

ITIS 5250  
Sneha Rangari  
Semester Project  
12/04/2018

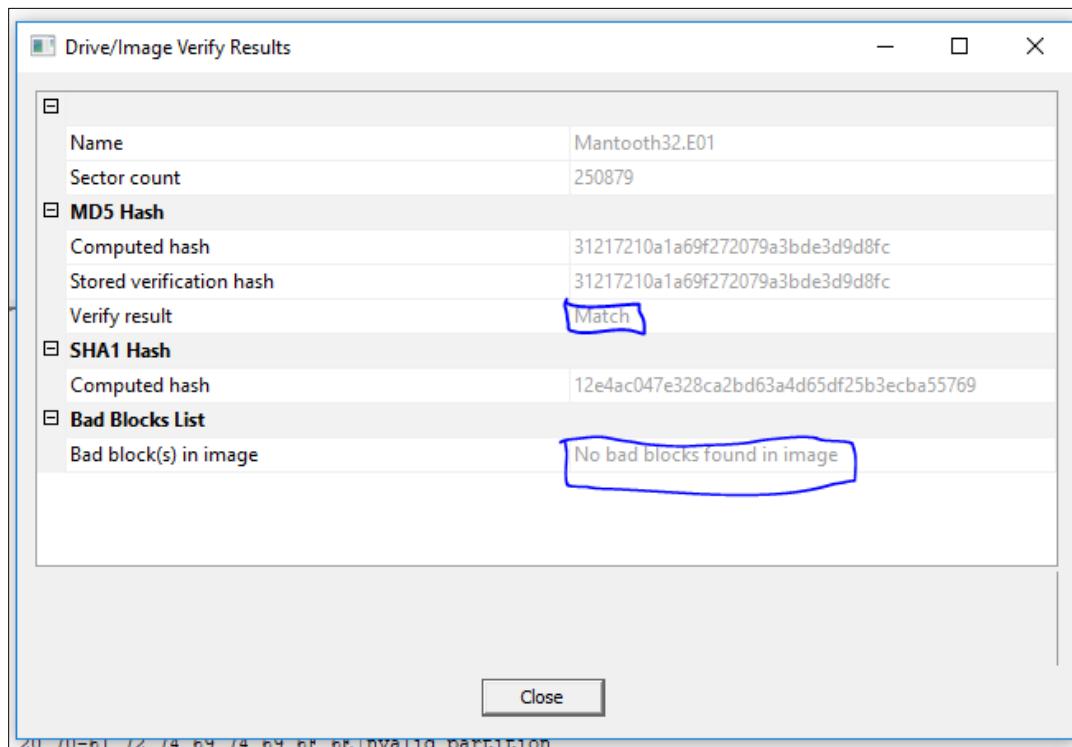
## Overview:

In this Project, I have been given EnCase E01 format forensic image (named Mantooth32.E01) by Detective Ketchum to investigate against local group of criminals has been involved in check fraud, credit card fraud, bad checks, ATM scams and other financial crimes. These criminals have shown varying degrees of technical ability with computers, including steganography, encryption and anti-forensics. I have been asked to make use of the “FTK Tool” along with “FTK Imager Tool”, “Registry Viewer” and “PRTK” and gather certain shreds of evidence such as email address, email conversations, passwords and photographs from the image provided. Also, I have been asked to look for credit card numbers, checks, scam, browser history and information about the OS.

## Forensic Acquisition & Exam Preparation:

I accessed the Forensic images in the Shared Folder on the network from the Forensics Lab in Cone 169. I accessed images named ‘Mantooth32.E01’. Later, I loaded this image using FTK Imager. The software used for accessing & extracting information from the image is FTK Imager 4.1.1.1. The first step undertaken after accessing the image files was the Hash verification along with description of image from txt file and verified their integrity.

Later, I loaded this images using FTK Imager and verified their **integrity**.

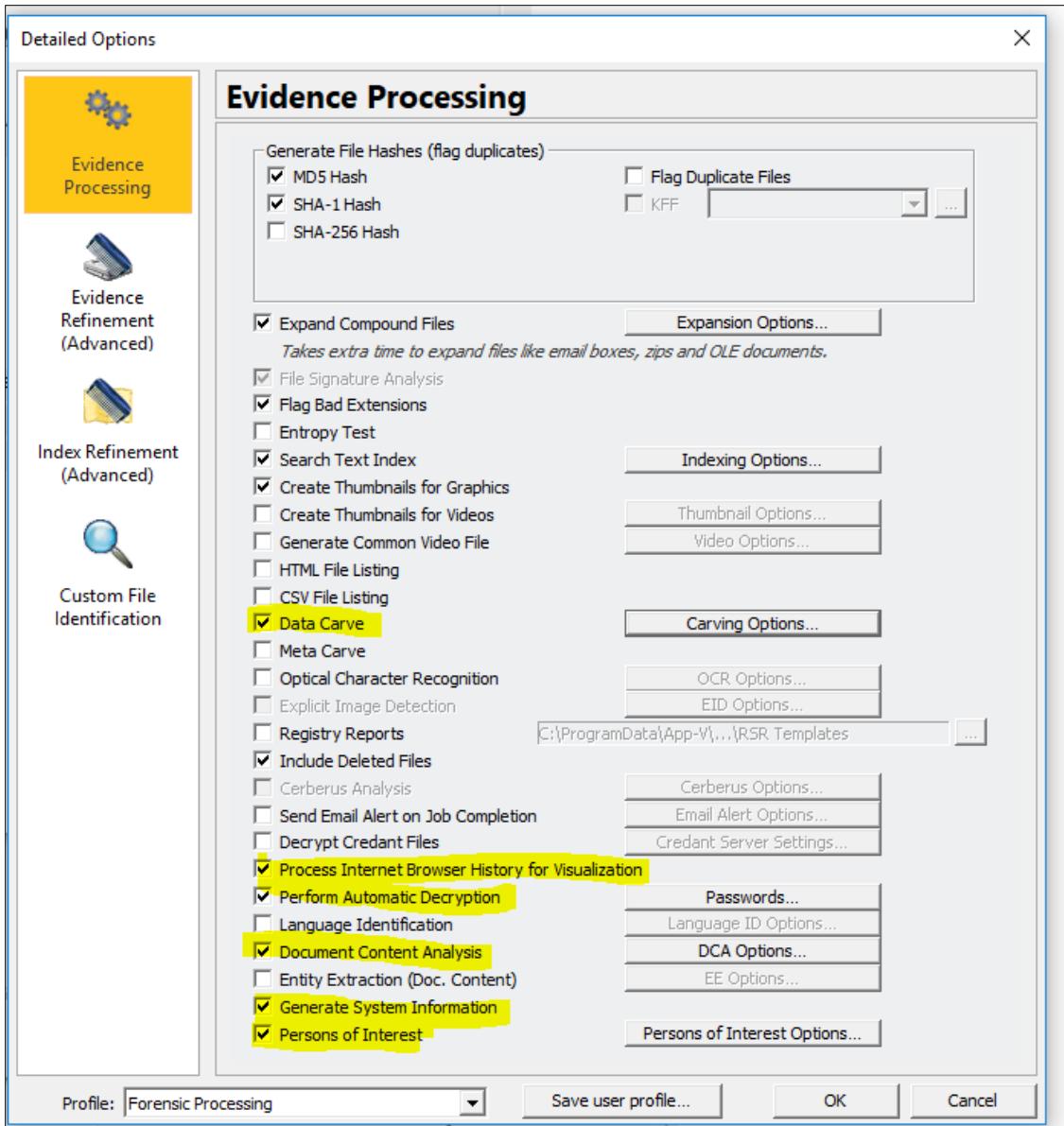


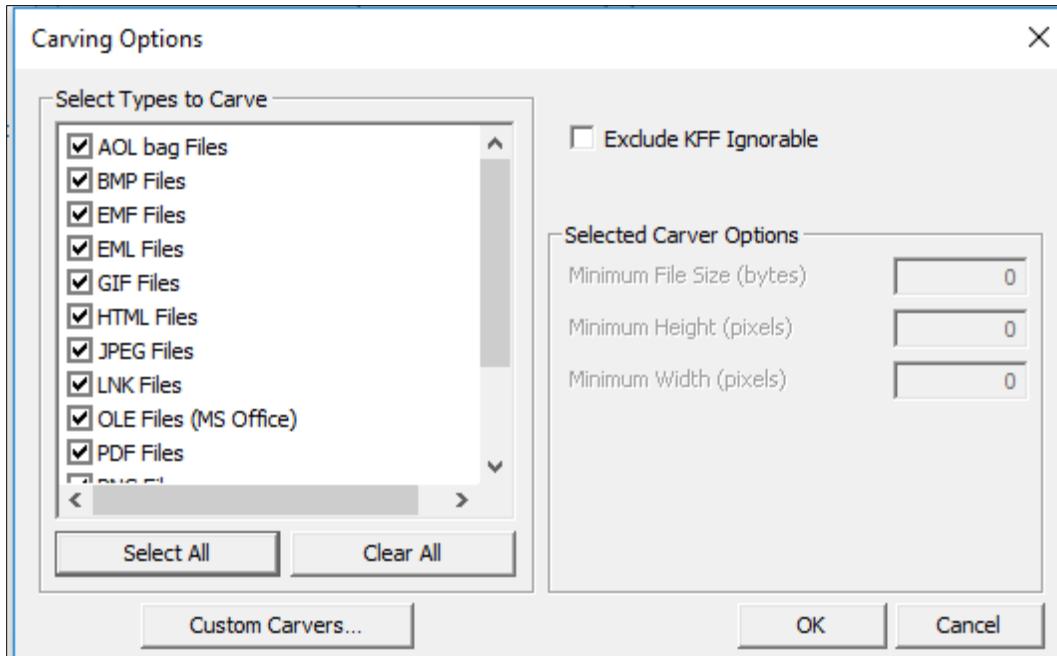
The above result show that this image was not tampered and then using FTK.  
I customized processing profile by adding options:

- Data Carve
- Process Internet Browser History for visualization
- Perform Automatic decryption
- Document content analysis
- Entity Extraction
- General System Information
- Persons of Interest

In Carving options, I selected all types to Carve.

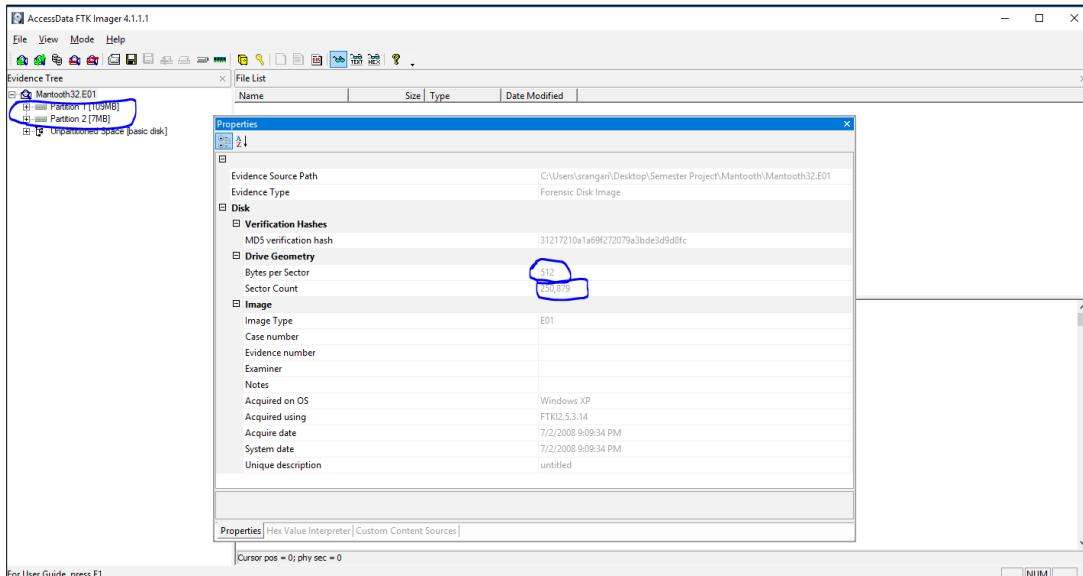
I processed them as shown:





## Findings and Report (Forensic Analysis)

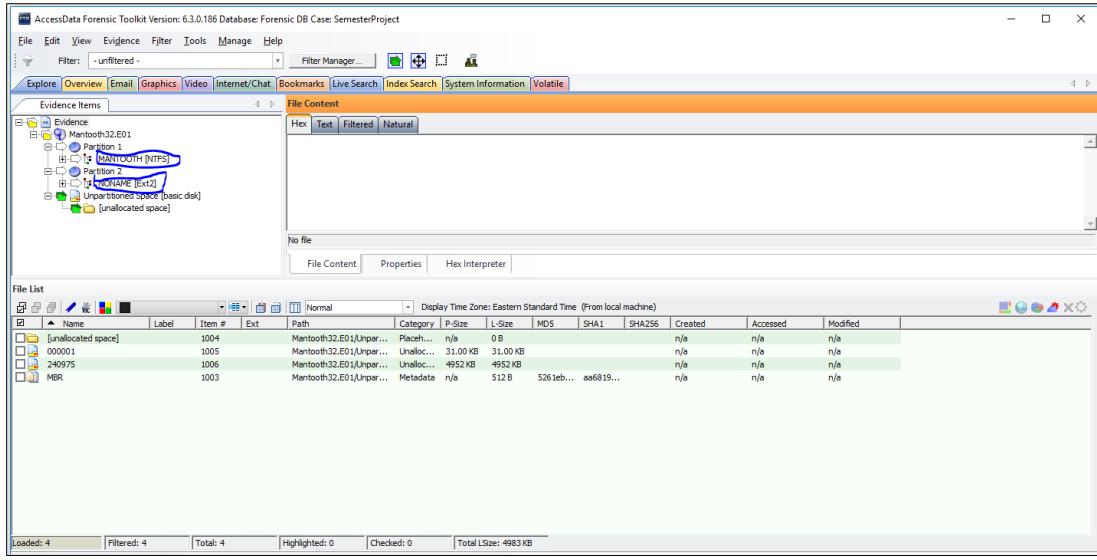
1. Account for how all the space on the computer hard drive was used (partitions, used/free).



The size of the computer hard drive is obtained by considering Drive Geometry in which Bytes per Sector are multiplied by Sector Count. i.e.  $512 \times 2,50,879 = 128,450,048$  bytes.

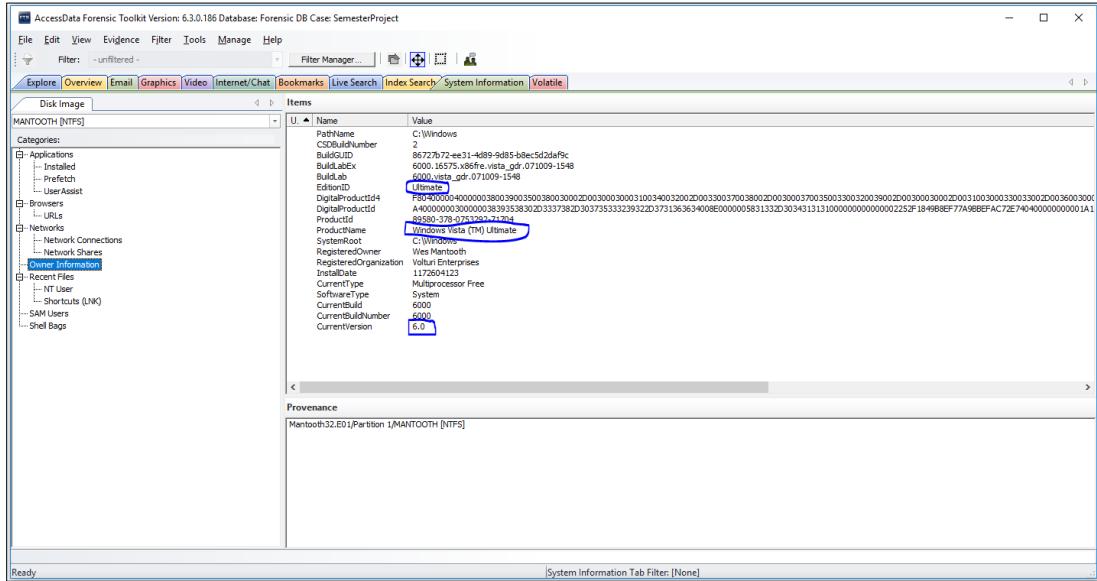
As shown in FTK Imager, total partition comprises of  $109\text{MB} + 7\text{MB} = 116\text{ MB}$  which is used.

## **2. Identify the types of file systems in use.**



FTK shows two types of file systems in use, which are **NTFS** and **Ext2**.

### **3. Identify the version and service pack of the operating system.**



‘System Information’ in FTK shows the service pack of the Operating System is ‘**Windows Vista Ultimate**’ and the current version is **6.0**.

Similar information is evident when **SOFTWARE** file from FTK is exported into “**Registry viewer**” as shown above.

The screenshot shows the AccessData Forensic Toolkit interface. The main window displays a file list titled 'File List' under the 'Case Overview' tab. The list contains 7 items, all of which are system files located at 'M:\Windows\System32\config'. The columns in the table include ID, Name, Label, Item #, Ext, Path, Category, P-Size, L-Size, MD5, SHA1, and SH4256. The last three columns show the creation, access, and modification dates. The total size of the selected files is 36.77 MB.

ID	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SH4256	Created	Accessed	Modified
001	DEFAUL.T.SAV		1550	sav	Mantooth32.E01\Part...\\Windows\System32\config	File	20.00 KB	20.00 KB	dbbed8... 3ad5c2...			11/2/2006 5:22...	11/2/2006 5:34...	11/2/2006 5:34...
002	NTUSER.DAT		1551	dat	Mantooth32.E01\Part...\\Windows\System32\config	File	512.0 KB	512.0 KB	37898... 6d84ef...			3/5/2007 8:26...	6/23/2007 8:24...	6/23/2007 8:24...
003	NTUSER		1589	dat	Mantooth32.E01\Part...\\Windows\System32\config	File	1792 KB	1792 KB	9c0ee... 997da...			2/27/2007 1:33...	2/12/2008 6:00...	2/12/2008 4:44...
004	SAM		1549	<missin...	Mantooth32.E01\Part...\\Windows\System32\config	File	256.0 KB	256.0 KB	6b088f... 9adfc...			11/2/2006 5:22...	2/12/2008 3:46...	2/12/2008 3:13...
005	SECURITY		1546	<missin...	Mantooth32.E01\Part...\\Windows\System32\config	File	256.0 KB	256.0 KB	1229f... bba59...			11/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 1:40...
006	SOFTWARE		1543	<missin...	Mantooth32.E01\Part...\\Windows\System32\config	File	21.75 MB	41cd6... ad0e3a...				11/2/2006 5:22...	2/12/2008 3:46...	2/12/2008 3:13...
007	SYSTEM		1540	<missin...	Mantooth32.E01\Part...\\Windows\System32\config	File	12.25 MB	12.25 MB	152a40... 4e1683...			11/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 1:59...

The screenshot shows the AccessData Registry Viewer interface. The left pane displays a tree view of registry keys under the 'SOFTWARE' category. The right pane shows detailed information for the 'CurrentVersion' key under 'Windows NT\CurrentVersion'. The key has several sub-values, including 'CurrentVersion' (REG\_SZ, value 6.0), 'CurrentBuild' (REG\_SZ, value 6000), 'SoftwareType' (REG\_SZ, value System), 'CurrentType' (REG\_SZ, value Multiprocessor Free), 'InstallDate' (REG\_DWORD, value 0x45E484DB (1172604123)), 'RegisteredOwner' (REG\_SZ, value Voltum Enterprises), 'RegisteredOrganization' (REG\_SZ, value Wes Mantooth), 'SystemRoot' (REG\_SZ, value C:\Windows), 'ProductName' (REG\_SZ, value Windows Vista (TM) Ultimate), 'ProductID' (REG\_SZ, value 89580-378-0753292-71704), 'DigitalProductId' (REG\_BINARY, value A4 00 00 03 00 00 38 39 35 38 30 2D 33 37 38 2D ...), 'EditionID' (REG\_SZ, value Ultimate), 'BuildLab' (REG\_SZ, value 6000.vista\_gdr.071009-1548), 'BuildLabEx' (REG\_SZ, value 6000.16575.x86fre.vista\_gdr.071009-1548), 'BuildGUID' (REG\_SZ, value 86727b72-ee31-4d89-9d85-b8ec5d2daf9c), 'CSDBuildNumber' (REG\_SZ, value 2), and 'PathName' (REG\_SZ, value C:\Windows).

#### 4. Find the date the OS was installed

In FTK, 'Windows NT Registry' information shows the OS was installed on 2/27/2007.

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered -

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Case Overview

File Content

**Registry SOFTWARE Information**

Install Date	2/27/2007 2:22:03 PM -0500
Product Name	Windows Vista (TM) Ultimate
Registered Organization	Volturi Enterprises
Registered Owner	Wes Mantooth
Digital Product ID	A4 00 00 00 03 00 00 00 38 39 35 38 30 2D 33 37 38 2D 30 37 35 33 32 39 32 2D 37 31 36 36 34 00 8E 00 00 00 58 31 33 2D 30 34 31 31 30 00 00 00 00 22 52 F1 84 98 8E F7 7A 9B BE FA C7 2E 74 04 00 00 00 00 00 1A 13 E4 45 C8 A6 F6 13 00 C0 CA 89 7D

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	Created	Accessed	Modified
DEFAULT.SAV		1550	sav	Mantooth32.E01\Partit...	Wind...	20.00 KB	20.00 KB	dbbedb...	3ed5c2...	11/2/2006 5:22...	11/2/2006 5:34...	11/2/2006 5:34...
NTUSER.DAT		1531	dat	Mantooth32.E01\Partit...	Wind...	512.0 KB	\$12.0 KB	378e...	6d9ef...	3/5/2007 8...	6/6/2007 8:24...	6/23/2007 6:24...
NTUSER.DAT		1589	dat	Mantooth32.E01\Partit...	Wind...	1.92 KB	0 KB	9c9e...	979db...	2/27/2007 15:21...	2/27/2008 10:00...	2/12/2008 4:44...
SAM		1549	smss...	Mantooth32.E01\Partit...	Wind...	256.0 KB	256.0 KB	0000...	0000...	11/2/2006 5:22...	11/2/2006 5:22...	11/2/2006 5:22...
SECURITY		1548	secur...	Mantooth32.E01\Partit...	Wind...	256.0 KB	256.0 KB	bba3f8...	bba3f8...	11/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 3:49...
<b>SOFTWARE</b>		1583	<msasn...	Mantooth32.E01\Partit...	Wind...	21.75 MB	410000...	410000...	410000...	11/2/2006 5:22...	2/12/2008 3:46...	2/12/2008 3:13...
SYSTEM		1540	<msasn...	Mantooth32.E01\Partit...	Wind...	12.25 MB	12.25 MB	152a40...	4e1633...	11/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 1:59...

Loaded: 7 Filtered: 7 Total: 7 Highlighted: 1 Checked: 0 Total LSize: 36.77 MB

Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\root\Windows\System32\config\SOFTWARE

Ready [Overview Tab Filter: [None]]

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered -

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Disk Image

**MANTOOH [NTFS]**

Categories:

- Applications
  - Installed
  - Prefetch
  - User Assist
- Browsing
  - URLs
- Networks
  - Network Connections
  - Network Shares
- Owner Information
- Recent File
- User
  - Current User
  - Shared Folders (LNK)
- SAM Users
- Shell Bags

Items

U. ▲ Name	Value
PathName	C:\Windows
CSBuildNumber	2
BuildGUID	8672b72-ee31-4db9-9d85-b8ec5f2da9c
BuildLabEx	6000_16575_x86fre_vista_gdr_071009-1548
BuildLab	6000_vista_gdr_071009-1548
EditorID	Ultimate
DigitalProductId4	F80400000400000038003300030003000310034003200D003300370038002D00300370035003300320039002D0030033002D00360300
DigitalProductId	A4000000030000003893538302D3337382D030735332932D03731363634000E000005831332D03043131310000000000000000225F184988EF77A9B8EFA72E740400000000001A1
ProductName	Windows Vista (TM) Ultimate
SystemRoot	C:\Windows
RegisteredOwner	Wes Mantooth
RegisteredOrganization	Volturi Enterprises
InstallDate	2008-01-22T00:00:00Z
CurrentType	MultiProcessor Free
SoftwareType	System
CurrentBuild	6000
CurrentBuildNumber	6000
CurrentVersion	6.0

Provenance

Mantooth32.E01\Partition 1\MANTOOTH [NTFS]

Ready [System Information Tab Filter: [None]]

'System Information' in FTK shows epoch timestamp which I converted to human readable time format which also showed the OS was installed on **2/27/2007**

## Convert epoch to human readable date and vice versa

1172604123

Timestamp to Human date

[batch convert timestamps to human dates]

GMT: Tuesday, February 27, 2007 7:22:03 PM

Your time zone: Tuesday, February 27, 2007 2:22:03 PM GMT-05:00

Relative: 12 years ago

Mon Day Yr Hr Min Sec

11

/

25

/

2018

:

0

:

15

:

44

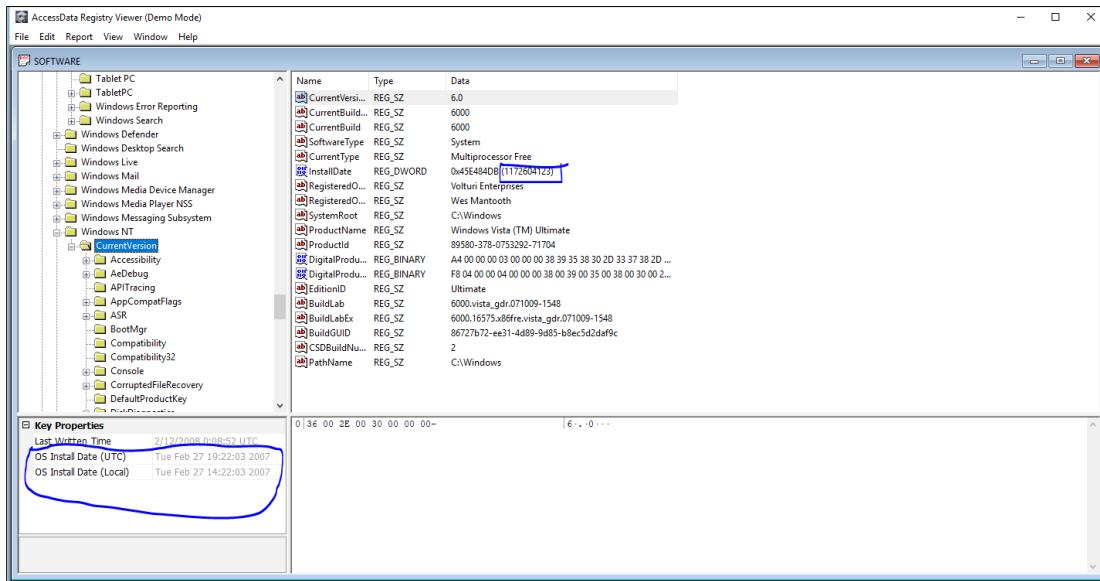
:

GMT

▼

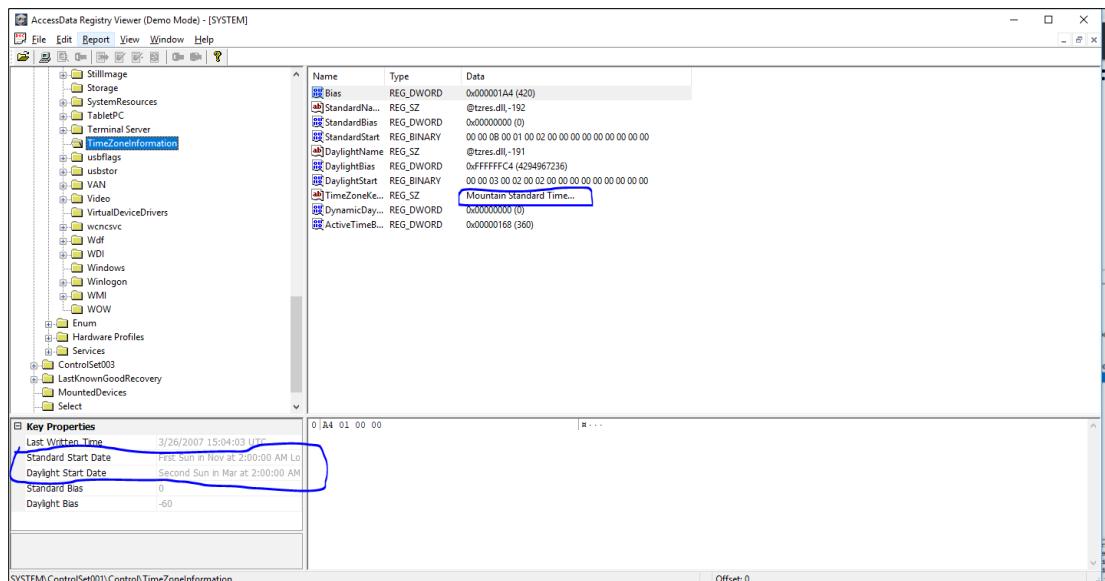
Human date to Timestamp

Likewise, when I exported **SOFTWARE** file from FTK into Access Data's Registry Viewer, I noticed installation date of the OS is **Tue Feb 27 19:22:03 2007** as shown.



## 5. Identify the Time Zone information for the computer.

After exporting the **SYSTEM** file into the registry viewer from FTK, under 'Terminal Server', time zone is shown as '**Mountain Standard Time**'.

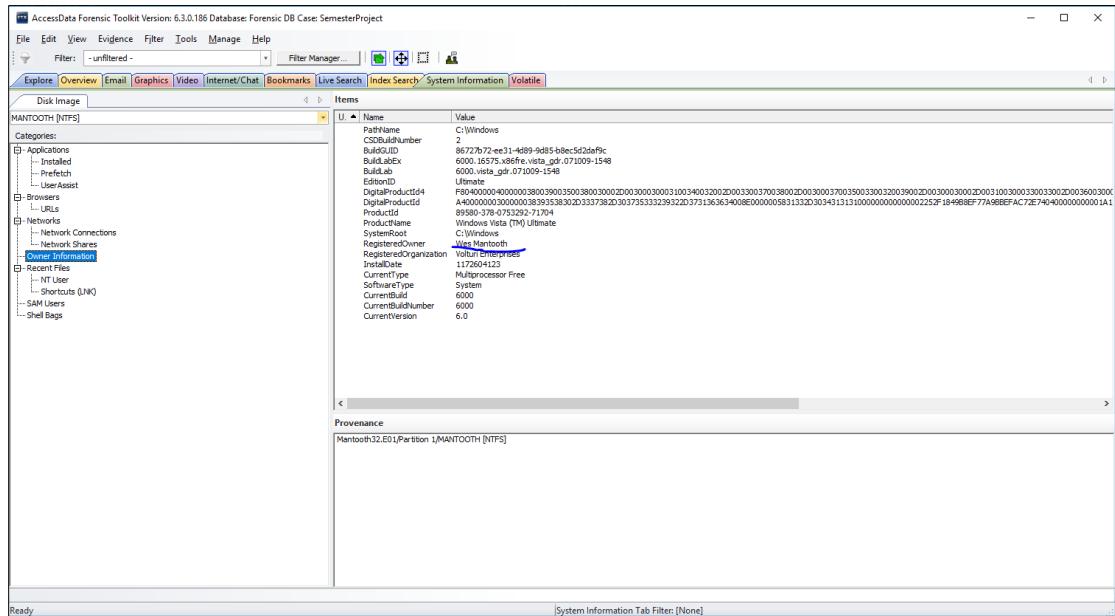


## **6. Show the owner of the computer.**

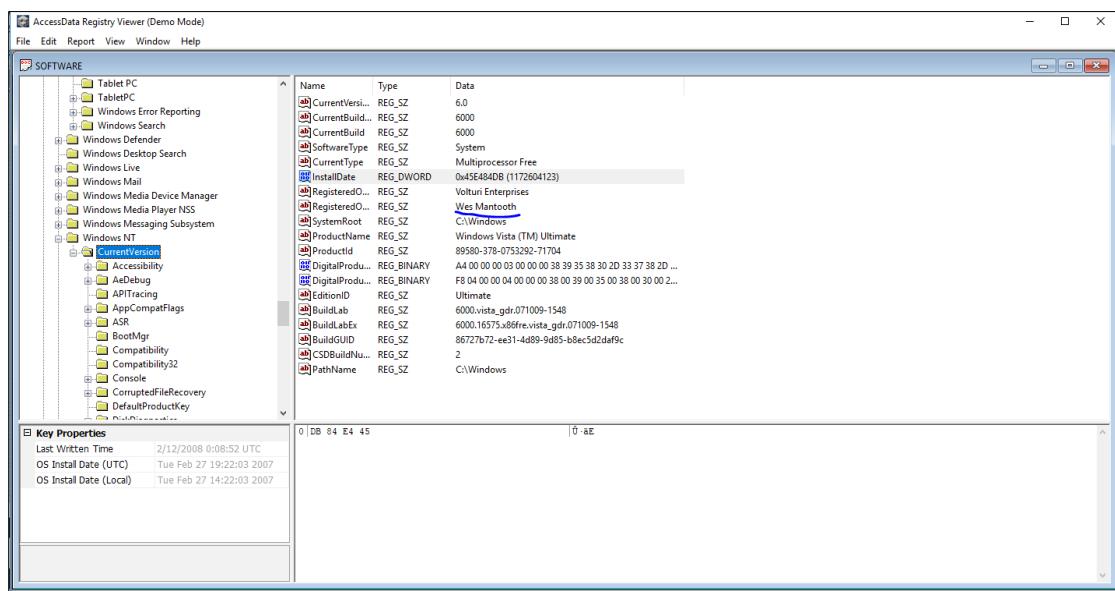
The screenshot shows the AccessData Forensic Toolkit interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, Help, and a Filter Manager dropdown. Below the menu is a toolbar with icons for Filter Manager, Find, Copy, Paste, and others. The main window has tabs for Explore, Overview, Email, Graphics, Video, Internet/Chat, Bookmarks, Live Search, Index Search, System Information, and Volatile. The 'Bookmarks' tab is selected. On the left is a tree view of the forensic case, showing categories like Graphics, Internet/Chat Files, Mobile Phone Files, Applications, CSFile System File, Disk Image, File System, Index Allocation, INDX Entry, Partition, Windows Event Log, Unknown Registry, Windows Shortcut, Other Encryption Files, Other Known Types, Plain Text, Slash-Free Spaces, Spreadsheets, Unknown Types, and User Types. The 'Unknown Registry' node is expanded. The right side displays two panes: 'Registry SOFTWARE Information' and 'File List'. The 'Registry SOFTWARE Information' pane shows details for the SOFTWARE key under HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. The 'File List' pane shows a table of files with columns: Name, Label, Item #, Ext, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, Accessed, and Modified. A file named 'SOFTWARE' is listed in the table.

In FTK, the **SOFTWARE** file shows the registered owner of the computer is '**Wes Mantooth**'.

Also, the ‘System Information’ shows the similar result as shown below.



Also, when the SOFTWARE file is exported from FTK to the registry viewer, I noticed the registered owner is named as '**Wes Mantooth**'.



## **7. Show the most active user of the computer and list all users**

SAM file in FTK displays **Wes Mantooth** has logon count of **96** as compared to other users like Administrator, Guest, Laurent and Dracula whose logon count are 1, 0, 0 and 3 respectively and hence is the most active user as shown.

The screenshot shows the AccessData Forensic Toolkit interface with the 'System Information' tab selected. The 'Item Data' table contains the following information:

Item	Item Data	hash	Item Des
Last Written time	2/12/2008 3:13:16 PM -0500		This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1000 (0x000003E8)		This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Wes Mantooth		This is the name of the user with this RID
Logon Count	96		The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	2/12/2008 2:12:08 PM -0500		This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	2/27/2007 1:29:13 PM -0500		The last time the password was changed
Expiration Time	Never		The time at which the Users password will expire
Invalid Logon count	3		The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	2/12/2008 3:13:16 PM -0500		The last time a failed logon occurred

The screenshot shows the AccessData Forensic Toolkit interface with the following details:

- User Account Information** table:
 

Item	Item Data	Item Des
Last Written time	2/27/2007 2:21:54 PM -0500	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	500 (0x000001F4)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Administrator	This is the name of the user with this RID
Description	Built-in account for administering the computer/domain	The Description of this User
Logon Count	1	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	11/2/2006 8:02:01 AM -0500	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	11/2/2006 8:08:15 AM -0500	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
- File List** table:
 

#	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
1	DEFAULT.SAV		1550	sev	Manthooth32.E01\Part1\	Wind\...	20,00 KB	20,00 KB	bdeb8b...	3d5c2...		11/2/2006 5:22...	11/2/2006 5:34...	11/2/2006 5:34...
2	NTUSER.DAT		1531	dat	Manthooth32.E01\Part1\	Wind\...	512,0 KB	512,0 KB	378989...	6d94ef...		3/5/2007 8:26...	6/2/2007 8:24...	6/2/2007 8:24...
3	NTUSER.DAT		1589	dat	Manthooth32.E01\Part1\	Wind\...	179,2 KB	179,2 KB	90dec...	997ddaa...		2/27/2007 1:33...	2/12/2008 6:00...	2/12/2008 4:44...
4	SAM		1540	<missn>	Manthooth32.E01\Part1\	Wind\...	256,0 KB	256,0 KB	6089f7...	9afdfc...		11/2/2006 5:22...	2/12/2008 9:46...	2/12/2008 3:13...
5	SECURITY		1546	<missn>	Manthooth32.E01\Part1\	Wind\...	256,0 KB	256,0 KB	bba595...			11/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 1:40...
6	SOFTWARE		1543	<missn>	Manthooth32.E01\Part1\	Wind\...	21,75 MB	21,75 MB	41c0e...	ad0e3a...		11/2/2006 5:22...	2/12/2008 3:13...	2/12/2008 3:13...
7	SYSTEM		1540	<missn>	Manthooth32.E01\Part1\	Wind\...	12,25 MB	12,25 MB	524a9...	4e1683...		11/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 1:59...

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: -Unfiltered - Filter Manager... | Hex Text Filtered Natural

Explorer Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Case Overview

File Content

Item	Item Data	Item Des
Last Written time	2/12/2008 3:13:17 PM -0500	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1002 (0x000003EA)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	dracula	This is the name of the user with this RID
Full Name	Count Dracula	The full name of the user
Description	The Tooth Account	The Description of this User
Logon Count	3	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	4/1/2007 8:30:58 PM -0400	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	4/1/2007 8:30:39 PM -0400	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	2	The number of times an unsuccessful logon attempt has been made since the last successful logon

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
DEFALKT.SAV		1500	sav	Manooth32.E01\Partit...	Wind...	20.00 KB	20.00 KB	dbbed3...	3d5c5...	11/2/2006 5:22...	11/2/2006 5:34...	11/2/2006 5:34...	
NTUSER.DAT		1531	dat	Manooth32.E01\Partit...	Wind...	512.0 KB	512.0 KB	378a8...	6d84ef...	3/6/2007 6:36...	6/2/2007 6:24...	6/2/2007 6:24...	
NTUSER.DAT		1598	dat	Manooth32.E01\Partit...	Wind...	1792 KB	1792 KB	9c0eac...	997d6f...	2/27/2007 1:33...	5/12/2008 6:00...	5/12/2008 6:44...	
SAM		1549	cnssm...	Manooth32.E01\Partit...	Wind...	256.0 KB	256.0 KB	bba99f...	9efffc...	11/2/2006 5:22...	2/12/2008 1:46...	2/12/2008 1:13...	
SECURITY		1546	<cnssm...>	Manooth32.E01\Partit...	Wind...	256.0 KB	256.0 KB	1229f6...	bba59...	11/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 1:40...	
SOFTWARE		1543	<cnssm...>	Manooth32.E01\Partit...	Wind...	21.75 MB	21.75 MB	41cded...	ad0e3a...	11/2/2006 5:22...	2/12/2008 3:46...	2/12/2008 3:13...	
SYSTEM		1540	<cnssm...>	Manooth32.E01\Partit...	Wind...	12.25 MB	12.25 MB	152a40...	4e1683...	11/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 1:59...	

Loaded: 7 Filtered: 7 Total: 7 Highlighted: 1 Checked: 0 Total LSize: 36.77 MB

Manooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\Windows\System32\config\SAM

Ready Overview Tab Filter: [None]

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: -Unfiltered - Filter Manager... | Hex Text Filtered Natural

Explorer Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Case Overview

File Content

Item	Item Data	Item Des
Last Written time	2/11/2008 7:13:36 PM -0500	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1003 (0x000003EB)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Laurent	This is the name of the user with this RID
Full Name	Laurent	The full name of the user
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
DEFALKT.SAV		1550	sav	Manooth32.E01\Partit...	Wind...	20.00 KB	20.00 KB	dbbed3...	3d5c5...	11/2/2006 5:22...	11/2/2006 5:34...	11/2/2006 5:34...	
NTUSER.DAT		1531	dat	Manooth32.E01\Partit...	Wind...	1792 KB	1792 KB	378a8...	6d84ef...	3/6/2007 6:36...	6/2/2007 6:24...	6/2/2007 6:24...	
NTUSER.DAT		1598	dat	Manooth32.E01\Partit...	Wind...	1792 KB	1792 KB	9c0eac...	997d6f...	2/27/2007 1:33...	5/12/2008 6:00...	5/12/2008 6:44...	
SAM		1549	cnssm...	Manooth32.E01\Partit...	Wind...	256.0 KB	256.0 KB	bba99f...	9efffc...	11/2/2006 5:22...	2/12/2008 1:46...	2/12/2008 1:13...	
SECURITY		1546	<cnssm...>	Manooth32.E01\Partit...	Wind...	256.0 KB	256.0 KB	1229f6...	bba59...	11/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 1:40...	
SOFTWARE		1543	<cnssm...>	Manooth32.E01\Partit...	Wind...	21.75 MB	21.75 MB	41cded...	ad0e3a...	11/2/2006 5:22...	2/12/2008 3:46...	2/12/2008 3:13...	
SYSTEM		1540	<cnssm...>	Manooth32.E01\Partit...	Wind...	12.25 MB	12.25 MB	152a40...	4e1683...	11/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 1:59...	

Loaded: 7 Filtered: 7 Total: 7 Highlighted: 1 Checked: 0 Total LSize: 36.77 MB

Manooth32.E01\Partition 1\MANTOOTH [NTFS]\[root]\Windows\System32\config\SAM

Ready Overview Tab Filter: [None]

**Case Overview**

- Graphics (770 / 770)
  - Internet/Chat Files (72 / 72)
  - Mobile Phone (0 / 0)
  - Multimedia (7 / 7)
    - Disk Image (1 / 1)
    - File System (2 / 2)
      - Index Allocation (124 / 124)
      - INDEX Entry (49 / 49)
      - Logical (2 / 2)
      - Windows Event Log (7 / 7)
      - Windows NT Registry (7 / 7)
      - Windows Shortcut (156 / 156)
    - Other Encryption Files (17 / 17)
    - Other Known Types (2 / 2)
    - Printers (2 / 2)
    - ScanFree Search (47 / 47)
    - Spreadsheets (2 / 2)
    - Unknown Types (219 / 219)
    - User Types (0 / 0)
  - Email Status (0 / 0)
  - Bookmarks (0 / 0)
  - Cluster Topic (0 / 0)

**File Content**

Key	Value	Description
LogonCount	0	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc). This is the unique identifier portion of the RID that identifies the user on the machine.
User Name	Guest	This is the name of the user with this RID
Description	Built-in account for guest access to the computer/domain	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the user's password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred

**File List**

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	Shr256	Created	Accessed	Modified
DEFAULT.SAV		1550	sav	Mantooth32.E01\Partiti...	Windo...	20,00 KB	20,00 KB	ddbe8...	3ad5c2...		11/2/2006 5:22...	11/2/2006 5:34...	11/2/2006 5:34...
NTUSER.DAT		1531	dat	Mantooth32.E01\Partiti...	Windo...	512,0 KB	512,0 KB	378a98...	6d94ef...		3/5/2007 8:24...	6/23/2007 8:24...	6/23/2007 8:24...
NTUSER.DAT		1589	dat	Mantooth32.E01\Partiti...	Windo...	1792 KB	970ce...	997dd...			2/27/2007 1:33...	2/12/2008 6:00...	2/12/2008 4:44...
SAM		1549	mssam	Mantooth32.E01\Partiti...	Windo...	256,0 KB	256,0 KB	600e9f...	faafdc...		11/2/2006 5:22...	2/12/2008 3:46...	2/12/2008 3:13...
SECURITY		1545	mssam	Mantooth32.E01\Partiti...	Windo...	256,0 KB	256,0 KB	1229fb...	bba9f9...		11/2/2006 5:22...	7/14/2007 3:40...	7/14/2007 1:40...
SOFTWARE		1543	mssam	Mantooth32.E01\Partiti...	Windo...	21,75 MB	21,75 MB	41ced0...	a0de3a...		11/2/2006 5:22...	2/12/2008 3:46...	2/12/2008 3:13...
SYSTEM		1540	mssam	Mantooth32.E01\Partiti...	Windo...	12,25 MB	12,25 MB	152a40...	4e1683...		11/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 1:59...

Loaded: 7 Filtered: 7 Total: 7 Highlighted: 1 Checked: 0 Total Size: 36.77 MB

Mantooth32.E01\partition 1\MANTOOTH [NTFS]\root\Windows\System32\config\SAM

Ready... [Overview Tab Filter: [None]]

## 8. Identify user accounts and who uses the account.

Exporting SAM file into registry viewer shows, user accounts are **Wes Mantooth, Dracula and Laurent, Administrator and Guest**. Their account disabled status is false. Amongst them, Wes Mantooth and Dracula uses their account since their logon count are 96 and 3 respectively as shown in “Key properties”.

**AccessData Registry Viewer - [SAM(1549).tmp]**

**Key Properties**

Last Written Time	2/27/2007 19:21:54 UTC
SID unique identifier	500
User Name	administrator
Description	Built-in account for administering the computer.
Logon Count	1
Last Logon Time	11/2/2006 13:02:01 UTC
Last Password Change Time	11/2/2006 13:08:15 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never

**File List**

Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 F6 63 5A 16 7F FE C6 01 00 00 ...
V	REG_BINARY	00 00 00 BC 00 00 02 00 01 BC 00 00 01 A0 00 ...

**Hex View**

```

00 02 00 01 00 00 00 00 F6 63 5A 16 7F FE C6 01 00 00 ...
10 00 00 00 00 00 00 00 E6 AD 81 F5 7F FE C6 01 00 00 ...
20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
30 F4 01 00 00 01 02 00 00 11 02 00 00 00 00 00 ...
40 00 00 01 00 01 00 00 00 00 00 00 00 33 00 00 00 ...

```

Offset: 0

AccessData Registry Viewer - [SAM[1549].tmp]

File Edit Report View Window Help

SAM[1549].tmp

SAM Domains Account Users Builtin RXACT

Name Type Data

F REG\_BINARY 02 00 01 00 00 00 00 4B E3 54 29 AB 6D C8 01 00 00 ...  
y REG\_BINARY 00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 18 00 ...  
UserPasswor... REG\_BINARY 69 00 6E 00 20 00 79 00 6F 00 75 00 72 00 20 00 66 00 ...  
UserTite REG\_BINARY 01 00 00 00 03 00 00 00 01 00 00 00 38 7C 00 00 42 4D ...

Key Properties

Last Written Time: 2/12/2008 20:13:16 UTC  
SID unique identifier: 1000  
User Name: Was Mantis  
Logon Count: 18  
Last Logon Time: 2/12/2008 19:12:08 UTC  
Last Password Change Time: 2/27/2007 18:29:13 UTC  
Expiration Time: Never  
Invalid Logon Count: 3  
Last Failed Login Time: 2/12/2008 20:13:16 UTC  
Account Disabled: False

00 02 00 01 00 00 00 00-4B E3 54 29 AB 6D C8 01 .....-K8]-mE-  
00 00 00 00 00 00 00-C6 F4 0A 2E 9D 5A C7 01 .....-E5-.-2C-  
20 FF FF FF FF FF FF 7F-B4 63 14 B4 B3 6D C8 01 yyyyyyy-c-`mE-  
30 E8 03 00 00 01 02 00 00-14 02 00 00 00 00 00 00 .....-.....-  
40 03 00 00 00 01 00 00 00-00 00 00 33 00 CC 2B 27 75 .....-3-i+u

SAM[1549].tmp\SAM.Domains\Account\Users\000003E8

Offset: 0

**AccessData Registry Viewer - [SAM[1549].tmp]**

File Edit Report View Window Help

SAM[1549].tmp

- SAM
  - Domains
    - Account
      - Aliases
      - Groups
      - Users
        - 000001F4
        - 000001F5
        - 000003E8
        - 000003EA**
        - 000003EB
        - Names
  - Builtin
  - RXACT

Name	Type	Data
<b>F</b>	REG_BINARY	02 00 01 00 00 00 00 72 FC 4C 2F BE 74 C7 01 00 ...
<b>V</b>	REG_BINARY	00 00 00 00 D4 00 00 00 02 00 01 00 D4 00 00 00 0E 00 ...

**Key Properties**

  - Last Written Time: 2/12/2008 20:13:17 UTC
  - SID unique identifier: 1002
  - User Name: Dracula
  - Full Name: Count Dracula
  - Description: The Tooth Account
  - Logon Count: 3
  - Last Logon Time: 4/2/2007 0:30:58 UTC
  - Last Password Change Time: 4/2/2007 0:30:39 UTC
  - Expiration Time: Never
  - Invalid Logon Count: 2

SAM[1549].tmp\SAM\Domains\Account\Users\000003EA

Offset: 0

**AccessData Registry Viewer - [SAM[1549].tmp]**

File Edit Report View Window Help

SAM[1549].tmp

- SAM
  - Domains
    - Account
      - Aliases
      - Groups
      - Users
        - 000001F4
        - 000001F5
        - 000003E8
        - 000003EA**
        - 000003EB**
        - Names
  - Builtin
  - RXACT

Name	Type	Data
<b>F</b>	REG_BINARY	02 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
<b>V</b>	REG_BINARY	00 00 00 00 D4 00 00 00 02 00 01 00 D4 00 00 00 0E 00 ...
<b>UserTile</b>	REG_BINARY	01 00 00 03 00 00 00 01 00 00 00 58 7C 00 00 42 4D ...

**Key Properties**

  - Last Written Time: 2/12/2008 0:13:36 UTC
  - SID unique identifier: 1003
  - User Name: Laurent
  - Full Name: Laurent
  - Logon Count: 0
  - Last Logon Time: Never
  - Last Password Change Time: Never
  - Expiration Time: Never
  - Invalid Logon Count: 0
  - Last Failed Login Time: Never

SAM[1549].tmp\SAM\Domains\Account\Users\000003EB

Offset: 0

## 9. Acquire user passwords.

I exported **SAM** and **SYSTEM** files to **PRTK** and cracked passwords of two user accounts namely Dracula and Wes Mantooth. The password for Dracula is “**canine**” while that for Wes Mantooth is “**tooth**”.

The screenshot shows the AccessData Forensic Toolkit interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, Help. The tabs at the top are Explorer, Overview, Email, Graphics, Video, Internet/Chat, Bookmarks, Live Search, Index Search, System Information, and Volatile. The main window has two panes: 'Case Overview' on the left and 'File Content' on the right. In 'Case Overview', there are several categories like Graphics, OS File System Files, and Other Evidence Types. In 'File Content', the 'User Account Information' tab is selected, displaying details for the Administrator account. The 'Item Data' section includes fields for Last Written time (2/27/2007 2:21:54 PM -0500), RID unique identifier (500 (0x000001F4)), User Name (Administrator), Description (Built-in account for administering the computer/domain), Logon Count (1), Last Logon Time (11/2/2006 8:02:01 AM -0500), Last Password Change Time (11/2/2006 8:08:15 AM -0500), and Expiration Time (Never). The 'Item Des' column provides descriptions for each field. Below this is the 'File List' pane, which shows a table of files with columns: Name, Label, Item #, Ext, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, Accessed, and Modified. Several files are listed, including DEFAULT.SAV, NTUSER.DAT, and SYSTEM. The SYSTEM file is circled in blue. At the bottom, status bars show 'Loaded: 7', 'Filtered: 7', 'Total: 7', 'Highlighted: 1', 'Checked: 0', 'Total LSize: 36.77 MB', and 'Mantooth32.E01/Partition 1/MANTOTH (NTFS)/[root]/Windows/System32/config/SAM'. The status bar also indicates 'Ready'.

**Add Job Wizard (Page 2 of 2)**

**File Types**

SAM password file:

**Files**

C:\Users\srangari\Desktop\Semester Project\Final Project\3\SAM

**Module Options**

**File Info:**

File: C:\Users\srangari\Desktop\Semester Project\Final Project\3\SAM  
File type: SAM password file  
File version: N/A

**Available attacks for this file:**

Select a user and password hash version

<b>Administrator</b>
<input checked="" type="checkbox"/> NT hash
<b>Dracula</b>
<input checked="" type="checkbox"/> NT hash

Enter a file with the startkey information for this SAM file. The startkey is usually found in the file called 'SYSTEM' located in 'Windows\System32\config'. Occasionally the startkey is found on a floppy disk in a file named 'startkey.key'

In rare cases the startkey is not contained in any file and is instead derived from a passphrase. If you know the passphrase, enter it here:

If the startkey is derived from a passphrase and you do not know it, check this box to run a dictionary attack on it. (All other jobs from this SAM file will have to wait until this job is successful.)

**Buttons:**  
Apply Save File Type Defaults Go Back Finish Cancel

AccessData Password Recovery Toolkit

File Edit View Tools Help

View All

Job Name	Attack Type	Status	Result
SAM	Windows account: Administrator [NT hash]	Finished	*Empty*
SAM	Windows account: Dracula [NT hash]	Finished	canine [HEX=00630061006e...]
SAM	Windows account: Guest [LAN hash]	Finished	*Empty*
SAM	Windows account: Laurent [LAN hash]	Finished	*Empty*
SAM	Windows account: Wes Mantooth [NT hash]	Finished	tooth [HEX=0074006f006f00...

**Properties**

**Job Information**

- Attack Type:
- Module:
- Profile:
- Status:
- Difficulty:
- Begin Time:
- End Time:
- Timeout After:
- Decryptable:
- Result Type:
- Results:
- Comments:

**File Information**

- Filename:
- Type:
- Version:
- Size:
- MD5:
- SHA-1:
- Created:
- Modified:

## 10. Identify the last date Wes Mantooth logged on.

SAM file delineates last logon date of Wes Mantooth was **2/12/2008** as shown in below screenshot.

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: unfiltered Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Case Overview

File Content

Last Written time: 2/27/2007 2:21:54 PM -0500

Item Data

RID unique identifier	500 (0x000001F4)	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
User Name	Administrator	This is the unique identifier portion of the RID that identifies the user on the machine
Description	Built-in account for administering the computer/domain	The Description of this User
Logon Count	1	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	11/2/2006 8:02:01 AM -0500	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	11/2/2006 8:08:15 AM -0500	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	True	This account has been disabled by the administrator

File List

Name	Label	Item #	Ext.	Path	Category	P.Size	L.Size	MD5	SHA1	SHA256	Created	Accessed	Modified
DEFAULT.SAV		1550	sav	Mantooth32.E01\Partitions\Wind...	Wind...	20.00 KB	20.00 KB	dbe8d1...	3ef5c2...	11/2/2006 5:22...	11/2/2006 5:24...	11/2/2006 5:24...	
NTUSER.DAT		1531	dat	Mantooth32.E01\Partitions\Wind...	Wind...	512.0 KB	512.0 KB	378a9...	6d94ef...	3/5/2007 8:26...	6/23/2007 8:24...	6/23/2007 8:24...	
NTUSER.DAT		1589	dat	Mantooth32.E01\Partitions\Wind...	Wind...	1792 KB	90ece...	997d4a...		2/27/2007 1:33...	2/12/2008 6:09...	2/12/2008 4:44...	
SAM		1549	<missin...	Mantooth32.E01\Partitions\Wind...	Wind...	256.0 KB	256.0 KB	6089ff...	9afdfc...	11/2/2006 5:22...	2/12/2008 3:46...	2/12/2008 3:13...	
SECURITY		1546	<missin...	Mantooth32.E01\Partitions\Wind...	Wind...	256.0 KB	1229ff...	bba5f9...		11/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 1:40...	
SOFTWARF		1543	<missin...	Mantooth32.E01\Partitions\Wind...	Wind...	21.75 MB	21.75 MB	41r9n...	ad9e%	11/7/2006 5:22...	7/17/2008 3:46...	7/17/2008 3:13...	

Loaded: 7 Filtered: 7 Total: 7 Highlighted: 1 Checked: 0 Total LSize: 36.77 MB

Mantooth32.E01\Partition 1\MANTOOOTH [NTFS]\root\Windows\System32\config\SAM

Ready Overview Tab Filter: [None]

## 11. Identify files placed in the recycle bin by Wes Mantooth.

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Disk Image

	SID	User Name	Current LAN Hash	Previous LAN Hash	Current NT Hash	Previous NT Hash
5-1-21-3166329-3263506726-1320359247-1000	<u>Wes Mantooth</u>				4F892A810F871BC640DC16B932220E9	
5-1-21-3166329-3263506726-1320359247-500	Administrator				31D6CFE0D16AE931B73C5907E0C089C0	
5-1-21-3166329-3263506726-1320359247-1003	Laurent				D90D8508030C90473114B90EFF3FE9E	
5-1-21-3166329-3263506726-1320359247-1002	Dracula					

Categories:

- Applications
  - Installed
  - Prefetch
  - User Assist
- Browsers
  - URLs
- Networks
  - Host Connections
  - Network Shares
- Owner Information
- Recent Files
  - NT User
  - Shortcuts (.LNK)
- SAM Users
- Shell Bags

Provenance

Mantooth32.E01\Partition 1\MANTOOOTH [NTFS]

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

File Content

Hex Text Filtered Natural

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Carved [103924].html		4193	html	Mantooth32.E01\Partit...	HTML	n/a	448 B	9363b...	532e2...		n/a	n/a	n/a
Carved [1309543].bmp		4194	bmp	Mantooth32.E01\Partit...	Bitmap	n/a	2102 B	6d979...	030117...		n/a	n/a	n/a
Carved [1311839].html		4195	html	Mantooth32.E01\Partit...	HTML	n/a	13 B	b249c...	1ae52...		n/a	n/a	n/a
Carved [1311715].html		4196	html	Mantooth32.E01\Partit...	HTML	n/a	76 B	0e6f0...	54620...		n/a	n/a	n/a
Carved [1311781].html		4197	html	Mantooth32.E01\Partit...	HTML	n/a	18 B	e3fffa...	00174...		n/a	n/a	n/a
Carved [1321579].bmp		4198	bmp	Mantooth32.E01\Partit...	Bitmap	n/a	62 B	663aa...	a0992...		n/a	n/a	n/a
Carved [1321719].bmp		4199	bmp	Mantooth32.E01\Partit...	Bitmap	n/a	54 B	6a665...		n/a	n/a	n/a	
Carved [1322719].bmp		4200	bmp	Mantooth32.E01\Partit...	Bitmap	n/a	62 B	13262...	17746...		n/a	n/a	n/a
Carved [1359421].bmp		4201	bmp	Mantooth32.E01\Partit...	Bitmap	n/a	62 B	13262...	17746...		n/a	n/a	n/a
Carved [1400].jpg		4245	jpg	Mantooth32.E01\Partit...	JPEG	n/a	4276 B	f7777...	f63be2...		n/a	n/a	n/a
Carved [1400].png		4237	png	Mantooth32.E01\Partit...	JPEG	n/a	4203 B	d169m...	21867...		n/a	n/a	n/a
Carved [1452].jpg		4239	jpg	Mantooth32.E01\Partit...	JPEG	n/a	4299 B	9926b...	9b567...		n/a	n/a	n/a
Carved [1501].jpg		4235	jpg	Mantooth32.E01\Partit...	JPEG	n/a	4039 B	03011...	03473...		n/a	n/a	n/a
Carved [1591].jpg		4230	jpg	Mantooth32.E01\Partit...	JPEG	n/a	1470 B	78a4b...	8901b...		n/a	n/a	n/a
Carved [2051].png		4322	png	Mantooth32.E01\Partit...	JPEG	n/a	1525 B	f363e...	79814...		n/a	n/a	n/a
Carved [332].jpg		4243	jpg	Mantooth32.E01\Partit...	JPEG	n/a	1784 B	7c153...	abf49...		n/a	n/a	n/a
Carved [332].png		4231	png	Mantooth32.E01\Partit...	JPEG	n/a	1525 B	f363e...	79814...		n/a	n/a	n/a
Carved [332].jpeg		4235	jpeg	Mantooth32.E01\Partit...	JPEG	n/a	1884 B	74593...	0f251...		n/a	n/a	n/a
Carved [332].peo		4233	peo	Mantooth32.E01\Partit...	JPEG	n/a	1713 B	0841f...	799bd...		n/a	n/a	n/a
Carved [332].peo		4254	peo	Mantooth32.E01\Partit...	JPEG	n/a	1801 B	0841f...	0841f...		n/a	n/a	n/a
Carved [332].peo		4247	peo	Mantooth32.E01\Partit...	JPEG	n/a	1801 B	6-6514...	04948...		n/a	n/a	n/a
Carved [332].peo		4241	peo	Mantooth32.E01\Partit...	JPEG	n/a	1723 B	77844...	4d30e...		n/a	n/a	n/a
Carved [332].peo		4249	peo	Mantooth32.E01\Partit...	JPEG	n/a	1470 B	7644b...	8901b...		n/a	n/a	n/a

Load: 111 Filtered: 111 Total: 111 Highlighted: 1 Checked: 0 Total LSC: 11,241MB

Mantooth32.E01\Partition 1\MANTOOOTH [NTFS]\\$recycle.Bin\\$1-5-21-3166329-3263506726-1320359247-1000\\$R61QDF.exe-Carved[1311839].bmp

Ready Explore Tab Filter: (None)

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

File Content Hex Text Filtered Natural

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified		
Carved [111].jpeg		4240	jpeg	Mantooth32.E01\Partit...	JPEG	n/a	4299	992fb...	9d4d73...	n/a	n/a	n/a	n/a		
Carved [7409].html		4253	html	Mantooth32.E01\Partit...	HTML	n/a	79	8000...	792f9...	n/a	n/a	n/a	n/a		
Carved [8226].html		4252	html	Mantooth32.E01\Partit...	HTML	n/a	152	152	792f9...	n/a	n/a	n/a	n/a		
chromecast_firming_teeth...		1456	html	Mantooth32.E01\Partit...	HTML	n/a	39,50 KB	39,50 KB	7294b...	7/25/2007 7:41...	7/25/2007 7:41...	7/24/2007 4:35...	7/24/2007 4:35...		
dcl_beard.jpg		1462	jpg	Mantooth32.E01\Partit...	JPEG	n/a	38,68 KB	f05c1...	e4f94...	7/25/2007 7:41...	7/24/2007 7:41...	10/6/2006 10:5...	10/6/2006 10:5...		
DCL.jpg		3493	jpg	Mantooth32.E01\Partit...	JPEG	n/a	8889 B	8889 B	ad368...	a8f4e...	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
DCIGR.jpg		3494	jpg	Mantooth32.E01\Partit...	JPEG	n/a	8070 B	e1862...	29129...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
desktop.ini		1248	ini	Mantooth32.E01\Partit...	7-bit text	136 B	129	a5269...	2d952...	2/27/2007 1:34...	9/26/2007 3:56...	2/27/2007 1:34...	2/27/2007 1:34...		
desktop.ini		1479	ini	Mantooth32.E01\Partit...	INDEX E...	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	
DISCGR.jpg		3495	jpg	Mantooth32.E01\Partit...	JPEG	n/a	10,76 KB	c0545...	9d5...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
FILBLIST.properties		3497	propert...	Mantooth32.E01\Partit...	7-bit text	n/a	1389 B	1fe5d...	207676...	n/a	n/a	n/a	10/9/2006 9:36...	10/9/2006 9:36...	
FINGERPRINT.jpg		3498	jpg	Mantooth32.E01\Partit...	JPEG	n/a	78,81 KB	5cd2d...	5c9295...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
go.jpg		3810	jpg	Mantooth32.E01\Partit...	JPEG E...	n/a	16,80 KB	18d9...	c9831c...	n/a	n/a	n/a	10/9/2006 9:40...	10/9/2006 9:40...	
go_press.jpg		3811	jpg	Mantooth32.E01\Partit...	JPEG E...	n/a	16,40 KB	18d90...	18d909...	n/a	n/a	n/a	10/9/2006 9:35...	10/9/2006 9:35...	
go_...		3812	jpg	Mantooth32.E01\Partit...	JPEG E...	n/a	16,40 KB	18d90...	18d909...	n/a	n/a	n/a	10/9/2006 9:35...	10/9/2006 9:35...	
KCB.jpg		3499	jpg	Mantooth32.E01\Partit...	JPEG	n/a	12331 B	17565...	b594...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
KCRG.jpg		3500	jpg	Mantooth32.E01\Partit...	JPEG	n/a	7110 B	6004c...	b594de...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
MANIFEST.MF		3817	mf	Mantooth32.E01\Partit...	7-bit text	n/a	112 B	2e702...	ac1b80...	n/a	n/a	n/a	1/1/2007 9:33...	1/1/2007 9:33...	
MBR		1003		Mantooth32.E01\Untar...	Metadata	n/a	512 B	5361b...	a6819...	n/a	n/a	n/a	n/a	n/a	
MC.jpg		3801	jpg	Mantooth32.E01\Partit...	JPEG	n/a	12,93 KB	45329...	488369...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
MCGR.jpg		3802	jpg	Mantooth32.E01\Partit...	JPEG	n/a	9823 B	45323...	d88369...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
META-INF		3816		Mantooth32.E01\Partit...	Folder	n/a	0 B	0 B	00139...	00139...	n/a	n/a	n/a	1/13/2007 3:44...	1/13/2007 3:44...
old_people.json		1460	jpg	Mantooth32.E01\Partit...	JPEG	n/a	29,50 KB	29,36 KB	9a2c5...	cce5f...	7/25/2007 7:41...	7/25/2007 7:41...	7/24/2007 4:32...	7/24/2007 4:32...	
old_people.json		1461	json	Mantooth32.E01\Partit...	JSON	n/a	174 B	174 B	174 B	174 B	7/25/2007 7:41...	7/25/2007 7:41...	7/25/2007 7:41...	7/25/2007 7:41...	
optionCorrupted.jpg		3813	jpg	Mantooth32.E01\Partit...	JPEG E...	n/a	16,43 KB	46d69c...	289...	n/a	n/a	n/a	10/4/2006 8:53...	10/4/2006 8:53...	
optionCorrupted.jpg		3814	jpg	Mantooth32.E01\Partit...	JPEG E...	n/a	15,47 KB	d2846...	13e32...	n/a	n/a	n/a	10/4/2006 8:58...	10/4/2006 8:58...	
optionCorrupted.jpg		3815	jpg	Mantooth32.E01\Partit...	JPEG E...	n/a	17,57 KB	9af1c...	9af1c...	n/a	n/a	n/a	10/4/2006 8:57...	10/4/2006 8:57...	
Readme.txt		3405	txt	Mantooth32.E01\Partit...	7-bit text	n/a	354 B	627ed...	5eb9d...	n/a	n/a	n/a	1/30/2007 5:48...	1/30/2007 5:48...	
Really Old Image		1457		Mantooth32.E01\Partit...	Folder	n/a	56 B	56 B	56 B	56 B	7/25/2007 7:41...	7/25/2007 7:41...	8/4/2007 12:04...	8/4/2007 12:04...	
StringImage.jpg		1458	jpg	Mantooth32.E01\Partit...	JPEG	n/a	11,50 KB	2e702...	490ef8...	n/a	n/a	n/a	7/25/2007 7:41...	7/25/2007 7:41...	
User Old Images		1459		Mantooth32.E01\Partit...	Folder	n/a	131 B	131 B	131 B	131 B	7/25/2007 7:41...	7/25/2007 7:41...	7/25/2007 7:41...	7/25/2007 7:41...	
Thumbnail		3803	db	Mantooth32.E01\Partit...	Thumbn...	n/a	76,50 KB	3687b...	5094c...	n/a	n/a	n/a	1/13/2007 3:45...	1/13/2007 3:45...	
validateCreditCard1.d...		3818	class	Mantooth32.E01\Partit...	Java Cl...	n/a	436 B	f4f4...	ee7610...	n/a	n/a	n/a	1/1/2007 9:30...	1/1/2007 9:30...	
validateCreditCard1.d...		3819	class	Mantooth32.E01\Partit...	Java Cl...	n/a	1479 B	7d6e2...	88452...	n/a	n/a	n/a	1/1/2007 9:30...	1/1/2007 9:30...	
validateCreditCard1.d...		3820	class	Mantooth32.E01\Partit...	Java Cl...	n/a	1248 B	0a49cc...	f03018...	n/a	n/a	n/a	1/1/2007 9:30...	1/1/2007 9:30...	
validateCreditCard1.d...		3821	class	Mantooth32.E01\Partit...	Java Cl...	n/a	17,47 KB	40f1c...	203139...	n/a	n/a	n/a	1/1/2007 9:30...	1/1/2007 9:30...	
validateCreditCard1.d...		3824	class	Mantooth32.E01\Partit...	Java Cl...	n/a	40 B	40 B	40 B	40 B	n/a	n/a	1/13/2007 3:45...	1/13/2007 3:45...	
VCC_ABOUT.jpg		3804	jpg	Mantooth32.E01\Partit...	JPEG	n/a	14,37 KB	1cc140...	5d61ff...	n/a	n/a	n/a	1/13/2007 3:45...	1/13/2007 3:45...	
VISA.jpg		3805	jpg	Mantooth32.E01\Partit...	JPEG	n/a	9680 B	8d448...	8d4b2...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
VISAGI.jpg		3806	jpg	Mantooth32.E01\Partit...	JPEG	n/a	7223 B	3758b...	5d600...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
woman.jpg		1455	jpg	Mantooth32.E01\Partit...	JPEG	n/a	11,50 KB	11,53 KB	a2b9e...	e6558b...	7/25/2007 7:41...	7/25/2007 7:41...	7/24/2007 4:36...	7/24/2007 4:36...	

Loaded: 111 | Filtered: 111 | Total: 111 | Highlighted: 1 | Checked: 0 | Total Size: 11.24 MB

Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\root\\$Recycle.Bin\\$-1-5-21-3166329-3263506726-1320359247-1000\\$R61QDF.exe-Carved [131189].bmp

Ready | Explore Tab Filter: [None]

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

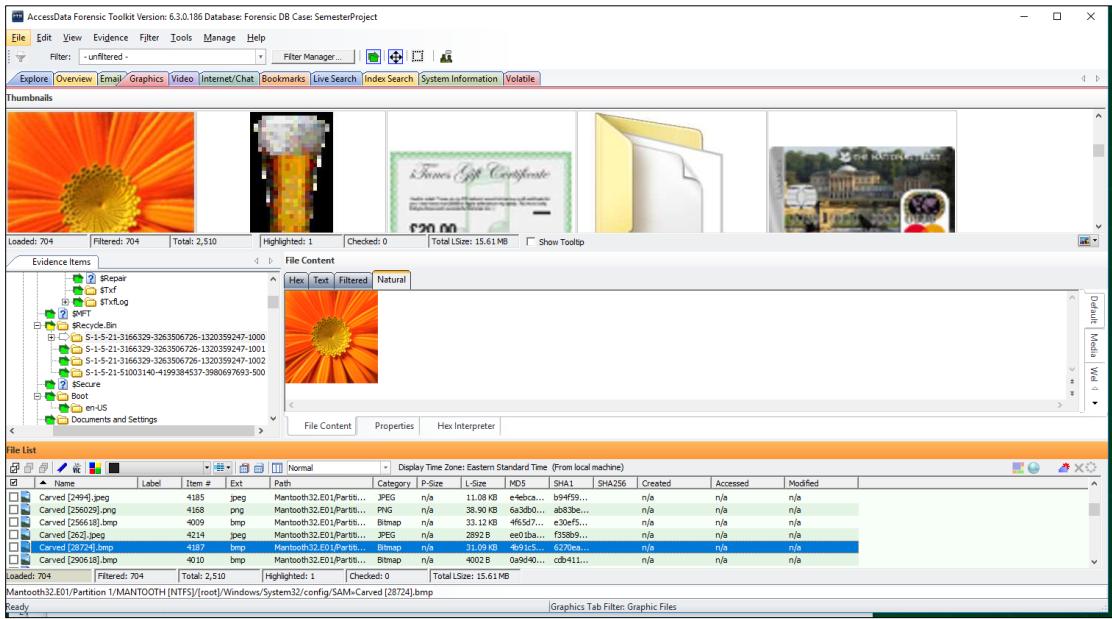
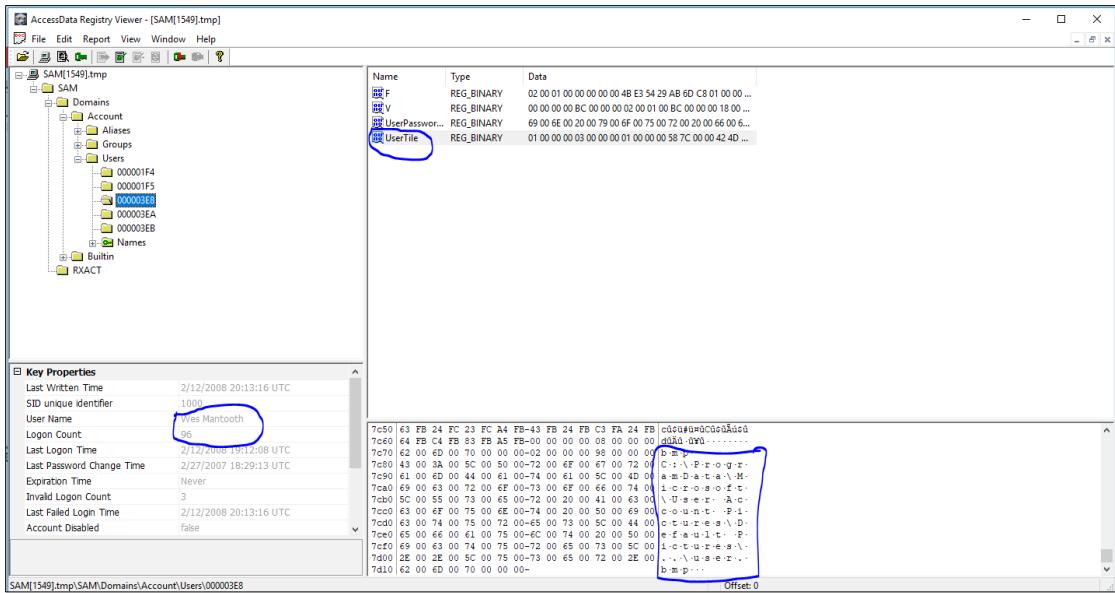
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

File Content Hex Text Filtered Natural

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified		
Carved [111].jpeg		4240	jpeg	Mantooth32.E01\Partit...	JPEG	n/a	4299	992fb...	9d4d73...	n/a	n/a	n/a	n/a		
Carved [7409].html		4253	html	Mantooth32.E01\Partit...	HTML	n/a	79	8000...	792f9...	n/a	n/a	n/a	n/a		
Carved [8226].html		4252	html	Mantooth32.E01\Partit...	HTML	n/a	152	152	792f9...	n/a	n/a	n/a	n/a		
chromecast_firming_teeth...		1456	html	Mantooth32.E01\Partit...	HTML	n/a	39,50 KB	39,50 KB	7294b...	7/25/2007 7:41...	7/25/2007 7:41...	7/24/2007 4:35...	7/24/2007 4:35...		
dcl_beard.jpg		1462	jpg	Mantooth32.E01\Partit...	JPEG	n/a	38,68 KB	f05c1...	e4f94...	7/25/2007 7:41...	7/24/2007 7:41...	10/6/2006 10:5...	10/6/2006 10:5...		
DCL.jpg		3493	jpg	Mantooth32.E01\Partit...	JPEG	n/a	8889 B	8889 B	ad368...	a8f4e...	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
DCIGR.jpg		3494	jpg	Mantooth32.E01\Partit...	JPEG	n/a	8070 B	e1862...	29129...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
desktop.ini		1248	ini	Mantooth32.E01\Partit...	7-bit text	136 B	129	a5269...	2d952...	2/27/2007 1:34...	9/26/2007 3:56...	2/27/2007 1:34...	2/27/2007 1:34...		
desktop.ini		1479	ini	Mantooth32.E01\Partit...	INDEX E...	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	
DISCGR.jpg		3495	jpg	Mantooth32.E01\Partit...	JPEG	n/a	10,76 KB	c0545...	9d5...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
FILBLIST.properties		3497	propert...	Mantooth32.E01\Partit...	7-bit text	n/a	1389 B	1fe5d...	207676...	n/a	n/a	n/a	10/9/2006 9:36...	10/9/2006 9:36...	
FINGERPRINT.jpg		3498	jpg	Mantooth32.E01\Partit...	JPEG	n/a	78,81 KB	5cd2d...	5c9295...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
go.jpg		3810	jpg	Mantooth32.E01\Partit...	JPEG E...	n/a	16,80 KB	18d9...	c9831c...	n/a	n/a	n/a	10/9/2006 9:40...	10/9/2006 9:40...	
go_press.jpg		3811	jpg	Mantooth32.E01\Partit...	JPEG E...	n/a	16,40 KB	18d90...	18d909...	n/a	n/a	n/a	10/9/2006 9:35...	10/9/2006 9:35...	
go_...		3812	jpg	Mantooth32.E01\Partit...	JPEG E...	n/a	16,40 KB	18d90...	18d909...	n/a	n/a	n/a	10/9/2006 9:35...	10/9/2006 9:35...	
KCB.jpg		3499	jpg	Mantooth32.E01\Partit...	JPEG	n/a	12331 B	17565...	b594...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
KCRG.jpg		3500	jpg	Mantooth32.E01\Partit...	JPEG	n/a	7110 B	6004c...	b594de...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
MANIFEST.MF		3817	mf	Mantooth32.E01\Partit...	7-bit text	n/a	112 B	2e702...	ac1b80...	n/a	n/a	n/a	1/1/2007 9:33...	1/1/2007 9:33...	
MBR		1003		Mantooth32.E01\Untar...	Metadata	n/a	512 B	5361b...	a6819...	n/a	n/a	n/a	n/a	n/a	
MC.jpg		3801	jpg	Mantooth32.E01\Partit...	JPEG	n/a	12,93 KB	45329...	488369...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
MCGR.jpg		3802	jpg	Mantooth32.E01\Partit...	JPEG	n/a	9823 B	45323...	d88369...	n/a	n/a	n/a	10/6/2006 10:5...	10/6/2006 10:5...	
META-INF		3816		Mantooth32.E01\Partit...	Folder	n/a	0 B	0 B	00139...	00139...	n/a	n/a	n/a	1/13/2007 3:44...	1/13/2007 3:44...
old_people.json		1460	jpg	Mantooth32.E01\Partit...	JPEG	n/a	29,50 KB	29,36 KB	9a2c5...	cce5f...	7/25/2007 7:41...	7/25/2007 7:41...	7/24/2007 4:32...	7/24/2007 4:32...	
old_people.json		1461	json	Mantooth32.E01\Partit...	JSON	n/a	174 B	174 B	174 B	174 B	7/25/2007 7:41...	7/25/2007 7:41...	7/25/2007 7:41...	7/25/2007 7:41...	
optionCorrupted.jpg		3813	jpg	Mantooth32.E01\Partit...	JPEG E...	n/a	16,43 KB	46d69c...	289...	n/a	n/a	n/a	10/4/2006 8:53...	10/4/2006 8:53...	
optionCorrupted.jpg		3814	jpg	Mantooth32.E01\Partit...	JPEG E...	n/a	15,47 KB	d2846...	13e32...	n/a	n/a	n/a	10/4/2006 8:58...	10/4/2006 8:58...	
optionCorrupted.jpg		3815	jpg	Mantooth32.E01\Partit...	JPEG E...	n/a	17,57 KB	9af1c...	9af1c...	n/a	n/a	n/a	10/4/2006 8:57...	10/4/2006 8:57...	
Readme.txt		3405	txt	Mantooth32.E01\Partit...	7-bit text	n/a	354 B	627ed...	5eb9d...	n/a	n/a	n/a	1/30/2007 5:48...	1/30/2007 5:48...	
Really Old Image		1457		Mantooth32.E01\Partit...	Folder	n/a	56 B	56 B	56 B	56 B	7/25/2007 7:41...	7/25/2007 7:41...	8/4/2007 12:04...	8/4/2007 12:04...	
StringImage.jpg		1458	jpg	Mantooth32.E01\Partit...	JPEG	n/a	11,50 KB	2e702...	490ef8...	n/a	n/a	n/a	7/25/2007 7:41...	7/25/2007 7:41...	
User Old Images		1459		Mantooth32.E01\Partit...	Folder	n/a	131 B	131 B	131 B	131 B	7/25/2007 7:41...	7/25/2007 7:41...	7/25/2007 7:41...	7/25/2007 7:41...	
Thumbnail		3803	db	Mantooth32.E01\Partit...	Thumbn...	n/a	76,50 KB	3687b...	5094c...	n/a	n/a	n/a	1/13/2007 3:45...	1/13/2007 3:45...	
validateCreditCard1.d...		3818	class	Mantooth32.E01\Partit...	Java Cl...	n/a	436 B	f4f4...	ee7610...	n/a	n/a	n/a	1/1/2007 9:30...	1/1/2007 9:30...	
validateCreditCard1.d...		3819	class	Mantooth32.E0											



### 13. Identify any pictures of Wes Mantooth.

In FTK, email attachments shows this email that is identified as 'Wes.jpg'. Furthermore, after exploring graphics, I was able to view the photograph named **Wes.jpg**.

The screenshot shows the AccessData Forensic Toolkit interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, Help, and a Filter Manager. Below the menu is a toolbar with icons for Overview, Email, Graphics, Video, Internet/Chat, Bookmarks, Live Search, Index Search, System Information, and Volatile. The main window has tabs for Email, Overview, Email, Graphics, Video, Internet/Chat, Bookmarks, Live Search, Index Search, System Information, and Volatile. The Email tab is selected. On the left is a tree view of the evidence structure:

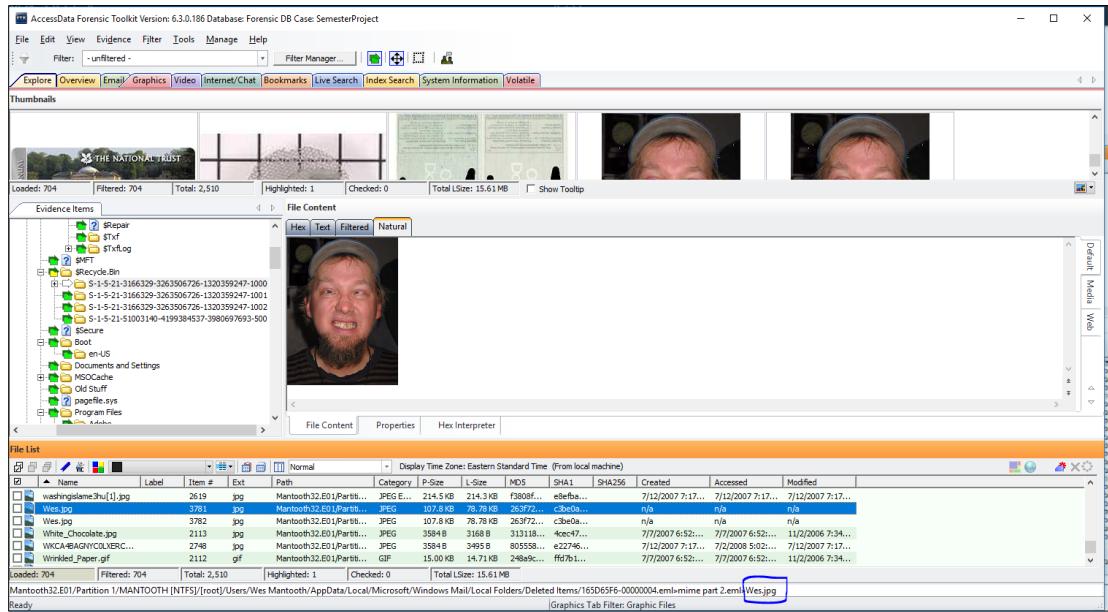
- Email Status
  - Email Attachments (135 / 135)
  - Deleted Items (From Email) (255 / 255)
  - Email Reply (12 / 12)
  - Forwarded Email (9 / 0)
- Email Archives
- Email by Date
- Email by Addresses
- Email (93 / 93)

The central pane displays a list of emails with columns for Subject, Name, To, From, CC, BCC, Submit..., Deliver..., Unread, Unsent, Has Att..., Priority, Email, Created, and Accessed. One email is selected, showing details: From: "Wes Mantooth" <dollhyde86@comcast.net>, Sent: 7/12/2007 7:36:36 PM -0400, To: toothfairy@mental dental.com, Subject: Hey Mom, Attachments: 1Wes.jpg. The email content pane shows the following text:

Hey there mom. How is it going?  
Dad said that you needed a pic of me for the weding annoucment?  
Here is a good one.  
Thanks for all your help with that. I am so busy with school, I don't know how I would have planned it!

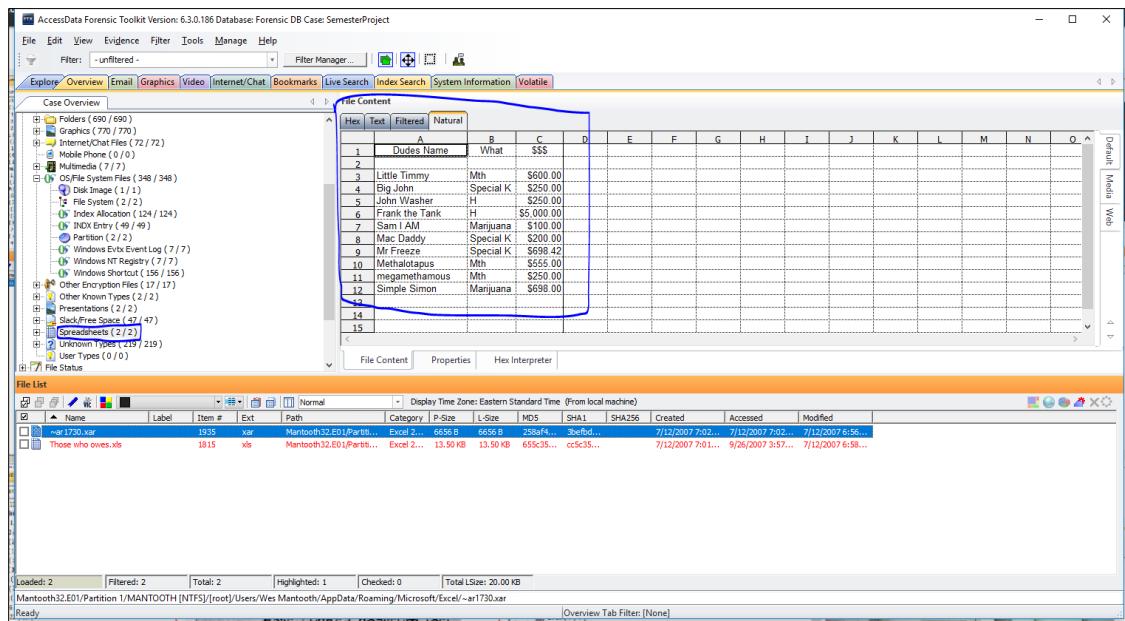
The bottom status bar shows the path: Manooth32.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Deleted Items\165D65F6-00000004.eml-mime part 2.eml Ready and the filter: Email Files and Attachments.

A screenshot of the AccessData Forensic Toolkit interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, and Help. A toolbar below has icons for Filter Manager, Find, Copy, Paste, and others. The main window shows a 'Thumbnails' view with several image files and a file tree under 'Evidence Items'. The file tree shows a folder named 'S-1-5-21-3166329-3263506726-1320359247-1000' containing various files like 'S-1-5-21-3166329-3263506726-1320359247-1000.log', 'S-1-5-21-3166329-3263506726-1320359247-1002', and 'S-1-5-21-3166329-3263506726-1320359247-1002.log'. Below the file tree is a preview window showing a smiling man's face. The bottom section displays a 'File List' table with columns for Name, Label, Item #, Ext, Path, Category, P-Size, L-Size, SHA1, SHA256, Created, Accessed, and Modified. The table lists several files, including 'Carved [237152].jpg', 'Carved [2494].jpeg', 'Carved [256029].png', 'Carved [256618].bmp', 'Carved [262].jpeg', and 'Carved [28724].bmp'. The total size of the files listed is 15.61 MB.



**14. Identify any pictures related to the fraud or financial crimes.**

In the overview tab, I was able to find pictures related to the fraud or financial crimes as shown below.



The screenshot shows the AccessData Forensic Toolkit interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, Help, and several tabs: Filter Manager..., Hex, Text, Filtered, and Natural. Below the menu is a navigation bar with links: Explore, Overview, Email, Graphics, Video, Internet/Chat, Bookmarks, Live Search, Index Search, System Information, and Volatile.

The main pane displays a tree view of file types and their counts: Folders (690 / 690), Graphics (770 / 770), Internet/Chat (72 / 72), Mobile Phone (0 / 0), Multimedia (77 / 77), OS/FS System Files (348 / 348), Other Encrypted Files (17 / 17), Other Files (17 / 17), and User Types (0 / 0). A status bar at the bottom indicates loaded: 2, filtered: 2, total: 2, highlighted: 1, checked: 0, and total LSize: 1115 KB.

A central panel titled "File Content" shows a preview of a Microsoft Word document named "ATM\_THEFTS1.docx". The preview image features a yellow key and a person using an ATM, with the title "ATM THEFTS" overlaid. To the right of the preview is a text box containing the following text:

In our first slide you see an individual who is attempting to make a bank transaction at the ATM.

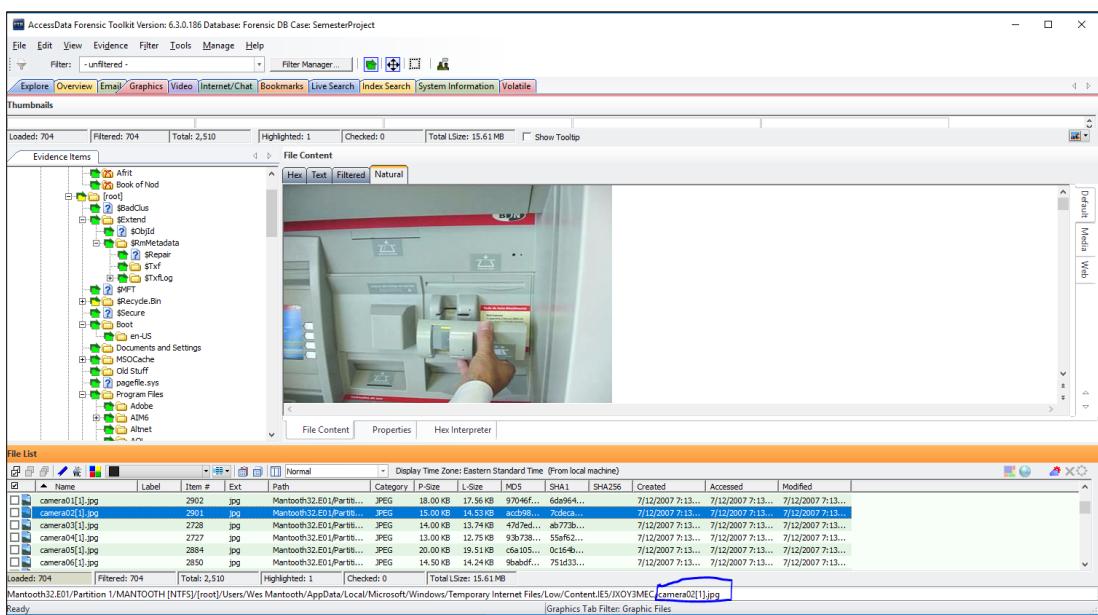
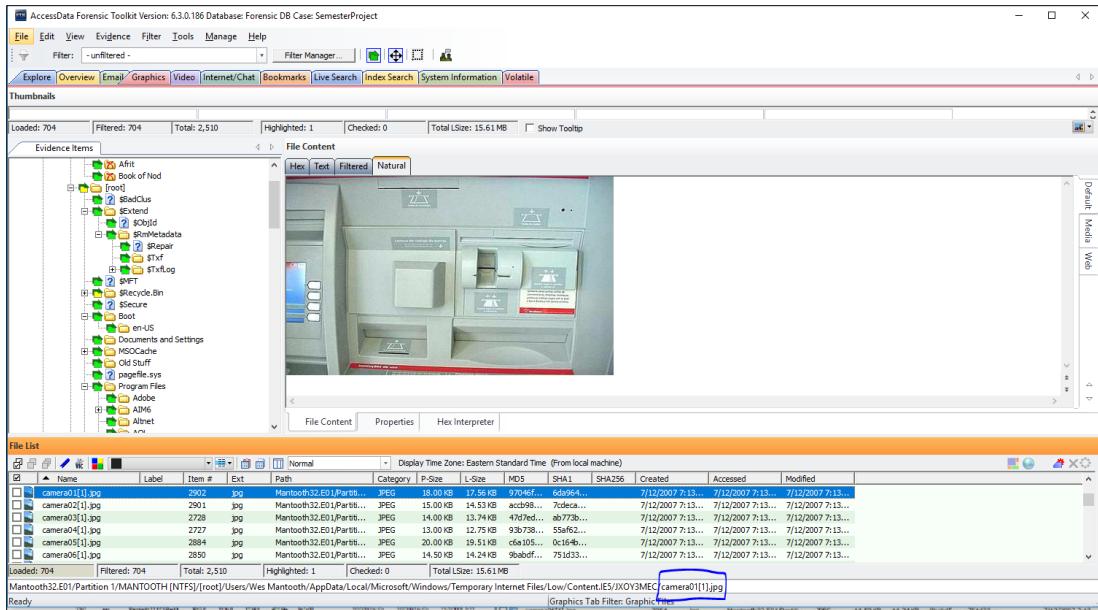
Below the preview are tabs for File Content, Properties, and Hex Interpreter.

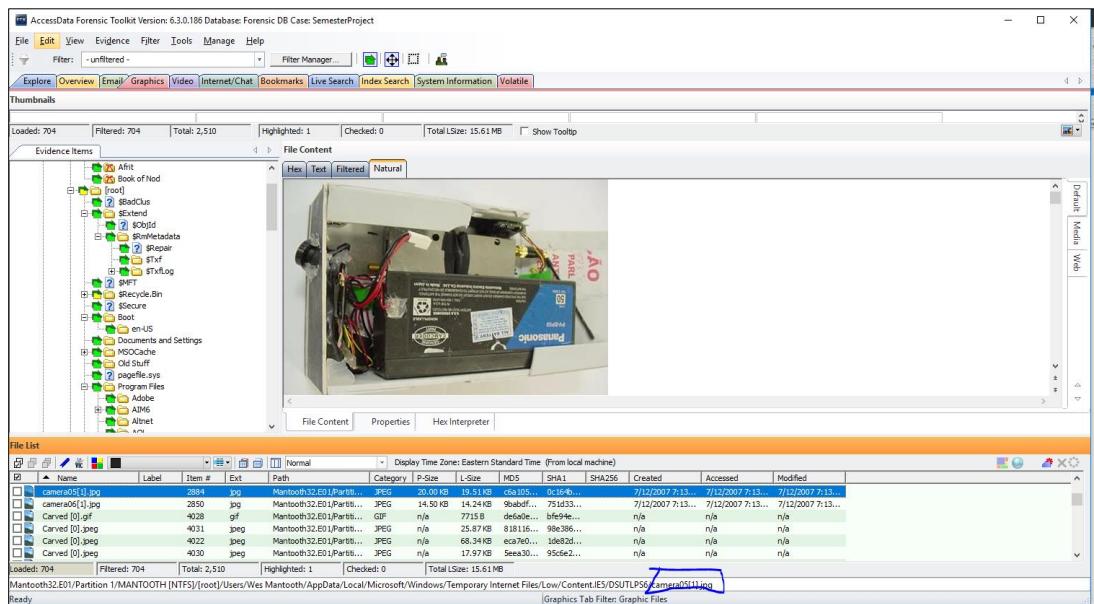
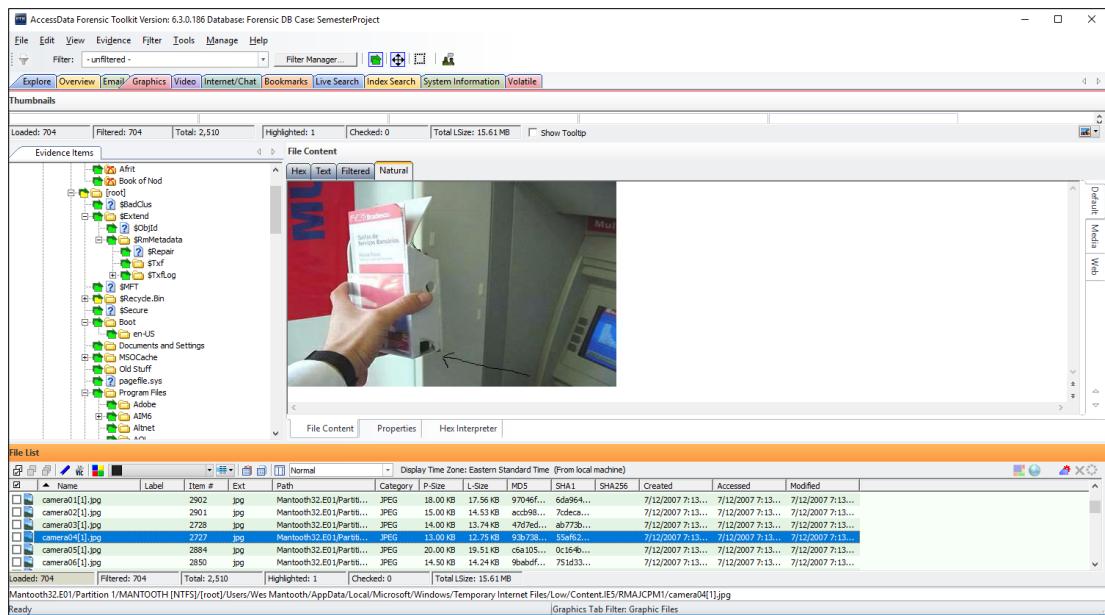
The bottom pane, titled "File List", shows a table of files found in the "ATM\_THEFTS" folder. The columns are Name, Label, Item #, Ext, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, Accessed, and Modified. The table contains two entries:

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
ATM_THEFTS1.docx		3701	docx	Manooth32.E01\Partitions\PowerP...\\Local Folders\Index\40A511AF-00000008.eml	PowerP...	762.9 KB	557.5 KB	f3e7d1...	6bdbc...	n/a	n/a	n/a	n/a
ATM_THEFTS1.pptx		1366	pptx	Manooth32.E01\Partitions\PowerP...\\Local Folders\Index\40A511AF-00000008.eml	PowerP...	762.9 KB	557.5 KB	f3e7d1...	6bdbc...	n/a	n/a	n/a	n/a

The status bar at the bottom also shows the path: Manooth32.E01\Partition 1\MANTOTH (NTFS)\root\Users\Wes Manooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Index\40A511AF-00000008.eml\ATM\_THEFTS1.ppt

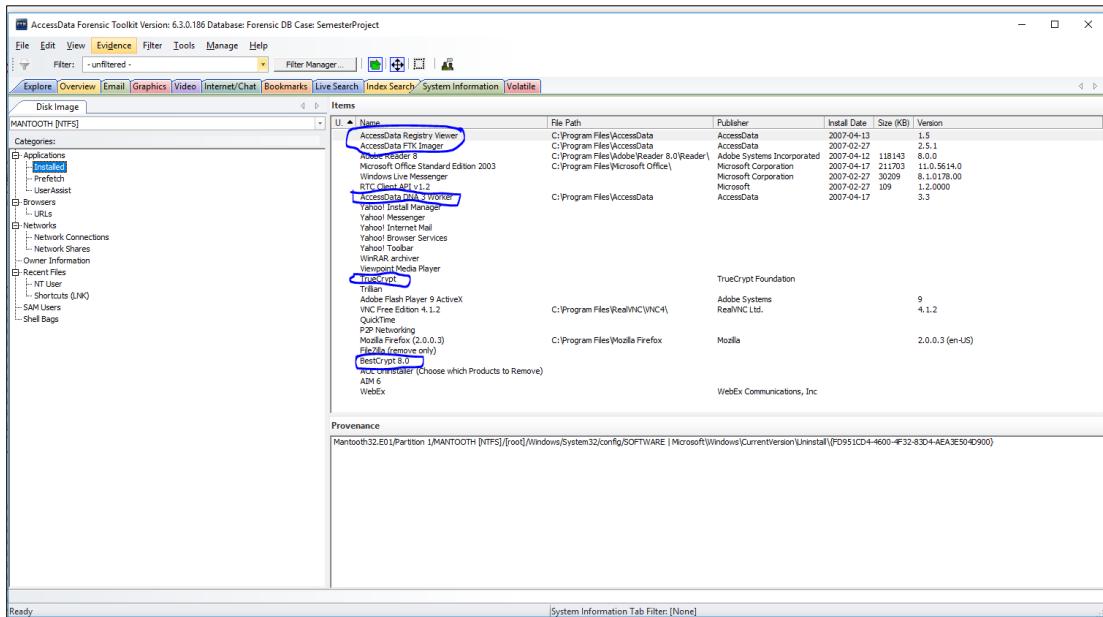
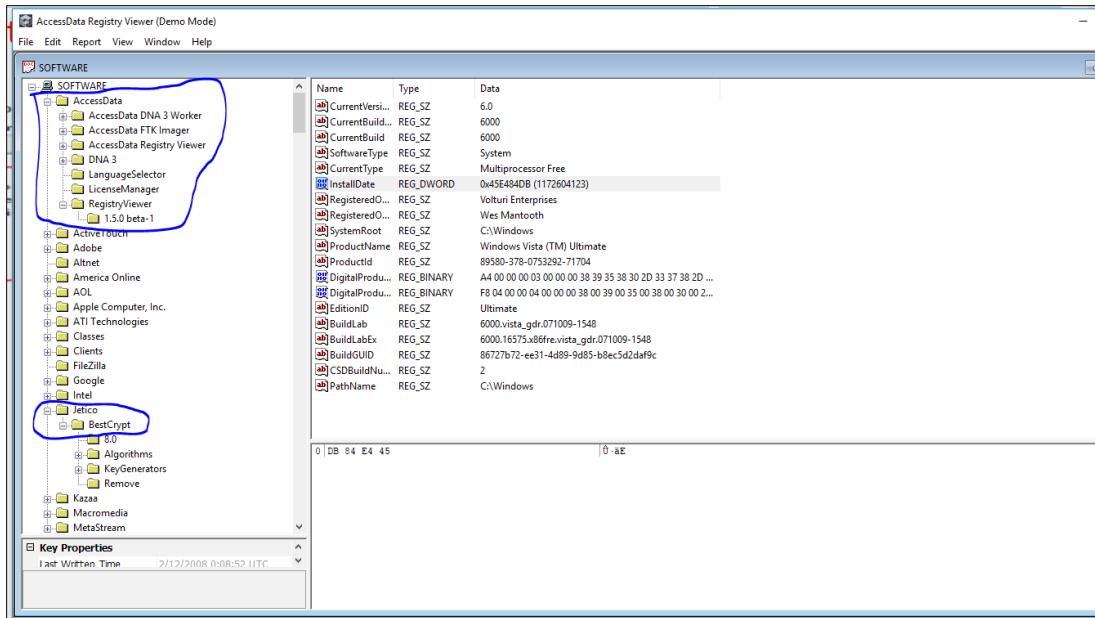
The screenshot shows the AcusData Forensic Toolkit interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, Help. The main window has tabs for Explore, Overview, Email, Graphics, Video, Internet/Chat, Bookmarks, Live Search, Index Search, System Information, and Volatile. A sidebar on the left shows a file tree with various file types like DLL, EXE, PDF, and JPEG. The central area displays a preview of a JPEG file with the text 'Invalid Card Number' and 'Fails Luhn's Checksum test' overlaid. Below the preview is a file list table with columns: Name, Label, Item #, Ext, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, Accessed, Modified. The table lists numerous files, many of which are marked as 'Carved'. The bottom status bar shows the total size of 532.6 KB and highlights the file 'Carved [140].jpeg'.





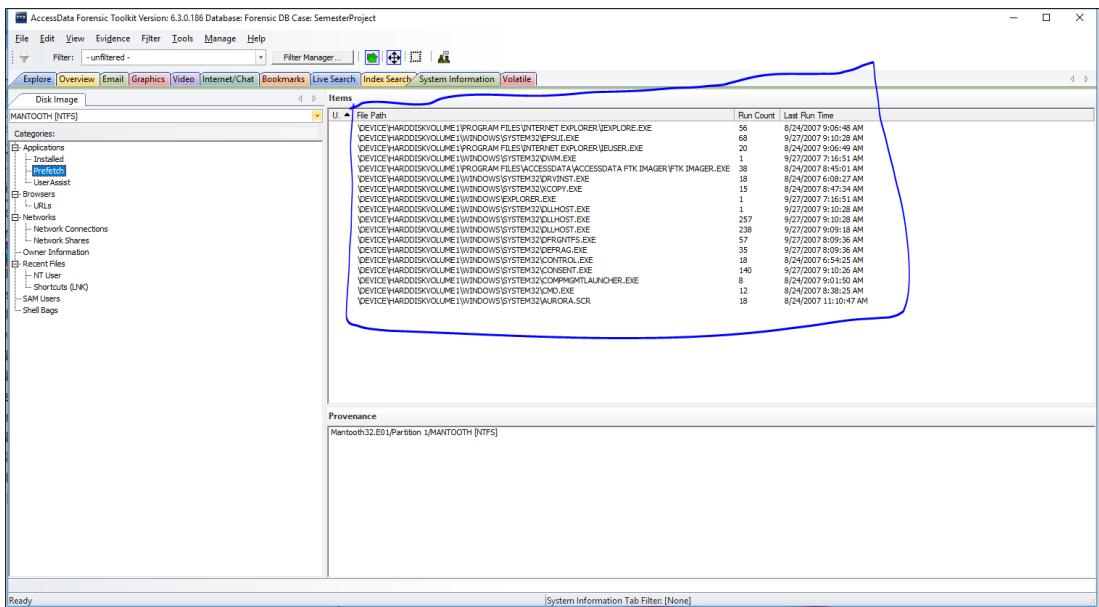
## 15. Identify any software that can be used to encrypt, obscure or forensically analyze data, or defeat forensics.

After exporting **SOFTWARE** file from FTK into registry viewer, I discovered these softwares. Additionally, in 'System Information' of FTK, I found these above highlighted softwares which were installed on the computer.



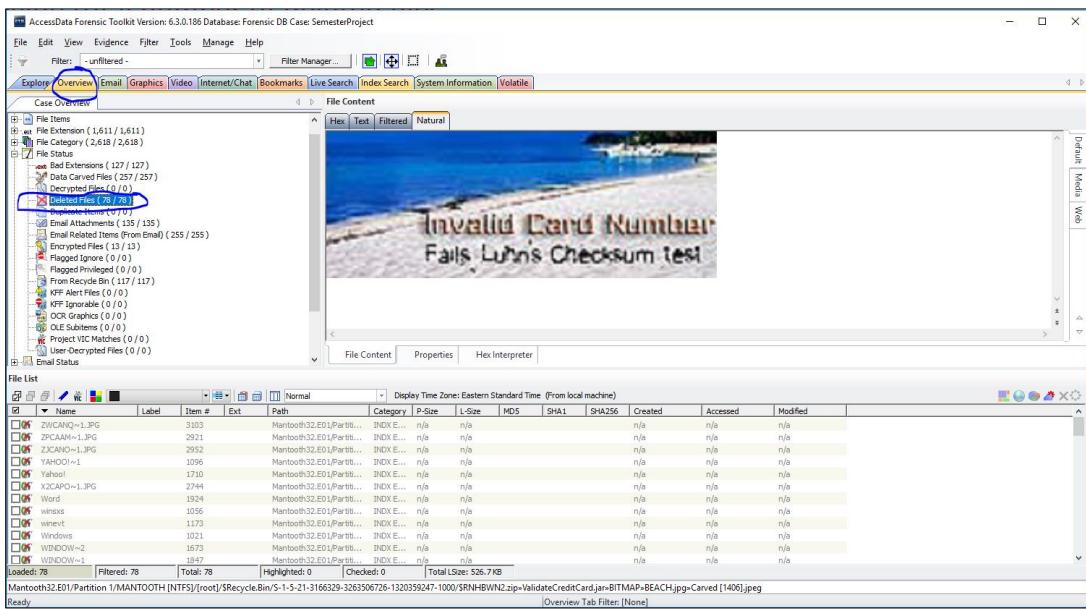
## 16. Identify the most commonly opened programs.

In FTK, under 'System Information', prefetch shows most commonly opened programs as displayed.



## 17. Provide total number of deleted files.

'Overview' tab shows 78 deleted files.



## 18. Perform file carving and find total number of carved files.

The screenshot shows the AccessData Forensic Toolkit interface. The 'Overview' tab is selected. A large list of 257 files is displayed, including:

- Carved [99856].gif
- Carved [99882].gif
- Carved [99780].gif
- Carved [99776].gif
- Carved [996].eml
- Carved [964016].gif
- Carved [964017].gif
- Carved [964018].gif
- 422.html
- Carved [93432].png
- Carved [93128].png
- Carved [93250].gif
- Carved [93250].png
- Carved [889240].jpeg

File details table:

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Carved [99856].gif		4104	.gif	Manitobah32.E01\Part0...	GIF	n/a	129 B	2ed38...	6d8b9e...	n/a	n/a	n/a	n/a
Carved [99882].gif		4103	.gif	Manitobah32.E01\Part0...	GIF	n/a	9464ec...	b7ec2b...	n/a	n/a	n/a	n/a	n/a
Carved [99780].gif		4102	.gif	Manitobah32.E01\Part0...	GIF	n/a	151 B	a1881...	d75423...	n/a	n/a	n/a	n/a
Carved [99776].gif		4101	.gif	Manitobah32.E01\Part0...	GIF	n/a	140 B	bf2879...	3426f...	n/a	n/a	n/a	n/a
Carved [996].eml		4219	.eml	Manitobah32.E01\Part0...	7 Bit text	n/a	50 B	f82e1...	092d24...	n/a	n/a	n/a	n/a
Carved [964016].gif		4100	.gif	Manitobah32.E01\Part0...	GIF	n/a	198 B	0447e...	88641...	n/a	n/a	n/a	n/a
Carved [964017].gif		4099	.gif	Manitobah32.E01\Part0...	GIF	n/a	128 B	77763...	36151...	n/a	n/a	n/a	n/a
Carved [964018].gif		4098	.gif	Manitobah32.E01\Part0...	GIF	n/a	59 B	5943...	220251...	n/a	n/a	n/a	n/a
422.html		4222	.html	Manitobah32.E01\Part0...	HTML	n/a	860 B	16511...	16511...	n/a	n/a	n/a	n/a
Carved [93432].png		4165	.png	Manitobah32.E01\Part0...	PNG	n/a	59 K	6930c...	220251...	n/a	n/a	n/a	n/a
Carved [93128].png		4098	.png	Manitobah32.E01\Part0...	PNG	n/a	285 B	656790...	269566...	n/a	n/a	n/a	n/a
Carved [93250].gif		4097	.gif	Manitobah32.E01\Part0...	GIF	n/a	42 B	b46250...	320e47...	n/a	n/a	n/a	n/a
Carved [93250].png		4096	.png	Manitobah32.E01\Part0...	PNG	n/a	374 B	7c122f...	6a8d2d...	n/a	n/a	n/a	n/a

After carving operation, I found **257** data carved files.

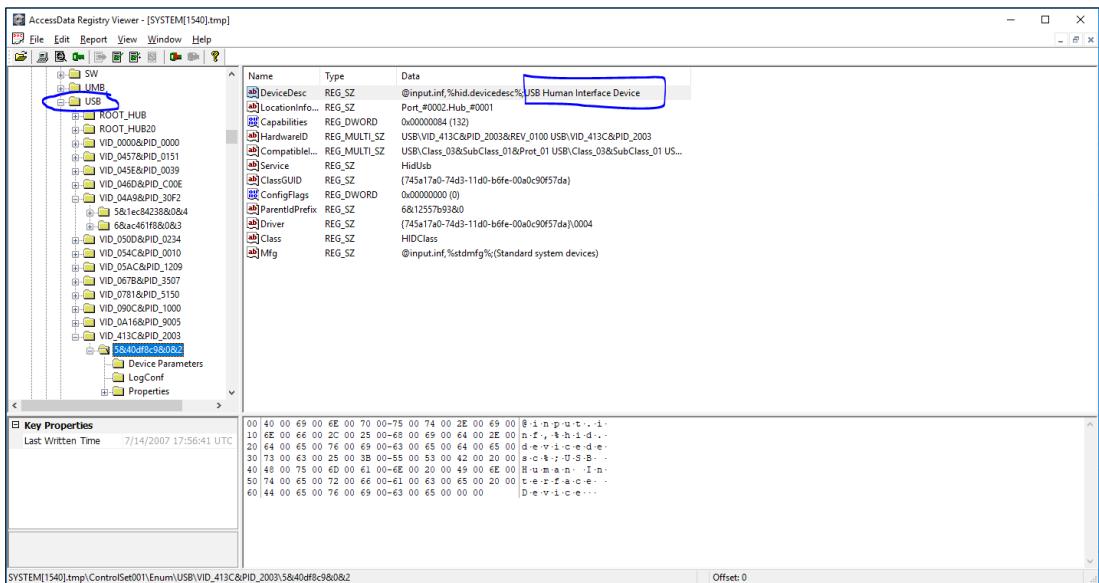
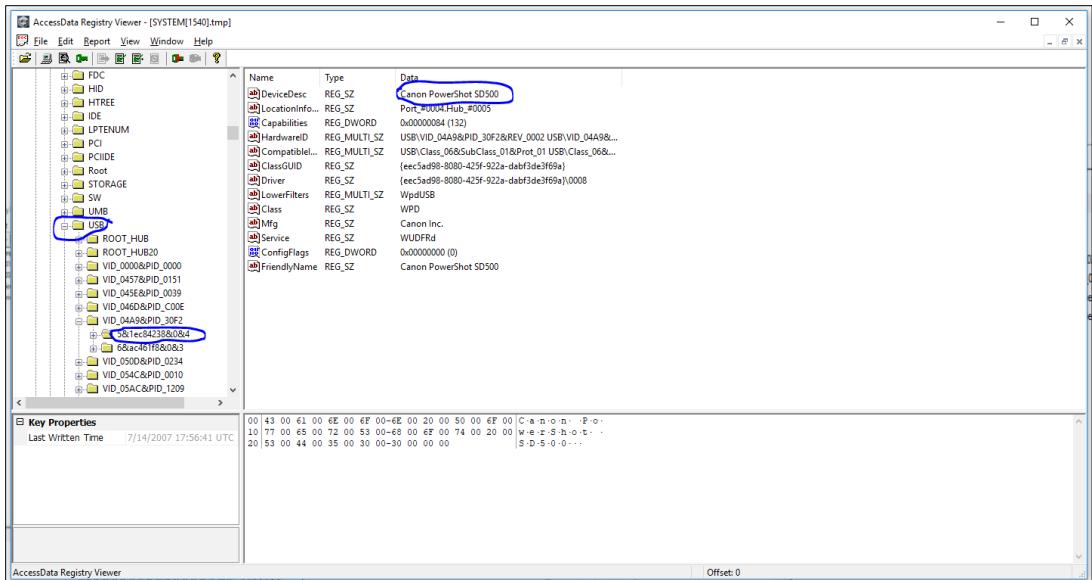
## 19. Identify any cameras, USB drives or other devices that have been attached to the computer.

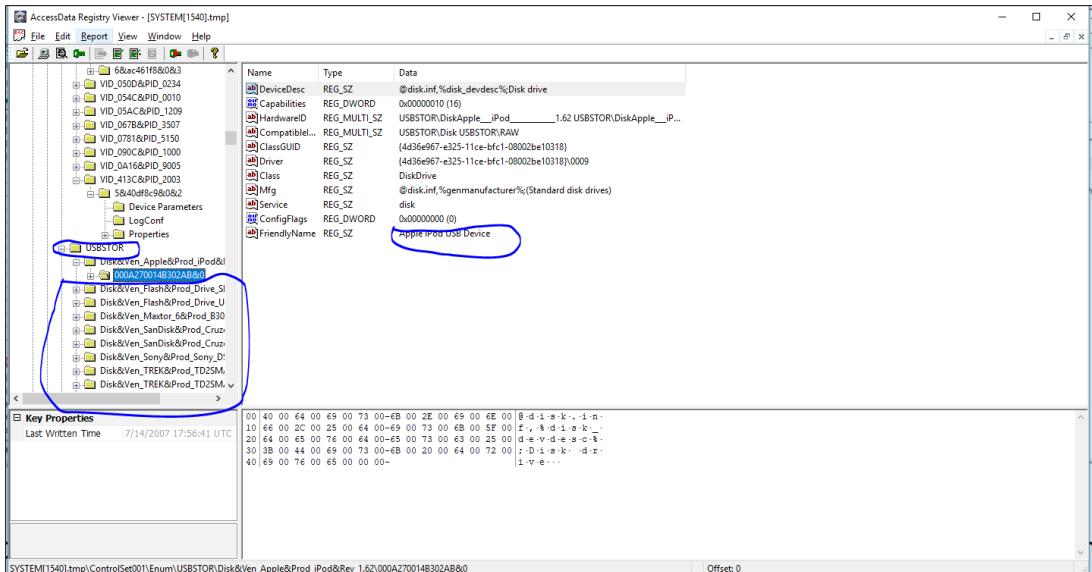
I exported SYSTEM file into registry viewer and found USB attachments under 'MountedDevices' as shown. Moreover, after exploring subfolders under 'USB' I found **USB drives, camera attachment and human interface device**.

The screenshot shows the AccessData Registry Viewer interface. The 'SYSTEM' key is expanded, showing subkeys like ControlSet001, ControlSet003, LstKnownGoodRecovery, and MountedDevices. The MountedDevices key is highlighted and expanded, showing subkeys like Select, Setup, and WPA. The 'Key Properties' table shows the last written time as 7/14/2007 17:58:46 UTC.

Name	Type	Data
(DosDevices)\C:	REG_BINARY	34 28 9A 3B 00 00 10 00 00 00 00 00
\Volume{3e0315b5-c697-11d...	REG_BINARY	34 28 9A 3B 00 00 10 00 00 00 00 00
\Volume{3e0315b8-c697-11d...	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\Volume{3e0315b9-c697-11d...	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
(DosDevices)\A:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
(DosDevices)\D:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\Volume{3c24c063-c694-11d...	REG_BINARY	7D EB 85 E4 00 7E 00 00 00 00 00 00
(DosDevices)\E:	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 33 00 54 00 ...
\Volume{996fc08-c839-11d...	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 ...
\Volume{0a0827ef-08d6-11d...	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 ...
\Volume{4397a97-cfb9-11d...	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 ...
\Volume{4397b9a-cfb9-11d...	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 ...
\Volume{ddb574d-cdb5-11...	REG_BINARY	03 F8 D8 F9 00 7E 00 00 00 00 00 00
\Volume{ddb5774-cdb5-11...	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 ...
(DosDevices)\F:	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 ...
\Volume{6e45a80c-dd60-11...	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 ...
\Volume{6e45a829-dd60-11...	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 ...
\Volume{aebc7494-e7b1-11...	REG_BINARY	54 72 75 65 43 43 72 79 74 AF
\Volume{3e4bf6f7-e955-11d...	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 ...
(DosDevices)\G:	REG_BINARY	54 72 75 65 43 43 72 79 74 AF
\Volume{3e4bf6f7-e955-11d...	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 ...
(DosDevices)\H:	REG_BINARY	#3ebfbffcc955-11db-bfe7-00...
\Volume{3e4bf70f-e955-11d...	REG_BINARY	54 72 75 65 43 43 72 79 74 AF

AccessData Registry Viewer (Demo Mode) - [SYSTEM]			
File	Edit	Report	View
ControlSet001 ControlSet003 LastKnownGoodRecovery MountedDevices Select Setup WPA			
Name	Type	Data	Offset:
DosDevices\:\	REG_BINARY	34 28 9A 3B 00 00 10 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{3e0315b5-c697-11db-80e9-806fe6fe6963}	REG_BINARY	34 28 9A 3B 00 00 10 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{3e0315b8-c697-11db-80e9-806fe6fe6963}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 05 45 00 23 00 43 00	... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{3e0315b9-c697-11db-80e9-806fe6fe6963}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 03 40 00 23 00 47 00	... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DosDevices\A:\	REG_BINARY	5C 00 3F 00 3F 00 5C 00 46 00 44 03 40 00 23 00 47 00	... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DosDevices\D:\	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 05 45 00 23 00 43 00	... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{3c24c063-c694-11db-b9eb-0011097fc487}	REG_BINARY	7D EB 85 E4 00 7E 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
DosDevices\E:\	REG_BINARY	5C 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{996f6c08-c839-11db-8794-006fe6fe6963}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{0a0827ef-d8d6-11db-8ee3-0003a0000015}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{43f97a97-cbf1-11db-a6db-806fe6fe6963}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{43f97b9a-cbf1-11db-a6db-0003a0000015}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{ddba574d-cdb5-11db-8899-0003a0000015}	REG_BINARY	03 F8 D9 F9 00 7E 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
??\Volume{ddba5774-cdb5-11db-8899-0003a0000015}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DosDevices\F:\	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{e645a80c-dd60-11db-bd31-0003a0000015}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{e645a829-dd60-11db-bd31-0003a0000015}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{eab74a4-e7b1-11db-b806-0003a0000015}	REG_BINARY	54 72 75 65 43 72 79 70 74 4F	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{e4bf6f7-e955-11db-bfe7-0003a0000015}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DosDevices\G:\	REG_BINARY	54 72 75 65 43 72 79 70 74 4F	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
??\Volume{3eabf70f-e955-11db-bfe7-0003a0000015}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	Last Written Time	7/14/2009 17:58:46 UTC	
00 5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...	7-7-7-7-U-S-B-S		
10 54 00 4F 00 52 00 23 00 44 00 69 00 73 00 68 00 7E 00 4F 00 4...	T-O-R-F-D-i-s-k		
20 26 00 58 00 65 00 6E 00 5F 00 54 00 52 00 45 00 64 00 5F 00 54 00 4...	V-E-n-n-T-R-E		
30 4B 00 22 00 50 00 72 00 66 00 64 00 5F 00 54 00 K-P-g-o-d-T	K-P-g-o-d-T		
40 44 00 32 00 53 00 4D 00 41 00 52 00 54 00 57 00 D-2-S-M-A-R-T	D-2-S-M-A-R-T		
50 47 00 33 00 4D 00 26 00 52 00 65 00 76 00 57 00 S-E-N-G-E-R-E-V	S-E-N-G-E-R-E-V		
60 32 00 2E 00 34 00 30 00 23 00 31 00 30 00 31 00 2-4-0-4-#1-0-1-			
70 32 00 30 00 35 00 31 00 36 00 37 00 32 00 31 00 2-0-5-6-7-2-1-			
80 35 00 31 00 38 00 26 00 30 00 23 00 7B 00 35 00 5-1-B-8-0-#1-[5-			
90 33 00 66 00 35 00 36 00 33 00 30 00 37 00 20 00 3-f-5-6-3-0-7- -			
a0 62 00 36 00 62 00 66 00 2D 00 31 00 31 00 64 00 b-6-9-f-1-1-d	b-6-9-f-1-1-d		
b0 30 00 28 00 39 00 34 00 66 00 32 00 2D 00 30 00 0-9-4-f-2- -0-	0-9-4-f-2- -0-		
c0 30 00 61 00 30 00 63 00 39 00 31 00 65 00 66 00 0-a-0-c-9-1-e- -f-	0-a-0-c-9-1-e- -f-		
SYSTEM\MountedDevices			Offset: 0





## 20. Identify the most recently run programs

User	File Path	Run Count	Last Run Time
Draula	UEME_RUNPATH\%SystemRoot%\System32\Windows Photo Gallery.lnk	1	4/1/2007 8:29:39 PM
Draula	UEME_RUNPATH\%SystemRoot%\System32\Media Center.lnk	17	3/5/2007 8:24:53 PM
Draula	UEME_RUNPATH\%SystemRoot%\System32\Windows Collaboration.lnk	20	3/5/2007 8:24:53 PM
Draula	UEME_RUNPATH\%SystemRoot%\System32\Windows Media Player.lnk	15	3/5/2007 8:24:58 PM
Draula	UEME_RUNPATH\%SystemRoot%\System32\Windows Media Player Center.lnk	18	3/5/2007 8:24:58 PM
Draula	UEME_RUNPATH\%SystemRoot%\System32\Windows Media Player Control.lnk	21	3/5/2007 8:24:58 PM
Draula	UEME_RUNPATH\%SystemRoot%\System32\CompMgmtLauncher.exe	1	4/1/2007 8:29:39 PM
Draula	UEME_RUNPATH\%SystemRoot%\System32\Windows DVD Maker.lnk	16	3/5/2007 8:24:58 PM
Draula	UEME_RUNPATH\%SystemRoot%\System32\Windows Extra and Upgrades\Windows Ultimate Extras.lnk	19	3/5/2007 8:24:58 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Extra and Upgrades\Windows Ultimate Extras.lnk	1	2/12/2008 2:21:39 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Install.exe	1	2/12/2008 2:20:24 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Install.exe	1	2/12/2008 12:57:49 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Accessories\NotePad.lnk	1	2/12/2008 12:57:49 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Accessories\NotePad.lnk	1	9/27/2007 3:32:28 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Accessories\NotePad.lnk	4	9/27/2007 12:14:22 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Family Pictures.lnk	2	9/27/2007 10:32:10 AM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Family Pictures.lnk	2	9/27/2007 10:32:10 AM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Messenger\YahooMessenger.exe	8	7/1/2007 6:17:20 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Messenger\YahooMessenger.exe	8	7/1/2007 6:17:20 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Microsoft Office Word 2003.lnk	1	8/5/2007 4:59:39 AM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Microsoft Office Word 2003.lnk	1	8/5/2007 4:59:39 AM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Microsoft Office Word 2003.lnk	15	8/20/2007 10:44:40 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Microsoft Office Word 2003.lnk	2	6/18/2007 8:15:56 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows explorer.exe	2	2/12/2008 2:25:50 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows explorer.exe	1	2/12/2008 2:20:38 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Media Player\lmplayer.exe	2	2/12/2008 2:20:38 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Media Player\lmplayer.exe	1	2/12/2008 2:20:38 PM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Media Player\lmplayer.exe	1	2/12/2008 11:52:30 AM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Media Player\Wordpad.lnk	2	9/2/2007 8:21:02 AM
Wes Mantooth	UEME_RUNPATH\%SystemRoot%\System32\Windows Media Player\Wordpad.lnk	1	9/27/2007 12:31:17 PM

'UserAssist' in FTK explains which programs were recently run.

## 21. Identify any URLs that were visited by manually typing the address.

'Internet/Chat' files in FTK reveals URLs that were manually typed.

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager... |

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Internet/Chat

Internet/Chat Files (72 / 72)

- AOL (9 / 9)
- Internet Explorer Browser (59 / 59)
- Mozilla Files (4 / 4)
  - Firefox History (1 / 1)
  - Mozilla Cookie Index (1 / 1)
  - Mozilla Form History (1 / 1)
  - Mozilla History (2 / 2)

File List

Name	Item #	Last Visit Time	URL	URL Title
history.dat	2310			

File Content

Hex Text Filtered Natural

byreorder LE

URL http://en-us.www.mozilla.com/en-US/firefox/2.0.0.3/firstrun/

LastVisitDate 4/10/2007 1:55:43 PM -0400

FirstVisitDate 4/10/2007 1:55:43 PM -0400

Hostname en-us.www.mozilla.com

Name Welcome to Firefox

URL http://en-us.start2.mozilla.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official

LastVisitDate 4/10/2007 4:19:45 PM -0400

FirstVisitDate 4/10/2007 1:55:43 PM -0400

Hostname en-us.start2.mozilla.com

Hidden 1

VisitCount 3

URL http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official

LastVisitDate 4/10/2007 4:19:45 PM -0400

FirstVisitDate 4/10/2007 1:55:43 PM -0400

Hostname google.com

Name Mozilla Firefox Start Page

VisitCount 3

URL http://www.google.com/

LastVisitDate 4/10/2007 4:20:19 PM -0400

FirstVisitDate 4/10/2007 3:45:24 PM -0400

Hostname google.com

Typed 1

VisitCount 4

File Content Properties Hex Interpreter

Default Media Web

Ready

Internet/Chat Tab Filter: [None]

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager... |

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Internet/Chat

Internet/Chat Files (72 / 72)

- AOL (9 / 9)
- Internet Explorer Browser (59 / 59)
- Mozilla Files (4 / 4)
  - Firefox History (1 / 1)
  - Mozilla Cookie Index (1 / 1)
  - Mozilla Form History (1 / 1)
  - Mozilla History (1 / 1)

File List

Name	Item #	Last Visit Time	URL	URL Title
history.dat	2310			

File Content

Hex Text Filtered Natural

URL http://en.wikipedia.org/wiki/Human\_body\_disposal#Secret\_disposal

LastVisitDate 4/10/2007 4:21:40 PM -0400

FirstVisitDate 4/10/2007 4:21:40 PM -0400

Hostname en.wikipedia.org

URL http://www.mamma.com/

LastVisitDate 4/10/2007 4:21:56 PM -0400

FirstVisitDate 4/10/2007 4:21:56 PM -0400

Hostname mamma.com

Typed 1

VisitCount 2

Name Mamma Metasearch - The Mother of All Search Engines

URL http://www.mamma.com/Mamma?utfout=1&qtype=0&query=stealing+checks&Submit=%C2%A0%C2%A0Search%C2%A0%C2%A0

LastVisitDate 4/10/2007 4:22:17 PM -0400

FirstVisitDate 4/10/2007 4:22:17 PM -0400

Referer http://www.mamma.com/

Hostname mamma.com

Name stealing checks - Mamma Metasearch

URL http://www.mamma.com/Mamma?utfout=1&qtype=0&query=making+meth&Submit=%C2%A0%C2%A0Search%C2%A0%C2%A0

LastVisitDate 4/10/2007 4:22:30 PM -0400

FirstVisitDate 4/10/2007 4:22:30 PM -0400

Referer http://www.mamma.com/

File Content Properties Hex Interpreter

Default Media Web

Ready

Internet/Chat Tab Filter: [None]

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: unfiltered Filter Manager

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Internet/Chat

Internet/Chat Files (72 / 72)

- AOL (9 / 9)
- Internet Explorer Browser ( 59 / 59 )
- Mozilla (4 / 4)
  - Firefox Browser ( 1 / 1 )
  - Mozilla Cookie Index ( 1 / 1 )
  - Mozilla Form History ( 1 / 1 )
  - Mozilla History ( 1 / 1 )

File List

Name	Item #	Last Visit Time	URL	URL Title
history.dat	2310			

File Content

Hex Text Filtered Natural

FirstVisitDate 4/10/2007 4:22:42 PM -0400  
 Referrer http://www.mamma.com/Mamma/utfout=1&qttype=0&query=making+meth&Submit=>  
 Hostname tmsyn.wc.ask.com  
 Hidden 1  
 URL http://www.totse.com/en/drugs/speedy\_drugs/165183.html  
 LastVisitDate 4/10/2007 4:22:42 PM -0400  
 FirstVisitDate 4/10/2007 4:22:42 PM -0400  
 Referrer http://www.mamma.com/Mamma/  
 utfout=1&qttype=0&query=making+meth&Submit=%C2%A0%C2%A0Search%C2%A0  
 Hostname totse.com  
 Name totse.com | Crystal Meth Ingredients  
 URL http://www.gmail.com/  
 LastVisitDate 4/10/2007 4:38:09 PM -0400  
 FirstVisitDate 4/10/2007 4:38:09 PM -0400  
 Hostname gmail.com  
 Typed 1  
 VisitCount 2  
 URL http://mail.google.com/mail/  
 LastVisitDate 4/10/2007 4:47:35 PM -0400  
 FirstVisitDate 4/10/2007 4:38:09 PM -0400  
 Hostname mail.google.com  
 Hidden 1  
 VisitCount 2  
 Referrer http://mail.google.com/support/bin/answer.py?  
 answer=1176&query=ifhook+express&topic=%E4%BA%8B%E4%BB%BB&tname=f&cty=search

File Content Properties Hex Interpreter

Ready

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: unfiltered Filter Manager

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Internet/Chat

Internet/Chat Files (72 / 72)

- AOL (9 / 9)
- Internet Explorer Browser ( 59 / 59 )
- Mozilla (4 / 4)
  - Firefox Browser ( 1 / 1 )
  - Mozilla Cookie Index ( 1 / 1 )
  - Mozilla Form History ( 1 / 1 )
  - Mozilla History ( 1 / 1 )

File List

Name	Item #	Last Visit Time	URL	URL Title
history.dat	2310			

File Content

Hex Text Filtered Natural

URL http://www.pgp.com/downloads/desktoptrialthankyou.html  
 LastVisitDate 4/12/2007 6:55:39 PM -0400  
 FirstVisitDate 4/12/2007 6:55:39 PM -0400  
 Referrer http://woext.pgp.com/cgi-bin/WebObjects/Trial.woa/4/wo/VhhSTLDgxEb0kngFKQD5M/0.0.7.1  
 Hostname pgp.com  
 Name PGP Corporation - Downloads - PGP Desktop 9.0 30-Day Trial  
 URL http://www.adobe.com/  
 LastVisitDate 4/12/2007 7:01:29 PM -0400  
 FirstVisitDate 4/12/2007 7:01:29 PM -0400  
 Hostname adobe.com  
 Typed 1  
 VisitCount 2  
 Name Adobe  
 URL http://www.google.com/  
 LastVisitDate 4/12/2007 7:01:23 PM -0400  
 FirstVisitDate 4/10/2007 3:45:24 PM -0400  
 Hostname google.com  
 Typed 1  
 VisitCount 9  
 Name Google  
 URL http://www.adobe.com/products/acrobat/readstep2.html  
 LastVisitDate 4/12/2007 7:01:44 PM -0400  
 FirstVisitDate 4/12/2007 7:01:44 PM -0400  
 Referrer http://www.adobe.com/

File Content Properties Hex Interpreter

Ready

## 22. Identify any credit card numbers on the drive.

After performing **Live search** and **Index search** in FTK, I recovered these credit card numbers as shown.

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: [unfiltered] Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Test Pattern Hex

Add Clear Export Import

Agg Unicode Case Sensitive

Search Term: Type: Code Pages

Max Hits Per File: 200 Search Filter: [unfiltered]

File Content

Hex Text Filtered Natural

File List

#	Name	Label	File #	Ext	Path	Category	P-Date	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified	
1	News.Report.doc	3001	doc		Manorth32.E01\Partit...	Microsoft Word Document	47.50 KB	0f8647...	964111...	n/a	n/a	n/a	n/a	n/a	
2	NTUSER.DAT	1599	det		Manorth32.E01\Partit...	Windows Registry	1792 KB	90e0e...	9976d6...	2/27/2007 1:23...	2/2/2008 6:00...	2/12/2008	2/12/2008	2/12/2008	
3	pagefile.sys	1012	sys		Manorth32.E01\Partit...	Unknown	2048 KB	d6ef07...	4d6087...	7/26/2007 4:29...	2/12/2008 5:57...	7/25/2007	7/25/2007	7/25/2007	
4	SOFTWARE	1543	cmiss...		Manorth32.E01\Partit...	Windows Registry	21.75 MB	21.75 MB	adfe3a...	1/12/2008 5:22...	2/12/2008 3:46...	2/12/2008	3:46	2/12/2008	
5	SOFTWARE.LOG1	1544	log		Manorth32.E01\Partit...	Windows Registry	12.25 MB	12.25 MB	152a40...	4e1683...	1/12/2008 5:22...	2/12/2008 3:46...	2/12/2008	3:46	2/12/2008
6	SYSTEM	1540	cess...		Manorth32.E01\Partit...	Windows Registry	12.25 MB	12.25 MB	152a40...	4e1683...	1/12/2008 5:22...	7/14/2007 3:24...	7/14/2007	7:09	7/14/2007
7	split.dat	2050	dat		Manorth32.E01\Partit...	7-bit text	1.00 KB	90.96 KB	804006...	6cd038...	7/7/2007 6:57...	7/7/2007 6:57...	4/18/2007	4:57	4/18/2007

Loaded: 7 Filtered: 7 Total: 7 Highlighted: 1 Checked: 0 Total Size: 38.14MB

Manorth32.E01\Partition 1\MANTOOTH\NTFS\root\pagefile.sys

Live Search Test Clean Home

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: [unfiltered] Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Test Pattern Hex

Add Clear Export Import

Agg Unicode Case Sensitive

Search Term: Type: Code Pages

Max Hits Per File: 200 Search Filter: [unfiltered]

File Content

Hex Text Filtered Natural

File List

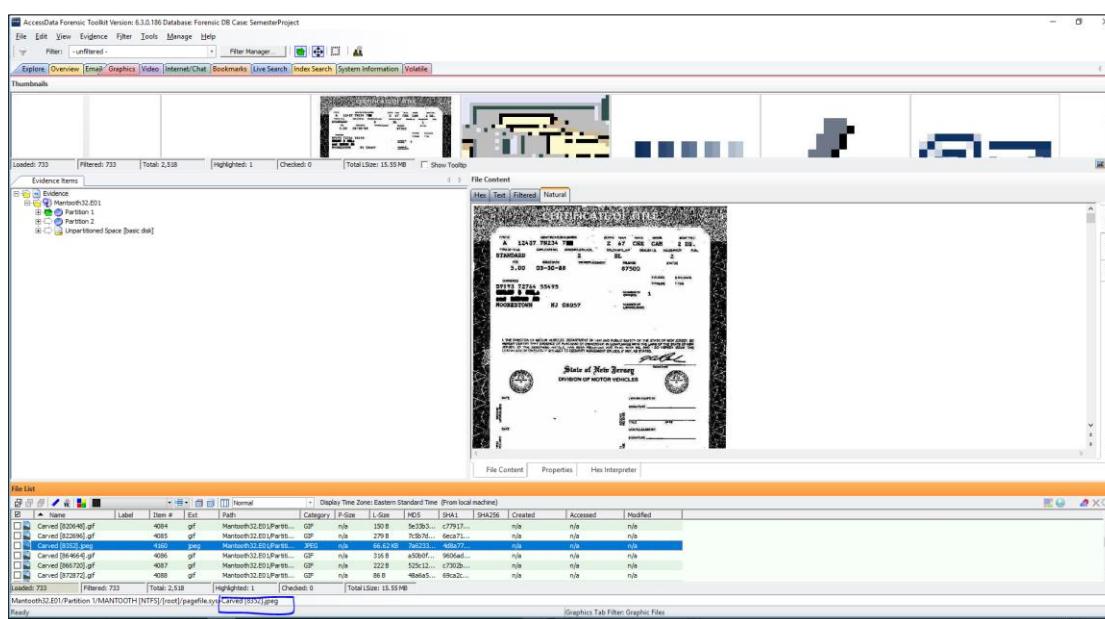
#	Name	Label	File #	Ext	Path	Category	P-Date	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified	
1	News.Report.doc	3001	doc		Manorth32.E01\Partit...	Microsoft Word Document	47.50 KB	0f8647...	964111...	n/a	n/a	n/a	n/a	n/a	
2	NTUSER.DAT	1599	det		Manorth32.E01\Partit...	Windows Registry	1792 KB	90e0e...	9976d6...	2/27/2007 1:23...	2/2/2008 6:00...	2/12/2008	2/12/2008	2/12/2008	
3	pagefile.sys	1012	sys		Manorth32.E01\Partit...	Unknown	2048 KB	d6ef07...	4d6087...	7/26/2007 4:29...	2/12/2008 5:57...	7/25/2007	7/25/2007	7/25/2007	
4	SOFTWARE	1543	cmiss...		Manorth32.E01\Partit...	Windows Registry	21.75 MB	21.75 MB	adfe3a...	1/12/2008 5:22...	2/12/2008 3:46...	2/12/2008	3:46	2/12/2008	
5	SOFTWARE.LOG1	1544	log		Manorth32.E01\Partit...	Windows Registry	12.25 MB	12.25 MB	152a40...	4e1683...	1/12/2008 5:22...	2/12/2008 3:46...	2/12/2008	3:46	2/12/2008
6	SYSTEM	1540	cess...		Manorth32.E01\Partit...	Windows Registry	12.25 MB	12.25 MB	152a40...	4e1683...	1/12/2008 5:22...	7/14/2007 3:24...	7/14/2007	7:09	7/14/2007
7	split.dat	2050	dat		Manorth32.E01\Partit...	7-bit text	1.00 KB	90.96 KB	804006...	6cd038...	7/7/2007 6:57...	7/7/2007 6:57...	4/18/2007	4:57	4/18/2007

Loaded: 7 Filtered: 7 Total: 7 Highlighted: 1 Checked: 0 Total Size: 38.14MB

Manorth32.E01\Partition 1\MANTOOTH\NTFS\root\pagefile.sys

Live Search Test Clean Home

**23. Provide a few examples of theft, title, checks, scam, and forensics.**



The screenshot shows the AccessData Forensic Toolkit version 6.3.0.186 Database Forensic DB Case SemesterProject. The interface includes a top menu bar with File, Edit, View, Evidence, Filter, Tools, Manage, Help, and a Filter Manager button. Below the menu is a toolbar with icons for Open, Save, Print, Copy, Paste, and others. A navigation bar at the top right includes Explore, Overview, Email, Graphics, Video, Internet/Chat, Bookmarks, Live Search, Index Search, System Information, and Volatile. The main area is titled 'Thumbnails' and displays several evidence items as thumbnails: a woman's face, a skull and crossbones logo, a check from 'The Cable Company', a graph, a mechanical diagram, a laboratory scene, and a washing machine. Below the thumbnails, file details are listed: Loaded: 733, Filtered: 733, Total: 2,518, Highlighted: 1, Checked: 0, Total Size: 15.55 MB, and Show Tools. A 'File Content' tab is open, showing a detailed view of the check from 'The Cable Company' for \$10.00, dated 7/12/2007. The left sidebar shows the evidence tree with 'Evidence' expanded, showing 'Manooth32.E01' (containing 'Partition 1', 'Partition 2', and 'Unpartitioned Space [basic disk]') and 'File List' (containing 'image[1].jpg', 'image[2].jpg', 'image[3].jpg', 'image[4].jpg', 'image[5].jpg', 'image[6].jpg', and 'image[7].jpg'). The bottom status bar shows 'Selected: 733', 'Filtered: 733', 'Total: 2,518', 'Highlighted: 1', 'Checked: 0', 'Total User: 15.55 MB', and the path 'Manooth32.E01\Partition 1\MANOOT\OTH [NTFS]\prod\Users\Vihs\Manooth\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\3HQCZYX\image[1].jpg'. The bottom right corner indicates '(Graphics Tab Filter: Graphic Files)'.

AccessData Forensic Toolkit Version: 6.3.0.186 Database Forensic DB Case SemesterProject

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager... Filter

Explore Overview Email Graphics Video Internet/Chat Bookmarks LiveSearch Index Search System Information Volatile

Case Overview

File Content

Logos, Nigeria  
Attention: The President/CEO

Dear Sir,

Confidential Business Proposal

Having consulted with my colleagues and based on the information gathered from the Nigerian Chambers Of Commerce and Industry, I have the privilege to request your assistance to transfer the sum of \$47,500,000.00 (forty seven million, five hundred thousand US Dollars) into your accounts. The above sum resulted from an over-invoiced contract, executed, commissioned and paid for about five years (5) ago by a foreign contractor. This action was however intentional and since then the fund has been in a suspense account at The Central Bank Of Nigeria Apex Bank.

We are now ready to transfer the fund overseas and that is where you come in. It is important to inform you that as civil servants, we are forbidden to operate a foreign account, that is why we require your assistance. The total sum will be shared as follows: 70% for us, 25% for you and 5% for local and international expenses incidental to the transfer.

The transfer is risk free on both sides. I am an accountant with the Nigerian National Petroleum Corporation (NNPC). If you find this proposal acceptable, we shall require the following documents:

(a) Your banker's name, telephone, account and fax numbers.

(b) Your private telephone and fax numbers — for confidentiality and easy communication.

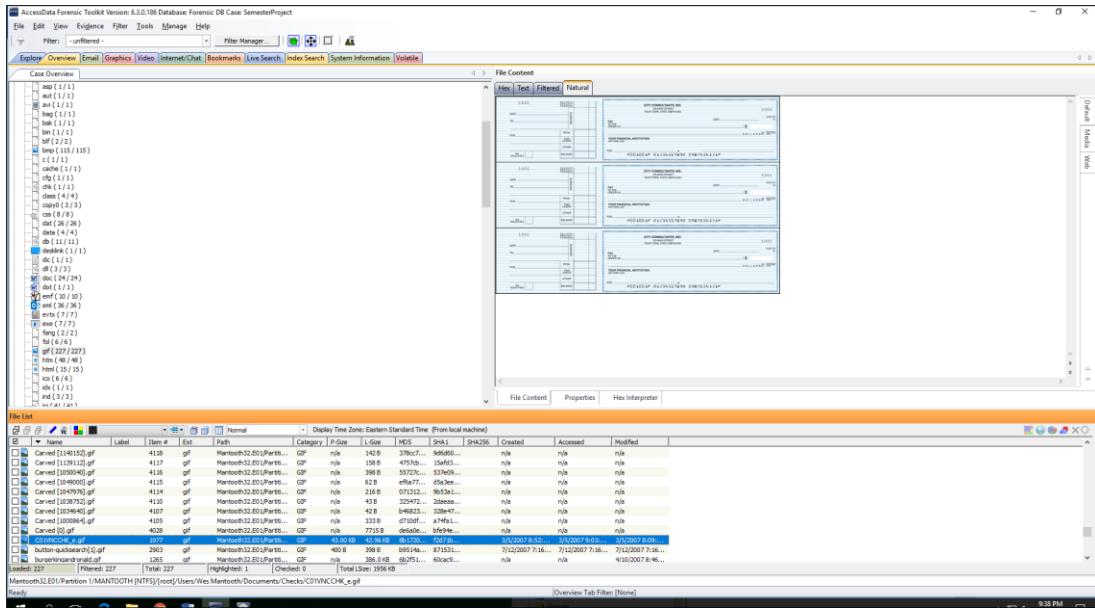
File List

#	Name	Label	Item #	Ext	Path	Category	Size	MD5	SHA1	File256	Created	Accessed	Modified
1	News Report.doc		3591	doc	M:\MFT\32.01\Perfis...	Microsoft Word Document	65,01 KB	b6967d	564113...		n/a	n/a	n/a
2	John...		1789	doc	M:\MFT\32.01\Perfis...	Microsoft Word Document	21,50 KB	23,50 KB	20800...	db725f...	3/1/2007 14:...	3/1/2007 14:...	3/1/2007 14:...
3	John...		1379	doc	M:\MFT\32.01\Perfis...	Microsoft Word Document	20,00 KB	25,00 KB	20800...	5e0465...	9/25/2007 405...	7/9/2006 14:...	4/1/2007 14:...
4	To Be Dealt With...		3451	doc	M:\MFT\32.01\Perfis...	Microsoft Word Document	9,95 KB	10,00 KB	51841...	523371...	1/2/2008 14:...	1/2/2008 14:...	1/2/2008 14:...
5	Exhume...		1367	doc	M:\MFT\32.01\Perfis...	Microsoft Word Document	46,00 KB	40,00 KB	52863...	ab940d...	2/1/2008 15:...	2/1/2008 7:30...	2/1/2008 7:30...
6	Dear Sweeney...		1766	doc	M:\MFT\32.01\Perfis...	Microsoft Word Document	63,50 KB	63,50 KB	59441...	b79149...	7/12/2007 15:...	7/13/2008 7:36...	7/14/2007 17:...
7	Confidential Business...		3333	doc	M:\MFT\32.01\Perfis...	Microsoft Word Document	28,13 KB	28,77 KB	30483...	n/a	n/a	n/a	n/a
8	Career [1]3665...		4177	doc	M:\MFT\32.01\Perfis...	Microsoft Word Document	19,00 KB	19,00 KB	49470...	n/a	n/a	n/a	n/a
9	Career [2]3665...		4178	doc	M:\MFT\32.01\Perfis...	Microsoft Word Document	19,00 KB	19,00 KB	49471...	n/a	n/a	n/a	n/a
10	Career [3]3665...		4179	doc	M:\MFT\32.01\Perfis...	Microsoft Word Document	72,09 KB	110KB...	594631...	n/a	n/a	n/a	n/a
11	Career [4]3665...		4028	doc	M:\MFT\32.01\Perfis...	Microsoft Word Document	38,00 KB	38,00 KB	70962...	n/a	n/a	n/a	n/a

located: 24    Filtered: 24    Total: 24    Rightclick: 1    Checked: 0    Total size: 676,3 KB

Manchot32.01\Partition 1\MANCOTH (NTFS)\root\Users\Wes\Manchot\AppData\Local\Microsoft\Outlook\Outlook.pst\Personal Folders\top of Personal Folders\index.htm - Confidential Business Letter.doc

[Open] [Save] [Edit] [Help]



Few examples of theft, title, checks, and scam are evident in multiple locations in FTK.

## Conclusion

In this project, a carefully scrutiny of the given image revealed relevant information that was requested by Detective Ketchum and the UNCC Police Department. Using tools like FTK and Registry Viewer. After obtaining and verifying the forensic images, I performed operation using FTK Imager Tool to verify the integrity. I used PRTK which is used to access password-protected files or system passwords.

I figured out following:

1. User passwords using PRTK tool,
2. scams and frauds images from FTK
3. Credit card numbers from Live search and Index search in FTK
4. Visited URLs from ‘Internet/Chat’ files in FTK
5. User account information,
6. Tools installed,
7. Browser history,
8. Deleted files from data carving,
9. Commonly run programs, etc.

Thus I examined the provided image and found out information relating in the image from multiple locations.