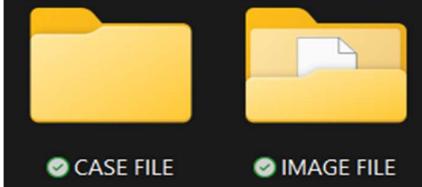
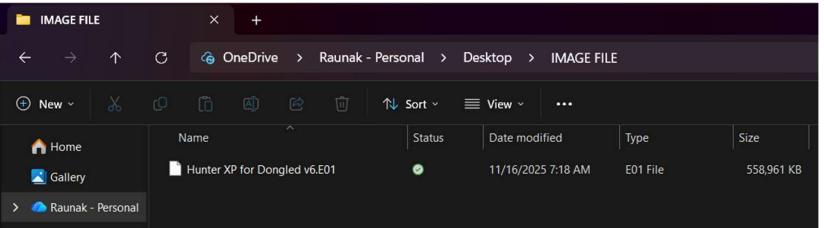
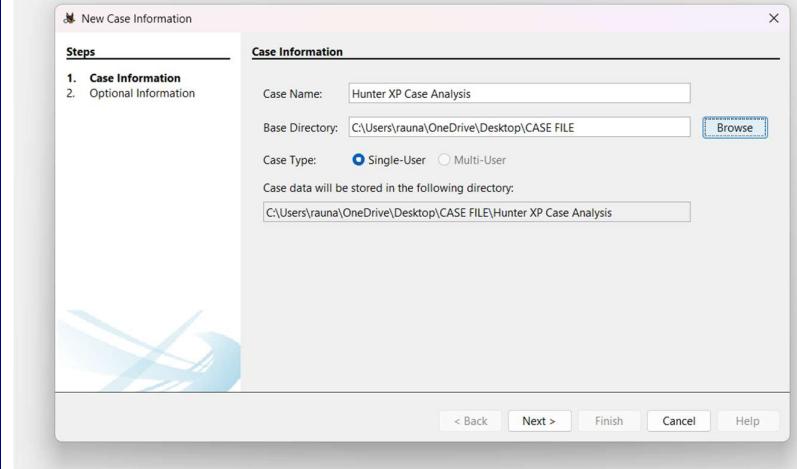
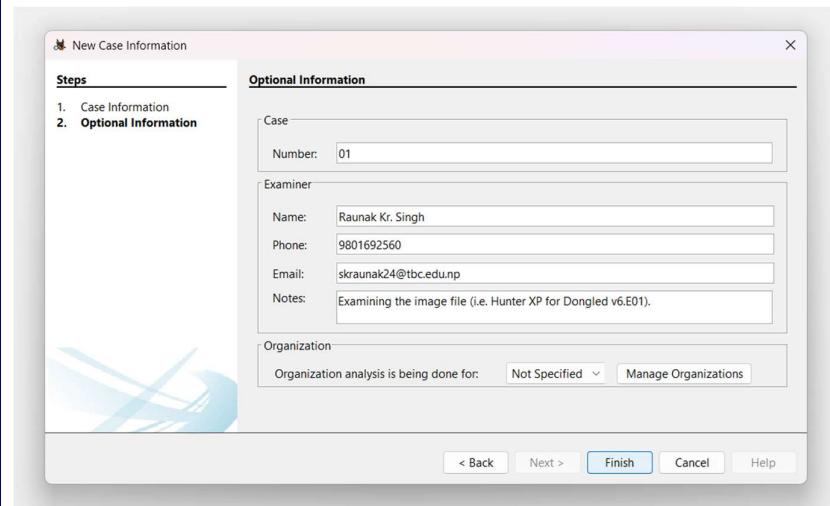


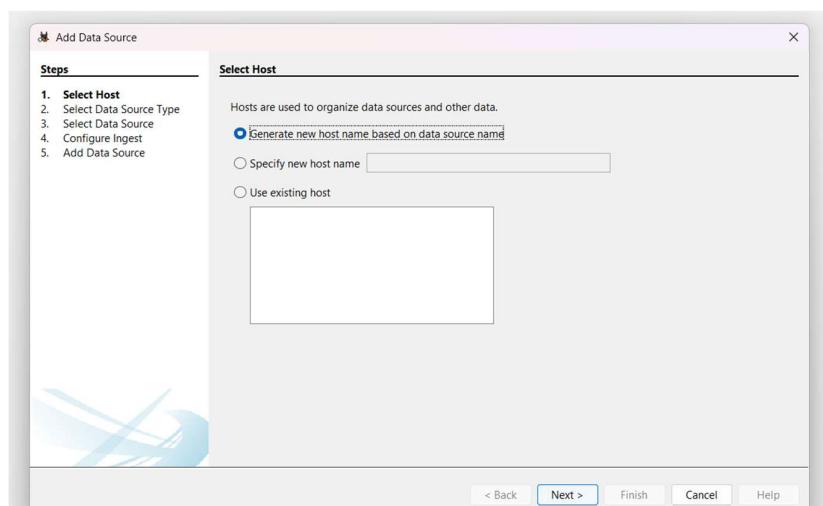
## Contemporaneous Notes

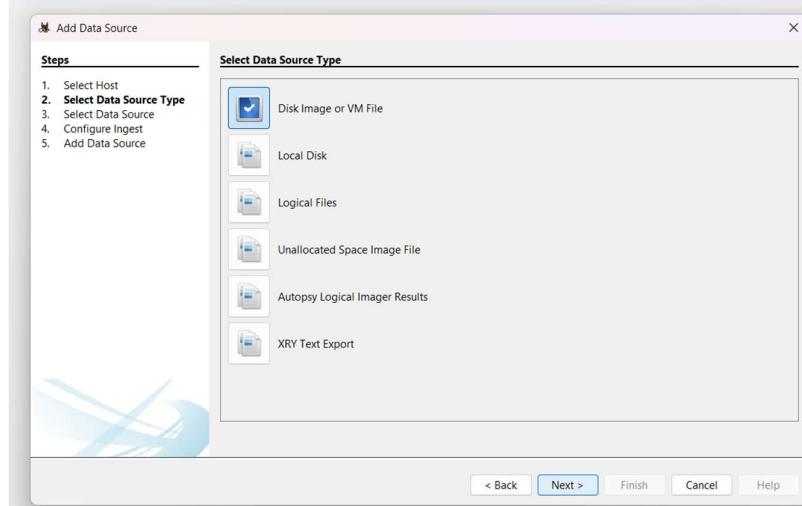
Examiner	Name: Raunak Kr. Singh Email: <a href="mailto:raunak2.singh@live.uwe.ac.uk">raunak2.singh@live.uwe.ac.uk</a> UWE ID: 24071246	Exam commenced	2025/12/8 – 2025/12/16
Other relevant information	<ol style="list-style-type: none"><li>1. The given Hunter XP case image file was investigated. The steps are listed below along with the screenshots of each in detail.</li><li>2. Additional artefacts studied and analysed.</li></ol>	Software used, versions and licensing	Autopsy v4.22.1 RegRipper v3.0-master AccessData FTK Imager v4.7.1 AccessData Registry Viewer v1.8.0.5 (DEMO) 7-Zip File Manager v25.01 Ophcrack 3.8.0 Hex Editor (HxD) Oracle VirtualBox v7.2.0 -Kali Linux (Debian x64)

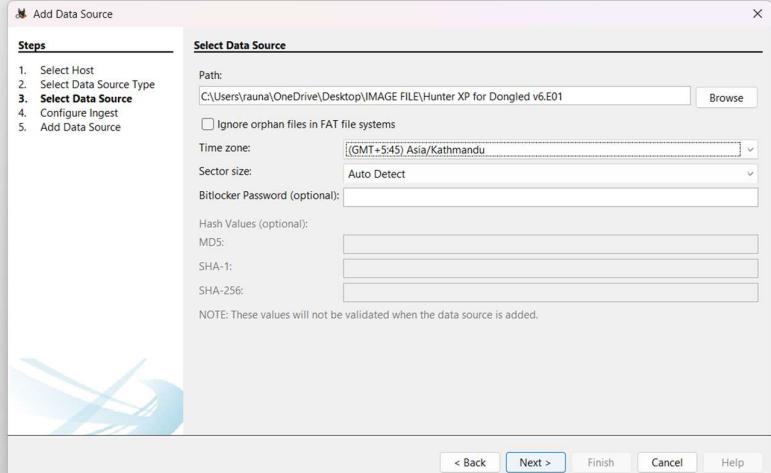
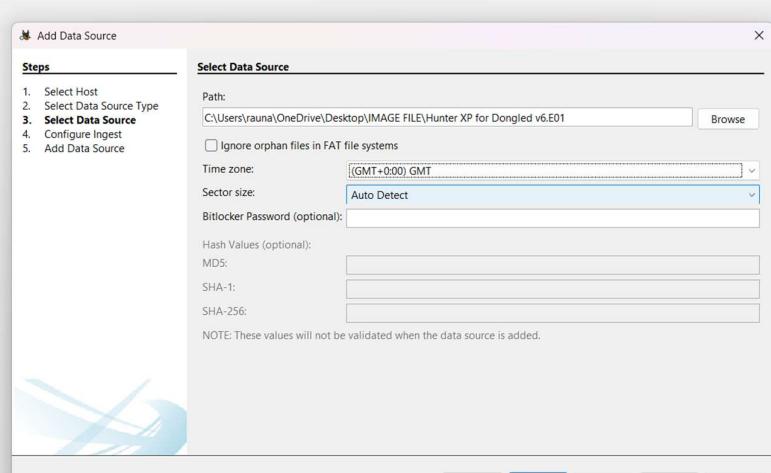
Action	Done?	Date (YY/MM/DD)	Time	Notes
Load case and verify image	Done	2025/12/8	6:00 PM (UTC +5:45)	 <p>Basically, I made 2 folders.</p> <p><b>1.Case File – Used for keeping database extracted from Autopsy.</b></p> <p><b>2.Image File – Used for storing Image file of Hunter XP.</b></p>  <p>I opened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

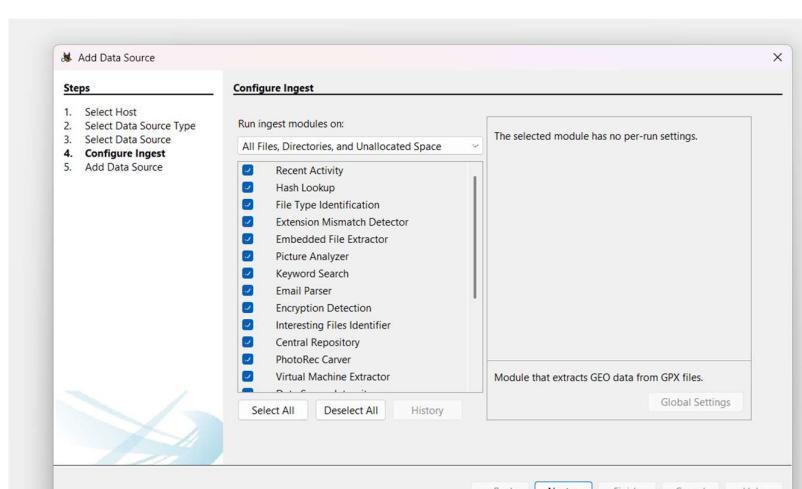
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Welcome</p> <p>New Case</p> <p>Open Recent Case</p> <p>Open Case</p> <p>Close</p> <p>I added Case Name and Base Directory.</p> <p><b>Case Name: Hunter XP Case Analysis</b></p> <p><b>Base Directory: Case File (where database is saved)</b></p>

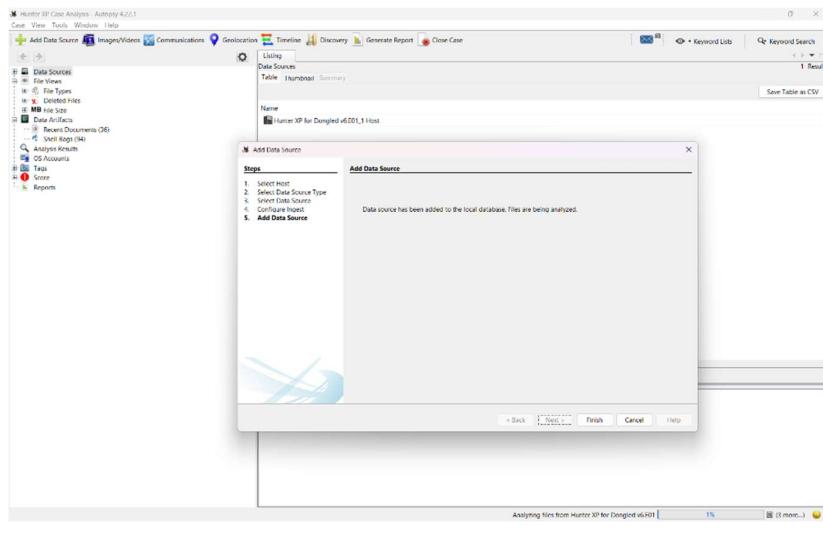
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>I added option information important for the case.</p> 

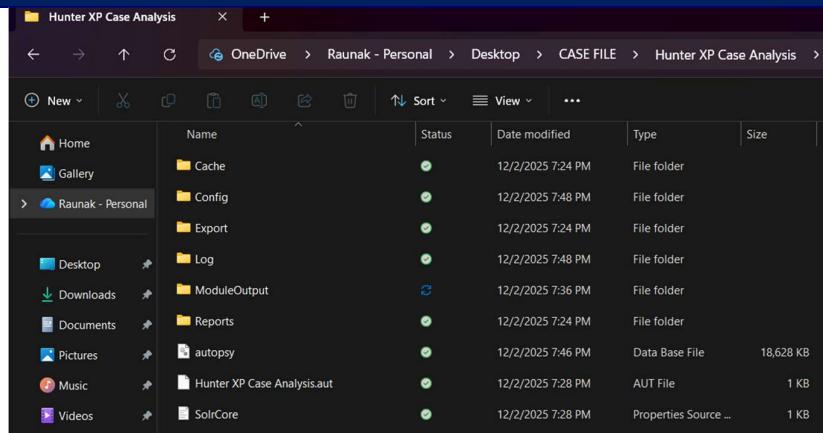
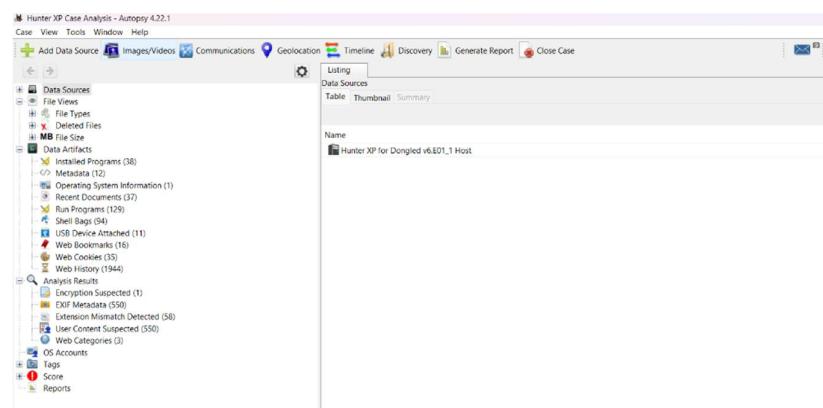
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>I choose disk image because the give file is an image file of Hunter XP.</p>

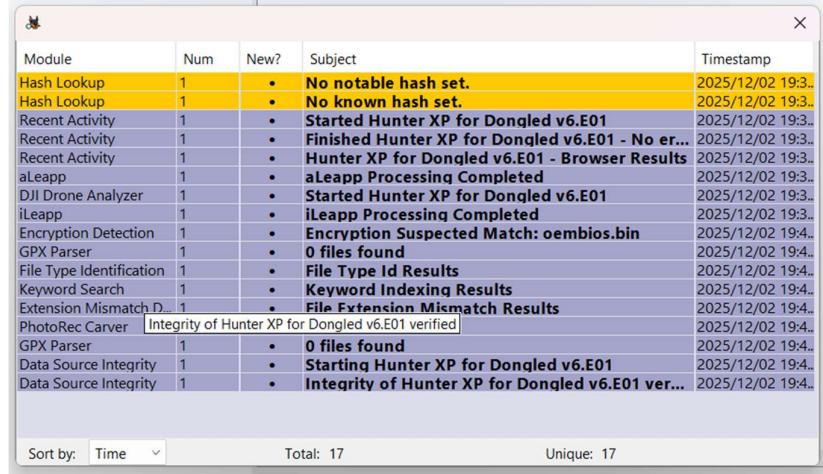
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>I added the data source.</p> <p><b>Path: Image File&gt;Hunter XP for Dongled v6. E01</b>  <b>Time zone: (GMT +0:00) GMT (Adjusted)</b></p>

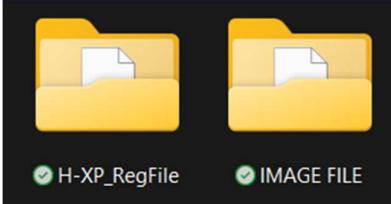
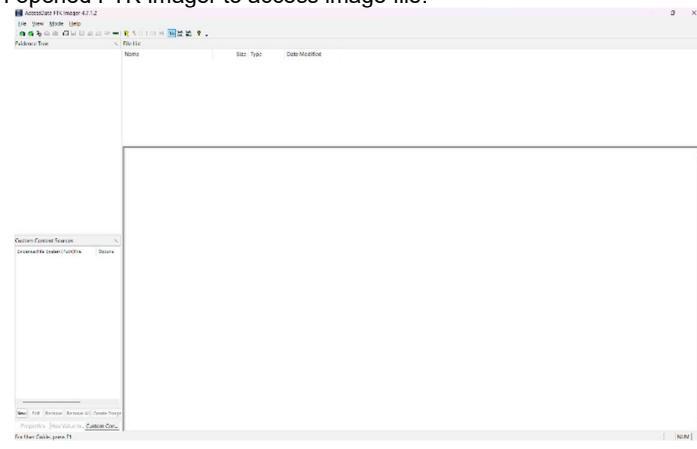
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p><b>Select Data Source</b></p> <p>Path: C:\Users\rauna\OneDrive\Desktop\IMAGE FILE\Hunter XP for Dongled v6.E01 <input type="button" value="Browse"/></p> <p><input type="checkbox"/> Ignore orphan files in FAT file systems</p> <p>Time zone: (GMT+5:45) Asia/Kathmandu</p> <p>Sector size: Auto Detect</p> <p>Bitlocker Password (optional):</p> <p>Hash Values (optional):</p> <p>MDS:</p> <p>SHA-1:</p> <p>SHA-256:</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;"/> Finish Cancel Help</p>
				 <p><b>Select Data Source</b></p> <p>Path: C:\Users\rauna\OneDrive\Desktop\IMAGE FILE\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>Bitlocker Password (optional):</p> <p>Hash Values (optional):</p> <p>MDS:</p> <p>SHA-1:</p> <p>SHA-256:</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;"/> Finish Cancel Help</p>

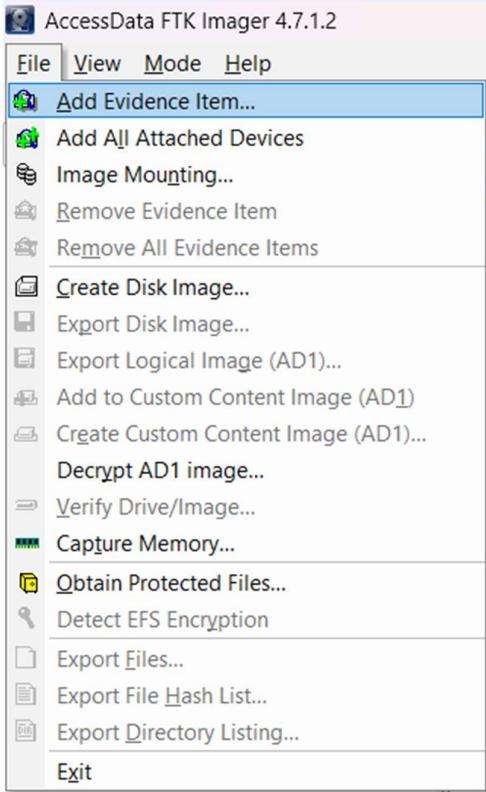
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p>I configured required ingest module for the case for further investigation. They are:</p> <ul style="list-style-type: none"> <li>• <b>Recent Activity</b></li> <li>• <b>Hash Lookup</b></li> <li>• <b>File Type Identification</b></li> <li>• <b>Extension Mismatch Detector</b></li> <li>• <b>Embedded File Extractor</b></li> <li>• <b>Picture Analyzer</b></li> <li>• <b>Keyword search</b></li> <li>• <b>Email Parser</b></li> <li>• <b>Encryption Detection</b></li> <li>• <b>Interesting Files Identifier</b></li> <li>• <b>Central Repository</b></li> <li>• <b>PhotoRec Carver</b></li> <li>• <b>Data Source Integrity</b></li> <li>• <b>GPX Parser</b></li> </ul> 

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

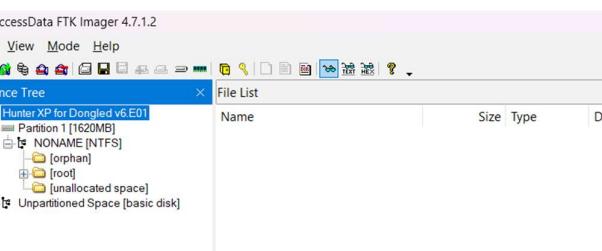
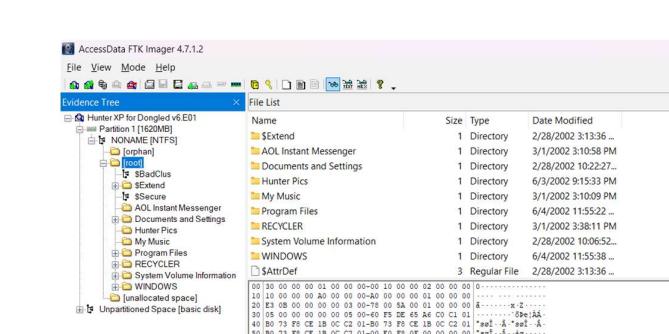
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Now, I clicked on the mail icon for further process.</p>  <p>Required Hash Value for Data Integrity has been obtained.</p>

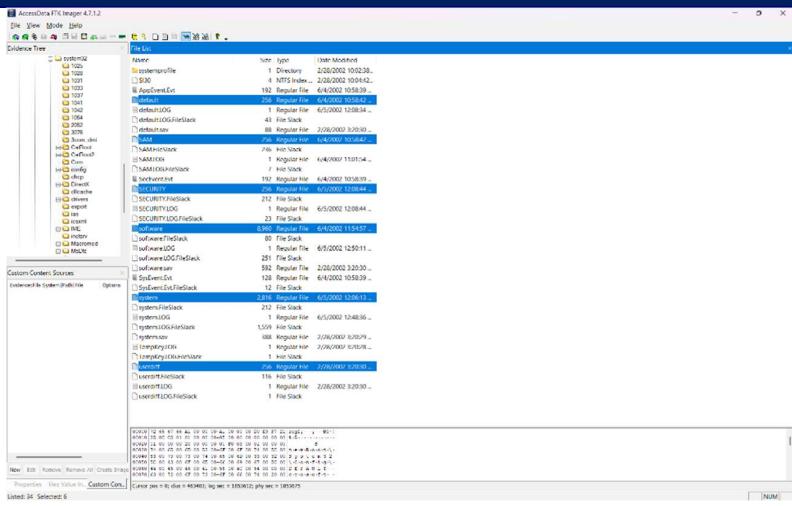
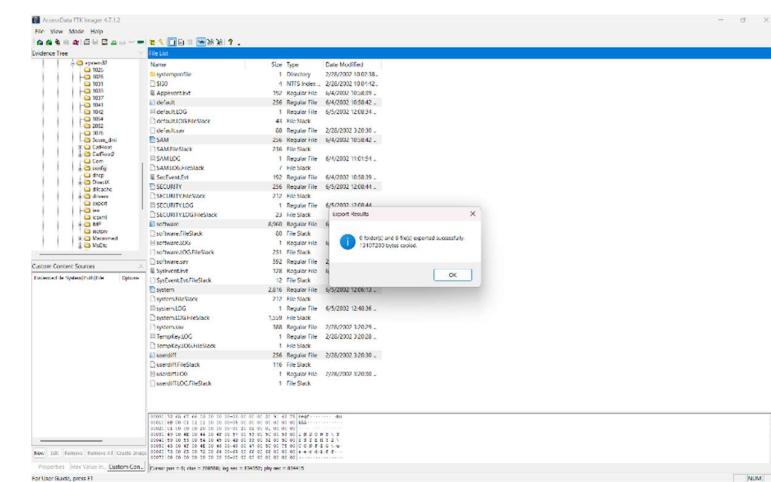
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Here is the required hash value which will show the integrity throughout the investigation.</p> 

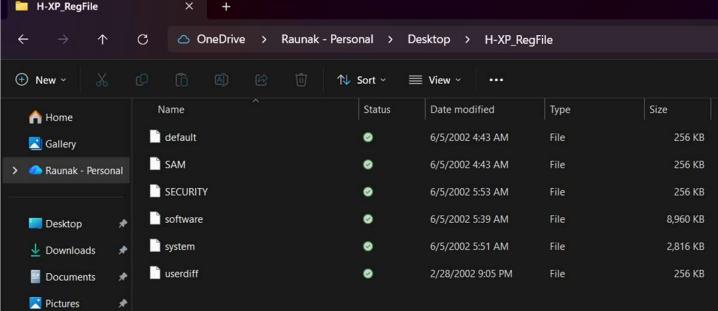
Action	Done?	Date (YY/MM/DD)	Time	Notes
Load Case into second forensic tool for dual verification of at least 2 key artefacts, evidence items	Done	2025/12/8	7:00 PM (UTC +5:45)	 <p>Basically, Here I Created 2 folders.</p> <p>1.H-XP_RegFile – Used for storing extracted Registry from the image.      2.Image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

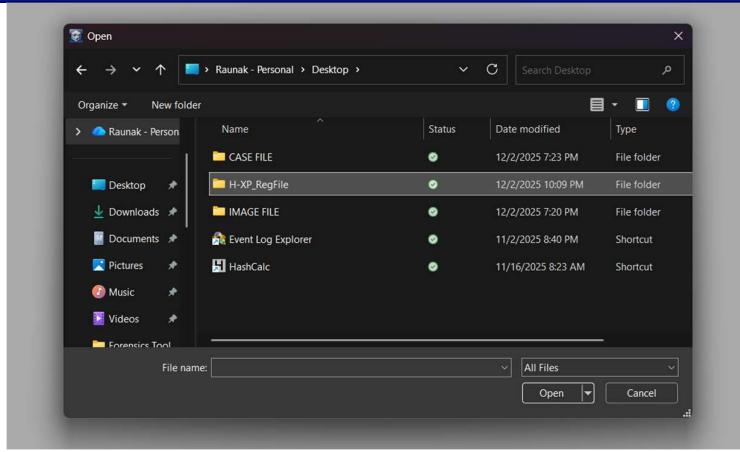
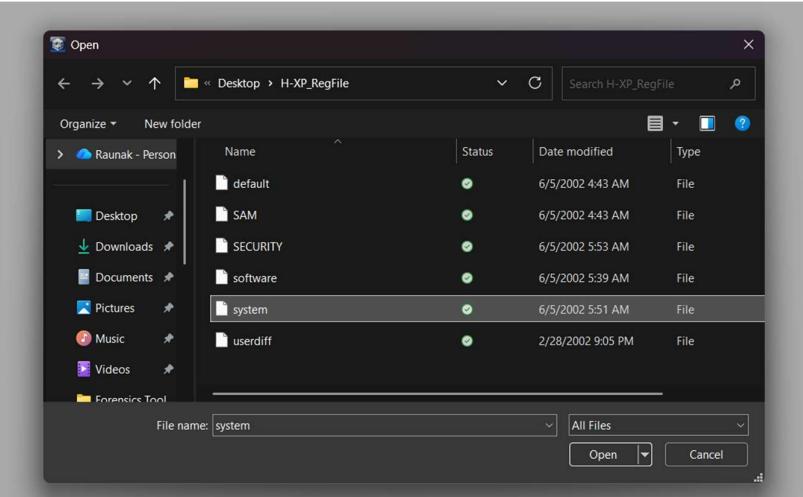
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>As Hunter XP being an image file so while adding evidence item I selected Image file.</p>

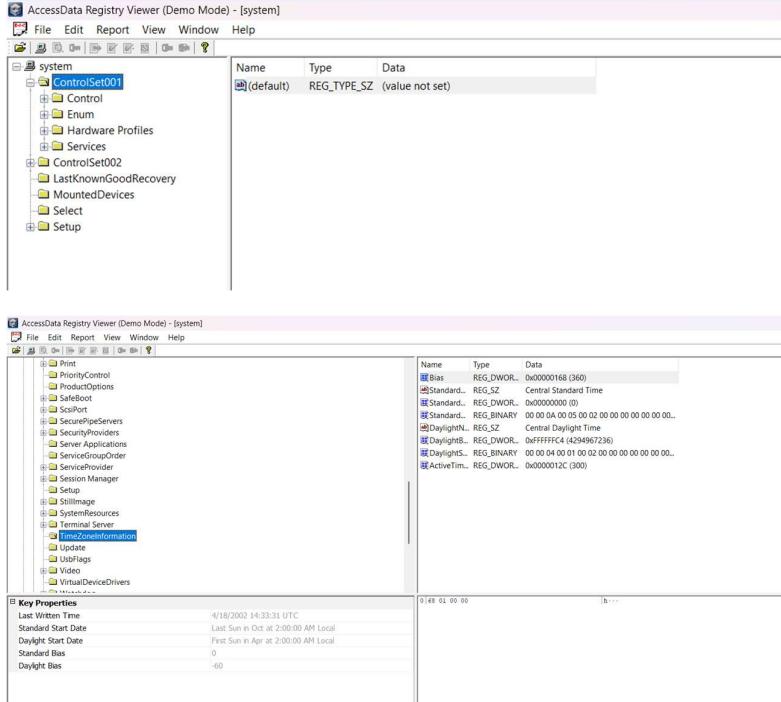
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p>Select Source</p> <p>Please Select the Source Evidence Type</p> <p><input type="radio"/> Physical Drive</p> <p><input type="radio"/> Logical Drive</p> <p><input checked="" type="radio"/> Image File</p> <p><input type="radio"/> Contents of a Folder (logical file-level analysis only; excludes deleted, unallocated, etc.)</p> <p>&lt; Back <span style="background-color: #0078D4; color: white; border: 1px solid #0078D4; padding: 2px 10px;">Next &gt;</span> Cancel Help</p> <p>Select File</p> <p>Evidence Source Selection</p> <p>Please enter the source path: C:\Users\rauna\OneDrive\Desktop\IMAGE FILE\Hunter XP for C</p> <p>Browse...</p> <p>&lt; Back Finish Cancel Help</p> <p>Process to access Registry File from this image. <b>Partition 1&gt;ROOT&gt;WINDOWS&gt;SYSTEM32&gt;CONFIG</b></p>

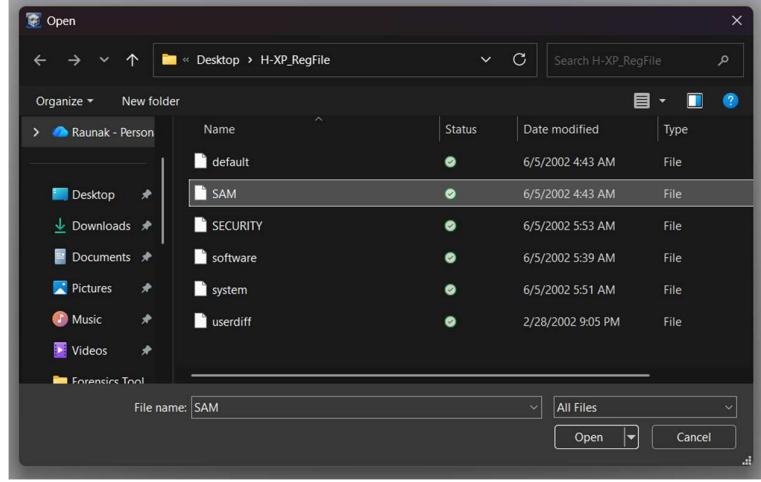
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 

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

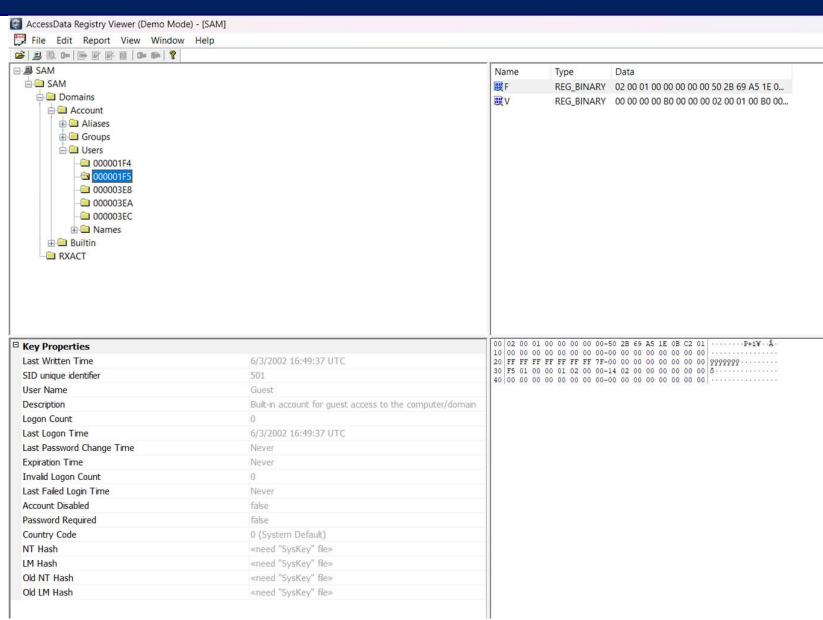
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Now, I opened Registry Viewer.</p> 

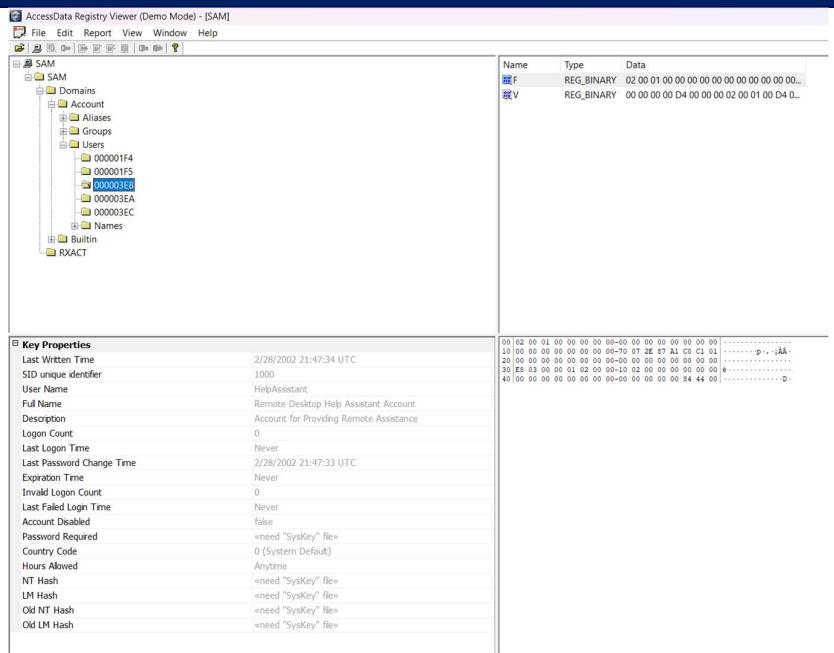
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>I loaded System Registry file to view information about Time Zone.</p>  <p>Process to reach till Time Zone:  <b>System&gt;ControlSet001&gt;Control&gt;TimeZoneInformation</b></p>

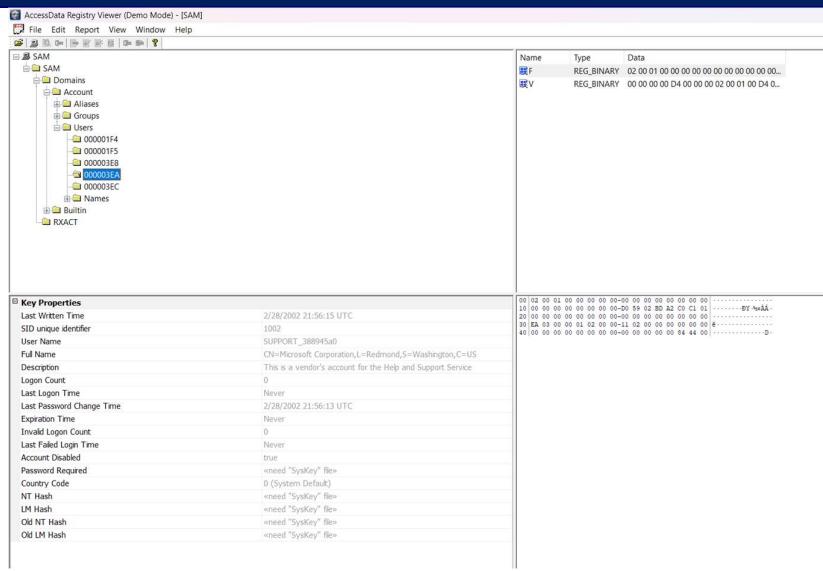
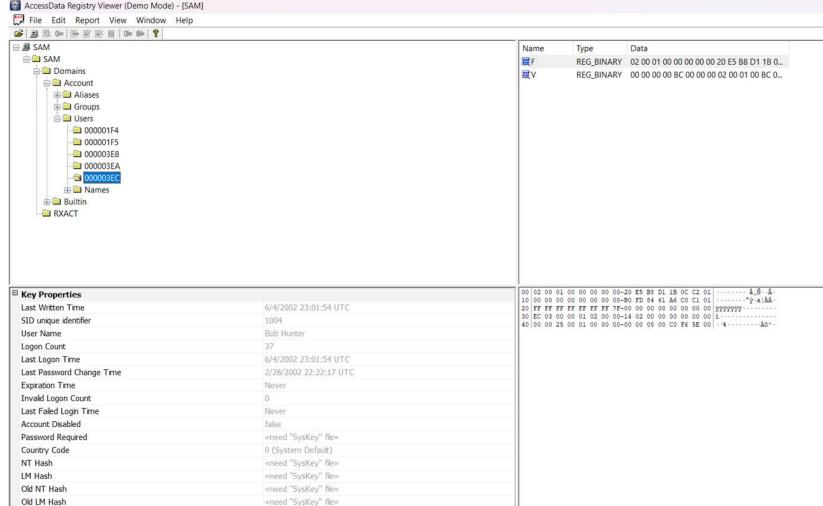
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Now, I loaded Sam Registry File in the registry viewer to access information about users.</p>

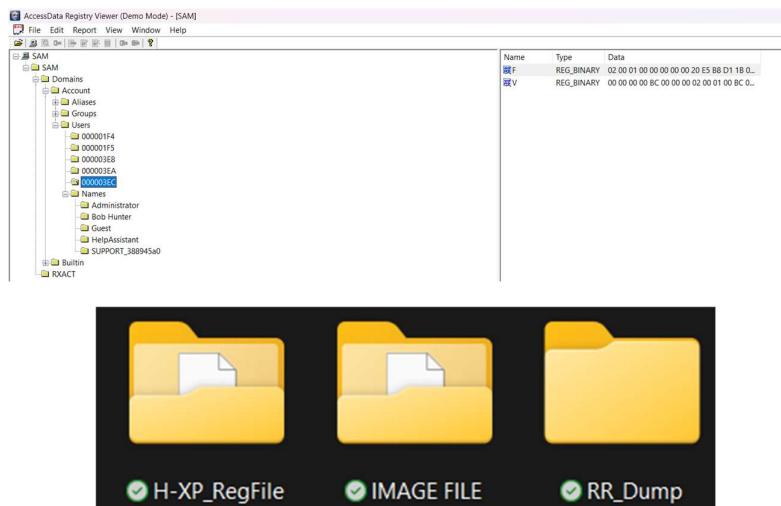
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Process to access Users:  <b>Sam&gt;Domains&gt;Users</b></p> 

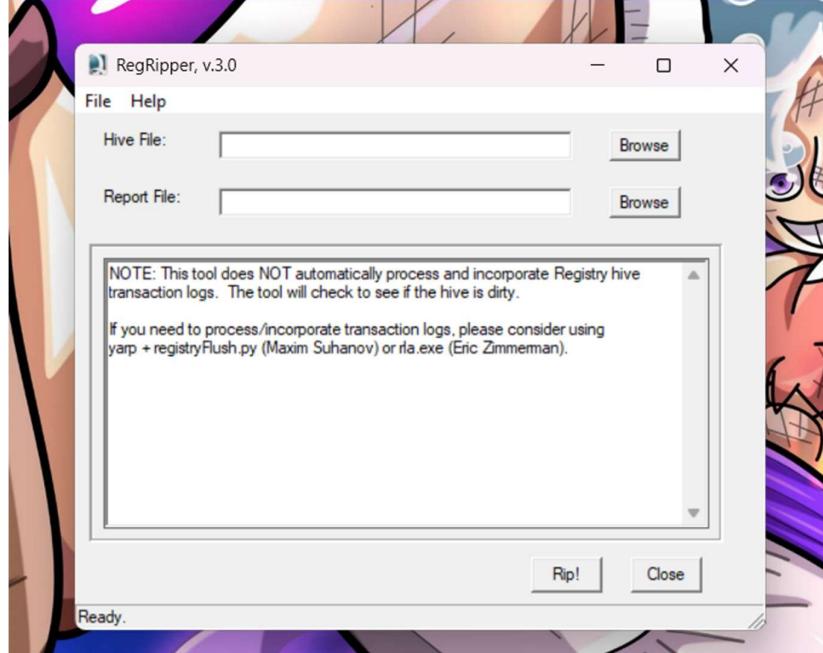


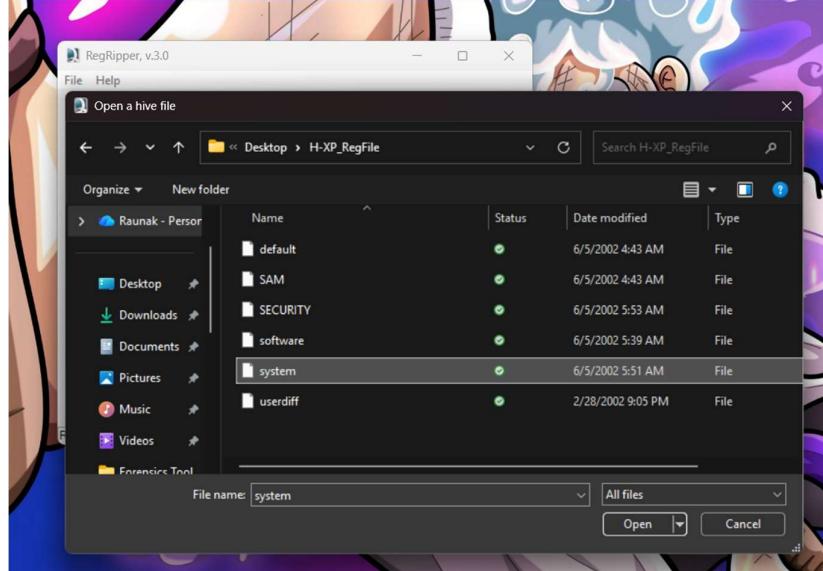
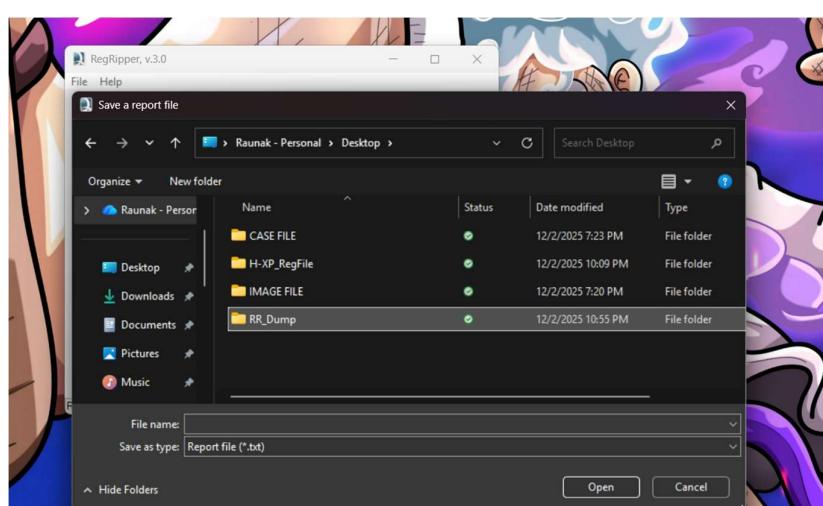
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>The screenshot shows the AccessData Registry Viewer interface. The left pane displays a tree view of the SAM database, with the 'Users' node expanded to show several user entries. The 'Guest' account is selected. The right pane contains two windows: one titled 'Key Properties' showing details for the Guest account, and another window showing binary data or registry keys.</p> <p><b>Key Properties</b></p> <ul style="list-style-type: none"> <li>Last Written Time: 6/3/2002 16:49:37 UTC</li> <li>SID unique identifier: 501</li> <li>User Name: Guest</li> <li>Description: Built-in account for guest access to the computer/domain</li> <li>Logon Count: 0</li> <li>Last Logon Time: 6/3/2002 16:49:37 UTC</li> <li>Last Password Change Time: Never</li> <li>Expiration Time: Never</li> <li>Invalid Logon Count: 0</li> <li>Last Failed Logon Time: Never</li> <li>Account Disabled: false</li> <li>Password Required: 0 (System Default)</li> <li>Country Code: &lt;need "SysKey" file&gt;</li> <li>NT Hash: &lt;need "SysKey" file&gt;</li> <li>LM Hash: &lt;need "SysKey" file&gt;</li> <li>Old NT Hash: &lt;need "SysKey" file&gt;</li> <li>Old LM Hash: &lt;need "SysKey" file&gt;</li> </ul>

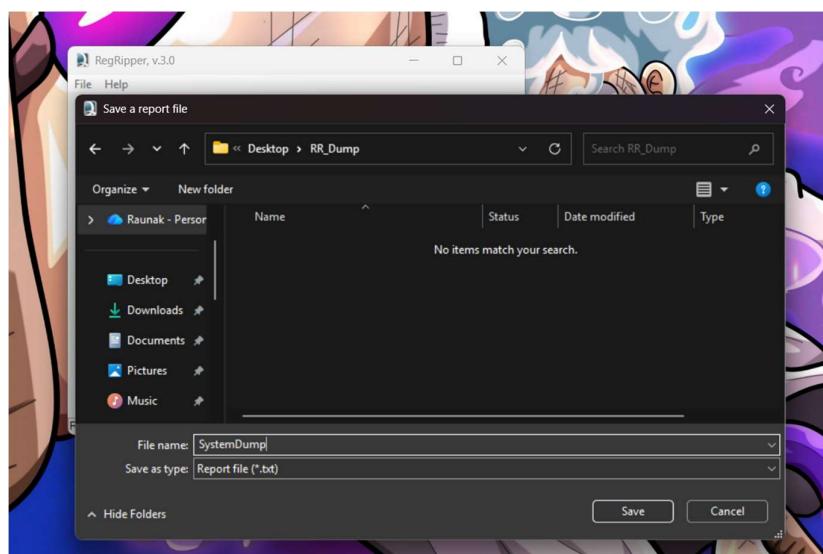
Action	Done?	Date (YY/MM/DD)	Time	Notes																																																	
				 <p>The screenshot shows the AccessData Registry Viewer interface with the title 'AccessData Registry Viewer (Demo Mode) - [SAM]'. The left pane displays a tree view of the SAM database structure under the 'SAM' node, including Domains, Account, Aliases, Groups, and Users. The 'Users' node is expanded, showing several entries such as '000001F4', '000001F5', '000003E8', '000003EA', '000003EC', and 'Names'. The 'Builtin' and 'RXACT' nodes are also visible. The right pane contains two tables: 'Name' and 'Type' with corresponding data values, and 'Key Properties' with detailed account settings.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>f</td> <td>REG_BINARY</td> <td>02 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00</td> </tr> <tr> <td>V</td> <td>REG_BINARY</td> <td>00 00 00 00 D4 00 00 02 00 01 00 04 00 ..</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="2">Key Properties</th> </tr> </thead> <tbody> <tr> <td>Last Written Time</td> <td>2/28/2002 21:47:34 UTC</td> </tr> <tr> <td>SID unique identifier</td> <td>1000</td> </tr> <tr> <td>User Name</td> <td>HelpAssistant</td> </tr> <tr> <td>Full Name</td> <td>Remote Desktop Help Assistant Account</td> </tr> <tr> <td>Description</td> <td>Account for Providing Remote Assistance</td> </tr> <tr> <td>Logon Count</td> <td>0</td> </tr> <tr> <td>Last Logon Time</td> <td>Never</td> </tr> <tr> <td>Last Password Change Time</td> <td>2/28/2002 21:47:33 UTC</td> </tr> <tr> <td>Expiration Time</td> <td>Never</td> </tr> <tr> <td>Invalid Logon Count</td> <td>0</td> </tr> <tr> <td>Last Failed Logon Time</td> <td>Never</td> </tr> <tr> <td>Account Disabled</td> <td>false</td> </tr> <tr> <td>Password Required</td> <td>&lt;need "SysKey" file&gt;</td> </tr> <tr> <td>Country Code</td> <td>0 (System Default)</td> </tr> <tr> <td>Hours Allowed</td> <td>Anytime</td> </tr> <tr> <td>NT Hash</td> <td>&lt;need "SysKey" file&gt;</td> </tr> <tr> <td>LM Hash</td> <td>&lt;need "SysKey" file&gt;</td> </tr> <tr> <td>Old NT Hash</td> <td>&lt;need "SysKey" file&gt;</td> </tr> <tr> <td>Old LM Hash</td> <td>&lt;need "SysKey" file&gt;</td> </tr> </tbody> </table>	Name	Type	Data	f	REG_BINARY	02 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00	V	REG_BINARY	00 00 00 00 D4 00 00 02 00 01 00 04 00 ..	Key Properties		Last Written Time	2/28/2002 21:47:34 UTC	SID unique identifier	1000	User Name	HelpAssistant	Full Name	Remote Desktop Help Assistant Account	Description	Account for Providing Remote Assistance	Logon Count	0	Last Logon Time	Never	Last Password Change Time	2/28/2002 21:47:33 UTC	Expiration Time	Never	Invalid Logon Count	0	Last Failed Logon Time	Never	Account Disabled	false	Password Required	<need "SysKey" file>	Country Code	0 (System Default)	Hours Allowed	Anytime	NT Hash	<need "SysKey" file>	LM Hash	<need "SysKey" file>	Old NT Hash	<need "SysKey" file>	Old LM Hash	<need "SysKey" file>
Name	Type	Data																																																			
f	REG_BINARY	02 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00																																																			
V	REG_BINARY	00 00 00 00 D4 00 00 02 00 01 00 04 00 ..																																																			
Key Properties																																																					
Last Written Time	2/28/2002 21:47:34 UTC																																																				
SID unique identifier	1000																																																				
User Name	HelpAssistant																																																				
Full Name	Remote Desktop Help Assistant Account																																																				
Description	Account for Providing Remote Assistance																																																				
Logon Count	0																																																				
Last Logon Time	Never																																																				
Last Password Change Time	2/28/2002 21:47:33 UTC																																																				
Expiration Time	Never																																																				
Invalid Logon Count	0																																																				
Last Failed Logon Time	Never																																																				
Account Disabled	false																																																				
Password Required	<need "SysKey" file>																																																				
Country Code	0 (System Default)																																																				
Hours Allowed	Anytime																																																				
NT Hash	<need "SysKey" file>																																																				
LM Hash	<need "SysKey" file>																																																				
Old NT Hash	<need "SysKey" file>																																																				
Old LM Hash	<need "SysKey" file>																																																				

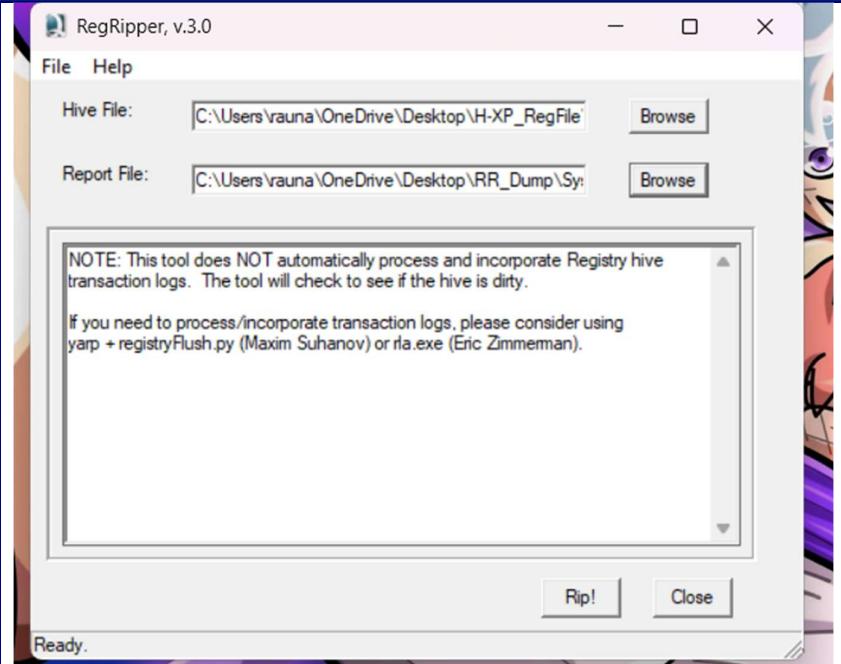
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p><b>Key Properties</b></p> <ul style="list-style-type: none"> <li>Last Written Time: 2/28/2002 21:56:15 UTC</li> <li>SID unique identifier: 1002</li> <li>User Name: SUPPORT_388945a0</li> <li>Full Name: CN=Microsoft Corporation,L=Redmond,S=Washington,C=US</li> <li>Description: This is a vendor's account for the Help and Support Service</li> <li>Logon Count: 0</li> <li>Last Logon Time: Never</li> <li>Last Password Change Time: 2/28/2002 21:56:13 UTC</li> <li>Expiration Time: Never</li> <li>Invalid Logon Count: 0</li> <li>Last Failed Logon Time: Never</li> <li>Account Disabled: true</li> <li>Password Required: &lt;need "SysKey" flex&gt;</li> <li>Country Code: 0 (System Default)</li> <li>NT Hash: &lt;need "SysKey" flex&gt;</li> <li>LM Hash: &lt;need "SysKey" flex&gt;</li> <li>Old NT Hash: &lt;need "SysKey" flex&gt;</li> <li>Old LM Hash: &lt;need "SysKey" flex&gt;</li> </ul>
				 <p><b>Key Properties</b></p> <ul style="list-style-type: none"> <li>Last Written Time: 6/4/2002 23:01:54 UTC</li> <li>SID unique identifier: 1004</li> <li>User Name: Bob_Hunter</li> <li>Logon Count: 37</li> <li>Last Logon Time: 6/4/2002 23:01:54 UTC</li> <li>Last Password Change Time: 2/28/2002 22:22:17 UTC</li> <li>Expiration Time: Never</li> <li>Invalid Logon Count: 0</li> <li>Last Failed Logon Time: Never</li> <li>Account Disabled: false</li> <li>Password Required: &lt;need "SysKey" flex&gt;</li> <li>Country Code: 0 (System Default)</li> <li>NT Hash: &lt;need "SysKey" flex&gt;</li> <li>LM Hash: &lt;need "SysKey" flex&gt;</li> <li>Old NT Hash: &lt;need "SysKey" flex&gt;</li> <li>Old LM Hash: &lt;need "SysKey" flex&gt;</li> </ul>

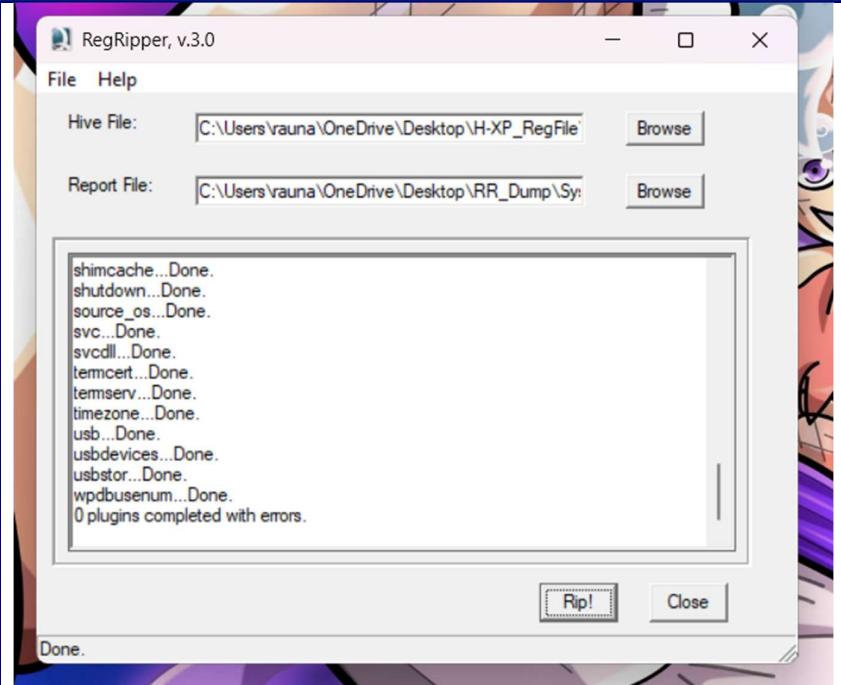
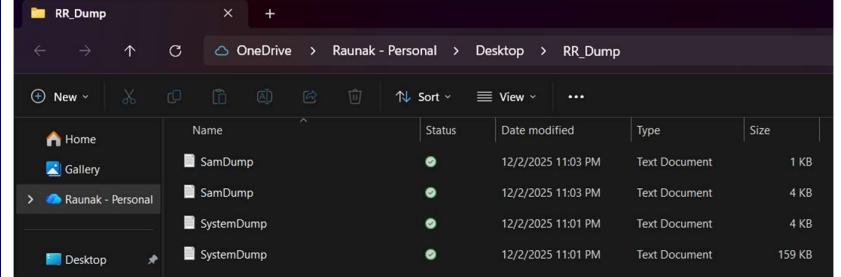
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Additionally, I made one more folder.</p> <p><b>RR_Dump – Used for saving dump file from Reg Ripper.</b></p> <p>Now, I opened Reg Ripper to get information about time zone.</p>

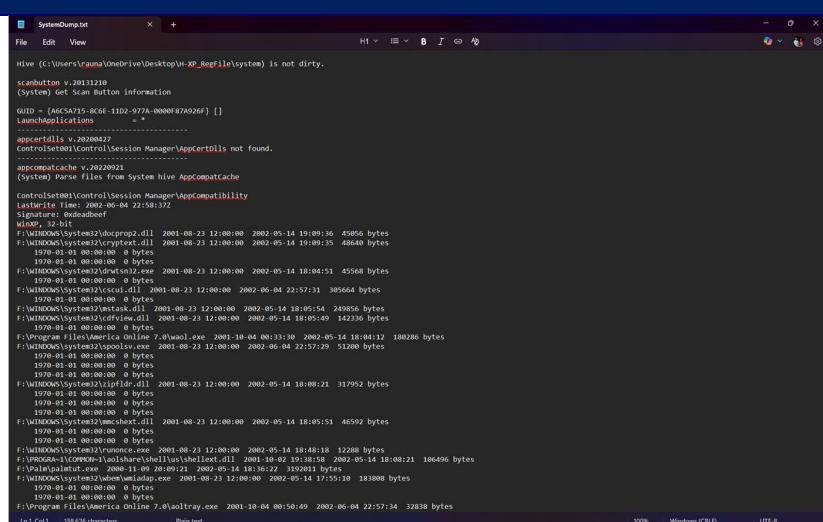
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>RegRipper, v.3.0</p> <p>File Help</p> <p>Hive File: <input type="text"/> <input type="button" value="Browse"/></p> <p>Report File: <input type="text"/> <input type="button" value="Browse"/></p> <p>NOTE: This tool does NOT automatically process and incorporate Registry hive transaction logs. The tool will check to see if the hive is dirty.</p> <p>If you need to process/incorporate transaction logs, please consider using yarp + registryFlush.py (Maxim Suhanov) or rla.exe (Eric Zimmerman).</p> <p>Rip! Close</p> <p>Ready.</p> <p>Now, I loaded System Registry to reg ripper to get detailed information about system in form of .txt.</p>

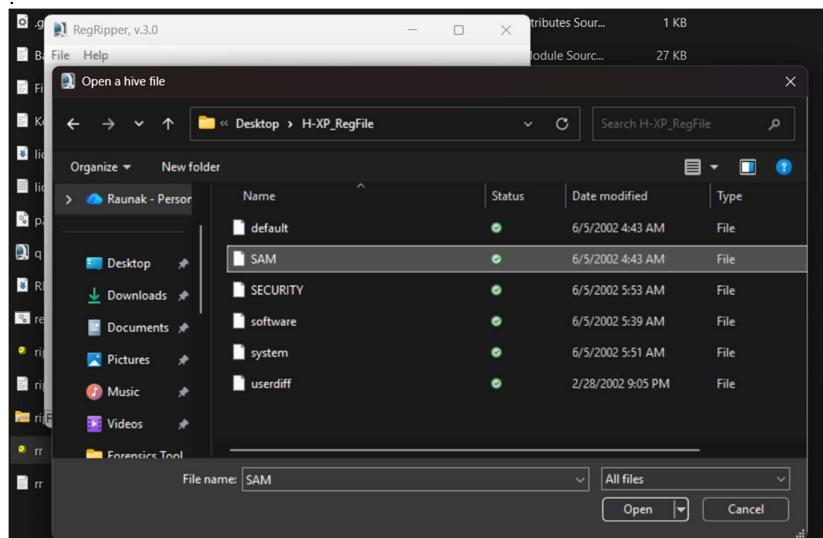
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 

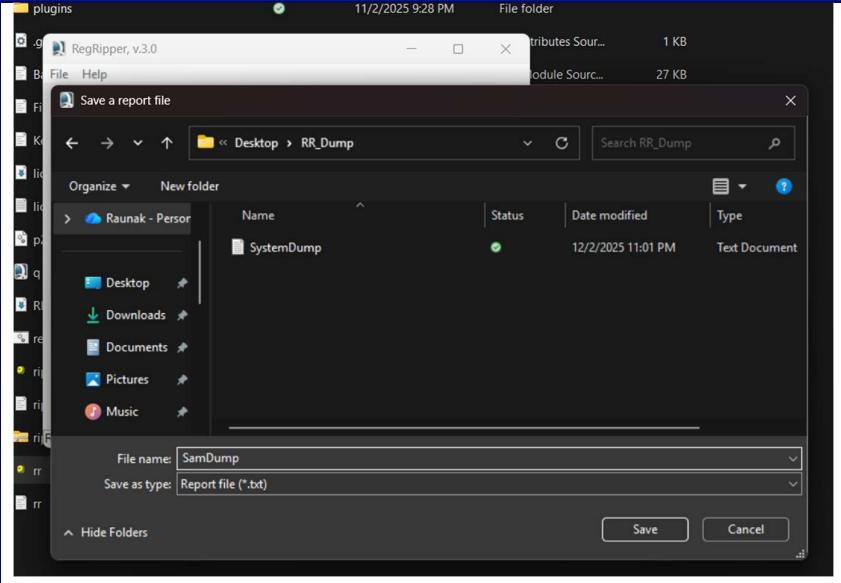
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p>I saved the dump as SystemDump.txt.</p> 

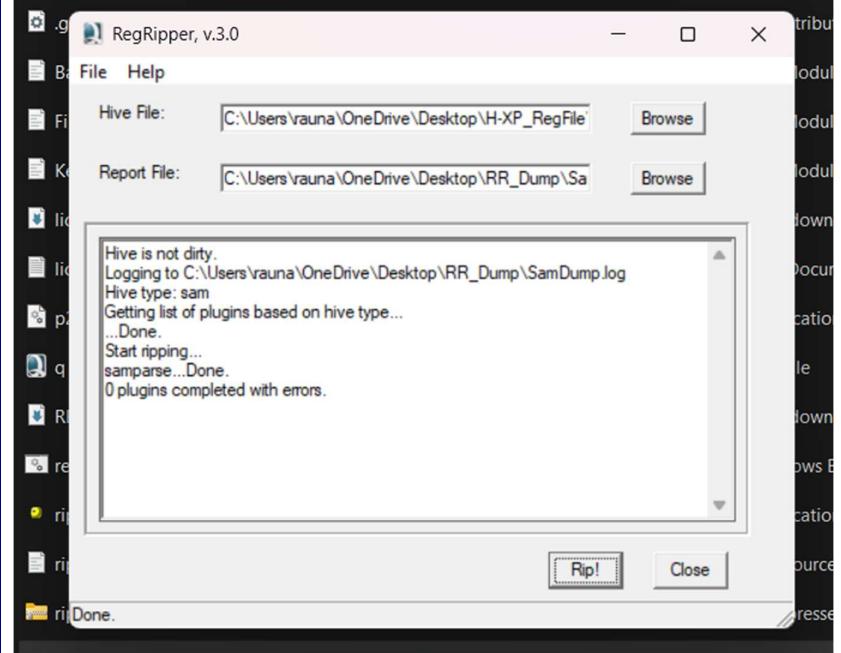
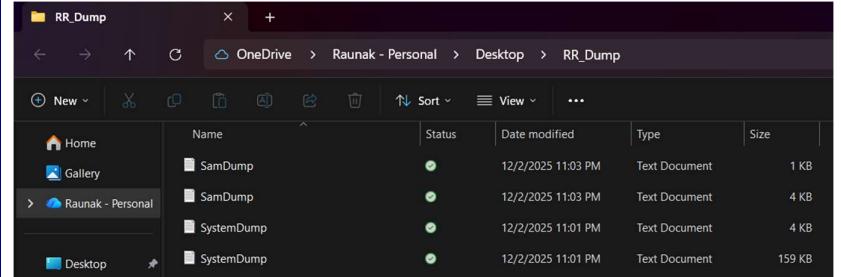
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>RegRipper, v.3.0</p> <p>File Help</p> <p>Hive File: C:\Users\vauna\OneDrive\Desktop\H-XP_RegFile <input type="button" value="Browse"/></p> <p>Report File: C:\Users\vauna\OneDrive\Desktop\RR_Dump\Sy: <input type="button" value="Browse"/></p> <p>NOTE: This tool does NOT automatically process and incorporate Registry hive transaction logs. The tool will check to see if the hive is dirty.</p> <p>If you need to process/incorporate transaction logs, please consider using yarp + registryFlush.py (Maxim Suhnov) or rla.exe (Eric Zimmerman).</p> <p>Rip! <input type="button" value="Close"/></p> <p>Ready.</p>

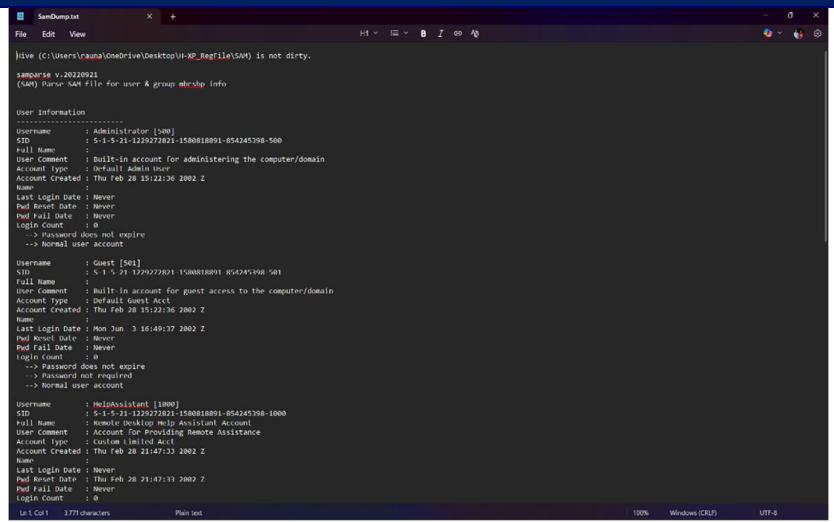
Action	Done?	Date (YY/MM/DD)	Time	Notes																									
				 <p>RegRipper, v.3.0</p> <p>Hive File: C:\Users\vauna\OneDrive\Desktop\H-XP_RegFile</p> <p>Report File: C:\Users\vauna\OneDrive\Desktop\RR_Dump\SystemDump.txt</p> <pre> shimcache...Done. shutdown...Done. source_os...Done. svc...Done. svcdll...Done. termcert...Done. termserv...Done. timezone...Done. usb...Done. usbdevices...Done. usbstor...Done. wpdbusenum...Done. 0 plugins completed with errors. </pre> <p>Rip! Close Done.</p> <p>Finally, System was ripped and we got the .txt file.</p>  <table border="1"> <thead> <tr> <th>Name</th> <th>Status</th> <th>Date modified</th> <th>Type</th> <th>Size</th> </tr> </thead> <tbody> <tr> <td>SamDump</td> <td>✓</td> <td>12/2/2025 11:03 PM</td> <td>Text Document</td> <td>1 KB</td> </tr> <tr> <td>SamDump</td> <td>✓</td> <td>12/2/2025 11:03 PM</td> <td>Text Document</td> <td>4 KB</td> </tr> <tr> <td>SystemDump</td> <td>✓</td> <td>12/2/2025 11:01 PM</td> <td>Text Document</td> <td>4 KB</td> </tr> <tr> <td>SystemDump</td> <td>✓</td> <td>12/2/2025 11:01 PM</td> <td>Text Document</td> <td>159 KB</td> </tr> </tbody> </table> <p>I opened SystemDump.txt to get information about Time Zone.</p>	Name	Status	Date modified	Type	Size	SamDump	✓	12/2/2025 11:03 PM	Text Document	1 KB	SamDump	✓	12/2/2025 11:03 PM	Text Document	4 KB	SystemDump	✓	12/2/2025 11:01 PM	Text Document	4 KB	SystemDump	✓	12/2/2025 11:01 PM	Text Document	159 KB
Name	Status	Date modified	Type	Size																									
SamDump	✓	12/2/2025 11:03 PM	Text Document	1 KB																									
SamDump	✓	12/2/2025 11:03 PM	Text Document	4 KB																									
SystemDump	✓	12/2/2025 11:01 PM	Text Document	4 KB																									
SystemDump	✓	12/2/2025 11:01 PM	Text Document	159 KB																									

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>After Scrolling down, I got time zone information.</p> <pre> ----- <b>timezone v.20200518</b> (<b>System</b>) Get <b>TimeZoneInformation</b> key contents  <b>TimeZoneInformation</b> key <b>ControlSet001\Control\TimeZoneInformation</b> <b>LastWrite Time</b> 2002-04-18 14:33:31Z   <b>DaylightName</b>    -&gt; Central Daylight Time   <b>StandardName</b>   -&gt; Central Standard Time   <b>Bias</b>          -&gt; 360 (6 hours)   <b>ActiveTimeBias</b> -&gt; 300 (5 hours) ----- </pre> <p>Similarly, For Sam Registry, I loaded it on reg ripper.</p>

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

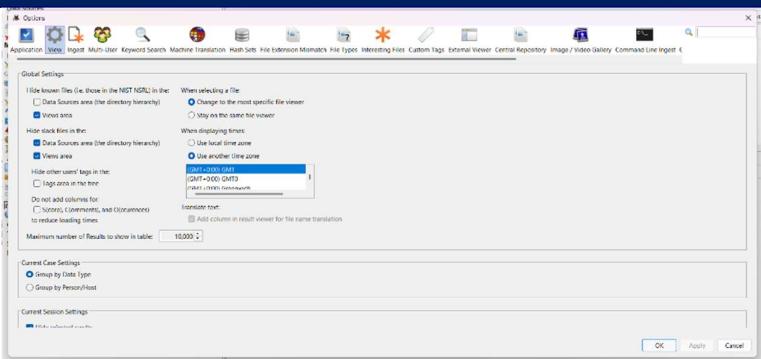
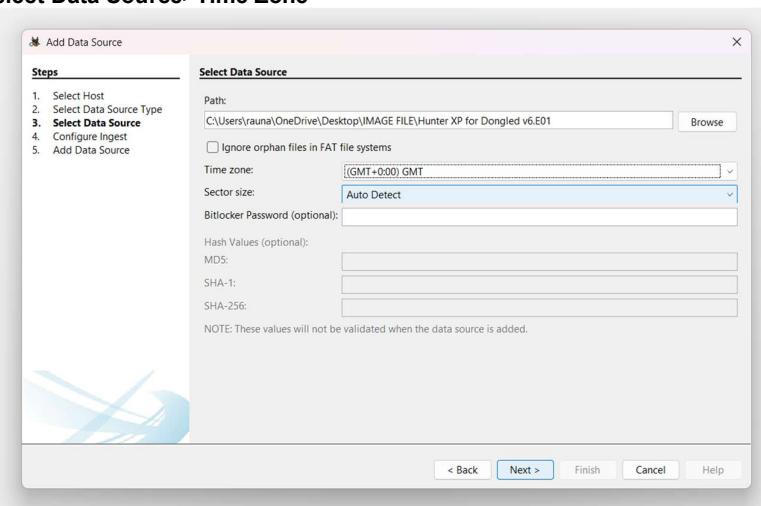
Action	Done?	Date (YY/MM/DD)	Time	Notes
				

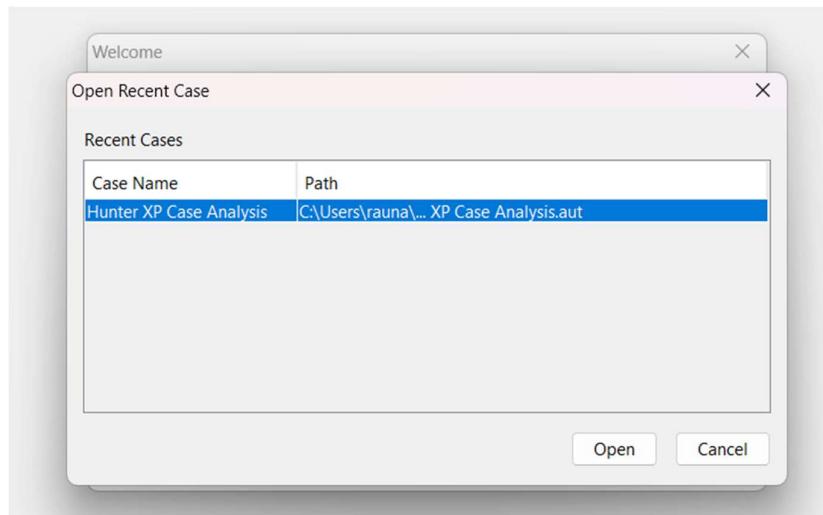
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>I ripped SAM in reg ripper and got detailed information in .txt format.</p>  <p>I opened SamDump.txt and got information about Users.</p>

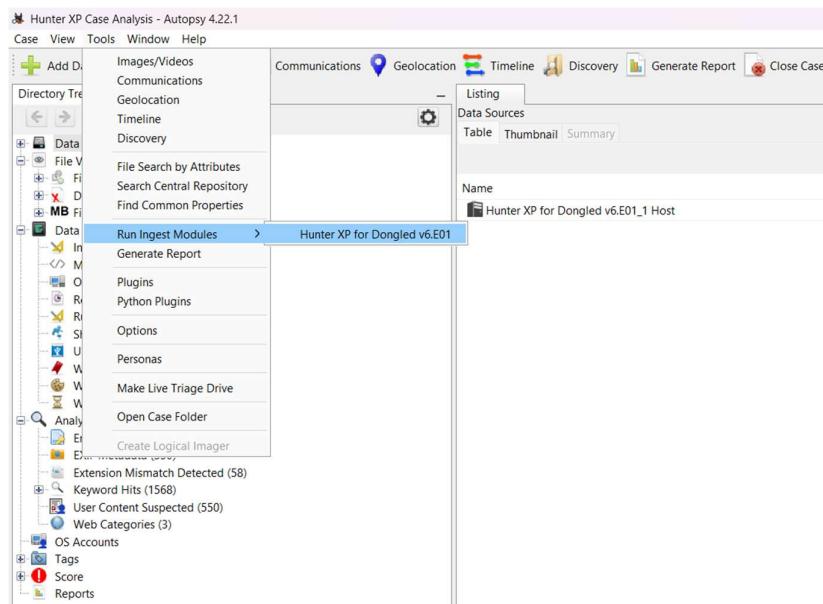
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <pre> SamDump.txt  File Edit View H I B Z A  java -jar C:\users\lauan\OneDrive\Desktop\UXP_RegFile\Samdump.jar  samparse v2.02202921 (SAM) Parse SAM file for user &amp; group membership info  User Information ----- Username : Administrator [S-0-0] SID : S-1-5-21-1234567890-1234567890-1234567890-500 Full Name : User Comment : Built-in account for administering the computer/domain Account Type : Default Admin User Account Created : Thu Feb 28 23:22:36 2002 Z Name : Last Login Date : Never Pad Reset Date : Never Pad Fail Date : Never Login Count : 0 --&gt; Password does not expire --&gt; Account does not expire --&gt; Normal user account  Username : Guest [S-0-1] SID : S-1-5-21-1234567890-1234567890-1234567890-501 Full Name : Built-in account for guest access to the computer/domain User Comment : Account Type : Default Guest Acc Account Created : Thu Feb 28 23:22:36 2002 Z Name : Last Login Date : Mon Jun 3 16:49:37 2002 Z Pad Reset Date : Never Pad Fail Date : Never Login Count : 0 --&gt; Password does not expire --&gt; Account does not expire --&gt; Normal user account  Username : HelpAssistant [S-0-1000] SID : S-1-5-21-1234567890-1234567890-1234567890-1000 Full Name : Remote Desktop Help Assistant Account User Comment : Account used for running Remote Assistance Account Type : Custom Limited Acc Account Created : Thu Feb 28 23:47:33 2002 Z Name : Last Login Date : Never Pad Reset Date : Thu Feb 28 23:47:33 2002 Z Pad Fail Date : Never Login Count : 0 Ln 1 Col 1 3771 characters Plain text. 100% Windows (CRU) UTF-8 </pre>

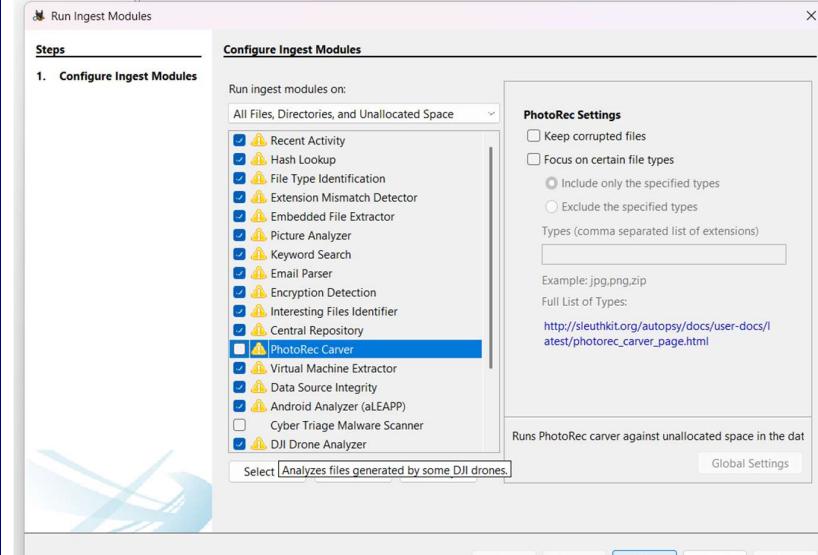
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<pre>User Information ----- Username      : Administrator [500] SID          : S-1-5-21-1229272821-1580818891-854245398-500 Full Name    : User Comment  : Built-in account for administering the computer/domain Account Type  : Default Admin User Account Created : Thu Feb 28 15:22:36 2002 Z Name         : Last Login Date : Never Pwd Reset Date : Never Pwd Fail Date  : Never Login Count    : 0 --&gt; Password does not expire --&gt; Normal user account  Username      : Guest [501] SID          : S-1-5-21-1229272821-1580818891-854245398-501 Full Name    : User Comment  : Built-in account for guest access to the computer/domain Account Type  : Default Guest Acct Account Created : Thu Feb 28 15:22:36 2002 Z Name         : Last Login Date : Mon Jun  3 16:49:37 2002 Z Pwd Reset Date : Never Pwd Fail Date  : Never Login Count    : 0 --&gt; Password does not expire --&gt; Password not required --&gt; Normal user account  Username      : HelpAssistant [1000] SID          : S-1-5-21-1229272821-1580818891-854245398-1000 Full Name    : Remote Desktop Help Assistant Account User Comment  : Account for Providing Remote Assistance Account Type  : Custom Limited Acct Account Created : Thu Feb 28 21:47:33 2002 Z Name         : Last Login Date : Never Pwd Reset Date : Thu Feb 28 21:47:33 2002 Z Pwd Fail Date  : Never Login Count    : 0 --&gt; Password does not expire --&gt; Normal user account</pre>

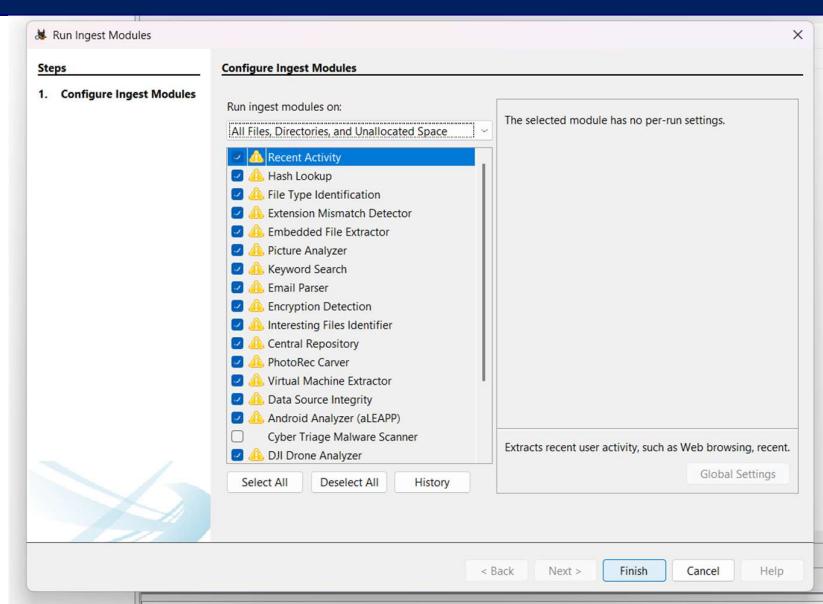
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<pre> Username      : SUPPORT_388945a0 [1002] SID          : S-1-5-21-1229272821-1580818891-854245398-1002 Full Name    : CN=Microsoft Corporation,L=Redmond,S=Washington,C=US User Comment  : This is a vendor's account for the Help and Support Service Account Type : Custom Limited Acct Account Created : Thu Feb 28 21:56:13 2002 Z Name         : Last Login Date : Never Pwd Reset Date : Thu Feb 28 21:56:13 2002 Z Pwd Fail Date : Never Login Count   : 0     --&gt; Password does not expire     --&gt; Account Disabled     --&gt; Normal user account  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  Group Membership Information ----- Group Name   : Users [2] LastWrite    : Thu Feb 28 15:25:12 2002 Z Group Comment: Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications Users       : S-1-5-4 S-1-5-11  Group Name   : Guests [1] LastWrite    : Thu Feb 28 15:22:36 2002 Z Group Comment: Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted Users       : S-1-5-21-1229272821-1580818891-854245398-501  Group Name   : Administrators [2] LastWrite    : Thu Feb 28 22:22:17 2002 Z Group Comment: Administrators have complete and unrestricted access to the computer Users       : S-1-5-21-1229272821-1580818891-854245398-500 S-1-5-21-1229272821-1580818891-854245398-1004  Analysis Tips: - For more known SIDs, see <a href="http://support.microsoft.com/kb/242330">http://support.microsoft.com/kb/242330</a>   - S-1-5-4 = Interactive   - S-1-5-11 = Authenticated Users - Correlate the user SIDs to the output of the ProfileList plugin </pre> <p>Here, I got all information about the users.</p>
Time Zone Adjusted? Report Time Zone used for Analysis.	Done	2025/12/8	6:10 PM (UTC +5:45)	<p>For this we can adjust the time zone at the start of loading the case as shown here.</p> <p>We can adjust time zone as follows: <b>TOOLS&gt;OPTIONS&gt;VIEW&gt;While Displaying Times</b></p>

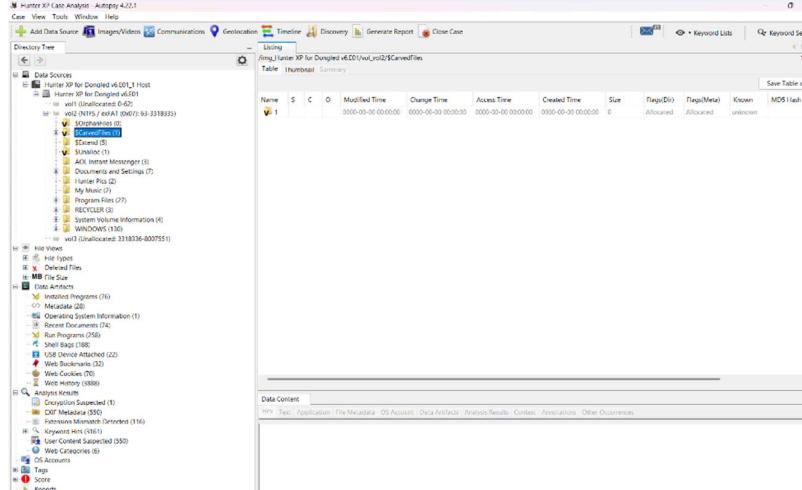
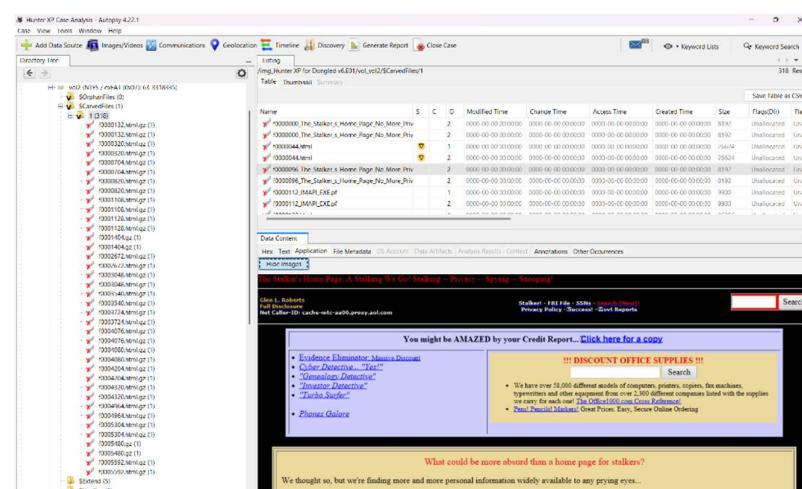
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>While adding the case, we can set it normally by:  <b>Process:</b>  <b>Select Data Source&gt;Time Zone</b></p>  <p>Time zone used for analysis is <b>(GMT +0:00) GMT</b>.</p>

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

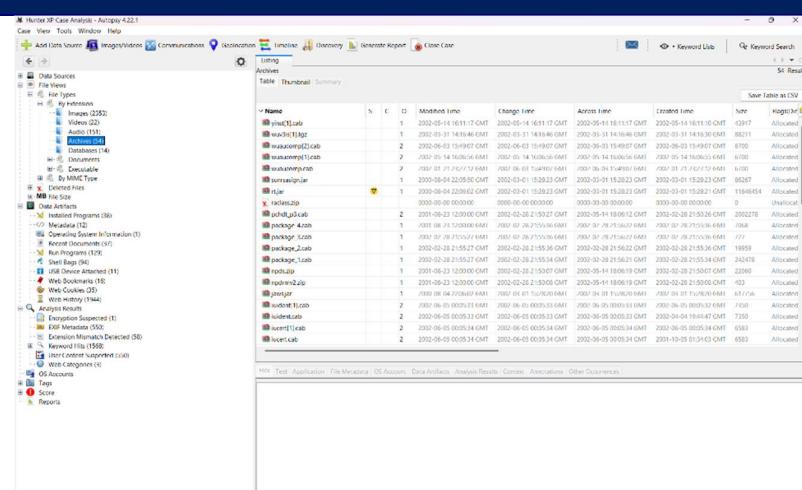
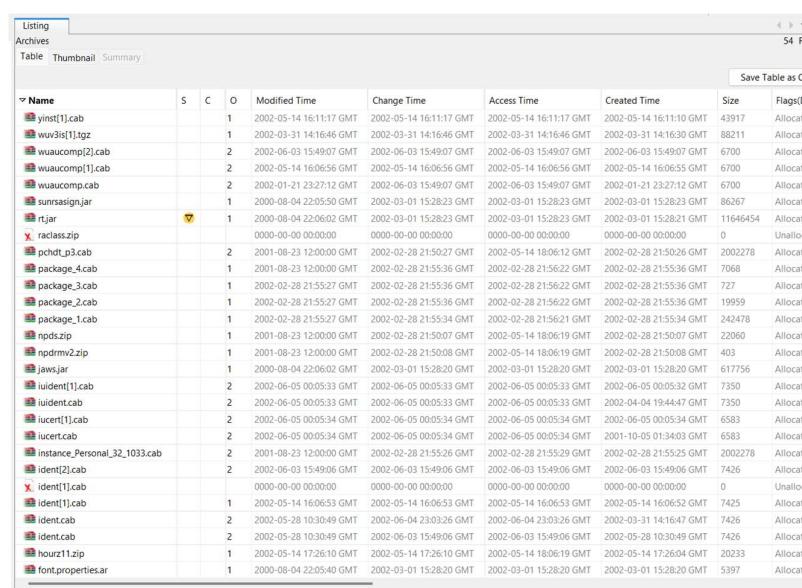
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p>To recover the lost folders, we go through the procedure of getting access of the lost files in the image. We do that by;</p> <p><b>Tools&gt;Run Ingest Modules&gt;PhotoRec Carver</b></p> 

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

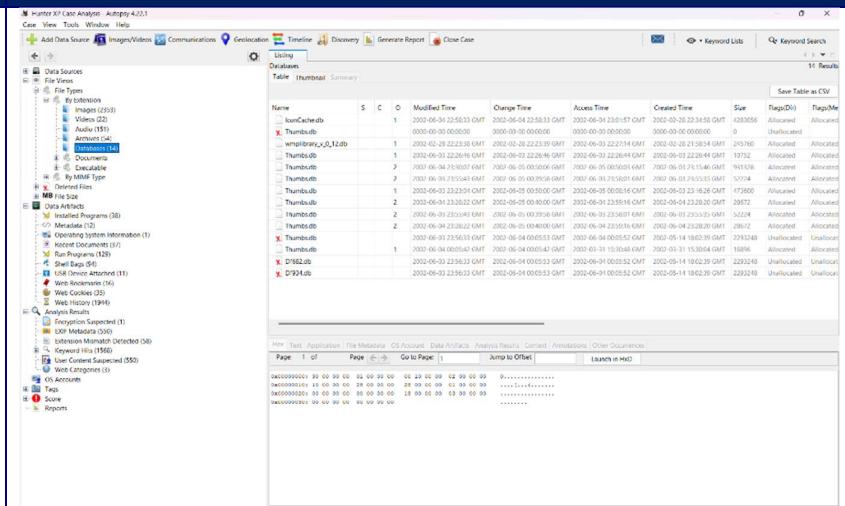
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>After selecting PhotoRec Caver Module we click finish and proceed. By selecting PhotoRec Caver we get access to these:</p> <p>Process: <b>Vol-Vol2&gt;CarvedFiles&gt;1</b></p> <p><b>Here we have File System with 318 items:</b></p>

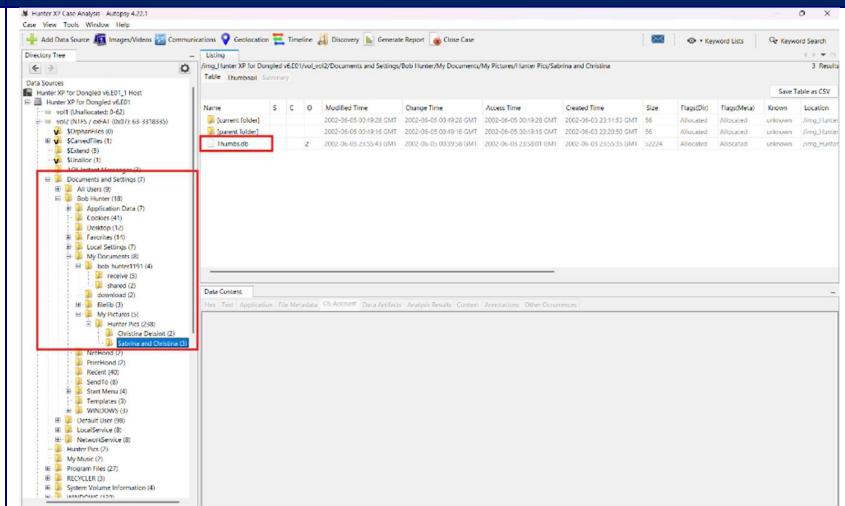
Action	Done?	Date (YY/MM/DD)	Time	Notes
				
				 <p>Here, we have File System with 1978 items. And All Files with 2296 items:</p>

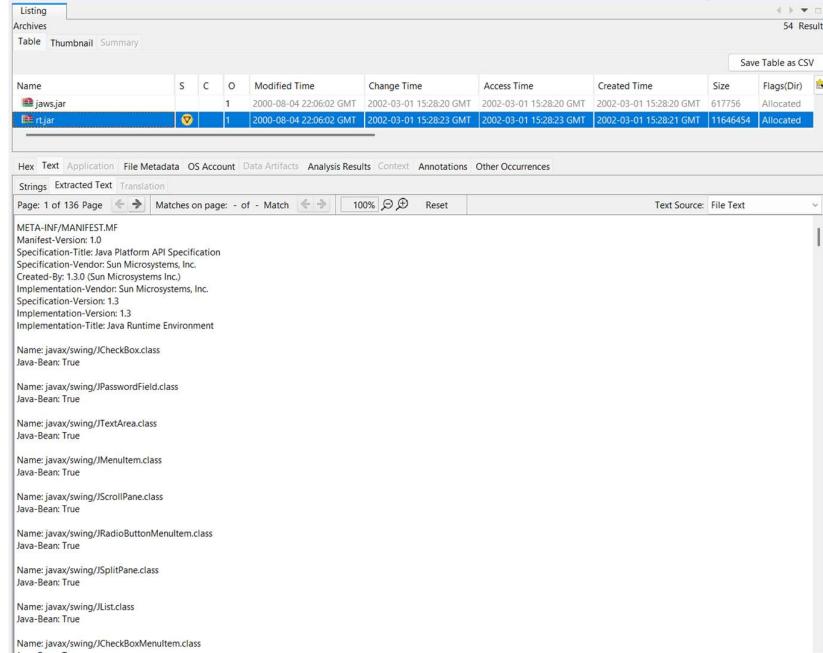


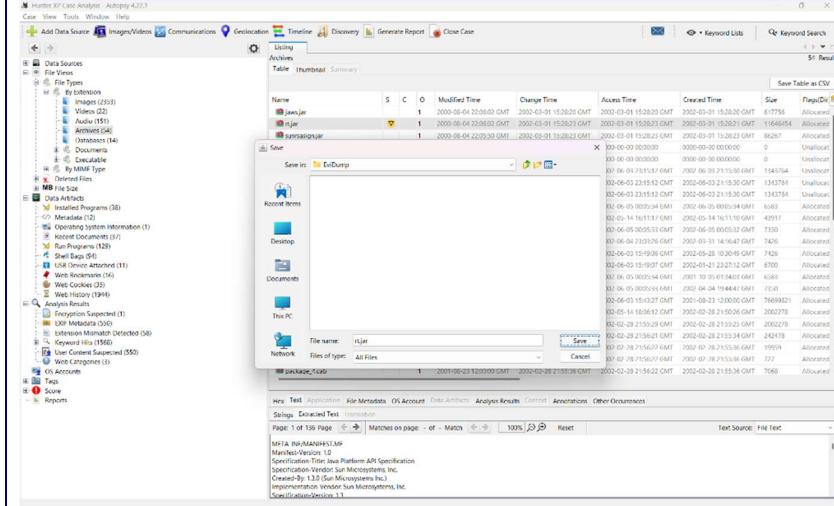
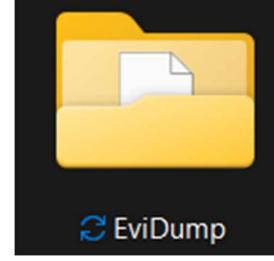
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>The screenshot shows the Merkle XP Case Analysis interface. At the top, there's a navigation bar with 'File', 'View', 'Tools', 'Window', 'Help'. Below it is a toolbar with icons for 'Add Data Source', 'Integrations', 'Communications', 'Dashboard', 'File Explorer', 'Diversity', 'Remote Report', and 'Close Case'. The main area has tabs for 'Listing' and 'Archives'. A search bar at the top right contains 'Keyword List' and 'Keyword Search' fields, with a 'Save Table as CSV' button. The 'Thumbnail' tab is selected, showing a summary of files. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and FlagsDir. The table lists numerous files, many of which are marked as 'Allocated'. Some entries have small yellow warning icons next to them.</p>
				 <p>This screenshot shows another view of the Merkle XP Case Analysis interface, likely a different section or a refresh of the same screen. It features a similar layout with a toolbar, search bar, and a table of file metadata. The table columns are identical: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and FlagsDir. The list of files includes many previously seen entries like 'yinst[1].cab', 'wuaucomp[1].cab', and various 'package_x.cab' files, along with new ones like 'font.properties.ar' and 'hour11.zip'. The 'Allocated' status is consistently shown for most files.</p>

Action	Done?	Date (YY/MM/DD)	Time	Notes																																																																																																																																																																																																																																																																																																												
				<p>Listing Archives Table Thumbnail Summary</p> <p>Save Table as CSV</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> <th>Size</th> <th>Flags/Dir</th> </tr> </thead> <tbody> <tr><td>hour21.zip</td><td></td><td>1</td><td></td><td>2002-05-14 17:26:10 GMT</td><td>2002-05-14 17:26:10 GMT</td><td>2002-05-14 18:06:19 GMT</td><td>2002-05-14 17:26:04 GMT</td><td>20233</td><td>Allocated</td></tr> <tr><td>font.properties.ar</td><td></td><td>1</td><td></td><td>2000-08-04 22:05:40 GMT</td><td>2002-03-01 15:28:20 GMT</td><td>2002-03-01 15:28:20 GMT</td><td>2002-03-01 15:28:20 GMT</td><td>5397</td><td>Allocated</td></tr> <tr><td>f0005592.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>2048</td><td>Unallocat.</td></tr> <tr><td>f0005480.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>57344</td><td>Unallocat.</td></tr> <tr><td>f0005304.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>22528</td><td>Unallocat.</td></tr> <tr><td>f0004964.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>38912</td><td>Unallocat.</td></tr> <tr><td>f0004320.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>71680</td><td>Unallocat.</td></tr> <tr><td>f0004204.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>59392</td><td>Unallocat.</td></tr> <tr><td>f0004080.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>63488</td><td>Unallocat.</td></tr> <tr><td>f0004076.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>2048</td><td>Unallocat.</td></tr> <tr><td>f0003724.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>2048</td><td>Unallocat.</td></tr> <tr><td>f0003540.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>94208</td><td>Unallocat.</td></tr> <tr><td>f0003076.cab</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>212</td><td>Unallocat.</td></tr> <tr><td>f0003046.cab</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>937</td><td>Unallocat.</td></tr> <tr><td>f0003056.cab</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>4096</td><td>Unallocat.</td></tr> <tr><td>f0003048.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>4096</td><td>Unallocat.</td></tr> <tr><td>f0002672.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>20480</td><td>Unallocat.</td></tr> <tr><td>f0001404.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>34016</td><td>Unallocat.</td></tr> <tr><td>f0001128.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>116736</td><td>Unallocat.</td></tr> <tr><td>f0001108.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>10240</td><td>Unallocat.</td></tr> <tr><td>f0000820.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>2048</td><td>Unallocat.</td></tr> <tr><td>f0000704.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>24576</td><td>Unallocat.</td></tr> <tr><td>f0000320.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>4096</td><td>Unallocat.</td></tr> <tr><td>f0000132.html.gz</td><td></td><td>1</td><td></td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>0000-00-00 00:00:00</td><td>96256</td><td>Unallocat.</td></tr> <tr><td>driver.cab</td><td></td><td>1</td><td></td><td>2001-08-23 12:00:00 GMT</td><td>2002-02-28 15:25:18 GMT</td><td>2002-06-03 15:43:27 GMT</td><td>2001-08-23 12:00:00 GMT</td><td>76699621</td><td>Allocated</td></tr> <tr><td>D19352.zip</td><td></td><td></td><td></td><td>2002-06-03 21:15:33 GMT</td><td>2002-06-03 23:23:54 GMT</td><td>2002-06-03 23:15:12 GMT</td><td>2002-06-03 21:15:30 GMT</td><td>1343764</td><td>Unallocat.</td></tr> <tr><td>D1782.zip</td><td></td><td></td><td></td><td>2002-06-03 21:15:33 GMT</td><td>2002-06-03 23:23:54 GMT</td><td>2002-06-03 23:15:12 GMT</td><td>2002-06-03 21:15:30 GMT</td><td>1343764</td><td>Unallocat.</td></tr> <tr><td>D1389.zip</td><td></td><td></td><td></td><td>2002-06-03 21:15:33 GMT</td><td>2002-06-03 23:23:54 GMT</td><td>2002-06-03 23:15:12 GMT</td><td>2002-06-03 21:15:30 GMT</td><td>1343764</td><td>Unallocat.</td></tr> <tr><td>CURREX-1.zip</td><td></td><td>1</td><td></td><td>2002-05-14 17:26:26 GMT</td><td>2002-05-14 17:26:26 GMT</td><td>2002-05-14 18:06:19 GMT</td><td>2002-05-14 17:26:24 GMT</td><td>2324</td><td>Allocated</td></tr> </tbody> </table> <p>Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences</p> <p>The zip files are located here.</p> <p>As for thumbs.db we go to this location Firstly, Location: <b>Files Views&gt;File Types&gt;By Extension&gt;Databases</b></p>	Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags/Dir	hour21.zip		1		2002-05-14 17:26:10 GMT	2002-05-14 17:26:10 GMT	2002-05-14 18:06:19 GMT	2002-05-14 17:26:04 GMT	20233	Allocated	font.properties.ar		1		2000-08-04 22:05:40 GMT	2002-03-01 15:28:20 GMT	2002-03-01 15:28:20 GMT	2002-03-01 15:28:20 GMT	5397	Allocated	f0005592.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2048	Unallocat.	f0005480.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	57344	Unallocat.	f0005304.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	22528	Unallocat.	f0004964.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	38912	Unallocat.	f0004320.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	71680	Unallocat.	f0004204.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	59392	Unallocat.	f0004080.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	63488	Unallocat.	f0004076.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2048	Unallocat.	f0003724.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2048	Unallocat.	f0003540.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	94208	Unallocat.	f0003076.cab		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	212	Unallocat.	f0003046.cab		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	937	Unallocat.	f0003056.cab		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocat.	f0003048.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocat.	f0002672.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20480	Unallocat.	f0001404.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	34016	Unallocat.	f0001128.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	116736	Unallocat.	f0001108.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10240	Unallocat.	f0000820.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2048	Unallocat.	f0000704.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	24576	Unallocat.	f0000320.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocat.	f0000132.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	96256	Unallocat.	driver.cab		1		2001-08-23 12:00:00 GMT	2002-02-28 15:25:18 GMT	2002-06-03 15:43:27 GMT	2001-08-23 12:00:00 GMT	76699621	Allocated	D19352.zip				2002-06-03 21:15:33 GMT	2002-06-03 23:23:54 GMT	2002-06-03 23:15:12 GMT	2002-06-03 21:15:30 GMT	1343764	Unallocat.	D1782.zip				2002-06-03 21:15:33 GMT	2002-06-03 23:23:54 GMT	2002-06-03 23:15:12 GMT	2002-06-03 21:15:30 GMT	1343764	Unallocat.	D1389.zip				2002-06-03 21:15:33 GMT	2002-06-03 23:23:54 GMT	2002-06-03 23:15:12 GMT	2002-06-03 21:15:30 GMT	1343764	Unallocat.	CURREX-1.zip		1		2002-05-14 17:26:26 GMT	2002-05-14 17:26:26 GMT	2002-05-14 18:06:19 GMT	2002-05-14 17:26:24 GMT	2324	Allocated
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags/Dir																																																																																																																																																																																																																																																																																																							
hour21.zip		1		2002-05-14 17:26:10 GMT	2002-05-14 17:26:10 GMT	2002-05-14 18:06:19 GMT	2002-05-14 17:26:04 GMT	20233	Allocated																																																																																																																																																																																																																																																																																																							
font.properties.ar		1		2000-08-04 22:05:40 GMT	2002-03-01 15:28:20 GMT	2002-03-01 15:28:20 GMT	2002-03-01 15:28:20 GMT	5397	Allocated																																																																																																																																																																																																																																																																																																							
f0005592.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2048	Unallocat.																																																																																																																																																																																																																																																																																																							
f0005480.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	57344	Unallocat.																																																																																																																																																																																																																																																																																																							
f0005304.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	22528	Unallocat.																																																																																																																																																																																																																																																																																																							
f0004964.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	38912	Unallocat.																																																																																																																																																																																																																																																																																																							
f0004320.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	71680	Unallocat.																																																																																																																																																																																																																																																																																																							
f0004204.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	59392	Unallocat.																																																																																																																																																																																																																																																																																																							
f0004080.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	63488	Unallocat.																																																																																																																																																																																																																																																																																																							
f0004076.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2048	Unallocat.																																																																																																																																																																																																																																																																																																							
f0003724.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2048	Unallocat.																																																																																																																																																																																																																																																																																																							
f0003540.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	94208	Unallocat.																																																																																																																																																																																																																																																																																																							
f0003076.cab		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	212	Unallocat.																																																																																																																																																																																																																																																																																																							
f0003046.cab		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	937	Unallocat.																																																																																																																																																																																																																																																																																																							
f0003056.cab		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocat.																																																																																																																																																																																																																																																																																																							
f0003048.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocat.																																																																																																																																																																																																																																																																																																							
f0002672.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20480	Unallocat.																																																																																																																																																																																																																																																																																																							
f0001404.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	34016	Unallocat.																																																																																																																																																																																																																																																																																																							
f0001128.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	116736	Unallocat.																																																																																																																																																																																																																																																																																																							
f0001108.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10240	Unallocat.																																																																																																																																																																																																																																																																																																							
f0000820.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2048	Unallocat.																																																																																																																																																																																																																																																																																																							
f0000704.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	24576	Unallocat.																																																																																																																																																																																																																																																																																																							
f0000320.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocat.																																																																																																																																																																																																																																																																																																							
f0000132.html.gz		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	96256	Unallocat.																																																																																																																																																																																																																																																																																																							
driver.cab		1		2001-08-23 12:00:00 GMT	2002-02-28 15:25:18 GMT	2002-06-03 15:43:27 GMT	2001-08-23 12:00:00 GMT	76699621	Allocated																																																																																																																																																																																																																																																																																																							
D19352.zip				2002-06-03 21:15:33 GMT	2002-06-03 23:23:54 GMT	2002-06-03 23:15:12 GMT	2002-06-03 21:15:30 GMT	1343764	Unallocat.																																																																																																																																																																																																																																																																																																							
D1782.zip				2002-06-03 21:15:33 GMT	2002-06-03 23:23:54 GMT	2002-06-03 23:15:12 GMT	2002-06-03 21:15:30 GMT	1343764	Unallocat.																																																																																																																																																																																																																																																																																																							
D1389.zip				2002-06-03 21:15:33 GMT	2002-06-03 23:23:54 GMT	2002-06-03 23:15:12 GMT	2002-06-03 21:15:30 GMT	1343764	Unallocat.																																																																																																																																																																																																																																																																																																							
CURREX-1.zip		1		2002-05-14 17:26:26 GMT	2002-05-14 17:26:26 GMT	2002-05-14 18:06:19 GMT	2002-05-14 17:26:24 GMT	2324	Allocated																																																																																																																																																																																																																																																																																																							

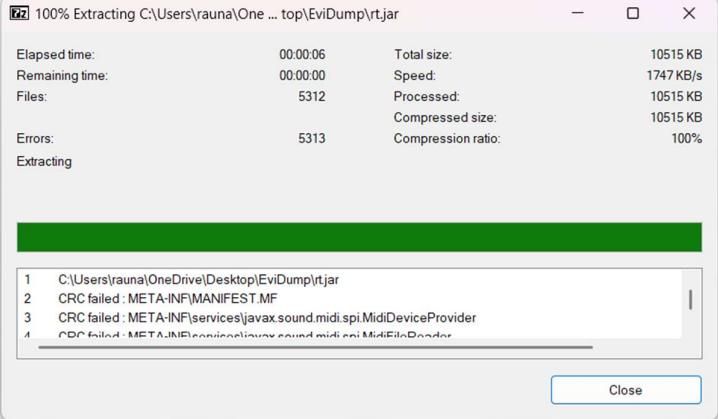
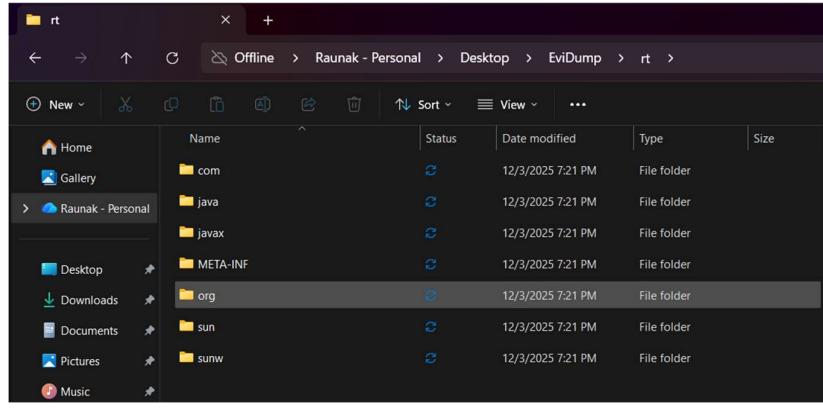
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p>Secondly, Location: <b>Vol-vol2&gt;Documents and setting&gt;bob hunter&gt;my documents&gt;my pictures&gt;hunter pics&gt;Sabrina and Christina</b></p> 

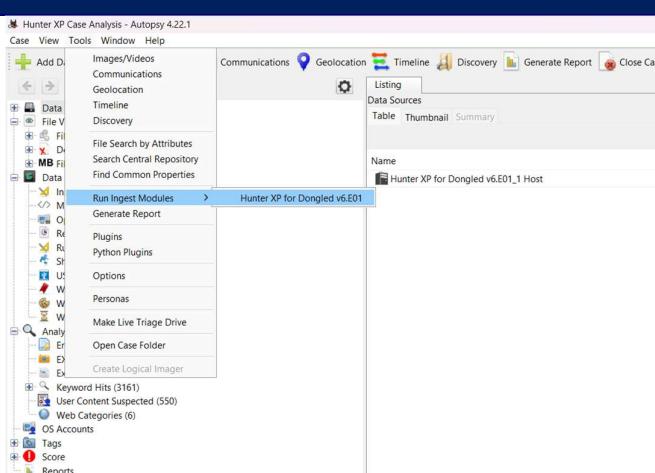
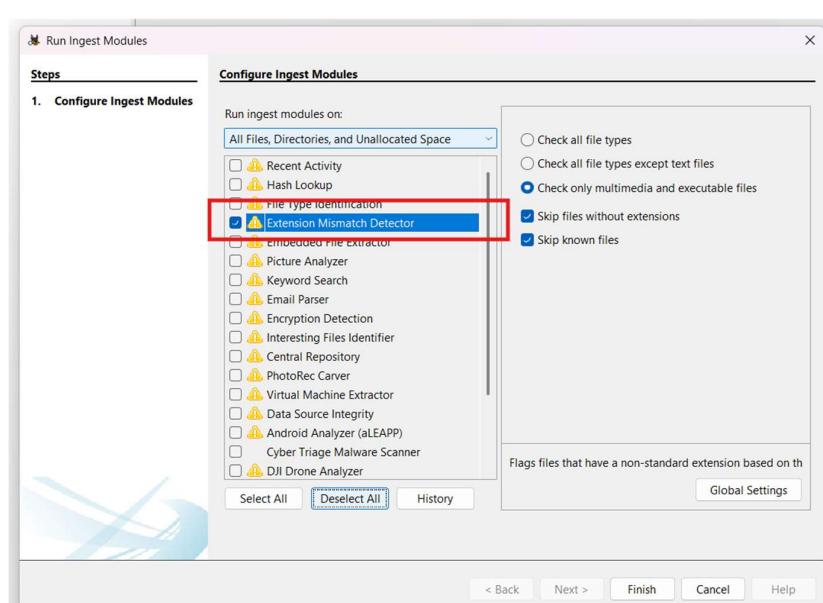
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Here we can find database file i.e. <b>Thumbs.db</b>.</p> <p>To mount it further, I extracted <b>rt.jar</b> zip file in my pc.</p>

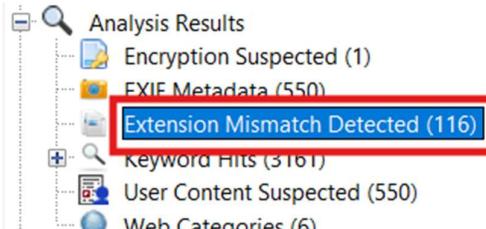
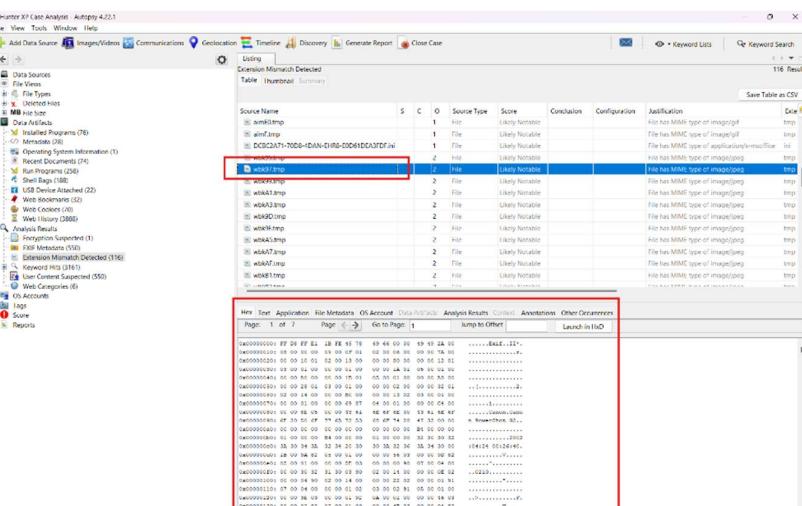
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>The screenshot shows a file analysis interface with two main sections:</p> <ul style="list-style-type: none"> <li><b>File Listing:</b> A table showing file details. The columns are Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). Two files are listed: 'jaws.jar' and 'rt.jar'. 'rt.jar' is selected, indicated by a blue background.</li> <li><b>Extracted Text:</b> A large text area displaying the contents of 'rt.jar'. The text is organized into sections such as META-INF/MANIFEST.MF, Java-Bean: True, and various class names like javax.swing.JButton.class, javax.swing.JList.class, etc.</li> </ul>

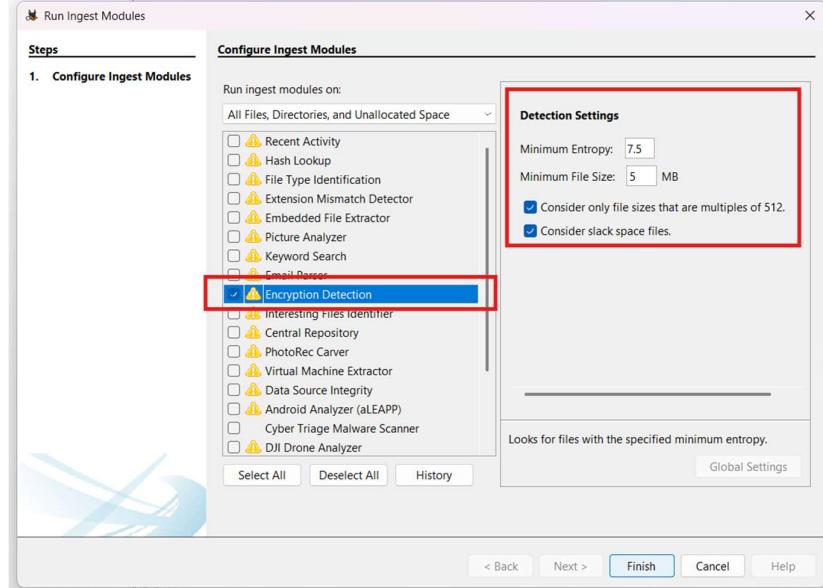
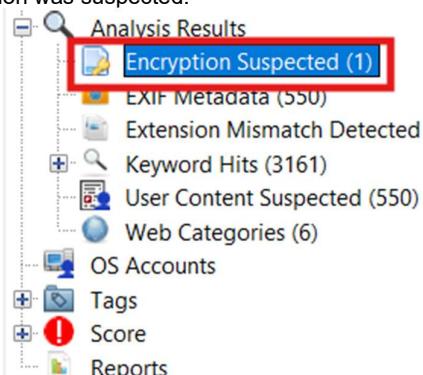
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Location of the extracted file: <b>Desktop&gt;EviDump</b></p>  <p>Then, I extracted it using <b>7-Zip Software</b>.</p>

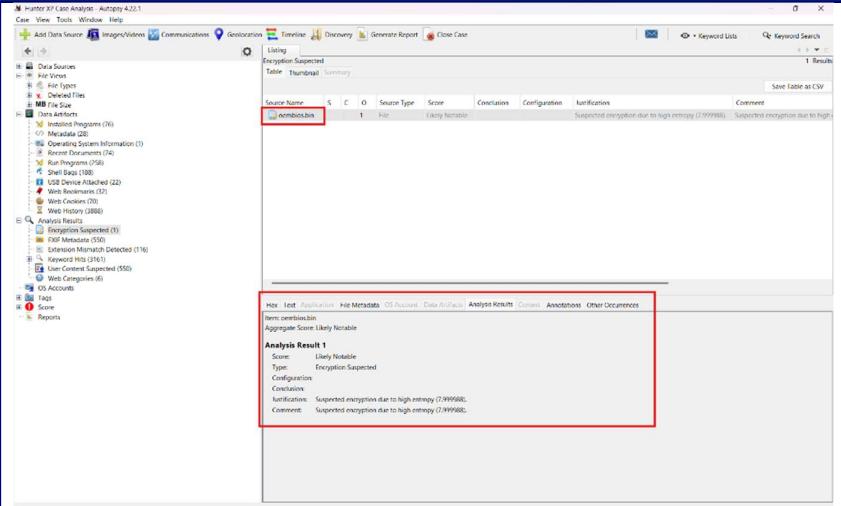
Action	Done?	Date (YY/MM/DD)	Time	Notes																																																																													
				<p>File C:\Users\rauna\OneDrive\</p> <p>File Edit View Favorites Tools Help</p> <p>Add Extract Test Copy Move Delete Info</p> <p>C:\Users\rauna\OneDrive\</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Size</th> <th>Modified</th> <th>Created</th> <th>Comment</th> <th>Folders</th> <th>Files</th> </tr> </thead> <tbody> <tr> <td>Attachments</td> <td></td> <td>2025-10-20...</td> <td>2025-10-20...</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Desktop</td> <td></td> <td>2025-12-03...</td> <td>2025-10-05...</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Documents</td> <td></td> <td>2025-12-03...</td> <td>2025-10-05...</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Pictures</td> <td></td> <td>2025-11-27...</td> <td>2025-10-05...</td> <td></td> <td></td> <td></td> </tr> <tr> <td>.849C9593-D756-4...</td> <td>63</td> <td>2025-12-03...</td> <td>2025-10-05...</td> <td></td> <td></td> <td></td> </tr> <tr> <td>desktop.ini</td> <td>96</td> <td>2025-10-05...</td> <td>2025-10-05...</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Getting started wit...</td> <td>1 053 417</td> <td>2025-10-05...</td> <td>2025-10-05...</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Personal Vault.ink</td> <td>1 140</td> <td>2025-12-03...</td> <td>2025-10-05...</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>File C:\Users\rauna\OneDrive\Desktop\EviDump\</p> <p>File Edit View Favorites Tools Help</p> <p>Add Extract Test Copy Move Delete Info</p> <p>C:\Users\rauna\OneDrive\Desktop\EviDump\</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Size</th> <th>Modified</th> <th>Created</th> <th>Comment</th> <th>Folders</th> <th>Files</th> </tr> </thead> <tbody> <tr> <td>rt.jar</td> <td>11 646 454</td> <td>2025-12-03...</td> <td>2025-12-03...</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Name	Size	Modified	Created	Comment	Folders	Files	Attachments		2025-10-20...	2025-10-20...				Desktop		2025-12-03...	2025-10-05...				Documents		2025-12-03...	2025-10-05...				Pictures		2025-11-27...	2025-10-05...				.849C9593-D756-4...	63	2025-12-03...	2025-10-05...				desktop.ini	96	2025-10-05...	2025-10-05...				Getting started wit...	1 053 417	2025-10-05...	2025-10-05...				Personal Vault.ink	1 140	2025-12-03...	2025-10-05...				Name	Size	Modified	Created	Comment	Folders	Files	rt.jar	11 646 454	2025-12-03...	2025-12-03...			
Name	Size	Modified	Created	Comment	Folders	Files																																																																											
Attachments		2025-10-20...	2025-10-20...																																																																														
Desktop		2025-12-03...	2025-10-05...																																																																														
Documents		2025-12-03...	2025-10-05...																																																																														
Pictures		2025-11-27...	2025-10-05...																																																																														
.849C9593-D756-4...	63	2025-12-03...	2025-10-05...																																																																														
desktop.ini	96	2025-10-05...	2025-10-05...																																																																														
Getting started wit...	1 053 417	2025-10-05...	2025-10-05...																																																																														
Personal Vault.ink	1 140	2025-12-03...	2025-10-05...																																																																														
Name	Size	Modified	Created	Comment	Folders	Files																																																																											
rt.jar	11 646 454	2025-12-03...	2025-12-03...																																																																														

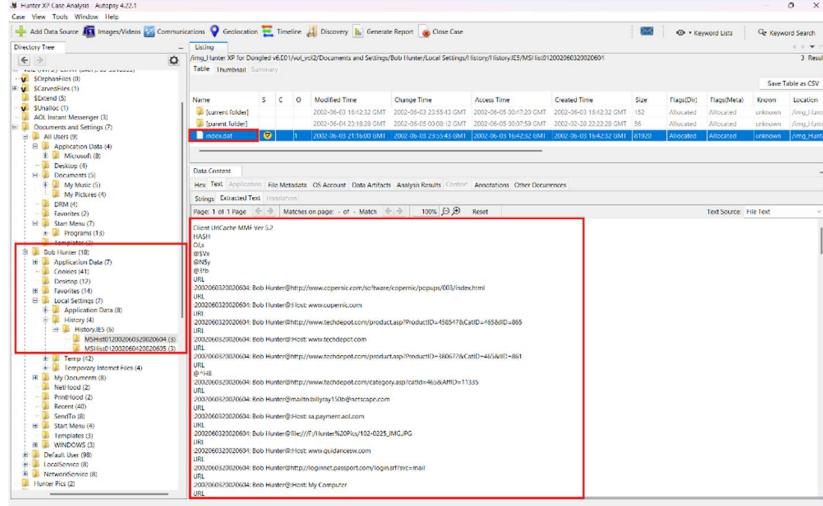
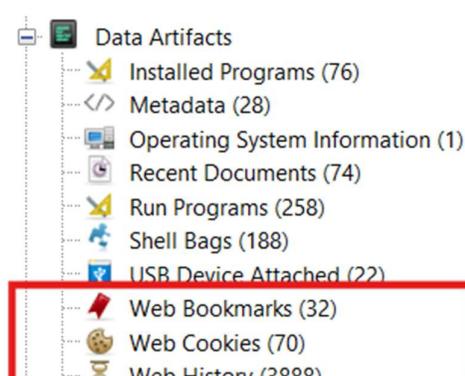
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Lastly, I mounted all of them and maximum were html-oriented files.</p> 
File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation)	Done	2025/12/10	6:30 PM (UTC +5:45)	<p>For this we run a ingest module called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

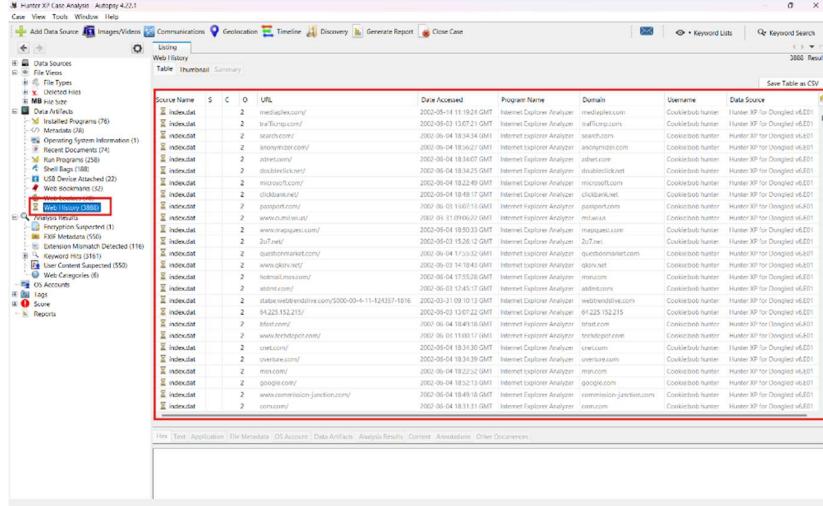
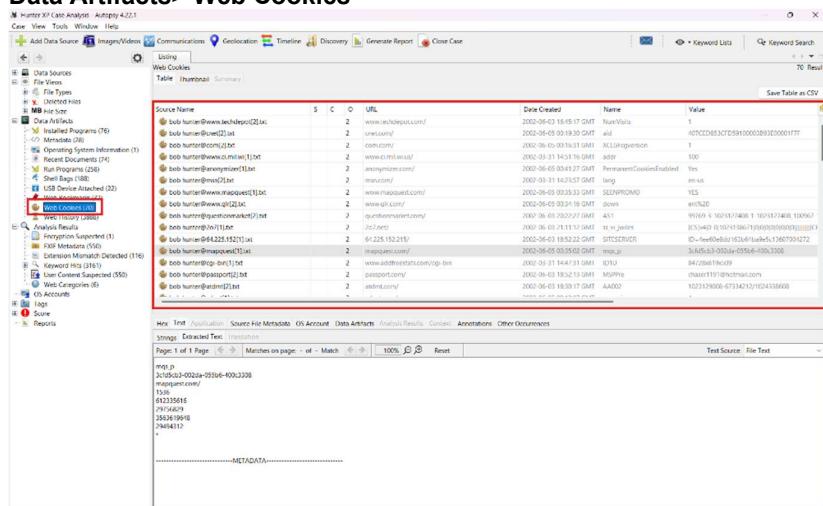
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 

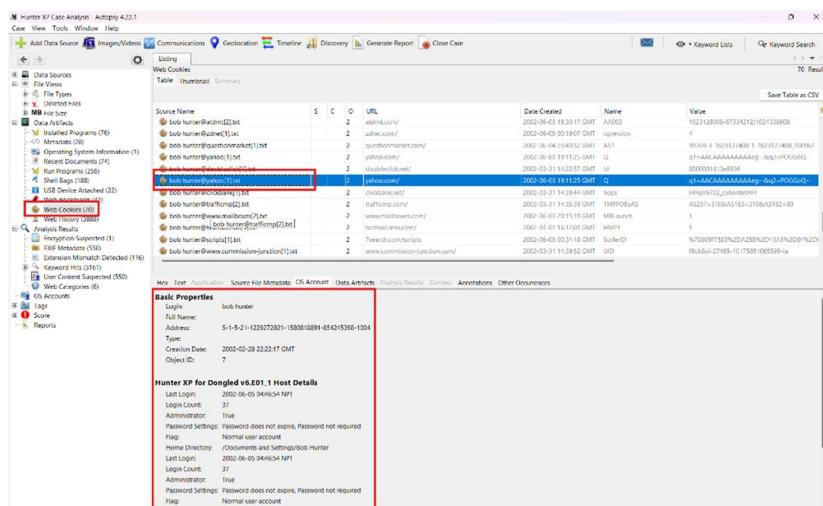
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p>Then we can find mismatch under Analysis Results.</p>  <p>Here 116 files suspected to have extension mismatch has been found.</p>  <p>Here the hash shows that this is a .JPEG file.</p> <p>For Encryption Detection, I used ingest module.</p> <p>Process: <b>TOOLS&gt;RUN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

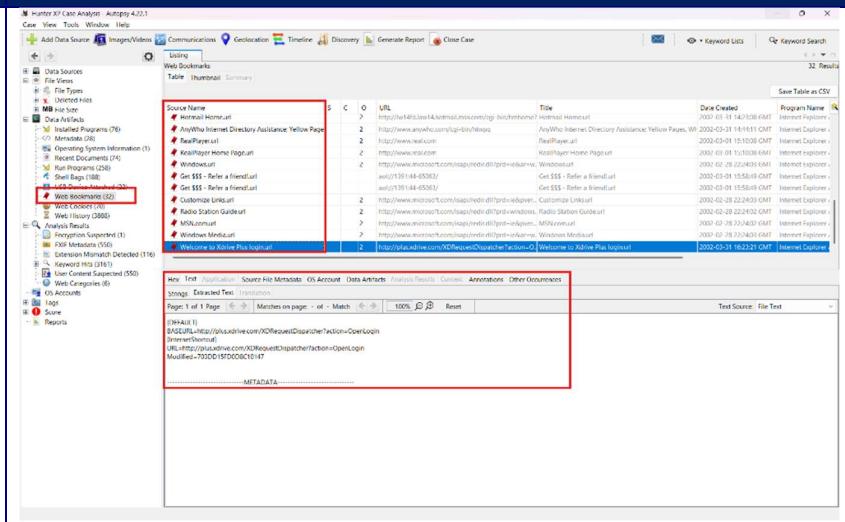
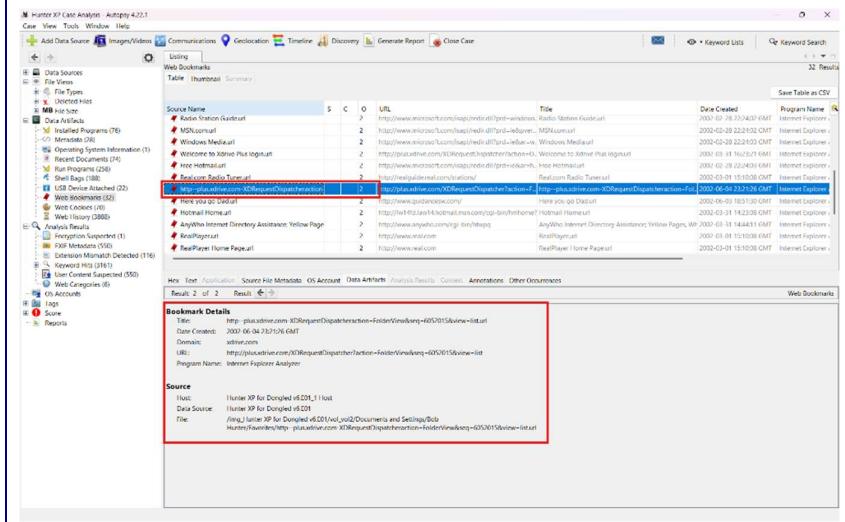
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>The screenshot shows the 'Configure Ingest Modules' dialog. Under 'Steps', the first step is '1. Configure Ingest Modules'. On the left, there is a list of modules with checkboxes: Recent Activity, Hash Lookup, File Type Identification, Extension Mismatch Detector, Embedded File Extractor, Picture Analyzer, Keyword Search, Email Parser, and Encryption Detection. The 'Encryption Detection' checkbox is checked and highlighted with a red box. On the right, there is a 'Detection Settings' section with fields for 'Minimum Entropy' (set to 7.5) and 'Minimum File Size' (set to 5 MB). There are also two checked checkboxes: 'Consider only file sizes that are multiples of 512.' and 'Consider slack space files.'.</p> <p>Here, 1 Encryption was suspected.</p>  <p>The screenshot shows the 'Analysis Results' tree view. The root node is 'Encryption Suspected (1)', which is highlighted with a red box. Other nodes include EXIF Metadata (550), Extension Mismatch Detected (116), Keyword Hits (3161), User Content Suspected (550), Web Categories (6), OS Accounts, Tags, Score, and Reports.</p>

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

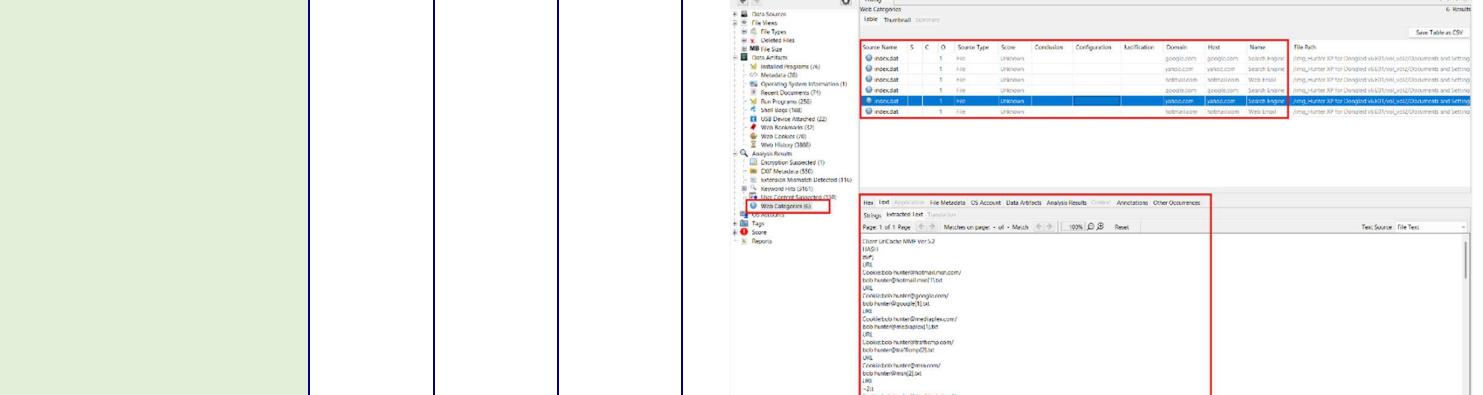
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Here, History can be seen.</p>  <p>Likewise, we can also find web history from <b>Data Artifacts&gt; Web History</b></p>

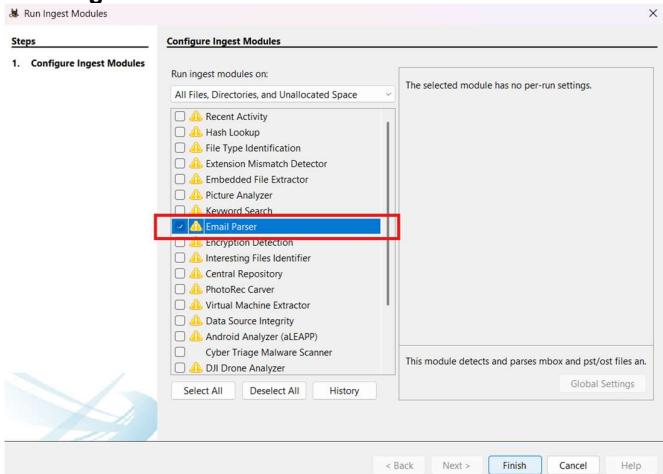
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Likewise, we can also find web cookies from <b>Data Artifacts&gt; Web Cookies</b></p> 

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Likewise, we can also find web bookmarks from <b>Data Artifacts&gt; Web Bookmarks</b></p>

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>The screenshot shows the Hunter X1 Case Analyst interface with the 'Discovery' tab selected. A search query for 'Web Bookmarks' has been entered. The results table displays several entries, each with a source name, count (S), confidence (C), URL, title, date created, and program name. One entry is highlighted with a red box: 'Welcome to Xdrive Plus logon!'. Below the table is a detailed view of this entry, showing its metadata and file test results. The file test results include a search bar and a table of findings.</p>
				 <p>This screenshot shows another search result for 'Web Bookmarks' in the Hunter X1 Case Analyst interface. The results table includes entries such as 'MSN.com', 'Windows Media', and 'Welcome to Xdrive Plus logon!'. One entry is highlighted with a red box: 'Here visit go Discard?'. Below the table is a detailed view of this entry, showing its metadata and file test results. The file test results include a search bar and a table of findings.</p>

Likewise, we can also find web categories from **Data Artifacts> Web Categories**

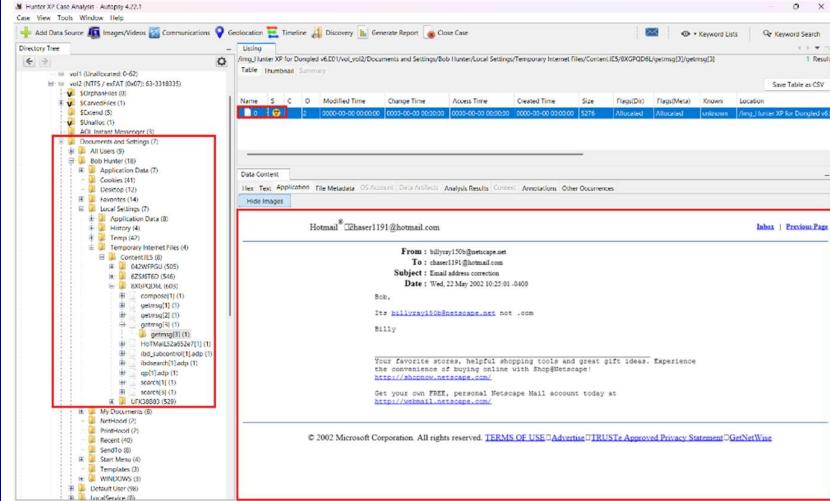
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>The screenshot shows the Hunter ID Case Analysis software interface. The main window displays a search results table for the query "bob hunter". The table includes columns for Source Name, C, O, Score, Confidence, Configuration, Facilitation, Domain, Host, and Name. A red box highlights the first few rows of the table. Below the table is a detailed view of a specific result, also with a red box highlighting it. The detailed view shows a list of URLs and associated data.</p> <pre> Client UrlCache MMF Ver 5.2 HASH z6E] URL Cookie:bob hunter@hotmail.msn.com/ bob hunter@hotmail.msn[1].txt URL Cookie:bob hunter@google.com/ bob hunter@google[1].txt URL Cookie:bob hunter@mediaplex.com/ bob hunter@mediaplex[1].txt URL Cookie:bob hunter@trafficimp.com/ bob hunter@trafficimp[2].txt URL Cookie:bob hunter@msn.com/ bob hunter@msn[2].txt URL ~2t Cookie:bob hunter@doubleclick.net/ bob hunter@doubleclick[1].txt URL Cookie:bob hunter@7search.com/scripts bob hunter@scripts[1].txt URL Cookie:bob hunter@clickbank.net/ bob hunter@clickbank[1].txt URL Cookie:bob hunter@www.addfreestats.com/cgi-bin/ bob hunter@cgi-bin[1].txt URL Cookie:bob hunter@www.commission-junction.com/ bob hunter@www.commission-junction[1].txt URL Cookie:bob hunter@bfast.com/ bob hunter@bfast[2].txt URL Cookie:bob hunter@www.ci.mil.wi.us/bob hunter@www.ci.mil.wi[1].txt URL Cookie:bob hunter@statae.webtrendslive.com/S000-00-4-11-124357-1816bob hunter\$S000-00-4-11-124357-1816[1].txt URL Cookie:bob hunter@mapquest.com/bob hunter@mapquest[1].txt </pre>

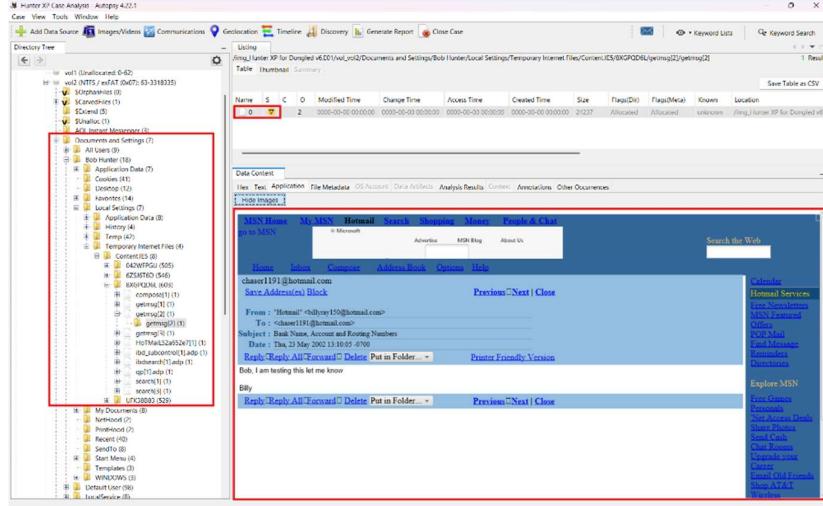
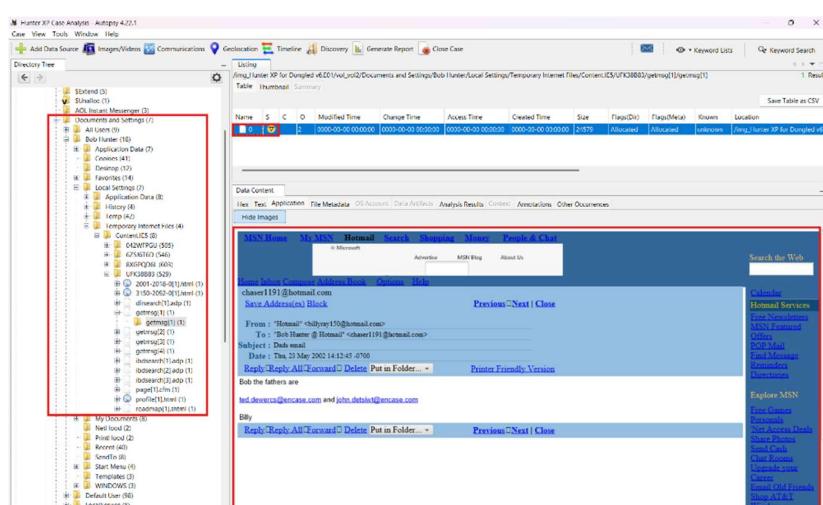
Action	Done?	Date (YY/MM/DD)	Time	Notes
Emails, local and web-based.	Done	2025/12/11	7:00 PM (UTC +5:45)	<p>For this, I used "<b>Email Parser</b>" ingest module.</p> <p>Process: <b>Tools&gt;Run Ingest Module&gt;Email Parser</b></p>  <p>The selected module has no per-run settings.</p> <p>This module detects and parses mbox and pst/ost files an.</p> <p>Global Settings</p> <p>&lt; Back Next &gt; Finish Cancel Help</p> <p>Then, I basically went to keyword search and choose Email Addresses.</p> <p>Process: <b>Analysis Results&gt;Keyword Hits&gt;Email Addresses</b></p>

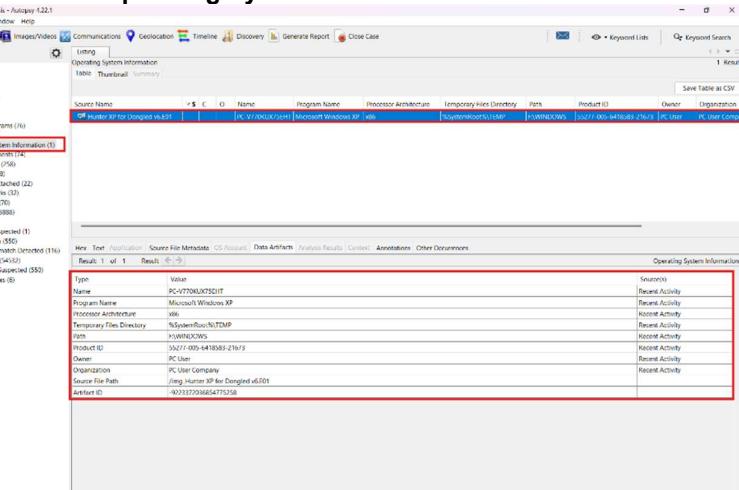
Action	Done?	Date (YY/MM/DD)	Time	Notes								
				<p>Hunter XP Case Analysis - Autopsy 4.2.1</p> <p>Case View Tools Window Help</p> <p>Directory Tree</p> <ul style="list-style-type: none"> <li>Data Sources</li> <li>File Views             <ul style="list-style-type: none"> <li>File Types                     <ul style="list-style-type: none"> <li>By Extension</li> <li>By MIME Type</li> </ul> </li> <li>Deleted Files</li> <li>MB File Size</li> </ul> </li> <li>Data Artifacts             <ul style="list-style-type: none"> <li>Installed Programs (76)</li> <li>Metadata (28)</li> <li>Operating System Information (1)</li> <li>Recent Documents (74)</li> <li>Run Programs (258)</li> <li>Shell Bags (188)</li> <li>USB Device Attached (22)</li> <li>Web Bookmarks (32)</li> <li>Web Cookies (70)</li> <li>Web History (888)</li> </ul> </li> <li>Analysis Results             <ul style="list-style-type: none"> <li>Encryption Suspected (1)</li> <li>EXIF Metadata (550)</li> <li>Extension Mismatch Detected (116)</li> <li>Keyword Hits (3161)                     <ul style="list-style-type: none"> <li>Single Literal Keyword Search (0)</li> <li>Single Regular Expression Search (0)</li> <li>Email Addresses (3161)</li> </ul> </li> <li>User Content Suspected (550)</li> <li>Web Categories (6)</li> </ul> </li> <li>OS Accounts</li> <li>Tags</li> <li>Score</li> <li>Reports</li> </ul> <p>Listing</p> <p>Keyword Hits</p> <table border="1"> <thead> <tr> <th>List Name</th> <th>Number of Children</th> </tr> </thead> <tbody> <tr> <td>Single Literal Keyword Search (0)</td> <td>0</td> </tr> <tr> <td>Single Regular Expression Search (0)</td> <td>0</td> </tr> <tr> <td>Email Addresses (3161)</td> <td>1</td> </tr> </tbody> </table> <p>Data Content</p> <p>Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences</p>	List Name	Number of Children	Single Literal Keyword Search (0)	0	Single Regular Expression Search (0)	0	Email Addresses (3161)	1
List Name	Number of Children											
Single Literal Keyword Search (0)	0											
Single Regular Expression Search (0)	0											
Email Addresses (3161)	1											

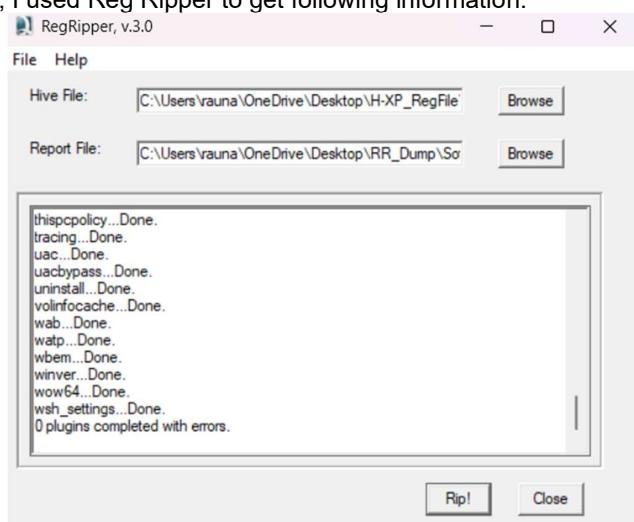




Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p>For specific mails we go to different locations. Here in this location</p> <p><b>vol.vol2&gt;Documents and Settings&gt;Bob Hunter&gt;Local Settings&gt;Temporary Internet Files&gt;Content.IE5&gt;8XGPQD6L&gt;getmsg[3]</b></p> <p>Here, we can see Billray sending mail to Chaser .</p>  <p>The screenshot shows the Autopsy 4.2.1 interface. The left pane displays a file system tree with several folders expanded, including 'Temporary Internet Files' and 'Content.IE5'. A red box highlights the 'Content.IE5' folder. The right pane shows a table of results for 'Using /tmp/jarvis/XP for Dumped v6.0/vol.vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/8XGPQD6L/getmsg[3]'. Below the table is a preview of an email message from 'billray1191@hotmail.com' to 'chaser1191@hotmail.com'. The message subject is 'Email address correction' and it contains a link to ShopMessage. A red box highlights the email preview.</p> <p>Likewise at the location</p> <p><b>vol.vol2&gt;Documents and Settings&gt;Bob Hunter&gt;Local Settings&gt;Temporary Internet Files&gt;Content.IE5&gt;8XGPQD6L</b></p> <p>Here,we can find other mails there from <b>getmsg[1]</b> and <b>getmsg[2]</b>.</p>

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

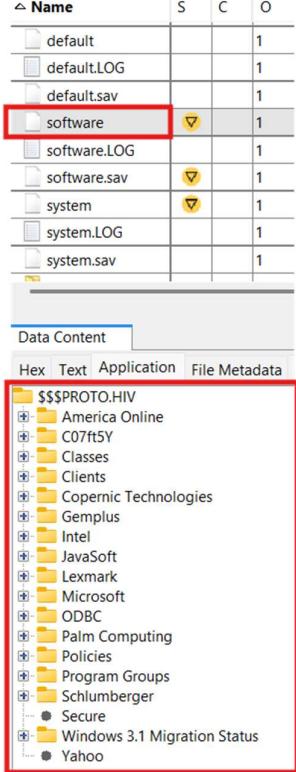
Action	Done?	Date (YY/MM/DD)	Time	Notes																								
				<p>Here are few notable email addresses:</p> <p><a href="mailto:billyray150@hotmail.com">billyray150@hotmail.com</a>  <a href="mailto:chaser1191@hotmail.com">chaser1191@hotmail.com</a>  <a href="mailto:billyray150b@netscape.net">billyray150b@netscape.net</a>  <a href="mailto:ted.dewercs@encase.com">ted.dewercs@encase.com</a>  <a href="mailto:john.detsiwt@encase.com">john.detsiwt@encase.com</a></p> <p>Others were also found asking for ransom and giving death threat.</p>																								
Retrieve operating system information, accounts information, software, time zone information etc.).	Done	2025/12/11	10:00 PM (UTC +5:45)	<p>For this we navigate to <b>Data Artifacts&gt;Operating System Information</b></p>  <table border="1"> <thead> <tr> <th>Source Name</th> <th>S</th> <th>C</th> <th>O</th> <th>Name</th> <th>Program Name</th> <th>Processor Architecture</th> <th>Temporary Files Directory</th> <th>Path</th> <th>Product ID</th> <th>Owner</th> <th>Organization</th> </tr> </thead> <tbody> <tr> <td>SPF Hunter XP for Dongle victim</td> <td></td> <td></td> <td></td> <td>PC-V770BLKNDTHT</td> <td>Microsoft Windows XP - Task</td> <td>x86</td> <td>%SystemRoot%\Temp</td> <td>\SystemRoot\Temp</td> <td>0277-000-04100027673</td> <td>PC User</td> <td>PC User Company</td> </tr> </tbody> </table>	Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID	Owner	Organization	SPF Hunter XP for Dongle victim				PC-V770BLKNDTHT	Microsoft Windows XP - Task	x86	%SystemRoot%\Temp	\SystemRoot\Temp	0277-000-04100027673	PC User	PC User Company
Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID	Owner	Organization																	
SPF Hunter XP for Dongle victim				PC-V770BLKNDTHT	Microsoft Windows XP - Task	x86	%SystemRoot%\Temp	\SystemRoot\Temp	0277-000-04100027673	PC User	PC User Company																	

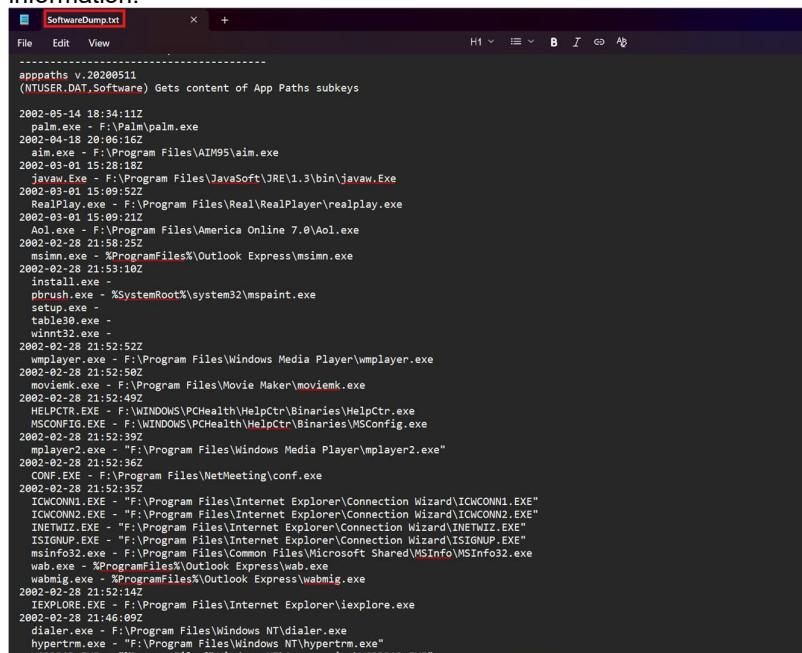
Action	Done?	Date (YY/MM/DD)	Time	Notes																							
				<table border="1"> <tr><td>Type</td><td>Value</td></tr> <tr><td>Name</td><td>PC-V770KUX75EHT</td></tr> <tr><td>Program Name</td><td>Microsoft Windows XP</td></tr> <tr><td>Processor Architecture</td><td>x86</td></tr> <tr><td>Temporary Files Directory</td><td>%SystemRoot%\TEMP</td></tr> <tr><td>Path</td><td>F:\WINDOWS</td></tr> <tr><td>Product ID</td><td>55277-005-6418583-21673</td></tr> <tr><td>Owner</td><td>PC User</td></tr> <tr><td>Organization</td><td>PC User Company</td></tr> <tr><td>Source File Path</td><td>/img_Hunter XP for Dongled v6.E01</td></tr> <tr><td>Artifact ID</td><td>-9223372036854775258</td></tr> </table> <p>Similarly, I used Reg Ripper to get following information:</p>  <p>The screenshot shows the RegRipper v.3.0 application window. It has two main input fields: 'Hive File' set to 'C:\Users\vauna\OneDrive\Desktop\H-XP_RegFile' and 'Report File' set to 'C:\Users\vauna\OneDrive\Desktop\RR_Dump\So'. Below these fields is a large text area containing a list of registry keys and their status: 'thispcpolicy...Done.', 'tracing...Done.', 'uac...Done.', 'uacbypass...Done.', 'uninstall...Done.', 'volinfoarchive...Done.', 'wab...Done.', 'watp...Done.', 'wbem...Done.', 'winver...Done.', 'wow64...Done.', 'wsh_settings...Done.', '0 plugins completed with errors.' At the bottom right of the window are 'Rip!' and 'Close' buttons.</p> <p>For OS, I checked SoftwareDump.txt:</p>	Type	Value	Name	PC-V770KUX75EHT	Program Name	Microsoft Windows XP	Processor Architecture	x86	Temporary Files Directory	%SystemRoot%\TEMP	Path	F:\WINDOWS	Product ID	55277-005-6418583-21673	Owner	PC User	Organization	PC User Company	Source File Path	/img_Hunter XP for Dongled v6.E01	Artifact ID	-9223372036854775258	
Type	Value																										
Name	PC-V770KUX75EHT																										
Program Name	Microsoft Windows XP																										
Processor Architecture	x86																										
Temporary Files Directory	%SystemRoot%\TEMP																										
Path	F:\WINDOWS																										
Product ID	55277-005-6418583-21673																										
Owner	PC User																										
Organization	PC User Company																										
Source File Path	/img_Hunter XP for Dongled v6.E01																										
Artifact ID	-9223372036854775258																										

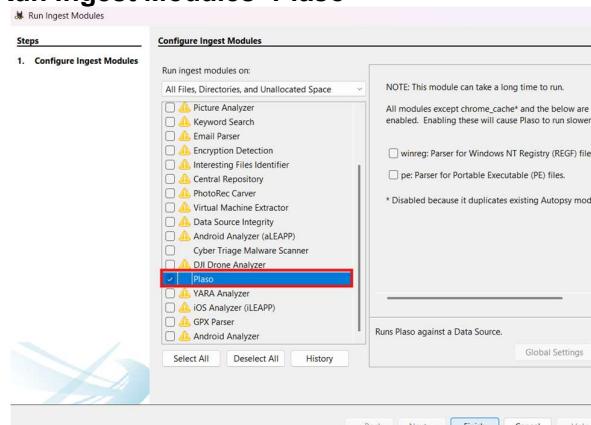
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<pre> winver v.20200525 (Software) Get Windows version &amp; build info  ProductName           Microsoft Windows XP BuildLab              2600.xpclnt_qfe.010827-1803 RegisteredOrganization PC User Company RegisteredOwner        PC User InstallDate         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

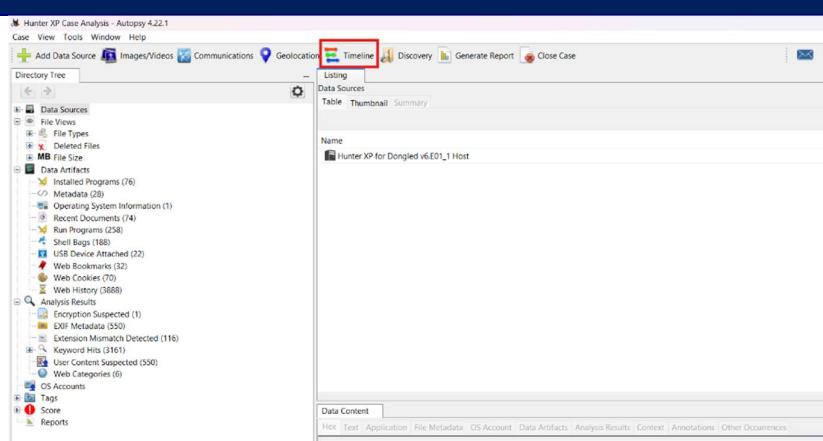
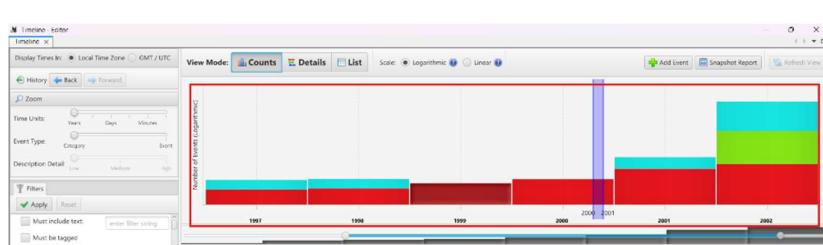
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<pre>User Information ----- Username      : Administrator [500] SID          : S-1-5-21-1229272821-1580818891-854245398-500 Full Name    : User Comment  : Built-in account for administering the computer/domain Account Type  : Default Admin User Account Created : Thu Feb 28 15:22:36 2002 Z Name         : Last Login Date : Never Pwd Reset Date : Never Pwd Fail Date  : Never Login Count    : 0 --&gt; Password does not expire --&gt; Normal user account  Username      : Guest [501] SID          : S-1-5-21-1229272821-1580818891-854245398-501 Full Name    : User Comment  : Built-in account for guest access to the computer/domain Account Type  : Default Guest Acct Account Created : Thu Feb 28 15:22:36 2002 Z Name         : Last Login Date : Mon Jun  3 16:49:37 2002 Z Pwd Reset Date : Never Pwd Fail Date  : Never Login Count    : 0 --&gt; Password does not expire --&gt; Password not required --&gt; Normal user account  Username      : HelpAssistant [1000] SID          : S-1-5-21-1229272821-1580818891-854245398-1000 Full Name    : Remote Desktop Help Assistant Account User Comment  : Account for Providing Remote Assistance Account Type  : Custom Limited Acct Account Created : Thu Feb 28 21:47:33 2002 Z Name         : Last Login Date : Never Pwd Reset Date : Thu Feb 28 21:47:33 2002 Z Pwd Fail Date  : Never Login Count    : 0 --&gt; Password does not expire --&gt; Normal user account</pre>

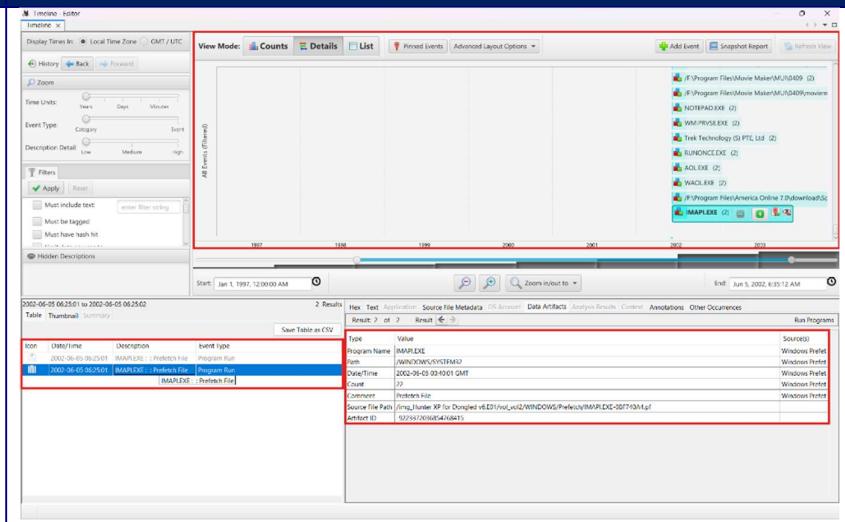
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<pre> Username      : SUPPORT_388945a0 [1002] SID          : S-1-5-21-1229272821-1580818891-854245398-1002 Full Name    : CN=Microsoft Corporation,L=Redmond,S=Washington,C=US User Comment  : This is a vendor's account for the Help and Support Service Account Type : Custom Limited Acct Account Created : Thu Feb 28 21:56:13 2002 Z Name         : Last Login Date : Never Pwd Reset Date : Thu Feb 28 21:56:13 2002 Z Pwd Fail Date : Never Login Count   : 0 --&gt; Password does not expire --&gt; Account Disabled --&gt; Normal user account  Username      : Bob Hunter [1004] SID          : S-1-5-21-1229272821-1580818891-854245398-1004 Full Name    : User Comment  : Account Type : Default Admin User Account Created : Thu Feb 28 22:22:17 2002 Z Name         : Last Login Date : Tue Jun  4 23:01:54 2002 Z Pwd Reset Date : Thu Feb 28 22:22:17 2002 Z Pwd Fail Date : Never Login Count   : 37 --&gt; Password does not expire --&gt; Password not required --&gt; Normal user account </pre> <p>For Software, Firstly I used Autopsy to directly get information about the software.</p> <p>Location:  <a href="#">Windows&gt;System32&gt;Config&gt;Software</a></p>

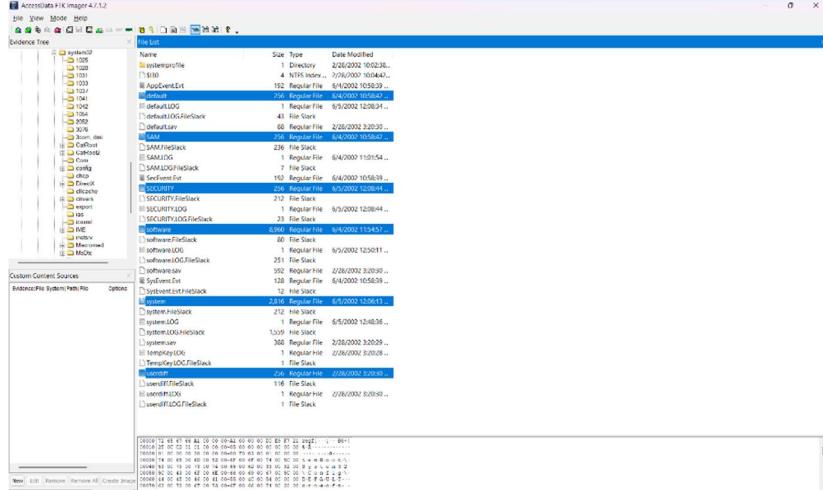
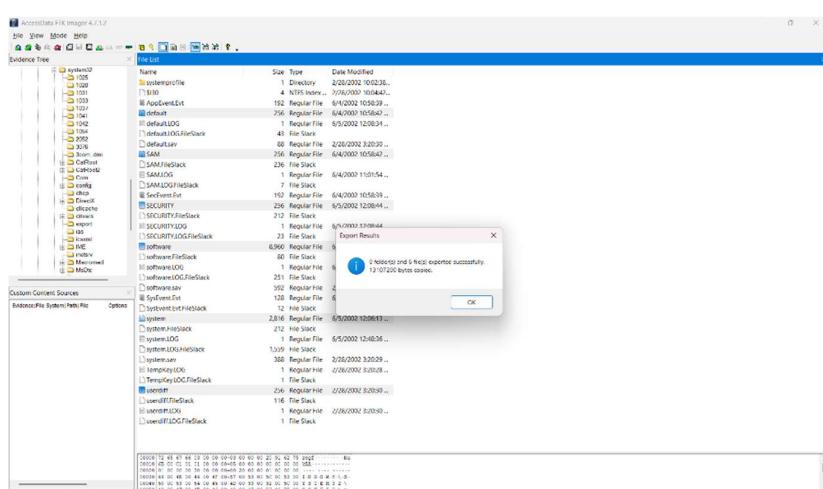
Action	Done?	Date (YY/MM/DD)	Time	Notes																																								
				 <p>The screenshot shows a file browser interface. At the top, there is a table with columns labeled 'Name', 'S', 'C', and 'O'. Below this table is a list of files and folders:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>S</th> <th>C</th> <th>O</th> </tr> </thead> <tbody> <tr> <td>default</td> <td></td> <td>1</td> <td></td> </tr> <tr> <td>default.LOG</td> <td></td> <td>1</td> <td></td> </tr> <tr> <td>default.sav</td> <td></td> <td>1</td> <td></td> </tr> <tr> <td><b>software</b></td> <td></td> <td>1</td> <td>▼</td> </tr> <tr> <td>software.LOG</td> <td></td> <td>1</td> <td></td> </tr> <tr> <td>software.sav</td> <td></td> <td>1</td> <td>▼</td> </tr> <tr> <td>system</td> <td></td> <td>1</td> <td>▼</td> </tr> <tr> <td>system.LOG</td> <td></td> <td>1</td> <td></td> </tr> <tr> <td>system.sav</td> <td></td> <td>1</td> <td></td> </tr> </tbody> </table> <p>Below the file list is a section titled "Data Content" with tabs for "Hex", "Text", "Application", and "File Metadata". The "Application" tab is selected, showing a tree view of application icons. A red box highlights the "Windows 3.1 Migration Status" icon, which is expanded to show its contents:</p> <ul style="list-style-type: none"> <li>\$\$\$PROTO.HIV       <ul style="list-style-type: none"> <li>America Online</li> <li>C07ft5Y</li> <li>Classes</li> <li>Clients</li> <li>Copernic Technologies</li> <li>Gemplus</li> <li>Intel</li> <li>JavaSoft</li> <li>Lexmark</li> <li>Microsoft</li> <li>ODBC</li> <li>Palm Computing</li> <li>Policies</li> <li>Program Groups</li> <li>Schlumberger</li> <li>Secure</li> <li>Windows 3.1 Migration Status</li> <li>Yahoo</li> </ul> </li> </ul>	Name	S	C	O	default		1		default.LOG		1		default.sav		1		<b>software</b>		1	▼	software.LOG		1		software.sav		1	▼	system		1	▼	system.LOG		1		system.sav		1	
Name	S	C	O																																									
default		1																																										
default.LOG		1																																										
default.sav		1																																										
<b>software</b>		1	▼																																									
software.LOG		1																																										
software.sav		1	▼																																									
system		1	▼																																									
system.LOG		1																																										
system.sav		1																																										

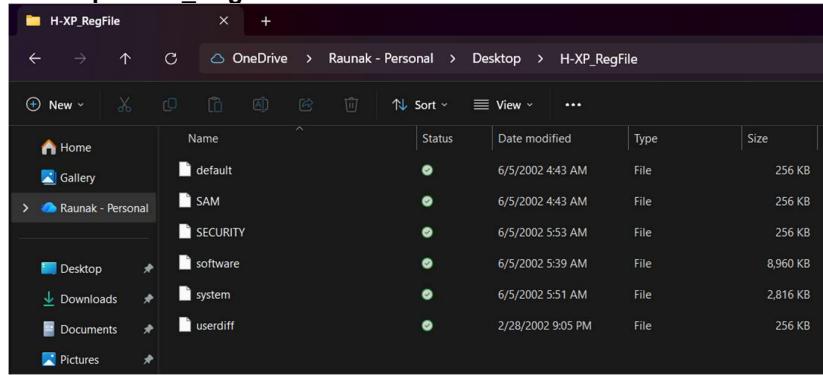
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p>Secondly, I checked SoftwareDump.txt to check about the software information.</p>  <pre> SoftwareDump.txt ----- apppaths v.20200511 (NTUSER.DAT.Software) Gets content of App Paths subkeys  2002-05-14 18:34:11Z palm.exe - F:\Palm\palm.exe 2002-04-18 20:06:16Z aim.exe - F:\Program Files\AIM95\aim.exe 2002-03-01 15:28:18Z javaw.exe - F:\Program Files\JavaSoft\JRE\1.3\bin\javaw.exe 2002-03-01 15:09:52Z RealPlay.exe - F:\Program Files\Real\RealPlayer\realplay.exe 2002-03-01 15:09:21Z Aol.exe - F:\Program Files\America Online 7.0\Aol.exe 2002-02-28 21:58:25Z msimn.exe - %ProgramFiles%\Outlook Express\msimn.exe 2002-02-28 21:53:10Z install.exe - pbrush.exe - %SystemRoot%\system32\mpaint.exe setup.exe - tabbed.exe - winmail.exe - 2002-02-28 21:52:52Z wmplayer.exe - F:\Program Files\Windows Media Player\wmplayer.exe 2002-02-28 21:52:50Z moviemk.exe - F:\Program Files\Movie Maker\moviemk.exe 2002-02-28 21:52:49Z HELPCTR.EXE - F:\WINDOWS\PCHealth\HelpCtr\Binaries\HelpCtr.exe MSCONFIG.EXE - F:\WINDOWS\VCHelp\HelpCtr\Binaries\MSConfig.exe 2002-02-28 21:52:39Z mplayer2.exe - "F:\Program Files\Windows Media Player\mplayer2.exe" 2002-02-28 21:52:36Z CONF.EXE - F:\Program Files\NetMeeting\conf.exe 2002-02-28 21:52:35Z ICWCONN1.EXE - "F:\Program File\Internet Explorer\Connection Wizard\ICWCONN1.EXE" ICWCONN2.EXE - "F:\Program File\Internet Explorer\Connection Wizard\ICWCONN2.EXE" INETWIZ.EXE - "F:\Program Files\Internet Explorer\Connection Wizard\INETWIZ.EXE" ISIGNUP.EXE - "F:\Program Files\Internet Explorer\Connection Wizard\ISIGNUP.EXE" MSINFO32.EXE - F:\Program Files\Common Files\Microsoft Shared\MSInfo\MSInfo32.exe wab.exe - %ProgramFiles%\Outlook Express\wab.exe wabnig.exe - %ProgramFiles%\Outlook Express\wabnig.exe 2002-02-28 21:52:14Z IEEXPLORE.EXE - F:\Program Files\Internet Explorer\iexplore.exe 2002-02-28 21:46:09Z dialer.exe - F:\Program Files\Windows NT\dialer.exe hyperterm.exe - "F:\Program Files\Windows NT\hyperterm.exe" WORDPAD.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE" </pre> <p>For Time Zone, I checked SystemDump.txt.</p>

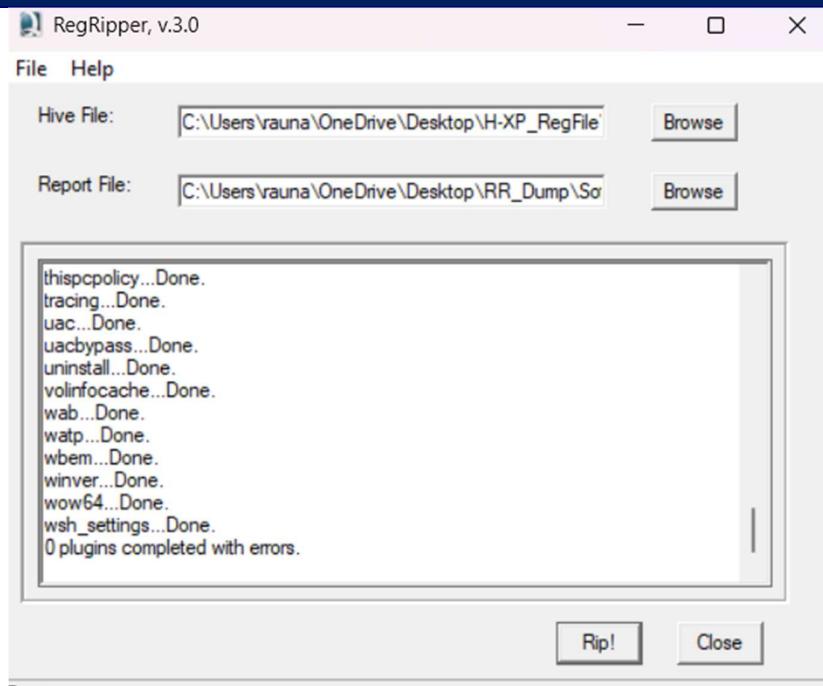
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<pre>----- timezone v.20200518 (System) Get TimeZoneInformation key contents  TimeZoneInformation key ControlSet001\Control\TimeZoneInformation LastWrite Time 2002-04-18 14:33:31Z DaylightName -&gt; Central Daylight Time StandardName -&gt; Central Standard Time Bias -&gt; 360 (6 hours) ActiveTimeBias -&gt; 300 (5 hours) -----</pre>
Timeline analysis- Note date of last activity on the computer. System profiling.	Done	2025/12/12	07:00 PM (UTC +5:45)	<p>For this we run <b>Tools&gt;Run Ingest Modules&gt;Plaso</b></p>  <p>With this we can access the timeline page at the top.</p>

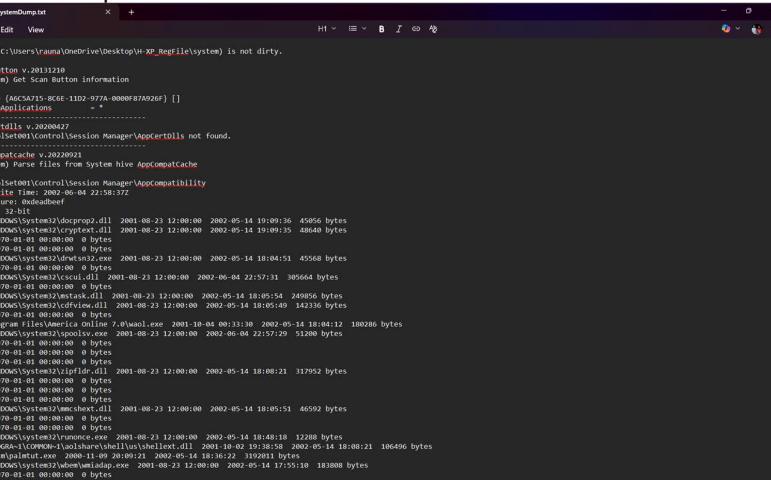
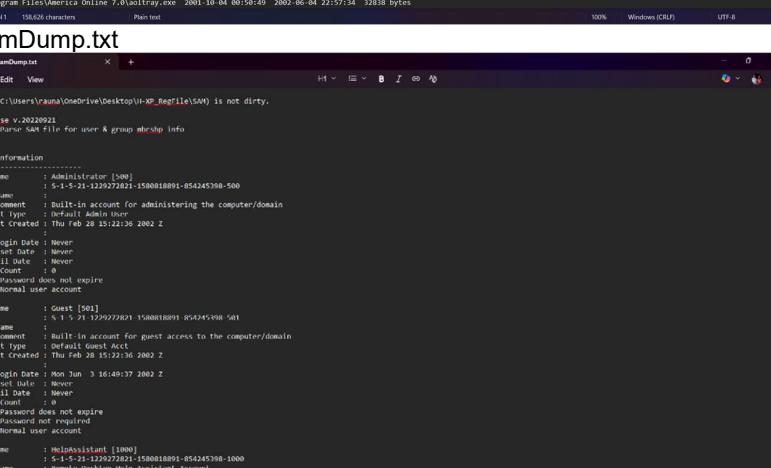
Action	Done?	Date (YY/MM/DD)	Time	Notes																						
				 <p>Here we can analyse, when different events happened. For the last activity we can select the bar graph to show the latest activities at the end of the computer.</p>  <table border="1"> <caption>Timeline Editor Data (Approximate)</caption> <thead> <tr> <th>Event Type</th> <th>Count</th> </tr> </thead> <tbody> <tr><td>File System</td><td>~1000</td></tr> <tr><td>Network</td><td>~500</td></tr> <tr><td>Process</td><td>~300</td></tr> <tr><td>User Activity</td><td>~200</td></tr> <tr><td>System Events</td><td>~100</td></tr> <tr><td>File Metadata</td><td>~50</td></tr> <tr><td>File Contents</td><td>~30</td></tr> <tr><td>File Hashes</td><td>~20</td></tr> <tr><td>File Names</td><td>~10</td></tr> <tr><td>File Types</td><td>~5</td></tr> </tbody> </table>	Event Type	Count	File System	~1000	Network	~500	Process	~300	User Activity	~200	System Events	~100	File Metadata	~50	File Contents	~30	File Hashes	~20	File Names	~10	File Types	~5
Event Type	Count																									
File System	~1000																									
Network	~500																									
Process	~300																									
User Activity	~200																									
System Events	~100																									
File Metadata	~50																									
File Contents	~30																									
File Hashes	~20																									
File Names	~10																									
File Types	~5																									

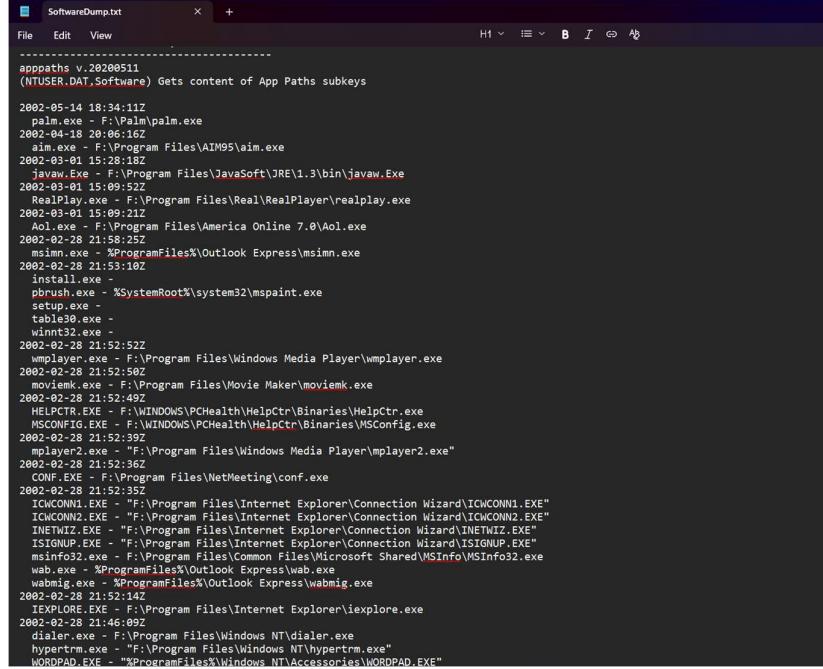
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Now we can see that at the end CD-burning tool IMAPI.exe was run.</p>
Registry analysis and Registry protected area	Done	2025/12/12	09:00 PM (UTC +5:45)	We used ftk to access the image file and go to this location <b>Windows&gt;System32&gt;Config</b>

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

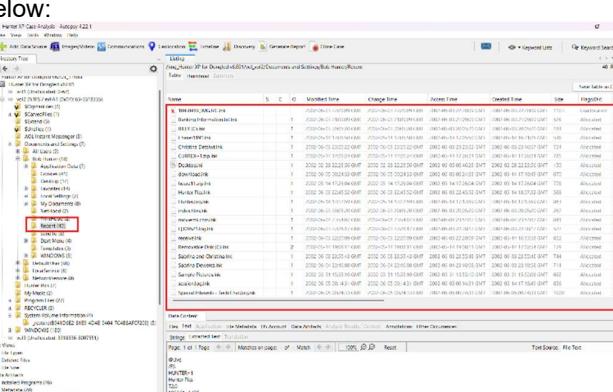
Action	Done?	Date (YY/MM/DD)	Time	Notes																																			
				<p>For this we extracted SAM, SECURITY, SYSTEM, SOFTWARE, and etc. Which is located at:</p> <p><b>Desktop&gt;H-XP_RegFile</b></p>  <table border="1"> <thead> <tr> <th>Name</th> <th>Status</th> <th>Date modified</th> <th>Type</th> <th>Size</th> </tr> </thead> <tbody> <tr> <td>default</td> <td>✓</td> <td>6/5/2002 4:43 AM</td> <td>File</td> <td>256 KB</td> </tr> <tr> <td>SAM</td> <td>✓</td> <td>6/5/2002 4:43 AM</td> <td>File</td> <td>256 KB</td> </tr> <tr> <td>SECURITY</td> <td>✓</td> <td>6/5/2002 5:53 AM</td> <td>File</td> <td>256 KB</td> </tr> <tr> <td>software</td> <td>✓</td> <td>6/5/2002 5:39 AM</td> <td>File</td> <td>8,960 KB</td> </tr> <tr> <td>system</td> <td>✓</td> <td>6/5/2002 5:51 AM</td> <td>File</td> <td>2,816 KB</td> </tr> <tr> <td>userdiff</td> <td>✓</td> <td>2/28/2002 9:05 PM</td> <td>File</td> <td>256 KB</td> </tr> </tbody> </table> <p>Now, I used Reg Ripper to RIP all the extracted registry files.</p>	Name	Status	Date modified	Type	Size	default	✓	6/5/2002 4:43 AM	File	256 KB	SAM	✓	6/5/2002 4:43 AM	File	256 KB	SECURITY	✓	6/5/2002 5:53 AM	File	256 KB	software	✓	6/5/2002 5:39 AM	File	8,960 KB	system	✓	6/5/2002 5:51 AM	File	2,816 KB	userdiff	✓	2/28/2002 9:05 PM	File	256 KB
Name	Status	Date modified	Type	Size																																			
default	✓	6/5/2002 4:43 AM	File	256 KB																																			
SAM	✓	6/5/2002 4:43 AM	File	256 KB																																			
SECURITY	✓	6/5/2002 5:53 AM	File	256 KB																																			
software	✓	6/5/2002 5:39 AM	File	8,960 KB																																			
system	✓	6/5/2002 5:51 AM	File	2,816 KB																																			
userdiff	✓	2/28/2002 9:05 PM	File	256 KB																																			

Action	Done?	Date (YY/MM/DD)	Time	Notes																																								
				 <p>RegRipper, v.3.0</p> <p>File Help</p> <p>Hive File: C:\Users\vauna\OneDrive\Desktop\H-XP_RegFile\ Report File: C:\Users\vauna\OneDrive\Desktop\RR_Dump\So</p> <pre>thispcpolicy...Done. tracing...Done. uac...Done. uacbypass...Done. uninstall...Done. volinfocache...Done. wab...Done. watp...Done. wbem...Done. winver...Done. wow64...Done. wsh_settings...Done. 0 plugins completed with errors.</pre> <p>Rip! Close</p> <p>Done.</p> <p>Dump of Ripped Files is at: <b>Desktop&gt;RR_Dump</b></p> <table border="1"> <tbody> <tr> <td>SamDump</td> <td>✓</td> <td>12/2/2025 11:03 PM</td> <td>Text Document</td> <td>1 KB</td> </tr> <tr> <td>SamDump</td> <td>✓</td> <td>12/2/2025 11:03 PM</td> <td>Text Document</td> <td>4 KB</td> </tr> <tr> <td>SecurityDump</td> <td>✓</td> <td>12/27/2025 6:32 PM</td> <td>Text Document</td> <td>1 KB</td> </tr> <tr> <td>SecurityDump</td> <td>✓</td> <td>12/27/2025 6:32 PM</td> <td>Text Document</td> <td>1 KB</td> </tr> <tr> <td>SoftwareDump</td> <td>✓</td> <td>12/27/2025 6:01 PM</td> <td>Text Document</td> <td>5 KB</td> </tr> <tr> <td>SoftwareDump</td> <td>✓</td> <td>12/27/2025 6:01 PM</td> <td>Text Document</td> <td>575 KB</td> </tr> <tr> <td>SystemDump</td> <td>✓</td> <td>12/2/2025 11:01 PM</td> <td>Text Document</td> <td>4 KB</td> </tr> <tr> <td>SystemDump</td> <td>✓</td> <td>12/2/2025 11:01 PM</td> <td>Text Document</td> <td>159 KB</td> </tr> </tbody> </table>	SamDump	✓	12/2/2025 11:03 PM	Text Document	1 KB	SamDump	✓	12/2/2025 11:03 PM	Text Document	4 KB	SecurityDump	✓	12/27/2025 6:32 PM	Text Document	1 KB	SecurityDump	✓	12/27/2025 6:32 PM	Text Document	1 KB	SoftwareDump	✓	12/27/2025 6:01 PM	Text Document	5 KB	SoftwareDump	✓	12/27/2025 6:01 PM	Text Document	575 KB	SystemDump	✓	12/2/2025 11:01 PM	Text Document	4 KB	SystemDump	✓	12/2/2025 11:01 PM	Text Document	159 KB
SamDump	✓	12/2/2025 11:03 PM	Text Document	1 KB																																								
SamDump	✓	12/2/2025 11:03 PM	Text Document	4 KB																																								
SecurityDump	✓	12/27/2025 6:32 PM	Text Document	1 KB																																								
SecurityDump	✓	12/27/2025 6:32 PM	Text Document	1 KB																																								
SoftwareDump	✓	12/27/2025 6:01 PM	Text Document	5 KB																																								
SoftwareDump	✓	12/27/2025 6:01 PM	Text Document	575 KB																																								
SystemDump	✓	12/2/2025 11:01 PM	Text Document	4 KB																																								
SystemDump	✓	12/2/2025 11:01 PM	Text Document	159 KB																																								

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

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <pre> SoftwareDump.txt File Edit View ----- apppaths v..20280511 (NTUSER.DAT.Software) Gets content of App Paths subkeys  2002-05-14 18:34:11Z palm.exe - F:\Palm\palm.exe 2002-04-18 20:06:16Z aim.exe - F:\Program Files\AIM95\aim.exe 2002-03-01 15:28:18Z javaw.exe - F:\Program Files\JavaSoft\JRE1.3\bin\javaw.exe 2002-03-01 15:29:09Z RealPlay.exe - F:\Program Files\Real\RealPlayer\realplay.exe 2002-03-01 15:09:21Z Aol.exe - F:\Program Files\America Online 7.0\Aol.exe 2002-02-28 21:58:25Z msimn.exe - %ProgramFiles%\Outlook Express\msimn.exe 2002-02-28 21:53:10Z install.exe - pbrush.exe - %SystemRoot%\system32\mspaint.exe setup.exe - table30.exe - winnn32.exe - 2002-02-28 21:52:52Z wmplayer.exe - F:\Program Files\Windows Media Player\wmplayer.exe 2002-02-28 21:52:50Z moviemk.exe - F:\Program Files\Movie Maker\moviemk.exe 2002-02-28 21:52:49Z HELPCTR.EXE - F:\WINDOWS\PCHHealth\HelpCtr\Binaries\HelpCtr.exe MSCONFIG.EXE - F:\WINDOWS\PCHealth\HelpCtr\Binaries\MSConfig.exe 2002-02-28 21:52:39Z mplayer2.exe - "F:\Program Files\Windows Media Player\mplayer2.exe" 2002-02-28 21:52:36Z CONF.EXE - F:\Program Files\NetMeeting\conf.exe 2002-02-28 21:52:35Z ICWCONN1.EXE - "F:\Program Files\Internet Explorer\Connection Wizard\ICWCONN1.EXE" ICWCONN2.EXE - "F:\Program Files\Internet Explorer\Connection Wizard\ICWCONN2.EXE" INETWIZ.EXE - "F:\Program Files\Internet Explorer\Connection Wizard\INETWIZ.EXE" ISIGNUP.EXE - "F:\Program Files\Internet Explorer\Connection Wizard\ISIGNUP.EXE" msinfo32.exe - F:\Program Files\Common Files\Microsoft Shared\MSInfo\MSInfo32.exe wab.exe - %ProgramFiles%\Outlook Express\wab.exe wabmg.exe - %ProgramFiles%\Outlook Express\wabmg.exe 2002-02-28 21:52:14Z IEEXPLORE.EXE - F:\Program Files\Internet Explorer\iexplore.exe 2002-02-28 21:46:09Z dialer.exe - F:\Program Files\Windows NT\dialer.exe hypertrm.exe - "F:\Program Files\Windows NT\hypertrm.exe" WORDPAD.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE" </pre> <p>SecurityDump.txt</p>

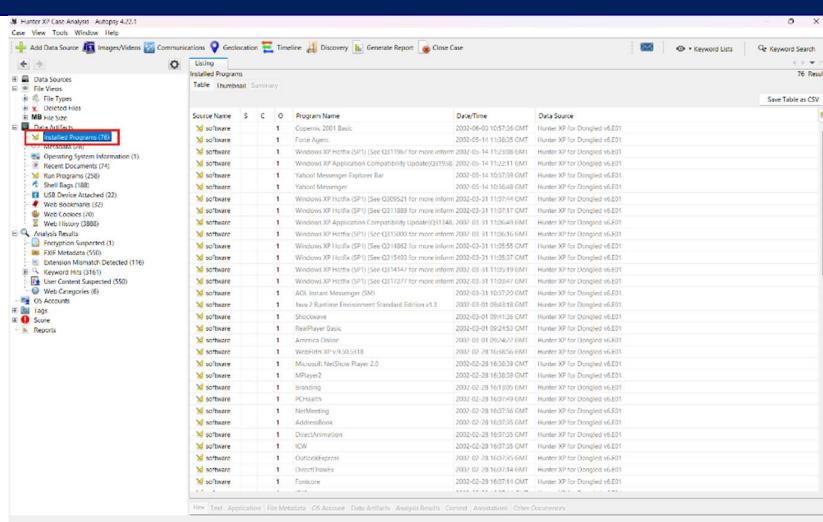
Action	Done?	Date (YY/MM/DD)	Time	Notes									
				<pre>SecurityDump.txt File Edit View Hive (C:\Users\rauna\OneDrive\Desktop\H-XP_RegFile\SECURITY) is not dirty.  auditpol v.20200515 (Security) Get audit policy from the Security hive file  auditpol Policy\PolAdtEv LastWrite Time 2002-02-28 15:25:30Z  Data Length: 0x2c 0x00000000: 01 00 07 00 03 00 00 00 03 00 00 00 00 00 00 00 ..... 0x00000010: 00 00 00 00 00 00 00 03 00 00 00 03 00 00 00 00 ..... 0x00000020: 00 00 00 03 00 00 00 09 00 00 00 00 00 00 00 00 ..... ----- secrets v.20200517 (Security) Get the last write time for the Policy\Secrets key  Policy\Secrets LastWrite Time 2002-03-31 14:27:32Z -----</pre> <p>We can also use Registry Viewer to see this information.  For E.g. SAM:  Location:  <b>SAM&gt;Domains&gt;Account&gt;Users&gt;Names</b></p>  <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>RF</td> <td>REG_BINARY</td> <td>02 00 01 00 00 00 00 20 E5 B8 D1 B0 ..</td> </tr> <tr> <td>RV</td> <td>REG_BINARY</td> <td>00 00 00 00 BC 00 00 02 00 01 00 BC ..</td> </tr> </tbody> </table> <p>Here, I viewed information about the users.</p>	Name	Type	Data	RF	REG_BINARY	02 00 01 00 00 00 00 20 E5 B8 D1 B0 ..	RV	REG_BINARY	00 00 00 00 BC 00 00 02 00 01 00 BC ..
Name	Type	Data											
RF	REG_BINARY	02 00 01 00 00 00 00 20 E5 B8 D1 B0 ..											
RV	REG_BINARY	00 00 00 00 BC 00 00 02 00 01 00 BC ..											

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

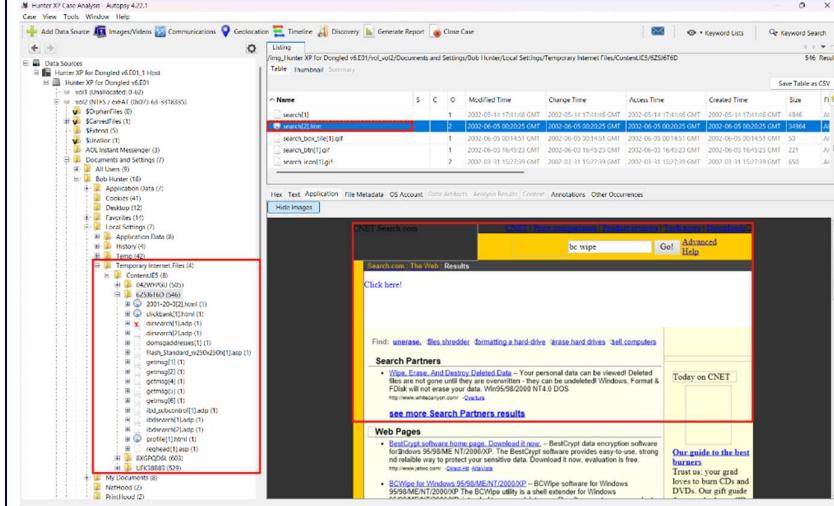
Action	Done?	Date (YY/MM/DD)	Time	Notes

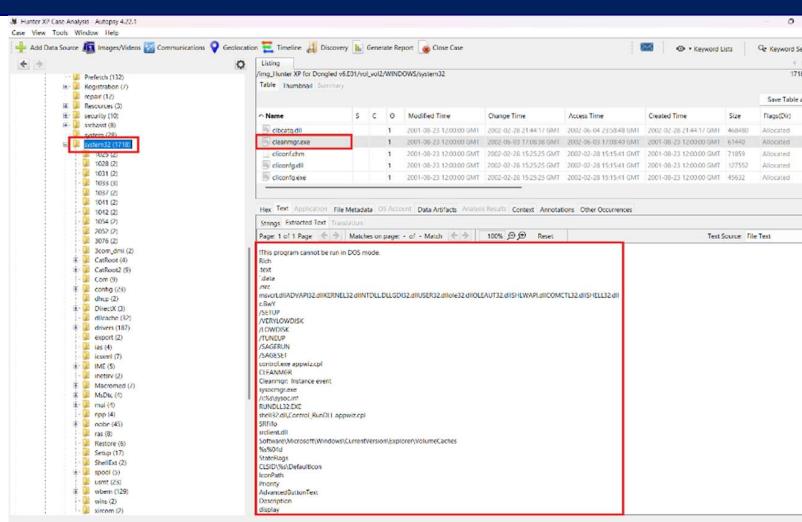
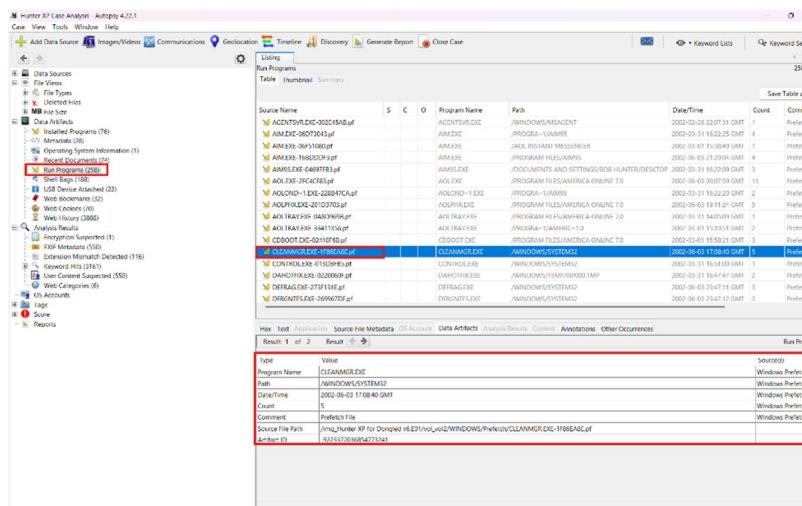
Action	Done?	Date (YY/MM/DD)	Time	Notes																					
				<p>Source   Type   Path</p> <table border="1"> <tr> <td>address.dat</td> <td>File</td> <td>/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/address/address.dat</td> </tr> <tr> <td>Saved_Preferences.PRC</td> <td>File</td> <td>/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/Backup/Saved_Preferences.PRC</td> </tr> <tr> <td>mempad.bak</td> <td>File</td> <td>/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/mempad/mempad.bak</td> </tr> <tr> <td>memopad.dat</td> <td>File</td> <td>/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/memopad/memopad.dat</td> </tr> <tr> <td>todo.bak</td> <td>File</td> <td>/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/todo/todo.bak</td> </tr> <tr> <td>D1035.JPG</td> <td>File</td> <td>/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11035.JPG</td> </tr> <tr> <td>D1034.JPG</td> <td>File</td> <td>/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11034.JPG</td> </tr> </table> <p>Data Content</p> <p>Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences</p> <p>Strings Extracted Text Translation</p> <p>Page: 1 of 1 Page <input type="button" value="Previous"/> <input type="button" value="Next"/> Matches on page: - of - Match <input type="button" value="Previous"/> <input type="button" value="Next"/> 100% <input type="button" value="Zoom In"/> <input type="button" value="Zoom Out"/> Reset Text Source: File Text</p> <p>B4E#0!Pam!HunterB\address\address.dat:Custom 1 Custom 2 Custom 3 Custom 4 01234 0000 Business Business Personal Personal QuickList QuickList Hammer Willy Ray Director - Sales Marine Services 626 555-1212 626 229-9199 billray150@hotmail.com 572 E. Green Street Pasadena Econfirm the work address and the friends name double check with Bill</p>	address.dat	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/address/address.dat	Saved_Preferences.PRC	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/Backup/Saved_Preferences.PRC	mempad.bak	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/mempad/mempad.bak	memopad.dat	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/memopad/memopad.dat	todo.bak	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/todo/todo.bak	D1035.JPG	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11035.JPG	D1034.JPG	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11034.JPG
address.dat	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/address/address.dat																							
Saved_Preferences.PRC	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/Backup/Saved_Preferences.PRC																							
mempad.bak	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/mempad/mempad.bak																							
memopad.dat	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/memopad/memopad.dat																							
todo.bak	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11040/HunterB/todo/todo.bak																							
D1035.JPG	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11035.JPG																							
D1034.JPG	File	/Img_Hunter_XP_for_Dongled_v6.01/vol_vo12/RECYCLER/5-1-5-1-122972821-150808891-854245398-1004/D11034.JPG																							

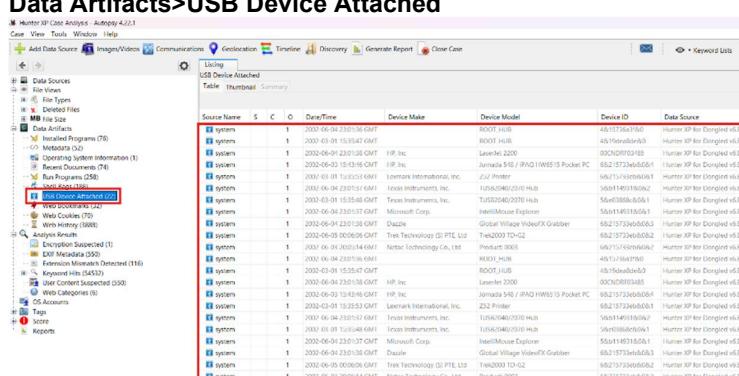
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p>Source Type Path</p> <ul style="list-style-type: none"> <li>address.dat File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/address/address.dat</li> <li>Saved_Preferences.PRC File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/Backup/Saved_Preferences.PRC</li> <li>memopad.bak File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/memopad/memopad.bak</li> <li>memopad.dat File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/memopad.dat</li> <li>todo.bak File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/todo.todo.bak</li> <li>DH105.JPG File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1035.JPG</li> <li>DH104.JPG File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1034.JPG</li> </ul> <p>Data Content</p> <p>Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences</p> <p>Page: 1 of 1 Page &lt; &gt; Matches on page: - of - Match &lt; &gt; 75% ⌂ ⌃ ⌄ ⌅ Reset Text Source: File Text</p> <pre>PMF(PalmHunter)@all 0x0 0 0 00000X Business Business Personal Personal@  chaser1991@all 0x0 0 0 00000X Business Business Personal Personal@  chaser1991@hotmail.com 0x0 0 0 00000X Business Business Personal Personal@  chaser1991@hotmail.com 0x0 0 0 00000X Business Business Personal Personal@  chaser1991@hotmail.com 1191 http://plus.advice.com/XDRRequestDispatcher?action=OpenLogin http://plus.advice.com/XDRRequestDispatcher?action=OpenLogin  I am leaving soon so I thought I would jot this note down to send later. I will be flying to LA to confirm the work address and find and confirm the friends name. I want to be able to send the information to the family soon. I agree that \$50,000 is a good amount to st I think the daughters safety is worth that don't you? I can't believe that they did not even know that it was us taking the photos. She even talked to me once. I will let you know as soon as I learn anything.</pre> <p>Source Type Path</p> <ul style="list-style-type: none"> <li>address.dat File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/address/address.dat</li> <li>Saved_Preferences.PRC File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/Backup/Saved_Preferences.PRC</li> <li>memopad.bak File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/memopad/memopad.bak</li> <li>memopad.dat File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/memopad.dat</li> <li>todo.bak File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/todo.todo.bak</li> <li>DH105.JPG File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1035.JPG</li> <li>DH104.JPG File /Img_Hunter XP for Dongled v6.E01/vol_vo2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1034.JPG</li> </ul> <p>Data Content</p> <p>Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences</p> <p>Page: 1 of 1 Page &lt; &gt; Matches on page: - of - Match &lt; &gt; 75% ⌂ ⌃ ⌄ ⌅ Reset Text Source: File Text</p> <pre>F:\PalmHunter\Todo\todo.todo.dat 10 0 5 1 1 0 0 0 0 0 0 ICO Business Business Personal Personal Personal  Send Kim's information to Billy/Billy Send Kim's information to Billy/Billy Check the green street address billy</pre>
Instant Messaging clients	Done	2025/12/13	10:00 PM (UTC +5:45)	For this we navigate to <b>Data Artifacts&gt;Installed Programs</b>

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

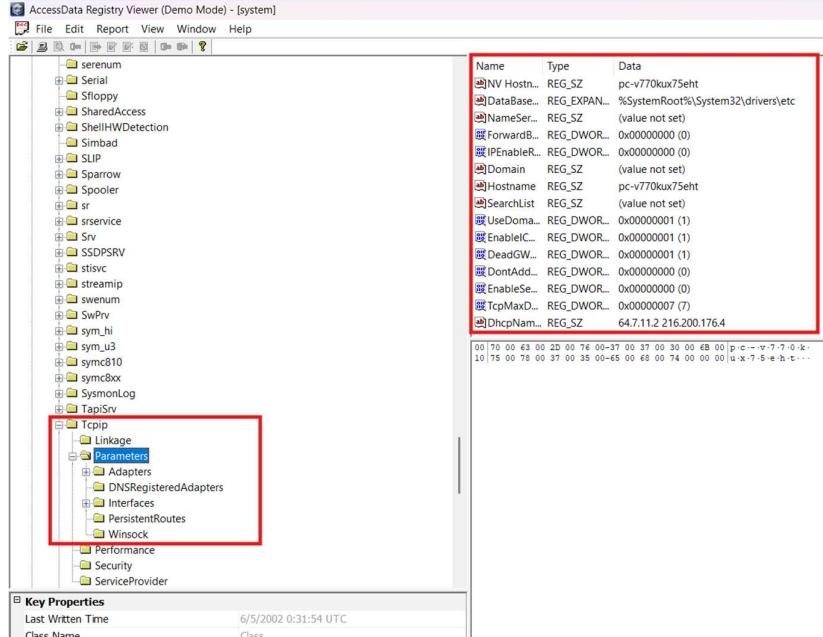
Action	Done?	Date (YY/MM/DD)	Time	Notes																																																																																																																																																																																																																														
				<p>Installed Programs</p> <p>Table Thumbnail Summary</p> <table border="1"> <thead> <tr> <th>Source Name</th> <th>S</th> <th>C</th> <th>O</th> <th>Program Name</th> <th>Date/Time</th> <th>Data Source</th> </tr> </thead> <tbody> <tr><td>software</td><td>1</td><td></td><td></td><td>Copernic 2001 Basic</td><td>2002-06-03 10:57:36 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Forté Agent</td><td>2002-05-14 11:38:35 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Windows XP Hotfix (SP1) [See Q311967 for more information]</td><td>2002-05-14 11:23:08 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Windows XP Application Compatibility Update[Q319580]</td><td>2002-05-14 11:22:11 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Yahoo! Messenger Explorer Bar</td><td>2002-05-14 10:37:39 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Yahoo! Messenger</td><td>2002-05-14 10:36:48 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Windows XP Hotfix (SP1) [See Q309521 for more information]</td><td>2002-03-31 11:07:44 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Windows XP Hotfix (SP1) [See Q311889 for more information]</td><td>2002-03-31 11:07:17 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Windows XP Application Compatibility Update[Q313484]</td><td>2002-03-31 11:06:49 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Windows XP Hotfix (SP1) [See Q315000 for more information]</td><td>2002-03-31 11:06:16 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Windows XP Hotfix (SP1) [See Q314662 for more information]</td><td>2002-03-31 11:05:55 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Windows XP Hotfix (SP1) [See Q315403 for more information]</td><td>2002-03-31 11:05:37 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Windows XP Hotfix (SP1) [See Q314147 for more information]</td><td>2002-03-31 11:05:19 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Windows XP Hotfix (SP1) [See Q317277 for more information]</td><td>2002-03-31 11:03:47 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>AOL Instant Messenger (SM)</td><td>2002-03-31 10:37:20 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Java 2 Runtime Environment Standard Edition v1.3</td><td>2002-03-01 09:43:18 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Shockwave</td><td>2002-03-01 09:41:36 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>RealPlayer Basic</td><td>2002-03-01 09:24:53 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>America Online</td><td>2002-03-01 09:24:22 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>WebFids XP v.9.50.5318</td><td>2002-02-28 16:38:56 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Microsoft NetShow Player 2.0</td><td>2002-02-28 16:38:39 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>MPlayer2</td><td>2002-02-28 16:38:39 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>Branding</td><td>2002-02-28 16:13:05 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>PCHealth</td><td>2002-02-28 16:07:49 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>NetMeeting</td><td>2002-02-28 16:07:36 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>AddressBook</td><td>2002-02-28 16:07:35 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>DirectAnimation</td><td>2002-02-28 16:07:35 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>ICW</td><td>2002-02-28 16:07:35 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>OutlookExpress</td><td>2002-02-28 16:07:35 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td>software</td><td>1</td><td></td><td></td><td>DirectDrawEx</td><td>2002-02-28 16:07:14 GMT</td><td>Hunter XP for Dongled v6.E01</td></tr> <tr><td></td><td></td><td></td><td></td><td>Entire row highlighted in grey.</td></tr> </tbody> </table>	Source Name	S	C	O	Program Name	Date/Time	Data Source	software	1			Copernic 2001 Basic	2002-06-03 10:57:36 GMT	Hunter XP for Dongled v6.E01	software	1			Forté Agent	2002-05-14 11:38:35 GMT	Hunter XP for Dongled v6.E01	software	1			Windows XP Hotfix (SP1) [See Q311967 for more information]	2002-05-14 11:23:08 GMT	Hunter XP for Dongled v6.E01	software	1			Windows XP Application Compatibility Update[Q319580]	2002-05-14 11:22:11 GMT	Hunter XP for Dongled v6.E01	software	1			Yahoo! Messenger Explorer Bar	2002-05-14 10:37:39 GMT	Hunter XP for Dongled v6.E01	software	1			Yahoo! Messenger	2002-05-14 10:36:48 GMT	Hunter XP for Dongled v6.E01	software	1			Windows XP Hotfix (SP1) [See Q309521 for more information]	2002-03-31 11:07:44 GMT	Hunter XP for Dongled v6.E01	software	1			Windows XP Hotfix (SP1) [See Q311889 for more information]	2002-03-31 11:07:17 GMT	Hunter XP for Dongled v6.E01	software	1			Windows XP Application Compatibility Update[Q313484]	2002-03-31 11:06:49 GMT	Hunter XP for Dongled v6.E01	software	1			Windows XP Hotfix (SP1) [See Q315000 for more information]	2002-03-31 11:06:16 GMT	Hunter XP for Dongled v6.E01	software	1			Windows XP Hotfix (SP1) [See Q314662 for more information]	2002-03-31 11:05:55 GMT	Hunter XP for Dongled v6.E01	software	1			Windows XP Hotfix (SP1) [See Q315403 for more information]	2002-03-31 11:05:37 GMT	Hunter XP for Dongled v6.E01	software	1			Windows XP Hotfix (SP1) [See Q314147 for more information]	2002-03-31 11:05:19 GMT	Hunter XP for Dongled v6.E01	software	1			Windows XP Hotfix (SP1) [See Q317277 for more information]	2002-03-31 11:03:47 GMT	Hunter XP for Dongled v6.E01	software	1			AOL Instant Messenger (SM)	2002-03-31 10:37:20 GMT	Hunter XP for Dongled v6.E01	software	1			Java 2 Runtime Environment Standard Edition v1.3	2002-03-01 09:43:18 GMT	Hunter XP for Dongled v6.E01	software	1			Shockwave	2002-03-01 09:41:36 GMT	Hunter XP for Dongled v6.E01	software	1			RealPlayer Basic	2002-03-01 09:24:53 GMT	Hunter XP for Dongled v6.E01	software	1			America Online	2002-03-01 09:24:22 GMT	Hunter XP for Dongled v6.E01	software	1			WebFids XP v.9.50.5318	2002-02-28 16:38:56 GMT	Hunter XP for Dongled v6.E01	software	1			Microsoft NetShow Player 2.0	2002-02-28 16:38:39 GMT	Hunter XP for Dongled v6.E01	software	1			MPlayer2	2002-02-28 16:38:39 GMT	Hunter XP for Dongled v6.E01	software	1			Branding	2002-02-28 16:13:05 GMT	Hunter XP for Dongled v6.E01	software	1			PCHealth	2002-02-28 16:07:49 GMT	Hunter XP for Dongled v6.E01	software	1			NetMeeting	2002-02-28 16:07:36 GMT	Hunter XP for Dongled v6.E01	software	1			AddressBook	2002-02-28 16:07:35 GMT	Hunter XP for Dongled v6.E01	software	1			DirectAnimation	2002-02-28 16:07:35 GMT	Hunter XP for Dongled v6.E01	software	1			ICW	2002-02-28 16:07:35 GMT	Hunter XP for Dongled v6.E01	software	1			OutlookExpress	2002-02-28 16:07:35 GMT	Hunter XP for Dongled v6.E01	software	1			DirectDrawEx	2002-02-28 16:07:14 GMT	Hunter XP for Dongled v6.E01					Entire row highlighted in grey.
Source Name	S	C	O	Program Name	Date/Time	Data Source																																																																																																																																																																																																																												
software	1			Copernic 2001 Basic	2002-06-03 10:57:36 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Forté Agent	2002-05-14 11:38:35 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Windows XP Hotfix (SP1) [See Q311967 for more information]	2002-05-14 11:23:08 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Windows XP Application Compatibility Update[Q319580]	2002-05-14 11:22:11 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Yahoo! Messenger Explorer Bar	2002-05-14 10:37:39 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Yahoo! Messenger	2002-05-14 10:36:48 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Windows XP Hotfix (SP1) [See Q309521 for more information]	2002-03-31 11:07:44 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Windows XP Hotfix (SP1) [See Q311889 for more information]	2002-03-31 11:07:17 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Windows XP Application Compatibility Update[Q313484]	2002-03-31 11:06:49 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Windows XP Hotfix (SP1) [See Q315000 for more information]	2002-03-31 11:06:16 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Windows XP Hotfix (SP1) [See Q314662 for more information]	2002-03-31 11:05:55 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Windows XP Hotfix (SP1) [See Q315403 for more information]	2002-03-31 11:05:37 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Windows XP Hotfix (SP1) [See Q314147 for more information]	2002-03-31 11:05:19 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Windows XP Hotfix (SP1) [See Q317277 for more information]	2002-03-31 11:03:47 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			AOL Instant Messenger (SM)	2002-03-31 10:37:20 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Java 2 Runtime Environment Standard Edition v1.3	2002-03-01 09:43:18 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Shockwave	2002-03-01 09:41:36 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			RealPlayer Basic	2002-03-01 09:24:53 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			America Online	2002-03-01 09:24:22 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			WebFids XP v.9.50.5318	2002-02-28 16:38:56 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Microsoft NetShow Player 2.0	2002-02-28 16:38:39 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			MPlayer2	2002-02-28 16:38:39 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			Branding	2002-02-28 16:13:05 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			PCHealth	2002-02-28 16:07:49 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			NetMeeting	2002-02-28 16:07:36 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			AddressBook	2002-02-28 16:07:35 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			DirectAnimation	2002-02-28 16:07:35 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			ICW	2002-02-28 16:07:35 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			OutlookExpress	2002-02-28 16:07:35 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
software	1			DirectDrawEx	2002-02-28 16:07:14 GMT	Hunter XP for Dongled v6.E01																																																																																																																																																																																																																												
				Entire row highlighted in grey.																																																																																																																																																																																																																														
Clean-up/Wiping utilities. Check log files. Anything used?	Done	2025/12/13	10:45 PM (UTC +5:45)	<p>Info related to disk wiping was found in this location:</p> <p><b>vol_vol2&gt;Documents and Settings&gt;Bob Hunter&gt;Local Settings&gt;Temporary Internet Files&gt;Content.IE5&gt;6ZSJ6T6D&gt;Search [2].htm.</b></p>																																																																																																																																																																																																																														

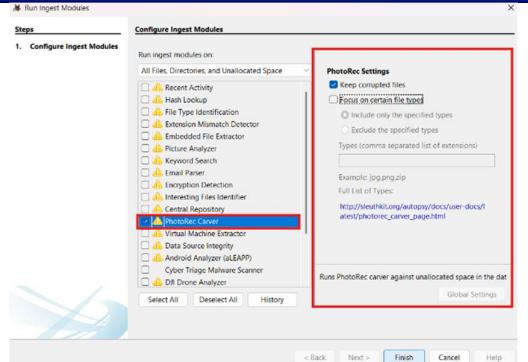
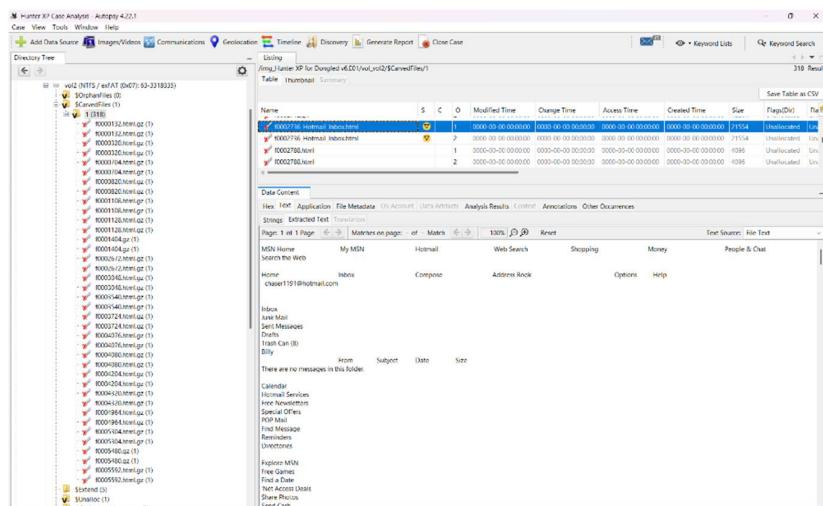
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>BC Wipe is a secure file deletion tool used to remove data beyond recovery.</p> <p>In system32 folder we can see that cleanmgr.exe was found.</p>

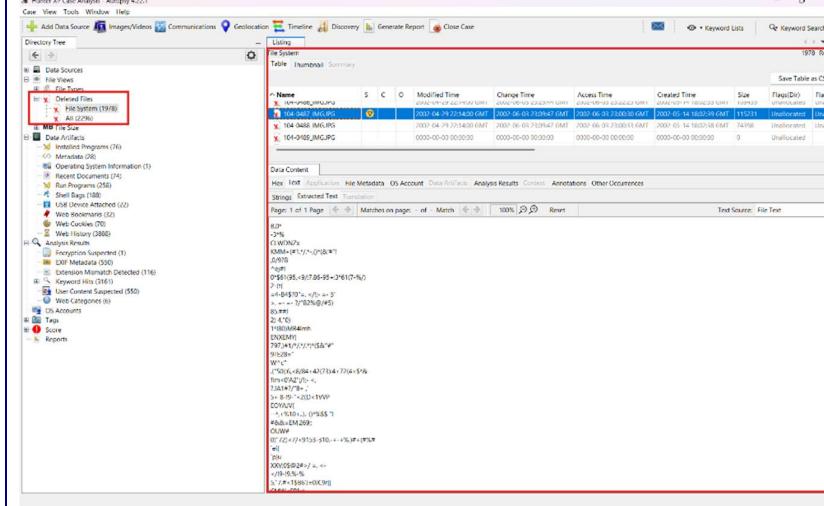
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p><b>Cleanmgr.exe is the Windows Disk Cleanup utility.</b></p>  <p>The screenshot shows the Autopsy 4.2.1 interface with the Timeline tab selected. A red box highlights the entry for 'cleanmgr.exe' in the list of running processes. The timeline table includes columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags/DUO, and File. The 'cleanmgr.exe' entry has a modified time of 2001-09-21 12:00:00 GMT and a change time of 2001-09-21 21:44:17 GMT.</p> <p><b>Cleanmgr.exe is the Windows Disk Cleanup utility.</b></p>  <p>The screenshot shows the Autopsy 4.2.1 interface with the Run Programs tab selected. A red box highlights the entry for 'cleanmgr.exe' in the list of run programs. The run programs table includes columns for Source Name, S, C, O, Program Name, Path, Date/Time, Count, and Comment. The 'cleanmgr.exe' entry has a date/time of 2002-09-28 22:07:31 GMT and a count of 1.</p>

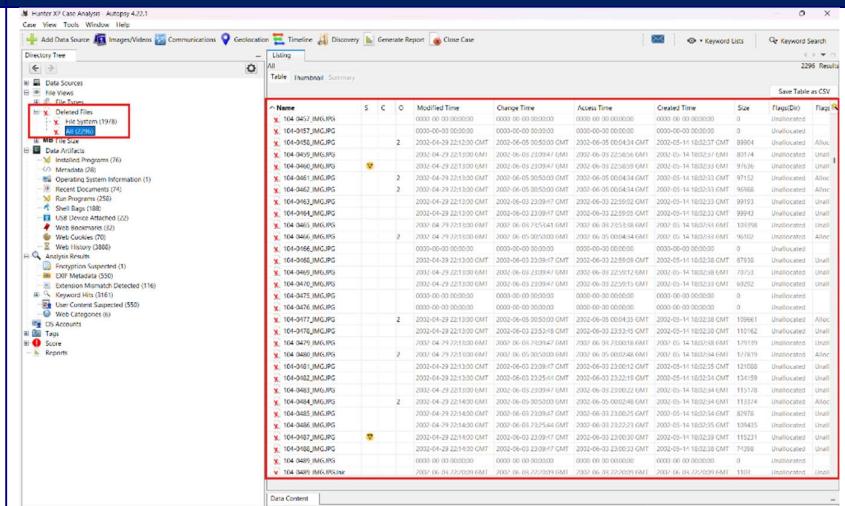
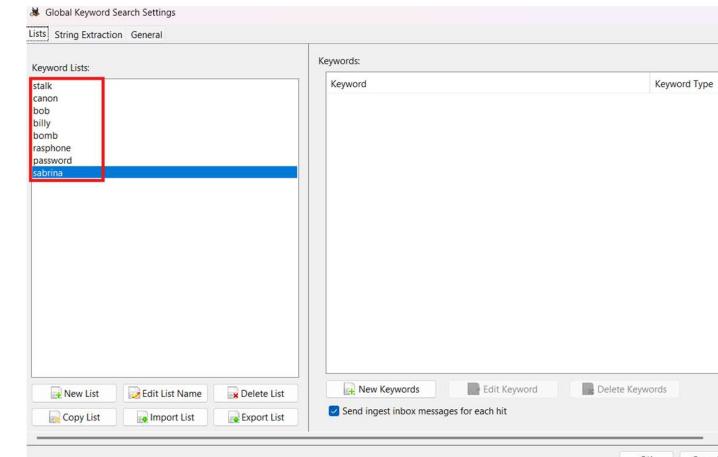
Action	Done?	Date (YY/MM/DD)	Time	Notes
External drives; Network connections	Done	2025/12/14	6:00 PM (UTC +5:45)	<p>We can get the attached USB devices by navigating to Process:  <b>Data Artifacts&gt;USB Device Attached</b></p>  <p>We can also get info by extracting and going to this location using "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

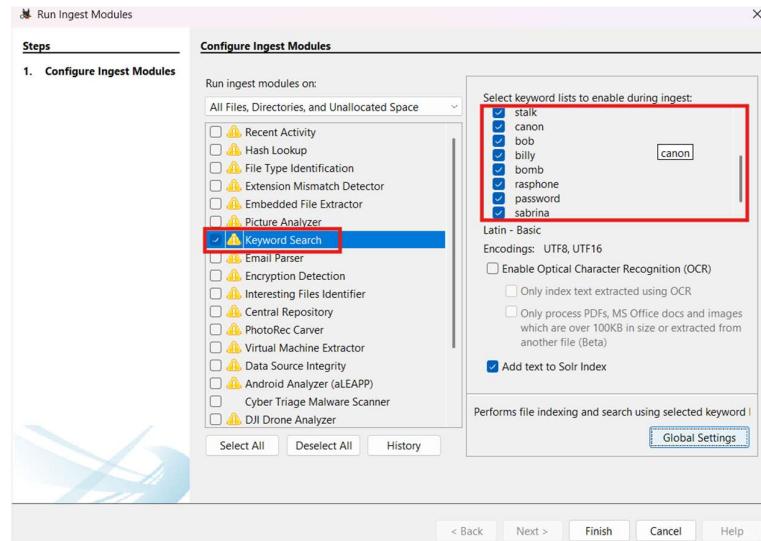
Action	Done?	Date (YY/MM/DD)	Time	Notes																																							
				<p>AccessData Registry Viewer (Demo Mode) - [system]</p> <p>File Edit Report View Window Help</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>DeviceDevs</td> <td>REG_SZ</td> <td>Disk drive</td> </tr> <tr> <td>Capabilities</td> <td>REG_DWORD</td> <td>0x00000000 (0)</td> </tr> <tr> <td>Hardware</td> <td>REG_MULTI_SZ</td> <td>USBSTOR\DiskNetac__OnlyDisk_20...</td> </tr> <tr> <td>Compatibility</td> <td>REG_MULTI_SZ</td> <td>USBSTOR\Disk USBSTOR\RAW</td> </tr> <tr> <td>ClassGUID</td> <td>REG_SZ</td> <td>{4D36E967-E325-11CE-BFC1-08002BE103...}</td> </tr> <tr> <td>Service</td> <td>REG_SZ</td> <td>disk</td> </tr> <tr> <td>ConfigFlags</td> <td>REG_DWORD</td> <td>0x00000000 (0)</td> </tr> <tr> <td>ParentalControl</td> <td>REG_SZ</td> <td>8&amp;1076ba5&amp;0</td> </tr> <tr> <td>Driver</td> <td>REG_SZ</td> <td>{4D36E967-E325-11CE-BFC1-08002BE103...}</td> </tr> <tr> <td>Class</td> <td>REG_SZ</td> <td>DiskDrive</td> </tr> <tr> <td>Mfg</td> <td>REG_SZ</td> <td>(Standard disk drives)</td> </tr> <tr> <td>FriendlyName</td> <td>REG_SZ</td> <td>Netac OnlyDisk USB Device</td> </tr> </tbody> </table> <p>00 44 00 69 00 73 00 6B 00-20 00 64 00 72 00 69 00 01-a-k- d-e... 10 76 00 65 00 00 00 00  v-e...</p> <p>Likewise for network connections we go to Process: <b>SYSTEM&gt;CurrentControlSet&gt;Services&gt;Tcpip&gt;Parameters</b></p>	Name	Type	Data	DeviceDevs	REG_SZ	Disk drive	Capabilities	REG_DWORD	0x00000000 (0)	Hardware	REG_MULTI_SZ	USBSTOR\DiskNetac__OnlyDisk_20...	Compatibility	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW	ClassGUID	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE103...}	Service	REG_SZ	disk	ConfigFlags	REG_DWORD	0x00000000 (0)	ParentalControl	REG_SZ	8&1076ba5&0	Driver	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE103...}	Class	REG_SZ	DiskDrive	Mfg	REG_SZ	(Standard disk drives)	FriendlyName	REG_SZ	Netac OnlyDisk USB Device
Name	Type	Data																																									
DeviceDevs	REG_SZ	Disk drive																																									
Capabilities	REG_DWORD	0x00000000 (0)																																									
Hardware	REG_MULTI_SZ	USBSTOR\DiskNetac__OnlyDisk_20...																																									
Compatibility	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW																																									
ClassGUID	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE103...}																																									
Service	REG_SZ	disk																																									
ConfigFlags	REG_DWORD	0x00000000 (0)																																									
ParentalControl	REG_SZ	8&1076ba5&0																																									
Driver	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE103...}																																									
Class	REG_SZ	DiskDrive																																									
Mfg	REG_SZ	(Standard disk drives)																																									
FriendlyName	REG_SZ	Netac OnlyDisk USB Device																																									

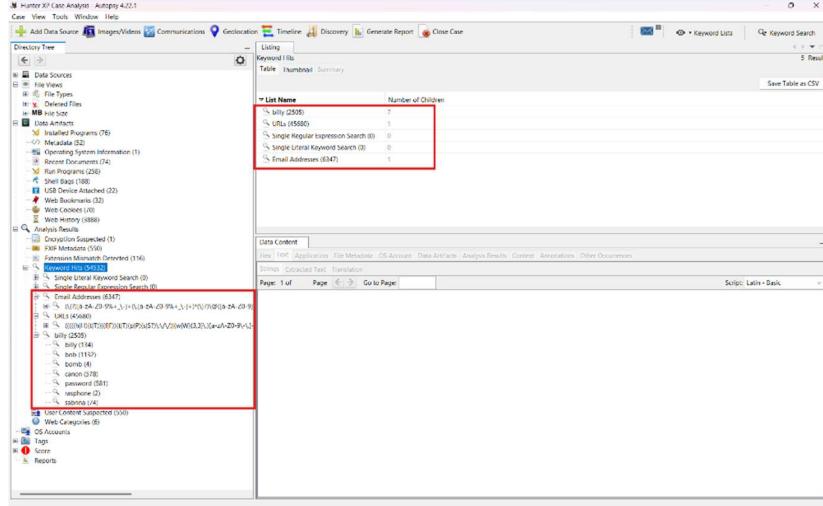
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>From this location we can get network connections.</p>
Perform data carving	Done	2025/12/14	8:00 PM (UTC +5:45)	<p>For this we run a ingest module called "<b>PhotoRec Caver</b>".</p> <p>Process: <b>Tools&gt;Run Ingest Modules&gt;PhotoRec Caver</b></p>

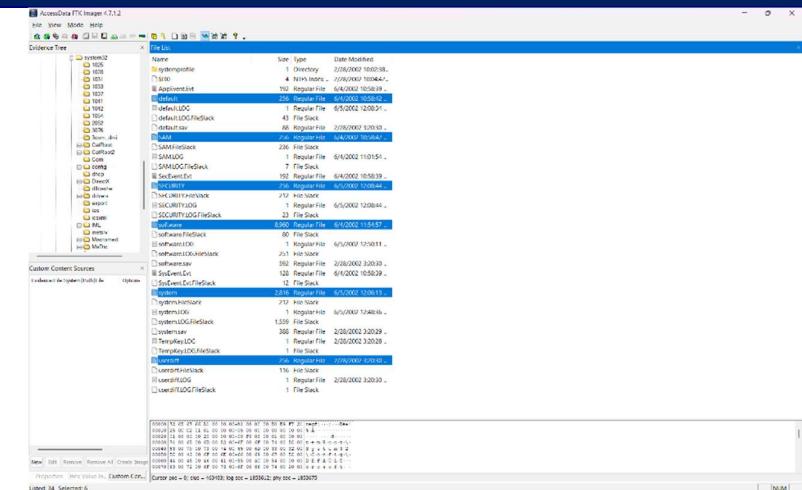
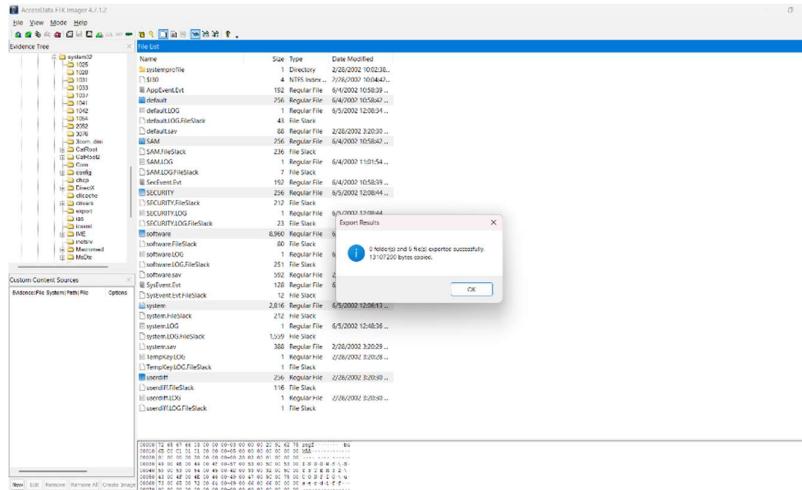
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>After selecting "<b>PhotoRec Caver Module</b>" we click finish and proceed. By selecting PhotoRec Caver we get access to these:</p> <p><b>Process:</b>  <b>Data Source &gt; Hunter XP Dongled &gt; VOL2 &gt; CarvedFiles &gt; 1</b></p> 

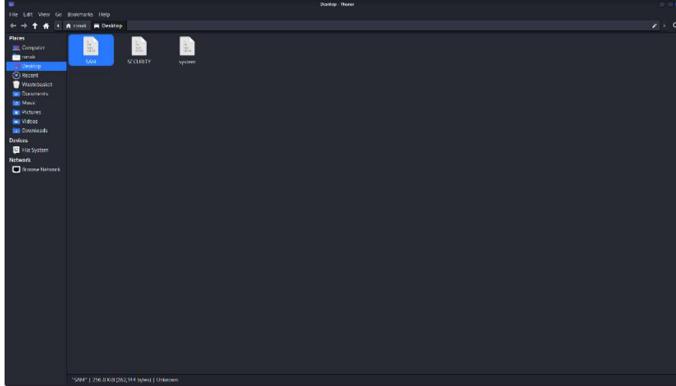
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p>Process: <b>Deleted Files&gt;File System</b></p>  <p>Process: <b>Deleted Files&gt;All</b></p>

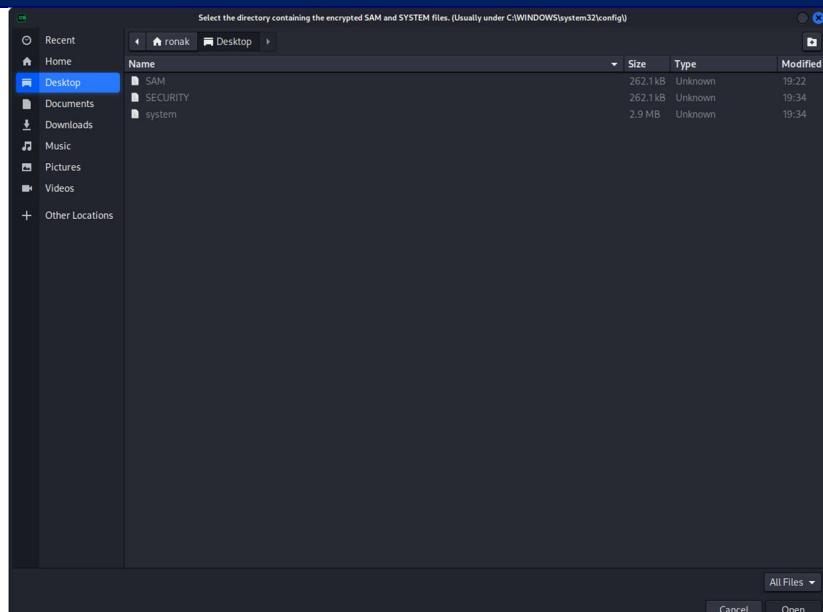
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>With this we are able to recover lost files and the deleted files were carved.</p>
Run relevant keyword searches; Did you index the evidence file?	Done	2025/12/14	10:00 PM (UTC +5:45)	 <p>I mentioned few single-word keywords in the module “<b>Keyword Search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

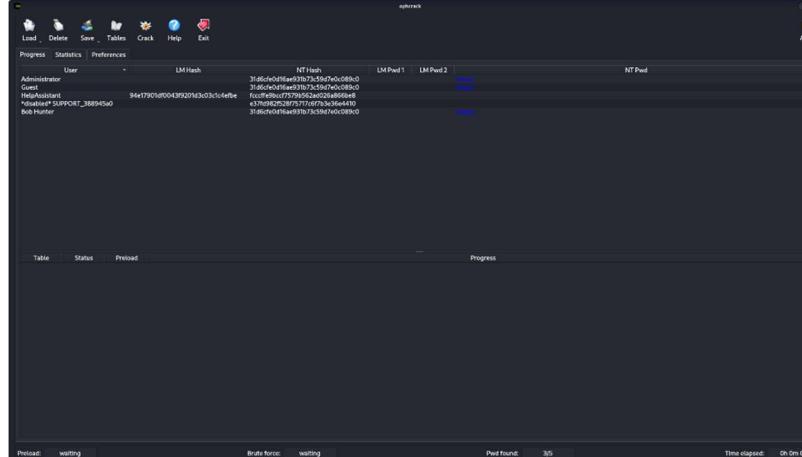
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p>For this a ingest module was run called "<b>keyword search</b>".</p>  <p>The screenshot shows the 'Configure Ingest Modules' dialog. Under the 'Run ingest modules on:' dropdown, 'All Files, Directories, and Unallocated Space' is selected. In the list of modules, 'Recent Activity', 'Hash Lookup', 'File Type Identification', 'Extension Mismatch Detector', 'Embedded File Extractor', 'Picture Analyzer', and 'Keyword Search' are listed. 'Recent Activity' has a yellow warning icon. 'Keyword Search' has a blue checkmark icon and is highlighted with a red box. To the right of the list, there's a section titled 'Select keyword lists to enable during ingest:' containing a list of keywords: 'stalk', 'canon', 'bob', 'billy', 'bomb', 'rasphone', 'password', and 'sabrina'. A red box highlights this list. Below the list are sections for 'Latin - Basic' encodings (UTF8, UTF16), OCR options, and file size filtering. At the bottom are buttons for 'Select All', 'Deselect All', 'History', and navigation links ('&lt; Back', 'Next &gt;', 'Finish', 'Cancel', 'Help').</p> <p>As shown below relevant search has been done:</p>

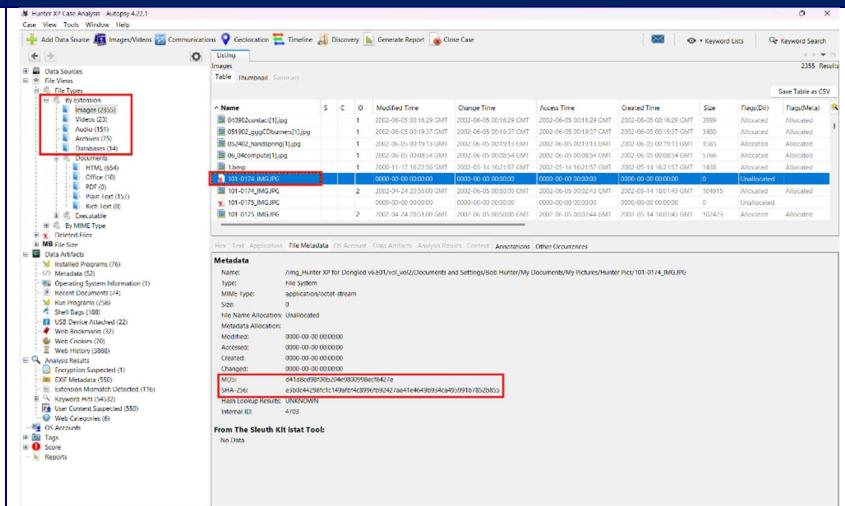
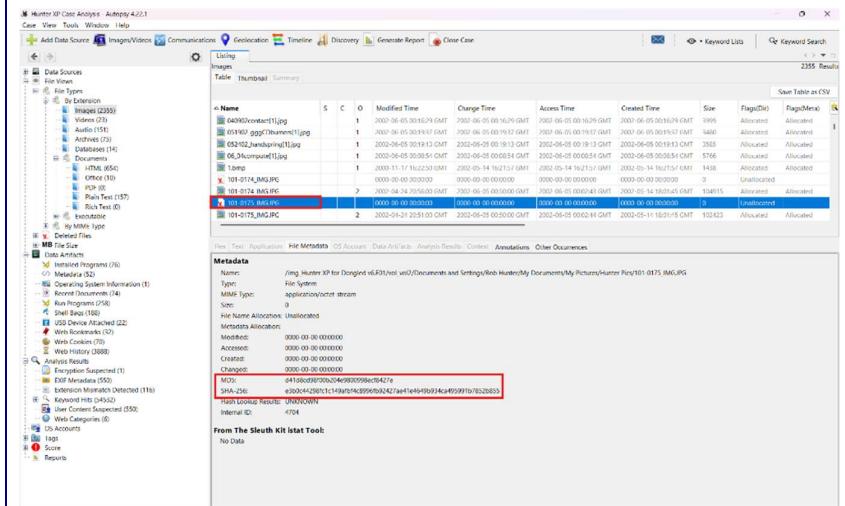
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Under the Single-Keyword Search (<b>Billy</b>), I found information about:</p> <ul style="list-style-type: none"> <li>1.Billy</li> <li>2.Bob</li> <li>3.Bomb</li> <li>4.Canon</li> <li>5.Password</li> <li>6.Rasphone</li> <li>7.Sabrina</li> </ul>
Recover Log-on passwords – use SAMInside/Ophcrack/Encase	Done	2025/12/15	6:00 PM (UTC +5:45)	For this we extract the <b>SAM</b> , <b>SECURITY</b> , and <b>SYSTEM</b> files using ftk imager.

Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>We used ftk to access the image file and go to this location <b>Windows&gt;System32&gt;Config</b></p>
				 <p>2 objects and 6 files exported successfully. 13/107200 bytes copied.</p>

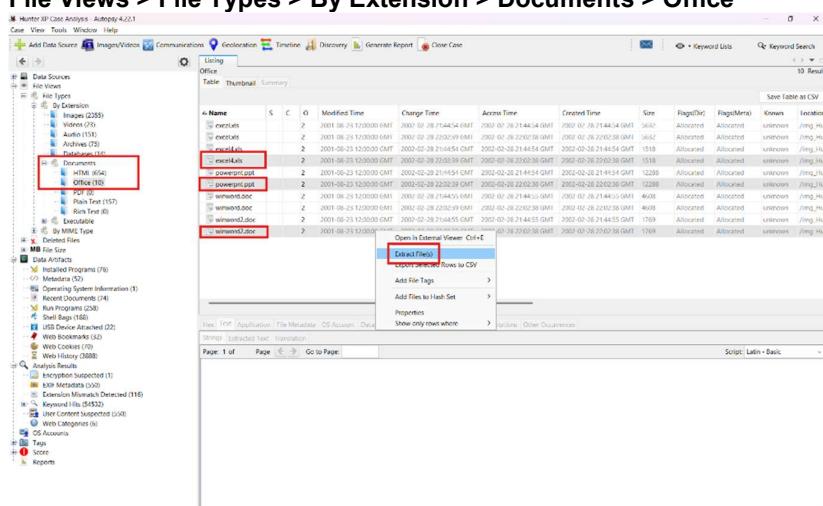
Action	Done?	Date (YY/MM/DD)	Time	Notes
				<p>Here, I extracted the Registry files.  <b>Location: Extract Files&gt;Desktop&gt;H-XP_RegFiles</b></p> <p>I used Kali Linux to run <b>OPHCRACK</b>.  So, I moved these 3 (<b>Sam, Security, and System</b>) in Kali Linux.</p>  <p>Now we load up <b>ophcrack</b>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

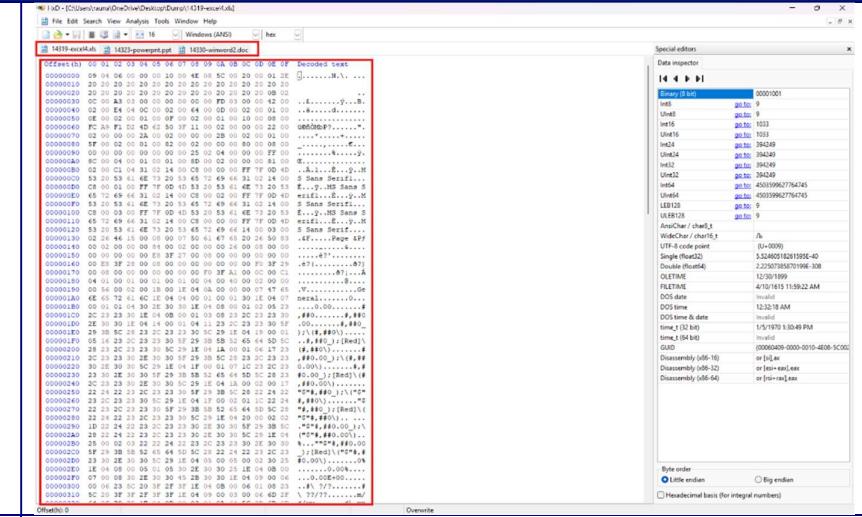
Action	Done?	Date (YY/MM/DD)	Time	Notes																
				 <p>Select the directory containing the encrypted SAM and SYSTEM files. (Usually under C:\WINDOWS\system32\config)</p> <p>Recent</p> <ul style="list-style-type: none"><li>Home</li><li>Desktop</li><li>Documents</li><li>Downloads</li><li>Music</li><li>Pictures</li><li>Videos</li><li>Other Locations</li></ul> <table border="1"><thead><tr><th>Name</th><th>Size</th><th>Type</th><th>Modified</th></tr></thead><tbody><tr><td>SAM</td><td>262.1kB</td><td>Unknown</td><td>19:22</td></tr><tr><td>SECURITY</td><td>262.1kB</td><td>Unknown</td><td>19:34</td></tr><tr><td>system</td><td>2.9 MB</td><td>Unknown</td><td>19:34</td></tr></tbody></table> <p>All Files Cancel Open</p> <p>With this we are able to get the info we need.</p>	Name	Size	Type	Modified	SAM	262.1kB	Unknown	19:22	SECURITY	262.1kB	Unknown	19:34	system	2.9 MB	Unknown	19:34
Name	Size	Type	Modified																	
SAM	262.1kB	Unknown	19:22																	
SECURITY	262.1kB	Unknown	19:34																	
system	2.9 MB	Unknown	19:34																	

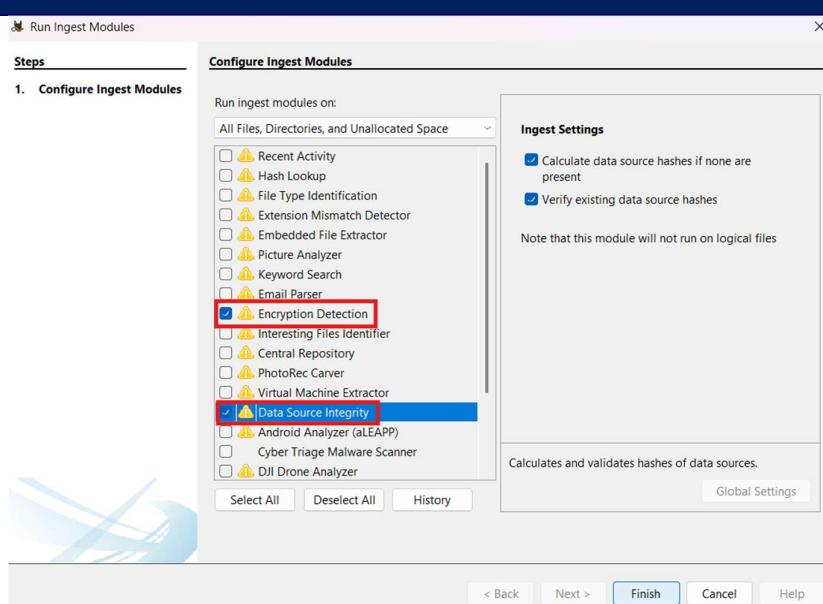
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>We get the following hash which means that there is no password in the system.</p>
Examine different file types: Export doc/office and exe files; look at Metadata if required	Done	2025/12/15	9:00 PM (UTC +5:45)	<p>Here, we analysed the file types in autopsy.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

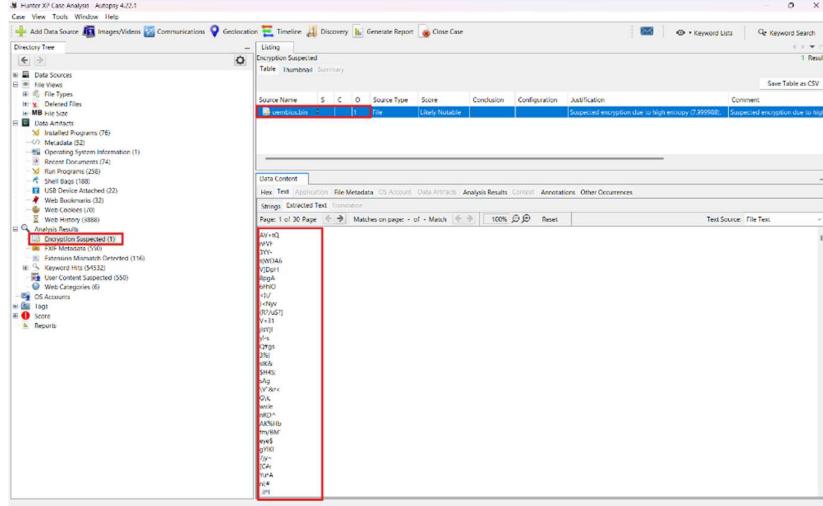
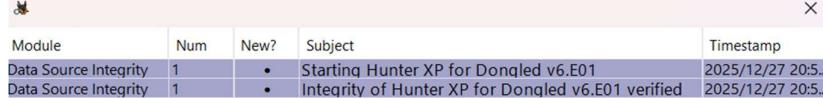
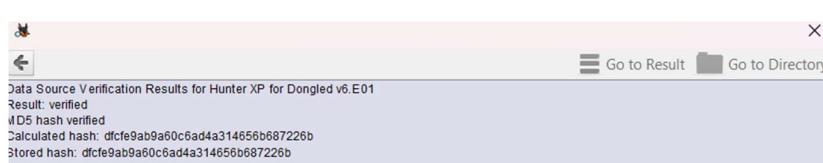
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>The screenshot shows two separate windows of the Hunter X Case Analyst tool. Both windows display a list of files under the 'File Types' category, specifically 'Images'. Two specific files are highlighted in red: '101-0174.JPG' and '101-0175.JPG'. The details pane for each file shows identical metadata, including:</p> <ul style="list-style-type: none"> <li><b>MD5:</b> e4180809000000000000000000000000</li> <li><b>SHA-256:</b> e300442051119049409598e5427e</li> <li><b>File System Type:</b> application/octet-stream</li> <li><b>File Name Allocation:</b> Unallocated</li> <li><b>Metadata Allocation:</b> Unallocated</li> <li><b>Accessed:</b> 0000-00-00 00:00:00</li> <li><b>Created:</b> 0000-00-00 00:00:00</li> <li><b>Changed:</b> 0000-00-00 00:00:00</li> </ul>
				 <p>This row contains the same information as the previous one, showing two more instances of the same image files ('101-0174.JPG' and '101-0175.JPG') with identical hash values and metadata across both tool instances.</p>

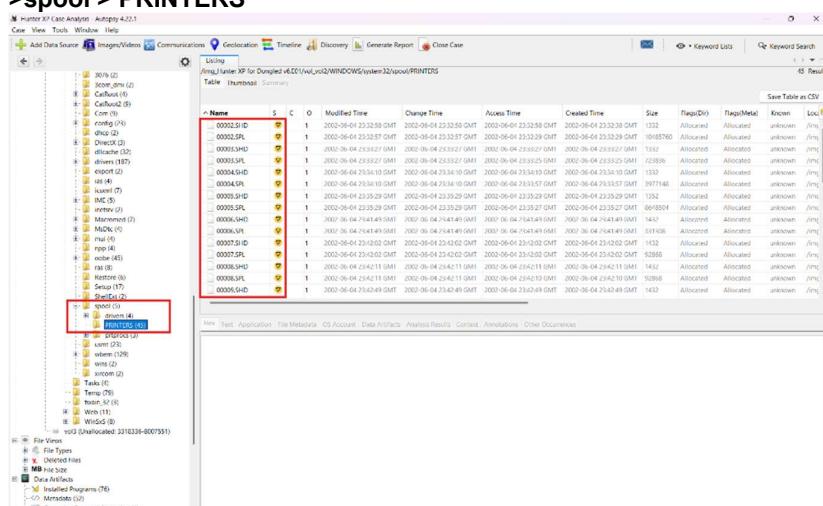
The MD5 and SHA -256 of all the image files have the same hash values.

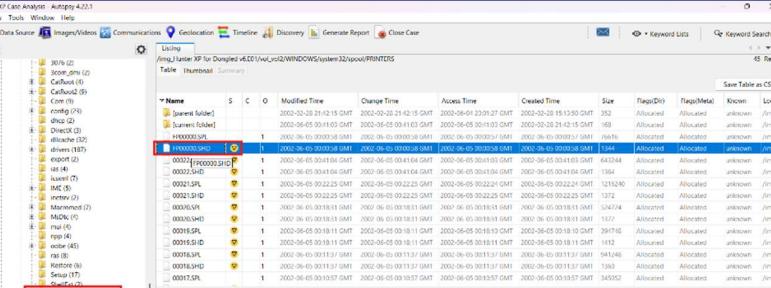
Action	Done?	Date (YY/MM/DD)	Time	Notes												
				<p>Similarly, For the purpose of inspection, we extracted the doc files. In order to do this, we go to <b>File Views &gt; File Types &gt; By Extension &gt; Documents &gt; Office</b></p>  <p>Then we extract the doc files. <b>Location: Extract files&gt;Desktop&gt;Dump (Folder)</b></p> <table border="1"> <tbody> <tr> <td>14319-excel4</td> <td>12/27/2025 8:28 PM</td> <td>Microsoft Excel 97...</td> <td>2 KB</td> </tr> <tr> <td>14323-powerpt</td> <td>12/27/2025 8:28 PM</td> <td>Microsoft PowerPo...</td> <td>12 KB</td> </tr> <tr> <td>14330-winword2</td> <td>12/27/2025 8:28 PM</td> <td>Microsoft Word 97...</td> <td>2 KB</td> </tr> </tbody> </table> <p>And put it through <b>HxD</b>. Through which we are able to take a look at the binary data of the doc files.</p>	14319-excel4	12/27/2025 8:28 PM	Microsoft Excel 97...	2 KB	14323-powerpt	12/27/2025 8:28 PM	Microsoft PowerPo...	12 KB	14330-winword2	12/27/2025 8:28 PM	Microsoft Word 97...	2 KB
14319-excel4	12/27/2025 8:28 PM	Microsoft Excel 97...	2 KB													
14323-powerpt	12/27/2025 8:28 PM	Microsoft PowerPo...	12 KB													
14330-winword2	12/27/2025 8:28 PM	Microsoft Word 97...	2 KB													

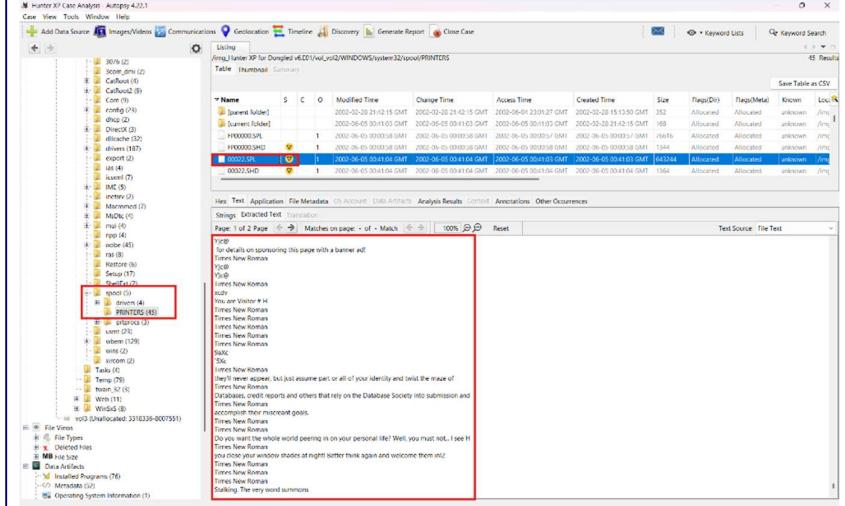
Action	Done?	Date (YY/MM/DD)	Time	Notes
				
Encryption, Steganalysis (any indications? Entropy or Autopsy can be used)	Done	2025/12/15	11:30 PM (UTC +5:45)	<p>For this process, we run a ingest module called "<b>Encryption Detection</b>". Also, if you want to check the integrity of the file, you can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

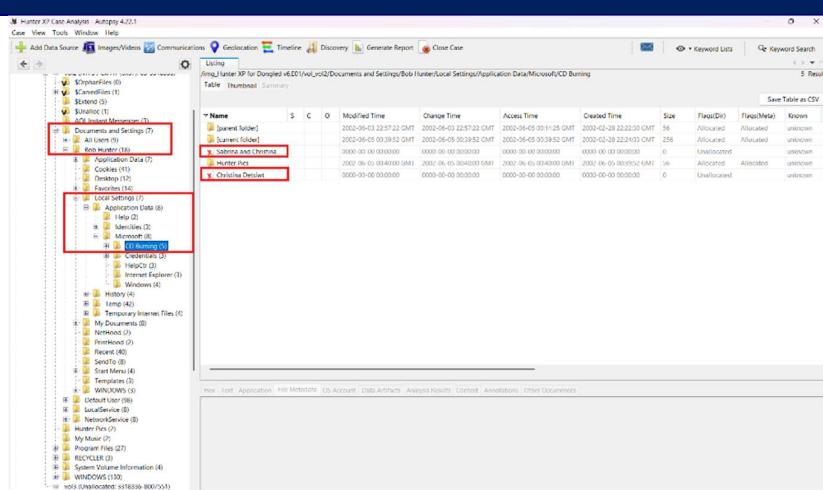
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>With this we can find the Encryption Suspected tab under Analysis Result.</p>

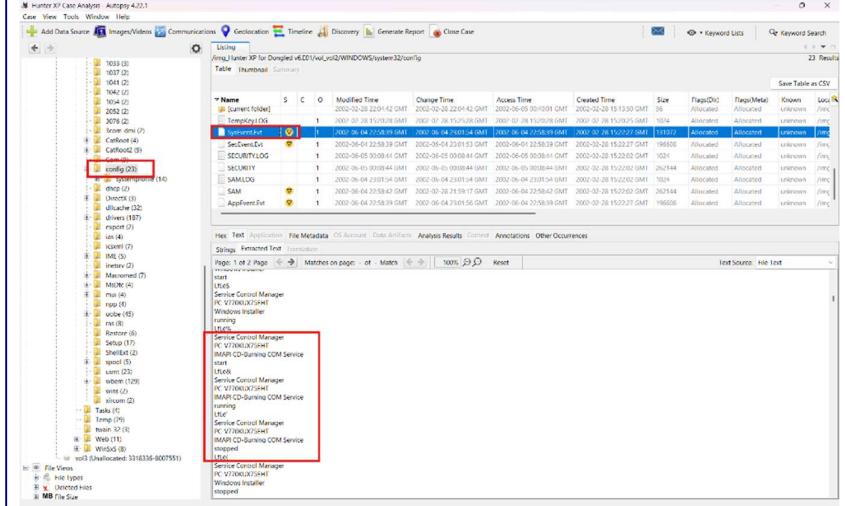
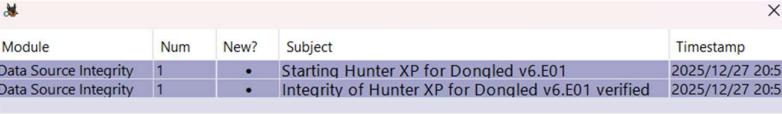
Action	Done?	Date (YY/MM/DD)	Time	Notes
				 <p>Here the file <b>oembios.bin</b> are suspected to be encrypted.</p> <p>I performed this module to check if the file was tampered or not while performing any task which shows if the file was encrypted or not.</p>  <p>Here is the hash value of the image.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

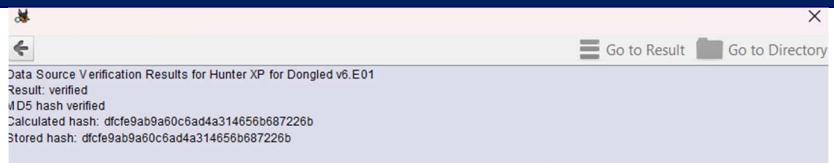
Action	Done?	Date (YY/MM/DD)	Time	Notes
Print artefacts	Done	2025/12/16	8:00 PM (UTC +5:45)	<p>To find the print artifacts we first navigate to</p> <p>Process:</p> <p><b>Data Source &gt; Hunter XP Dongled &gt; VOL2 &gt; WINDOWS &gt; system32 &gt;spool &gt; PRINTERS</b></p>  <p>Here, we check the .SHD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

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

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

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

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

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

#### Additional Notes/Artefacts Examined:


Colour-coding Legend	Tasks
	Fundamental
	Basic
	Elementary
	Secondary
	Advanced
	Exceptional