Lab 2
An Introduction to Forensic Data Analysis

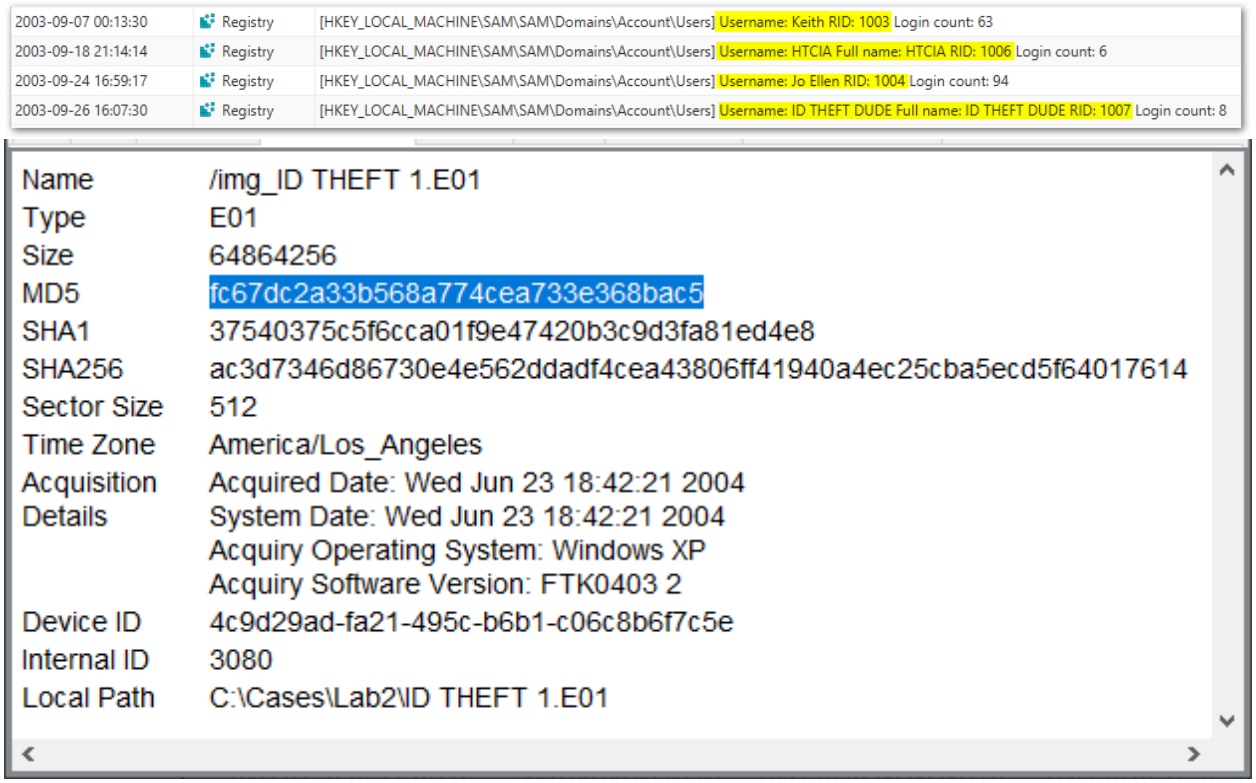
CAL POLY POMONA
CIS 4810-03 GROUP 7

Aaron Robinson
David Flores
Luis Zamudio
Salam Mashal

Part 1

Question 1: Use FTK to create a new case called Lab1. Then add the ID THEFT1.E01image with all processing options except a SHA1hash.

In lieu of FTK, we used Autopsy 4.16.0. For this case, our team created a new folder under C drive called "Cases". Then, we created a folder under "Cases" called "Lab2". The path for this case is C:\Cases\Lab2. To begin our forensic examination we started up Autopsy. We created a new case with the Case Name of "Lab1" with the base directory being "C:\Cases\". We named the Case Number as "001" and the examiner name as "Group 7". To add the data source, we loaded up the image file type of "C:\Cases\LAB2\ID THEFT 1.E01." For the input timezone, we set the local timezone to "America/Los Angeles." In the configure ingest modules tab, we selected all of the ingest modules. We then let Autopsy finish processing the image file.
The MD5 signature of the E01 file is: fc67dc2a33b568a774cea733e368bac5



2003-09-07 00:13:30	Registry [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: Keith RID: 1003 Login count: 63
2003-09-18 21:14:14	Registry [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: HTCIA Full name: HTCIA RID: 1006 Login count: 6
2003-09-24 16:59:17	Registry [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: Jo Ellen RID: 1004 Login count: 94
2003-09-26 16:07:30	Registry [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: ID THEFT DUDE Full name: ID THEFT DUDE RID: 1007 Login count: 8

Name	/img_ID THEFT 1.E01
Type	E01
Size	64864256
MD5	fc67dc2a33b568a774cea733e368bac5
SHA1	37540375c5f6cca01f9e47420b3c9d3fa81ed4e8
SHA256	ac3d7346d86730e4e562ddadf4cea43806ff41940a4ec25cba5ecd5f64017614
Sector Size	512
Time Zone	America/Los_Angeles
Acquisition Details	Acquired Date: Wed Jun 23 18:42:21 2004 System Date: Wed Jun 23 18:42:21 2004 Acquiry Operating System: Windows XP Acquiry Software Version: FTK0403 2
Device ID	4c9d29ad-fa21-495c-b6b1-c06c8b6f7c5e
Internal ID	3080
Local Path	C:\Cases\Lab2\ID THEFT 1.E01

Figure 1-1. File Metadata information of the case file that we added to our Autopsy software.

Question 2: Locate the evidence that can assist in prosecuting the following offenses:

To find evidence relating to each of the following offenses we took a similar approach to each one. In Autopsy, the bitstream image is analyzed, it gives an outline of data we can look through in the navigation pane. It is categorized into different views such as exploring the file system itself, by file types, deleted files, extracted recent documents, email addresses and more. By exploring the file system of the bitstream image we were able to look through files and registry to find relevant evidence for each of the following categories. Here is a screenshot to show what we were looking at during the examination.

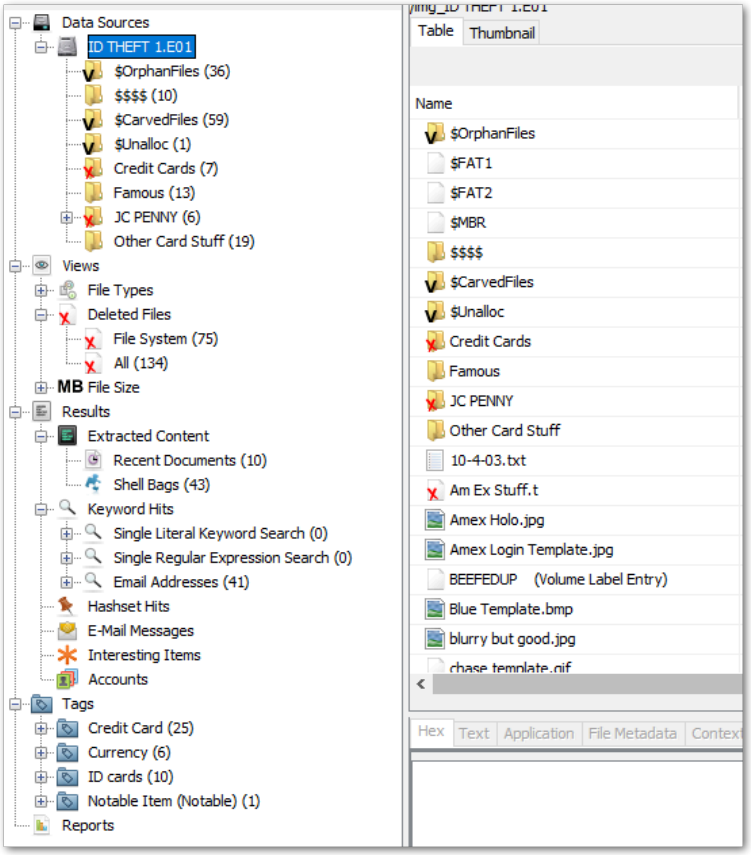


Figure 2-1. Navigation pane of Autopsy.

a. Counterfeiting U.S. Currency

To find evidence relevant to counterfeiting U.S. currency, we looked through the files and through the registry. Luckily, Autopsy shows us deleted files in place and carved files denoted with a scalpel icon. These files were recovered from unallocated space.

There were six files found relating to U.S. currency and the counterfeiting of it. These were mostly image files with one Word document which includes the statement, “I even know how to make counterfeit money”. One image file is a carved file indicating that this was effort put forth to delete or conceal this data. All of these files were organized under the *Currency* tag in Autopsy with a comment added for each item briefly describing it. The first following image was outputted by first creating the Currency tag, tagging and commenting all relevant evidence, then generating a report to show just those items tagged

Currency. In the report, click the *Tagged Files* link and it will show the following output. By clicking the *Tagged Images* link in this report, we get the output of the second image.

Contains files that were tagged with one of the following:Currency

Tag	File	Comment
Currency	/img_ID THEFT 1.E01/$$$$/BEWARE !!.jpg	Cash register UV lamp.
Currency	/img_ID THEFT 1.E01/$$$$/dots off.jpg	Counterfeit current marker.
Currency	/img_ID THEFT 1.E01//$CarvedFiles/f0000672.jpg	Displayed bills. Carved file.
Currency	/img_ID THEFT 1.E01/How to Steal IDs.doc	"I even know how to make counterfeit money"
Currency	/img_ID THEFT 1.E01/$$$$/High Dollar Purchase.jpg	Displayed bills.
Currency	/img_ID THEFT 1.E01/$$$$/50 off.jpg	$50 bill with notable markers.

Figure 1a-1. Files tagged under Currency.

Contains thumbnails of images that are associated with tagged files and results.

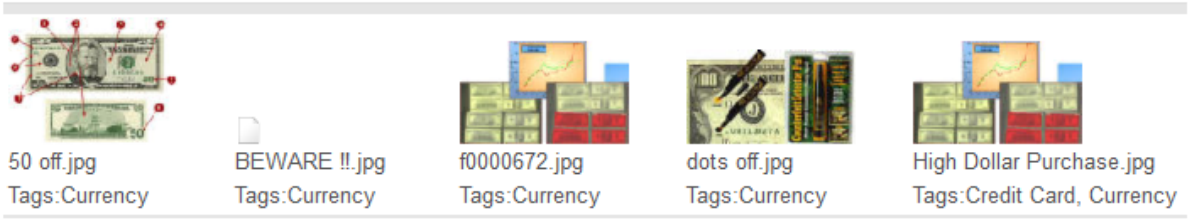


Figure 1a-2. Thumbnails of images tagged under Currency.

b. Counterfeiting U.S. Passports

There are 10 files on this bitstream image relating to U.S. passports and general counterfeit government-issued identification, with the totality being picture files. These files were each tagged under *ID cards* and a comment briefly describing the picture was added. This can be observed in the following figure. The first following image was outputted by first creating the *ID cards* tag, tagging and commenting all relevant evidence, then generating a report to show just those items tagged *ID Cards*. In the report, click the *Tagged Files* link and it will show the following output. By clicking the *Tagged Images* link in this report, we get the output of the second image.

Tagged Files

Contains files that were tagged with one of the following:ID cards

Tag	File	Comment
ID cards	/img_ID THEFT 1.E01/Other Card Stuff/dreamin.jpg	Many ID cards.
ID cards	/img_ID THEFT 1.E01/Other Card Stuff/fake ids.jpg	Examples of fake ID cards.
ID cards	/img_ID THEFT 1.E01/Other Card Stuff/uk id 2.jpg	Example of a UK ID card.
ID cards	/img_ID THEFT 1.E01/Other Card Stuff/uk id.jpg	Example of a UK ID card backside.
ID cards	/img_ID THEFT 1.E01/Other Card Stuff/watch out.jpg	Student ID card.
ID cards	/img_ID THEFT 1.E01//$CarvedFiles/f0000525.jpg	Driver license. Carved file.
ID cards	/img_ID THEFT 1.E01/Other Card Stuff/top this.jpg	Three men holding ID cards.
ID cards	/img_ID THEFT 1.E01/Other Card Stuff/this could be handy.jpg	Police ID card.
ID cards	/img_ID THEFT 1.E01/Other Card Stuff/fake ids.jpg	Four fake ID cards.
ID cards	/img_ID THEFT 1.E01/blurry but good.jpg	Blurry driver license.

Figure 1b-1. Items tagged under ID cards.

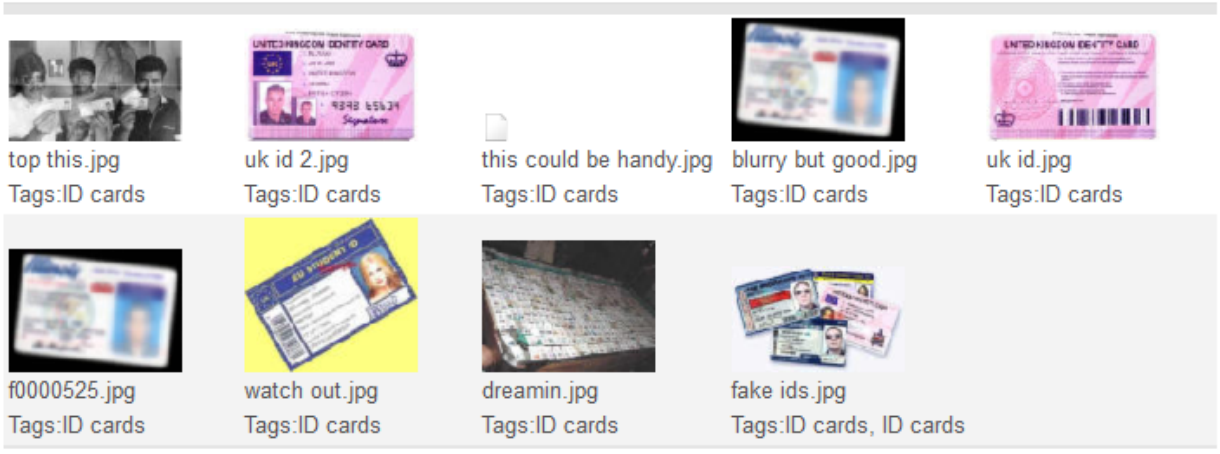


Figure 1b-2. Thumbnails of pictures tagged under ID cards.

c. Theft of Credit Card Information

There are 25 files on this bitstream image relating to credit card information, with the majority being picture files, some web page files, and a Word document file. Many of these files are duplicated however as some are deleted files or carved files, indicating that there was effort put forth to delete or conceal this data. All of these files were organized under the *Credit Card* tag in Autopsy with a comment added for each item briefly describing it.

Notably, there are web site files (.htm and .html) along with image assets that point to the possible use of a scam credit card site used to phish for credentials and sensitive banking information. The first following image was outputted by first creating the *Credit Card* tag, tagging and commenting all relevant evidence, then generating a report to show just those items tagged *Credit Card*. In the report, click the *Tagged Files* link and it will show the following output. By clicking the *Tagged Images* link in this report, we get the output of the second image.

Tag	File	Comment
Credit Card	/img_ID THEFT 1.E01//$CarvedFiles/f0000681.txt	Stolen credit card details found in bathroom.
Credit Card	/img_ID THEFT 1.E01//$CarvedFiles/f0000683.txt	Multiple stolen credit card details.
Credit Card	/img_ID THEFT 1.E01/JC PENNY/Jc Penny Credit Cards Application.htm	Fake JC Penny credit card scam site.
Credit Card	/img_ID THEFT 1.E01/JC PENNY/JCPenney.htm	Counterfeit JCPenny site with copyright and legal notice.
Credit Card	/img_ID THEFT 1.E01//$CarvedFiles/f0000001_Jc_Penny_Credit_Cards_Application.html	Fake JC Penny credit card scam site. Carved file.
Credit Card	/img_ID THEFT 1.E01//$CarvedFiles/f0000021_JCPenney.html	Counterfeit JCPenny site with copyright and legal notice. Carved file.
Credit Card	/img_ID THEFT 1.E01/Credit Cards/Blue Template.bmp	Blue Cash advertisement picture. Unallocated file.
Credit Card	/img_ID THEFT 1.E01/Blue Template.bmp	Blue Cash advertisement picture.
Credit Card	/img_ID THEFT 1.E01//$CarvedFiles/f0000492.bmp	Blue Cash advertisement picture. Carved file.
Credit Card	/img_ID THEFT 1.E01//$CarvedFiles/f0000602.bmp	Business Gold advertisement picture. Carved file.
Credit Card	/img_ID THEFT 1.E01/Famous/made the news !!.jpg	Credit card skimmer article.
Credit Card	/img_ID THEFT 1.E01/Famous/This is why JCPENNY !!!.jpg	JC Penny fraud complaint.
Credit Card	/img_ID THEFT 1.E01/Credit Cards/Am Ex Logo.jpg	American Express logo picture. Unallocated file.
Credit Card	/img_ID THEFT 1.E01/Credit Cards/Amex Holo.jpg	American Express holographic pattern. Unallocated file.
Credit Card	/img_ID THEFT 1.E01/Credit Cards/Amex Login Template.jpg	Login template for website.
Credit Card	/img_ID THEFT 1.E01/Amex Holo.jpg	American Express holographic pattern.
Credit Card	/img_ID THEFT 1.E01/Amex Login Template.jpg	Login template for website.
Credit Card	/img_ID THEFT 1.E01//$CarvedFiles/f0000455.jpg	American Express logo picture. Carved file.
Credit Card	/img_ID THEFT 1.E01//$CarvedFiles/f0000459.jpg	American Express holographic pattern. Carved file.
Credit Card	/img_ID THEFT 1.E01//$CarvedFiles/f0000472.jpg	Login template for website. Carved file.
Credit Card	/img_ID THEFT 1.E01//$CarvedFiles/f0098044.jpg	Credit card skimmer article. Carved file.
Credit Card	/img_ID THEFT 1.E01/$$$$/High Dollar Purchase.jpg	Cash displayed. Unallocated file.
Credit Card	/img_ID THEFT 1.E01//$CarvedFiles/f0098277.jpg	Making a deal? Green truck and three men. Carved file.
Credit Card	/img_ID THEFT 1.E01/How to Steal IDs.doc	Admittance to stealing credit cards.
Credit Card	/img_ID THEFT 1.E01/Other Card Stuff/passport.jpg	Fake passport.

Figure 1c-1. Items tagged under Credit Card.

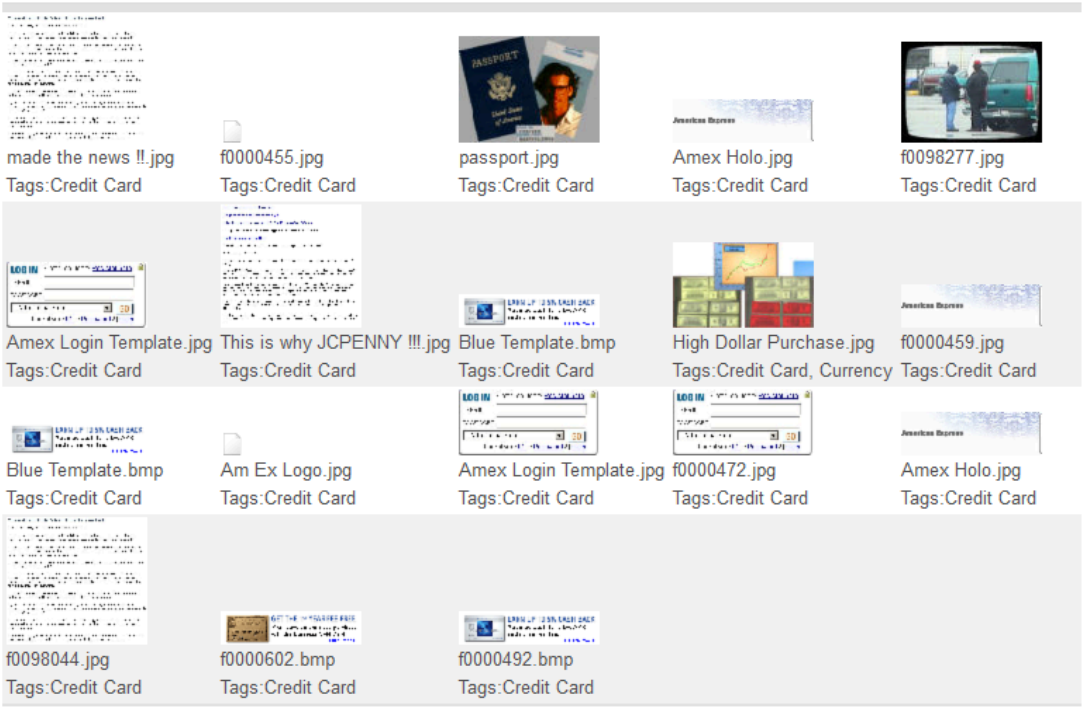


Figure 1c-2. Thumbnails of images tagged under Credit Card.

Question 3: If possible, ascertain if Elvis has any upcoming travel plans.

Looking at previous evidence found, Elvis may have been looking to travel to Dallas, Las Vegas, or even the U.K. Dallas and Las Vegas are possible destinations because in question 6 we need to find the last entered URLs. These addresses were extracted from the NTUSER.DAT file in the NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs key: “http://www.lasvegas.com/”, “http://www.dallas.com/”, and “http://www.usair.com”. The last URL is also important because Elvis may be flying through US Air to get to one of these possible destinations. We also have reason to believe he may be travelling to the U.K. because we found a picture of a counterfeit U.K. ID.

Figure 3-1 UK ID card

Question 4: Bookmark and document findings including the registry file analysis in your case report.

Screenshot of locating the registry files and NTUSER.DAT. Right-click *Add File Tag* and *Bookmark* to mark the important find. These same steps can be used on other registry files.

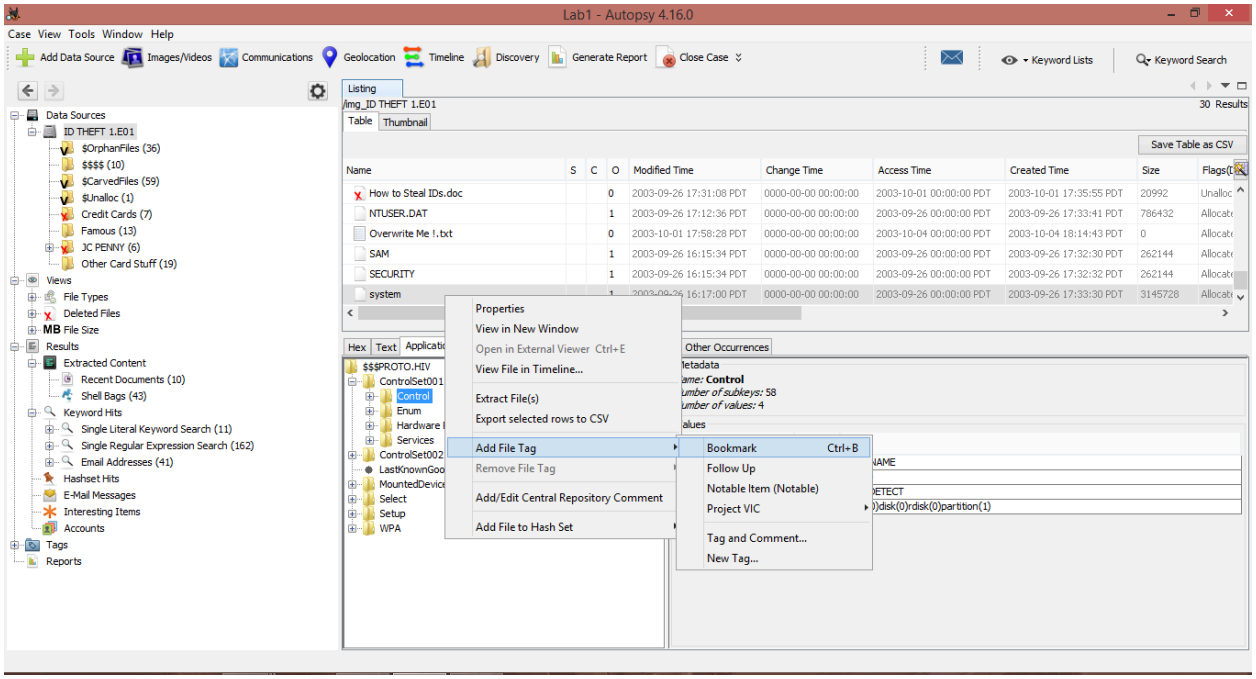


Figure 4-1 Creating a bookmark in the SYSTEM registry.

Part 2

Question 1: Police suspect that Elvis was in possession of illegal MP3 files obtained from an RIAA sting operation. How can you determine if Elvis possessed any of the following files?

a. “La Femme Nikita” Maine Theme (club Version)

We found the “La Femme Nikita” Maine Theme (club Version) MP3 files by performing a keyword search for “Club Version”.

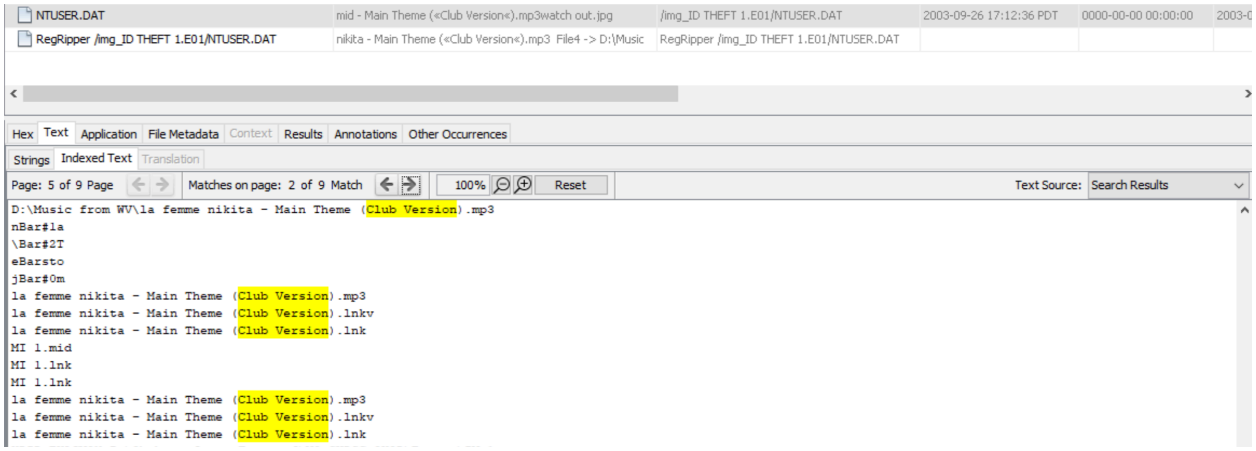


Figure 2a-1. Result listing the MP3 file after keyword searching Club Version.

b.

b. Copy of “La Femme Nikita”, “Spies” by Coldplay

We were able to find the Copy of “La Femme Nikita”, “Spies” by Coldplay MP3 by performing a keyword search for “La Femme”.

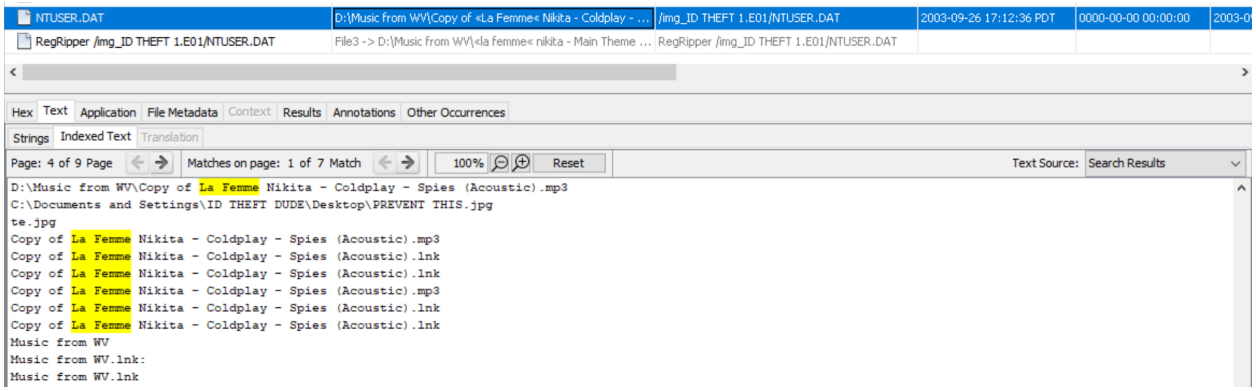


Figure 2b-1. Result listing the MP3 file by Coldplay after keyword searching La Femme.

c. “How You Remind Me” (Acoustic) by Nickelback

We were able to find the “How You Remind Me” (Acoustic) by Nickelback MP3 by performing a keyword search for “Nickelback”.

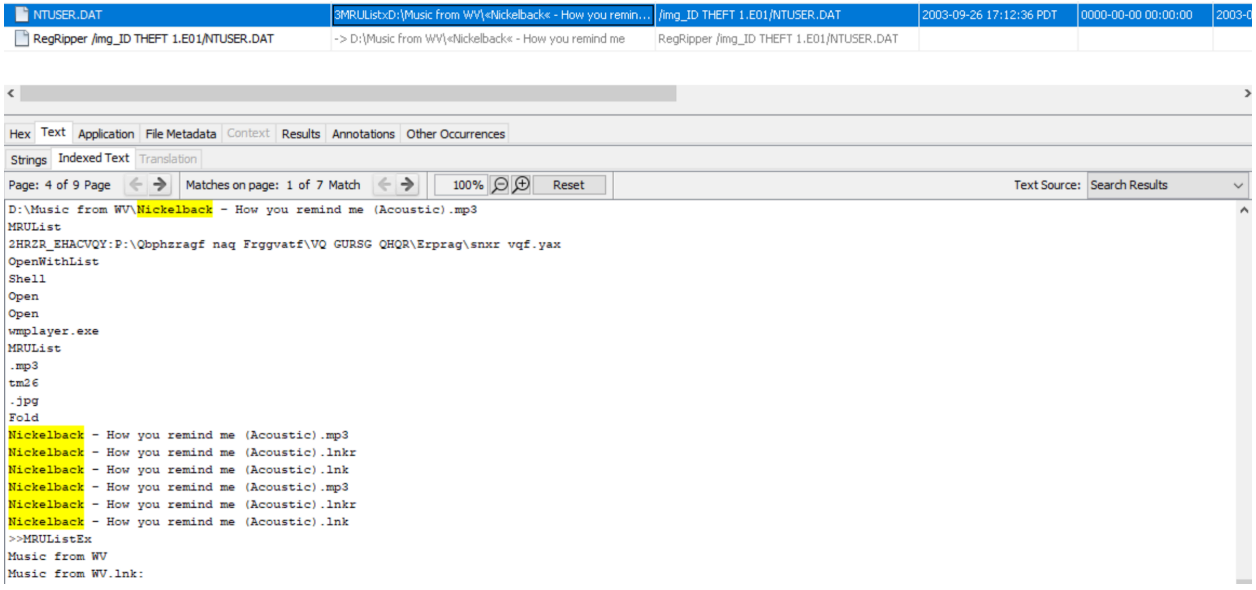


Figure 2c-1. Result listing the MP3 file by Nickelback after keyword searching Nickelback.

Question 2: Several paper documents were recovered in Elvis' locker. Document analysis has begun. What printer was Elvis using?

We found the printer that Elvis was using by navigating into the NTUSER.DAT and locating the folder called "Printer". Here we found the value stating the printer Elvis was using "hp deskjet 3820 series, winspool, Ne00". The pathway for this is NTUSER.DAT\Printers\DeviceOld.

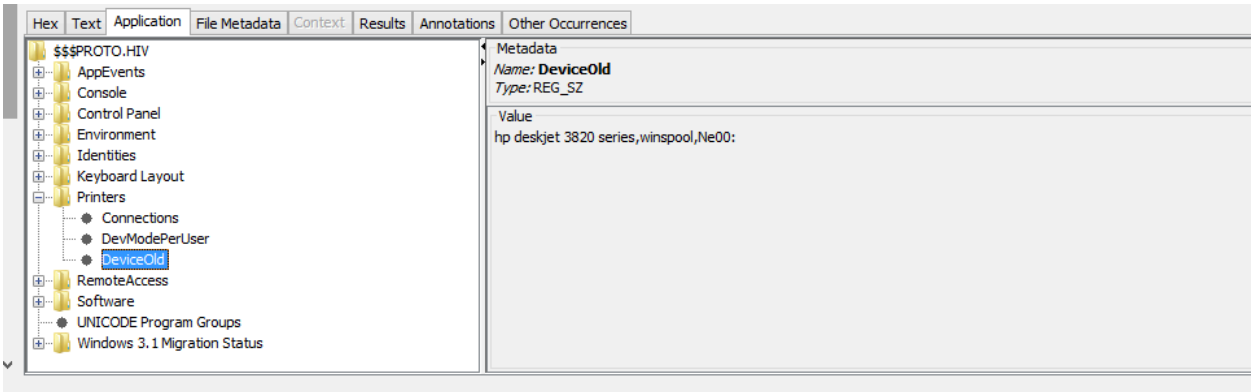


Figure 2-2. Location and name of the printer that Elvis was using.

Question 3: Elvis maintained a POP e-mail account with the IRS fake-ID site. Provide evidence of this account as well as the password Elvis was using to access that account. Add this key to the report.

We found the POP email account with the IRS fake-ID site that Elvis was using by navigating into the NTUSER.DAT and finding the folder called "Internet Account Manager". Within this folder was another folder called "Accounts". Within this folder was another folder called "00000001". In this folder was a file of interest called "SMTP Email Address" containing the POP email named "lD.THEFT.DUDE@FAKEID.COM". We verified the email by matching its name with the POP3 User Name. Lastly, we located the final two files named "POP3 Password2" and "POP3 Prompt for Password", which gave us the password information for the account.

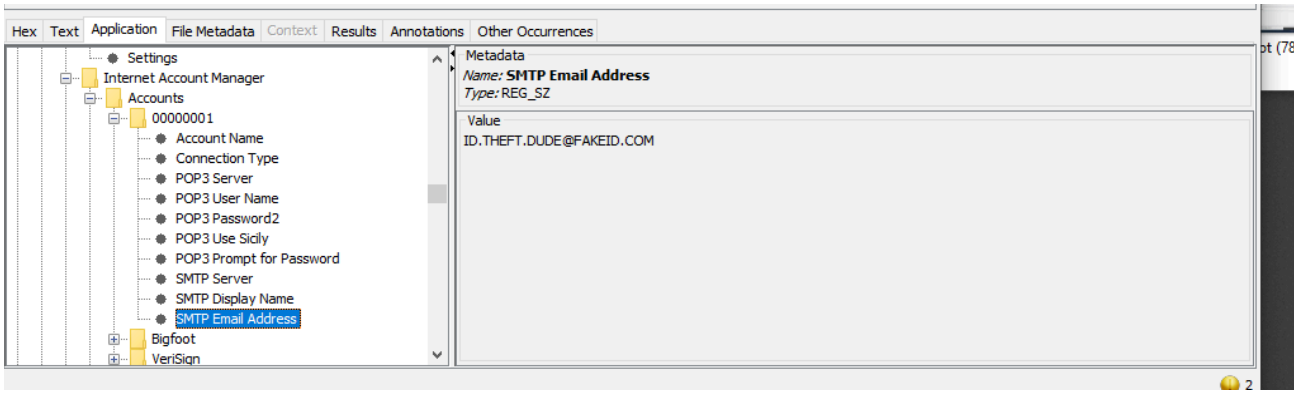


Figure 3-1. File name SMTP Email Address providing information about POP e-mail address that Elvis owned.

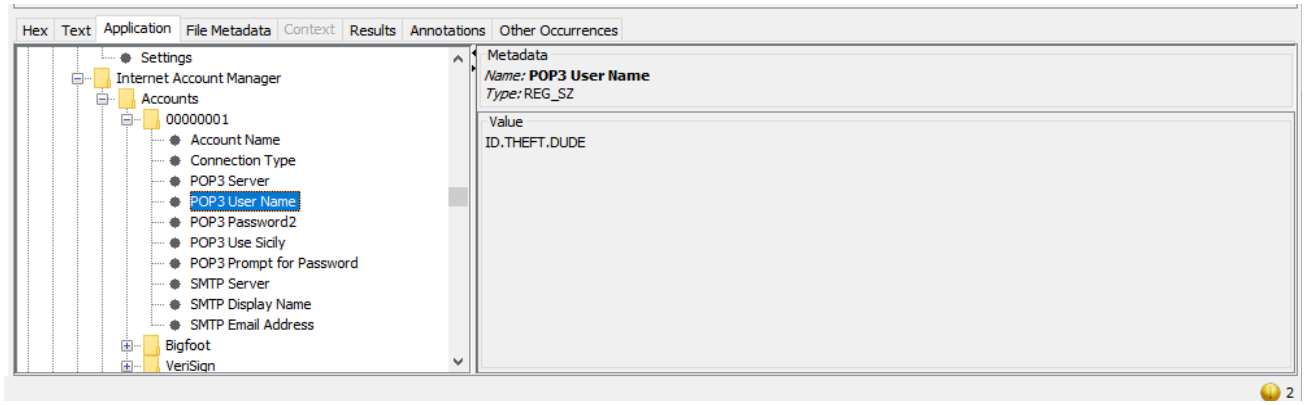


Figure 3-2. File name POP3 User Name verifying the information about POP e-mail address that Elvis owned.

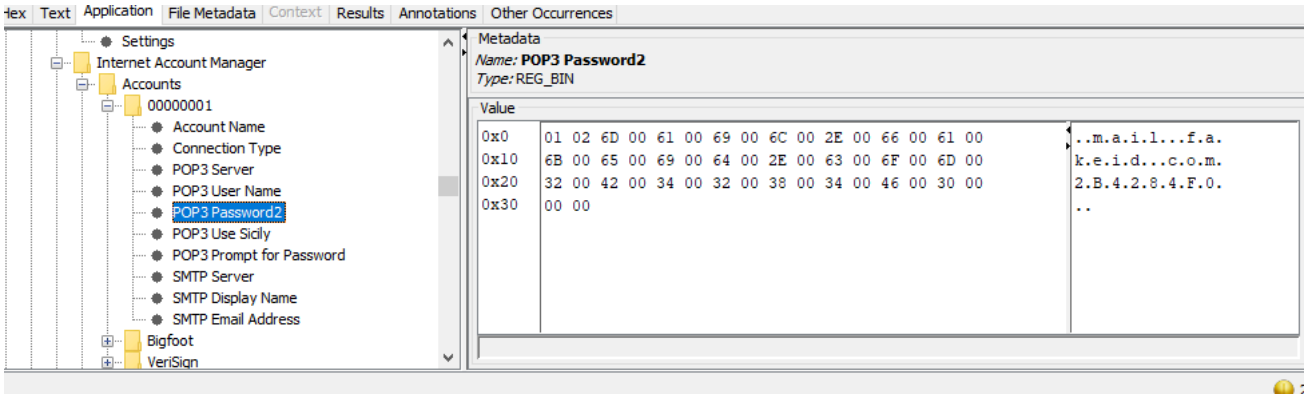


Figure 3-3. File name POP3 Password2 providing password information about POP e-mail address that Elvis owned.

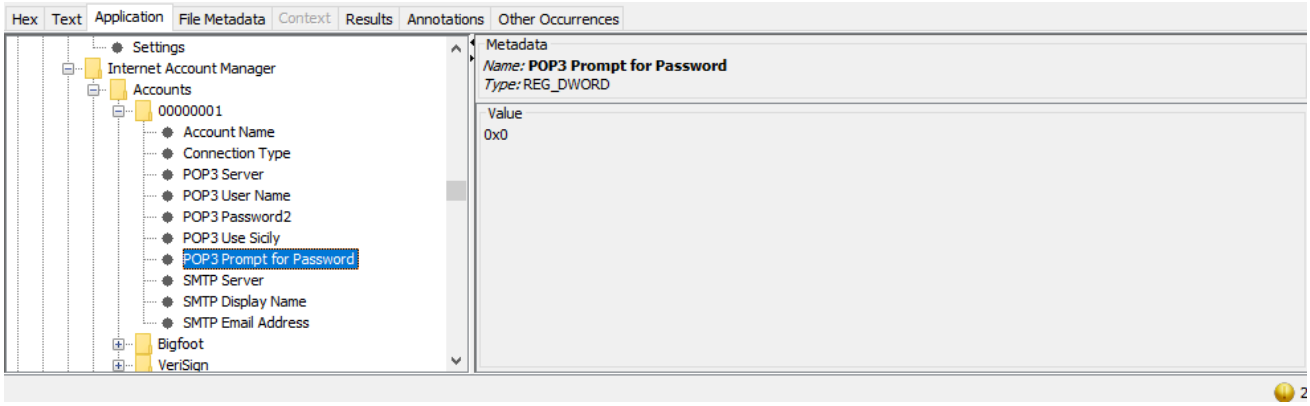


Figure 3-3. File name POP3 Prompt for Password providing password information about POP e-mail address that Elvis owned.

Question 4: What was Elvis' Internet Explorer homepage?

We found Elvis' homepage by looking up NTUSER.DAT and finding the folder of "Internet Explorer". To get to Elvis' homepage we went through the pathway of NTUSER.DAT\Software\Microsoft\Internet Explorer\Main\Start Page. Looking at the Start Page we know the homepage is http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome.

NTUSER.DAT\Software\Microsoft\Internet Explorer\Main\Start Page

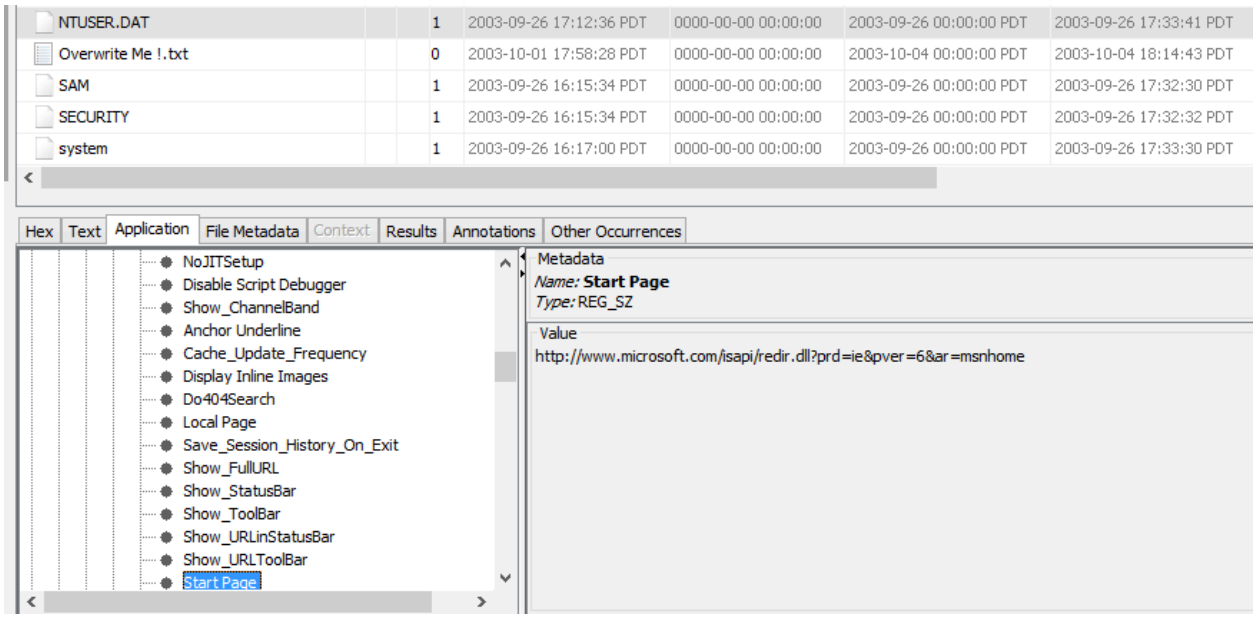


Figure 4-1. Location of the homepage website of Internet Explorer of Elvis.

Question 5: What was the last location that Elvis downloaded something from using Internet Explorer?

The last location that Elvis downloaded something from Internet Explorer was "http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome", his homepage.
This was found in NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs as the last value of the key, "url13".

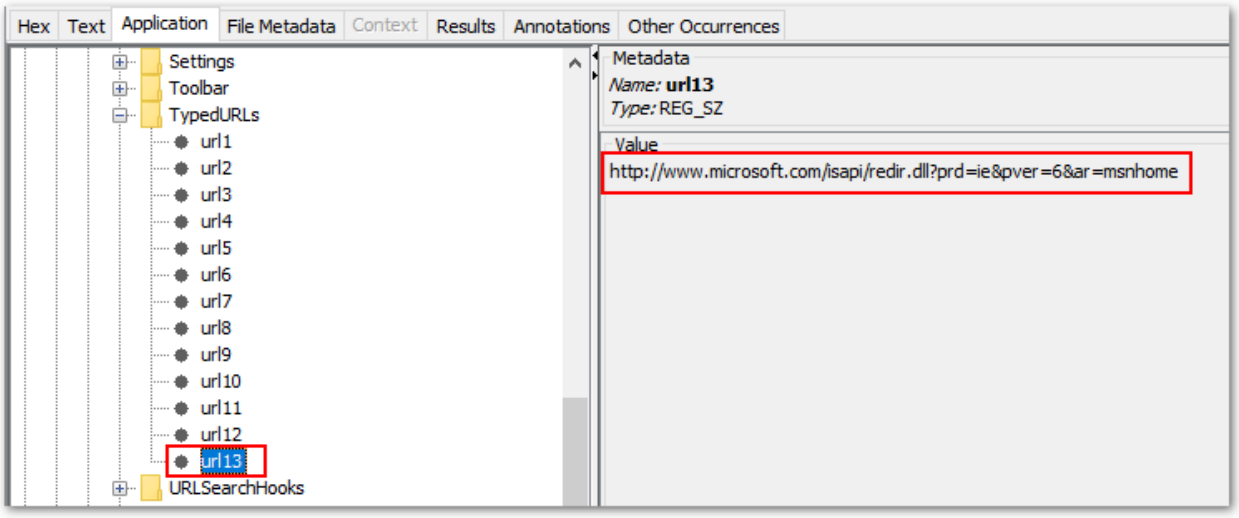


Figure 5-1 Last URL opened and downloaded from Internet Explorer.

Question 6: Add the following to your report:

a. Internet Explorer Typed URLs

This version of Internet Explorer would save its typed URLs into the web browser into the Windows registry. We are able to open the NTUSER.DAT file and explore the registry. Here are the values found in the
NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs key.
The websites typed relate to identity theft, credit card theft, and possible travel.

Website URL	Possible clues
http://www.usair.com/	Travel plans to escape
http://www.americanexpress.com/	Copy the bank login format
www.stealmycard.com	Site for stealing cards
www.lostID.com	Site for stealing identity

http://www.lasvegas.com/	Destination location for escape
http://www.dallas.com/	Destination location for escape
www.creditstealer.com	Site for stealing cards
http://www.fakeid.com/	Site for counterfeit ID
http://www.idtheft.com/	Site for stealing identity

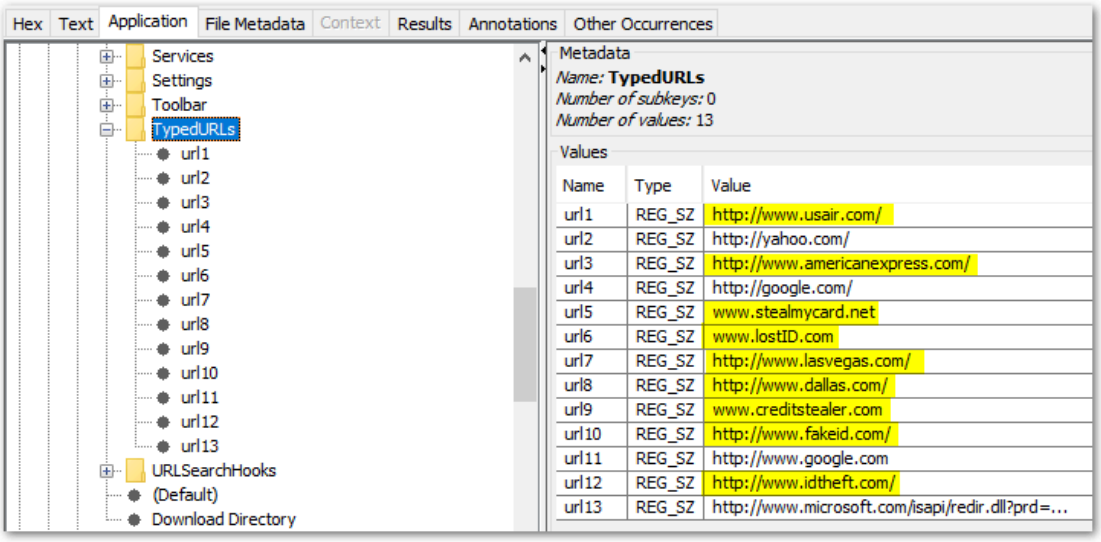


Figure 6a-1. Output at NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs.

b. Recent Documents

To find Recent Documents (all categories) we accessed the NTUSER.DAT file. We followed the pathway of NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs. Here we can find all the recent docs in various categories.

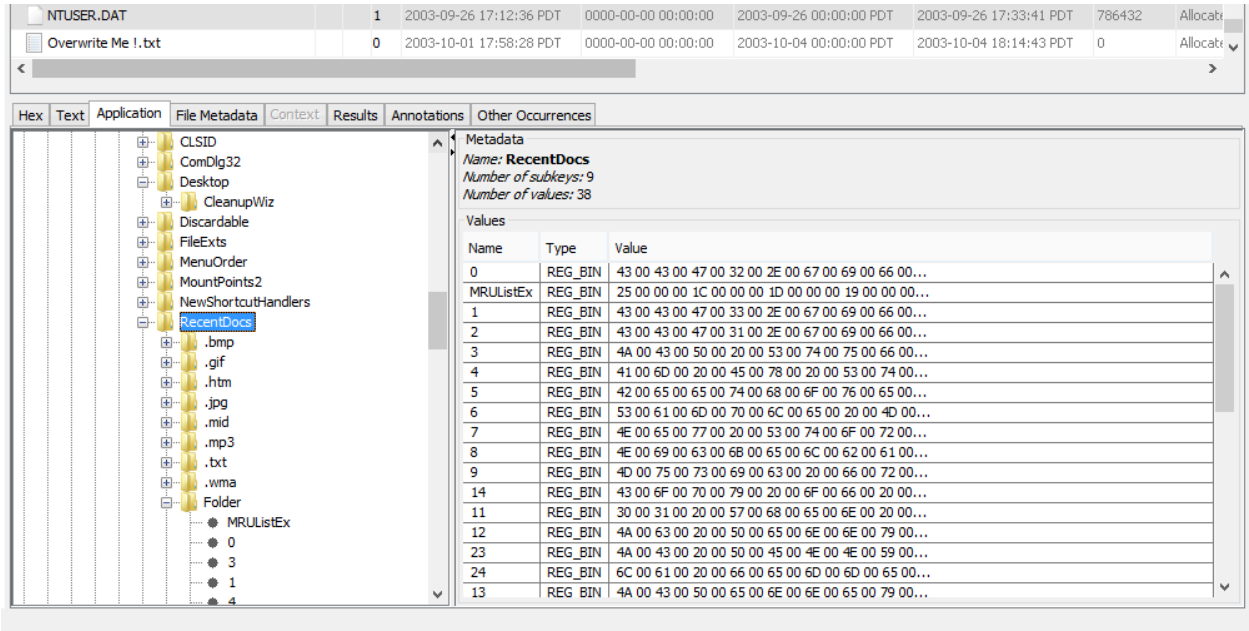


Figure 6b-1. Recent Documents folder contents.

c. Run MRU list information

The Run MRU list information was found by looking in the Window's Registry and then navigating to NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU.

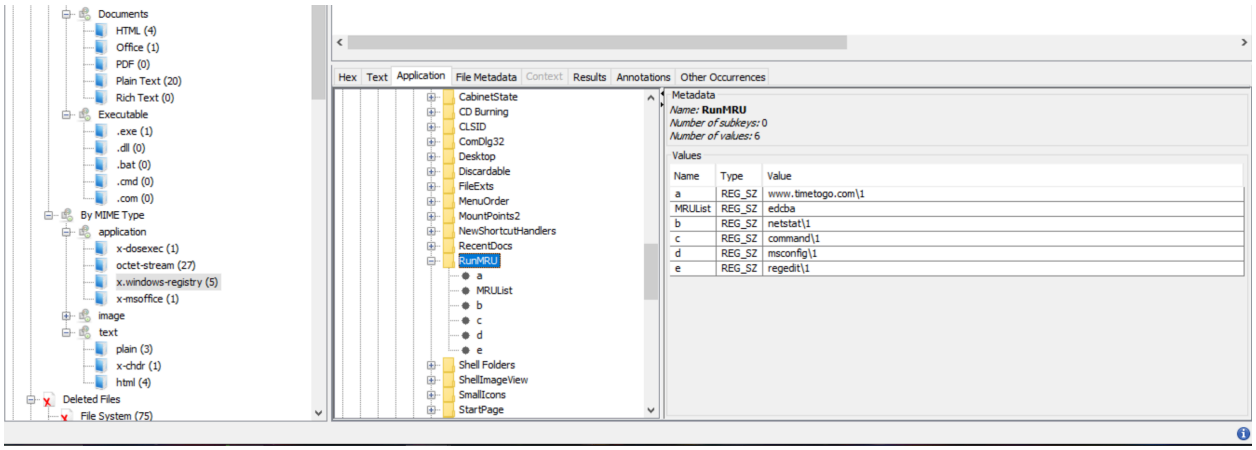


Figure 6c-1. Run MRU list information.

d. Last Visited MRU information

Path NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU.

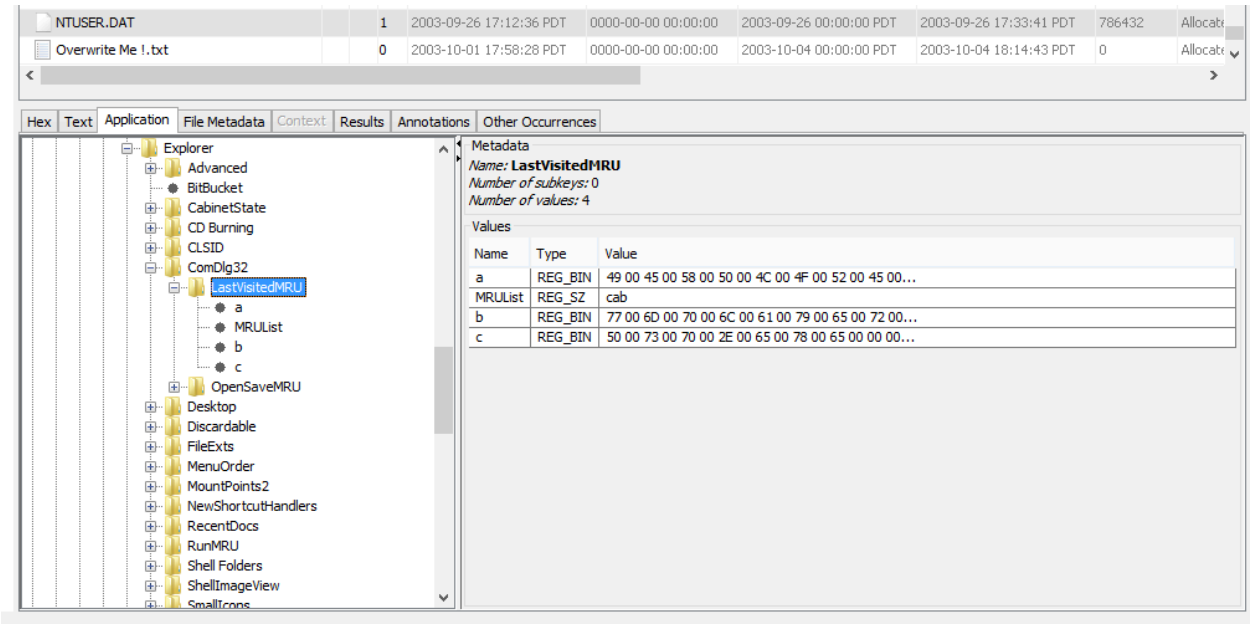


Figure 6d-1.Last Visited MRU information.

e. Open Saved MRU information (Open With or Save as Dialog)

Path NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU.

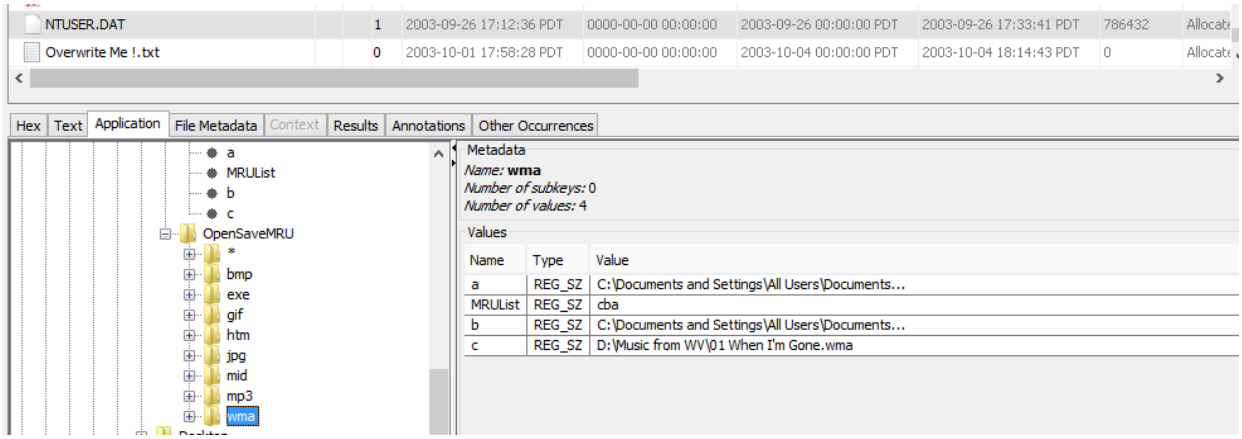


Figure 6e-1. Open With or Save as Dialog MRU information.

Question 7: Generate a report based on NTUSER.DAT file.

We were unable to generate a report on the NTUSER.DAT file, but we were able to extract valuable metadata and explore through the contents of the file.

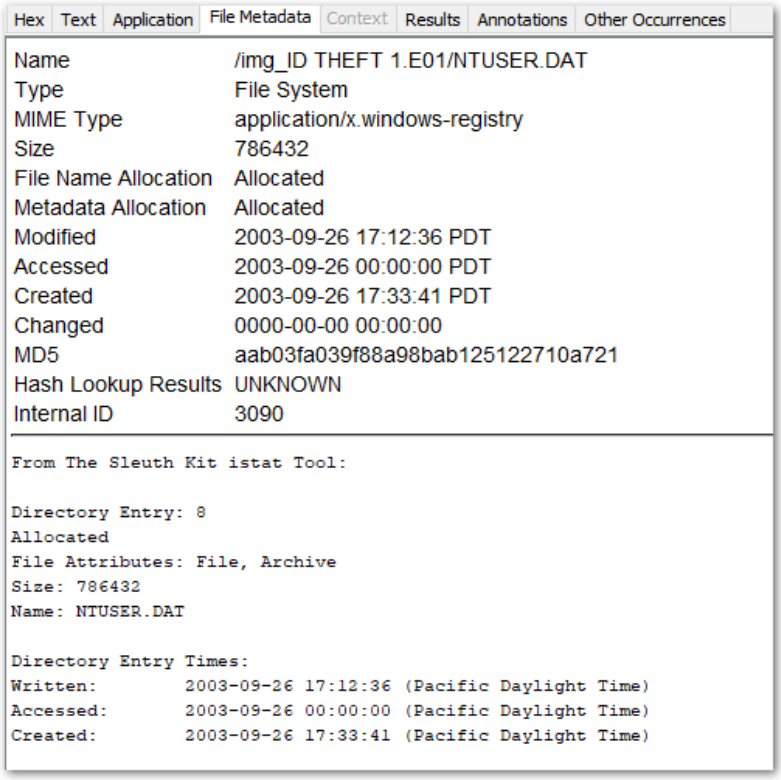


Figure 7-1. NTUSER.DAT metadata.

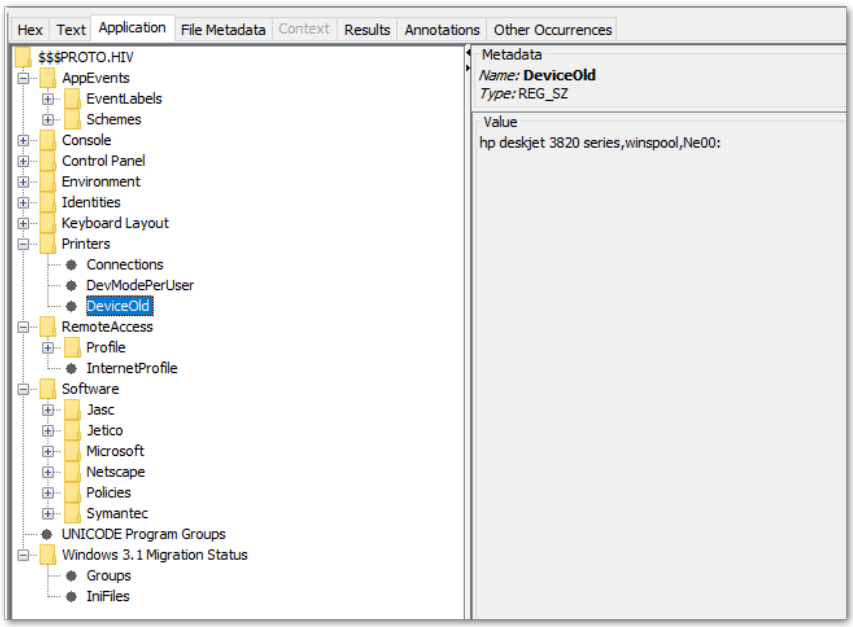


Figure 7-2. NTUSER.DAT contents.

Question 8: Answer the following questions using the SYSTEM file.

a. Elvis is known to transport illicit files on portable storage devices. The Pomona PD has several portable storage devices in their possession from Elvis' school locker. Can you give them any information that can help them determine if Elvis has connected to these portable storage devices?

We found Elvis' connected portable storage devices by going into the SYSTEM hive and locating the folder "MountedDevices". The pathway for this is SYSTEM\MountedDevices.

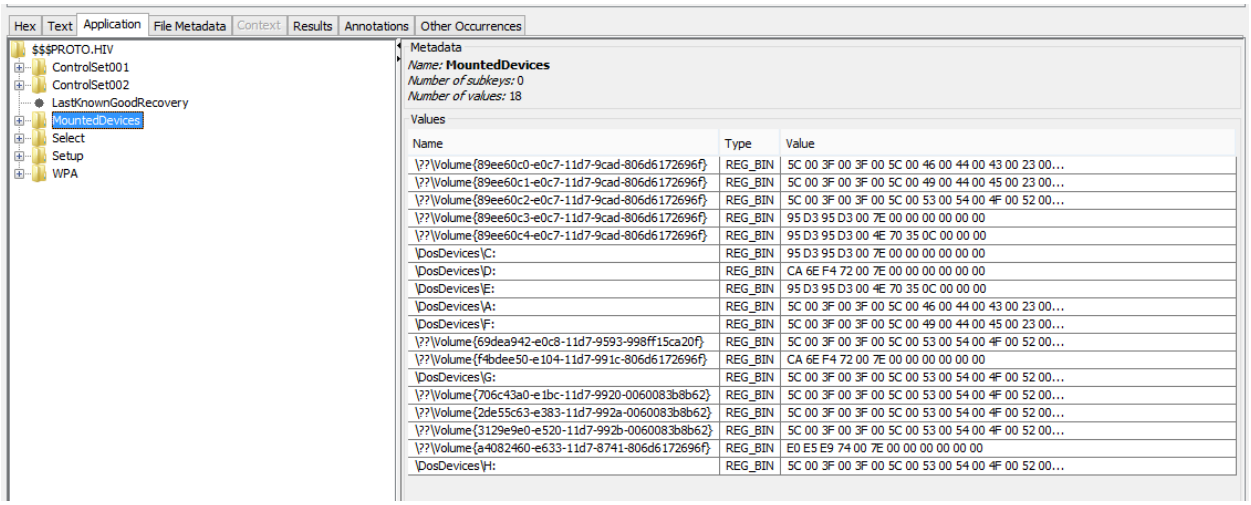


Figure 8a-1 MountedDevices

b. Elvis' computer has been attempting to hack several Salt Lake City credit card sites. The event logs continually show a reference to KAL as an incoming computer name. Look for information that supports this and list a location that could be used to corroborate it.

We found Elvis' computer name by going in the "SYSTEM" hive, "ControlSet001" folder, "Control" folder, "ComputerName" folder, and then finding the ComputerName value of "KAL". This key is changed when the local computer is renamed. The suspect's local computer name was "KAL". That's why the event logs on the Salt Lake City credit card sites see the computer name as "KAL".

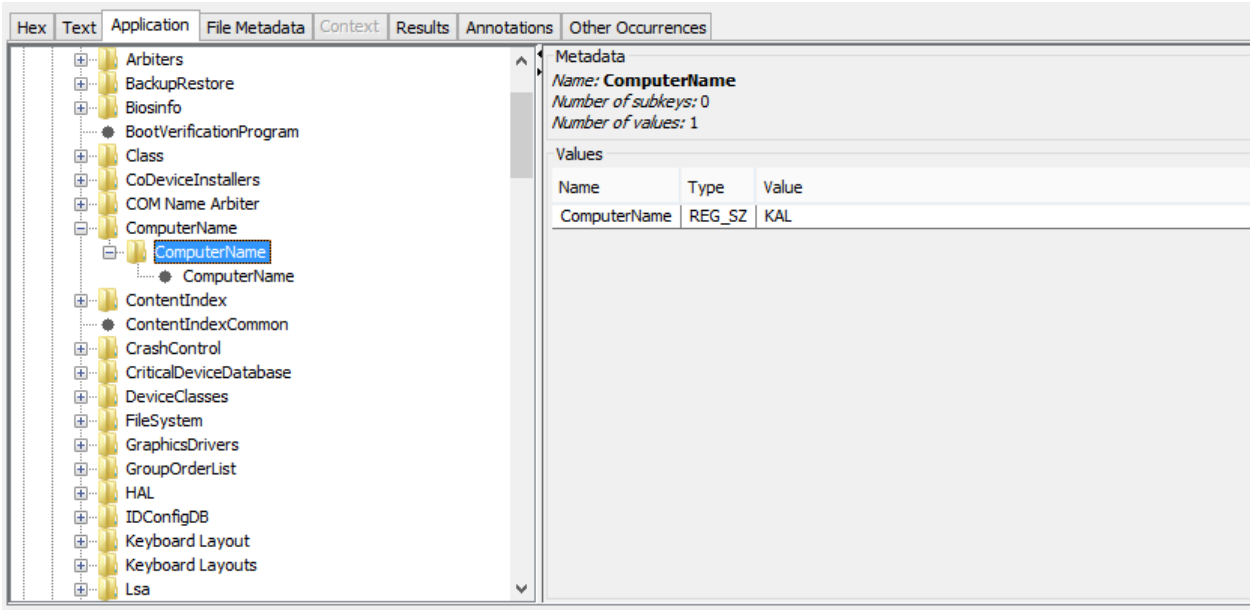


Figure 8b-1. SYSTEM\ControlSet001\Control\ComputerName.

Question 9: Generate a report based on the System file.

Using the Timeline tool we were able to generate a report that included all items originating from the SYSTEM file. Using the filter, we searched on “HKEY_LOCAL_MACHINE\SYSTEM\” and generated a report. It contained 438 items.

Timeline Snapshot

Date/Time	Event Type	Description	Tagged
1998-05-28 04:01:00	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 46 Path: \??\C:\Program Files\Paint Shop Pro 5\Psp.exe	
1998-05-28 04:01:00	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 46 Path: \??\C:\Program Files\Paint Shop Pro 5\Psp.exe	
2001-02-12 22:59:14	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 14 Path: \??\C:\Program Files\Microsoft Office\Office10\msohev.dll	
2001-02-12 22:59:14	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 14 Path: \??\C:\Program Files\Microsoft Office\Office10\msohev.dll	
2001-02-23 08:07:30	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 7 Path: \??\C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe	
2001-02-23 08:07:30	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 7 Path: \??\C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe	
2001-02-26 21:05:16	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 59 Path: \??\C:\Program Files\Microsoft Office\Office10\MLSHEXT.DLL	
2001-02-26 21:05:16	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 59 Path: \??\C:\Program Files\Microsoft Office\Office10\MLSHEXT.DLL	
2001-08-13 22:18:36	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 42 Path: \??\C:\Program Files\Common Files\Symantec Shared\Script Blocking\SBServ.exe	
2001-08-13 22:18:36	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 42 Path: \??\C:\Program Files\Common Files\Symantec Shared\Script Blocking\SBServ.exe	
2001-09-11 13:59:58	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 86 Path: \??\C:\Program Files\AccessData\Dongle Driver\KEYSETUP.EXE	
2001-09-11 13:59:58	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 86 Path: \??\C:\Program Files\AccessData\Dongle Driver\KEYSETUP.EXE	
2001-12-11 09:31:00	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 55 Path: \??\C:\Program Files\AccessData\Dongle Driver\INSTALL.EXE	
2001-12-11 09:31:00	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 55 Path: \??\C:\Program Files\AccessData\Dongle Driver\INSTALL.EXE	
2002-03-28 00:50:29	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 47 Path: \??\C:\WINDOWS\system32\spool\drivers\w32x86\3\hpzstw05.exe	
2002-03-28 00:50:29	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 96 Path: \??\C:\WINDOWS\system32\spool\drivers\w32x86\3\hpzstc05.exe	
2002-03-28 00:50:29	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 50 Path: \??\C:\WINDOWS\system32\spool\drivers\w32x86\3\hpzeng05.exe	
2002-03-28 00:50:29	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 96 Path: \??\C:\WINDOWS\system32\spool\drivers\w32x86\3\hpzstc05.exe	
2002-03-28 00:50:29	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 47 Path: \??\C:\WINDOWS\system32\spool\drivers\w32x86\3\hpzstw05.exe	
2002-03-28 00:50:29	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 50 Path: \??\C:\WINDOWS\system32\spool\drivers\w32x86\3\hpzeng05.exe	
2002-04-29 11:47:46	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 49 Path: \??\C:\Program Files\Microsoft Office\Office10\OLKFSTUB.DLL	
2002-04-29 11:47:46	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 49 Path: \??\C:\Program Files\Microsoft Office\Office10\OLKFSTUB.DLL	
2002-07-30 14:16:20	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 53 Path: \??\C:\WINDOWS\wanmpsvc.exe	
2002-07-30 14:16:20	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 53 Path: \??\C:\WINDOWS\wanmpsvc.exe	
2002-08-07 08:04:28	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 67 Path: \??\C:\Program Files\Symantec\LiveUpdate\NDETECT.EXE	
2002-08-07 08:04:28	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 41 Path: \??\C:\Program Files\Symantec\LiveUpdate\AUPDATE.EXE	
2002-08-07 08:04:28	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatibility] Cached entry: 38 Path: \??\C:\Program Files\Symantec\LiveUpdate\LuComServer.EXE	
2002-08-07 08:04:28	Registry	[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatibility] Cached entry: 38 Path: \??\C:\Program Files\Symantec\LiveUpdate\LuComServer.EXE	

Time Range: Thursday, May 28, 1998 4:01:00 AM -07:00 to Wednesday, October 15, 2003 4:26:50 PM -07:00

Figure 9-1. Timeline snapshot of all items from the SYSTEM file.

Question 10: Even though Elvis had his SAM file on this thumb drive, document when Elvis last logged on to his machine using the SAM file. His machine account name is ID THEFT DUDE. Generate a report.

Elvis last logged on his machine on September 26, 2003 at 16:07:30 PDT.

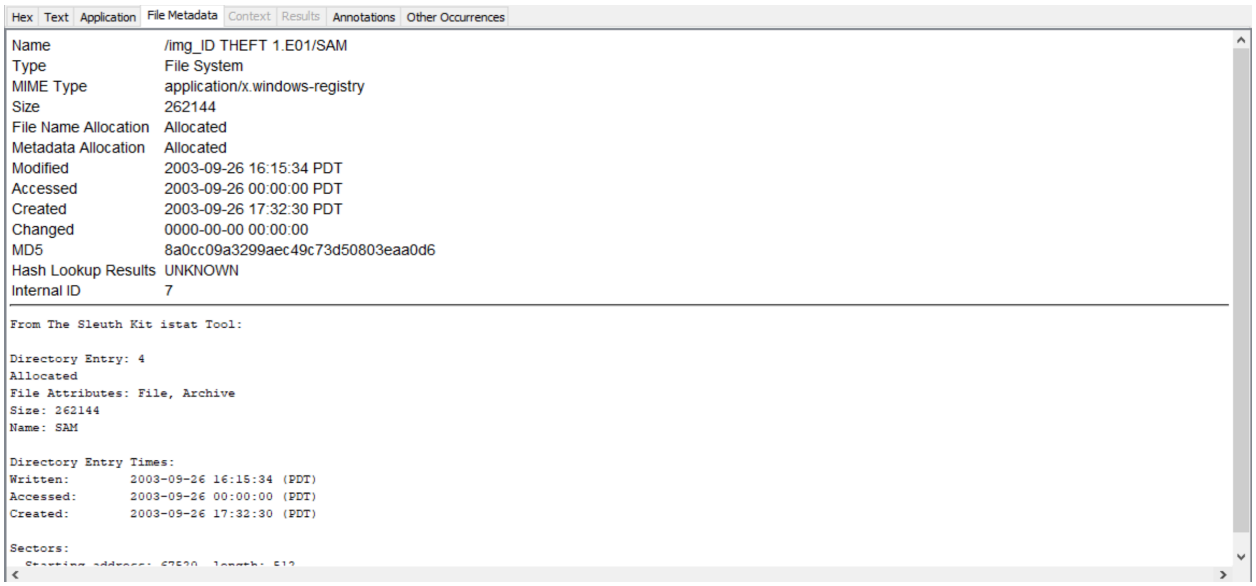


Figure 10-1. File metadata for the SAM file.

By going into the Timeline tool, we were able to search on all items in the bitstream image from May 28, 1998 through Oct 15, 2003. By using the filter feature, we searched on all types of items, and only limited to an expression search. By searching “ID THEFT DUDE” or “1007” (his RID), we are able to see his last logon on September 26, 2003 at 16:07:30 PDT.

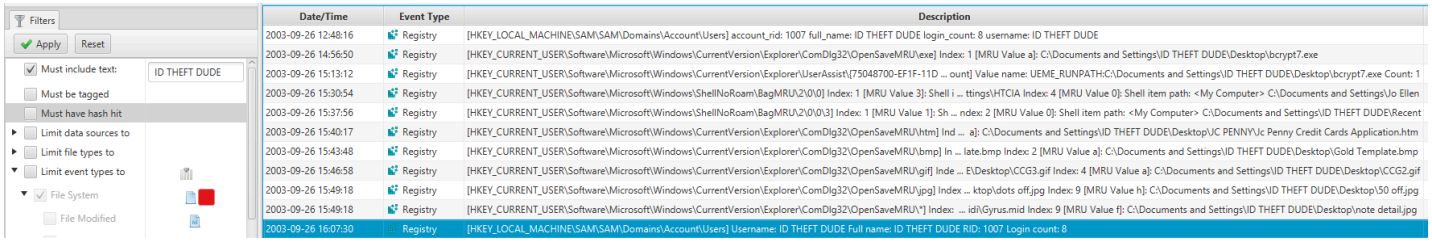
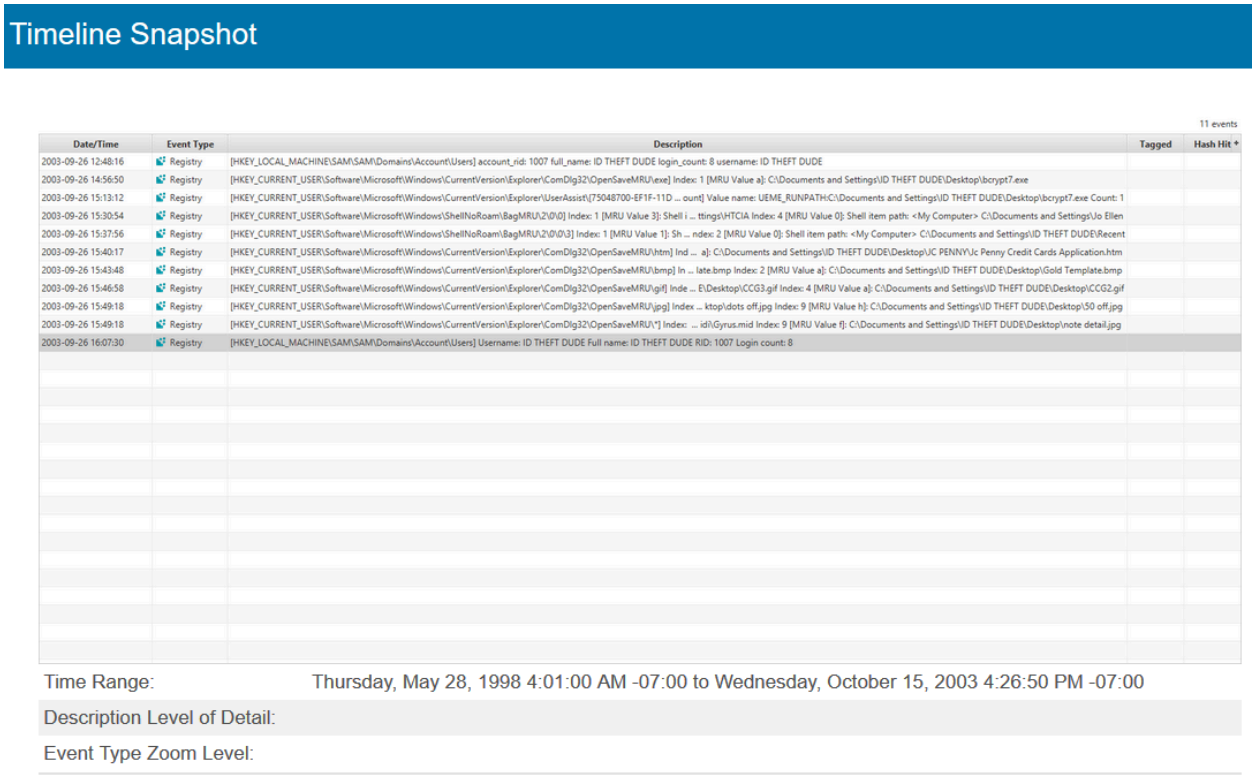


Figure 10-2. Filter items on “ID THEFT DUDE”.

Following is the report generated through Autopsy. It was an option to get a report of the *Timeline Snapshot*.



Timeline Snapshot

11 events

Date/Time	Event Type	Description	Tagged	Hash Hit
2003-09-26 12:48:16	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] account_rid: 1007 full_name: ID THEFT DUDE login_count: 8 username: ID THEFT DUDE		
2003-09-26 14:56:50	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\exe] Index: 1 [MRU Value a]: C:\Documents and Settings\ID THEFT DUDE\Desktop\bcrypt7.exe		
2003-09-26 15:13:12	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D ... ount] Value name: UEME_RUNPATH:C:\Documents and Settings\ID THEFT DUDE\Desktop\bcrypt7.exe Count: 1		
2003-09-26 15:30:54	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\BagMRU\2\0\0] Index: 1 [MRU Value 3]: Shell i ... ttings\HTCIA Index: 4 [MRU Value 0]: Shell item path: <My Computer> C:\Documents and Settings\Jo Ellen		
2003-09-26 15:37:56	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\BagMRU\2\0\0\3] Index: 1 [MRU Value 1]: Sh ... ndex: 2 [MRU Value 0]: Shell item path: <My Computer> C:\Documents and Settings\ID THEFT DUDE\Recent		
2003-09-26 15:40:17	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\htm] Ind ... a]: C:\Documents and Settings\ID THEFT DUDE\Desktop\JC PENNY\Jc Penny Credit Cards Application.htm		
2003-09-26 15:43:48	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\bmp] In ... late.bmp Index: 2 [MRU Value a]: C:\Documents and Settings\ID THEFT DUDE\Desktop\Gold Template.bmp		
2003-09-26 15:46:58	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\gif] Inde ... E\Desktop\CCG3.gif Index: 4 [MRU Value a]: C:\Documents and Settings\ID THEFT DUDE\Desktop\CCG2.gif		
2003-09-26 15:49:18	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\jpg] Index ... ktop\dots off.jpg Index: 9 [MRU Value h]: C:\Documents and Settings\ID THEFT DUDE\Desktop\50 off.jpg		
2003-09-26 15:49:18	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*] Index: ... id\Gyrus.mid Index: 9 [MRU Value f]: C:\Documents and Settings\ID THEFT DUDE\Desktop\note detail.jpg		
2003-09-26 16:07:30	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: ID THEFT DUDE Full name: ID THEFT DUDE RID: 1007 Login count: 8		

Time Range: Thursday, May 28, 1998 4:01:00 AM -07:00 to Wednesday, October 15, 2003 4:26:50 PM -07:00

Description Level of Detail:

Event Type Zoom Level:

Figure 10-3. Timeline Snapshot of “ID THEFT DUDE” registry activity.

Question 11: Generate a report based on the SAM file.

Using the Timeline tool we were able to generate a report that included all items originating from the SAM file. This included 21 items.

Timeline Snapshot

Date/Time	Event Type	Description
2003-09-06 17:16:01	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] account_rid: 501 comments: Built-in account for guest access to the computer/domain login_count: 0 username: Guest
2003-09-06 17:16:01	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] account_rid: 500 comments: Built-in account for administering the computer/domain login_count: 0 username: Administrator
2003-09-06 17:23:33	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: Administrator Comments: Built-in account for administering the computer/domain RID: 500 Login count: 0
2003-09-06 23:31:50	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: HelpAssistant Full name: Remote D ... Assistant Account Comments: Account for Providing Remote Assistance RID: 1000 Login count: 0
2003-09-06 23:31:50	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] account_rid: 1000 comments: Account for Pro ... stance full_name: Remote Desktop Help Assistant Account login_count: 0 username: HelpAssistant
2003-09-06 23:35:15	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] account_rid: 1002 comments: This is a ve ... Microsoft Corporation,L=Redmond,S=Washington,C=US login_count: 0 username: SUPPORT_388945a0
2003-09-06 23:35:15	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: SUPPORT_388945a0 Full name: CN=M ... omments: This is a vendor's account for the Help and Support Service RID: 1002 Login count: 0
2003-09-06 23:48:44	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] account_rid: 1004 login_count: 94 username: Jo Ellen
2003-09-06 23:48:44	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] account_rid: 1003 login_count: 63 username: Keith
2003-09-06 23:48:44	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: Jo Ellen RID: 1004 Login count: 94
2003-09-07 00:13:30	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: Keith RID: 1003 Login count: 63
2003-09-18 19:20:43	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] account_rid: 1006 full_name: HTCIA login_count: 6 username: HTCIA
2003-09-18 21:14:14	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: HTCIA Full name: HTCIA RID: 1006 Login count: 6
2003-09-24 16:59:17	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: Jo Ellen RID: 1004 Login count: 94
2003-09-26 00:00:00	_A__	/SAM
2003-09-26 12:48:16	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] account_rid: 1007 full_name: ID THEFT DUDE login_count: 8 username: ID THEFT DUDE
2003-09-26 15:29:43	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\BagMRU\2\3\0] Index: 1 [MRU Value 0]: Shell item path: <My Computer> <UNKNOWN: 0x00>\My Music\Sample Music
2003-09-26 15:34:25	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\ ... ettings\All Users\Documents\My Music\Sample Music\Beethoven's Symphony No. 9 (Scherzo).wma
2003-09-26 16:07:30	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: ID THEFT DUDE Full name: ID THEFT DUDE RID: 1007 Login count: 8
2003-09-26 16:08:07	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder] Index: 1 ... m: [Music from WV.lnk] Index: 7 [MRU Value 0]: Path: Sample Music, Shell item: [Sample Music.lnk]
2003-09-26 16:08:07	Registry	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder] Index: ... U Value 1]: JC PENNY Index: 6 [MRU Value 3]: Music from WV Index: 7 [MRU Value 0]: Sample Music
2003-09-26 16:12:38	Registry	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: Keith RID: 1003 Login count: 63
2003-09-26 16:15:34	M___	/SAM
2003-09-26 17:32:30	__B_	/SAM

Figure 11-1. Timeline snapshot of all items from the SAM file.

Question 12: Use the File Filter Manager to create and apply the following filters to this case. Document the number of times resulting from each filter.

a. Display all allocated graphics created on October 1, 2003. How many hits result?

87 hits result. We found this in Autopsy by using the *Timeline-Editor*. In the *Timeline-Editor,* we filtered the data by *File Created* and *Start Date* between "Oct 1, 2003 12:00:00 AM PDT" and "Oct 2, 2003 12:00:00 AM PDT".

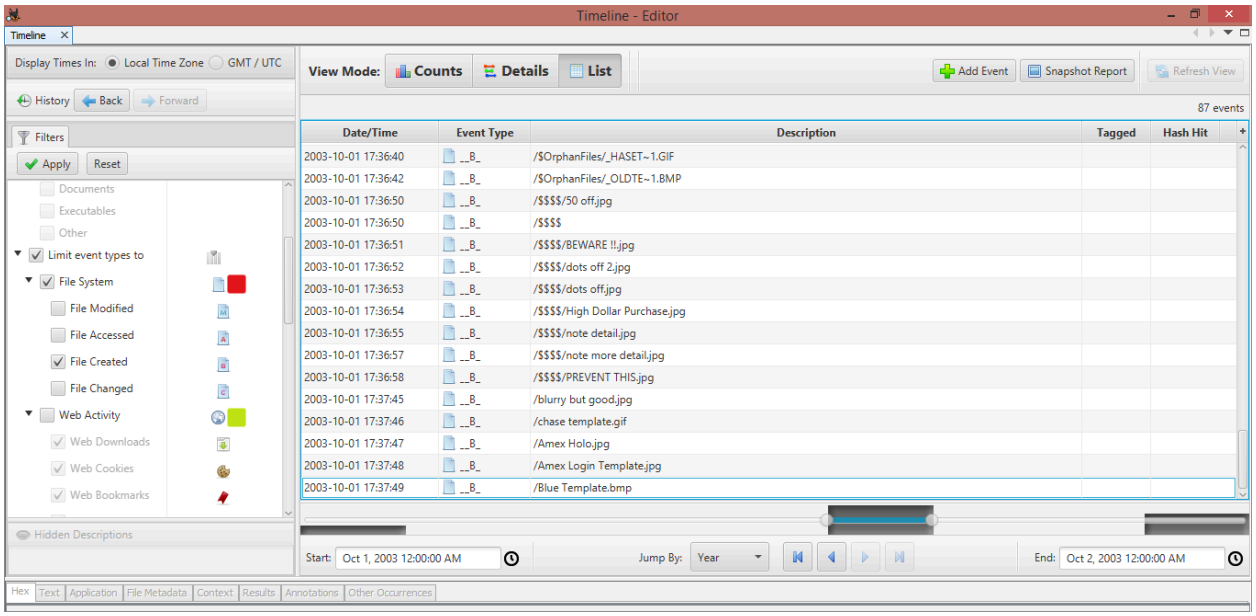


Figure 12a-1. All graphics created on October 1, 2003.

b. Display only deleted graphics. How many hits result?

29 hits result. We found this in Autopsy by using the *Timeline-Editor*. In the *Timeline-Editor,* we filtered the data by *File Modified* and *Start Date* between "Oct 1, 2003 12:00:00 AM PDT" and "Oct 2, 2003 12:00:00 AM PDT."

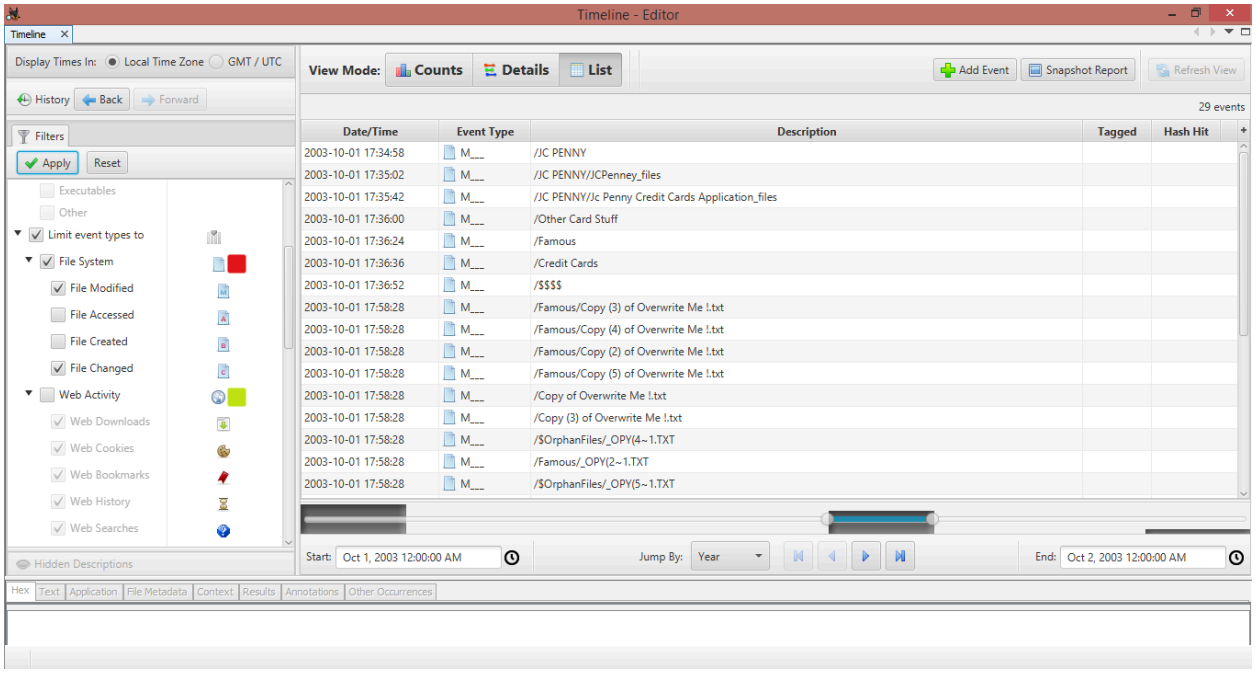
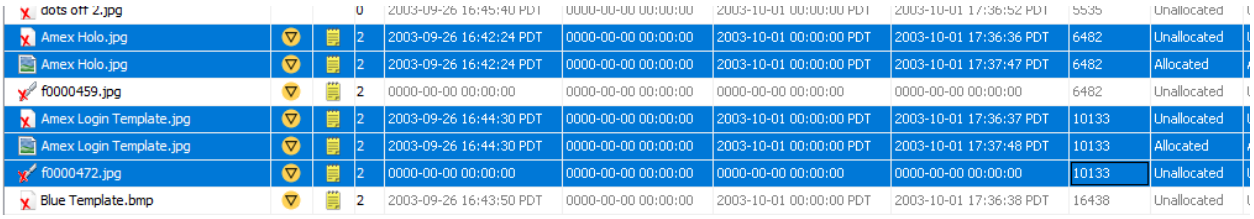


Figure 12b-1. All Graphics that were deleted on October 1, 2003.

c. Display all allocated duplicate graphics with a logical size between 6-11 KB. How many hits result?

We were unable to find duplicate graphics with a logical size of 6-11 KB as Autopsy has set file size ranges, but not able to set our own specified range. But by showing all images and sorting by file size we are able to see duplicates by finding multiple files that have the same file size and hash values. Between 6 and 11 KB there were two distinct files that had duplicates. One was the "Amex holo.jpg" file and the other was the "Amex Login Template.jpg" file. In both instances, they had duplicates that were found deleted, and the second file had a duplicate found in unallocated space. The screenshot below shows what we were able to find:



dots off 2.jpg			0	2003-09-26 16:45:40 PDT	0000-00-00 00:00:00	2003-10-01 00:00:00 PDT	2003-10-01 17:36:52 PDT	5535	Unallocated
Amex Holo.jpg			2	2003-09-26 16:42:24 PDT	0000-00-00 00:00:00	2003-10-01 00:00:00 PDT	2003-10-01 17:36:36 PDT	6482	Unallocated
Amex Holo.jpg			2	2003-09-26 16:42:24 PDT	0000-00-00 00:00:00	2003-10-01 00:00:00 PDT	2003-10-01 17:37:47 PDT	6482	Allocated
f0000459.jpg			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6482	Unallocated
Amex Login Template.jpg			2	2003-09-26 16:44:30 PDT	0000-00-00 00:00:00	2003-10-01 00:00:00 PDT	2003-10-01 17:36:37 PDT	10133	Unallocated
Amex Login Template.jpg			2	2003-09-26 16:44:30 PDT	0000-00-00 00:00:00	2003-10-01 00:00:00 PDT	2003-10-01 17:37:48 PDT	10133	Allocated
f0000472.jpg			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10133	Unallocated
Blue Template.bmp			2	2003-09-26 16:43:50 PDT	0000-00-00 00:00:00	2003-10-01 00:00:00 PDT	2003-10-01 17:36:38 PDT	16438	Unallocated

Figure 12c-1. Duplicate graphics between 6-11 KB.