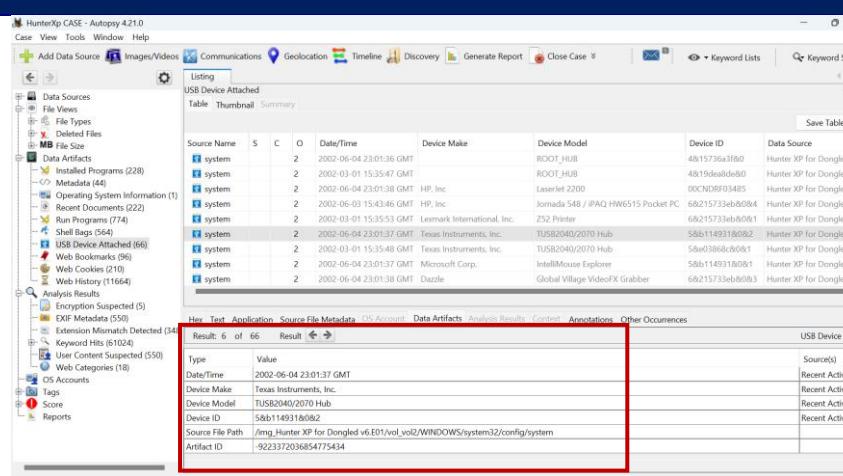
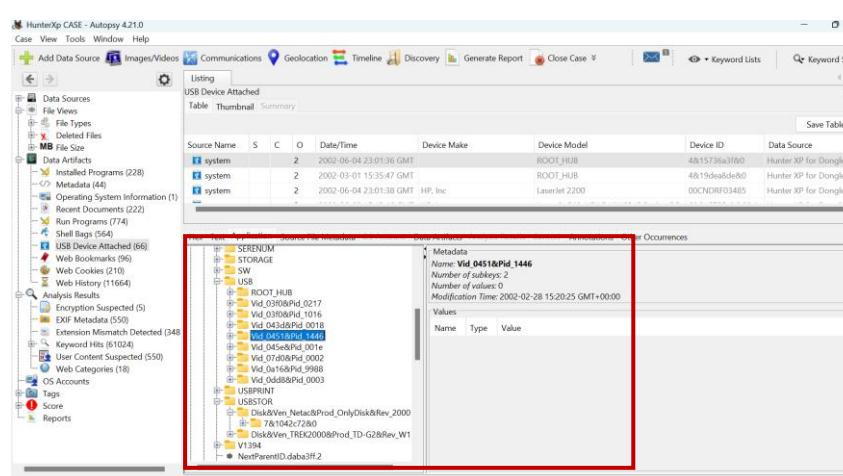
Action	Done?	Date	Time	Notes
				 <p><b>Step2:</b></p> <p>After finishing this process.</p> <ul style="list-style-type: none"> <li>➤ I clicked on data artifacts and found installed Programs.</li> <li>➤ I clicked on installed programs and found that there were only two instant messaging apps used.             <ul style="list-style-type: none"> <li>a. <b>Yahoo messenger</b></li> <li>b. <b>AOL Instant Messenger</b></li> </ul> </li> </ul>

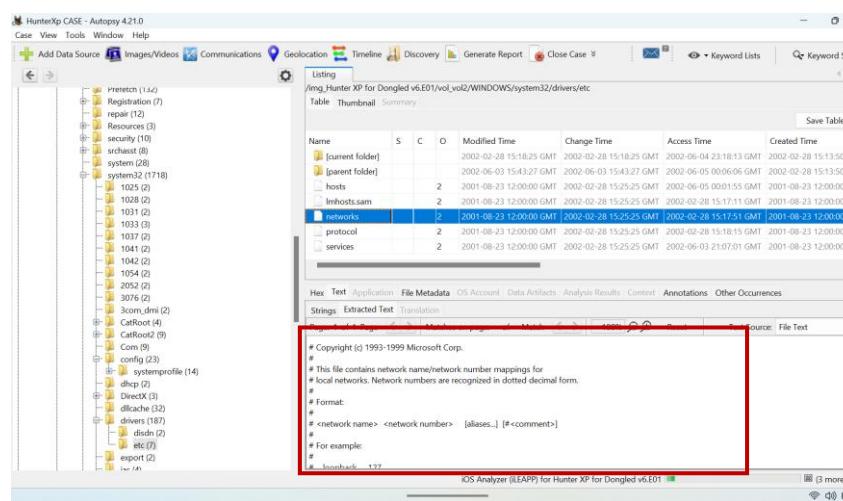
Action	Done?	Date	Time	Notes
				
Clean-up/Wiping utilities. Check log files. Anything used?	YES	21/12/2024	01:00 PM	<p>Clean-up and wiping activities are done in the given evidence file. I found the clean-up and wiping utilities artifacts are found in website search, .exe file and .pf file was executed.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

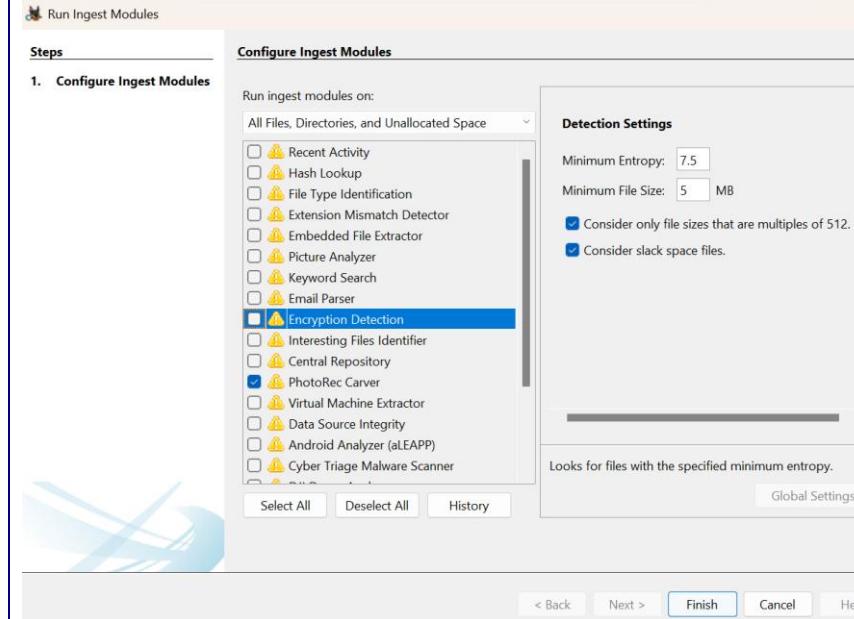
Action	Done?	Date	Time	Notes
				 <p><b>Step2:</b></p> <p>I found that cleanmgr.exe file is in the system32 folder and traces of this file execution is also stored in the prefetch folder cleanmgr.exe....pf.</p> <p>Path browsed to find prefetch file is given below:</p> <p>Path:</p> <p>/img_Hunter XP for Dongled v6.E01/vol_vo2/WINDOWS/Prefetch/CLEANMGR.EXE-1F86EA8E.pf</p>

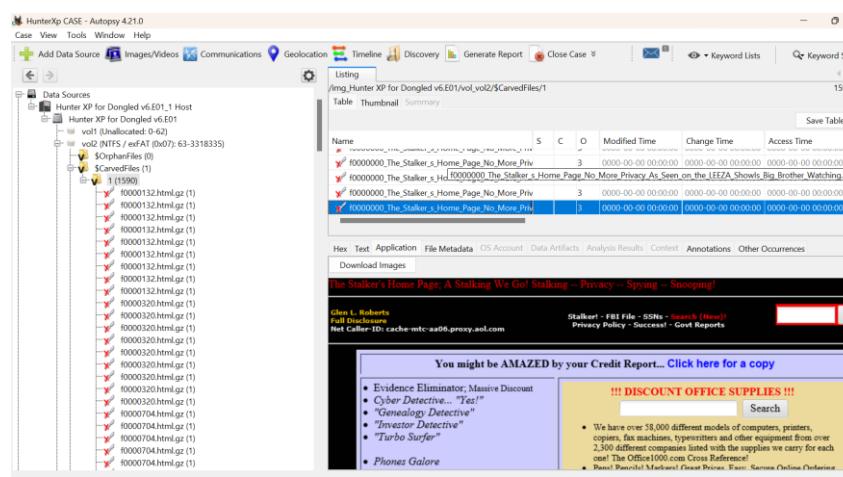
Action	Done?	Date	Time	Notes
				 <p>To find the cleanmgr.exe file I browsed the path:</p> <p>/img_Hunter XP for Dongled v6.E01/vol.vol2/WINDOWS/system32</p>  <pre> cleanmgr.exe ===== You can free more disk space by removing programs that you do not use. Clean up... System Restore You can free more disk space by removing all but the most recent restore point. &amp;Clean up... Disk Cleanup MS Shell Dlg If this drive runs low on disk space, automatically run Disk Cleanup. The following settings apply to DRIVE (C) Select Drive MS Shell Dlg [...] Select the drive you want to clean up. &amp;Ok[...] </pre>

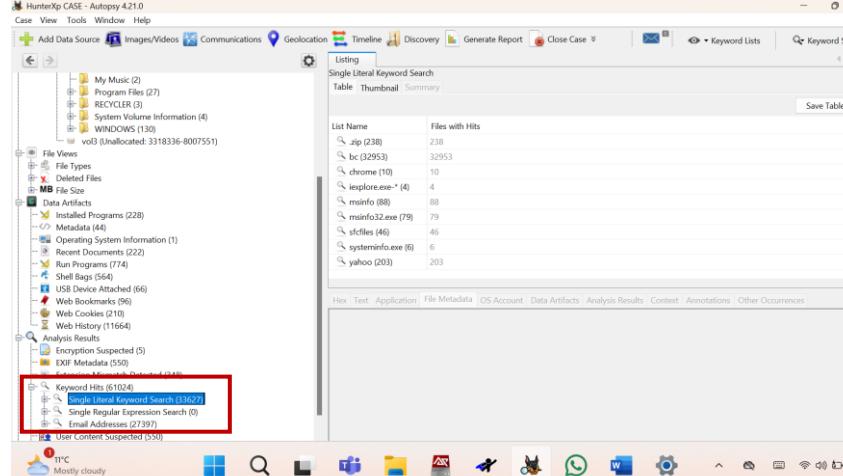
Action	Done?	Date	Time	Notes
External drives; Network connections	Yes	21/12/2024	03:00 PM	<p>To find whether external drives were used in <b>Hunter XP for Dongled v6.E01</b>, follow these steps:</p> <ol style="list-style-type: none"> <li>1. Open <b>Hunter XP</b> and load the <b>Dongled v6.E01</b> image.</li> <li>2. Navigate to <b>System Artifacts &gt; USB Device Attached</b></li> <li>3. Also Analyzed the registry entries under <b>SYSTEM &gt; CurrentControlSet &gt; Enum &gt; USBSTOR</b>.</li> </ol> <p><b>Step2:</b></p> <p>I followed the following path to find <b>External drive artifacts</b> is;</p> <p>Path:</p> <p><a href="#">/img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/config</a></p>

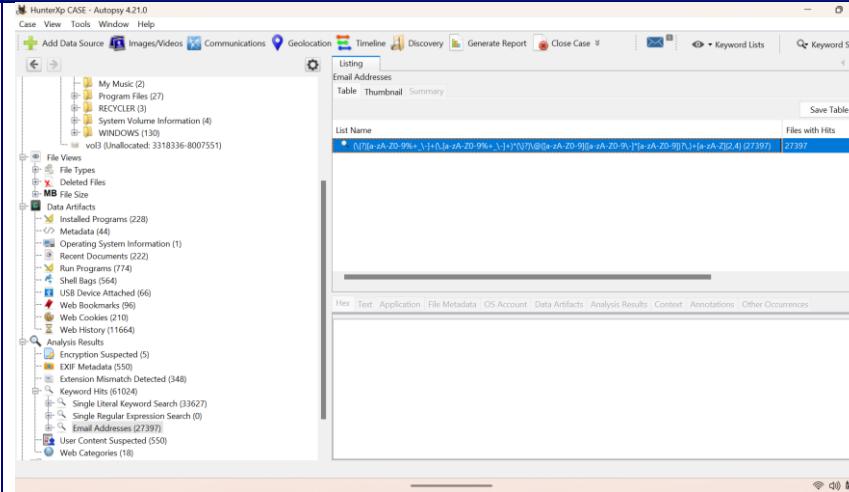
Action	Done?	Date	Time	Notes																																																																																										
				 <p>HunterXP CASE - Autopsy 4.21.0</p> <p>Case View Tools Window Help</p> <p>Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search</p> <p>USB Device Attached</p> <p>Listing Table Thumbnail Summary</p> <table border="1"> <thead> <tr> <th>Source Name</th> <th>S</th> <th>C</th> <th>O</th> <th>Date/Time</th> <th>Device Make</th> <th>Device Model</th> <th>Device ID</th> <th>Data Source</th> </tr> </thead> <tbody> <tr><td>system</td><td>2</td><td></td><td></td><td>2002-06-04 23:01:36 GMT</td><td>ROOT_HUB</td><td>ROOT_HUB</td><td>4b15733e3f80</td><td>Hunter XP for Dongled</td></tr> <tr><td>system</td><td>2</td><td></td><td></td><td>2002-03-01 15:35:47 GMT</td><td></td><td></td><td>4b15d6a0de00</td><td>Hunter XP for Dongled</td></tr> <tr><td>system</td><td>2</td><td></td><td></td><td>2002-06-04 23:01:38 GMT</td><td>HP, Inc.</td><td>LaserJet 2200</td><td>00CNDRF034B5</td><td>Hunter XP for Dongled</td></tr> <tr><td>system</td><td>2</td><td></td><td></td><td>2002-06-03 15:43:46 GMT</td><td>HP, Inc.</td><td>Jornada 548 / iPAQ HW6515 Pocket PC</td><td>68215733eb0b084</td><td>Hunter XP for Dongled</td></tr> <tr><td>system</td><td>2</td><td></td><td></td><td>2002-03-01 15:35:53 GMT</td><td>Leimark International, Inc.</td><td>Z52 Printer</td><td>68215733eb0b091</td><td>Hunter XP for Dongled</td></tr> <tr><td>system</td><td>2</td><td></td><td></td><td>2002-06-04 23:01:37 GMT</td><td>Texas Instruments, Inc.</td><td>TUSB2040/2070 Hub</td><td>56b11493186582</td><td>Hunter XP for Dongled</td></tr> <tr><td>system</td><td>2</td><td></td><td></td><td>2002-03-01 15:35:40 GMT</td><td>Texas Instruments, Inc.</td><td>TUSB2040/2070 Hub</td><td>56b03366b8081</td><td>Hunter XP for Dongled</td></tr> <tr><td>system</td><td>2</td><td></td><td></td><td>2002-06-04 23:01:37 GMT</td><td>Microsoft Corp.</td><td>Intellimouse Explorer</td><td>56b11493186801</td><td>Hunter XP for Dongled</td></tr> <tr><td>system</td><td>2</td><td></td><td></td><td>2002-06-04 23:01:38 GMT</td><td>Dazzle</td><td>Global Village VideoFX Grabber</td><td>6b215733eb0b093</td><td>Hunter XP for Dongled</td></tr> </tbody> </table> <p>Result 6 of 66 Result ⏪ ⏩</p> <p>USB Device Attached</p> <p>Type Value</p> <p>Date/Time 2002-06-04 23:01:37 GMT</p> <p>Device Make Texas Instruments, Inc.</p> <p>Device Model TUSB2040/2070 Hub</p> <p>Device ID 56b11493186582</p> <p>Source File Path /img/Hunter_XP_for_Dongled.v6.E01/vol.vol2/WINDOWS/system32/config/system</p> <p>Artifact ID 9233720368547575434</p>	Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source	system	2			2002-06-04 23:01:36 GMT	ROOT_HUB	ROOT_HUB	4b15733e3f80	Hunter XP for Dongled	system	2			2002-03-01 15:35:47 GMT			4b15d6a0de00	Hunter XP for Dongled	system	2			2002-06-04 23:01:38 GMT	HP, Inc.	LaserJet 2200	00CNDRF034B5	Hunter XP for Dongled	system	2			2002-06-03 15:43:46 GMT	HP, Inc.	Jornada 548 / iPAQ HW6515 Pocket PC	68215733eb0b084	Hunter XP for Dongled	system	2			2002-03-01 15:35:53 GMT	Leimark International, Inc.	Z52 Printer	68215733eb0b091	Hunter XP for Dongled	system	2			2002-06-04 23:01:37 GMT	Texas Instruments, Inc.	TUSB2040/2070 Hub	56b11493186582	Hunter XP for Dongled	system	2			2002-03-01 15:35:40 GMT	Texas Instruments, Inc.	TUSB2040/2070 Hub	56b03366b8081	Hunter XP for Dongled	system	2			2002-06-04 23:01:37 GMT	Microsoft Corp.	Intellimouse Explorer	56b11493186801	Hunter XP for Dongled	system	2			2002-06-04 23:01:38 GMT	Dazzle	Global Village VideoFX Grabber	6b215733eb0b093	Hunter XP for Dongled
Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source																																																																																						
system	2			2002-06-04 23:01:36 GMT	ROOT_HUB	ROOT_HUB	4b15733e3f80	Hunter XP for Dongled																																																																																						
system	2			2002-03-01 15:35:47 GMT			4b15d6a0de00	Hunter XP for Dongled																																																																																						
system	2			2002-06-04 23:01:38 GMT	HP, Inc.	LaserJet 2200	00CNDRF034B5	Hunter XP for Dongled																																																																																						
system	2			2002-06-03 15:43:46 GMT	HP, Inc.	Jornada 548 / iPAQ HW6515 Pocket PC	68215733eb0b084	Hunter XP for Dongled																																																																																						
system	2			2002-03-01 15:35:53 GMT	Leimark International, Inc.	Z52 Printer	68215733eb0b091	Hunter XP for Dongled																																																																																						
system	2			2002-06-04 23:01:37 GMT	Texas Instruments, Inc.	TUSB2040/2070 Hub	56b11493186582	Hunter XP for Dongled																																																																																						
system	2			2002-03-01 15:35:40 GMT	Texas Instruments, Inc.	TUSB2040/2070 Hub	56b03366b8081	Hunter XP for Dongled																																																																																						
system	2			2002-06-04 23:01:37 GMT	Microsoft Corp.	Intellimouse Explorer	56b11493186801	Hunter XP for Dongled																																																																																						
system	2			2002-06-04 23:01:38 GMT	Dazzle	Global Village VideoFX Grabber	6b215733eb0b093	Hunter XP for Dongled																																																																																						
				 <p>HunterXP CASE - Autopsy 4.21.0</p> <p>Case View Tools Window Help</p> <p>Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search</p> <p>USB Device Attached</p> <p>Listing Table Thumbnail Summary</p> <table border="1"> <thead> <tr> <th>Source Name</th> <th>S</th> <th>C</th> <th>O</th> <th>Date/Time</th> <th>Device Make</th> <th>Device Model</th> <th>Device ID</th> <th>Data Source</th> </tr> </thead> <tbody> <tr><td>system</td><td>2</td><td></td><td></td><td>2002-06-04 23:01:36 GMT</td><td>ROOT_HUB</td><td>ROOT_HUB</td><td>4b15733e3f80</td><td>Hunter XP for Dongled</td></tr> <tr><td>system</td><td>2</td><td></td><td></td><td>2002-03-01 15:35:47 GMT</td><td></td><td></td><td>4b15d6a0de00</td><td>Hunter XP for Dongled</td></tr> <tr><td>system</td><td>2</td><td></td><td></td><td>2002-06-04 23:01:38 GMT</td><td>HP, Inc.</td><td>LaserJet 2200</td><td>00CNDRF034B5</td><td>Hunter XP for Dongled</td></tr> </tbody> </table> <p>Result 6 of 66 Result ⏪ ⏩</p> <p>USB Device Attached</p> <p>Name: Vid_0451&amp;Pid_1446</p> <p>Number of subjects: 2</p> <p>Number of values: 0</p> <p>Modification Time: 2002-02-28 15:20:25 GMT+00:00</p> <p>Values</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr><td>Vid_0451&amp;Pid_1446</td><td></td><td></td></tr> <tr><td>Vid_0300&amp;Pid_0317</td><td></td><td></td></tr> <tr><td>Vid_0451&amp;Pid_1116</td><td></td><td></td></tr> <tr><td>Vid_0451&amp;Pid_0018</td><td></td><td></td></tr> <tr><td>Vid_0451&amp;Pid_1440</td><td></td><td></td></tr> <tr><td>Vid_0451&amp;Pid_001e</td><td></td><td></td></tr> <tr><td>Vid_0700&amp;Pid_0002</td><td></td><td></td></tr> <tr><td>Vid_0451&amp;Pid_0009</td><td></td><td></td></tr> <tr><td>Vid_0451&amp;Pid_0003</td><td></td><td></td></tr> <tr><td>USBPRINT</td><td></td><td></td></tr> <tr><td>USBSTOR</td><td></td><td></td></tr> <tr><td>Disk\Ven_NetgearProd_OnlyDisk&amp;Rev_2000</td><td></td><td></td></tr> <tr><td>781042c7280</td><td></td><td></td></tr> <tr><td>Disk&amp;Ven_TREK20008\Prod_TD-G2&amp;Rev_W1</td><td></td><td></td></tr> <tr><td>V1394</td><td></td><td></td></tr> <tr><td>NewParentID:dbba3ff2</td><td></td><td></td></tr> </tbody> </table> <p>For Network Connection:</p>	Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source	system	2			2002-06-04 23:01:36 GMT	ROOT_HUB	ROOT_HUB	4b15733e3f80	Hunter XP for Dongled	system	2			2002-03-01 15:35:47 GMT			4b15d6a0de00	Hunter XP for Dongled	system	2			2002-06-04 23:01:38 GMT	HP, Inc.	LaserJet 2200	00CNDRF034B5	Hunter XP for Dongled	Name	Type	Value	Vid_0451&Pid_1446			Vid_0300&Pid_0317			Vid_0451&Pid_1116			Vid_0451&Pid_0018			Vid_0451&Pid_1440			Vid_0451&Pid_001e			Vid_0700&Pid_0002			Vid_0451&Pid_0009			Vid_0451&Pid_0003			USBPRINT			USBSTOR			Disk\Ven_NetgearProd_OnlyDisk&Rev_2000			781042c7280			Disk&Ven_TREK20008\Prod_TD-G2&Rev_W1			V1394			NewParentID:dbba3ff2					
Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source																																																																																						
system	2			2002-06-04 23:01:36 GMT	ROOT_HUB	ROOT_HUB	4b15733e3f80	Hunter XP for Dongled																																																																																						
system	2			2002-03-01 15:35:47 GMT			4b15d6a0de00	Hunter XP for Dongled																																																																																						
system	2			2002-06-04 23:01:38 GMT	HP, Inc.	LaserJet 2200	00CNDRF034B5	Hunter XP for Dongled																																																																																						
Name	Type	Value																																																																																												
Vid_0451&Pid_1446																																																																																														
Vid_0300&Pid_0317																																																																																														
Vid_0451&Pid_1116																																																																																														
Vid_0451&Pid_0018																																																																																														
Vid_0451&Pid_1440																																																																																														
Vid_0451&Pid_001e																																																																																														
Vid_0700&Pid_0002																																																																																														
Vid_0451&Pid_0009																																																																																														
Vid_0451&Pid_0003																																																																																														
USBPRINT																																																																																														
USBSTOR																																																																																														
Disk\Ven_NetgearProd_OnlyDisk&Rev_2000																																																																																														
781042c7280																																																																																														
Disk&Ven_TREK20008\Prod_TD-G2&Rev_W1																																																																																														
V1394																																																																																														
NewParentID:dbba3ff2																																																																																														

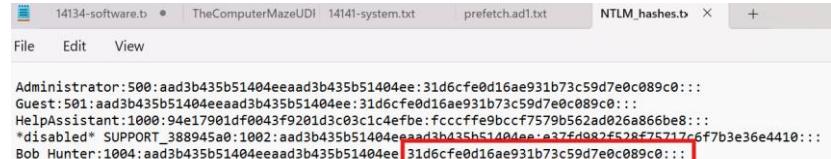
Action	Done?	Date	Time	Notes
				<p>To find the network connection used in <b>Hunter XP</b> for <b>Dongled v6.E01</b>, I have followed the path given below;</p> <p>Path:</p> <p><a href="#">/img_Hunter XP for Dongled v6.E01/vol_vo2/WINDOWS/system32/drivers/etc</a></p>  <p>after analyzing the files etc I found that the user used <b>TCP/IP</b> protocol and his file contains the Internet protocols as defined by RFC 1700.</p>

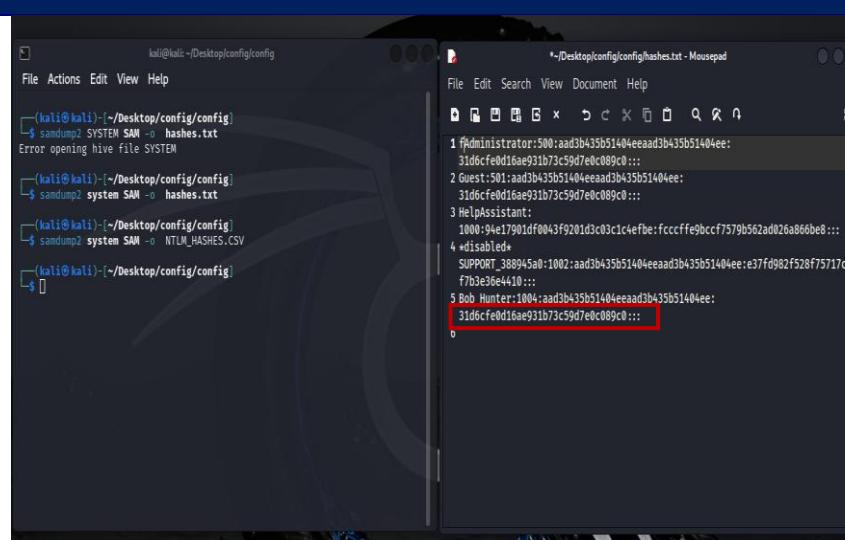
Action	Done?	Date	Time	Notes
Perform data carving	Yes	21/12/2024	03:40 PM	<p><b>Step1:</b></p> <p>To find instant messaging clients, I used the <b>run ingest module</b> and followed the steps such as:</p> <ul style="list-style-type: none"> <li>➤ Clicked on <b>tools</b></li> <li>➤ Chose <b>Run Ingest Module</b></li> <li>➤ Selected <b>Hunter XP for Dongled v6.E01.</b></li> <li>➤ Picked <b>photo rec carver.</b></li> </ul> 

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

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

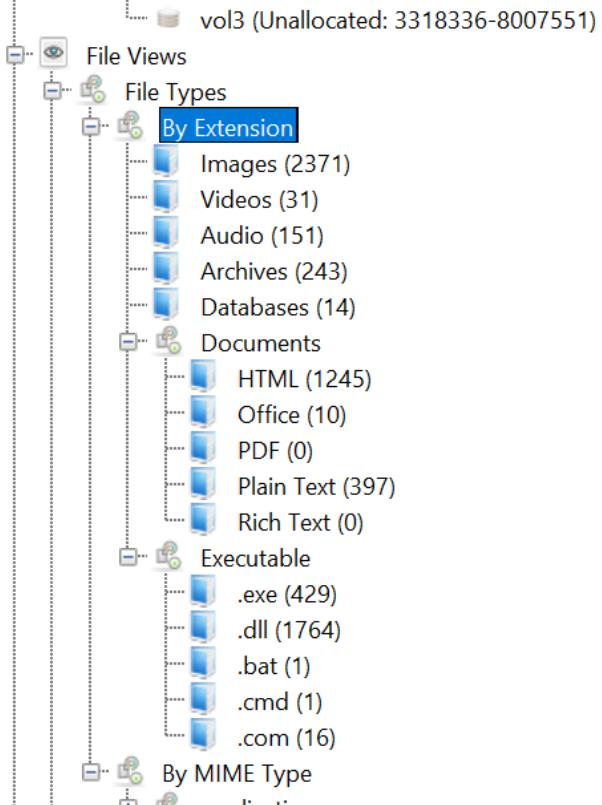
Action	Done?	Date	Time	Notes
				
Recover Log-on passwords – use SAMInside/Ophcrack/Encase	Yes	21/12/2024	04:50 PM	<p>To recover Password <b>SAM</b> and <b>System</b> is extracted from the Config folder. To explore Config folder I followed the path given below.</p> <p>Path:</p> <p><a href="#">/img_Hunter XP for Dongled v6.E01/vol.vol2/WINDOWS/system32/config</a></p> <p><b>Step2:</b></p> <p>After extracting <b>SAM</b> and <b>System</b> file, it is transferred to linux file.</p>

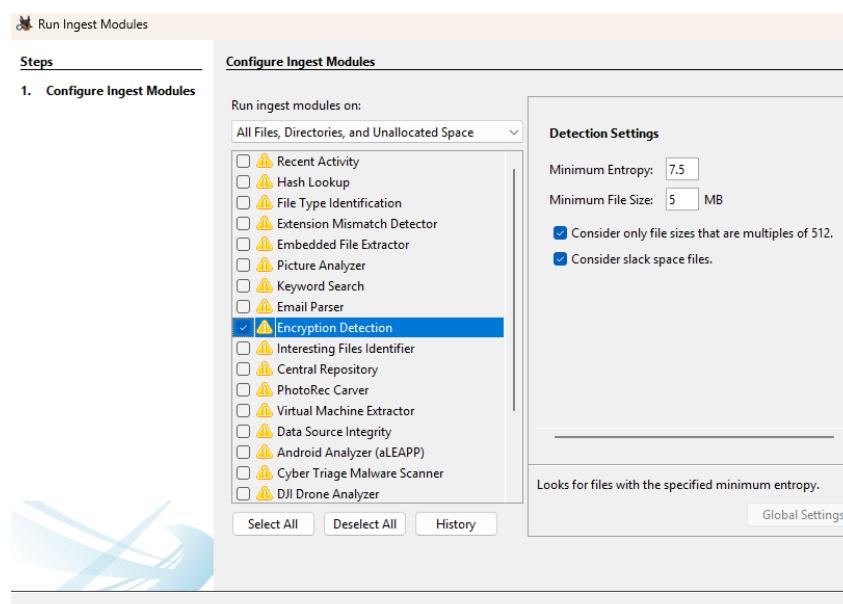
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>• In linux I used <b>Samdump2</b> tool to extract <b>NTLM_Hashes</b> of the <b>users</b>.</li> <li>• Then, I Copied <b>samdump2</b> tool source code from <b>Github</b>.</li> <li>• <b>Clonned</b> the source in the linux terminal</li> <li>• <b>After cloning</b> I opened terminal where I kept Sam and system File run the command to get .txt file of <b>NTLM_Hashes</b>.</li> </ul> <p><b>Command:</b></p> <pre>Samdump2 system SAM -o NTLM_Hashes.txt</pre> <pre>Samdump2 system SAM -o NTLM_Hashes.csv</pre> <p>And got all users <b>NTLM_Hashes</b> in the text file.</p>  <pre> Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: HelpAssistant:1000:94e17901df0043f9201d3c03c1c4efbe:fccffe9bccf7579b562ad026a866be8::: *disabled* SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:a37fd082ff528f755717c6f7b3e36e4410::: Bob Hunter:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: </pre>

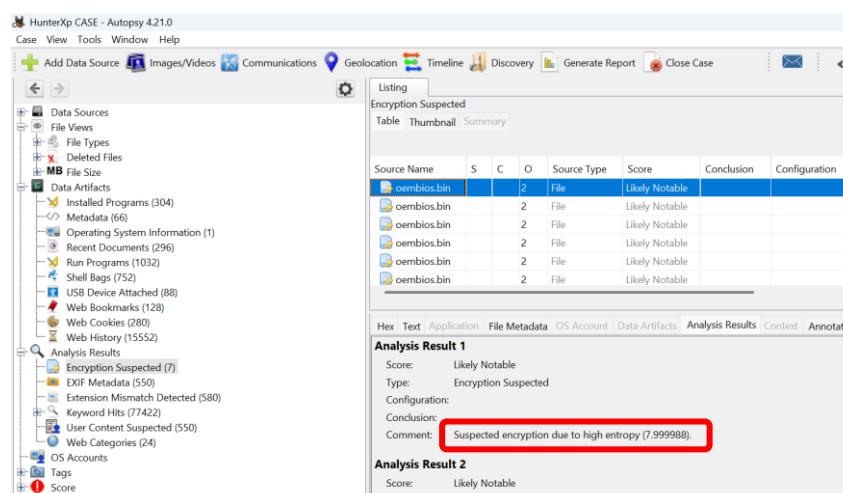
Action	Done?	Date	Time	Notes
				 <p>The <b>NTLM_hash</b> value of <b>BOB Hunter</b> is  <b>31d6cf0d16ae931b73c59d7e0c089c0</b>  It means there is <b>not any password</b> Used by <b>Bob Hunter</b>.</p>
Examine different file types:  Export doc/office and exe files; look at Metadata if required	YES	21/12/2024	06:15 PM	<p>After loading the case, I saw different types of files by following the path such as:</p> <p><a href="#">Path: /file Views/File Types/</a></p> <p>In this path, I found two types of files that are;</p> <ol style="list-style-type: none"> <li>1. By Extension</li> </ol>

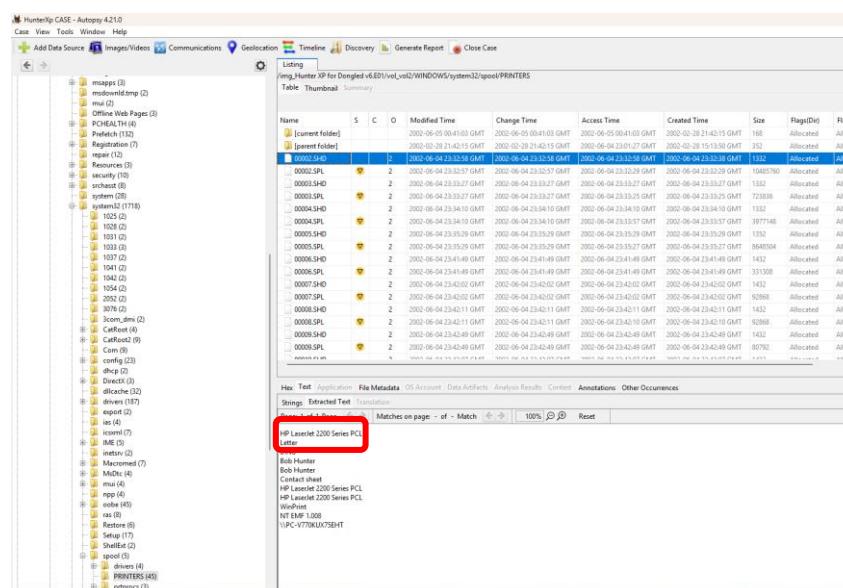
Action	Done?	Date	Time	Notes
				<p>2. By MIME Type</p> <p>When I viewed it by extension, I found that there are different file types such as.</p> <ul style="list-style-type: none"> <li>• Images (2371)</li> <li>• Videos (31)</li> <li>• Audio (151)</li> <li>• Archives (243)</li> <li>• Databases (14)</li> </ul> <p>After examination of these files, I also found that two more modules are:</p> <p>a. Documents</p> <ul style="list-style-type: none"> <li>• HTML (1245)</li> <li>• Office (10)</li> <li>• Pdf (0)</li> <li>• Plain text (397)</li> <li>• Rich text (0)</li> </ul>

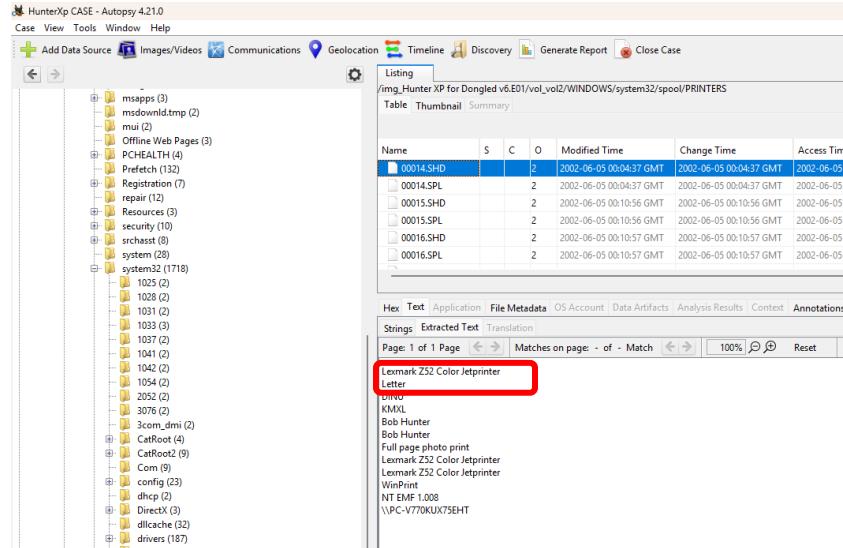
Action	Done?	Date	Time	Notes
				<p>b. Executable</p> <ul style="list-style-type: none"><li>• .exe (429)</li><li>• .dll (1764)</li><li>• .bat (1)</li><li>• .cmd (1)</li><li>• .com (16)</li></ul>

Action	Done?	Date	Time	Notes
				 <p>vol3 (Unallocated: 3318336-8007551)</p> <p>File Views</p> <p>File Types</p> <p>By Extension</p> <ul style="list-style-type: none"><li>Images (2371)</li><li>Videos (31)</li><li>Audio (151)</li><li>Archives (243)</li><li>Databases (14)</li></ul> <p>Documents</p> <ul style="list-style-type: none"><li>HTML (1245)</li><li>Office (10)</li><li>PDF (0)</li><li>Plain Text (397)</li><li>Rich Text (0)</li></ul> <p>Executable</p> <ul style="list-style-type: none"><li>.exe (429)</li><li>.dll (1764)</li><li>.bat (1)</li><li>.cmd (1)</li><li>.com (16)</li></ul> <p>By MIME Type</p>

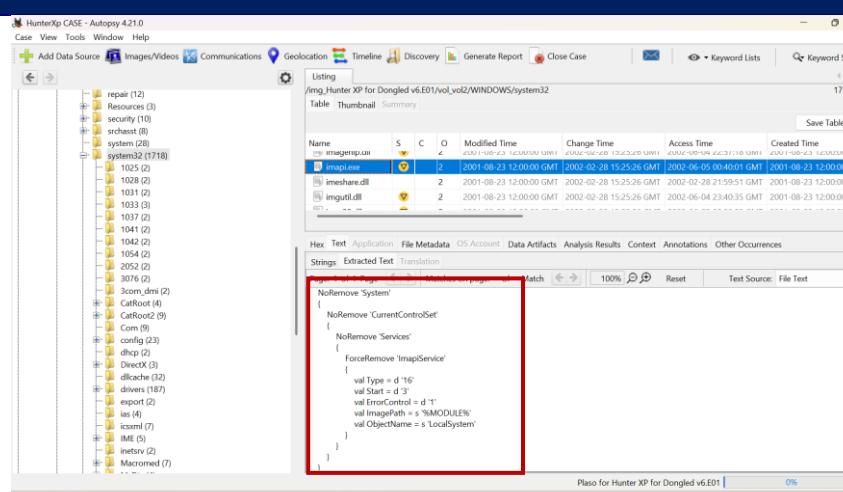
Action	Done?	Date	Time	Notes
Encryption, Steganalysis (any indications? Entropy or Autopsy can be used)	YES	21/12/2024	06:40 PM	<p>For analysis of Encryption, Steganalysis I run Encryption Detection in the ingest module, by following the given steps.</p> <ul style="list-style-type: none"> <li>➤ Clicked on <b>tools</b>.</li> <li>➤ Selected <b>run ingest module</b></li> <li>➤ Clicked <b>Hunter XP for Dongled v6.E01</b>.</li> <li>➤ Picked <b>Encryption Detection</b>.</li> </ul> 

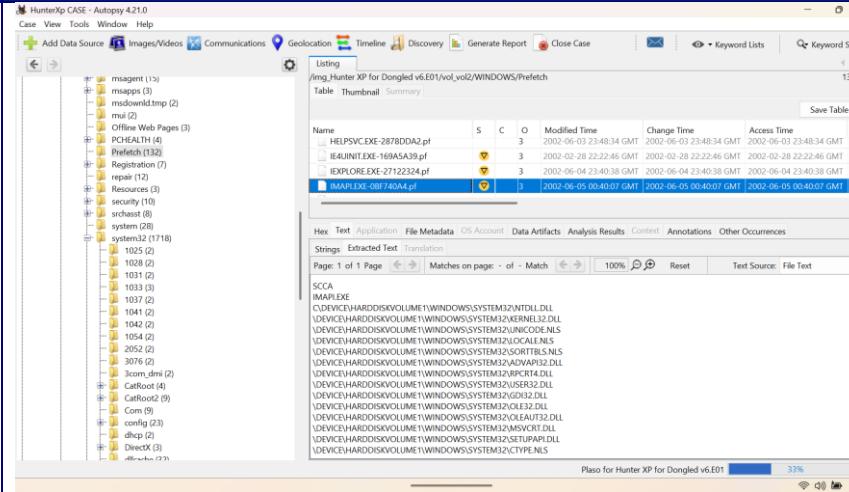
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>➤ After running this module, I found there was an encryption suspected header when I clicked <b>Analysis result</b>.</li> <li>➤ After analysis, only one encrypted file named '<b>oembios.bin</b>' was found. Entropy of <b>oembios.bin</b> file = <b>7.999988</b> (which is high)</li> </ul> 
Print artefacts	YES	21/12/2024	07:05 PM	For analysis of Print artifacts, I found two distinct file extensions with the print spooler to identify: ' <b>.shd</b> ' and ' <b>.spl</b> '.

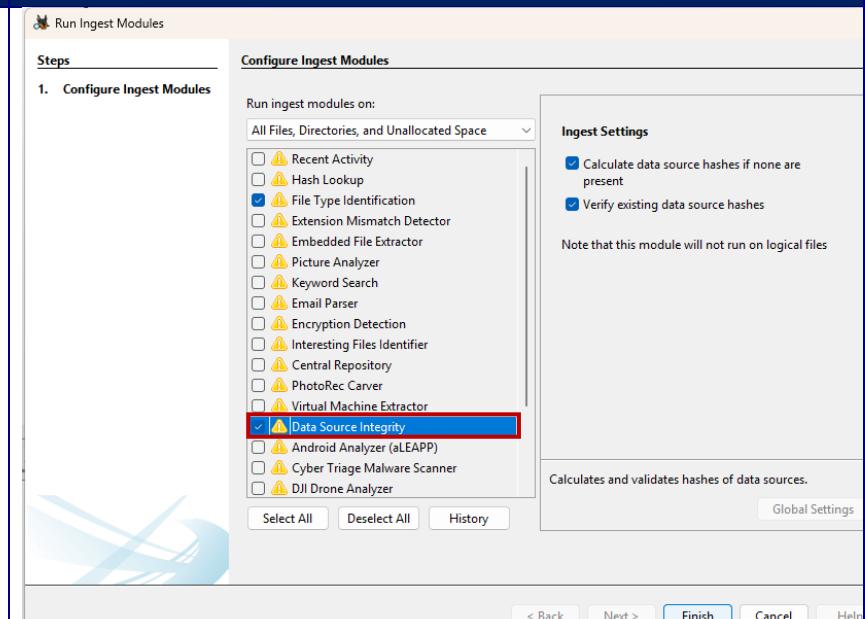
Action	Done?	Date	Time	Notes
				<p>The '.shd' (Shadow) files exclusively contained print job information, while the '.spl' (Spool) files housed the content in RAW format as generated during the printing process.</p> <p>For examination of these artifacts, I followed the path;</p> <p><b>Path: /img_Hunter XP for Dongled</b></p> <p><b>v6.E01/vol_vo2/WINDOWS/system32/spool/PRINTERS</b></p> 

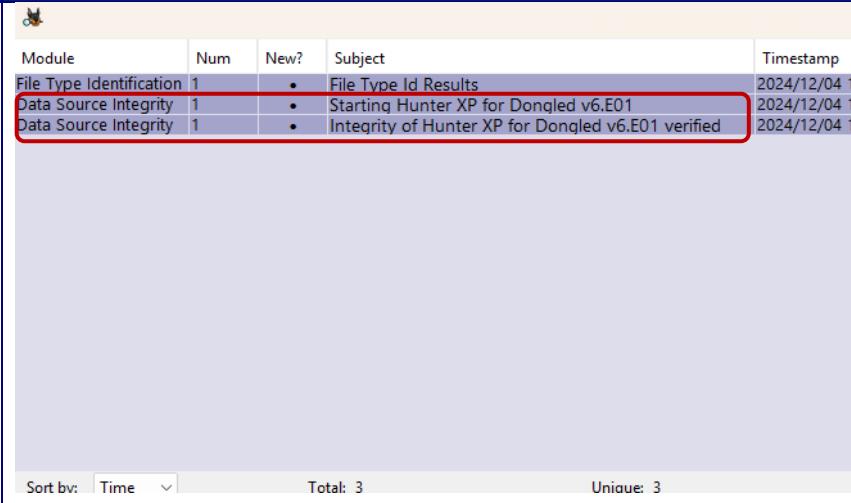
Action	Done?	Date	Time	Notes
				<ul style="list-style-type: none"> <li>➤ After analyzing the files in the <b>PRINTERS</b> folder, I found that the <b>HP LaserJet 2200 Series PCL Printer</b> is used for printing.</li> <li>➤ When I analyzed all the files in the folders, I found that one more printer was used for printing.</li> </ul>  <p>I found that the <b>Lexmark Z52 Color Jetprinter</b> was also used for printing purposes.</p>

Action	Done?	Date	Time	Notes
				<p>So, the printers used for printing are;</p> <ul style="list-style-type: none"> <li><b>1. Lexmark Z52 Color Jetprinter</b></li> <li><b>2. HP LaserJet 2200 Series PCL Printer</b></li> </ul>
CD/DVD burning apps; check log files	YES	21/12/2024	07:30 PM	<p>CD/DVD burning app was use by the user. To find the traces of CD/DVD burning I followed the following steps given below:</p> <p><b>Step1:</b></p> <p>I found the artifacts about the CD/DVD burning in system32 folder where <b>IMAPI.EXE</b> details and log is stored.</p> <p>Path:</p> <p style="color: blue;">/img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32</p>

Action	Done?	Date	Time	Notes
				 <p><b>Step2:</b></p> <p><b>imapi.exe</b> file is executed by the user. This file data execution details is stored store in prefetch folder. To find <b>imapi(pf</b> file I browsed the following path:</p> <p>Path:  <a href="#">/img_Hunter XP for Dongled v6.E01/vol_vo2/WINDOWS/Prefetch</a></p>

Action	Done?	Date	Time	Notes
				
Validate evidence integrity at the end of the examination	YES	22/12/2024	12:00 PM	<p>To validate evidence integrity; I go for the ingest module by following the given steps:</p> <ul style="list-style-type: none"> <li>➤ First of all, click on <b>tools</b>.</li> <li>➤ Selected <b>Run Ingest Module</b>.</li> <li>➤ Clicked on <b>Hunter XP for Dongled v6.E01</b>.</li> <li>➤ And selected <b>Data Source Integrity</b>.</li> </ul>

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

Action	Done?	Date	Time	Notes																				
				 <p>The screenshot shows a message box with the following log entries:</p> <table border="1"> <thead> <tr> <th>Module</th> <th>Num</th> <th>New?</th> <th>Subject</th> <th>Timestamp</th> </tr> </thead> <tbody> <tr> <td>File Type Identification</td> <td>1</td> <td></td> <td>• File Type Id Results</td> <td>2024/12/04 1</td> </tr> <tr> <td>Data Source Integrity</td> <td>1</td> <td></td> <td>• Starting Hunter XP for Dongled v6.E01</td> <td>2024/12/04 1</td> </tr> <tr> <td>Data Source Integrity</td> <td>1</td> <td></td> <td>• Integrity of Hunter XP for Dongled v6.E01 verified</td> <td>2024/12/04 1</td> </tr> </tbody> </table> <p>Sort by: Time Total: 3 Unique: 3</p> <p>When I opened the message box, I found that the Data Source integrity of <b>Hunter XP for Dongled v6.E01</b> was verified. When I opened this message, I saw that the result is verified and <b>MD5 HASH is also verified.</b></p>	Module	Num	New?	Subject	Timestamp	File Type Identification	1		• File Type Id Results	2024/12/04 1	Data Source Integrity	1		• Starting Hunter XP for Dongled v6.E01	2024/12/04 1	Data Source Integrity	1		• Integrity of Hunter XP for Dongled v6.E01 verified	2024/12/04 1
Module	Num	New?	Subject	Timestamp																				
File Type Identification	1		• File Type Id Results	2024/12/04 1																				
Data Source Integrity	1		• Starting Hunter XP for Dongled v6.E01	2024/12/04 1																				
Data Source Integrity	1		• Integrity of Hunter XP for Dongled v6.E01 verified	2024/12/04 1																				

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

#### Additional Notes/Artefacts Examined:


--	--	--	--	--	--

Colour-coding	Tasks
	Fundamental
	Basic
	Elementary
	Secondary
	Advanced
	Exceptional