Contemporaneous Notes

Note: This document forms the scope of your investigation, the Officer In Charge wants these areas examined. If you decide to omit a process, then you should provide your reasons for doing so here and in your statement. You may add additional rows, as appropriate.

Examiner	Sahifa Syed	Exam commenced	19/10/2023 – 11/01/2024
Other relevant information	-	Software used, versions and licensing	Encase Autopsy

Action	Done?	Date	Time	Notes
Load case and verify image	Yes, done	23/10/2023	10:00am	I have been asked to load the case HunterXP into encase and verify the image. To do this I downloaded the HunterXP image from the sway. Once that was completed I loaded the case into encase and verified the image. The image verified successfully without any errors and the acquisition and verfication values matched accurately. **(refer to figure 1 in the appendix below)** It COMPLETELY verified with 0 errors. **Acquisition MD5 dfcfe9ab9a60c6ad4a314656b687226b** **Verfication MD5 dfcfe9ab9a60c6ad4a314656b687226b**
Load Case into second forensic tool for dual verification of at least 2 key artefacts, evidence items	Yes, done	09/11/2023	03:14pm	I have been asked to load the case into another forensic tool for dual verification comparing two key artefacts (evidence items). AFTER successfully loading the case into **encase (forensic tool 1),** I chose **autopsy for my second forensic tool**. To do this I downloaded autopsy from the sway and loaded the case successfully. For dual verification I used an **image as my first key artefact**. I compared the same image in both autopsy and encase and all the values and dates matched .

Action	Done?	Date	Time	Notes
				Found Image 101-0188_IMG.JPG in both encase and autopsy. The MD5 value of the image is 5ead9d1c32a5deb91600b0783b7b4699. The image was last accessed 04/06/02 19:04:14 as stated in the image. (refer to figure 2 in the appendix below) For my **second key artefact** I chose to compare a **document** on encase and autopsy which consists of banking information. The values and dates once again matched on both forensic tools. **The MD5 value of the document is 2f3bf3218f33863fcb5990f64fb137ee4. The image was last accessed 03/06/02 16:09:36 as stated in the image. (refer to figure 3 in the appendix below)**
Time Zone Adjusted? Report Time Zone used for Analysis.	Yes, done	25/10/2023	02:00pm	I have been asked to adjust the time zone settings. In order to do this, I went to the system file at **C:\WINDOWS\system32\config\system**, and I mounted it successfully by accessing the file structures in the entries tab. A green plus icon in the figure below illustrates this process **(figure 4)**. I then performed a right-click on the Hunter XP picture folder and selected the modify Time Zone settings key **(figure 5)**. Before making any changes, I first made sure to confirm and verify the current settings of the time zones. This then resulted in the time zone being changed from Dublin to Central Time (US and Canada) **(figure 6)**. After making this modification, I verified the timestamps so that every piece of evidence was shown in Central Time **(figure 7)**. This was done in order to preserve consistency and relevance to the case. The modifications were appropriately implemented.
Recover lost folders (NTFS,FAT16&32)	Yes, done	26/10/2023	04:15pm	I was asked to recover lost folders in encase and to simultaneously check if the process ran successfully by using autopsy. To do this I selected the evidence processor in encase. Once that opened up, I clicked the hyper link for the recover lost folders section and checked in the box called 'reconstruct folder structure'. After checking in the hyperlink, I checked in the main recovery folders box and selected OK **(figure 8)** . Once verifying that the folders had been recovered correctly in Encase, I used Autopsy to perform a second examination to make sure everything about the folders was in working order **(refer to figure 9 in the appendix)**.
Mount archives; zip, thumbs.db, etc.	Yes, done	21/11/2023	03:34pm	I was asked to mount archive files which consists of zip files, thumbs and more. I opened up hunter XP on encase and processed the evidence. Once the evidence was processed and the evidence processor appeared. I checked in the boxes to

Action	Done?	Date	Time	Notes
				expand the compound files to enable access for all file types. This process has ran successfully as everything within encase is now decompressed **(see figure 10)**.
File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation)	Yes, done	20/11/2023	01:55pm	I have been asked to run the process of file signature analysis and examine the results it produces, compute hash values by enabling entropy as well as to record my observations if I found any alias or bad signature files. To do this I loaded and processed the evidence processor. Once that was complete, I carefully checked that the MD5, entropy, and SHA values were enabled and accurate **(see figure 11)**. *It is important to mention that the SHA value was not initially given in Encase when the case was first uploaded. This absence of the SHA value persisted throughout the entire investigation process*. Once all of the above was performed correctly, I then began to look for alias and bad signature files and after an in-depth search, I found internet jpeg files which were considered as false positives meaning they were executable **(see figure 12).**
Internet History, favourites, etc. Other browsers?	Yes, done	20/11/2023	04:11pm	I have been asked to recover and examine the internet history/web browser data contained within the device. To do this I used the 'Evidence Processor' within EnCase. I first enabled the find internet artefacts options within the evidence processor **(figure 13)**. The process had ran successfully as there was evidence to be examined in the records tab. On reviewing the extracted internet history I was able to find notable evidence that was related to stalking. There is evidence that a user has typed into a web browser searches (URLS) related to stalking **(refer to figure 14).**
Emails, local and web-based.	Yes, done	23/11/2023	03:00pm	I have been asked to examine different types of emails (local and web-based) using Encase. I utilized the 'evidence processor' and selected the find emails option. Once the process completed, options were shown and I selected a couple which I then chose to extract **(see figures 15 and 16)**. I then went to the 'Records tab' to thoroughly examine emails. I found some fishy deleted emails, and I've displayed it in the appendix below **(refer to figure 17)**. During this thorough examination I found an array of emails. These emails were exchanged between various individuals and they were closely related to the stalking activity under investigation. The content of these messages included the transmission of pictures of a woman getting out of her car, holding a letter and going to a post office and through the windows reflection, you can see a man with a camera. The woman in the pictures seems to be unaware of the pictures being taken of her. This finding was vital to building a clearer understanding of the case **(figure 17.1)**.

Action	Done?	Date	Time	Notes
Retrieve operating system information, accounts information, software, time zone information etc.).	Yes, done	30/11/2023	01:44pm	I have been asked to retrieve operating system information which includes information retrieved from accounts, software, time zone etc. To do this I processed and loaded the evidence processor. I then checked into the box for the system info parser and ran the process. Once the process ran successfully, I navigated to the view tab and then went into records for a more thorough examination of the results. This resulted in me finding information from various registry keys which included information about the time zone, service artefacts. This vital information has been displayed in the appendix for reference.
Timeline analysis- Note date of last activity on the computer. System profiling.	Yes, done	30/11/2023	01:44pm	I was asked to examine and analyse the timeline data within encase and record the install and the shutdown times on the device. I done this by using the evidence processor and selecting the system info parser. After the process had ran successfully I utilized the registry records to determine the installation and last shutdown dates and times of when the computer was in use **(as shown in figure 25)** . I also managed to find time zone information within the registry records **(refer to figure 26)**. It is essential to remember and mention that while there is a recorded shutdown time as stated in the appendix below, the computer was not shutdown correctly. This implies that the shutdown time is therefore unreliable and there is a possibility of file activity after the shutdown time meaning the computer could have been in use after the last recorded shutdown date.
Registry analysis and Registry protected area	Yes, done	10/12/2023	05:50pm	I was asked to carry out a thorough analysis within the registry and its protected area. To do this I used the evidence processor in Encase and selected the system information parser. Upon successful completion of this initial step, I examined the registry which consists of a number of 'hive' files. These hive files: SOFTWARE, SYSTEM, SAM, SECURITY were already analysed before. I have used the tools **registry viewer as well as RegRipper** to analyse these files. *[refer to the notes under the blue heading **Recover log-on passwords]* The Sam file Stores users' passwords in a hashed format, the system and security files aided me in determining that the device was not password protected and the software file enabled me to find out Operating System information **(refer to figure 53 and 54 in the appendix below).** This was all important information to know beforehand in order to proceed with this investigation further. **For the registry protected** area I manged to located and carefully examine various NTUSER.dat files. To analyse these files more accurately, I utilized

Action	Done?	Date	Time	Notes
				RegRipper, a well-known tool in digital forensics for parsing registry information. With the results from RegRipper, I was able to find relevant information about **the LastWrite Time, LastVisitedMRU , MRU list and the Last directory**. The specifics of this thorough analysis are documented in the provided appendix below **(figure 28)**.
Link files and Recycle Bin	Yes, done	07/12/2023	01:30pm	I was asked to identify .LNK files and view the recycle bins and record anything relevant to it. To do this I used the "Evidence Processor" within EnCase and processed the 'windows artefact parser' making sure that all the correct settings within the hyperlink were selected. After this process was successfully finished, I examined the files under the 'records' tab **(see figure 29)**. Following that, I processed the case analyser, went into the software usage section and found the executable .LNK files. I located a number of lnk files here and saved the ones that were relevant to the case **(figure 30).** I took a few actions in an attempt to make sure the Recycle Bin files were intact and to make sure there had been no bypass. Initially, I navigated to c:\WINDOWS\System32\config\software, where the software file was successfully mounted. I expanded the folders: **Microsoft ,Windows, Current Version, Explorer, Bitbucket to access the files inside.** I found the **'nuke on delete'** setting there, and its hex value of 00 00 00 00 meant that there had been no bypass and the files were correct and undamaged. ***I have also mentioned this in the appendix (figure 31).*** After that, I went back to the case analyser and discovered, among the files in the Recycle Bin, a noteworthy file called "Sabrina Dewercs" (**figure 32**).
Instant Messaging clients	Yes, done	30/11/2023	01:44pm	I was asked to examine instant messaging clients. To do this I used the evidence processor. Within the evidence processor, I expanded the folder 'modules' and selected the IM Parser **(see figure 33)**. After that, I executed the process, and it ran successfully. I navigated to the view tab and then went into records for a more thorough examination of the results. As a result, multiple messages that seemed to be of relevance to the case were found. I also looked into different chats. For detailed documentation and conclusions, ***please refer to the appendix below in figures 34, 35 and 36.***

Action	Done?	Date	Time	Notes
Clean-up/Wiping utilities. Check log files. Anything used?	Yes, done	06/12/2023	12:00pm	I have been asked to determine if any clean/wiping utility has been used by examining relevant program files, .log files , event logs and possibly examine the prefetch folder to see if a relevant program has been run. To do this I navigated to the 'records' tab and selected the 'Windows event log parser'. Within there, I then looked into System Event Log in which I found important information relevant to the case. This specific information linked to a source under the name "Remote Access", I've displayed the specifics in the appendix below **(see figure 37)**. Furthermore, I 'green plated' the Hunter XP, and this led me into locating and examining relevant .**log files under the folder called outlook express** as well as **executable files under the prefetch folder and the system32 folder. (Refer to figures 38, 39, 40 in the appendix below)**. These files contained valuable information relevant to the case related clean-up utilities as well as permissions within it relating to a user account.
External drives; Network connections	Yes, done	07/12/2023	2:08pm	I have been asked to examine the relevant registry artefacts to identify what external devices have been attached to the computer. To do this I used the evidence processor. Within the evidence processor I expanded the module folder, selected the system info parser option and managed to run it successfully. After execution of the system info parser, I examined the results by navigating to the 'records tab' **(figure 41)** and under the Hunter XP section, I found USB drives which are considered as external drives to be attached to the computer. **Figure 42** in the appendix below consists of specific information about the USB drive such as disk name and serial number, etc.
Perform data carving	Yes, done	30/11/2023	4:41pm	I have been asked to perform data carving within encase. To do this I used the evidence processor. Within the evidence processor, I expanded the folder 'modules' and selected the File Carver Option **(see figures 43 and 44).** After that, I executed the process, and it ran successfully. I carefully examined the results and amongst the findings, I found two specific files that was important to the case. It included mail sent from the device to the parent of the individual as it referred to the term 'daughter' more than once a well as images being sent of a woman who does not seem to know that someone is taking pictures of her. The specifics are included in the appendix below **(see figures 45, 46 and 47)**.

Action	Done?	Date	Time	Notes
Run relevant keyword searches; Did you index the evidence file?	Yes, done	23/11/2023	1:48pm	I was asked to run keyword searches relevant to the case by Indexing the evidence files and then examining the end results. To do this I indexed the case by using the evidence processor **(figure 49)**. Once the case was indexed successfully, the next step was to expand compound files which was already done **(see figure 10)**. I then began my keyword search specifically using terminology related to stalking (stalk, stalker etc..). This search resulted in various files appearing that could be evidence related to the case **(see figures 48 and 50)**. I then performed a raw search **(figures 51 and 52)**. For this part there is no need to process the evidence. I used the GREP function to zero in on specific terminology – in this case, the word "dad" in the Hunter Pics Folder. This search resulted in me finding useful information relevant to the case.
Recover Log-on passwords – use SAMInside/Ophcrack/Encase	Yes, done	16/11/2023	4:53pm	I was asked to recover log-on passwords and determine if the device was protected by a password or not. To do this I went to encase and selected the following directory **C: \WINDOWS \system32 \config \system**. I selected the files SAM,SYSTEM,SECURITY,SOFTWARE and copied the files into the registry viewer in order to view an analyse them **(figure 53).** Once that was successfully completed I downloaded a tool called '**saminside'** from the sway and opened up the files SYSTEM and SECURITY which led me into finding out that this device was not password protected **(figure 54).**
Examine different file types: Export doc/office and exe files; look at Metadata if required	Yes, done	14/12/2023	02:00pm	I have been asked to examine and document different file types most relevant to the case as well as the meta data of notable files. To do this I utilized the filter option on encase. I filtered my selection by finding files based on their extensions **(figure 55)** . I managed to find a jpeg file and two executable files which seemed of significance to the case. I also bookmarked these files. More information about these files, their relevance, and their context in the investigation can be found in the appendix below **(refer to figure 56)** as well as the SS2 :evidence record provided in separate document.
Encryption, Steganalysis (any indications? Entropy or Autopsy can be used)	Yes, done	07/12/2023	5:00pm	Jay had given me specific instructions to identify and determine for encryption using encase and to not perform a steganalysis during this investigation as we have not yet covered it in the curriculum. Initially, I made sure to check that the hash analysis option and within it the entropy option has been enabled. This was done by loading the evidence

Action	Done?	Date	Time	Notes
				processor, selecting the hash analysis hyperlink and finally checking in the box to enable the entropy. **This process was already done in one of the earlier processes (refer to figure 11)**. I then 'green plated' Hunter XP to simplify my search and the results of this process and analysis led to a display of a column consisting of multiple entropy values dedicated to files within encase. The process of entropy analysis involves evaluating the degree of randomness present in data in which Encase assigns an entropy value to each folder and file. **Generally, a higher entropy value indicates a greater probability of encryption**. More specifically, files with entropy values ranging from 6 to 8 are regarded as strong contenders for encryption. In my analysis, I looked for files which had the entropy of the first set till 7 values , as they usually offer the most dependable clues regarding encryption if there is no file signature on them. Once I found the files with the highest entropy values, I conducted a thorough examination of their hex representation and it seemed messy and random. The results of this analysis, including specifics about the files that have the highest entropy levels, have been recorded and added to the appendix for a thorough and targeted investigation of any possible encryption within the dataset. **(refer to figure 57)** Upon closer inspection, I managed to identify an MZ executable file, which had a high entropy value of **7.9867..** , was a false positive as it turned out to be an archive file **(refer to figure 58)**.
Print artefacts	Yes, done	21/11/2023	4:25pm	I was asked to find print artefacts in encase. To do this I chose to manually search for .SPL and .SHD files when the automated process failed to locate them. I went to the printers directory located at C:\WINDOWS\system32\spool\printers and within there were a range of .SPL and .SHD files. Starting with the .SPL files, I began my search for the EMF marker. This was done by viewing each of the files Hex view. Once the EMF marker was located **(see figure 59)** . With the help of the GPS, I then managed to select the 41 bytes that came before the EMF sequence **(figure 60)**. By doing so, I successfully identified a notable document that had been sent to the printer which was indicated by the file 00018.SPL.**This notable file was relevant to the case as it consisted of an email within it a picture of a female and the subject titled: "Your daughters safety depends on this" (figure 61)**. *I've also bookmarked this piece of information within my evidence record (page 16)*

Action	Done?	Date	Time	Notes
				however when the evidence record was extracted out of encase, it repeatedly blocked out the text but kept the image (Jay said I should just mention this bit in my notes). Additionally, I investigated a .SHD file in the same directory within Encase. This also seemed relevant to the case as it held information about the type of printer in use **(figure 62).**
CD/DVD burning apps; check log files	Yes, done	07/12/2023	4:41pm	I was asked to see if CD/DVD burning apps were used by looking for relevant program files and relevant .log files and to examine the prefetch files to see if a relevant program has been run. To do this I began by green plating the Hunter XP case in the evidence tab on encase. This helps me in selecting everything at once and it enables me to simplify my selection by marking all the relevant items in the folder. I then began my search for CD related log files by looking through the hex data. After carefully examining multiple files and the hex data they contain. I came across one specific file that seemed of great relevance to the case. The file I found is called Hunter.log, within its hex data tab I found a conversation between two people discussing matters related to money, this could be seen as evidence to the case **(refer to figure 63).**
Validate evidence integrity at the end of the examination	Yes, done	15/12/2023	09:11am	I have been asked to validate evidence integrity at the end of the examination. To do this I went to the HunterXP case and viewed the fields tab. The evidence had been verified successfully without any errors and the acquisition and verfication values matched accurately. **(refer to figure 64 in the appendix below)** It COMPLETELY verified with 0 errors.

Additional Notes/Artefacts Examined:

Performing Bypass for Recycle bin	Yes, done.	07/12/2023	01:30pm	I took a few actions in an attempt to make sure the Recycle Bin files were intact and to make sure there had been no bypass. Initially, I navigated to c:\WINDOWS\System32\config\software, where the software file was successfully mounted. I expanded the folders: **Microsoft ,Windows, Current Version, Explorer, Bitbucket to access the files inside.** I found the **'nuke on delete'** setting there, and its hex value of 00 00 00 00 meant that there had been no bypass and the files were correct and undamaged. ***I have also mentioned this in the appendix (figure 31).***

Evidence Record issue for Print Artefacts image	-	-	-	Jay asked me to mention here the issue I faced when extracting the evidence record out of encase. **"This notable file was relevant to the case as it consisted of an email within it a picture of a female and the subject titled: "Your daughters safety depends on this" (figure 61 in the appendix below).** *I've also bookmarked this piece of information within my evidence report (page 16) however when the* ***SS2: evidence record*** *was extracted out of encase, it repeatedly blocked out the text but kept the image"*
Evidence Record issue	-	-	-	Another issue that kept on repeatedly happening was the pictures of interest page. Whilst I do have pictures and they do show up on the evidence record. The record keeps on adding a blank page for it every a couple of pages in after scrolling. All the data within it is correctly extracted from encase however there are some minor issues that keep appearing that is worth mentioning, in order to avoid confusion and any misconceptions

Colour-coding Legend	**Tasks**
	Fundamental
	Basic
	Elementary
	Secondary
	Advanced
	Exceptional

APPENDIX

Load case and verify image:

Figure 1 :

File Integrity	Completely Verified, 0 Errors
Acquisition MD5	dfcfe9ab9a60c6ad4a314656b687226b
Verification MD5	dfcfe9ab9a60c6ad4a314656b687226b

Load case into 2nd forensic tool with dual verification:

Figure 2 :

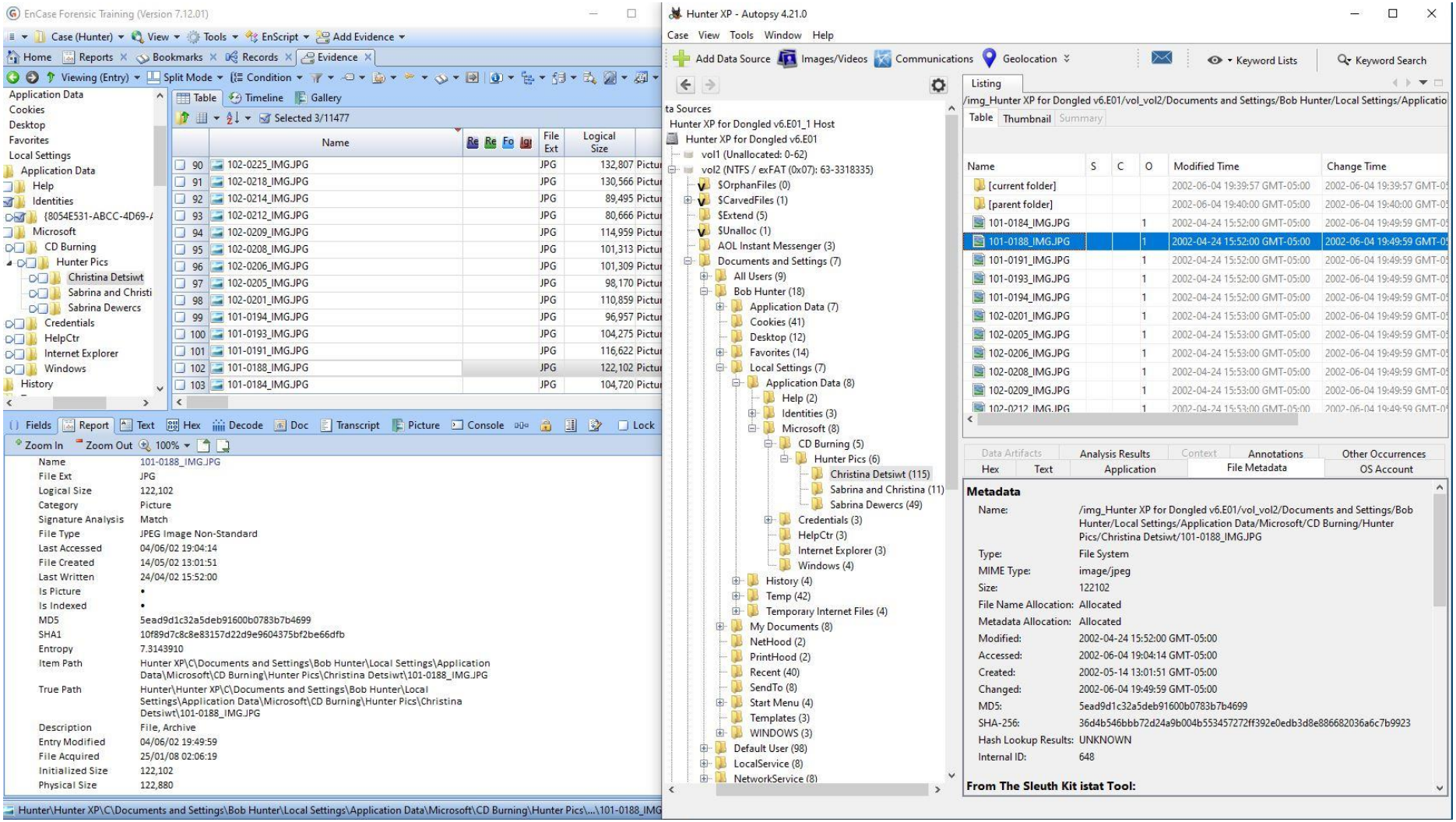
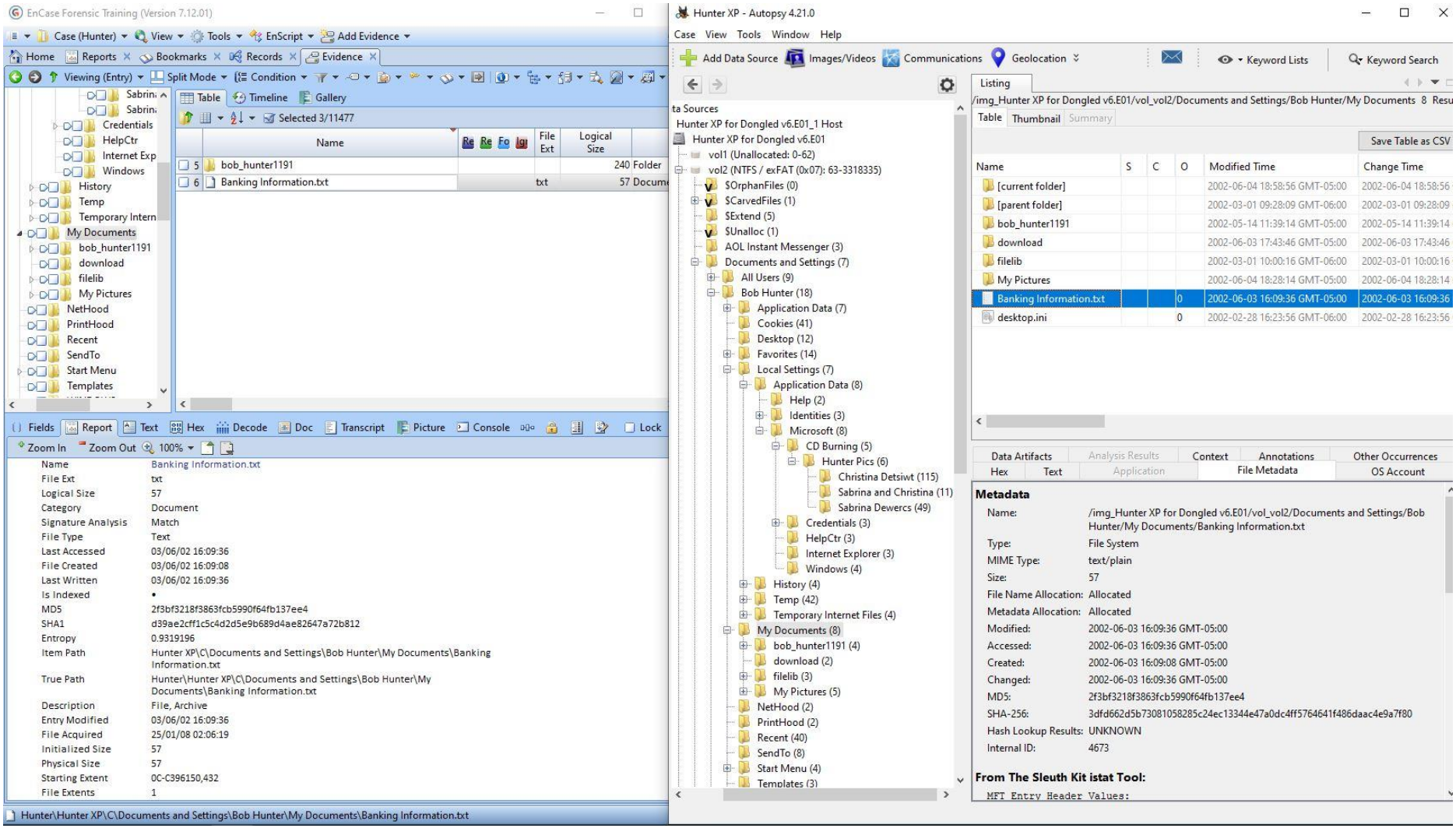


Figure 3 :


EnCase Forensic Training (Version 7.12.01)
Case (Hunter) View Tools EnScript Add Evidence
Home Reports Bookmarks Records Evidence
Viewing (Entry) Split Mode Condition
Table Timeline Gallery
Selected 3/11477
Name File Ext Logical Size
5 bob_hunter1191 240 Folder
6 Banking Information.txt txt 57 Docum
Credentials
HelpCtr
Internet Exp
Windows
History
Temp
Temporary Intern
My Documents
bob_hunter1191
download
filelib
My Pictures
NetHood
PrintHood
Recent
SendTo
Start Menu
Templates
Fields Report Text Hex Decode Doc Transcript Picture Console Lock
Zoom In Zoom Out 100%
Name Banking Information.txt
File Ext txt
Logical Size 57
Category Document
Signature Analysis Match
File Type Text
Last Accessed 03/06/02 16:09:36
File Created 03/06/02 16:09:08
Last Written 03/06/02 16:09:36
Is Indexed •
MD5 2f3bf3218f3863fcb5990f64fb137ee4
SHA1 d39ae2cff1c5c4d2d5e9b689d4ae82647a72b812
Entropy 0.9319196
Item Path Hunter XP\C\Documents and Settings\Bob Hunter\My Documents\Banking Information.txt
True Path Hunter\Hunter XP\C\Documents and Settings\Bob Hunter\My Documents\Banking Information.txt
Description File, Archive
Entry Modified 03/06/02 16:09:36
File Acquired 25/01/08 02:06:19
Initialized Size 57
Physical Size 57
Starting Extent 0C-C396150,432
File Extents 1
Hunter\Hunter XP\C\Documents and Settings\Bob Hunter\My Documents\Banking Information.txt
Hunter XP - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation
Keyword Lists Keyword Search
ta Sources
Hunter XP for Dongled v6.E01_1 Host
Hunter XP for Dongled v6.E01
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 63-3318335)
$OrphanFiles (0)
$CarvedFiles (1)
$Extend (5)
$Unalloc (1)
AOL Instant Messenger (3)
Documents and Settings (7)
All Users (9)
Bob Hunter (18)
Application Data (7)
Cookies (41)
Desktop (12)
Favorites (14)
Local Settings (7)
Application Data (8)
Help (2)
Identities (3)
Microsoft (8)
CD Burning (5)
Hunter Pics (6)
Christina Detsiwt (115)
Sabrina and Christina (11)
Sabrina Dewercs (49)
Credentials (3)
HelpCtr (3)
Internet Explorer (3)
Windows (4)
History (4)
Temp (42)
Temporary Internet Files (4)
My Documents (8)
bob_hunter1191 (4)
download (2)
filelib (3)
My Pictures (5)
NetHood (2)
PrintHood (2)
Recent (40)
SendTo (8)
Start Menu (4)
Templates (3)
Listing
/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/My Documents 8 Resu
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time
[current folder] 2002-06-04 18:58:56 GMT-05:00 2002-06-04 18:58:56
[parent folder] 2002-03-01 09:28:09 GMT-06:00 2002-03-01 09:28:09
bob_hunter1191 2002-05-14 11:39:14 GMT-05:00 2002-05-14 11:39:14
download 2002-06-03 17:43:46 GMT-05:00 2002-06-03 17:43:46
filelib 2002-03-01 10:00:16 GMT-06:00 2002-03-01 10:00:16
My Pictures 2002-06-04 18:28:14 GMT-05:00 2002-06-04 18:28:14
Banking Information.txt 0 2002-06-03 16:09:36 GMT-05:00 2002-06-03 16:09:36
desktop.ini 0 2002-02-28 16:23:56 GMT-06:00 2002-02-28 16:23:56
Data Artifacts Analysis Results Context Annotations Other Occurrences
Hex Text Application File Metadata OS Account
Metadata
Name: /img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/My Documents/Banking Information.txt
Type: File System
MIME Type: text/plain
Size: 57
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2002-06-03 16:09:36 GMT-05:00
Accessed: 2002-06-03 16:09:36 GMT-05:00
Created: 2002-06-03 16:09:08 GMT-05:00
Changed: 2002-06-03 16:09:36 GMT-05:00
MD5: 2f3bf3218f3863fcb5990f64fb137ee4
SHA-256: 3dfd662d5b73081058285c24ec13344e47a0dc4ff5764641f486daac4e9a7f80
Hash Lookup Results: UNKNOWN
Internal ID: 4673
From The Sleuth Kit istat Tool:
MFT Entry Header Values:

Modify Time Zone Settings:

Figure 4:

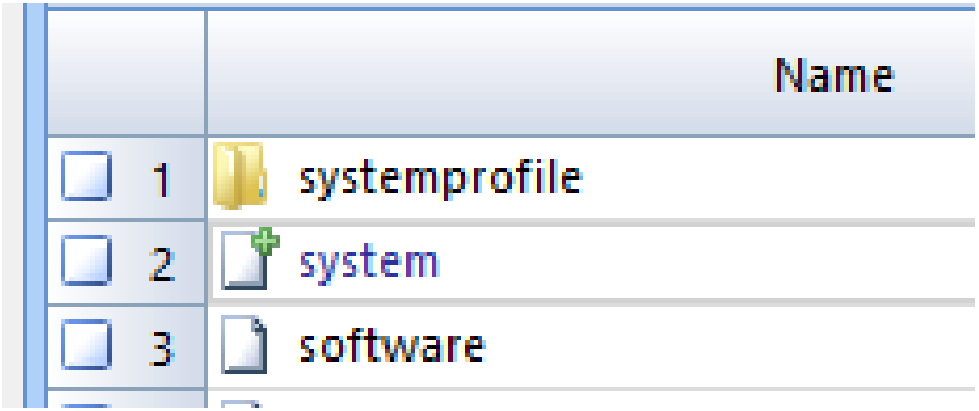


Figure 5:

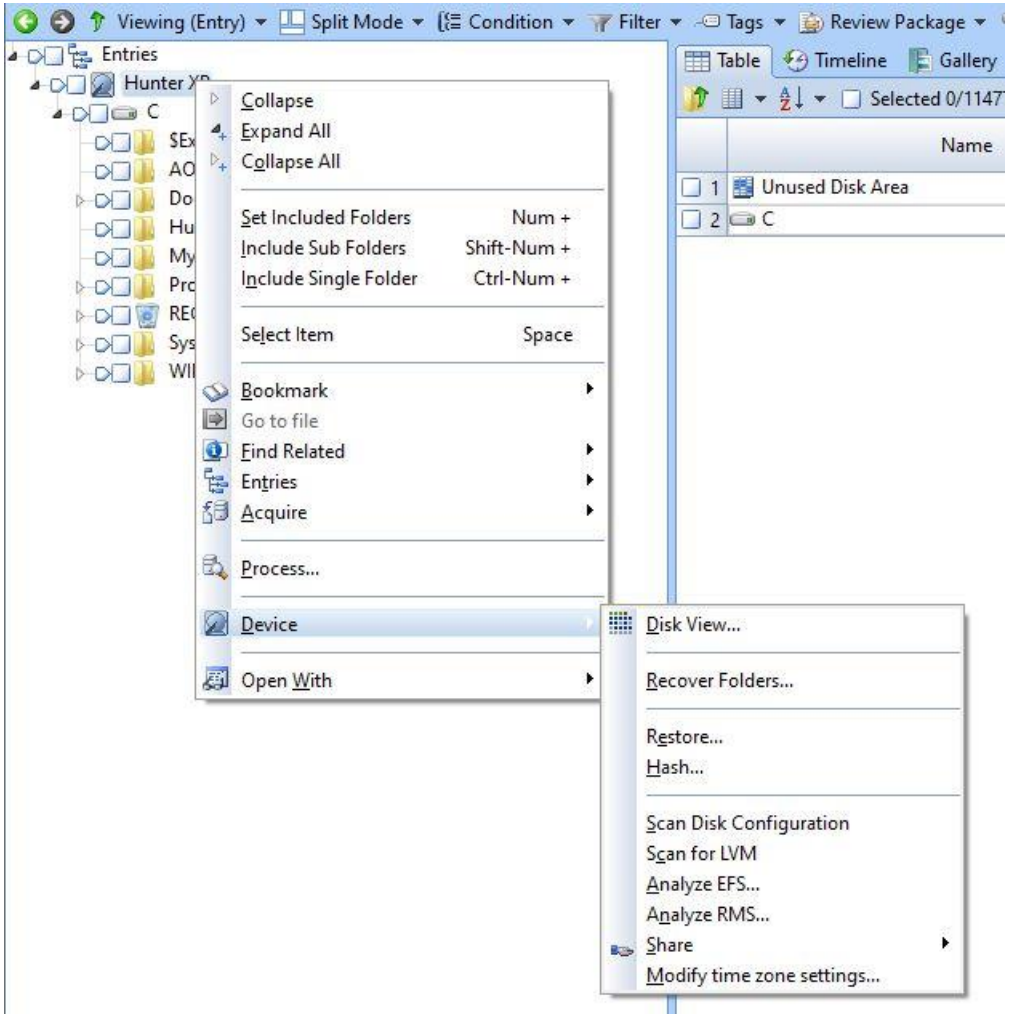

Viewing (Entry)
Split Mode
Condition
Filter
Tags
Review Package
Entries
Table
Timeline
Gallery
Selected 0/1147
Name
1 Unused Disk Area
2 C
Collapse
Expand All
Collapse All
Set Included Folders Num +
Include Sub Folders Shift-Num +
Include Single Folder Ctrl-Num +
Select Item Space
Bookmark
Go to file
Find Related
Entries
Acquire
Process...
Device
Open With
Disk View...
Recover Folders...
Restore...
Hash...
Scan Disk Configuration
Scan for LVM
Analyze EFS...
Analyze RMS...
Share
Modify time zone settings...

Figure 6:

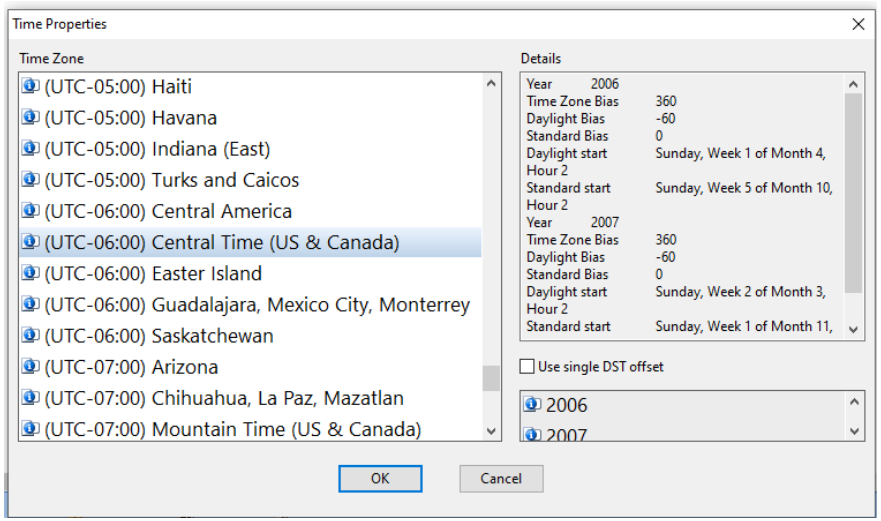
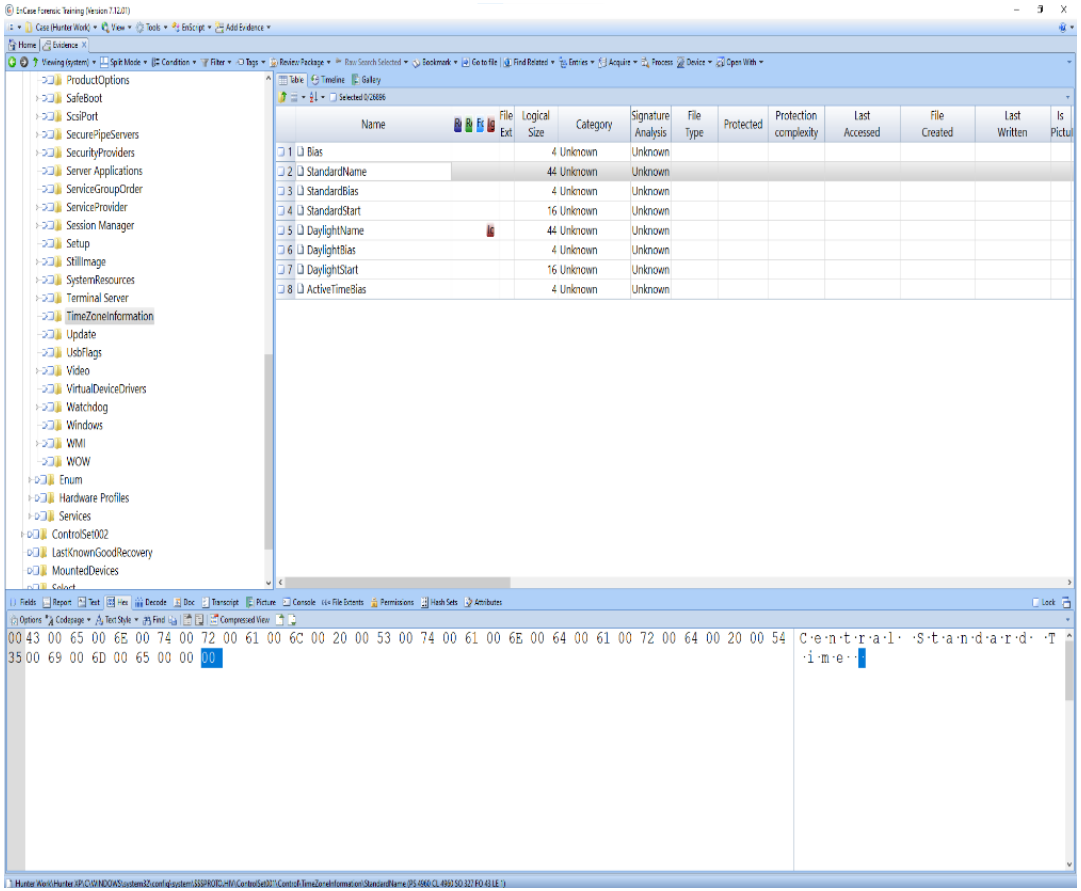

Time Properties
Time Zone
(UTC-05:00) Haiti
(UTC-05:00) Havana
(UTC-05:00) Indiana (East)
(UTC-05:00) Turks and Caicos
(UTC-06:00) Central America
(UTC-06:00) Central Time (US & Canada)
(UTC-06:00) Easter Island
(UTC-06:00) Guadalajara, Mexico City, Monterrey
(UTC-06:00) Saskatchewan
(UTC-07:00) Arizona
(UTC-07:00) Chihuahua, La Paz, Mazatlan
(UTC-07:00) Mountain Time (US & Canada)
Details
Year 2006
Time Zone Bias 360
Daylight Bias -60
Standard Bias 0
Daylight start Sunday, Week 1 of Month 4, Hour 2
Standard start Sunday, Week 5 of Month 10, Hour 2
Year 2007
Time Zone Bias 360
Daylight Bias -60
Standard Bias 0
Daylight start Sunday, Week 2 of Month 3, Hour 2
Standard start Sunday, Week 1 of Month 11,
Use single DST offset
2006
2007
OK
Cancel

Figure 7:


ProductOptions
SafeBoot
ScsiPort
SecurePipeServers
SecurityProviders
Server Applications
ServiceGroupOrder
ServiceProvider
Session Manager
Setup
StillImage
SystemResources
Terminal Server
TimeZoneInformation
Update
UsbFlags
Video
VirtualDeviceDrivers
Watchdog
Windows
WMI
WOW
Enum
Hardware Profiles
Services
ControlSet002
LastKnownGoodRecovery
MountedDevices
Name
File Ext
Logical Size
Category
Signature Analysis
File Type
Protected
Protection complexity
Last Accessed
File Created
Last Written
1 Bias 4 Unknown Unknown
2 StandardName 44 Unknown Unknown
3 StandardBias 4 Unknown Unknown
4 StandardStart 16 Unknown Unknown
5 DaylightName 44 Unknown Unknown
6 DaylightBias 4 Unknown Unknown
7 DaylightStart 16 Unknown Unknown
8 ActiveTimeBias 4 Unknown Unknown
00 43 00 65 00 6E 00 74 00 72 00 61 00 6C 00 20 00 53 00 74 00 61 00 6E 00 64 00 61 00 72 00 64 00 20 00 54
35 00 69 00 6D 00 65 00 00 00
C·e·n·t·r·a·l· ·S·t·a·n·d·a·r·d· ·T
·i·m·e··

Recover lost folders:

Figure 8:

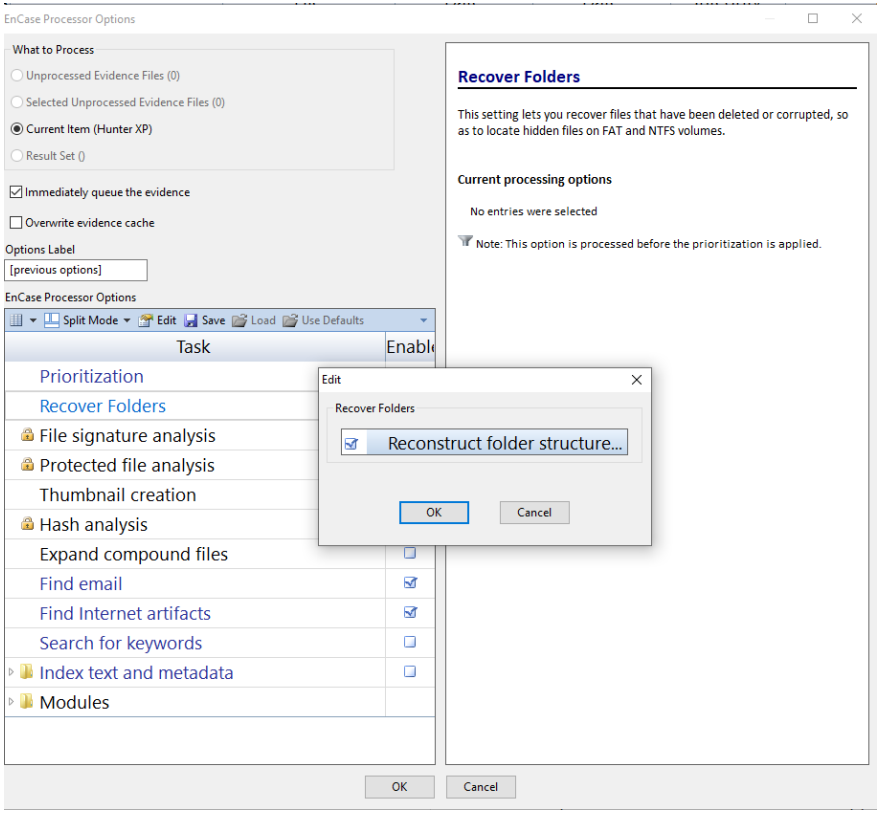
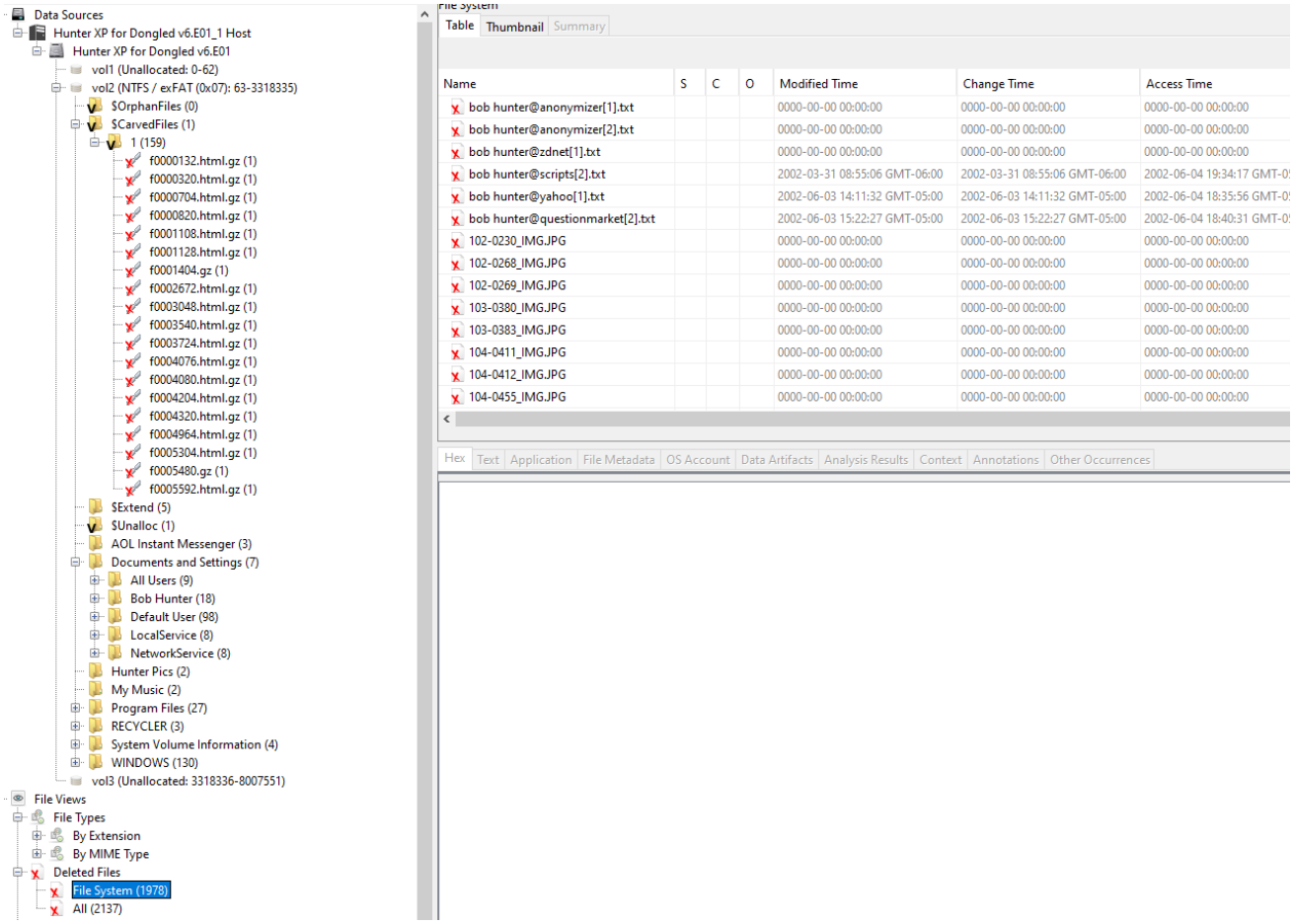
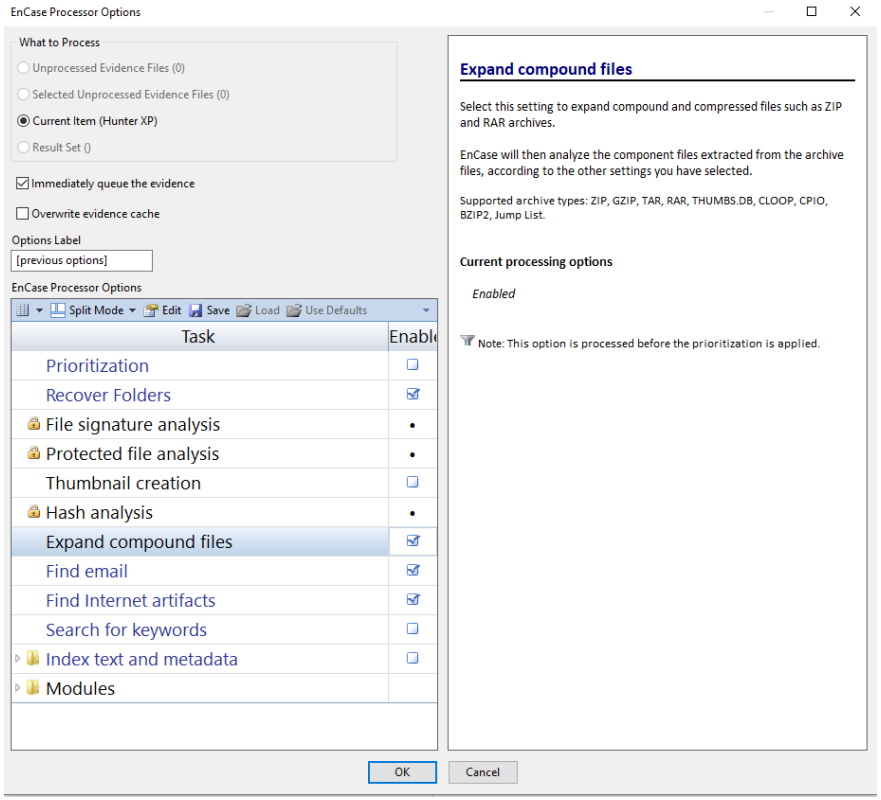


Figure 9:


Data Sources
Hunter XP for Dongled v6.E01_1 Host
Hunter XP for Dongled v6.E01
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 63-3318335)
$OrphanFiles (0)
$CarvedFiles (1)
1 (159)
f0000132.html.gz (1)
f0000320.html.gz (1)
f0000704.html.gz (1)
f0000820.html.gz (1)
f0001108.html.gz (1)
f0001128.html.gz (1)
f0001404.gz (1)
f0002672.html.gz (1)
f0003048.html.gz (1)
f0003540.html.gz (1)
f0003724.html.gz (1)
f0004076.html.gz (1)
f0004080.html.gz (1)
f0004204.html.gz (1)
f0004320.html.gz (1)
f0004964.html.gz (1)
f0005304.html.gz (1)
f0005480.gz (1)
f0005592.html.gz (1)
$Extend (5)
$Unalloc (1)
AOL Instant Messenger (3)
Documents and Settings (7)
All Users (9)
Bob Hunter (18)
Default User (98)
LocalService (8)
NetworkService (8)
Hunter Pics (2)
My Music (2)
Program Files (27)
RECYCLER (3)
System Volume Information (4)
WINDOWS (130)
vol3 (Unallocated: 3318336-8007551)
File Views
File Types
By Extension
By MIME Type
Deleted Files
File System (1978)
All (2137)
Table
Thumbnail
Summary
Name
S
C
O
Modified Time
Change Time
Access Time
bob hunter@anonymizer[1].txt
bob hunter@anonymizer[2].txt
bob hunter@zdnet[1].txt
bob hunter@scripts[2].txt
bob hunter@yahoo[1].txt
bob hunter@questionmarket[2].txt
102-0230_IMG.JPG
102-0268_IMG.JPG
102-0269_IMG.JPG
103-0380_IMG.JPG
103-0383_IMG.JPG
104-0411_IMG.JPG
104-0412_IMG.JPG
104-0455_IMG.JPG
0000-00-00 00:00:00
2002-03-31 08:55:06 GMT-06:00
2002-06-03 14:11:32 GMT-05:00
2002-06-03 15:22:27 GMT-05:00
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences

Mount Archives:

Figure 10:



File Signature Analysis:

Figure 11:

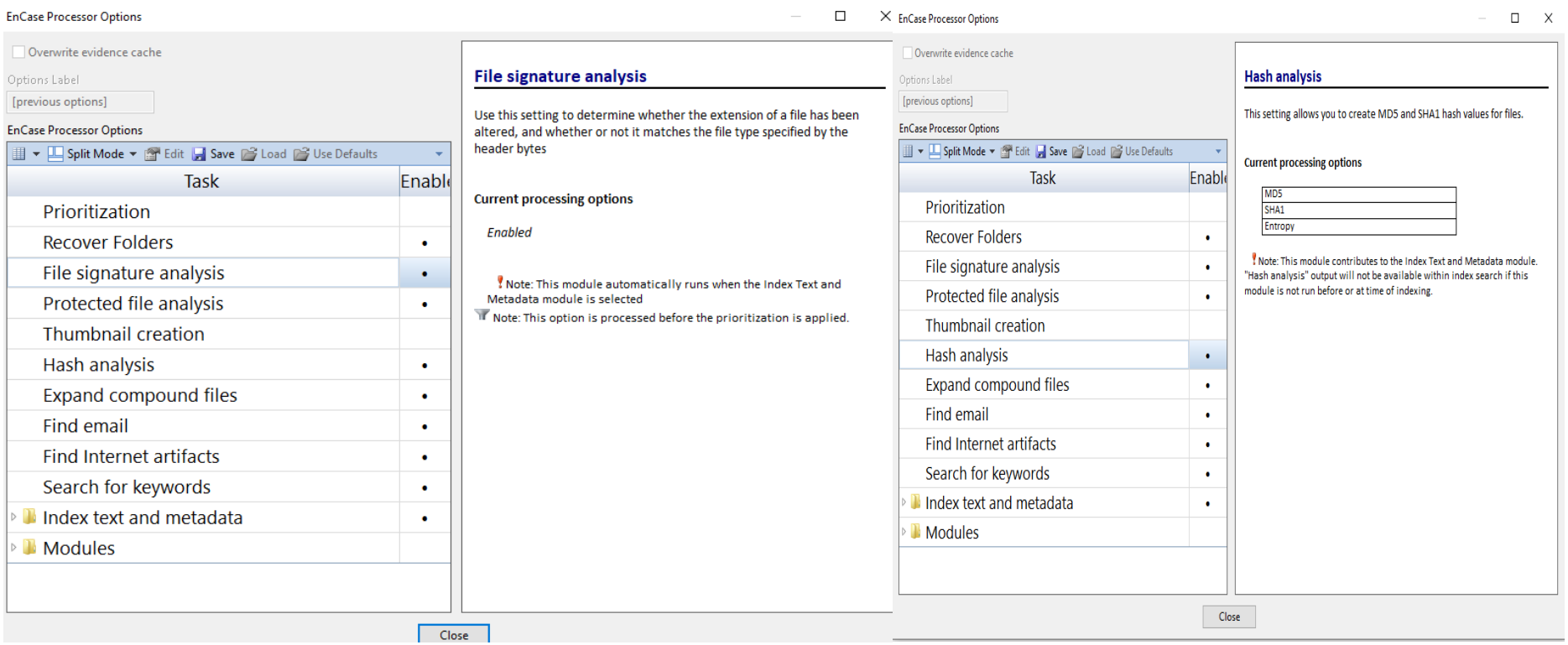
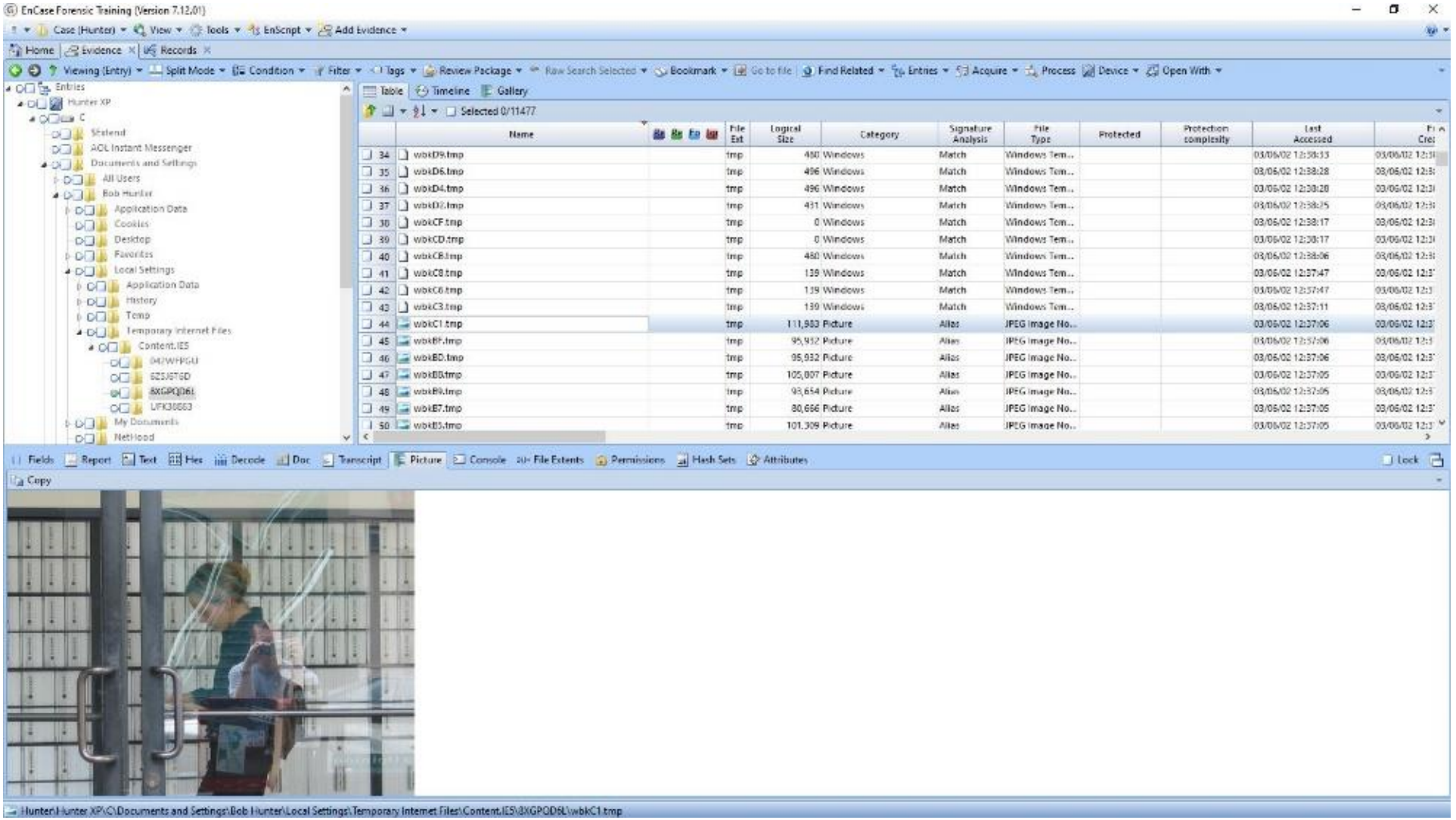


Figure 12:


EnCase Forensic Training (Version 7.12.01)
Case (Hunter)
View
Tools
EnScript
Add Evidence
Home
Evidence
Records
Viewing (Entry)
Split Mode
Condition
Filter
Tags
Review Package
Raw Search Selected
Bookmark
Go to File
Find Related
Entries
Acquire
Process
Device
Open With
Entries
Hunter XP
C
$Extend
AOL Instant Messenger
Documents and Settings
All Users
Bob Hunter
Application Data
Cookies
Desktop
Favorites
Local Settings
Application Data
History
Temp
Temporary Internet Files
Content.IE5
My Documents
NetHood
Table
Timeline
Gallery
Selected 0/11477
Name
File Ext
Logical Size
Category
Signature Analysis
File Type
Protected
Protection complexity
Last Accessed
wbkD9.tmp tmp 480 Windows Match Windows Tem...
wbkD6.tmp tmp 496 Windows Match Windows Tem...
wbkD4.tmp tmp 496 Windows Match Windows Tem...
wbkD2.tmp tmp 491 Windows Match Windows Tem...
wbkCF.tmp tmp 0 Windows Match Windows Tem...
wbkCD.tmp tmp 0 Windows Match Windows Tem...
wbkCB.tmp tmp 480 Windows Match Windows Tem...
wbkC8.tmp tmp 139 Windows Match Windows Tem...
wbkC6.tmp tmp 139 Windows Match Windows Tem...
wbkC3.tmp tmp 139 Windows Match Windows Tem...
wbkC1.tmp tmp 111,983 Picture Alias JPEG Image No...
wbkBF.tmp tmp 95,932 Picture Alias JPEG Image No...
wbkBD.tmp tmp 95,932 Picture Alias JPEG Image No...
wbkBB.tmp tmp 105,007 Picture Alias JPEG Image No...
wbkB9.tmp tmp 93,654 Picture Alias JPEG Image No...
wbkB7.tmp tmp 80,686 Picture Alias JPEG Image No...
wbkB5.tmp tmp 101,309 Picture Alias JPEG Image No...
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Console
File Extents
Permissions
Hash Sets
Attributes
Lock
Copy
Hunter\Hunter XP\C\Documents and Settings\Bob Hunter\Local Settings\Temporary Internet Files\Content.IE5\8XGPQD6L\wbkC1.tmp

Internet History, favourites, etc.
Other browsers:

Figure 13:

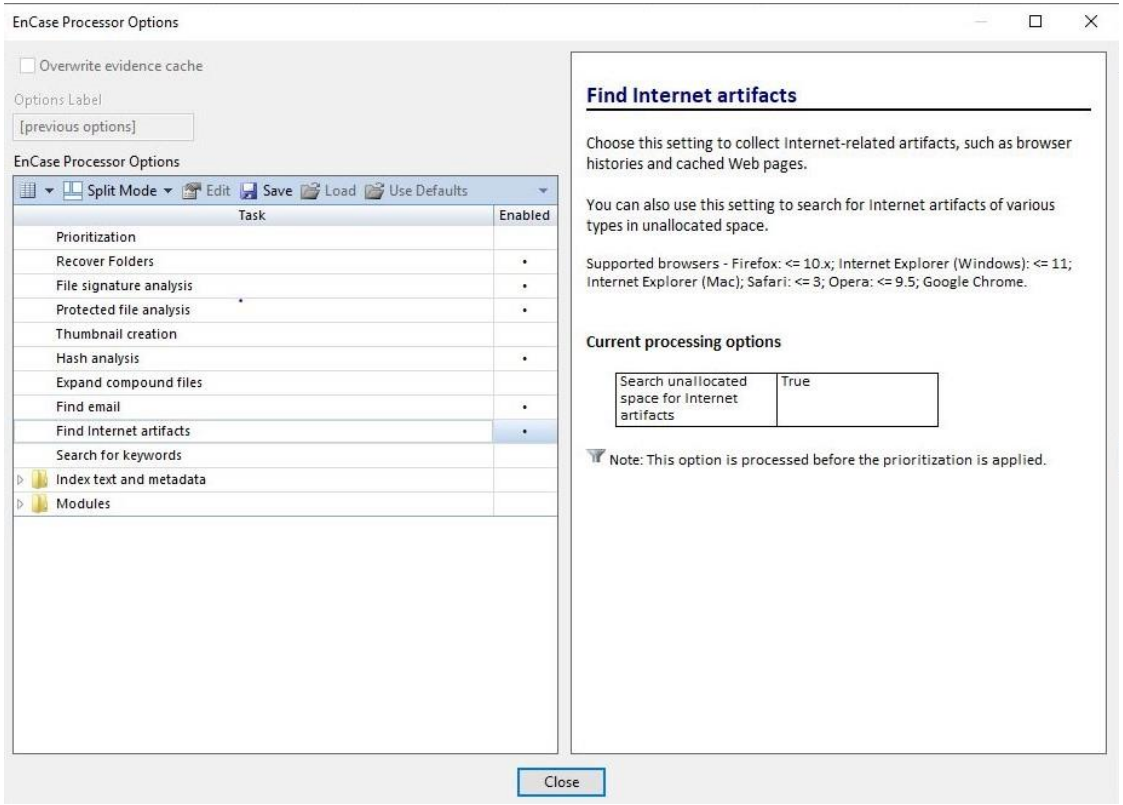
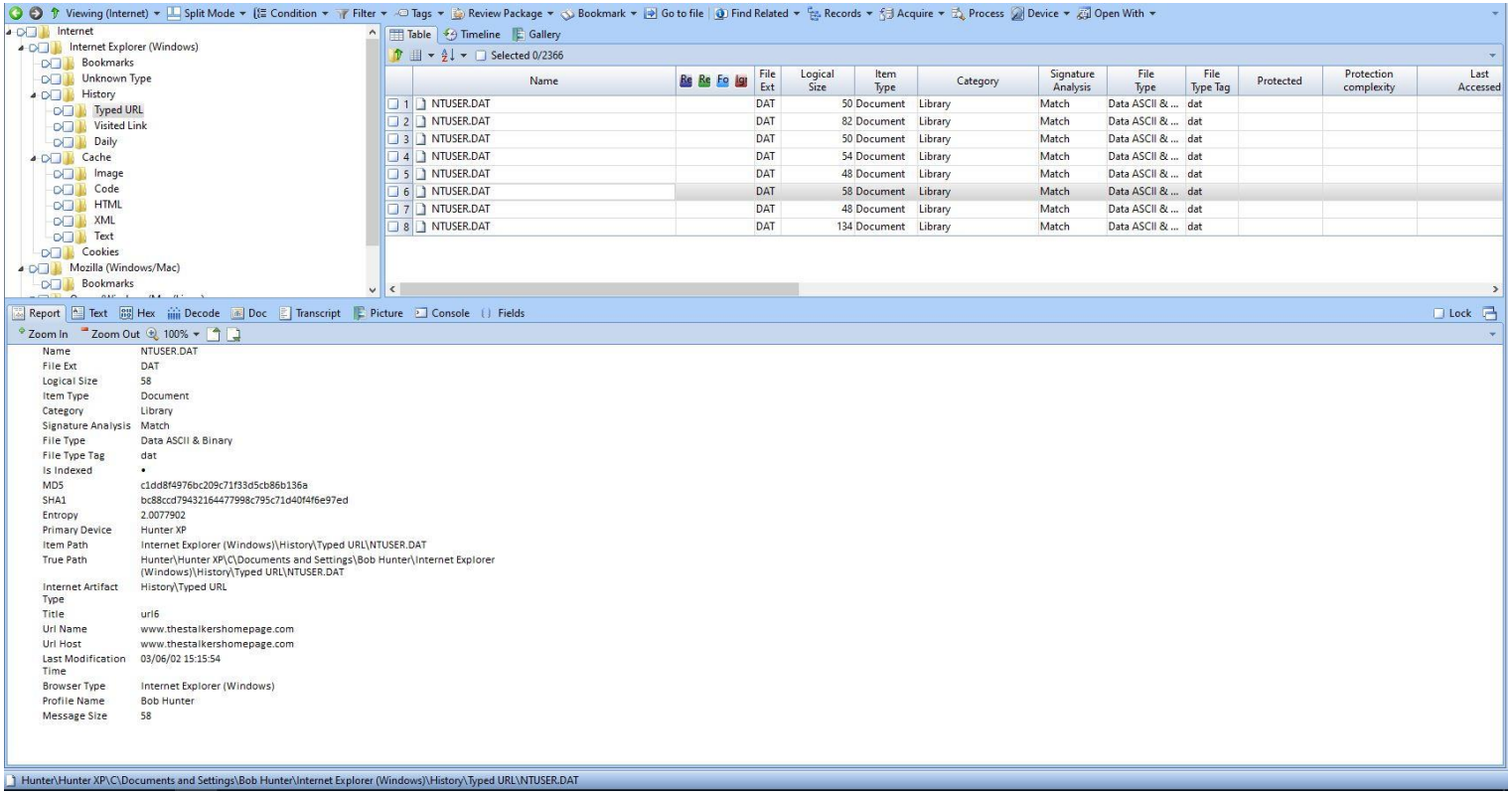


Figure 14:


Viewing (Internet)
Split Mode
Condition
Filter
Tags
Review Package
Bookmark
Go to file
Find Related
Records
Acquire
Process
Device
Open With
Internet
Internet Explorer (Windows)
Bookmarks
Unknown Type
History
Typed URL
Visited Link
Daily
Cache
Image
Code
HTML
XML
Text
Cookies
Mozilla (Windows/Mac)
Bookmarks
Table
Timeline
Gallery
Selected 0/2366
Name
File Ext
Logical Size
Item Type
Category
Signature Analysis
File Type
File Type Tag
Protected
Protection complexity
Last Accessed
1 NTUSER.DAT DAT 50 Document Library Match Data ASCII & ... dat
2 NTUSER.DAT DAT 82 Document Library Match Data ASCII & ... dat
3 NTUSER.DAT DAT 50 Document Library Match Data ASCII & ... dat
4 NTUSER.DAT DAT 54 Document Library Match Data ASCII & ... dat
5 NTUSER.DAT DAT 48 Document Library Match Data ASCII & ... dat
6 NTUSER.DAT DAT 58 Document Library Match Data ASCII & ... dat
7 NTUSER.DAT DAT 48 Document Library Match Data ASCII & ... dat
8 NTUSER.DAT DAT 134 Document Library Match Data ASCII & ... dat
Report
Text
Hex
Decode
Doc
Transcript
Picture
Console
Fields
Lock
Zoom In
Zoom Out
100%
Name NTUSER.DAT
File Ext DAT
Logical Size 58
Item Type Document
Category Library
Signature Analysis Match
File Type Data ASCII & Binary
File Type Tag dat
Is Indexed •
MD5 c1dd8f4976bc209c71f33d5cb86b136a
SHA1 bc88ccd79432164477998c795c71d40f4f6e97ed
Entropy 2.0077902
Primary Device Hunter XP
Item Path Internet Explorer (Windows)\History\Typed URL\NTUSER.DAT
True Path Hunter\Hunter XP\C\Documents and Settings\Bob Hunter\Internet Explorer (Windows)\History\Typed URL\NTUSER.DAT
Internet Artifact Type History\Typed URL
Title url6
Url Name www.thestalkershomepage.com
Url Host www.thestalkershomepage.com
Last Modification Time 03/06/02 15:15:54
Browser Type Internet Explorer (Windows)
Profile Name Bob Hunter
Message Size 58
Hunter\Hunter XP\C\Documents and Settings\Bob Hunter\Internet Explorer (Windows)\History\Typed URL\NTUSER.DAT

Emails, local and web-based:

Figure 15:

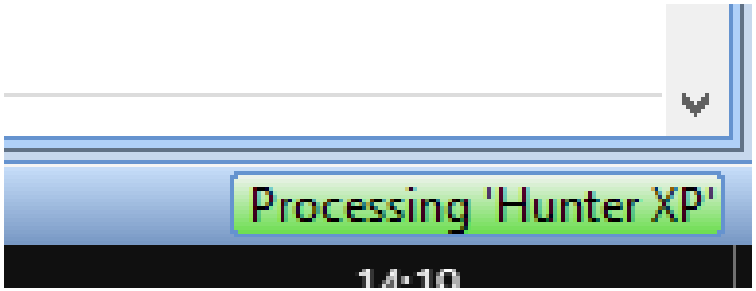


Figure 16:

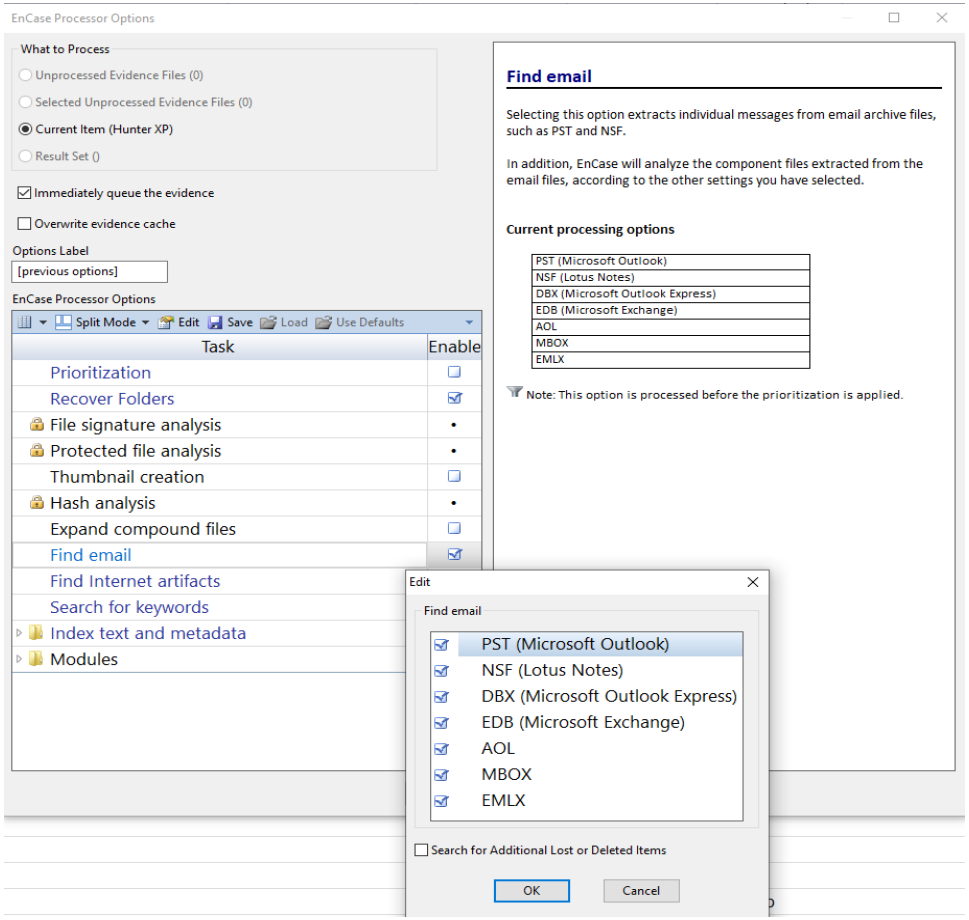

EnCase Processor Options
What to Process
Unprocessed Evidence Files (0)
Selected Unprocessed Evidence Files (0)
Current Item (Hunter XP)
Result Set ()
Immediately queue the evidence
Overwrite evidence cache
Options Label
[previous options]
EnCase Processor Options
Split Mode
Edit
Save
Load
Use Defaults
Task
Enable
Prioritization
Recover Folders
File signature analysis
Protected file analysis
Thumbnail creation
Hash analysis
Expand compound files
Find email
Find Internet artifacts
Search for keywords
Index text and metadata
Modules
Find email
Selecting this option extracts individual messages from email archive files, such as PST and NSF.
In addition, EnCase will analyze the component files extracted from the email files, according to the other settings you have selected.
Current processing options
PST (Microsoft Outlook)
NSF (Lotus Notes)
DBX (Microsoft Outlook Express)
EDB (Microsoft Exchange)
AOL
MBOX
EMLX
Note: This option is processed before the prioritization is applied.
Edit
Find email
PST (Microsoft Outlook)
NSF (Lotus Notes)
DBX (Microsoft Outlook Express)
EDB (Microsoft Exchange)
AOL
MBOX
EMLX
Search for Additional Lost or Deleted Items
OK
Cancel

Figure 17:

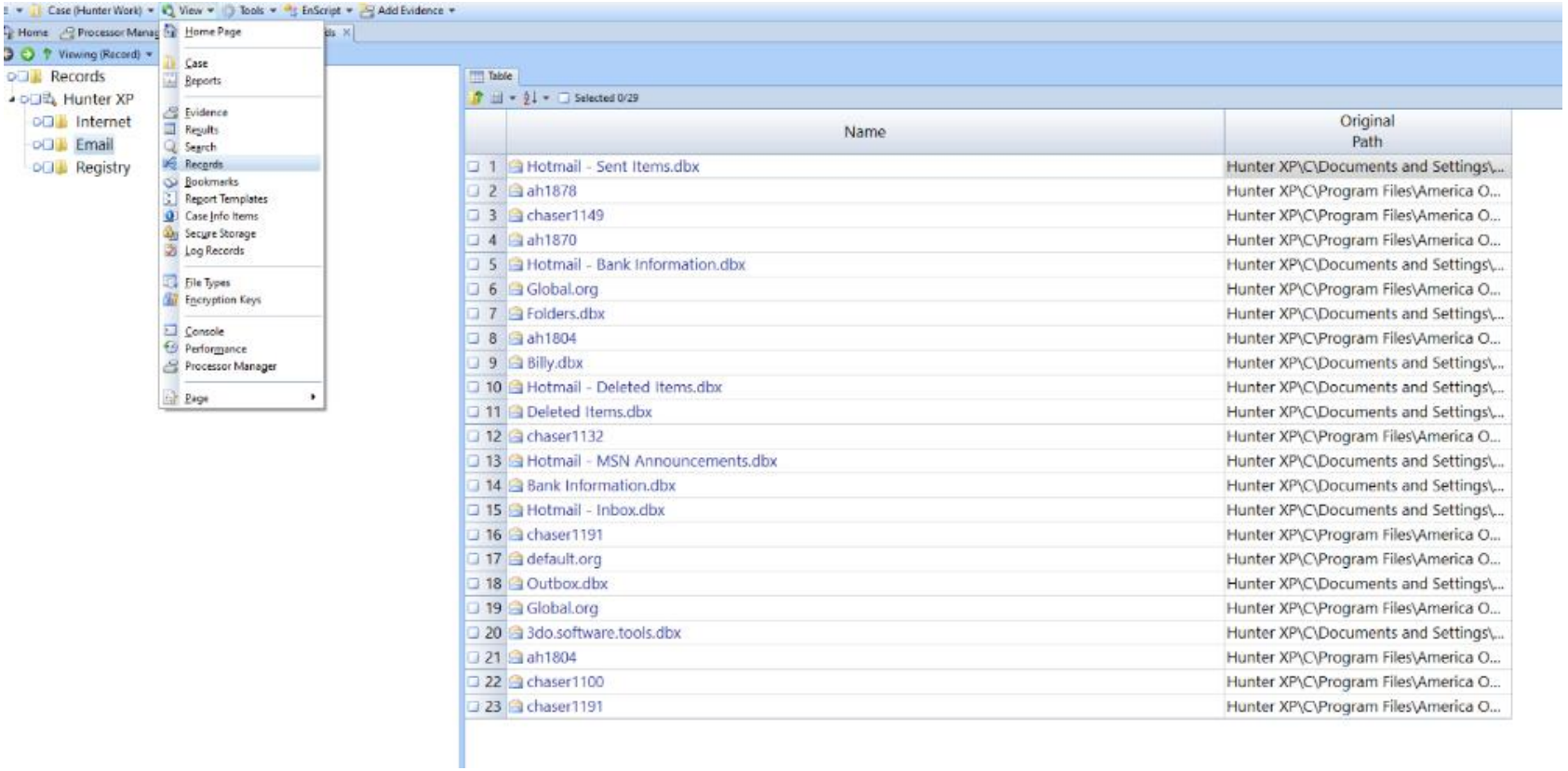

Case (Hunter Work)
View
Tools
EnScript
Add Evidence
Home
Processor Manag
Viewing (Record)
Records
Hunter XP
Internet
Email
Registry
Home Page
Case
Reports
Evidence
Results
Search
Records
Bookmarks
Report Templates
Case Info Items
Secure Storage
Log Records
File Types
Encryption Keys
Console
Performance
Processor Manager
Page
Table
Selected 0/29
Name
Original Path
1 Hotmail - Sent Items.dbx Hunter XP\C\Documents and Settings\...
2 ah1878 Hunter XP\C\Program Files\America O...
3 chaser1149 Hunter XP\C\Program Files\America O...
4 ah1870 Hunter XP\C\Program Files\America O...
5 Hotmail - Bank Information.dbx Hunter XP\C\Documents and Settings\...
6 Global.org Hunter XP\C\Program Files\America O...
7 Folders.dbx Hunter XP\C\Documents and Settings\...
8 ah1804 Hunter XP\C\Program Files\America O...
9 Billy.dbx Hunter XP\C\Documents and Settings\...
10 Hotmail - Deleted Items.dbx Hunter XP\C\Documents and Settings\...
11 Deleted Items.dbx Hunter XP\C\Documents and Settings\...
12 chaser1132 Hunter XP\C\Program Files\America O...
13 Hotmail - MSN Announcements.dbx Hunter XP\C\Documents and Settings\...
14 Bank Information.dbx Hunter XP\C\Documents and Settings\...
15 Hotmail - Inbox.dbx Hunter XP\C\Documents and Settings\...
16 chaser1191 Hunter XP\C\Program Files\America O...
17 default.org Hunter XP\C\Program Files\America O...
18 Outbox.dbx Hunter XP\C\Documents and Settings\...
19 Global.org Hunter XP\C\Program Files\America O...
20 3do.software.tools.dbx Hunter XP\C\Documents and Settings\...
21 ah1804 Hunter XP\C\Program Files\America O...
22 chaser1100 Hunter XP\C\Program Files\America O...
23 chaser1191 Hunter XP\C\Program Files\America O...

Figure 17.1:

From Billy Ray <billyray150@hotmail.com>
To chaser1191@hotmail.com
Sent 22/05/02 09:01:21
Subject Web Site

Bob here are some of the pics from the web page we are doing. I will be posting it later today, then we can send the letter to the ole man. if all goes well we will be rich men this summer.

I could not send all of the photos because of this hotmail limit, but we can hook up later by phone or IM or yahoo or something and I will show you the page.

Billy

Name 101-0192_IMG.JPG
Logical Size 99,921
101-0192_IMG.JPG

Name 101-0195_IMG.JPG
Logical Size 102,586
101-0195_IMG.JPG

Name 102-0206_IMG.JPG
Logical Size 101,309

Name 102-0212_IMG.JPG
Logical Size 80,666
102-0212_IMG.JPG

Name 102-0226_IMG.JPG
Logical Size 93,654
102-0226_IMG.JPG

Name 102-0244_IMG.JPG
Logical Size 105,807
102-0244_IMG.JPG

Name 102-0271_IMG.JPG
Logical Size 95,932
102-0271_IMG.JPG

Name 102-0271_IMG.JPG
Logical Size 95,932
102-0271_IMG.JPG

Name 102-0283_IMG.JPG
Logical Size 111,983
102-0283_IMG.JPG

From Billy Ray <billyray150@hotmail.com>
To chaser1191@hotmail.com
Sent 30/05/02 19:11:11
Subject Re: Web Page on Christina

yes I saw that too I will fix it, hold off on the email I tested his address its not working

>From: "IC YOU" <chaser1191@hotmail.com>
>To: billyray150@hotmail.com
>Subject: Web Page on Christina
>Date: Thu, 23 May 2002 08:48:19 -0500
>
>Billy,
>
>Page looks good, the old man should pay up. on one of the photos though you are in the reflection of the window, what where you thinking. Get that off of there, I will email dad today after you fix it.
>
>Bob
>

Retrieve operating system information, accounts information, software, time zone information etc :

Figure 18:

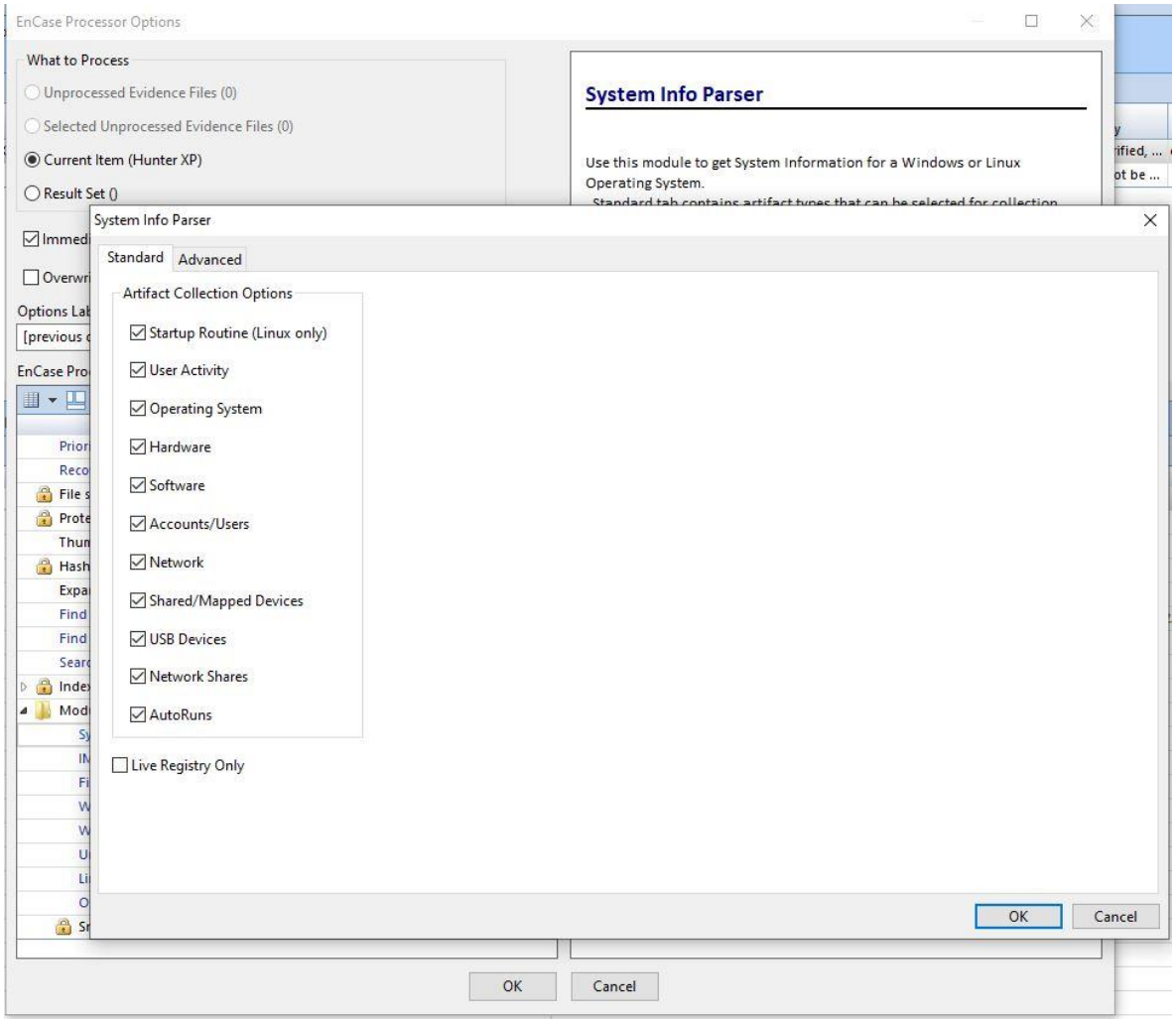


Figure 19:

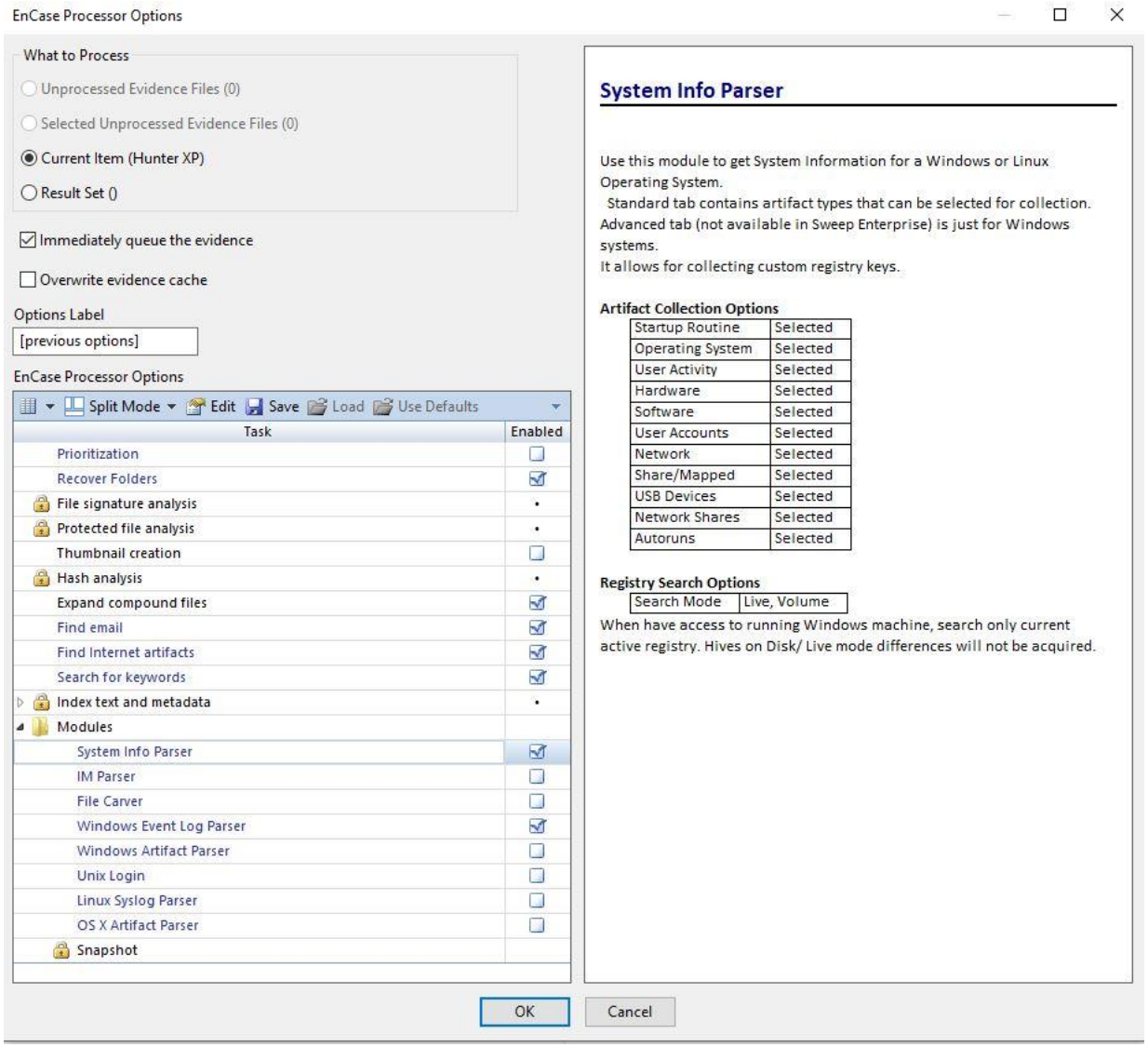

EnCase Processor Options
What to Process
Unprocessed Evidence Files (0)
Selected Unprocessed Evidence Files (0)
Current Item (Hunter XP)
Result Set ()
Immediately queue the evidence
Overwrite evidence cache
Options Label
[previous options]
EnCase Processor Options
Split Mode
Edit
Save
Load
Use Defaults
Task
Enabled
Prioritization
Recover Folders
File signature analysis
Protected file analysis
Thumbnail creation
Hash analysis
Expand compound files
Find email
Find Internet artifacts
Search for keywords
Index text and metadata
Modules
System Info Parser
IM Parser
File Carver
Windows Event Log Parser
Windows Artifact Parser
Unix Login
Linux Syslog Parser
OS X Artifact Parser
Snapshot
System Info Parser
Use this module to get System Information for a Windows or Linux Operating System.
Standard tab contains artifact types that can be selected for collection.
Advanced tab (not available in Sweep Enterprise) is just for Windows systems.
It allows for collecting custom registry keys.
Artifact Collection Options
Startup Routine Selected
Operating System Selected
User Activity Selected
Hardware Selected
Software Selected
User Accounts Selected
Network Selected
Share/Mapped Selected
USB Devices Selected
Network Shares Selected
Autoruns Selected
Registry Search Options
Search Mode Live, Volume
When have access to running Windows machine, search only current active registry. Hives on Disk/ Live mode differences will not be acquired.
OK
Cancel

Figure 20:

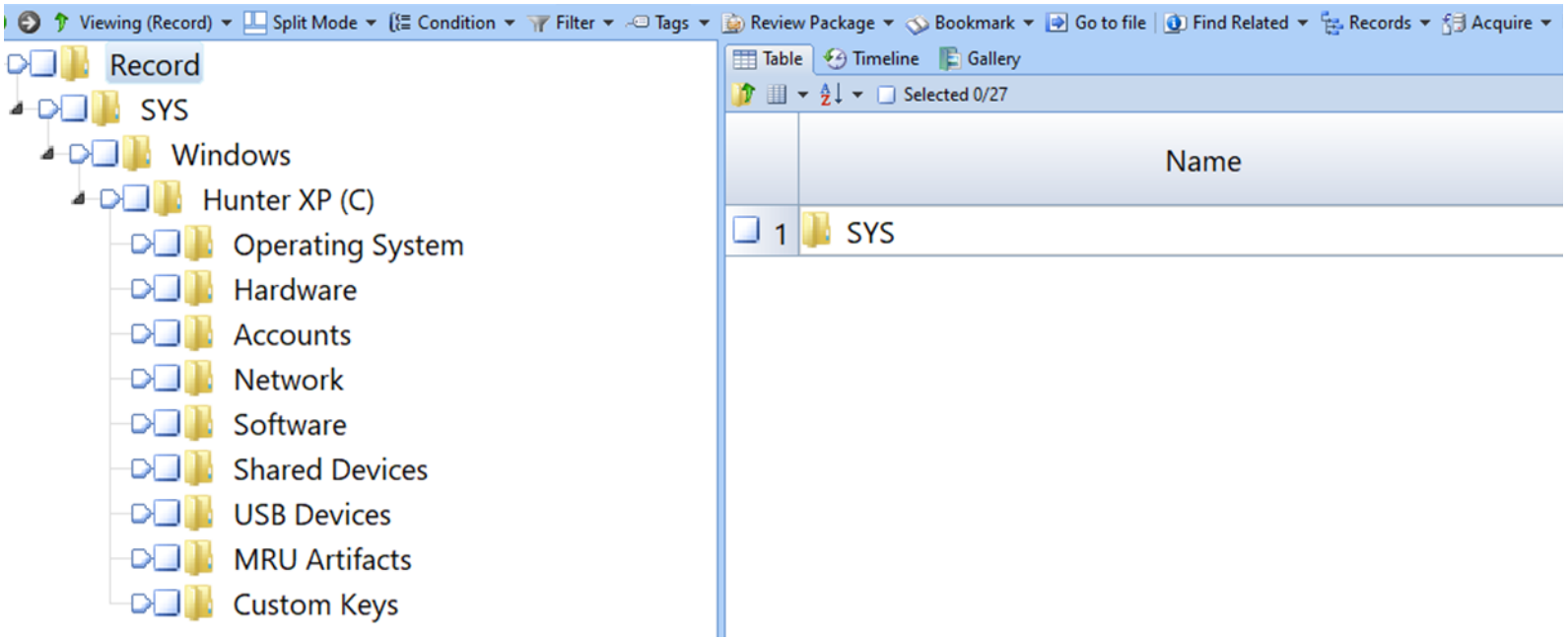
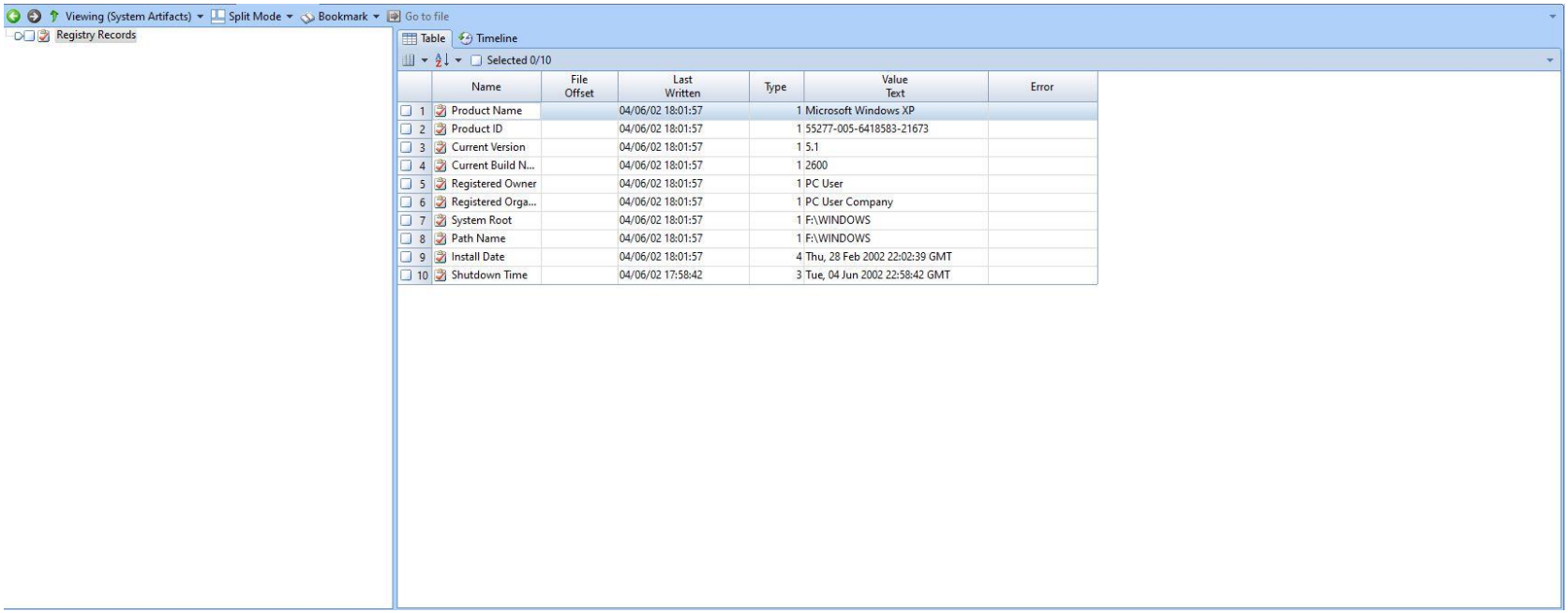
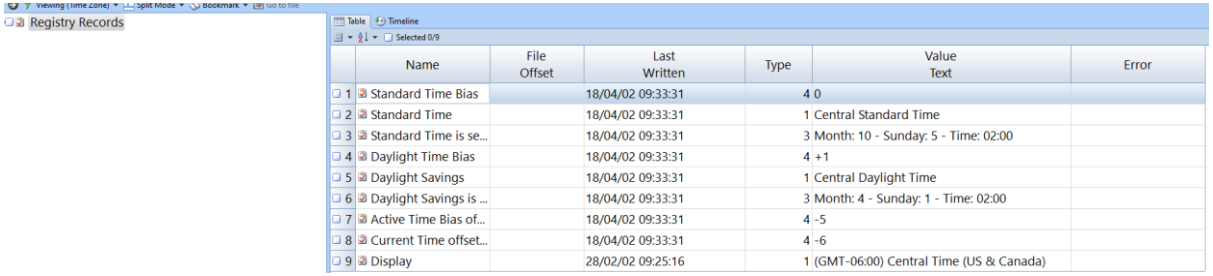

Viewing (Record)
Split Mode
Condition
Filter
Tags
Review Package
Bookmark
Go to file
Find Related
Records
Acquire
Record
SYS
Windows
Hunter XP (C)
Operating System
Hardware
Accounts
Network
Software
Shared Devices
USB Devices
MRU Artifacts
Custom Keys
Table
Timeline
Gallery
Selected 0/27
Name
1
SYS

Figure 21:



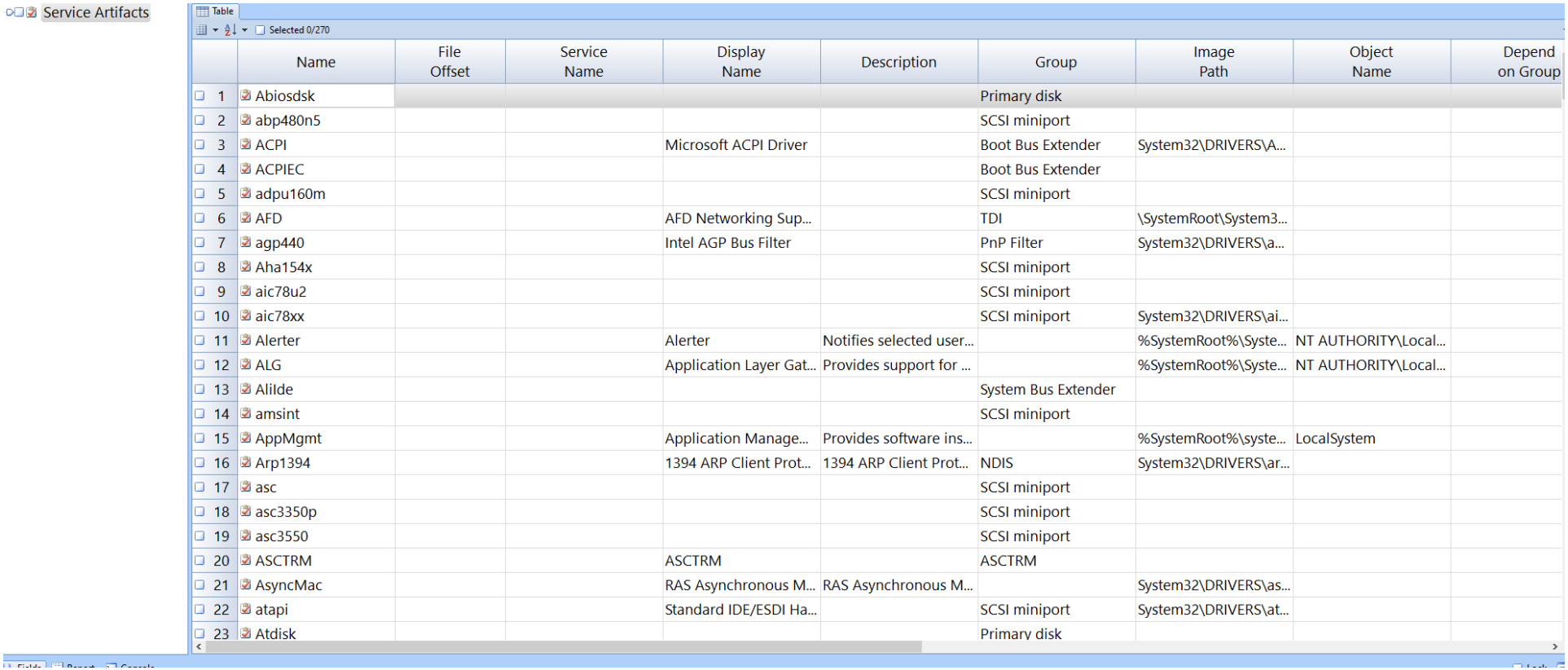
	Name	File Offset	Last Written	Type	Value Text	Error
1	Product Name		04/06/02 18:01:57	1	Microsoft Windows XP	
2	Product ID		04/06/02 18:01:57	1	55277-005-6418583-21673	
3	Current Version		04/06/02 18:01:57	1	5.1	
4	Current Build N...		04/06/02 18:01:57	1	2600	
5	Registered Owner		04/06/02 18:01:57	1	PC User	
6	Registered Orga...		04/06/02 18:01:57	1	PC User Company	
7	System Root		04/06/02 18:01:57	1	F:\WINDOWS	
8	Path Name		04/06/02 18:01:57	1	F:\WINDOWS	
9	Install Date		04/06/02 18:01:57	4	Thu, 28 Feb 2002 22:02:39 GMT	
10	Shutdown Time		04/06/02 17:58:42	3	Tue, 04 Jun 2002 22:58:42 GMT	

Figure 22:



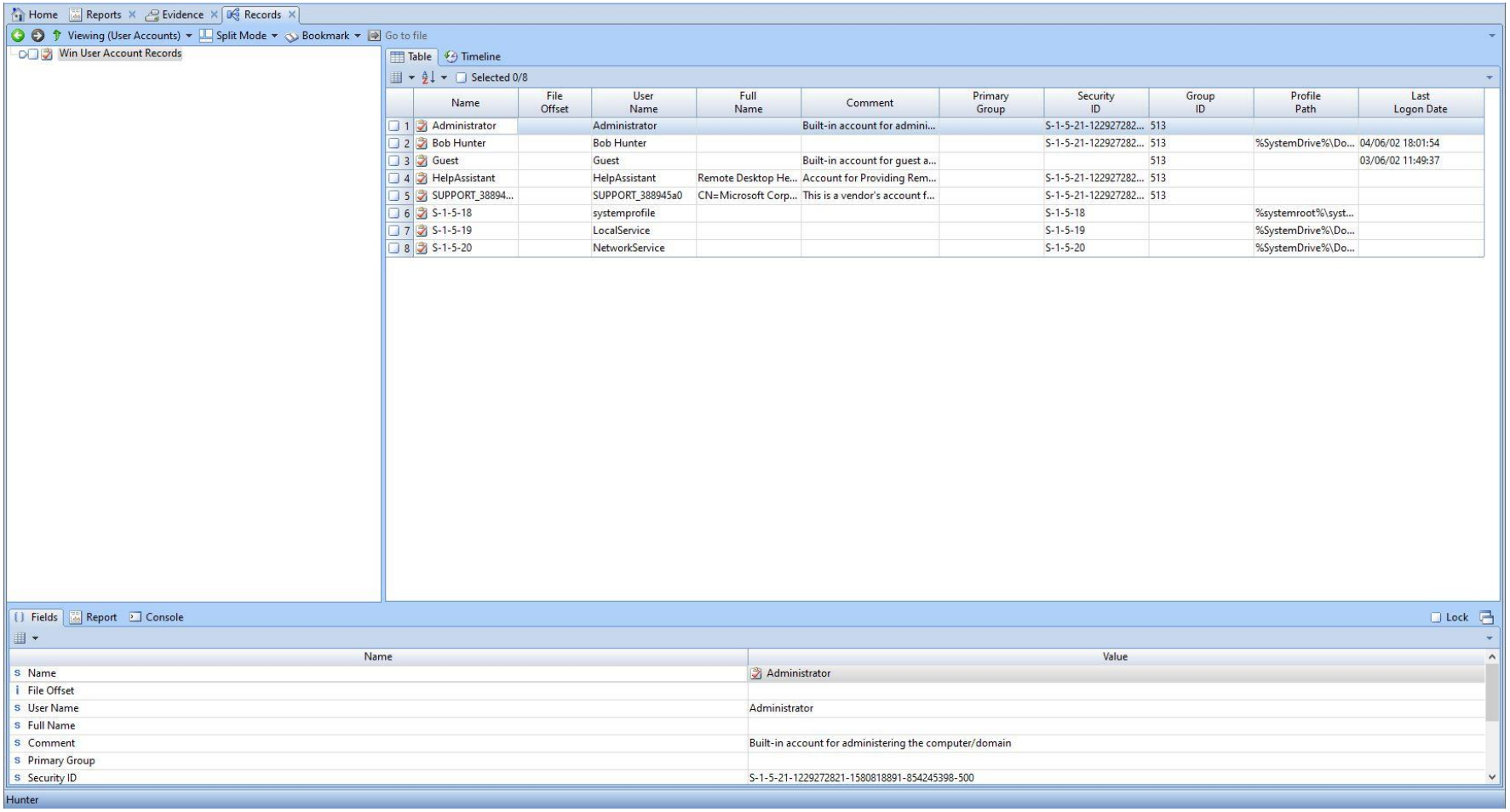
	Name	File Offset	Last Written	Type	Value Text	Error
1	Standard Time Bias		18/04/02 09:33:31	4	0	
2	Standard Time		18/04/02 09:33:31	1	Central Standard Time	
3	Standard Time is se...		18/04/02 09:33:31	3	Month: 10 - Sunday: 5 - Time: 02:00	
4	Daylight Time Bias		18/04/02 09:33:31	4	+1	
5	Daylight Savings		18/04/02 09:33:31	1	Central Daylight Time	
6	Daylight Savings is ...		18/04/02 09:33:31	3	Month: 4 - Sunday: 1 - Time: 02:00	
7	Active Time Bias of...		18/04/02 09:33:31	4	-5	
8	Current Time offset...		18/04/02 09:33:31	4	-6	
9	Display		28/02/02 09:25:16	1	(GMT-06:00) Central Time (US & Canada)	

Figure 23:



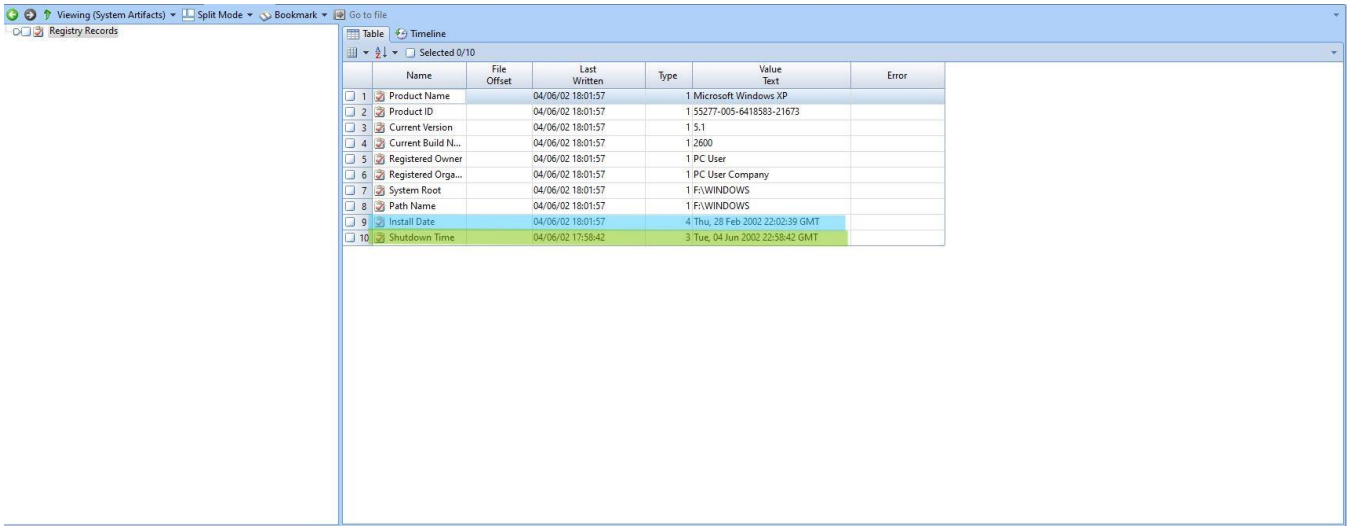
	Name	File Offset	Service Name	Display Name	Description	Group	Image Path	Object Name	Depend on Group
1	Abiosdsk					Primary disk			
2	abp480n5					SCSI miniport			
3	ACPI			Microsoft ACPI Driver		Boot Bus Extender	System32\DRIVERS\A...		
4	ACPIEC					Boot Bus Extender			
5	adpu160m					SCSI miniport			
6	AFD			AFD Networking Sup...		TDI	\SystemRoot\System3...		
7	agp440			Intel AGP Bus Filter		PnP Filter	System32\DRIVERS\a...		
8	Aha154x					SCSI miniport			
9	aic78u2					SCSI miniport			
10	aic78xx					SCSI miniport	System32\DRIVERS\ai...		
11	Alerter			Alerter	Notifies selected user...		%SystemRoot%\Syste...	NT AUTHORITY\Local...	
12	ALG			Application Layer Gat...	Provides support for ...		%SystemRoot%\Syste...	NT AUTHORITY\Local...	
13	AliIde					System Bus Extender			
14	amsint					SCSI miniport			
15	AppMgmt			Application Manage...	Provides software ins...		%SystemRoot%\syste...	LocalSystem	
16	Arp1394			1394 ARP Client Prot...	1394 ARP Client Prot...	NDIS	System32\DRIVERS\ar...		
17	asc					SCSI miniport			
18	asc3350p					SCSI miniport			
19	asc3550					SCSI miniport			
20	ASCTRM			ASCTRM		ASCTRM			
21	AsyncMac			RAS Asynchronous M...	RAS Asynchronous M...		System32\DRIVERS\as...		
22	atapi			Standard IDE/ESDI Ha...		SCSI miniport	System32\DRIVERS\at...		
23	Atdisk					Primary disk			

Figure 24:


Home
Reports
Evidence
Records
Viewing (User Accounts)
Split Mode
Bookmark
Go to file
Win User Account Records
Table
Timeline
Selected 0/8
Name
File Offset
User Name
Full Name
Comment
Primary Group
Security ID
Group ID
Profile Path
Last Logon Date
1 Administrator Administrator Built-in account for admini... S-1-5-21-122927282... 513
2 Bob Hunter Bob Hunter S-1-5-21-122927282... 513 %SystemDrive%\Do... 04/06/02 18:01:54
3 Guest Guest Built-in account for guest a... 513 03/06/02 11:49:37
4 HelpAssistant HelpAssistant Remote Desktop He... Account for Providing Rem... S-1-5-21-122927282... 513
5 SUPPORT_38894... SUPPORT_388945a0 CN=Microsoft Corp... This is a vendor's account f... S-1-5-21-122927282... 513
6 S-1-5-18 systemprofile S-1-5-18 %systemroot%\syst...
7 S-1-5-19 LocalService S-1-5-19 %SystemDrive%\Do...
8 S-1-5-20 NetworkService S-1-5-20 %SystemDrive%\Do...
Fields
Report
Console
Lock
Name
Value
Name Administrator
File Offset
User Name Administrator
Full Name
Comment Built-in account for administering the computer/domain
Primary Group
Security ID S-1-5-21-1229272821-1580818891-854245398-500
Hunter

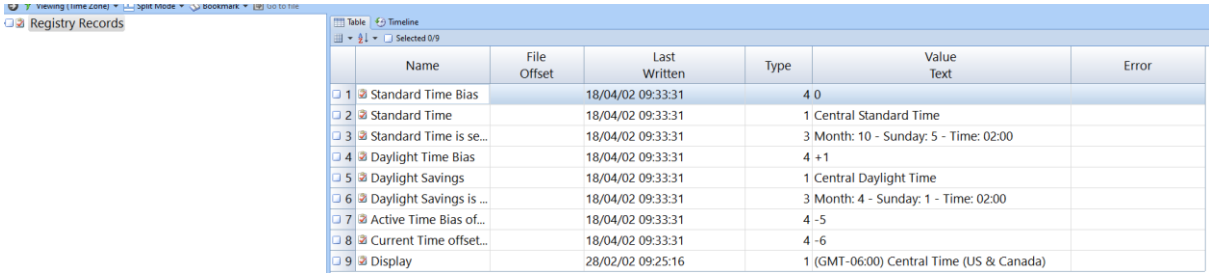
Timeline Analysis:

Figure 25:



	Name	File Offset	Last Written	Type	Value Text	Error
1	Product Name		04/06/02 18:01:57	1	Microsoft Windows XP	
2	Product ID		04/06/02 18:01:57	1	55277-005-6418583-21673	
3	Current Version		04/06/02 18:01:57	1	5.1	
4	Current Build N...		04/06/02 18:01:57	1	2600	
5	Registered Owner		04/06/02 18:01:57	1	PC User	
6	Registered Orga...		04/06/02 18:01:57	1	PC User Company	
7	System Root		04/06/02 18:01:57	1	F:\WINDOWS	
8	Path Name		04/06/02 18:01:57	1	F:\WINDOWS	
9	Install Date		04/06/02 18:01:57	4	Thu, 28 Feb 2002 22:02:39 GMT	
10	Shutdown Time		04/06/02 17:58:42	3	Tue, 04 Jun 2002 22:58:42 GMT	

Figure 26:



	Name	File Offset	Last Written	Type	Value Text	Error
1	Standard Time Bias		18/04/02 09:33:31	4	0	
2	Standard Time		18/04/02 09:33:31	1	Central Standard Time	
3	Standard Time is se...		18/04/02 09:33:31	3	Month: 10 - Sunday: 5 - Time: 02:00	
4	Daylight Time Bias		18/04/02 09:33:31	4	+1	
5	Daylight Savings		18/04/02 09:33:31	1	Central Daylight Time	
6	Daylight Savings is ...		18/04/02 09:33:31	3	Month: 4 - Sunday: 1 - Time: 02:00	
7	Active Time Bias of...		18/04/02 09:33:31	4	-5	
8	Current Time offset...		18/04/02 09:33:31	4	-6	
9	Display		28/02/02 09:25:16	1	(GMT-06:00) Central Time (US & Canada)	

Registry Analysis And Registry Protected Area :

Figure 27:

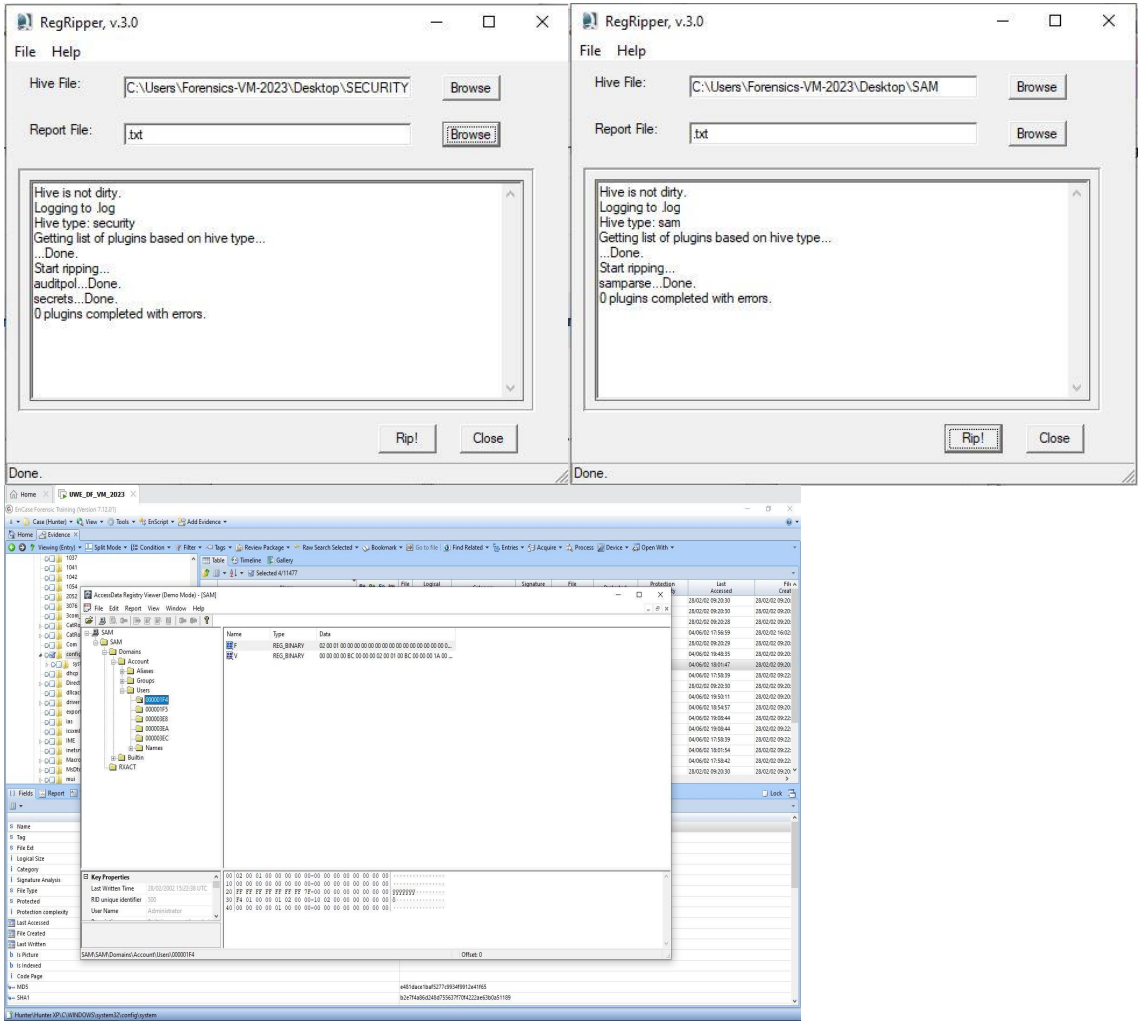
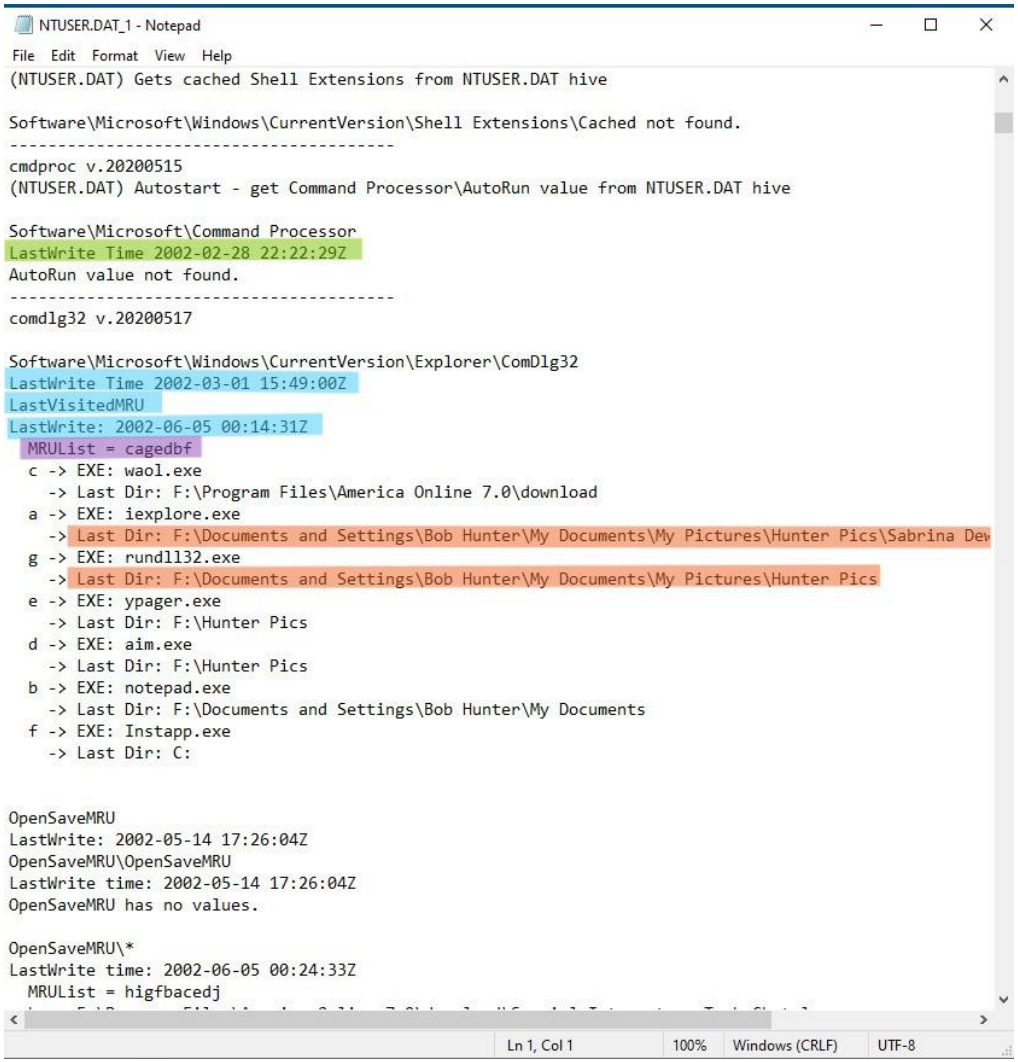


Figure 28:


NTUSER.DAT_1 - Notepad
File Edit Format View Help
(NTUSER.DAT) Gets cached Shell Extensions from NTUSER.DAT hive
Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached not found.
cmdproc v.20200515
(NTUSER.DAT) Autostart - get Command Processor\AutoRun value from NTUSER.DAT hive
Software\Microsoft\Command Processor
LastWrite Time 2002-02-28 22:22:29Z
AutoRun value not found.
comdlg32 v.20200517
Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
LastWrite Time 2002-03-01 15:49:00Z
LastVisitedMRU
LastWrite: 2002-06-05 00:14:31Z
MRUList = cagedbf
c -> EXE: waol.exe
-> Last Dir: F:\Program Files\America Online 7.0\download
a -> EXE: iexplore.exe
-> Last Dir: F:\Documents and Settings\Bob Hunter\My Documents\My Pictures\Hunter Pics\Sabrina Dev
g -> EXE: rundll32.exe
-> Last Dir: F:\Documents and Settings\Bob Hunter\My Documents\My Pictures\Hunter Pics
e -> EXE: ypager.exe
-> Last Dir: F:\Hunter Pics
d -> EXE: aim.exe
-> Last Dir: F:\Hunter Pics
b -> EXE: notepad.exe
-> Last Dir: F:\Documents and Settings\Bob Hunter\My Documents
f -> EXE: Instapp.exe
-> Last Dir: C:
OpenSaveMRU
LastWrite: 2002-05-14 17:26:04Z
OpenSaveMRU\OpenSaveMRU
LastWrite time: 2002-05-14 17:26:04Z
OpenSaveMRU has no values.
OpenSaveMRU*
LastWrite time: 2002-06-05 00:24:33Z
MRUList = higfbacedj
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8

Link files and Recycle Bin:

Figure 29:

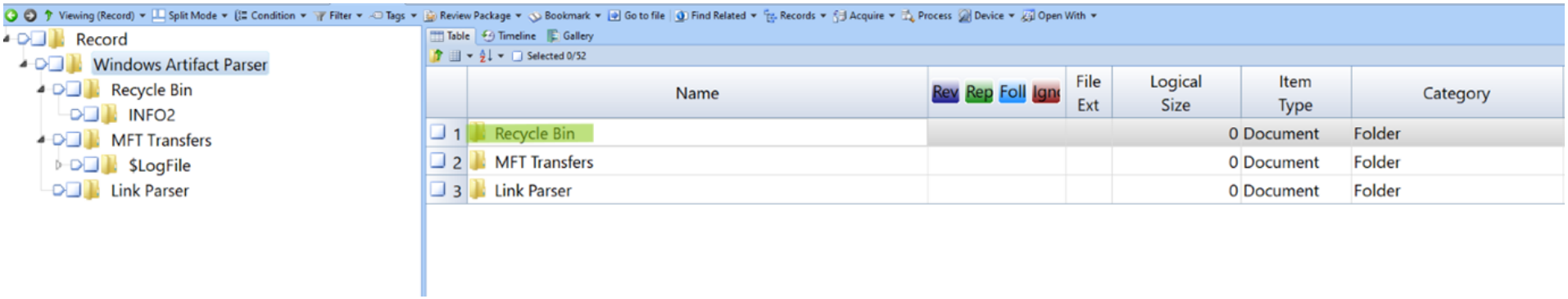
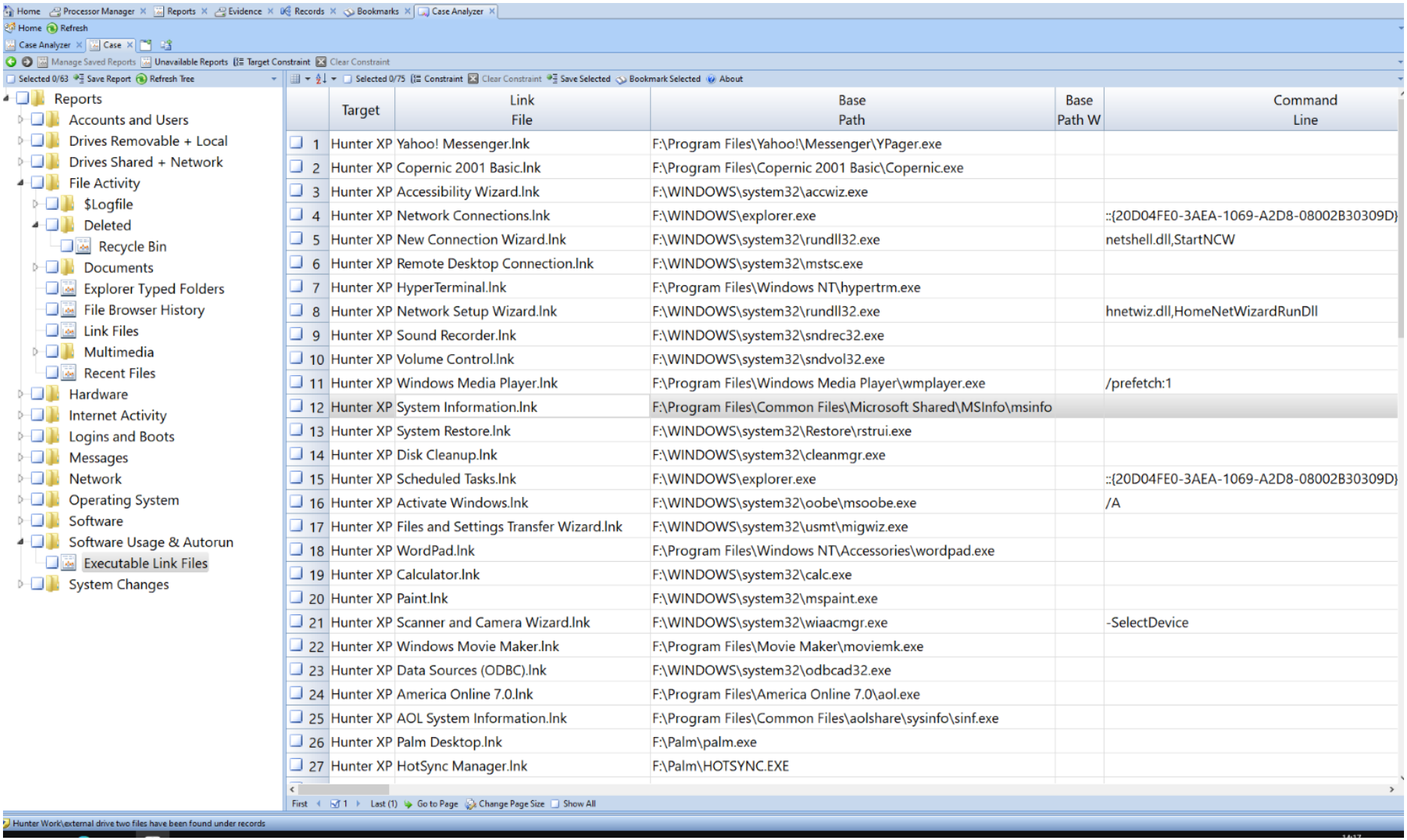


Figure 30:



	Target	Link File	Base Path	Base Path W	Command Line
1	Hunter XP	Yahoo! Messenger.lnk	F:\Program Files\Yahoo!\Messenger\YPager.exe		
2	Hunter XP	Copernic 2001 Basic.lnk	F:\Program Files\Copernic 2001 Basic\Copernic.exe		
3	Hunter XP	Accessibility Wizard.lnk	F:\WINDOWS\system32\accwiz.exe		
4	Hunter XP	Network Connections.lnk	F:\WINDOWS\explorer.exe		::{20D04FE0-3AEA-1069-A2D8-08002B30309D}
5	Hunter XP	New Connection Wizard.lnk	F:\WINDOWS\system32\rundll32.exe		netshell.dll,StartNCW
6	Hunter XP	Remote Desktop Connection.lnk	F:\WINDOWS\system32\mstsc.exe		
7	Hunter XP	HyperTerminal.lnk	F:\Program Files\Windows NT\hypertrm.exe		
8	Hunter XP	Network Setup Wizard.lnk	F:\WINDOWS\system32\rundll32.exe		hnetwiz.dll,HomeNetWizardRunDll
9	Hunter XP	Sound Recorder.lnk	F:\WINDOWS\system32\sndrec32.exe		
10	Hunter XP	Volume Control.lnk	F:\WINDOWS\system32\sndvol32.exe		
11	Hunter XP	Windows Media Player.lnk	F:\Program Files\Windows Media Player\wmplayer.exe		/prefetch:1
12	Hunter XP	System Information.lnk	F:\Program Files\Common Files\Microsoft Shared\MSInfo\msinfo		
13	Hunter XP	System Restore.lnk	F:\WINDOWS\system32\Restore\rstrui.exe		
14	Hunter XP	Disk Cleanup.lnk	F:\WINDOWS\system32\cleanmgr.exe		
15	Hunter XP	Scheduled Tasks.lnk	F:\WINDOWS\explorer.exe		::{20D04FE0-3AEA-1069-A2D8-08002B30309D}
16	Hunter XP	Activate Windows.lnk	F:\WINDOWS\system32\oobe\msoobe.exe		/A
17	Hunter XP	Files and Settings Transfer Wizard.lnk	F:\WINDOWS\system32\usmt\migwiz.exe		
18	Hunter XP	WordPad.lnk	F:\Program Files\Windows NT\Accessories\wordpad.exe		
19	Hunter XP	Calculator.lnk	F:\WINDOWS\system32\calc.exe		
20	Hunter XP	Paint.lnk	F:\WINDOWS\system32\mspaint.exe		
21	Hunter XP	Scanner and Camera Wizard.lnk	F:\WINDOWS\system32\wiaacmgr.exe		-SelectDevice
22	Hunter XP	Windows Movie Maker.lnk	F:\Program Files\Movie Maker\moviemk.exe		
23	Hunter XP	Data Sources (ODBC).lnk	F:\WINDOWS\system32\odbcad32.exe		
24	Hunter XP	America Online 7.0.lnk	F:\Program Files\America Online 7.0\aol.exe		
25	Hunter XP	AOL System Information.lnk	F:\Program Files\Common Files\aolshare\sysinfo\sinf.exe		
26	Hunter XP	Palm Desktop.lnk	F:\Palm\palm.exe		
27	Hunter XP	HotSync Manager.lnk	F:\Palm\HOTSYNC.EXE		

Figure 31:

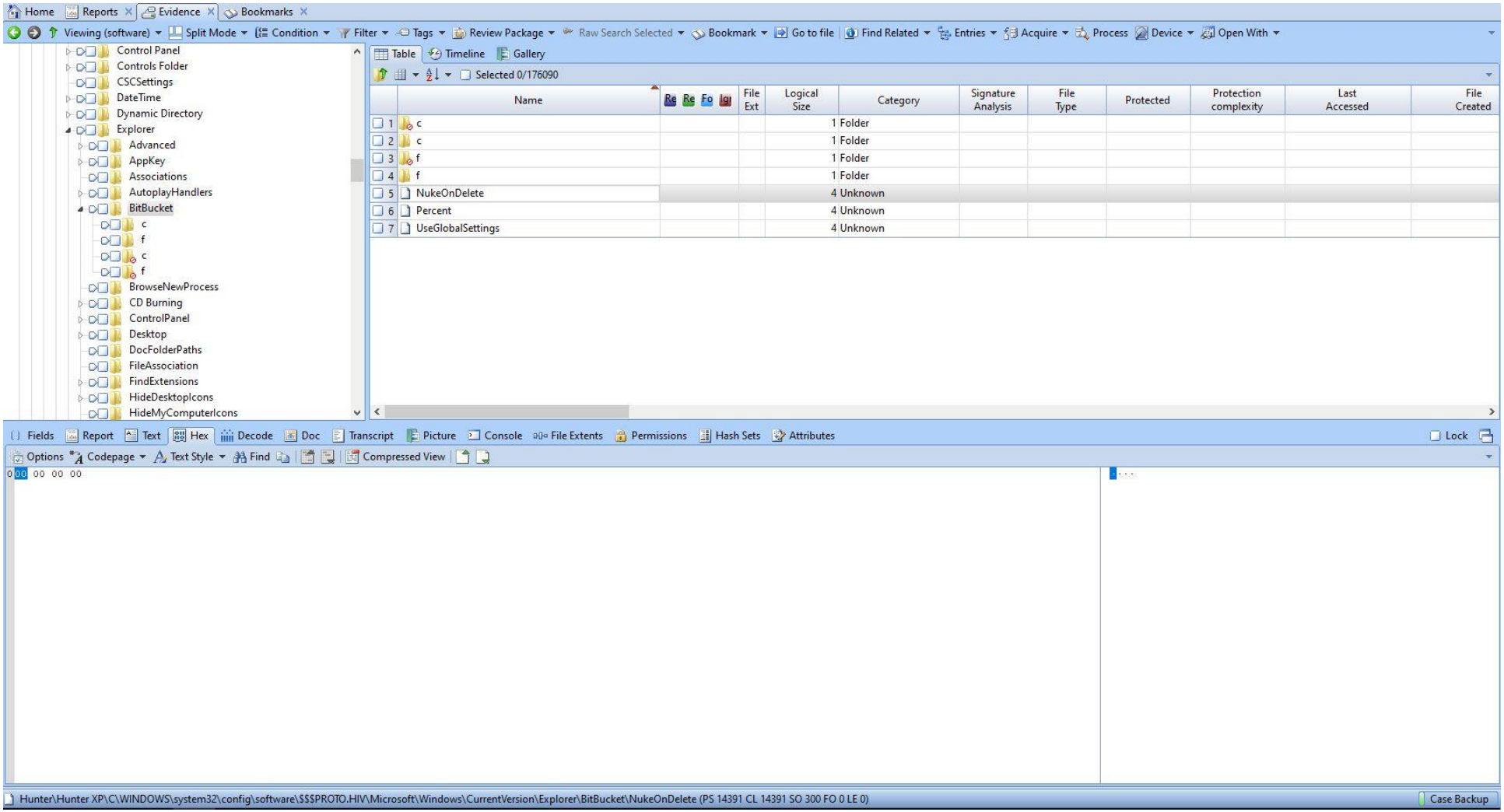
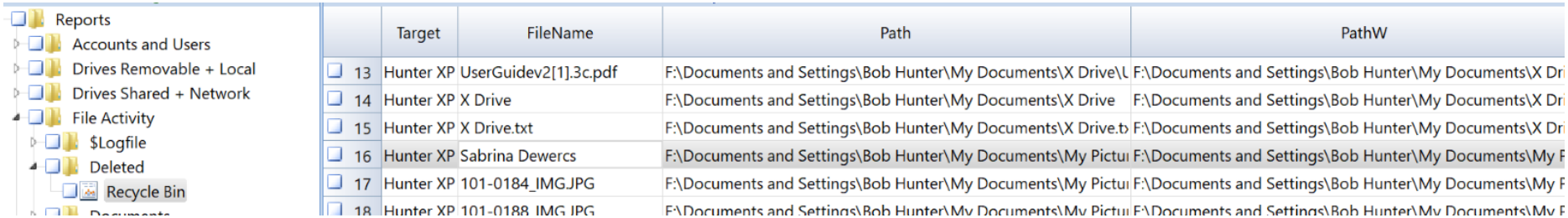

Home
Reports
Evidence
Bookmarks
Viewing (software)
Split Mode
Condition
Filter
Tags
Review Package
Raw Search Selected
Bookmark
Go to file
Find Related
Entries
Acquire
Process
Device
Open With
Control Panel
Controls Folder
CSCSettings
DateTime
Dynamic Directory
Explorer
Advanced
AppKey
Associations
AutoplayHandlers
BitBucket
c
f
c
f
BrowseNewProcess
CD Burning
ControlPanel
Desktop
DocFolderPaths
FileAssociation
FindExtensions
HideDesktopIcons
HideMyComputerIcons
Table
Timeline
Gallery
Selected 0/176090
Name
File Ext
Logical Size
Category
Signature Analysis
File Type
Protected
Protection complexity
Last Accessed
File Created
1 c 1 Folder
2 c 1 Folder
3 f 1 Folder
4 f 1 Folder
5 NukeOnDelete 4 Unknown
6 Percent 4 Unknown
7 UseGlobalSettings 4 Unknown
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Console
File Extents
Permissions
Hash Sets
Attributes
Lock
Options
Codepage
Text Style
Find
Compressed View
0 00 00 00 00
Hunter\Hunter XP\C\WINDOWS\system32\config\software\$$$PROTO.HIV\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\NukeOnDelete (PS 14391 CL 14391 SO 300 FO 0 LE 0)
Case Backup

Figure 32:


Reports
Accounts and Users
Drives Removable + Local
Drives Shared + Network
File Activity
$Logfile
Deleted
Recycle Bin
Target
FileName
Path
PathW
13 Hunter XP UserGuidev2[1].3c.pdf F:\Documents and Settings\Bob Hunter\My Documents\X Drive\U F:\Documents and Settings\Bob Hunter\My Documents\X Dri
14 Hunter XP X Drive F:\Documents and Settings\Bob Hunter\My Documents\X Drive F:\Documents and Settings\Bob Hunter\My Documents\X Dri
15 Hunter XP X Drive.txt F:\Documents and Settings\Bob Hunter\My Documents\X Drive.tx F:\Documents and Settings\Bob Hunter\My Documents\X Dri
16 Hunter XP Sabrina Dewercs F:\Documents and Settings\Bob Hunter\My Documents\My Pictur F:\Documents and Settings\Bob Hunter\My Documents\My P
17 Hunter XP 101-0184_IMG.JPG F:\Documents and Settings\Bob Hunter\My Documents\My Pictur F:\Documents and Settings\Bob Hunter\My Documents\My P

Instant Messaging Clients:

Figure 33:

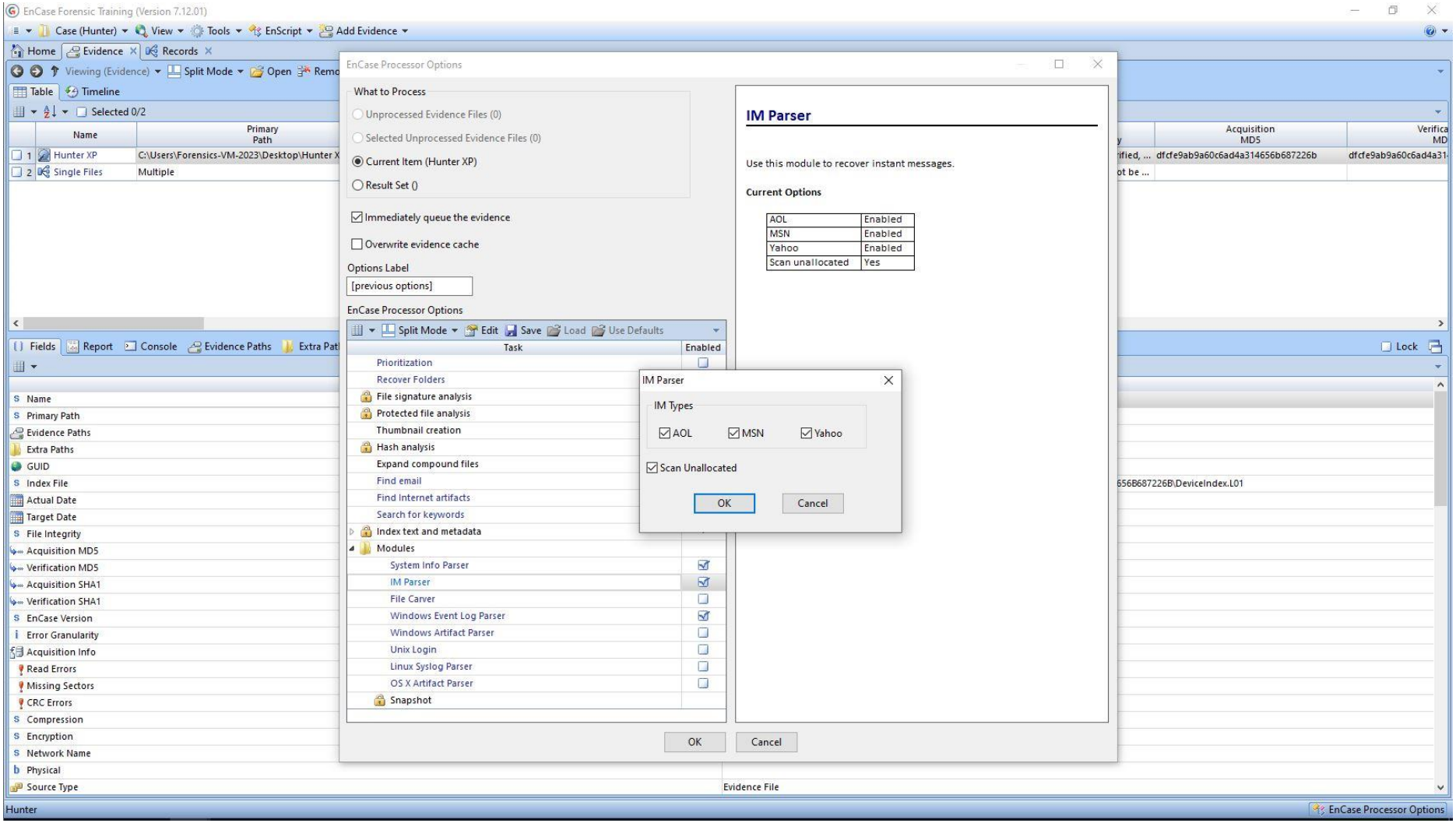


Figure 34:

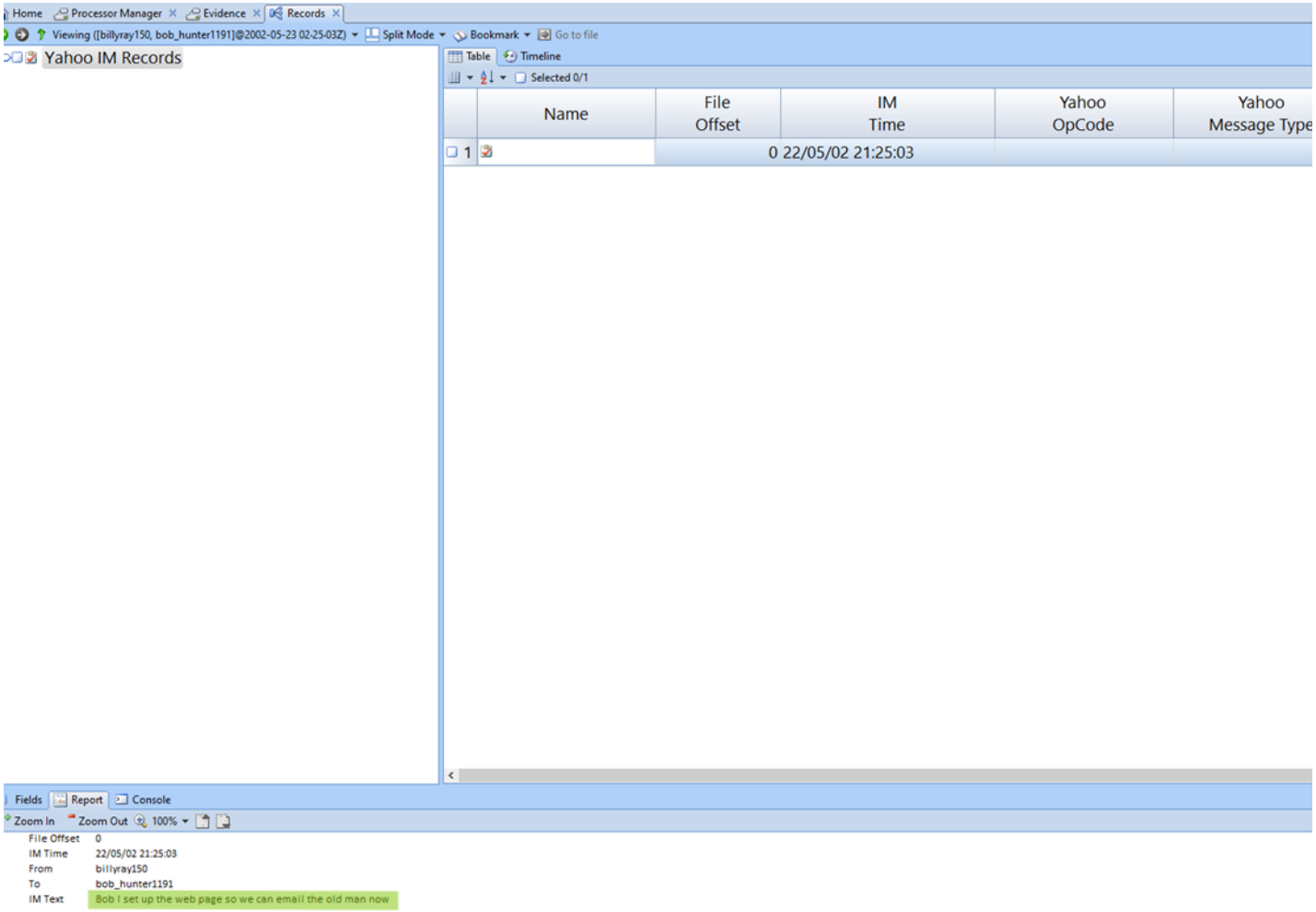
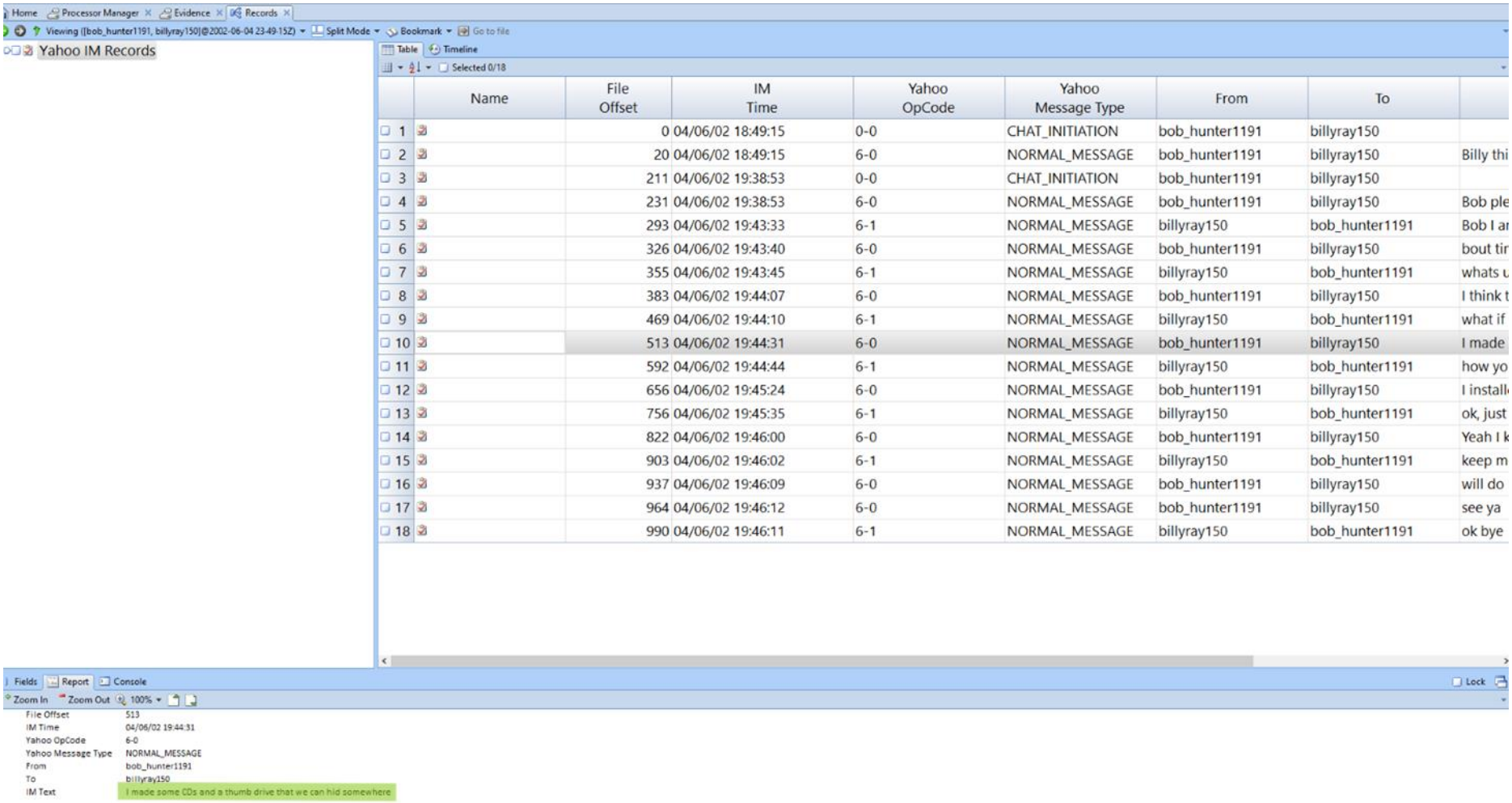
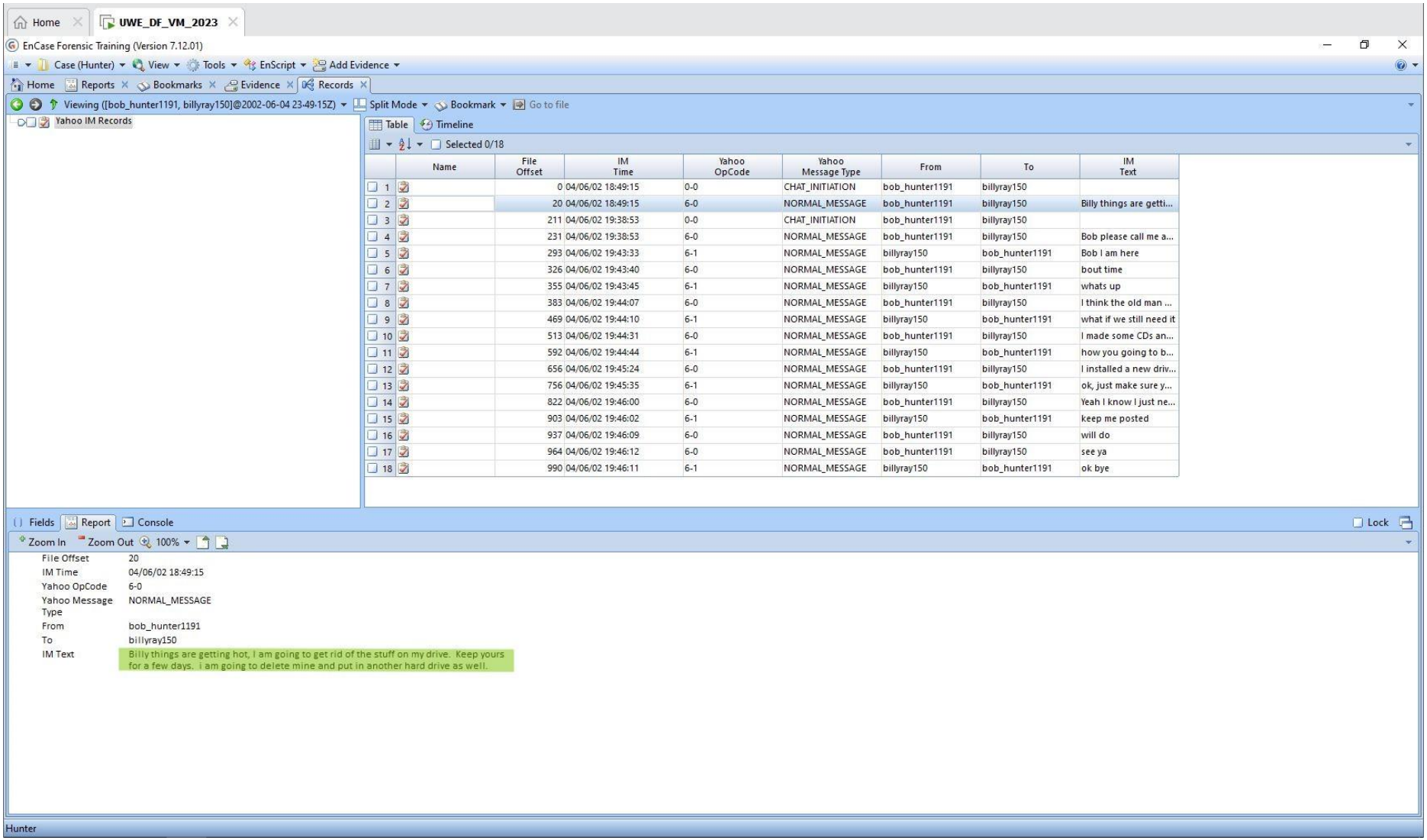

Home
Processor Manager
Evidence
Records
Viewing ([billyray150, bob_hunter1191]@2002-05-23 02-25-03Z)
Split Mode
Bookmark
Go to file
Yahoo IM Records
Table
Timeline
Selected 0/1
Name
File Offset
IM Time
Yahoo OpCode
Yahoo Message Type
1
0 22/05/02 21:25:03
Fields
Report
Console
Zoom In
Zoom Out
100%
File Offset 0
IM Time 22/05/02 21:25:03
From billyray150
To bob_hunter1191
IM Text Bob I set up the web page so we can email the old man now

Figure 35:



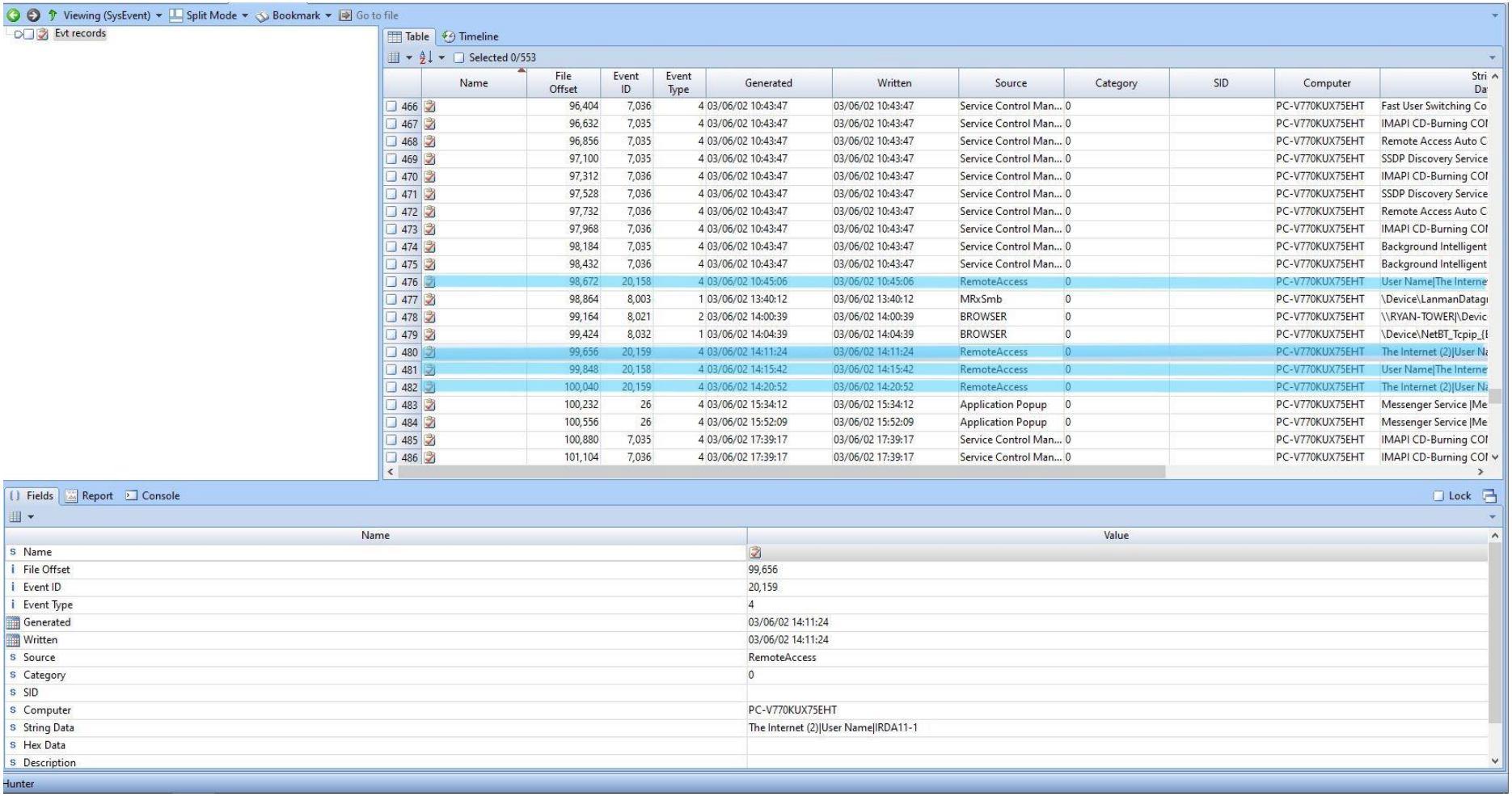
	Name	File Offset	IM Time	Yahoo OpCode	Yahoo Message Type	From	To	
1		0	04/06/02 18:49:15	0-0	CHAT_INITIATION	bob_hunter1191	billyray150	
2		20	04/06/02 18:49:15	6-0	NORMAL_MESSAGE	bob_hunter1191	billyray150	Billy thi
3		211	04/06/02 19:38:53	0-0	CHAT_INITIATION	bob_hunter1191	billyray150	
4		231	04/06/02 19:38:53	6-0	NORMAL_MESSAGE	bob_hunter1191	billyray150	Bob ple
5		293	04/06/02 19:43:33	6-1	NORMAL_MESSAGE	billyray150	bob_hunter1191	Bob I ar
6		326	04/06/02 19:43:40	6-0	NORMAL_MESSAGE	bob_hunter1191	billyray150	bout tir
7		355	04/06/02 19:43:45	6-1	NORMAL_MESSAGE	billyray150	bob_hunter1191	whats u
8		383	04/06/02 19:44:07	6-0	NORMAL_MESSAGE	bob_hunter1191	billyray150	I think t
9		469	04/06/02 19:44:10	6-1	NORMAL_MESSAGE	billyray150	bob_hunter1191	what if
10		513	04/06/02 19:44:31	6-0	NORMAL_MESSAGE	bob_hunter1191	billyray150	I made
11		592	04/06/02 19:44:44	6-1	NORMAL_MESSAGE	billyray150	bob_hunter1191	how yo
12		656	04/06/02 19:45:24	6-0	NORMAL_MESSAGE	bob_hunter1191	billyray150	I install
13		756	04/06/02 19:45:35	6-1	NORMAL_MESSAGE	billyray150	bob_hunter1191	ok, just
14		822	04/06/02 19:46:00	6-0	NORMAL_MESSAGE	bob_hunter1191	billyray150	Yeah I k
15		903	04/06/02 19:46:02	6-1	NORMAL_MESSAGE	billyray150	bob_hunter1191	keep m
16		937	04/06/02 19:46:09	6-0	NORMAL_MESSAGE	bob_hunter1191	billyray150	will do
17		964	04/06/02 19:46:12	6-0	NORMAL_MESSAGE	bob_hunter1191	billyray150	see ya
18		990	04/06/02 19:46:11	6-1	NORMAL_MESSAGE	billyray150	bob_hunter1191	ok bye

Figure 36:


Home
UWE_DF_VM_2023
EnCase Forensic Training (Version 7.12.01)
Case (Hunter) View Tools EnScript Add Evidence
Home Reports Bookmarks Evidence Records
Viewing ([bob_hunter1191, billyray150]@2002-06-04 23:49:15Z) Split Mode Bookmark Go to file
Yahoo IM Records
Table Timeline
Selected 0/18
Name | File Offset | IM Time | Yahoo OpCode | Yahoo Message Type | From | To | IM Text
1 | 0 | 04/06/02 18:49:15 | 0-0 | CHAT_INITIATION | bob_hunter1191 | billyray150 |
2 | 20 | 04/06/02 18:49:15 | 6-0 | NORMAL_MESSAGE | bob_hunter1191 | billyray150 | Billy things are getti...
3 | 211 | 04/06/02 19:38:53 | 0-0 | CHAT_INITIATION | bob_hunter1191 | billyray150 |
4 | 231 | 04/06/02 19:38:53 | 6-0 | NORMAL_MESSAGE | bob_hunter1191 | billyray150 | Bob please call me a...
5 | 293 | 04/06/02 19:43:33 | 6-1 | NORMAL_MESSAGE | billyray150 | bob_hunter1191 | Bob I am here
6 | 326 | 04/06/02 19:43:40 | 6-0 | NORMAL_MESSAGE | bob_hunter1191 | billyray150 | bout time
7 | 355 | 04/06/02 19:43:45 | 6-1 | NORMAL_MESSAGE | billyray150 | bob_hunter1191 | whats up
8 | 383 | 04/06/02 19:44:07 | 6-0 | NORMAL_MESSAGE | bob_hunter1191 | billyray150 | I think the old man ...
9 | 469 | 04/06/02 19:44:10 | 6-1 | NORMAL_MESSAGE | billyray150 | bob_hunter1191 | what if we still need it
10 | 513 | 04/06/02 19:44:31 | 6-0 | NORMAL_MESSAGE | bob_hunter1191 | billyray150 | I made some CDs an...
11 | 592 | 04/06/02 19:44:44 | 6-1 | NORMAL_MESSAGE | billyray150 | bob_hunter1191 | how you going to b...
12 | 656 | 04/06/02 19:45:24 | 6-0 | NORMAL_MESSAGE | bob_hunter1191 | billyray150 | I installed a new driv...
13 | 756 | 04/06/02 19:45:35 | 6-1 | NORMAL_MESSAGE | billyray150 | bob_hunter1191 | ok, just make sure y...
14 | 822 | 04/06/02 19:46:00 | 6-0 | NORMAL_MESSAGE | bob_hunter1191 | billyray150 | Yeah I know I just ne...
15 | 903 | 04/06/02 19:46:02 | 6-1 | NORMAL_MESSAGE | billyray150 | bob_hunter1191 | keep me posted
16 | 937 | 04/06/02 19:46:09 | 6-0 | NORMAL_MESSAGE | bob_hunter1191 | billyray150 | will do
17 | 964 | 04/06/02 19:46:12 | 6-0 | NORMAL_MESSAGE | bob_hunter1191 | billyray150 | see ya
18 | 990 | 04/06/02 19:46:11 | 6-1 | NORMAL_MESSAGE | billyray150 | bob_hunter1191 | ok bye
Fields Report Console
Lock
Zoom In Zoom Out 100%
File Offset 20
IM Time 04/06/02 18:49:15
Yahoo OpCode 6-0
Yahoo Message Type NORMAL_MESSAGE
From bob_hunter1191
To billyray150
IM Text Billy things are getting hot, I am going to get rid of the stuff on my drive. Keep yours for a few days. i am going to delete mine and put in another hard drive as well.
Hunter

Clean Up/ Wiping Utilities :

Figure 37:



	Name	File Offset	Event ID	Event Type	Generated	Written	Source	Category	SID	Computer	String Data
466		96,404	7,036	4	03/06/02 10:43:47	03/06/02 10:43:47	Service Control Man...	0		PC-V770KUX75EHT	Fast User Switching Co
467		96,632	7,035	4	03/06/02 10:43:47	03/06/02 10:43:47	Service Control Man...	0		PC-V770KUX75EHT	IMAPI CD-Burning COI
468		96,856	7,035	4	03/06/02 10:43:47	03/06/02 10:43:47	Service Control Man...	0		PC-V770KUX75EHT	Remote Access Auto C
469		97,100	7,035	4	03/06/02 10:43:47	03/06/02 10:43:47	Service Control Man...	0		PC-V770KUX75EHT	SSDP Discovery Service
470		97,312	7,036	4	03/06/02 10:43:47	03/06/02 10:43:47	Service Control Man...	0		PC-V770KUX75EHT	IMAPI CD-Burning COI
471		97,528	7,036	4	03/06/02 10:43:47	03/06/02 10:43:47	Service Control Man...	0		PC-V770KUX75EHT	SSDP Discovery Service
472		97,732	7,036	4	03/06/02 10:43:47	03/06/02 10:43:47	Service Control Man...	0		PC-V770KUX75EHT	Remote Access Auto C
473		97,968	7,036	4	03/06/02 10:43:47	03/06/02 10:43:47	Service Control Man...	0		PC-V770KUX75EHT	IMAPI CD-Burning COI
474		98,184	7,035	4	03/06/02 10:43:47	03/06/02 10:43:47	Service Control Man...	0		PC-V770KUX75EHT	Background Intelligent
475		98,432	7,036	4	03/06/02 10:43:47	03/06/02 10:43:47	Service Control Man...	0		PC-V770KUX75EHT	Background Intelligent
476		98,672	20,158	4	03/06/02 10:45:06	03/06/02 10:45:06	RemoteAccess	0		PC-V770KUX75EHT	User Name|The Interne
477		98,864	8,003	1	03/06/02 13:40:12	03/06/02 13:40:12	MRxSmb	0		PC-V770KUX75EHT	\Device\LanmanDatag
478		99,164	8,021	2	03/06/02 14:00:39	03/06/02 14:00:39	BROWSER	0		PC-V770KUX75EHT	\\RYAN-TOWER|\Devic
479		99,424	8,032	1	03/06/02 14:04:39	03/06/02 14:04:39	BROWSER	0		PC-V770KUX75EHT	\Device\NetBT_Tcpip_{E
480		99,656	20,159	4	03/06/02 14:11:24	03/06/02 14:11:24	RemoteAccess	0		PC-V770KUX75EHT	The Internet (2)|User Na
481		99,848	20,158	4	03/06/02 14:15:42	03/06/02 14:15:42	RemoteAccess	0		PC-V770KUX75EHT	User Name|The Interne
482		100,040	20,159	4	03/06/02 14:20:52	03/06/02 14:20:52	RemoteAccess	0		PC-V770KUX75EHT	The Internet (2)|User Na
483		100,232	26	4	03/06/02 15:34:12	03/06/02 15:34:12	Application Popup	0		PC-V770KUX75EHT	Messenger Service |Me
484		100,556	26	4	03/06/02 15:52:09	03/06/02 15:52:09	Application Popup	0		PC-V770KUX75EHT	Messenger Service |Me
485		100,880	7,035	4	03/06/02 17:39:17	03/06/02 17:39:17	Service Control Man...	0		PC-V770KUX75EHT	IMAPI CD-Burning COI
486		101,104	7,036	4	03/06/02 17:39:17	03/06/02 17:39:17	Service Control Man...	0		PC-V770KUX75EHT	IMAPI CD-Burning COI

Name	Value
Name	
File Offset	99,656
Event ID	20,159
Event Type	4
Generated	03/06/02 14:11:24
Written	03/06/02 14:11:24
Source	RemoteAccess
Category	0
SID	
Computer	PC-V770KUX75EHT
String Data	The Internet (2)|User Name|IRDA11-1
Hex Data	
Description	

Figure 38:

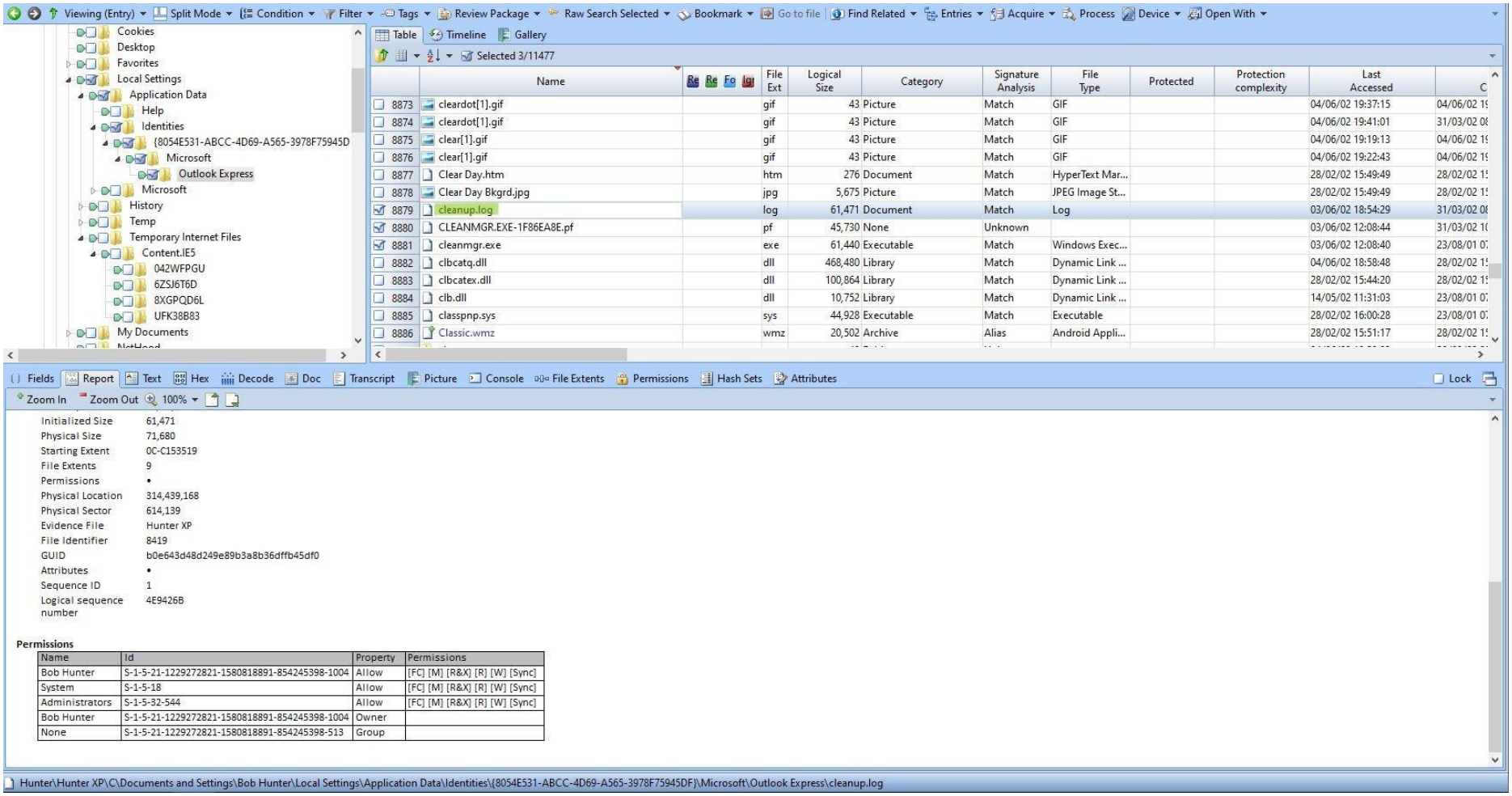

Viewing (Entry)
Split Mode
Condition
Filter
Tags
Review Package
Raw Search Selected
Bookmark
Go to file
Find Related
Entries
Acquire
Process
Device
Open With
Cookies
Desktop
Favorites
Local Settings
Application Data
Help
Identities
{8054E531-ABCC-4D69-A565-3978F75945D
Microsoft
Outlook Express
Microsoft
History
Temp
Temporary Internet Files
Content.IE5
042WFPGU
6ZSJ6T6D
8XGPQD6L
UFK38B83
My Documents
Table
Timeline
Gallery
Selected 3/11477
Name
File Ext
Logical Size
Category
Signature Analysis
File Type
Protected
Protection complexity
Last Accessed
8873 cleardot[1].gif gif 43 Picture Match GIF 04/06/02 19:37:15
8874 cleardot[1].gif gif 43 Picture Match GIF 04/06/02 19:41:01
8875 clear[1].gif gif 43 Picture Match GIF 04/06/02 19:19:13
8876 clear[1].gif gif 43 Picture Match GIF 04/06/02 19:22:43
8877 Clear Day.htm htm 276 Document Match HyperText Mar... 28/02/02 15:49:49
8878 Clear Day Bkgrd.jpg jpg 5,675 Picture Match JPEG Image St... 28/02/02 15:49:49
8879 cleanup.log log 61,471 Document Match Log 03/06/02 18:54:29
8880 CLEANMGR.EXE-1F86EA8E.pf pf 45,730 None Unknown 03/06/02 12:08:44
8881 cleanmgr.exe exe 61,440 Executable Match Windows Exec... 03/06/02 12:08:40
8882 clbcatq.dll dll 468,480 Library Match Dynamic Link ... 04/06/02 18:58:48
8883 clbcatex.dll dll 100,864 Library Match Dynamic Link ... 28/02/02 15:44:20
8884 clb.dll dll 10,752 Library Match Dynamic Link ... 14/05/02 11:31:03
8885 classpnp.sys sys 44,928 Executable Match Executable 28/02/02 16:00:28
8886 Classic.wmz wmz 20,502 Archive Alias Android Appli... 28/02/02 15:51:17
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Console
File Extents
Permissions
Hash Sets
Attributes
Lock
Zoom In
Zoom Out
100%
Initialized Size 61,471
Physical Size 71,680
Starting Extent 0C-C153519
File Extents 9
Permissions •
Physical Location 314,439,168
Physical Sector 614,139
Evidence File Hunter XP
File Identifier 8419
GUID b0e643d48d249e89b3a8b36dffb45df0
Attributes •
Sequence ID 1
Logical sequence number 4E9426B
Permissions
Name Id Property Permissions
Bob Hunter S-1-5-21-1229272821-1580818891-854245398-1004 Allow [FC] [M] [R&X] [R] [W] [Sync]
System S-1-5-18 Allow [FC] [M] [R&X] [R] [W] [Sync]
Administrators S-1-5-32-544 Allow [FC] [M] [R&X] [R] [W] [Sync]
Bob Hunter S-1-5-21-1229272821-1580818891-854245398-1004 Owner
None S-1-5-21-1229272821-1580818891-854245398-513 Group
Hunter\Hunter XP\C\Documents and Settings\Bob Hunter\Local Settings\Application Data\Identities\{8054E531-ABCC-4D69-A565-3978F75945DF}\Microsoft\Outlook Express\cleanup.log

Figure 39:

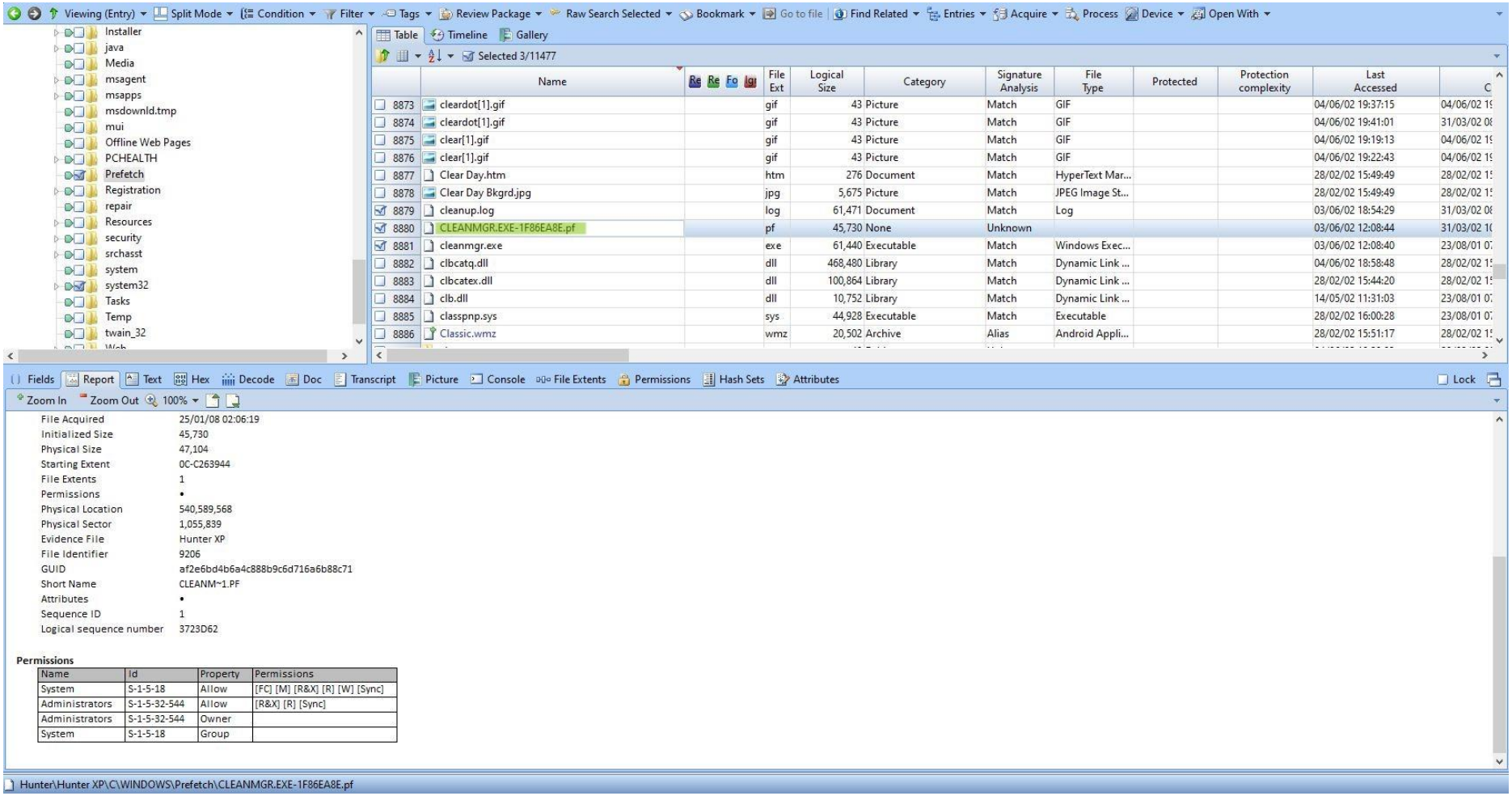
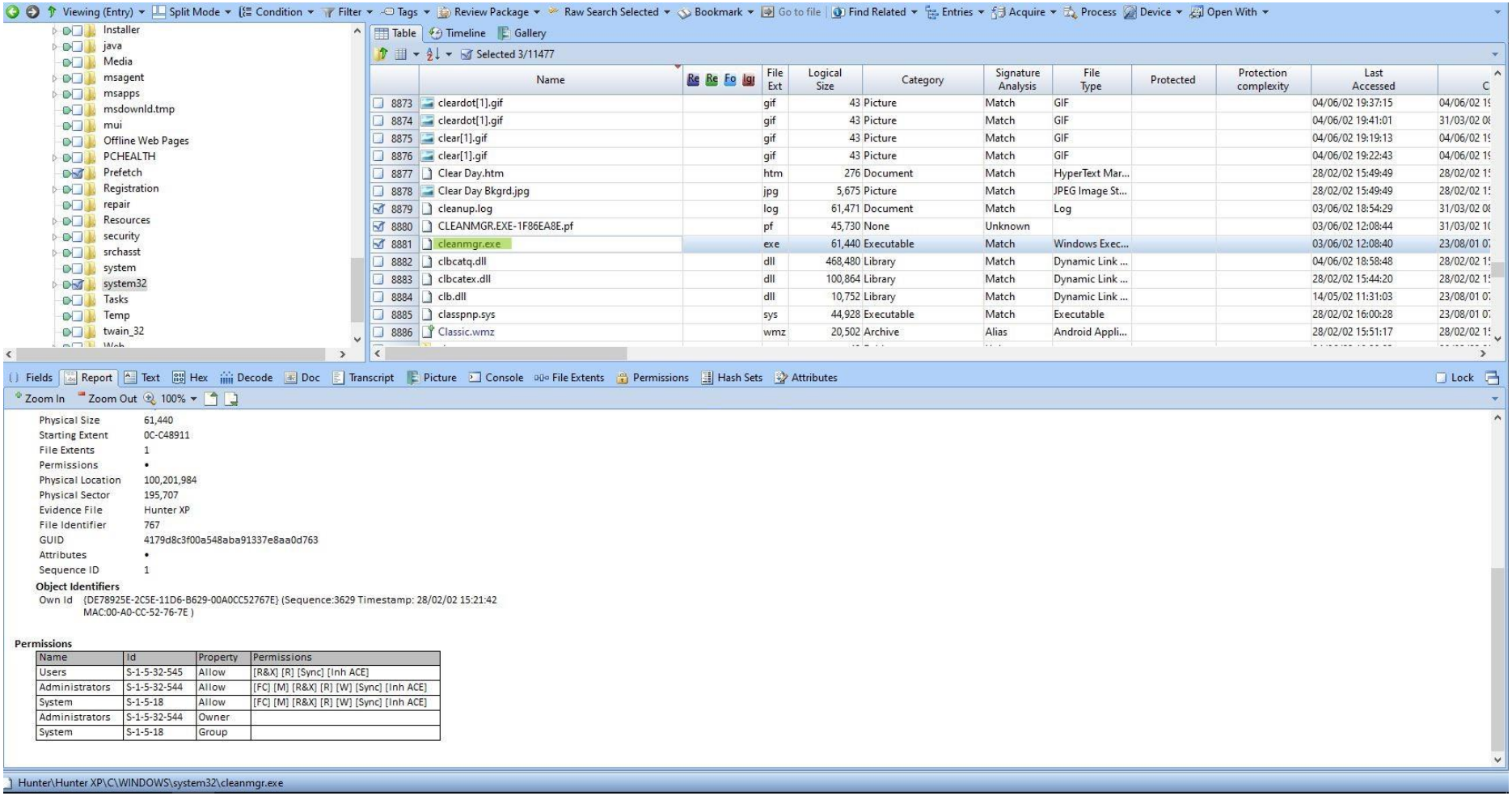

Viewing (Entry) Split Mode Condition Filter Tags Review Package Raw Search Selected Bookmark Go to file Find Related Entries Acquire Process Device Open With
Installer
java
Media
msagent
msapps
msdownld.tmp
mui
Offline Web Pages
PCHEALTH
Prefetch
Registration
repair
Resources
security
srchasst
system
system32
Tasks
Temp
twain_32
Table Timeline Gallery
Selected 3/11477
Name File Ext Logical Size Category Signature Analysis File Type Protected Protection complexity Last Accessed
8873 cleardot[1].gif gif 43 Picture Match GIF 04/06/02 19:37:15
8874 cleardot[1].gif gif 43 Picture Match GIF 04/06/02 19:41:01
8875 clear[1].gif gif 43 Picture Match GIF 04/06/02 19:19:13
8876 clear[1].gif gif 43 Picture Match GIF 04/06/02 19:22:43
8877 Clear Day.htm htm 276 Document Match HyperText Mar... 28/02/02 15:49:49
8878 Clear Day Bkgrd.jpg jpg 5,675 Picture Match JPEG Image St... 28/02/02 15:49:49
8879 cleanup.log log 61,471 Document Match Log 03/06/02 18:54:29
8880 CLEANMGR.EXE-1F86EA8E.pf pf 45,730 None Unknown 03/06/02 12:08:44
8881 cleanmgr.exe exe 61,440 Executable Match Windows Exec... 03/06/02 12:08:40
8882 clbcatq.dll dll 468,480 Library Match Dynamic Link ... 04/06/02 18:58:48
8883 clbcatex.dll dll 100,864 Library Match Dynamic Link ... 28/02/02 15:44:20
8884 clb.dll dll 10,752 Library Match Dynamic Link ... 14/05/02 11:31:03
8885 classpnp.sys sys 44,928 Executable Match Executable 28/02/02 16:00:28
8886 Classic.wmz wmz 20,502 Archive Alias Android Appli... 28/02/02 15:51:17
Fields Report Text Hex Decode Doc Transcript Picture Console File Extents Permissions Hash Sets Attributes Lock
Zoom In Zoom Out 100%
File Acquired 25/01/08 02:06:19
Initialized Size 45,730
Physical Size 47,104
Starting Extent 0C-C263944
File Extents 1
Permissions •
Physical Location 540,589,568
Physical Sector 1,055,839
Evidence File Hunter XP
File Identifier 9206
GUID af2e6bd4b6a4c888b9c6d716a6b88c71
Short Name CLEANM~1.PF
Attributes •
Sequence ID 1
Logical sequence number 3723D62
Permissions
Name Id Property Permissions
System S-1-5-18 Allow [FC] [M] [R&X] [R] [W] [Sync]
Administrators S-1-5-32-544 Allow [R&X] [R] [Sync]
Administrators S-1-5-32-544 Owner
System S-1-5-18 Group
Hunter\Hunter XP\C\WINDOWS\Prefetch\CLEANMGR.EXE-1F86EA8E.pf

Figure 40:


Viewing (Entry)
Split Mode
Condition
Filter
Tags
Review Package
Raw Search Selected
Bookmark
Go to file
Find Related
Entries
Acquire
Process
Device
Open With
Installer
java
Media
msagent
msapps
msdownld.tmp
mui
Offline Web Pages
PCHEALTH
Prefetch
Registration
repair
Resources
security
srchasst
system
system32
Tasks
Temp
twain_32
Table
Timeline
Gallery
Selected 3/11477
Name
File Ext
Logical Size
Category
Signature Analysis
File Type
Protected
Protection complexity
Last Accessed
8873 cleardot[1].gif gif 43 Picture Match GIF 04/06/02 19:37:15
8874 cleardot[1].gif gif 43 Picture Match GIF 04/06/02 19:41:01
8875 clear[1].gif gif 43 Picture Match GIF 04/06/02 19:19:13
8876 clear[1].gif gif 43 Picture Match GIF 04/06/02 19:22:43
8877 Clear Day.htm htm 276 Document Match HyperText Mar... 28/02/02 15:49:49
8878 Clear Day Bkgrd.jpg jpg 5,675 Picture Match JPEG Image St... 28/02/02 15:49:49
8879 cleanup.log log 61,471 Document Match Log 03/06/02 18:54:29
8880 CLEANMGR.EXE-1F86EA8E.pf pf 45,730 None Unknown 03/06/02 12:08:44
8881 cleanmgr.exe exe 61,440 Executable Match Windows Exec... 03/06/02 12:08:40
8882 clbcatq.dll dll 468,480 Library Match Dynamic Link ... 04/06/02 18:58:48
8883 clbcatex.dll dll 100,864 Library Match Dynamic Link ... 28/02/02 15:44:20
8884 clb.dll dll 10,752 Library Match Dynamic Link ... 14/05/02 11:31:03
8885 classpnp.sys sys 44,928 Executable Match Executable 28/02/02 16:00:28
8886 Classic.wmz wmz 20,502 Archive Alias Android Appli... 28/02/02 15:51:17
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Console
File Extents
Permissions
Hash Sets
Attributes
Lock
Zoom In
Zoom Out
100%
Physical Size 61,440
Starting Extent 0C-C48911
File Extents 1
Permissions •
Physical Location 100,201,984
Physical Sector 195,707
Evidence File Hunter XP
File Identifier 767
GUID 4179d8c3f00a548aba91337e8aa0d763
Attributes •
Sequence ID 1
Object Identifiers
Own Id {DE78925E-2C5E-11D6-B629-00A0CC52767E} (Sequence:3629 Timestamp: 28/02/02 15:21:42 MAC:00-A0-CC-52-76-7E)
Permissions
Name Id Property Permissions
Users S-1-5-32-545 Allow [R&X] [R] [Sync] [Inh ACE]
Administrators S-1-5-32-544 Allow [FC] [M] [R&X] [R] [W] [Sync] [Inh ACE]
System S-1-5-18 Allow [FC] [M] [R&X] [R] [W] [Sync] [Inh ACE]
Administrators S-1-5-32-544 Owner
System S-1-5-18 Group
Hunter\Hunter XP\C\WINDOWS\system32\cleanmgr.exe

External Drives; Network Connections:

Figure 41:

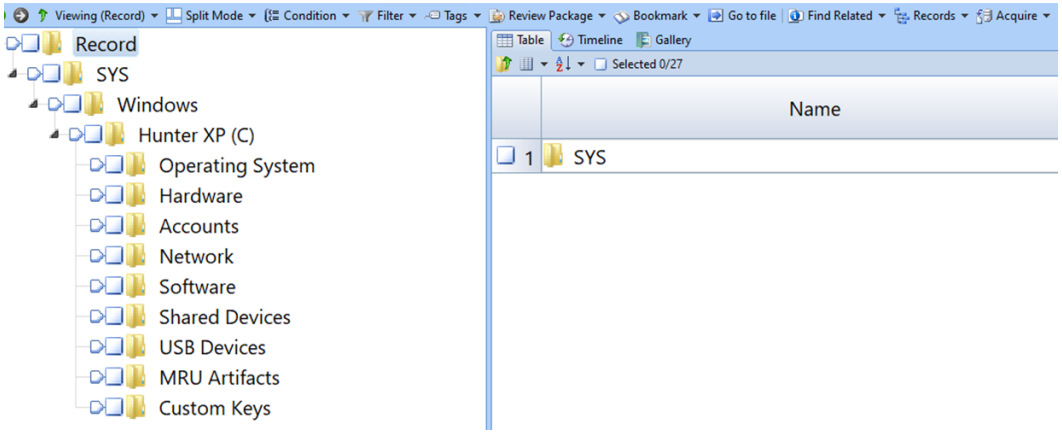


Figure 42:

Perform Data Carving:

Figure 43:

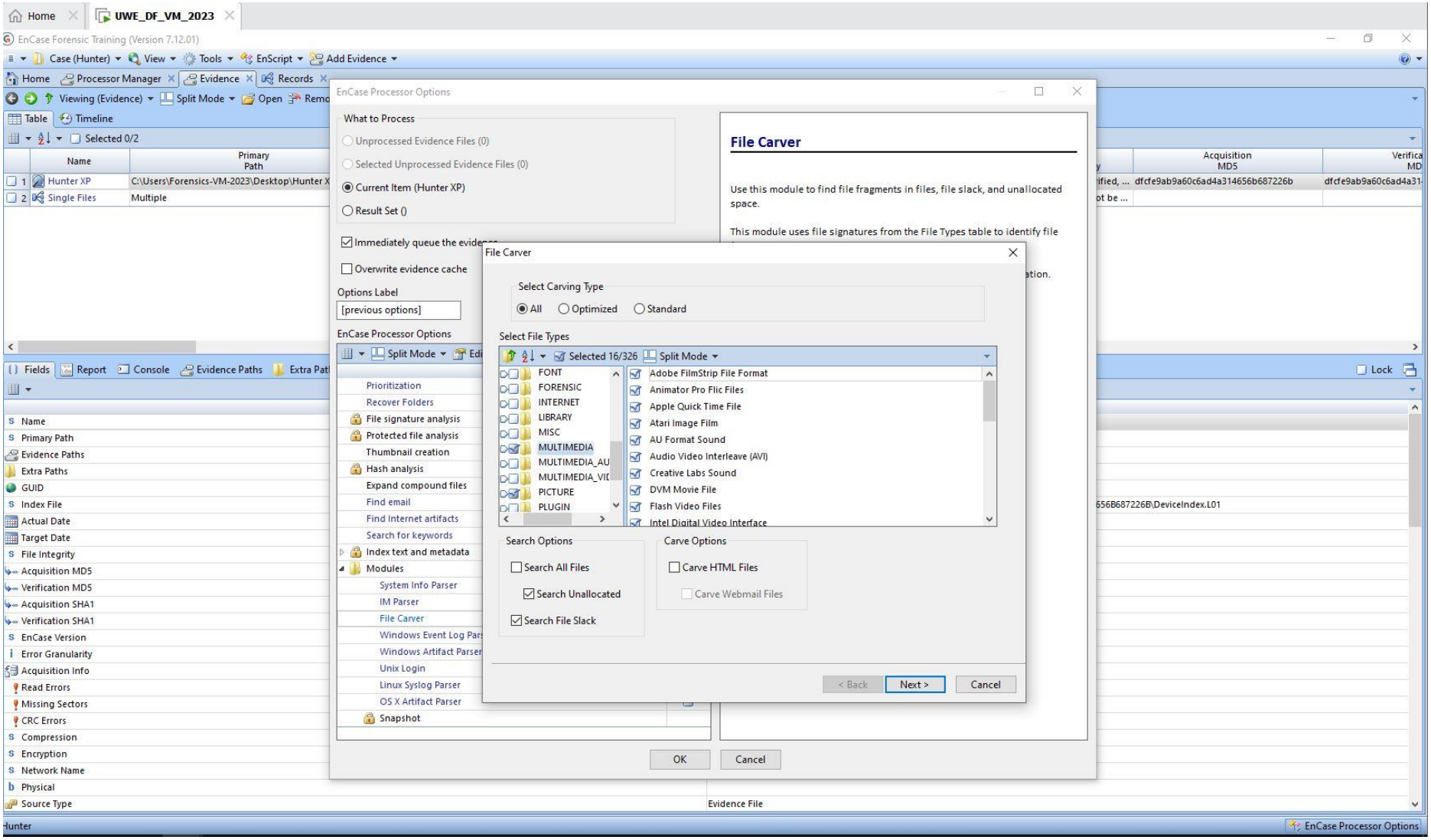


Figure 44:

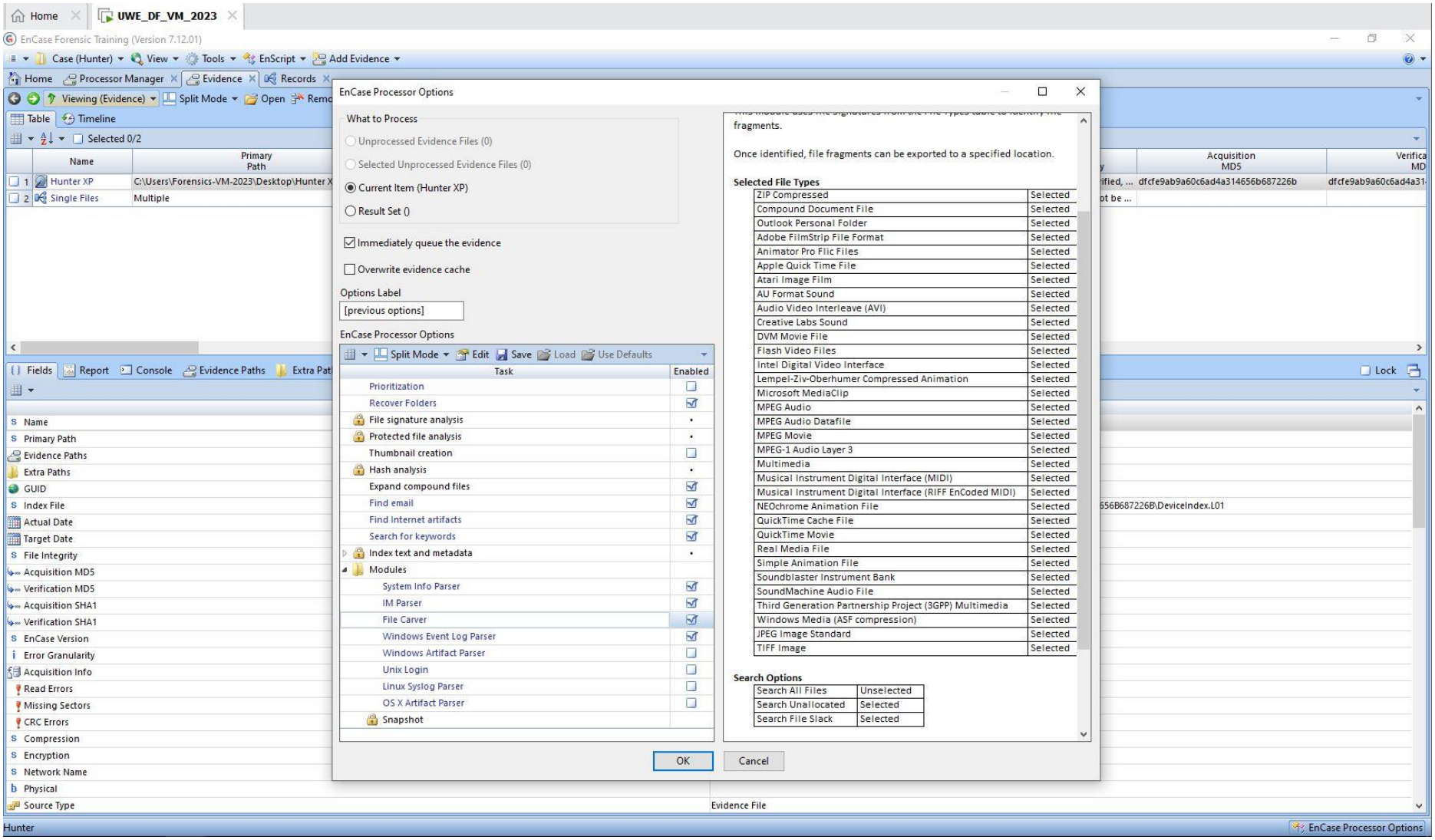

Home
UWE_DF_VM_2023
EnCase Forensic Training (Version 7.12.01)
Case (Hunter)
View
Tools
EnScript
Add Evidence
Processor Manager
Evidence
Records
Viewing (Evidence)
Split Mode
Open
Table
Timeline
Selected 0/2
Name
Primary Path
Hunter XP
C:\Users\Forensics-VM-2023\Desktop\Hunter X
Single Files
Multiple
Acquisition MD5
dfcfe9ab9a60c6ad4a314656b687226b
Fields
Report
Console
Evidence Paths
Extra Paths
Lock
Name
Primary Path
Evidence Paths
Extra Paths
GUID
Index File
Actual Date
Target Date
File Integrity
Acquisition MD5
Verification MD5
Acquisition SHA1
Verification SHA1
EnCase Version
Error Granularity
Acquisition Info
Read Errors
Missing Sectors
CRC Errors
Compression
Encryption
Network Name
Physical
Source Type
Evidence File
Hunter
EnCase Processor Options
EnCase Processor Options
What to Process
Unprocessed Evidence Files (0)
Selected Unprocessed Evidence Files (0)
Current Item (Hunter XP)
Result Set ()
Immediately queue the evidence
Overwrite evidence cache
Options Label
[previous options]
EnCase Processor Options
Split Mode
Edit
Save
Load
Use Defaults
Task
Enabled
Prioritization
Recover Folders
File signature analysis
Protected file analysis
Thumbnail creation
Hash analysis
Expand compound files
Find email
Find Internet artifacts
Search for keywords
Index text and metadata
Modules
System Info Parser
IM Parser
File Carver
Windows Event Log Parser
Windows Artifact Parser
Unix Login
Linux Syslog Parser
OS X Artifact Parser
Snapshot
fragments.
Once identified, file fragments can be exported to a specified location.
Selected File Types
ZIP Compressed Selected
Compound Document File Selected
Outlook Personal Folder Selected
Adobe FilmStrip File Format Selected
Animator Pro Flic Files Selected
Apple Quick Time File Selected
Atari Image Film Selected
AU Format Sound Selected
Audio Video Interleave (AVI) Selected
Creative Labs Sound Selected
DVM Movie File Selected
Flash Video Files Selected
Intel Digital Video Interface Selected
Lempel-Ziv-Oberhumer Compressed Animation Selected
Microsoft MediaClip Selected
MPEG Audio Selected
MPEG Audio Datafile Selected
MPEG Movie Selected
MPEG-1 Audio Layer 3 Selected
Multimedia Selected
Musical Instrument Digital Interface (MIDI) Selected
Musical Instrument Digital Interface (RIFF EnCoded MIDI) Selected
NEOchrome Animation File Selected
QuickTime Cache File Selected
QuickTime Movie Selected
Real Media File Selected
Simple Animation File Selected
Soundblaster Instrument Bank Selected
SoundMachine Audio File Selected
Third Generation Partnership Project (3GPP) Multimedia Selected
Windows Media (ASF compression) Selected
JPEG Image Standard Selected
TIFF Image Selected
Search Options
Search All Files Unselected
Search Unallocated Selected
Search File Slack Selected
OK
Cancel
EnCase Processor Options

Figure 45:

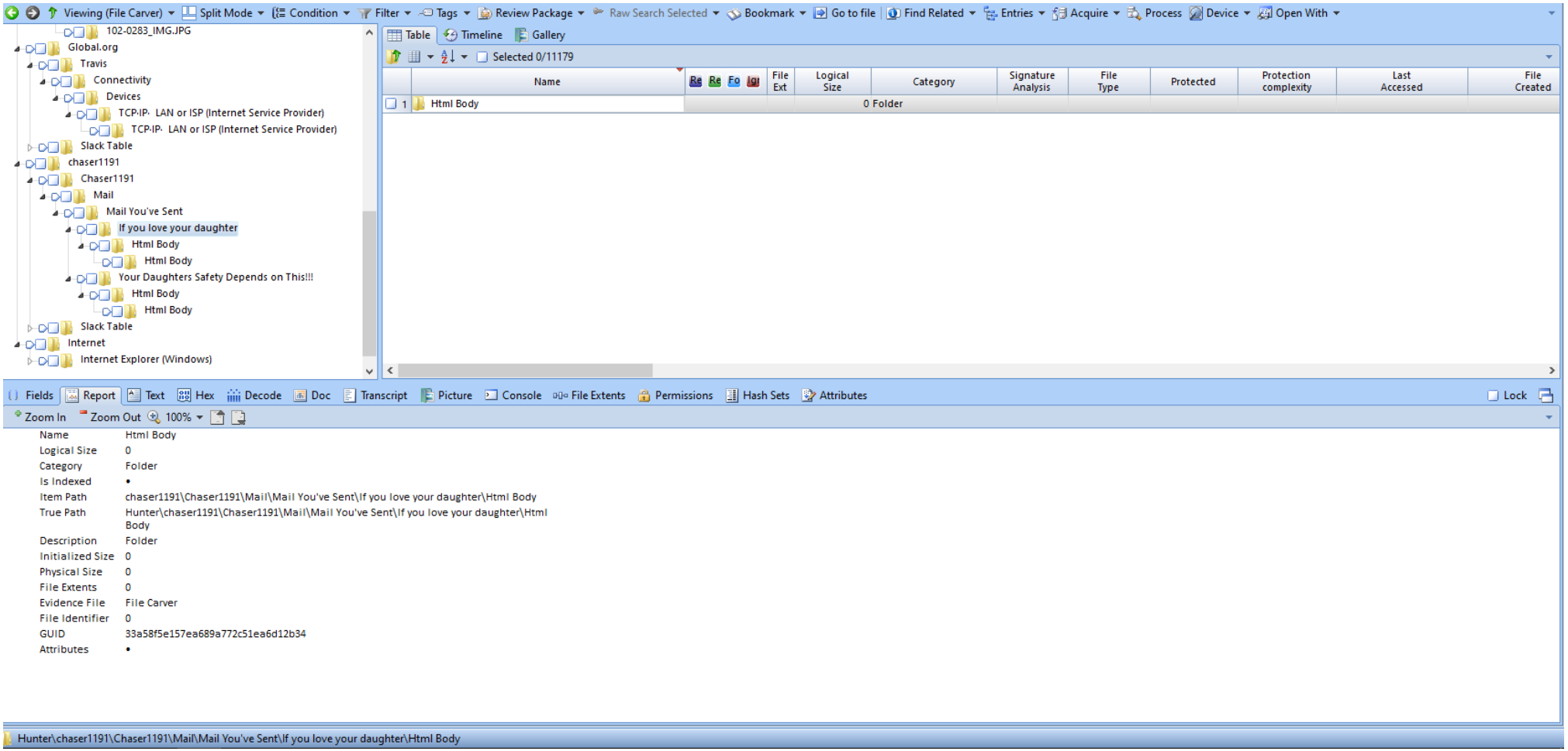

Viewing (File Carver)
Split Mode
Condition
Filter
Tags
Review Package
Raw Search Selected
Bookmark
Go to file
Find Related
Entries
Acquire
Process
Device
Open With
102-0283_IMG.JPG
Global.org
Travis
Connectivity
Devices
TCP-IP· LAN or ISP (Internet Service Provider)
TCP-IP· LAN or ISP (Internet Service Provider)
Slack Table
chaser1191
Chaser1191
Mail
Mail You've Sent
If you love your daughter
Html Body
Html Body
Your Daughters Safety Depends on This!!!
Html Body
Html Body
Slack Table
Internet
Internet Explorer (Windows)
Table
Timeline
Gallery
Selected 0/11179
Name
File Ext
Logical Size
Category
Signature Analysis
File Type
Protected
Protection complexity
Last Accessed
File Created
1
Html Body
0 Folder
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Console
File Extents
Permissions
Hash Sets
Attributes
Lock
Zoom In
Zoom Out
100%
Name Html Body
Logical Size 0
Category Folder
Is Indexed •
Item Path chaser1191\Chaser1191\Mail\Mail You've Sent\If you love your daughter\Html Body
True Path Hunter\chaser1191\Chaser1191\Mail\Mail You've Sent\If you love your daughter\Html Body
Description Folder
Initialized Size 0
Physical Size 0
File Extents 0
Evidence File File Carver
File Identifier 0
GUID 33a58f5e157ea689a772c51ea6d12b34
Attributes •
Hunter\chaser1191\Chaser1191\Mail\Mail You've Sent\If you love your daughter\Html Body

Figure 46:

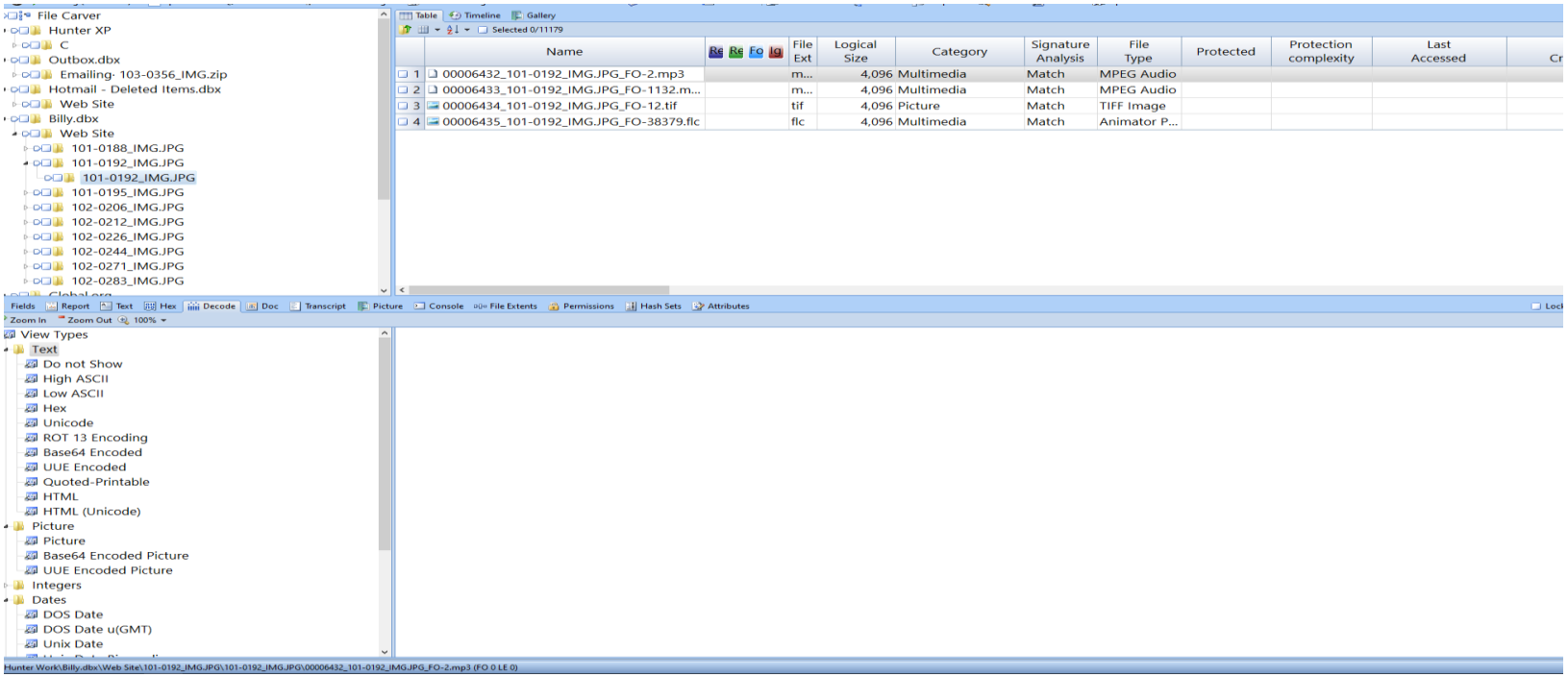
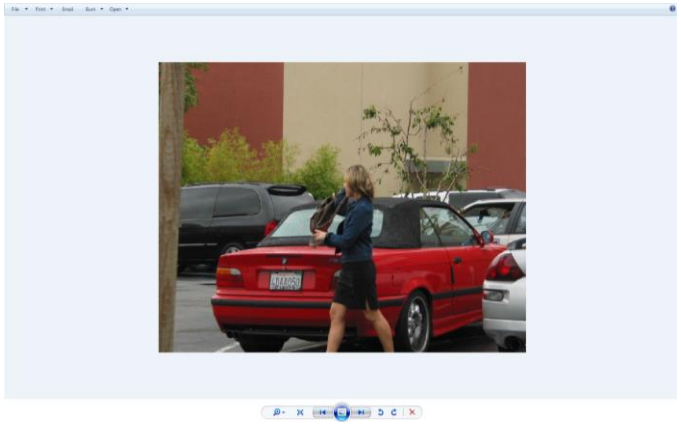


Figure 47:



Run Relevant Keyword Searches:

Figure 48:

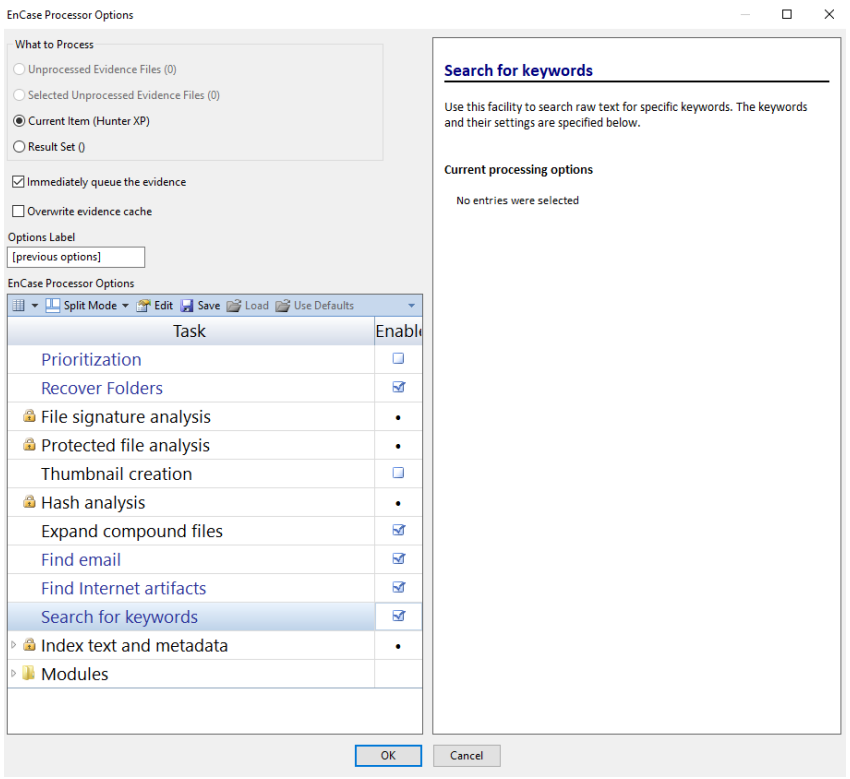


Figure 49:

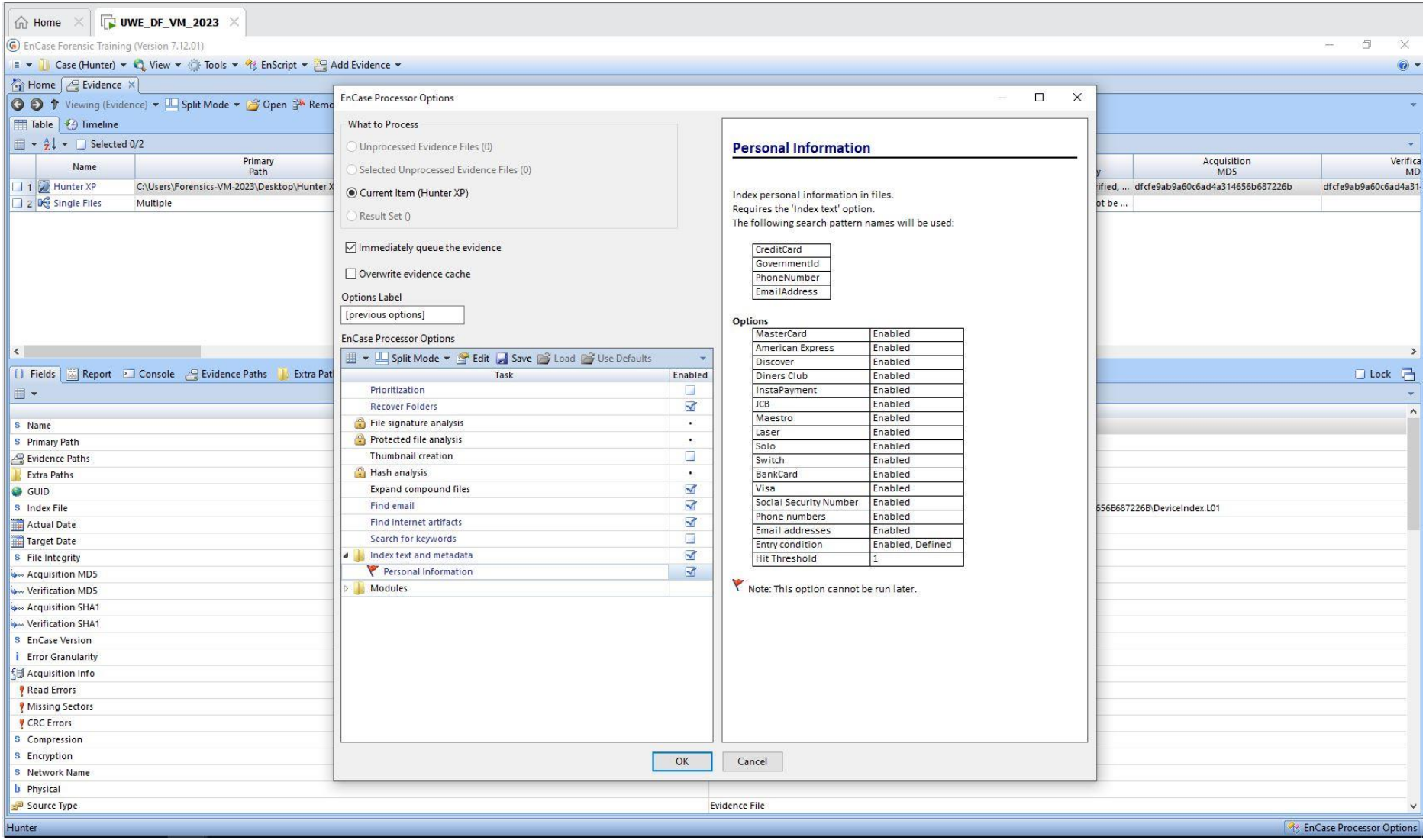

Home
UWE_DF_VM_2023
EnCase Forensic Training (Version 7.12.01)
Case (Hunter)
View
Tools
EnScript
Add Evidence
Evidence
Viewing (Evidence)
Split Mode
Open
Table
Timeline
Selected 0/2
Name
Primary Path
Hunter XP
C:\Users\Forensics-VM-2023\Desktop\Hunter X
Single Files
Multiple
Acquisition MD5
dfcfe9ab9a60c6ad4a314656b687226b
Fields
Report
Console
Evidence Paths
Extra Paths
GUID
Index File
Actual Date
Target Date
File Integrity
Acquisition MD5
Verification MD5
Acquisition SHA1
Verification SHA1
EnCase Version
Error Granularity
Acquisition Info
Read Errors
Missing Sectors
CRC Errors
Compression
Encryption
Network Name
Physical
Source Type
Evidence File
Hunter
EnCase Processor Options
What to Process
Unprocessed Evidence Files (0)
Selected Unprocessed Evidence Files (0)
Current Item (Hunter XP)
Result Set ()
Immediately queue the evidence
Overwrite evidence cache
Options Label
[previous options]
EnCase Processor Options
Split Mode
Edit
Save
Load
Use Defaults
Task
Enabled
Prioritization
Recover Folders
File signature analysis
Protected file analysis
Thumbnail creation
Hash analysis
Expand compound files
Find email
Find Internet artifacts
Search for keywords
Index text and metadata
Personal Information
Modules
OK
Cancel
Personal Information
Index personal information in files.
Requires the 'Index text' option.
The following search pattern names will be used:
CreditCard
GovernmentId
PhoneNumber
EmailAddress
Options
MasterCard Enabled
American Express Enabled
Discover Enabled
Diners Club Enabled
InstaPayment Enabled
JCB Enabled
Maestro Enabled
Laser Enabled
Solo Enabled
Switch Enabled
BankCard Enabled
Visa Enabled
Social Security Number Enabled
Phone numbers Enabled
Email addresses Enabled
Entry condition Enabled, Defined
Hit Threshold 1
Note: This option cannot be run later.

Figure 50:

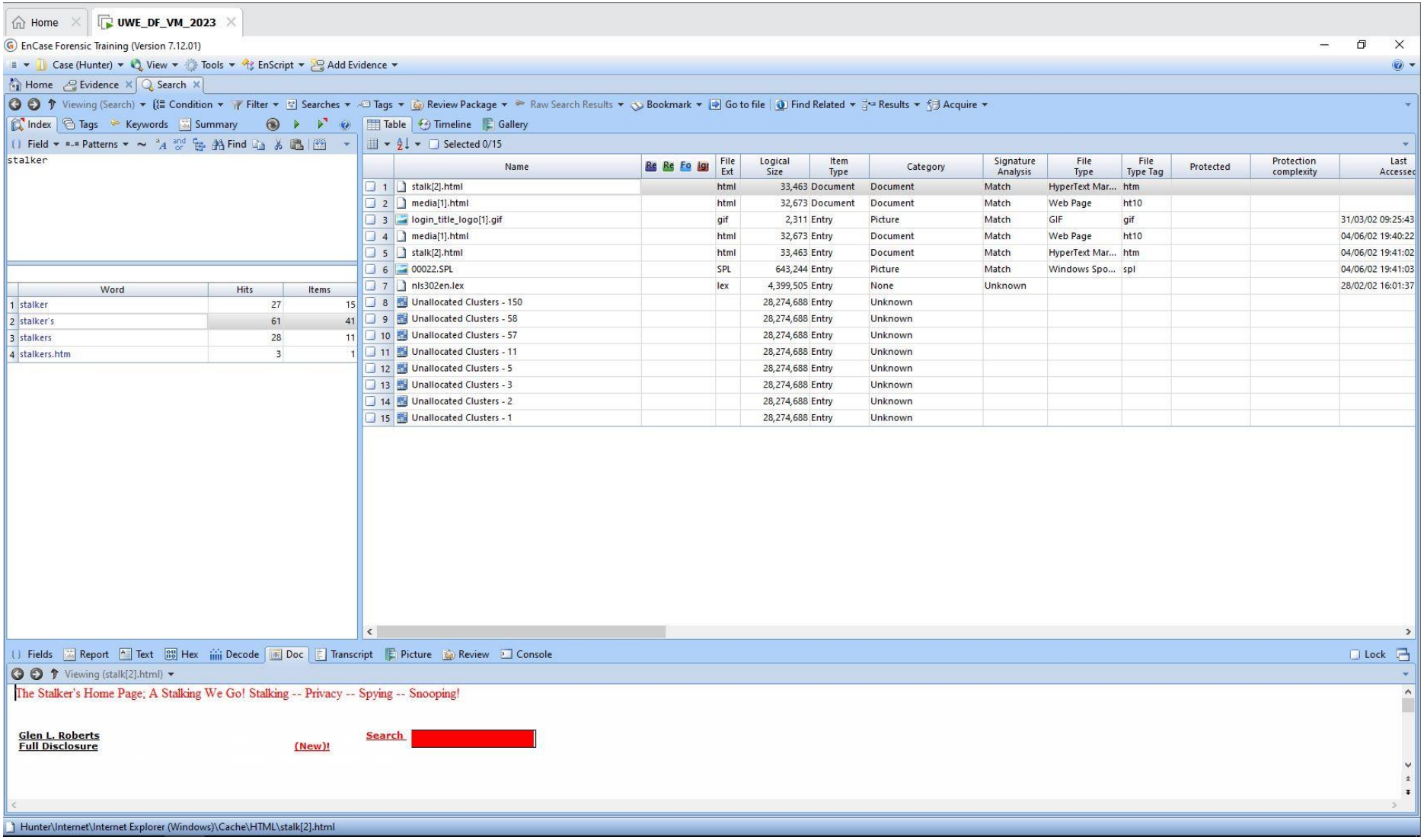

Home
UWE_DF_VM_2023
EnCase Forensic Training (Version 7.12.01)
Case (Hunter) View Tools EnScript Add Evidence
Home Evidence Search
Viewing (Search) Condition Filter Searches Tags Review Package Raw Search Results Bookmark Go to file Find Related Results Acquire
Index Tags Keywords Summary
Table Timeline Gallery
Field Patterns Find
Selected 0/15
stalker
Word Hits Items
1 stalker 27 15
2 stalker's 61 41
3 stalkers 28 11
4 stalkers.htm 3 1
Name File Ext Logical Size Item Type Category Signature Analysis File Type File Type Tag Protected Protection complexity Last Accessed
1 stalk[2].html html 33,463 Document Document Match HyperText Mar... htm
2 media[1].html html 32,673 Document Document Match Web Page ht10
3 login_title_logo[1].gif gif 2,311 Entry Picture Match GIF gif 31/03/02 09:25:43
4 media[1].html html 32,673 Entry Document Match Web Page ht10 04/06/02 19:40:22
5 stalk[2].html html 33,463 Entry Document Match HyperText Mar... htm 04/06/02 19:41:02
6 00022.SPL SPL 643,244 Entry Picture Match Windows Spo... spl 04/06/02 19:41:03
7 nls302en.lex lex 4,399,505 Entry None Unknown 28/02/02 16:01:37
8 Unallocated Clusters - 150 28,274,688 Entry Unknown
9 Unallocated Clusters - 58 28,274,688 Entry Unknown
10 Unallocated Clusters - 57 28,274,688 Entry Unknown
11 Unallocated Clusters - 11 28,274,688 Entry Unknown
12 Unallocated Clusters - 5 28,274,688 Entry Unknown
13 Unallocated Clusters - 3 28,274,688 Entry Unknown
14 Unallocated Clusters - 2 28,274,688 Entry Unknown
15 Unallocated Clusters - 1 28,274,688 Entry Unknown
Fields Report Text Hex Decode Doc Transcript Picture Review Console
Lock
Viewing (stalk[2].html)
The Stalker's Home Page; A Stalking We Go! Stalking -- Privacy -- Spying -- Snooping!
Glen L. Roberts
Full Disclosure
(New)!
Search
Hunter\Internet\Internet Explorer (Windows)\Cache\HTML\stalk[2].html

Figure 51:

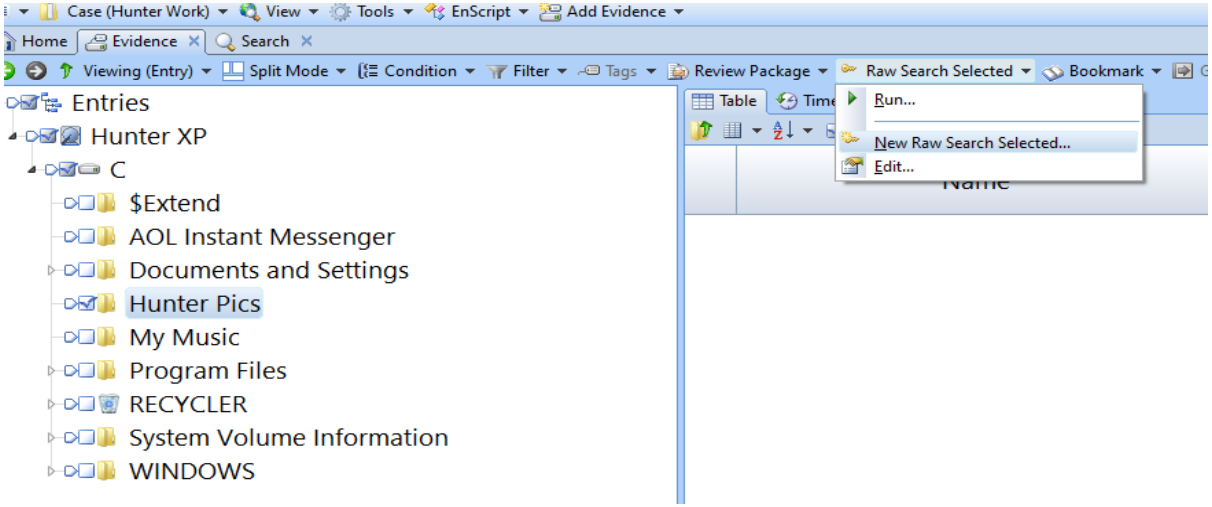
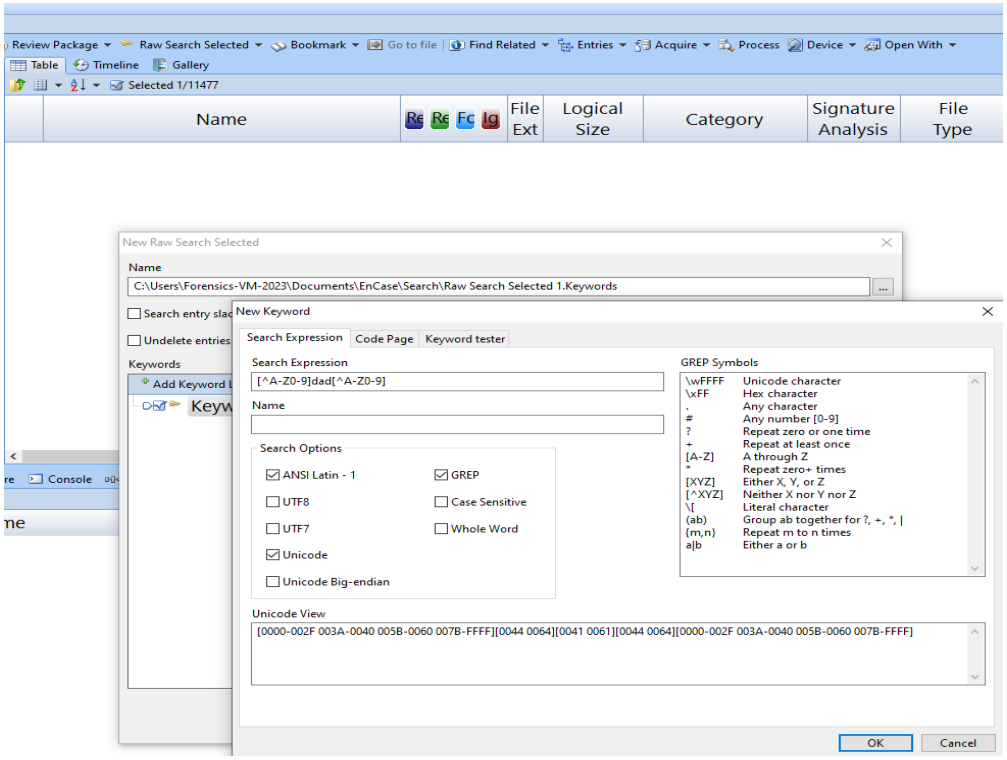

Case (Hunter Work)
View
Tools
EnScript
Add Evidence
Home
Evidence
Search
Viewing (Entry)
Split Mode
Condition
Filter
Tags
Review Package
Raw Search Selected
Bookmark
Table
Run...
New Raw Search Selected...
Edit...
Entries
Hunter XP
C
$Extend
AOL Instant Messenger
Documents and Settings
Hunter Pics
My Music
Program Files
RECYCLER
System Volume Information
WINDOWS

Figure 52:


Review Package
Raw Search Selected
Bookmark
Go to file
Find Related
Entries
Acquire
Process
Device
Open With
Table
Timeline
Gallery
Selected 1/11477
Name
File Ext
Logical Size
Category
Signature Analysis
File Type
New Raw Search Selected
Name
C:\Users\Forensics-VM-2023\Documents\EnCase\Search\Raw Search Selected 1.Keywords
Search entry slac
Undelete entries
Keywords
Add Keyword
Keyw
Console
ne
New Keyword
Search Expression
Code Page
Keyword tester
Search Expression
[^A-Z0-9]dad[^A-Z0-9]
Name
Search Options
ANSI Latin - 1
UTF8
UTF7
Unicode
Unicode Big-endian
GREP
Case Sensitive
Whole Word
GREP Symbols
\wFFFF Unicode character
\xFF Hex character
. Any character
Any number [0-9]
? Repeat zero or one time
+ Repeat at least once
[A-Z] A through Z
* Repeat zero+ times
[XYZ] Either X, Y, or Z
[^XYZ] Neither X nor Y nor Z
\[Literal character
(ab) Group ab together for ?, +, *, |
{m,n} Repeat m to n times
a|b Either a or b
Unicode View
[0000-002F 003A-0040 005B-0060 007B-FFFF][0044 0064][0041 0061][0044 0064][0000-002F 003A-0040 005B-0060 007B-FFFF]
OK
Cancel

Recover Log-On Passwords :

Figure 53:

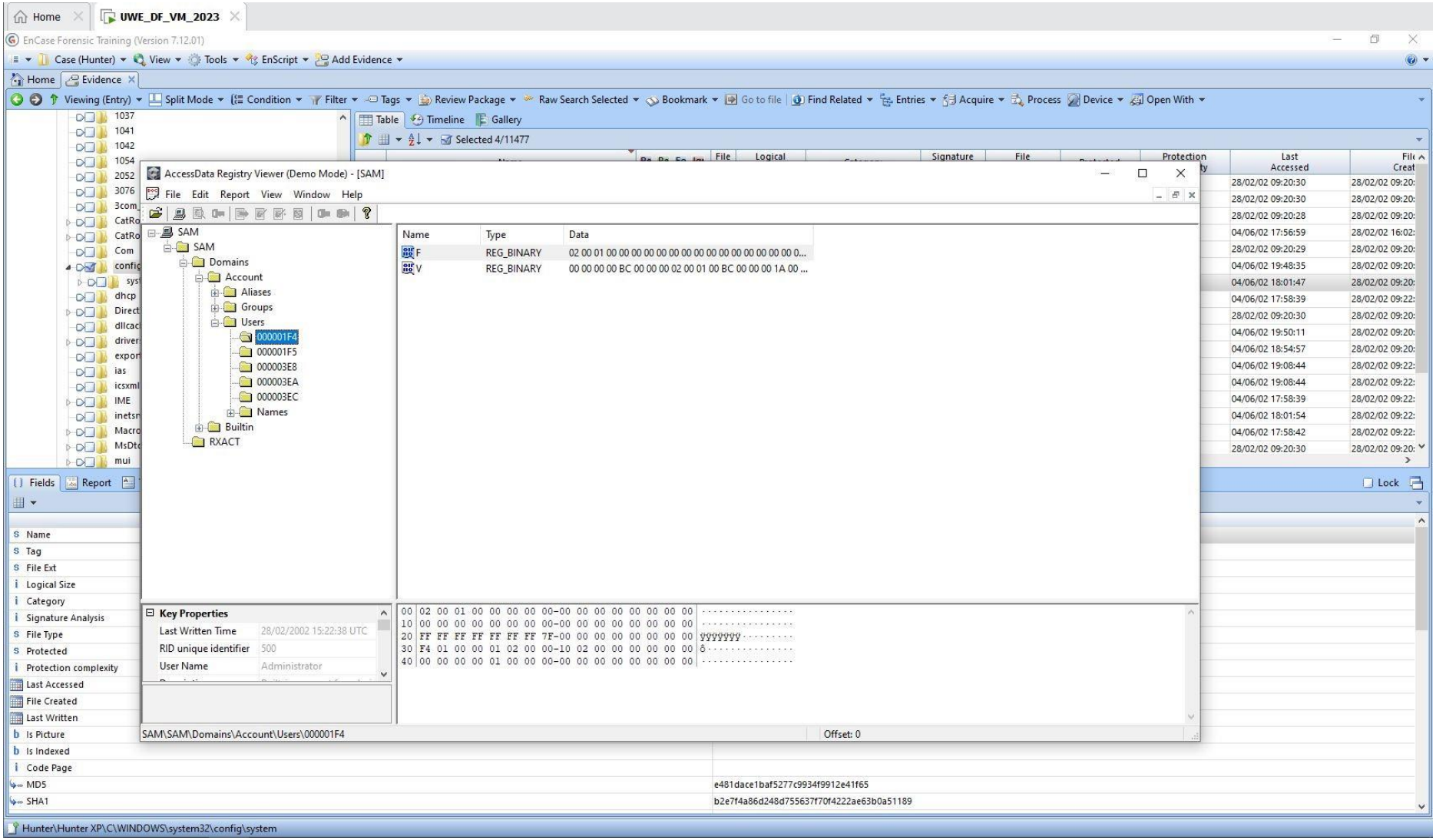
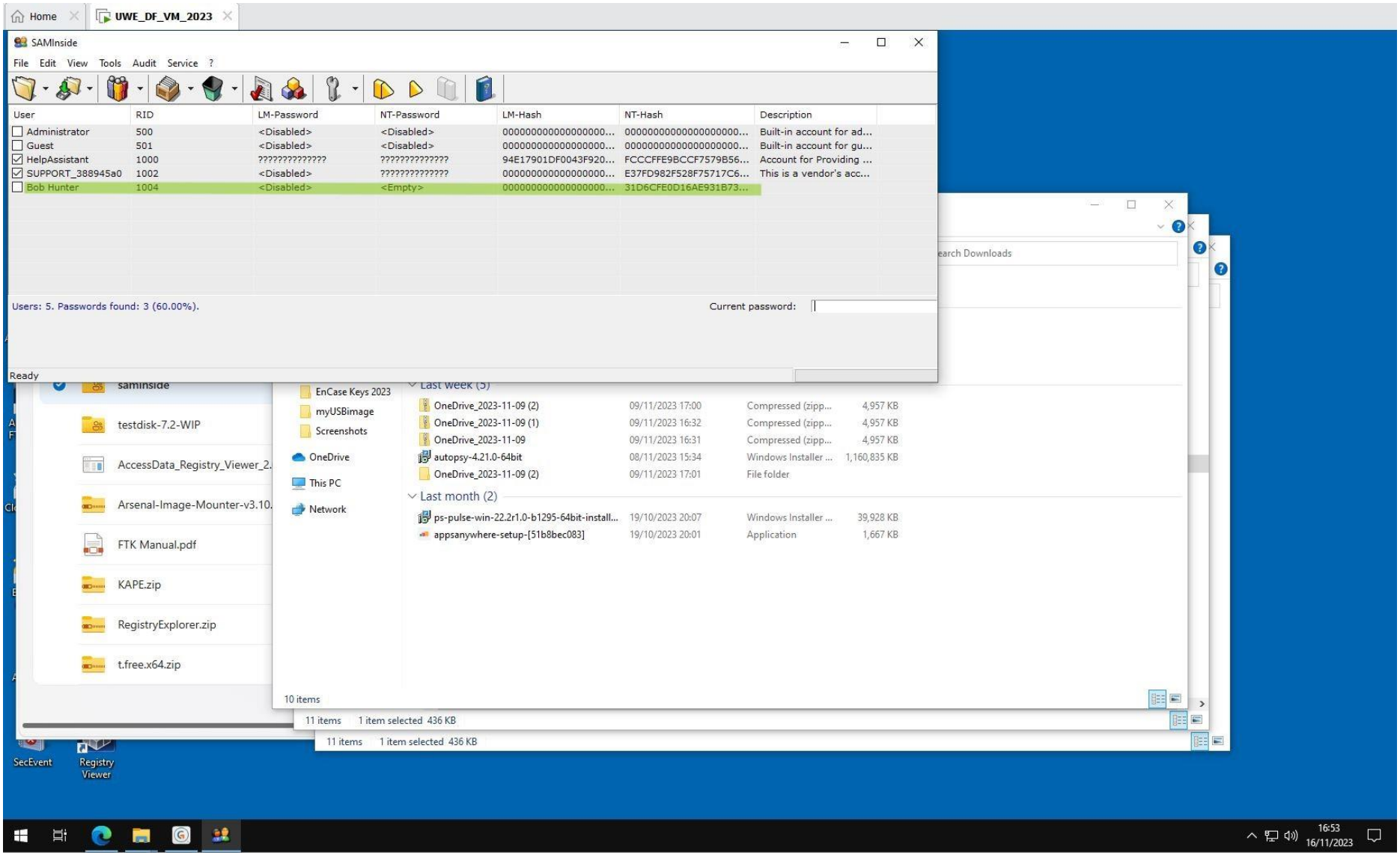
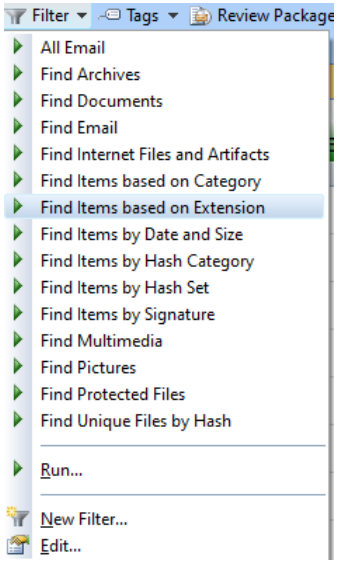


Figure 54:


Home
UWE_DF_VM_2023
SAMInside
File Edit View Tools Audit Service ?
User RID LM-Password NT-Password LM-Hash NT-Hash Description
Administrator 500 <Disabled> <Disabled> 00000000000000000... 00000000000000000000... Built-in account for ad...
Guest 501 <Disabled> <Disabled> 00000000000000000... 00000000000000000000... Built-in account for gu...
HelpAssistant 1000 ?????????????? ?????????????? 94E17901DF0043F920... FCCCFFE9BCCF7579B56... Account for Providing ...
SUPPORT_388945a0 1002 <Disabled> ?????????????? 00000000000000000... E37FD982F528F75717C6... This is a vendor's acc...
Bob Hunter 1004 <Disabled> <Empty> 00000000000000000... 31D6CFE0D16AE931B73...
Users: 5. Passwords found: 3 (60.00%).
Current password:
Ready
saminside
testdisk-7.2-WIP
AccessData_Registry_Viewer_2...
Arsenal-Image-Mounter-v3.10...
FTK Manual.pdf
KAPE.zip
RegistryExplorer.zip
t.free.x64.zip
EnCase Keys 2023
myUSBimage
Screenshots
OneDrive
This PC
Network
Last week (3)
OneDrive_2023-11-09 (2) 09/11/2023 17:00 Compressed (zipp... 4,957 KB
OneDrive_2023-11-09 (1) 09/11/2023 16:32 Compressed (zipp... 4,957 KB
OneDrive_2023-11-09 09/11/2023 16:31 Compressed (zipp... 4,957 KB
autopsy-4.21.0-64bit 08/11/2023 15:34 Windows Installer ... 1,160,835 KB
OneDrive_2023-11-09 (2) 09/11/2023 17:01 File folder
Last month (2)
ps-pulse-win-22.2r1.0-b1295-64bit-install... 19/10/2023 20:07 Windows Installer ... 39,928 KB
appsanywhere-setup-[51b8bec083] 19/10/2023 20:01 Application 1,667 KB
10 items
11 items 1 item selected 436 KB
11 items 1 item selected 436 KB
SecEvent
Registry Viewer
16:53
16/11/2023

Examine Different File Types :

Figure 55 :



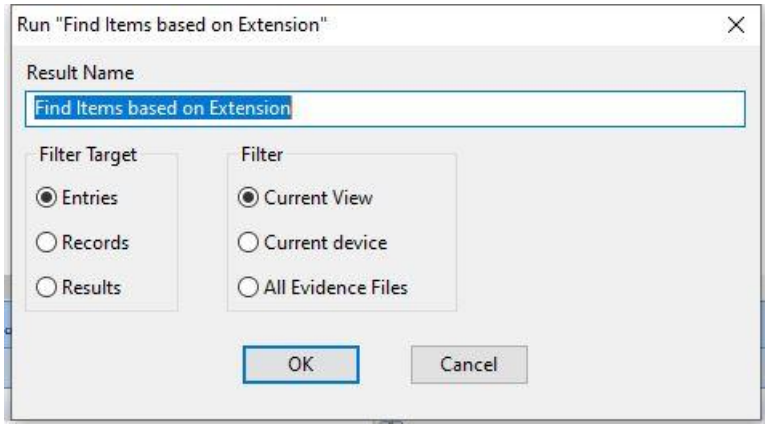


Figure 56 :

	Name	Comment	Start Sector	Sector offset	File Offset	Length				File Ext	Logical Size	Item Type	Category	Signatur Analysis	File Type	File Type Ta	Protected
1	102-0283_IMG[1].jpg		238,155	0						j...	3,044	Entry	Picture	Match	JPEG Im...	jpg1	
2	realplay.exe		1,887,0...							e...	26,112	Entry	Executable	Match	Windo...	exe	
3	cleanmgr.exe		195,707							e...	61,440	Entry	Executable	Match	Windo...	exe	

Encryption :

Figure 57 :

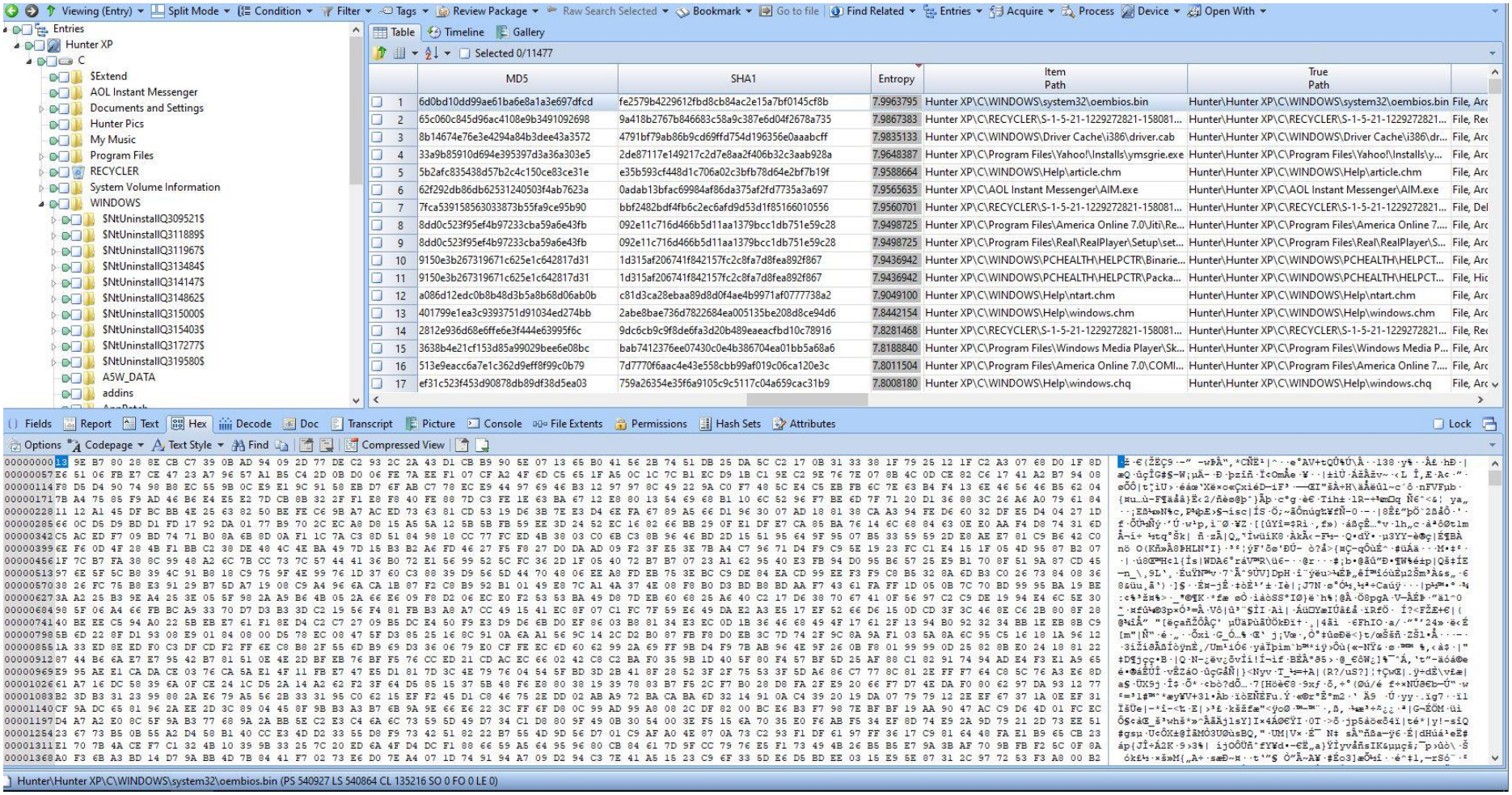
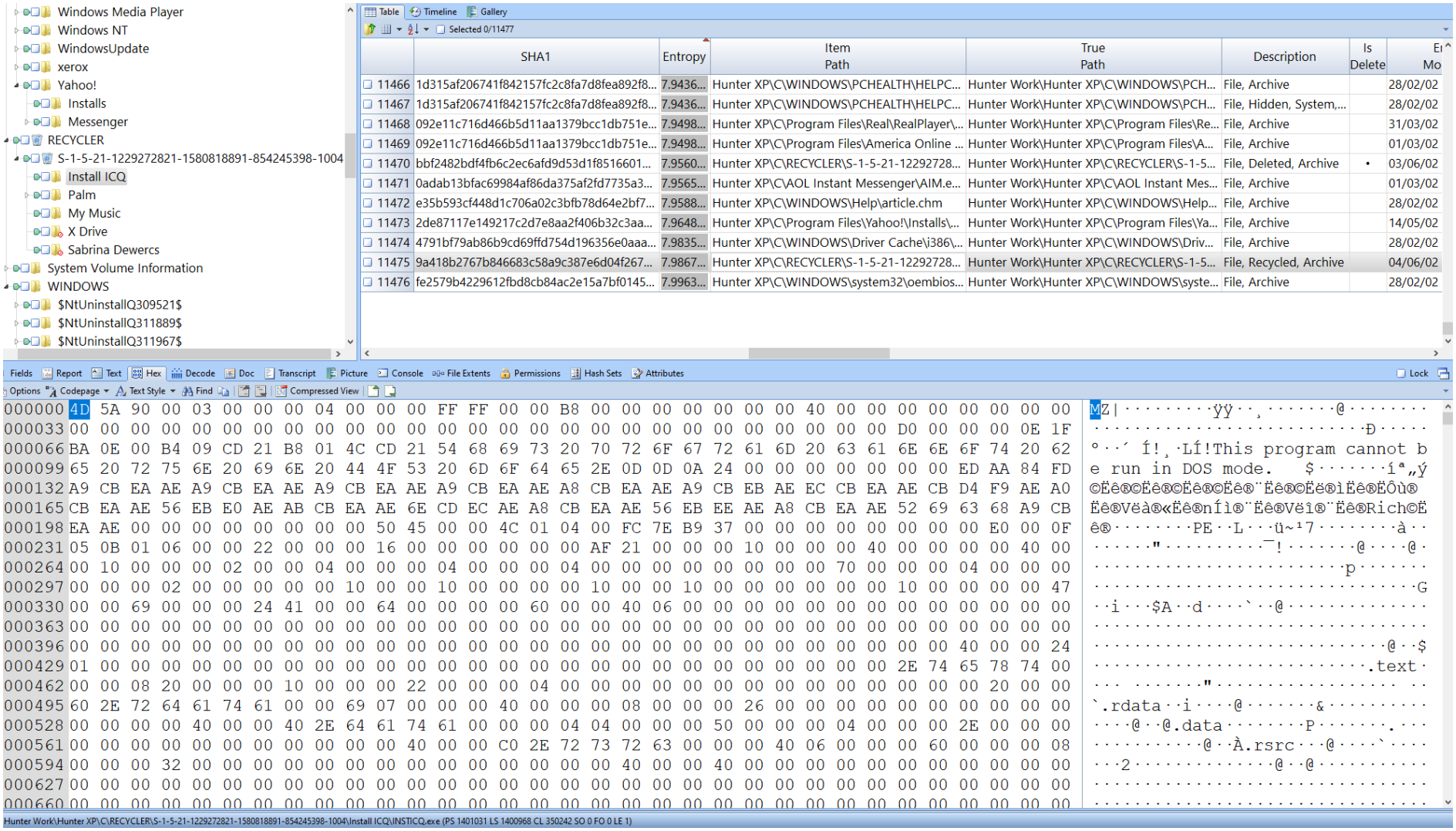


Figure 58 :


Windows Media Player
Windows NT
WindowsUpdate
xerox
Yahoo!
Installs
Messenger
RECYCLER
S-1-5-21-1229272821-1580818891-854245398-1004
Install ICQ
Palm
My Music
X Drive
Sabrina Dewercs
System Volume Information
WINDOWS
$NtUninstallQ309521$
$NtUninstallQ311889$
$NtUninstallQ311967$
Table
Timeline
Gallery
Selected 0/11477
SHA1
Entropy
Item Path
True Path
Description
Is Delete
11466 1d315af206741f842157fc2c8fa7d8fea892f8... 7.9436... Hunter XP\C\WINDOWS\PCHEALTH\HELPC... Hunter Work\Hunter XP\C\WINDOWS\PCH... File, Archive 28/02/02
11467 1d315af206741f842157fc2c8fa7d8fea892f8... 7.9436... Hunter XP\C\WINDOWS\PCHEALTH\HELPC... Hunter Work\Hunter XP\C\WINDOWS\PCH... File, Hidden, System,... 28/02/02
11468 092e11c716d466b5d11aa1379bcc1db751e... 7.9498... Hunter XP\C\Program Files\Real\RealPlayer\... Hunter Work\Hunter XP\C\Program Files\Re... File, Archive 31/03/02
11469 092e11c716d466b5d11aa1379bcc1db751e... 7.9498... Hunter XP\C\Program Files\America Online ... Hunter Work\Hunter XP\C\Program Files\A... File, Archive 01/03/02
11470 bbf2482bdf4fb6c2ec6afd9d53d1f8516601... 7.9560... Hunter XP\C\RECYCLER\S-1-5-21-12292728... Hunter Work\Hunter XP\C\RECYCLER\S-1-5... File, Deleted, Archive • 03/06/02
11471 0adab13bfac69984af86da375af2fd7735a3... 7.9565... Hunter XP\C\AOL Instant Messenger\AIM.e... Hunter Work\Hunter XP\C\AOL Instant Mes... File, Archive 01/03/02
11472 e35b593cf448d1c706a02c3bfb78d64e2bf7... 7.9588... Hunter XP\C\WINDOWS\Help\article.chm Hunter Work\Hunter XP\C\WINDOWS\Help... File, Archive 28/02/02
11473 2de87117e149217c2d7e8aa2f406b32c3aa... 7.9648... Hunter XP\C\Program Files\Yahoo!\Installs\... Hunter Work\Hunter XP\C\Program Files\Ya... File, Archive 14/05/02
11474 4791bf79ab86b9cd69ffd754d196356e0aaa... 7.9835... Hunter XP\C\WINDOWS\Driver Cache\i386\... Hunter Work\Hunter XP\C\WINDOWS\Driv... File, Archive 28/02/02
11475 9a418b2767b846683c58a9c387e6d04f267... 7.9867... Hunter XP\C\RECYCLER\S-1-5-21-12292728... Hunter Work\Hunter XP\C\RECYCLER\S-1-5... File, Recycled, Archive 04/06/02
11476 fe2579b4229612fbd8cb84ac2e15a7bf0145... 7.9963... Hunter XP\C\WINDOWS\system32\oembios... Hunter Work\Hunter XP\C\WINDOWS\syste... File, Archive 28/02/02
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Console
File Extents
Permissions
Hash Sets
Attributes
Lock
Options
Codepage
Text Style
Find
Compressed View
000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
000033 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 D0 00 00 00
000066 BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20
000099 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 ED AA 84
000132 A9 CB EA AE A9 CB EA AE A9 CB EA AE A9 CB EA AE A8 CB EA AE A9 CB EB AE EC CB EA AE CB D4 F9 AE
000165 CB EA AE 56 EB E0 AE AB CB EA AE 6E CD EC AE A8 CB EA AE 56 EB EE AE A8 CB EA AE 52 69 63 68 A9
000198 EA AE 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 FC 7E B9 37 00 00 00 00 00 00 00 00 E0 00
000231 05 0B 01 06 00 00 22 00 00 00 16 00 00 00 00 00 00 AF 21 00 00 00 10 00 00 00 40 00 00 00 00 40
000264 00 10 00 00 00 02 00 00 04 00 00 00 04 00 00 00 04 00 00 00 00 00 00 00 00 70 00 00 00 04 00 00
000297 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00
000330 00 00 69 00 00 00 24 41 00 00 64 00 00 00 00 60 00 00 40 06 00 00 00 00 00 00 00 00 00 00 00 00
000363 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000396 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00
000429 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2E 74 65 78 74
000462 00 00 08 20 00 00 00 10 00 00 00 22 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00
000495 60 2E 72 64 61 74 61 00 00 69 07 00 00 00 40 00 00 00 08 00 00 00 26 00 00 00 00 00 00 00 00 00
000528 00 00 00 00 40 00 00 40 2E 64 61 74 61 00 00 00 04 04 00 00 00 50 00 00 00 04 00 00 00 2E 00 00
000561 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0 2E 72 73 72 63 00 00 00 40 06 00 00 00 60 00 00 08
000594 00 00 00 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00
000627 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000660 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
MZ
This program cannot be run in DOS mode.
.text
.rdata
.data
.rsrc
Hunter Work\Hunter XP\C\RECYCLER\S-1-5-21-1229272821-1580818891-854245398-1004\Install ICQ\INSTICQ.exe (PS 1401031 LS 1400968 CL 350242 SO 0 FO 0 LE 1)

Print Artefacts :

Figure 59:

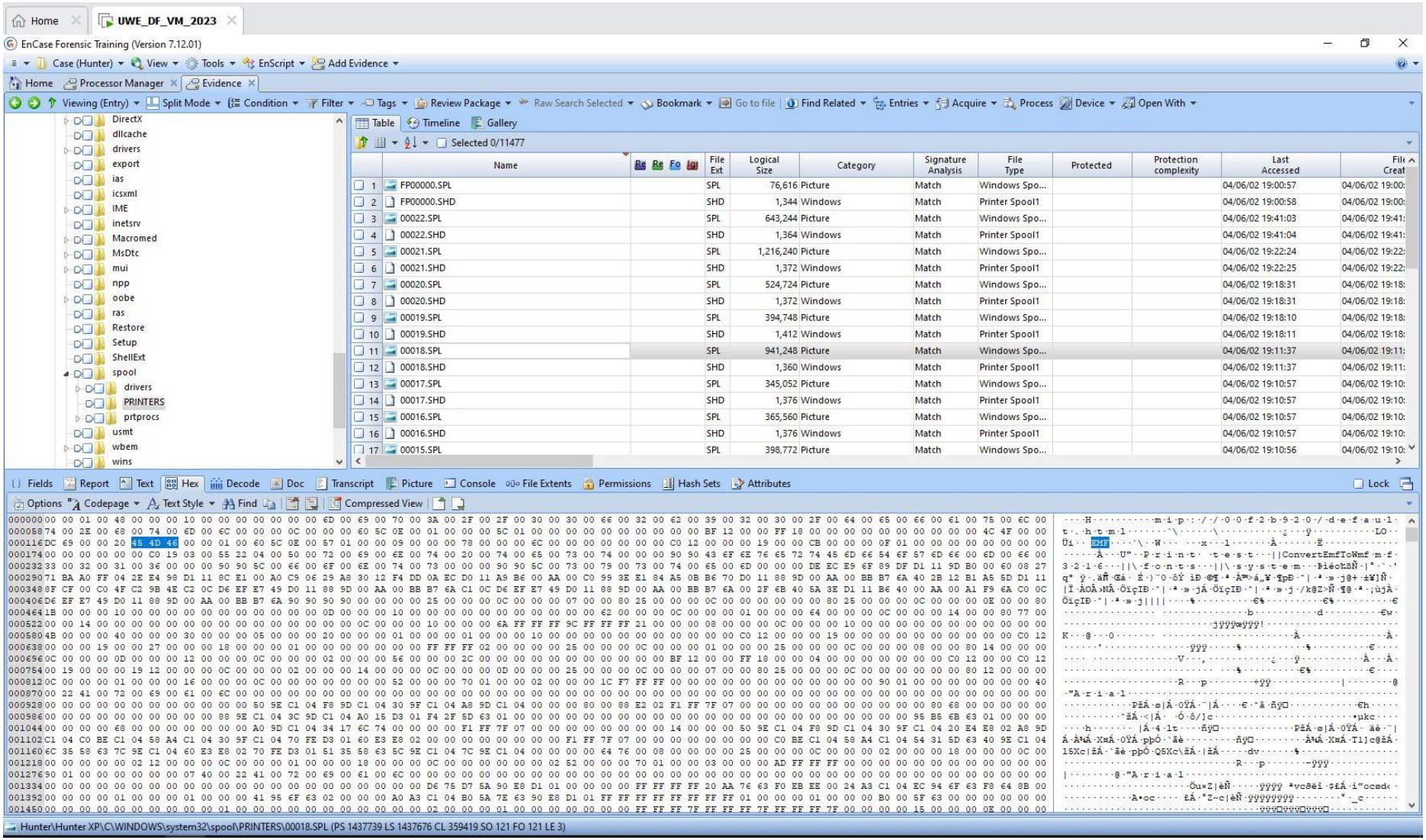


Figure 60:

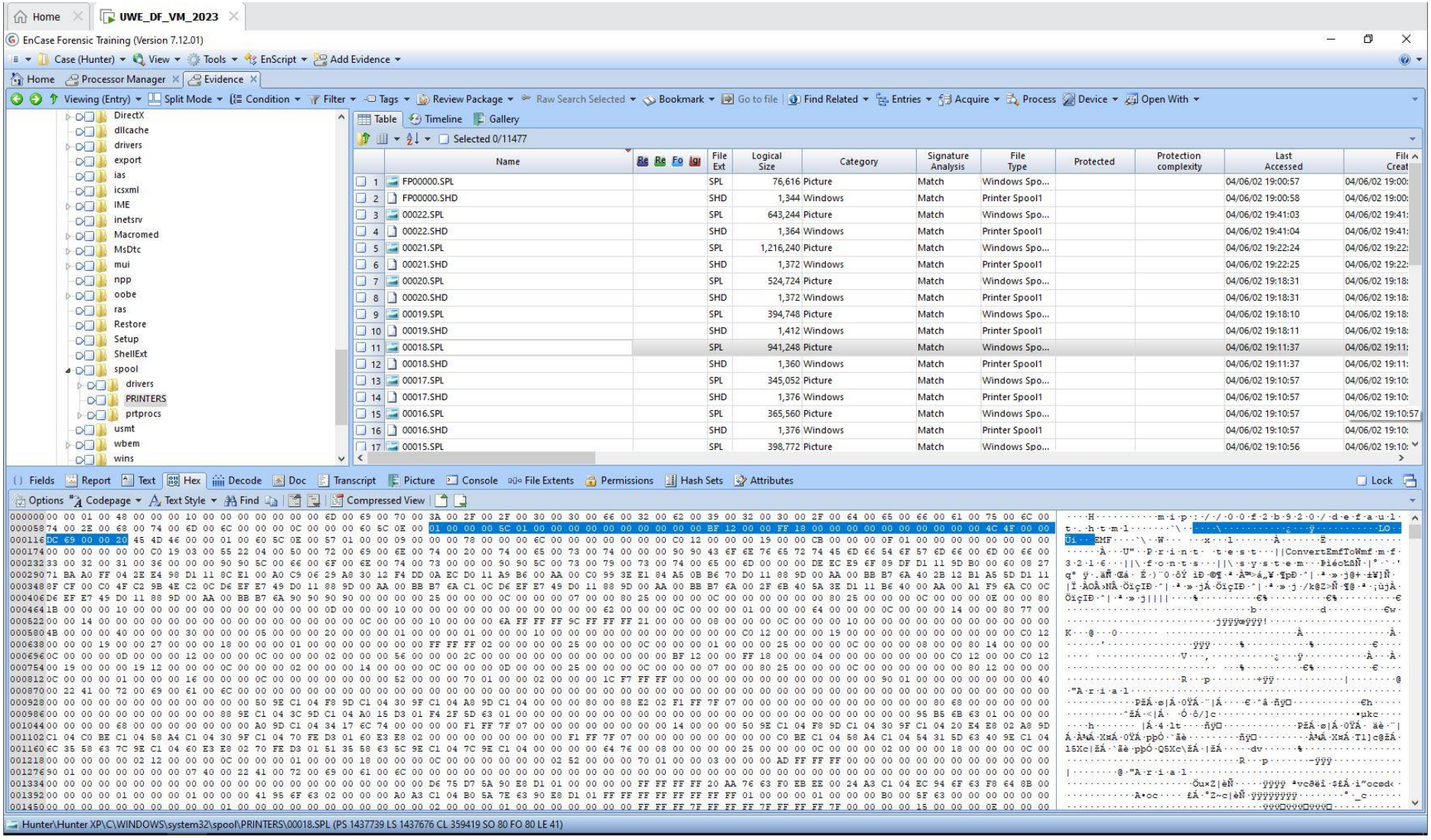

Home
UWE_DF_VM_2023
EnCase Forensic Training (Version 7.12.01)
Case (Hunter)
View
Tools
EnScript
Add Evidence
Processor Manager
Evidence
Viewing (Entry)
Split Mode
Condition
Filter
Tags
Review Package
Raw Search Selected
Bookmark
Go to file
Find Related
Entries
Acquire
Process
Device
Open With
Table
Timeline
Gallery
Selected 0/11477
Name
File Ext
Logical Size
Category
Signature Analysis
File Type
Protected
Protection complexity
Last Accessed
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Console
File Extents
Permissions
Hash Sets
Attributes
Lock
Options
Codepage
Text Style
Find
Compressed View
Hunter\Hunter XP\C\WINDOWS\system32\spool\PRINTERS\00018.SPL (PS 1437739 LS 1437676 CL 359419 SO 80 FO 80 LE 41)

Figure 61:

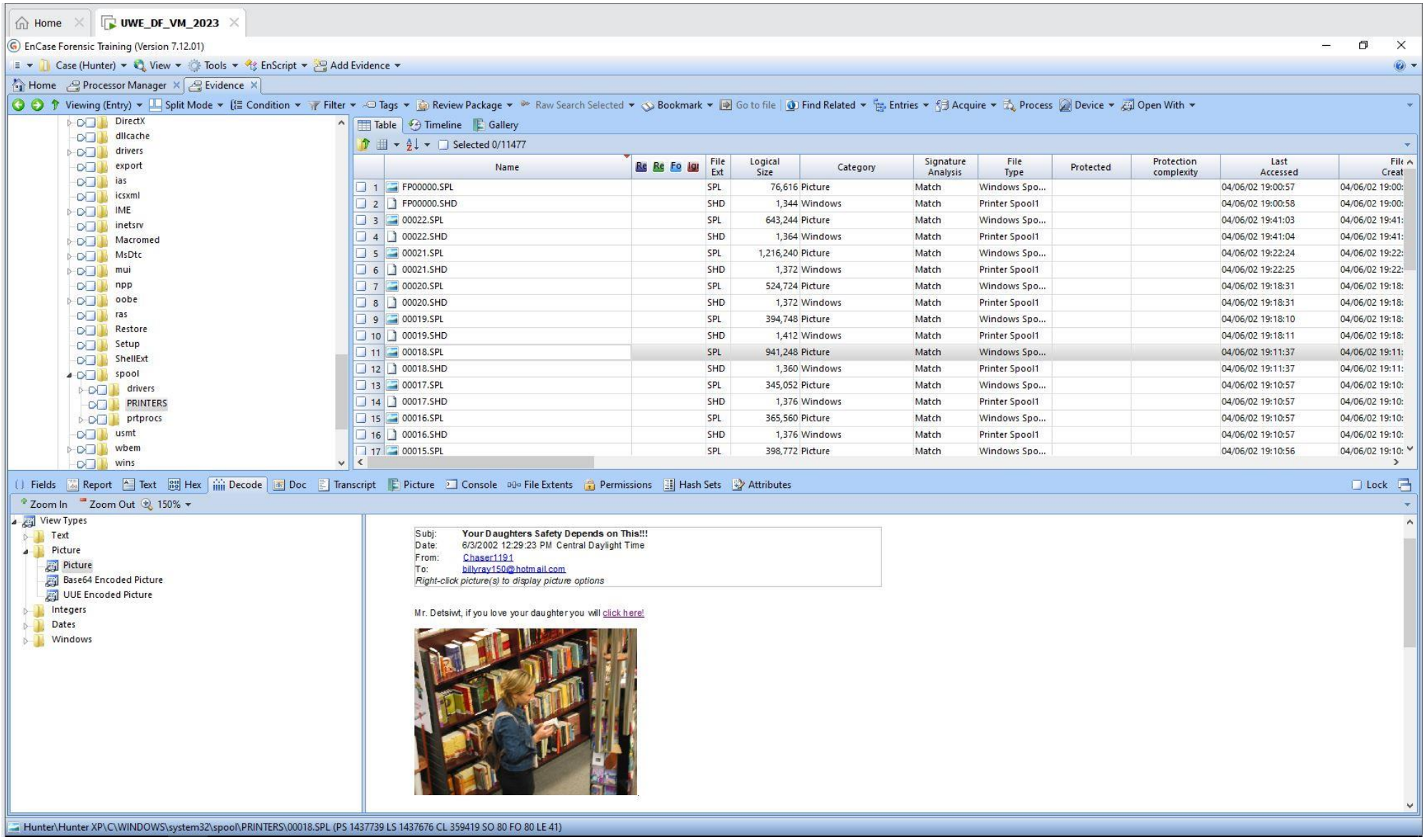
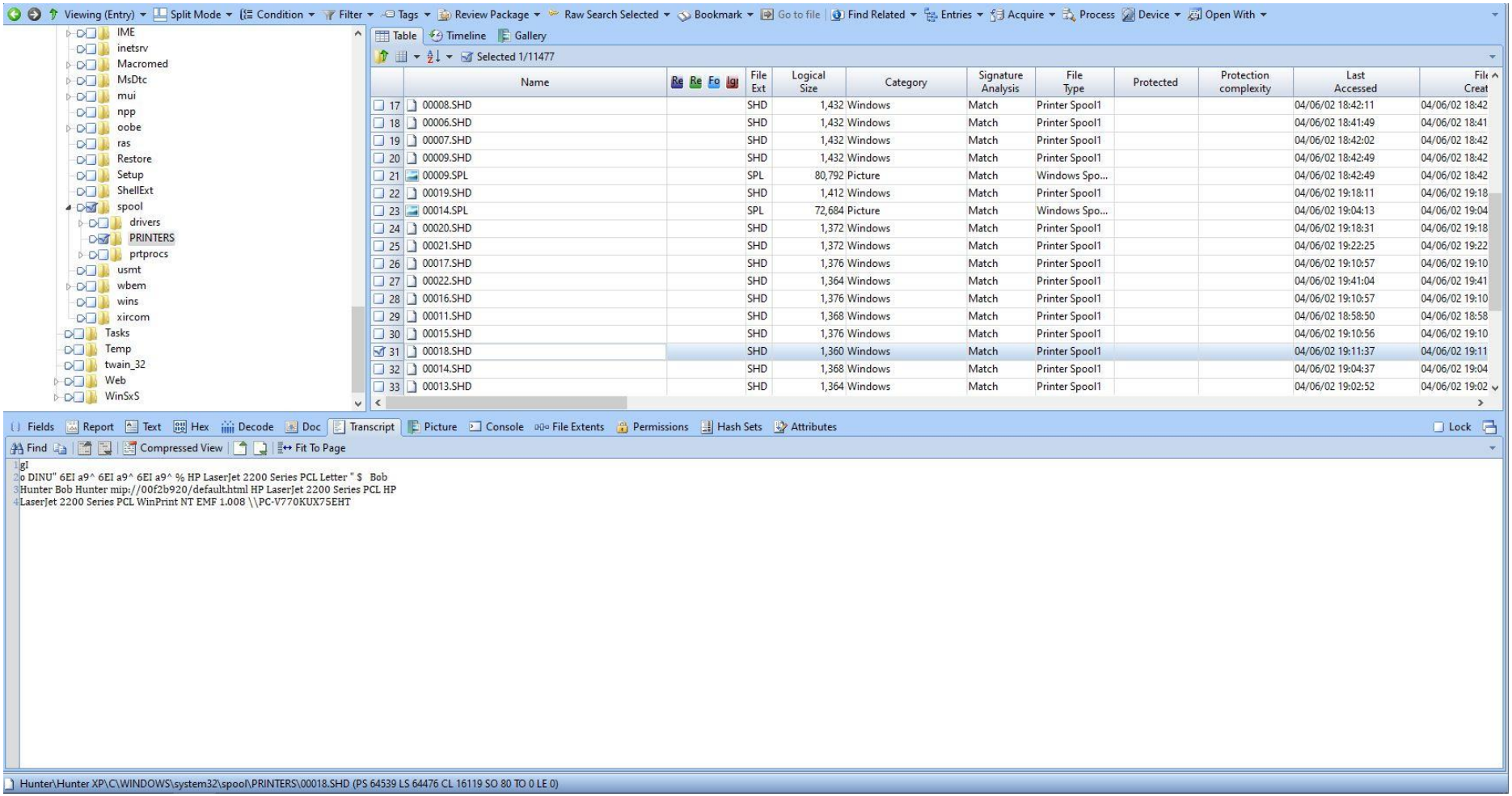
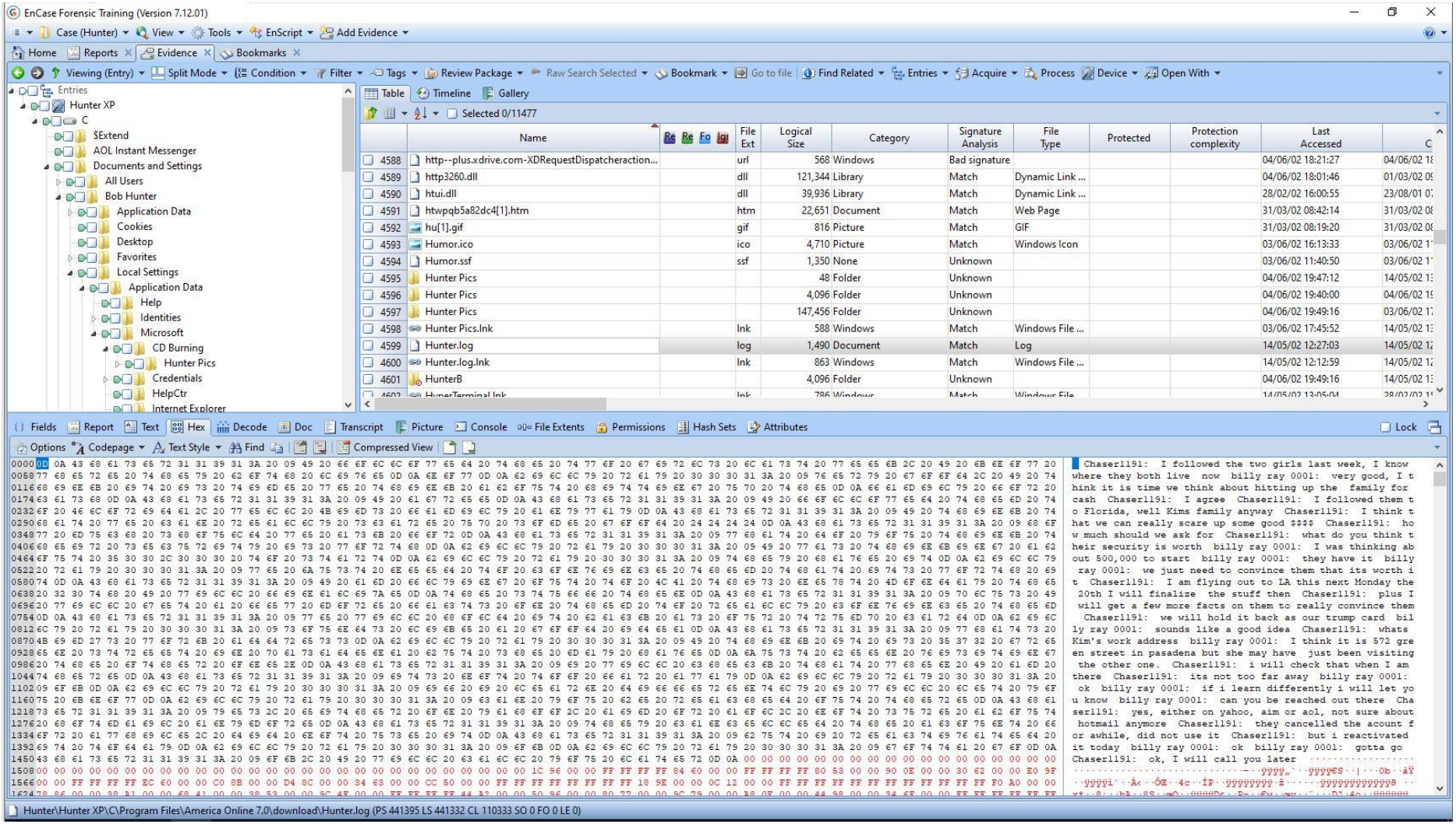

Home
UWE_DF_VM_2023
EnCase Forensic Training (Version 7.12.01)
Case (Hunter)
View
Tools
EnScript
Add Evidence
Processor Manager
Evidence
Viewing (Entry)
Split Mode
Condition
Filter
Tags
Review Package
Raw Search Selected
Bookmark
Go to file
Find Related
Entries
Acquire
Process
Device
Open With
Table
Timeline
Gallery
Selected 0/11477
Name
File Ext
Logical Size
Category
Signature Analysis
File Type
Protected
Protection complexity
Last Accessed
1 FP00000.SPL SPL 76,616 Picture Match Windows Spo... 04/06/02 19:00:57
2 FP00000.SHD SHD 1,344 Windows Match Printer Spool1 04/06/02 19:00:58
3 00022.SPL SPL 643,244 Picture Match Windows Spo... 04/06/02 19:41:03
4 00022.SHD SHD 1,364 Windows Match Printer Spool1 04/06/02 19:41:04
5 00021.SPL SPL 1,216,240 Picture Match Windows Spo... 04/06/02 19:22:24
6 00021.SHD SHD 1,372 Windows Match Printer Spool1 04/06/02 19:22:25
7 00020.SPL SPL 524,724 Picture Match Windows Spo... 04/06/02 19:18:31
8 00020.SHD SHD 1,372 Windows Match Printer Spool1 04/06/02 19:18:31
9 00019.SPL SPL 394,748 Picture Match Windows Spo... 04/06/02 19:18:10
10 00019.SHD SHD 1,412 Windows Match Printer Spool1 04/06/02 19:18:11
11 00018.SPL SPL 941,248 Picture Match Windows Spo... 04/06/02 19:11:37
12 00018.SHD SHD 1,360 Windows Match Printer Spool1 04/06/02 19:11:37
13 00017.SPL SPL 345,052 Picture Match Windows Spo... 04/06/02 19:10:57
14 00017.SHD SHD 1,376 Windows Match Printer Spool1 04/06/02 19:10:57
15 00016.SPL SPL 365,560 Picture Match Windows Spo... 04/06/02 19:10:57
16 00016.SHD SHD 1,376 Windows Match Printer Spool1 04/06/02 19:10:57
17 00015.SPL SPL 398,772 Picture Match Windows Spo... 04/06/02 19:10:56
DirectX
dllcache
drivers
export
ias
icsxml
IME
inetsrv
Macromed
MsDtc
mui
npp
oobe
ras
Restore
Setup
ShellExt
spool
drivers
PRINTERS
prtprocs
usmt
wbem
wins
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Console
File Extents
Permissions
Hash Sets
Attributes
Lock
Zoom In
Zoom Out
150%
View Types
Text
Picture
Picture
Base64 Encoded Picture
UUE Encoded Picture
Integers
Dates
Windows
Subj: Your Daughters Safety Depends on This!!!
Date: 6/3/2002 12:29:23 PM Central Daylight Time
From: Chaser1191
To: billyray150@hotmail.com
Right-click picture(s) to display picture options
Mr. Detsiwt, if you love your daughter you will click here!
Hunter\Hunter XP\C\WINDOWS\system32\spool\PRINTERS\00018.SPL (PS 1437739 LS 1437676 CL 359419 SO 80 FO 80 LE 41)

Figure 62:


Viewing (Entry)
Split Mode
Condition
Filter
Tags
Review Package
Raw Search Selected
Bookmark
Go to file
Find Related
Entries
Acquire
Process
Device
Open With
IME
inetsrv
Macromed
MsDtc
mui
npp
oobe
ras
Restore
Setup
ShellExt
spool
drivers
PRINTERS
prtprocs
usmt
wbem
wins
xircom
Tasks
Temp
twain_32
Web
WinSxS
Table
Timeline
Gallery
Selected 1/11477
Name
File Ext
Logical Size
Category
Signature Analysis
File Type
Protected
Protection complexity
Last Accessed
17 00008.SHD SHD 1,432 Windows Match Printer Spool1 04/06/02 18:42:11 04/06/02 18:42
18 00006.SHD SHD 1,432 Windows Match Printer Spool1 04/06/02 18:41:49 04/06/02 18:41
19 00007.SHD SHD 1,432 Windows Match Printer Spool1 04/06/02 18:42:02 04/06/02 18:42
20 00009.SHD SHD 1,432 Windows Match Printer Spool1 04/06/02 18:42:49 04/06/02 18:42
21 00009.SPL SPL 80,792 Picture Match Windows Spo... 04/06/02 18:42:49 04/06/02 18:42
22 00019.SHD SHD 1,412 Windows Match Printer Spool1 04/06/02 19:18:11 04/06/02 19:18
23 00014.SPL SPL 72,684 Picture Match Windows Spo... 04/06/02 19:04:13 04/06/02 19:04
24 00020.SHD SHD 1,372 Windows Match Printer Spool1 04/06/02 19:18:31 04/06/02 19:18
25 00021.SHD SHD 1,372 Windows Match Printer Spool1 04/06/02 19:22:25 04/06/02 19:22
26 00017.SHD SHD 1,376 Windows Match Printer Spool1 04/06/02 19:10:57 04/06/02 19:10
27 00022.SHD SHD 1,364 Windows Match Printer Spool1 04/06/02 19:41:04 04/06/02 19:41
28 00016.SHD SHD 1,376 Windows Match Printer Spool1 04/06/02 19:10:57 04/06/02 19:10
29 00011.SHD SHD 1,368 Windows Match Printer Spool1 04/06/02 18:58:50 04/06/02 18:58
30 00015.SHD SHD 1,376 Windows Match Printer Spool1 04/06/02 19:10:56 04/06/02 19:10
31 00018.SHD SHD 1,360 Windows Match Printer Spool1 04/06/02 19:11:37 04/06/02 19:11
32 00014.SHD SHD 1,368 Windows Match Printer Spool1 04/06/02 19:04:37 04/06/02 19:04
33 00013.SHD SHD 1,364 Windows Match Printer Spool1 04/06/02 19:02:52 04/06/02 19:02
Fields
Report
Text
Hex
Decode
Doc
Transcript
Picture
Console
File Extents
Permissions
Hash Sets
Attributes
Lock
Find
Compressed View
Fit To Page
1 gI
2 o DINU" 6EI a9^ 6EI a9^ 6EI a9^ % HP LaserJet 2200 Series PCL Letter " $ Bob
3 Hunter Bob Hunter mip://00f2b920/default.html HP LaserJet 2200 Series PCL HP
4 LaserJet 2200 Series PCL WinPrint NT EMF 1.008 \\PC-V770KUX75EHT
Hunter\Hunter XP\C\WINDOWS\system32\spool\PRINTERS\00018.SHD (PS 64539 LS 64476 CL 16119 SO 80 TO 0 LE 0)

CD/DVD burning apps:

Figure 63:



Validate Evidence Integrity At The End Of The Examination:

Figure 64:

File Integrity	Completely Verified, 0 Errors
Acquisition MD5	dfcfe9ab9a60c6ad4a314656b687226b
Verification MD5	dfcfe9ab9a60c6ad4a314656b687226b