

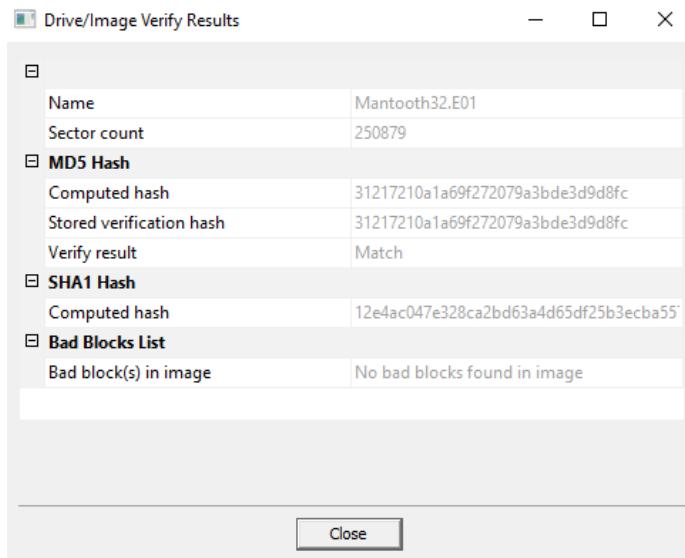
ITIS 5250
Parag Mhatre
Semester Project
Dec 4th 2018

Overview:

In this project, Detective Ketchum, has given me an image of a desktop computer, belonging to a gang member “Wes Mantooth”. The image is in EnCase E01 format. I will examine this image and try to find evidence of the accused being involved in crimes. I will use different methods like File carving, Password Recovery, searching emails, etc. to find the evidence.

Forensic Acquisition & Exam Preparation:

I accessed the shared drive from the Forensics Lab in Cone to access “Mantooth32.E01” image and transferred it to my machine. I used FTK Imager to Hash and Verify Integrity of the Image which came as a “Match”. I am using FTK, FTK Imager and PRTK for processing the file.

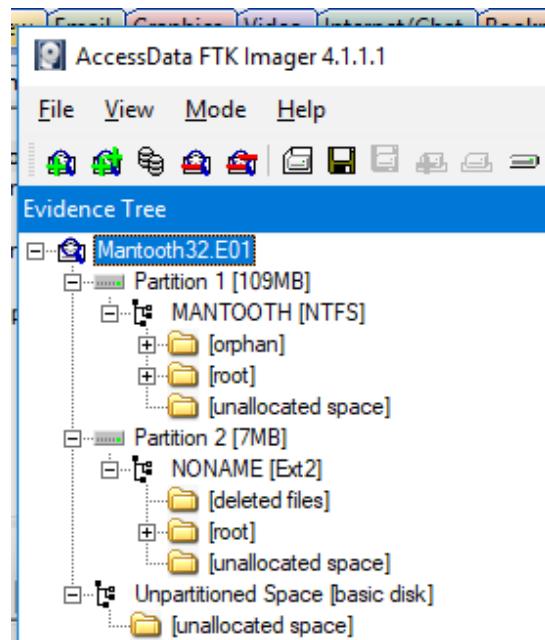


Then, I loaded up the file in FTK 6.3 with relevant Refinement options like Data and Meta Carving, Process Internet history for visualization, Performance Automatic Decryption, Document content Analysis, etc.

Findings and Report (Forensic Analysis):

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

I loaded the image on FTK Imager to see that the “Partition 1” has a total size of 109 Mb and “Partition 2” has a size of 7 Mb. Thus the total used space is $109+7 = 116\text{Mb}$ out of 128Mb.



2. Identify the type of file systems in use.

The file systems in use are as follows:

- a. Partition 1 – NTFS
- b. Partition 2 – Ext2

Evidence Tree

- Mantooth32.E01
 - Partition 1 [109MB]
 - MANTOOTH [NTFS]
 - [orphan]
 - [root]
 - [unallocated space]
 - Partition 2 [7MB]
 - NONAME [Ext2]
 - [deleted files]
 - [root]
 - [unallocated space]
 - Unpartitioned Space [basic disk]
 - [unallocated space]

File List

Name	Size	Type	Date Modified
[orphan]	0	Folder (Placeholder)	2/13/2008 12:5...
[root]	1	Directory	2/13/2008 12:5...
[unallocated space]	0	Unallocated Space	
backup boot sector	1	Filesystem Metadata	

Hex Editor

Address	Value	Content
0000000	EB 52 90 4E 54 46 53 20-20 20 20 00 02 01 00 00	�R-NTFS
0000010	00 00 00 00 00 F8 00 00-3F 00 FF 00 3F 00 00 00�-?.....
0000020	00 00 00 00 80 00 00 00-4E 6E 03 00 00 00 00 00�-Nn.....
0000030	C5 2A 01 00 00 00 00 00 27 B7 01 00 00 00 00 00	�.....

3. Identify the version and service pack of the Operating System.

The System Information tab of the FTK shows that the OS is:

Windows Vista Ultimate 6.0 where 6.0 is the current version.

U.	Name	Value
	PathName	C:\Windows
	CSDBuildNumber	2
	BuildGUID	86727b72-ee31-4d89-9d85-b8ec5d2daf9c
	BuildLabEx	6000.16575.x86fre.vista_gdr.071009-1548
	BuildLab	6000.vista_gdr.071009-1548
	EditionID	Ultimate
	DigitalProductId4	F804000004000000380039003500380030002D00
	DigitalProductId	A40000000300000038393538302D3337382D303
	ProductId	89580-378-0753292-71704
	ProductName	Windows Vista (TM) Ultimate
	SystemRoot	C:\Windows
	RegisteredOwner	Wes Mantooth
	RegisteredOrganization	Volturi Enterprises
	InstallDate	1172604123
	CurrentType	Multiprocessor Free
	SoftwareType	System
	CurrentBuild	6000
	CurrentBuildNumber	6000
	CurrentVersion	6.0

4. Find the date the OS was installed.

I opened the Software file in the Registry viewer, and found out the “InstallDate” value as “1172604123”.

Name	Type	Data
CurrentVersion	REG_SZ	6.0
CurrentBuildNumber	REG_SZ	6000
CurrentBuild	REG_SZ	6000
SoftwareType	REG_SZ	System
CurrentType	REG_SZ	Multiprocessor Free
InstallDate	REG_DWORD	0x45E484DB (1172604123)
RegisteredOrganization	REG_SZ	Volturi Enterprises
RegisteredOwner	REG_SZ	Wes Mantooth
SystemRoot	REG_SZ	C:\Windows
ProductName	REG_SZ	Windows Vista (TM) Ultimate
ProductId	REG_SZ	89580-378-0753292-71704
DigitalProductId	REG_BINARY	A4 00 00 03 00 00 38 39 35 38 30 2D
DigitalProductId4	REG_BINARY	F8 04 00 00 04 00 00 38 00 39 00 35 00
EditionID	REG_SZ	Ultimate
BuildLab	REG_SZ	6000.vista_gdr.071009-1548
BuildLabEx	REG_SZ	6000.16575.x86fre.vista_gdr.071009-1548
BuildGUID	REG_SZ	86727b72-ee31-4d89-9d85-b8ec5d2daf9c
CSDBuildNumber	REG_SZ	2
PathName	REG_SZ	C:\Windows

When I decoded the Epoch time to Human Readable time, the time was Tuesday 2/27/2007.

The screenshot shows the EpochConverter website. At the top, it displays "The current Unix epoch time is 1543687662". Below this, there's a form to convert between epoch and human date. The input field contains "1172604123" and the output field shows "Tuesday, February 27, 2007 7:22:03 PM". The "Batch convert timestamps to human dates" button is visible. Below the form, it says "GMT: Tuesday, February 27, 2007 7:22:03 PM" and "Your time zone: Tuesday, February 27, 2007 2:22:03 PM GMT-05:00". A note indicates "Relative: 12 years ago". At the bottom, there's a date/time selector and a "Human date to Timestamp" button. Above the form, there are two banners for Kefler Kia Black Friday deals.

5. Identify the Time Zone information for the computer.

I opened the System file in Registry Viewer and found under “TimeZoneInformation”, that the key name for the set timezone is “Mountain Standard Time”.

The screenshot shows the Windows Registry Editor with the title "Data Registry Viewer (Demo Mode) - [SYSTEM]". The left pane shows a tree view of registry keys under "SafeBoot", "ServiceGroupOrder", "Session Manager", "Storage", "SystemResources", "Terminal Server", and "TimezoneInformation". The "TimezoneInformation" key is selected. The right pane shows a table of properties:

Name	Type	Data
\$Bias	REG_DWORD	0x000001A4 (420)
StandardName	REG_SZ	@tzres.dll.-192
StandardBias	REG_DWORD	0x00000000 (0)
StandardStart	REG_BINARY	00 00 08 00 01 00 02 00 00 00 00 00 00 00 00 00
DaylightName	REG_SZ	@tzres.dll.-191
DaylightBias	REG_DWORD	0xFFFFFC4 (4294967236)
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Mountain Standard Time...
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
ActiveTimeBias	REG_DWORD	0x00000168 (360)

Below the table, the "Properties" section shows:

- Item Time: 3/26/2007 15:04:03 UTC
- Start Date: First Sun in Nov at 2:00:00
- Start Date: Second Sun in Mar at 2:00
- Bias: 0
- Bias: -60

6. Show the owner of the computer.

In the “Owner Information” tab of “System Information”, the Registered Owner is given as “Wes Mantooth”.

MANTOOTH [NTFS]

Categories:

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

Items	Name	Value
U.	PathName	C:\Windows
	CSDBuildNumber	2
	BuildGUID	86727b72-ee31-4d89-9d85-b8ec5d2daf9c
	BuildLabEx	6000.16575.x86fre.vista_gdr.071009-1548
	BuildLab	6000.vista_gdr.071009-1548
	EditionID	Ultimate
	DigitalProductId4	F80400000400000380039003500380030002D00300030003
	DigitalProductId	A4000000030000038393538302D3337382D303735333239
	Productid	89580-378-0753292-71704
	ProductName	Windows Vista (TM) Ultimate
	SystemRoot	C:\Windows
	RegisteredOwner	Wes Mantooh
	RegisteredOrganization	Volturi Enterprises
	InstallDate	1172604123
	CurrentType	Multiprocessor Free
	SoftwareType	System
	CurrentBuild	6000
	CurrentBuildNumber	6000
	CurrentVersion	6.0

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

The list of all users is as given below as found from SAM Users category from “System Information” from FTK.

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

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

MANTOOOTH [NTFS]

Categories:

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

Items

U	SID	User Name	Current LAN Hash	Previous LAN Ha...	Current NT Hash	Previous NT Hash
S-1-5-21-3166329-3263506726-1320359247-1000	Wes Mantooth				4F892A810F871BC64DDC16B932204E9	
S-1-5-21-3166329-3263506726-1320359247-501	Guest					
S-1-5-21-3166329-3263506726-1320359247-500	Administrator				31D6CFE0016AE931B73C59D7E0C089C0	
S-1-5-21-3166329-3263506726-1320359247-1003	Laurent					
S-1-5-21-3166329-3263506726-1320359247-1002	Dracula				D90D8508030C90473114BD90EFF3FE9E	

The user with the most logon count is “Wes Mantooth” with a logon count of 96. I found this out by opening the SAM file on Registry Viewer. Others have logon counts as follows:

Administrator – 1, Guest – 0, Laurent – 0 and Dracula – 3.

The screenshot shows the AccessData Registry Viewer interface. The left pane displays a tree view of the SAM database structure under the 'SAM' key. The 'Users' node is expanded, showing several entries, with '000003E8' (Wes Mantooth) highlighted. The right pane, titled 'Key Properties', lists various account details for 'Wes Mantooth'. Key entries include:

Last Written Time	2/12/2008 20:13:16 UTC
SID unique identifier	1000
User Name	Wes Mantooth
Logon Count	96
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
Password Required	«need "SysKey" file»
Country Code	0 (System Default)
NT Hash	«need "SysKey" file»
LM Hash	«need "SysKey" file»
Old NT Hash	«need "SysKey" file»
Old LM Hash	«need "SysKey" file»

8. Identify user accounts and who uses the account.

The user accounts are – Wes Mantooth, Dracula and Laurent.

Wes Mantooth and Dracula use their accounts with a login count of 96 and 3 respectively.

Laurent had not logged into his account even once.

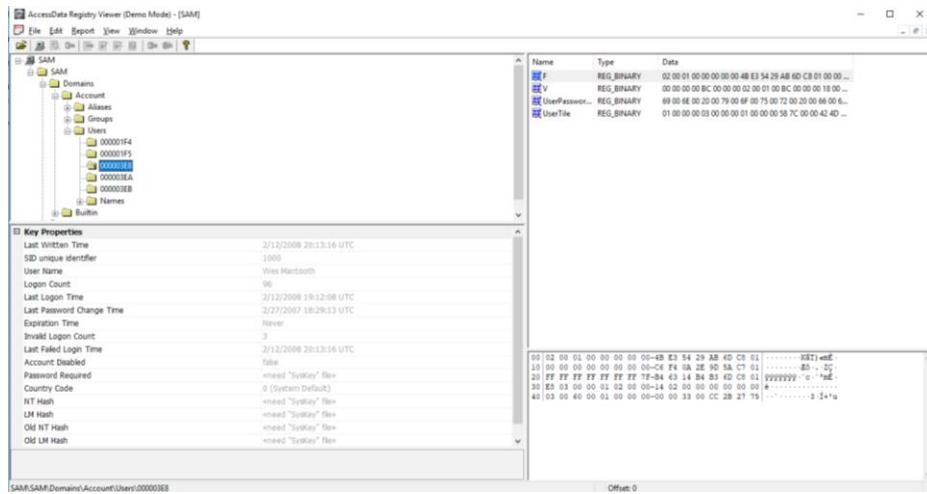
9. Acquire user passwords.

I exported the SAM and SYSTEM files from FTK and loaded them into the Password Recovery Toolkit. The cracked passwords for the users Wes_Mantooth and Dracula are “tooth” and “canine” respectively.

The screenshot shows the AccessData Password Recovery Toolkit interface. On the left, a table titled 'View All' lists four jobs, each corresponding to a Windows account: 'Administrator [NT hash]', 'Dracula [NT hash]', 'Guest [LAN hash]', and 'Laurent [LAN hash]'. All four jobs are listed as 'Finished'. The 'Result' column shows the cracked password for each account: 'canine' for Dracula, 'empty' for Guest and Laurent, and 'tooth' for Administrator. On the right, there are two detailed panes: 'Job Information' and 'File Information'. The 'Job Information' pane provides general details about the attack type (Windows account: Administrator [NT hash]), module (SAM File Module), status (Finished), difficulty (Officer), duration (0:01:13.14-30:21), and end time (12/1/08 14:30:22). It also notes that the attack was not timeouted and is decryptable. The 'File Information' pane shows the file path as 'C:\Windows\system32\config\SAM', type as 'SAM password file', version as 'Unknown', size as '212144', MD5 hash as '021d049d4f1a2370a8be2a369d7ef04', SHA-1 hash as 'baef4d04767a0005eef03d64e5e1299ed30f6c52', and creation date as 'Unknown'.

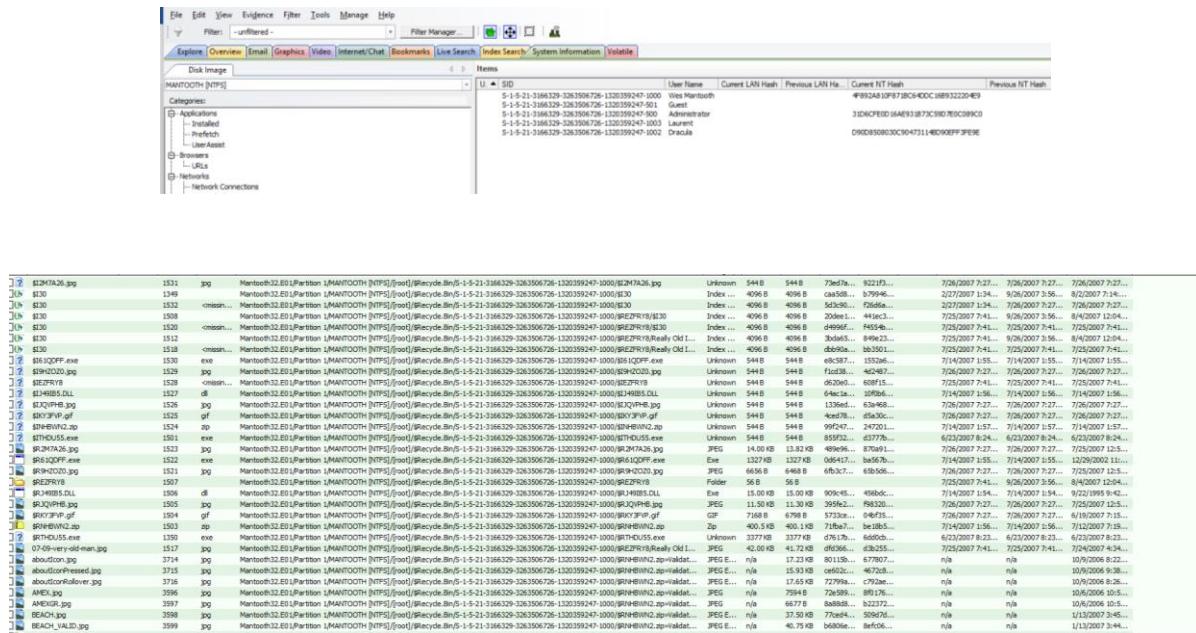
10. Identify the last date Wes Mantooth logged on.

The last login date as shown from the screenshot of the SAM file opened in Registry viewer is 2/12/2008.



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

To find the files placed in the registry by Wes Mantooth, I followed a two-step process. Opening up the SAM file, I checked the SID for Wes Mantooth is “S-1-5-21-31663293263506726-1320359247-1000”. When I checked this specific SID folder from Recycle bin, I could see all the long list of files that were deleted by that particular user as shown in the screenshots below.

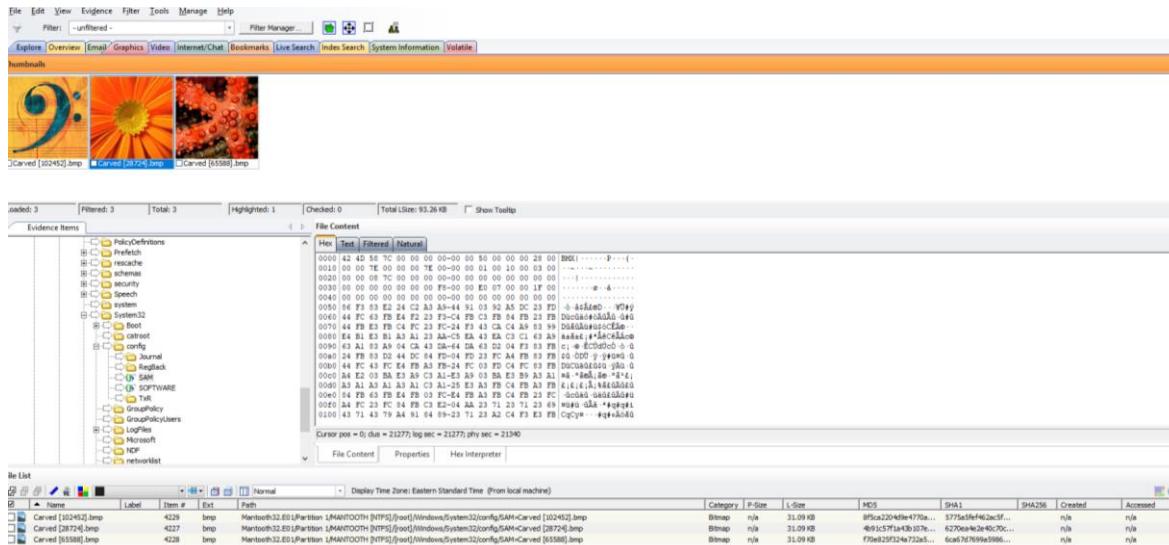
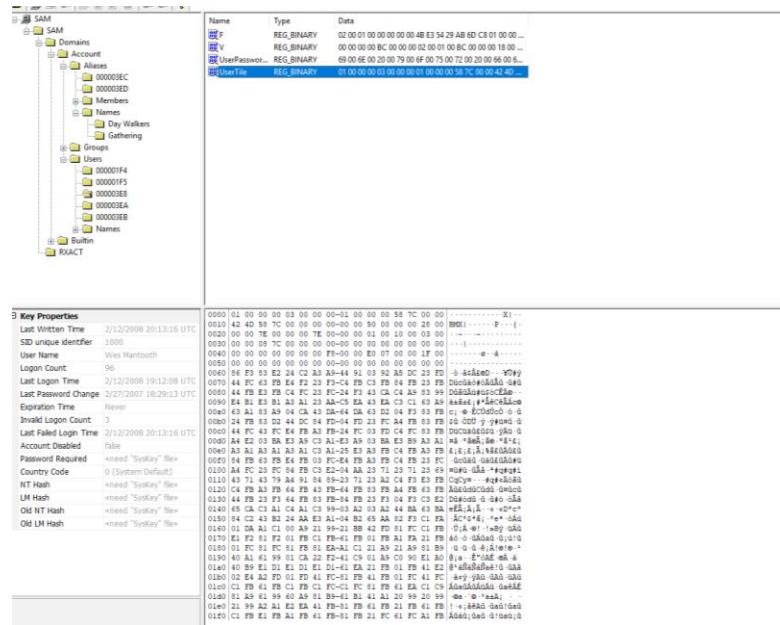


BITMAP	3995	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	Bitmap	0	0	n/a	n/a	1/13/2007 3:44...
Carved [1034924].html	4241	html	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	HTM	448	9363B...	53d2B...	n/a
Carved [1059433].bmp	4242	bmp	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	Bitmap	21022	64979...	03117...	n/a
Carved [111389].bmp	4243	bmp	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	Bitmap	479	db32E...	e1373...	n/a
Carved [111390].bmp	4244	bmp	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	Bitmap	213	1334A...	00000...	n/a
Carved [111391].bmp	4245	bmp	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	Bitmap	76	05f94...	54525...	n/a
Carved [111392].bmp	4246	bmp	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	Bitmap	1188	a11F9...	a2174...	n/a
Carved [111393].bmp	4247	bmp	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	Bitmap	628	6528A...	a0992...	n/a
Carved [1122319].htm	4248	htm	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	HTM	549	1a5E8...	6e466...	n/a
Carved [1122320].htm	4249	htm	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	HTM	549	1a5E8...	6e466...	n/a
Carved [1468].jpg	4252	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	4276	6a777...	f13E2...	n/a
Carved [1483].jpg	4292	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	40318	d169A...	21670...	n/a
Carved [1485].jpg	4295	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	4298	952B9...	98473...	n/a
Carved [1512].jpg	4298	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	199	045Bc...	26472...	n/a
Carved [1513].jpg	4299	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	4524	045Bc...	26472...	n/a
Carved [1515].jpg	4279	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1573	f330E...	7911F...	n/a
Carved [1516].jpg	4276	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1784	7c153...	ab46B...	n/a
Carved [1517].jpg	4275	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1525	f330E...	7911F...	n/a
Carved [1518].jpg	4280	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	3894	052D9...	052D9...	n/a
Carved [1519].jpg	4286	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1712	0914d...	0914d...	n/a
Carved [1520].jpg	4284	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1398	045F0...	26472...	n/a
Carved [1521].jpg	4289	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1881	64514...	04486...	n/a
Carved [1522].jpg	4285	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1723	78941...	46286...	n/a
Carved [1523].jpg	4284	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1493	045F0...	26472...	n/a
Carved [1524].jpg	4296	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1902	b6d3B...	54645...	n/a
Carved [1525].jpg	4281	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1713	0914d...	7989d...	n/a
Carved [1526].jpg	4277	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1723	78941...	46286...	n/a
Carved [1527].jpg	4287	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1746	1133E...	00000...	n/a
Carved [1528].jpg	4288	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	3923	045Bc...	54645...	n/a
Carved [1529].jpg	4300	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1818	045F0...	26472...	n/a
Carved [1636].jpg	4289	jpg	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	JPEG	1884	74459...	05133...	n/a
Carved [46464].htm	4239	htm	Harmless-32.03 [Partition] MANTICORE [INFS] (local)\Manticore\B-0-1-21-16329-28330679-[...]-12039247-1000[B4]_C0PPI_Car-Validated	HTM	118	b24E...	iae520...	n/a

Name	Label	Item #	Ext	Path	Category	P-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
DISC.jpg		3702	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	14.42 KB	91389...	a13b...	n/a	10/6/2006 10:3...
DISCR.jpg		3703	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	10.36 KB	41098...	e8d1...	n/a	10/6/2006 10:3...
FULLEST_properies		3704	propert...	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	717 byte	1389...	1fa7f...	n/a	10/6/2006 10:3...
FINERSPRT2.jpg		3705	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	78.13 KB	82518...	5c929...	n/a	10/6/2006 10:3...
go_1000.jpg		3712	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	15.46 KB	60096...	1a1e...	n/a	10/6/2006 10:3...
go_1001.jpg		3719	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	17.65 KB	61262...	e9d4...	n/a	10/6/2006 9:3...
KJB.jpg		3706	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	9.333 KB	875e...	cb585...	n/a	10/6/2006 10:3...
JKCRS.jpg		3707	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	7.108 KB	60026...	fbd1...	n/a	10/6/2006 10:3...
HANIFEST.MF		3708	MF	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	710 byte	267027...	ac880...	n/a	1/1/2007 7:41...
HCGR.jpg		3709	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	5326 KB	82518...	5c929...	n/a	10/6/2006 10:3...
HTA-2.NEF		3723	Nef	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	Folder	0 KB	n/a	n/a	n/a	1/1/2007 3:44...
old_purple_lilac.jpg		1514	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	29.50 KB	28.38 KB	98268...	cene...	7/25/2007 7:41...
old_purple_pics.jpg		1515	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	174.03 KB	173.15 KB	3c3ca...	act5c...	7/25/2007 7:41...
optioncontrolswipe.jpg		3720	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	15.46 KB	60096...	1a1e...	n/a	10/6/2006 9:3...
optioncontrolswipe2.jpg		3721	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	15.47 KB	60096...	1a1e...	n/a	10/6/2006 9:3...
Readme.txt		3582	txt	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	17.57 KB	98f0e...	49f18...	n/a	10/20/2006 8:57...
Really Old Images		1511	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	354 KB	627eb...	5ef9d...	n/a	1/1/2007 5:45...
ScreenShot		1510	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	Folder	56 KB	n/a	n/a	n/a	7/25/2007 7:41...
ScreenShot Old Images		1513	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	20 KB	20...	400...	n/a	7/25/2007 7:41...
Thumbnail		3710	db	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	Thumbn...	512 B	512 B	n/a	n/a	1/1/2007 3:44...
validateCard1SSL...		3725	class	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	Java Cls...	456 KB	36078...	505e...	n/a	1/1/2007 3:44...
validateCard1CSC...		3726	class	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	Java Cls...	1479 KB	76de...	8b54...	n/a	1/1/2007 3:40...
validateCard1CSC...		3727	class	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	Java Cls...	1241 KB	694fc...	f330...	n/a	1/1/2007 3:40...
ValidateCard1CSC...		3883	class	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	Java Cls...	801 KB	50510...	5449...	n/a	1/1/2007 3:40...
VCC_ABOUT.jpg		3711	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	14.37 KB	1ec4...	567ff...	n/a	1/1/2007 3:40...
VISA.jpg		3712	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	968 KB	32481...	bb982...	n/a	10/6/2006 10:3...
VIISAGR.jpg		3713	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	7225 KB	37589...	98e80...	n/a	10/6/2006 10:3...
woman.jpg		3809	JPG	H:\arbeit\2010\LMAR\TOOTH\{0795}\root\	Image/Bin-0-5-21	3346329-32350678-12330924-1000\#BIN\02_Q,root=0...	PIES...	11.56 KB	113 KB	98f0e...	n/a	7/25/2007 7:41...

12. Recover the user picture tile for Wes Mantooth's account. (Or tell me where it should be and that it isn't there – no credit for finding it, but I promise it is there)

Opening up the SAM file in the registry viewer and checking out the UserTile value, gives me the hex of the user image tile that's supposed to be there. I also checked the SAM file in the graphics tab in FTK and I could see 3 carved files, and Hex value matching identified the User picture tile for Wes Mantooth's account. It is a picture of a sunflower.



13. Identify any pictures of Wes Mantooth.

While surfing through emails, I found one email from the defendant which was sent to his mother. Also, a picture file, attachment was found with the mail which is named "wes.jpg". This is as said by Wes Mantooth, his own photo for printing on wedding announcement.

The screenshot shows a digital forensic tool's interface. At the top, there are tabs for 'Explore', 'Overview', 'Email', 'Graphics', 'Video', 'Internet/Chat', 'Bookmarks', 'Live Search', 'Index Search', 'System Information', and 'Variable'. Below this is a navigation bar with icons for 'File List', 'Email Status', 'Has Att...', 'Priority', 'Email', 'Created', 'Accessed', 'Modified', 'Item #', 'Category', 'P-Size', and 'L-Size'. A status bar at the bottom indicates 'Display Time Zone: Eastern Standard Time (from local machine)'.

The main area displays a table titled 'File List' with columns corresponding to the navigation bar. The table lists various files, including several GIF images and a JPEG image named 'wes.jpg'. The table includes columns for 'Item #', 'Category', 'P-Size', 'L-Size', and 'Path'.

Below the table, there are buttons for 'Loaded: 135', 'Filtered: 135', 'Total: 135', 'Highlighted: 1', 'Checked: 0', and 'Total Size: 4501 KB'.

The 'Content' tab is selected, showing the email message details:

```
From: "Wes Mantooth" <dohertydell@comcast.net>
To: 7/12/2007 7:36:36 PM -0400
X-Mailer: tootmam@mentaldental.com
Subject: Hey Mom
Attachments: wes.jpg
```

The message body contains:

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

les

Received: from [REDACTED] (local[127.0.0.1]) by Comcast.net (esmtpc12) with ESMTP id <20070711203706m13062x57e> on Wed, 11 Jul 2007 20:37:06 +0000

File Content Properties Hex Interpreter

The 'Email Attachments' tab shows a list of attachments, including '165049F8-00000004.eml' and 'wes.jpg'.

The 'Email Conversation' tab shows a single entry: '[hey Mom]'.

The 'Main Web' tab is also visible.

A preview window shows the image 'wes.jpg', which is a photograph of a man with a beard and a baseball cap, smiling.

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

While examining the image on various tabs, I found the following pictures which were related to financial crimes.

Loaded: 770 Filtered: 770 Total: 2,618 Highlighted: 1 Checked: 0 Total LSize: 16.47 MB Show Tooltip

Evidence Items

- Evidence
- Mantooth32.E01

File Content

Hex Test Filtered Natural

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Camera.bmp		1962	bmp	Mantooth32.E01\Partition 1\MANTOOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Mail\Local Folders\Sent Items\59914090-00000002.eml-Camera.bmp	Bitmap	401.2 KB	406.2 KB	729b14d4-0b00-0000-0000-000000000000	4c1139a4-0b00-0000-0000-000000000000	n/a	n/a	n/a	

Loaded: 770 Filtered: 770 Total: 2,618 Highlighted: 1 Checked: 0 Total LSize: 16.47 MB

File Content

Hex Test Filtered Natural

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
camera0211.jpg		3946	jpg	Mantooth32.E01\Partition 1\MANTOOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\HOY3MEC\camera0211.jpg	JPG	15.00 KB	14.51 KB	4e1f40e1-7f60-4e40-8440-37fbef025a3r	37fbef025a3r	37fbef025a3r	3/17/2007 7:11:51 AM	3/17/2007 7:11:51 AM	3/17/2007 7:11:51 AM

Loaded: 770 Filtered: 770 Total: 2,618 Highlighted: 1 Checked: 0 Total LSize: 16.47 MB

File Content

Hex Test Filtered Natural

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
camera0211.jpg		3946	jpg	Mantooth32.E01\Partition 1\MANTOOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\DSUTLPS6\camera0211.jpg	JPG	15.00 KB	14.51 KB	4e1f40e1-7f60-4e40-8440-37fbef025a3r	37fbef025a3r	37fbef025a3r	3/17/2007 7:11:51 AM	3/17/2007 7:11:51 AM	3/17/2007 7:11:51 AM

Loaded: 770 Filtered: 770 Total: 2,618 Highlighted: 1 Checked: 0 Total LSize: 16.47 MB

File Content

Hex Test Filtered Natural

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
camera0211.jpg		3946	jpg	Mantooth32.E01\Partition 1\MANTOOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\DSUTLPS6\camera0211.jpg	JPG	15.00 KB	14.51 KB	4e1f40e1-7f60-4e40-8440-37fbef025a3r	37fbef025a3r	37fbef025a3r	3/17/2007 7:11:51 AM	3/17/2007 7:11:51 AM	3/17/2007 7:11:51 AM

Loaded: 770 Filtered: 770 Total: 2,618 Highlighted: 1 Checked: 0 Total LSize: 16.47 MB

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

The following softwares can be used to encrypt, obscure or forensically analyze data or defeat forensics.

AccessData Registry Viewer, AccessData FTK Imager, AccessData DNA 3 Worker, Truecrypt, BestCrypt 8.0

Name	File Path	Publisher	Install Date	Size (KB)	Version
AccessData Registry Viewer	C:\Program Files\AccessData	AccessData	2007-04-13	1.5	
AccessData FTK Imager	C:\Program Files\AccessData	AccessData	2007-02-27	2.5.1	
Adobe Reader 8	C:\Program Files\Adobe\Reader\	Adobe Systems Incorporated	2007-04-12	118143	8.0.0
Microsoft Office Standard Edition 2003	C:\Program Files\Microsoft Office\	Microsoft Corporation	2007-04-17	211703	11.0.5614.0
Windows Live Mail		Microsoft Corporation	2007-02-27	30209	8.1.0178.00
RTC Client API v1.2		Microsoft	2007-02-27	109	1.2.0000
AccessData DNA 3 Worker	C:\Program Files\AccessData	AccessData	2007-04-17	3.3	
Yahoo! Install Manager					
Yahoo! Messenger					
Yahoo! Internet Mail					
Yahoo! Browser Services					
Yahoo! Toolbar					
WinRAR archive					
VLC media player					
TrueCrypt		TrueCrypt Foundation			
Trollan					
Adobe Flash Player 9 ActiveX					
VNC Free Edition 4.1.2	C:\Program Files\RealVNC\VNC4\	Adobe Systems			
QuickTime		RealVNC Ltd.			
P2P Networking					
Mozilla Firefox (2.0.0.3)	C:\Program Files\Mozilla Firefox	Mozilla			
Firefox (remove only)					
BestCrypt 8.0					
AOL ClickToInstall (Choose which Products to Remove)					
AIM 6					
WebEx		WebEx Communications, Inc			

16. Identify the most commonly opened programs

The most commonly opened programs can be viewed in the prefetch. The FTK tool provides a direct access to the contents of the prefetch and as seen in the screen shot below, there is a list of programs in descending order of their frequency of being launched. From the list, user launchable programs, Internet Explorer is the most opened program with 56 launches.

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Sem_Parag_Day3_39991

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager | Live Search Index Search System Information Volatile

Items

User	File Path	Run C.	Last Run Time
	[DEVICE]\HARDISKVOLUME1\WINDOWS\SYSTEM32\DHHOST.EXE	257	9/27/2007 10:28 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\SYSTEM32\DHHOST.DLL	258	9/27/2007 10:28 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\SYSTEM32\CONSENT.DXE	140	9/27/2007 10:26 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\SYSTEM32\CPUSLICE.DXE	68	9/27/2007 10:28 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\SYSTEM32\DEVMGR.DXE	57	9/27/2007 10:28 AM
	[DEVICE]\HARDISKVOLUME1\PROGRAM FILES\INTERNET EXPLORER\EXPLORE.EXE	56	8/24/2007 9:06:48 AM
	[DEVICE]\HARDISKVOLUME1\PROGRAM FILES\ACCESSDATA\ITK IMAGER\ITK IMAGER.EXE	38	8/24/2007 8:45:01 AM
	[DEVICE]\HARDISKVOLUME1\PROGRAM FILES\ITK IMAGER\ITK IMAGER.DLL	35	8/24/2007 8:45:01 AM
	[DEVICE]\HARDISKVOLUME1\PROGRAM FILES\INTERNET EXPLORER\USER.EXE	20	8/24/2007 9:06:49 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\SYSTEM32\DRIVERS\DRIVERS.EVE	18	8/24/2007 9:06:27 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\SYSTEM32\DRIVERS\DRIVERS.DLL	18	8/24/2007 9:06:44 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\SYSTEM32\AURORA.SCR	18	8/24/2007 11:10:47 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\SYSTEM32\CHOCO.DXE	15	8/24/2007 9:06:48 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\SYSTEM32\COMPAGMTLAUNCHER.EXE	12	8/24/2007 9:06:25 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\SYSTEM32\COMPAGMTLAUNCHER.DLL	8	8/24/2007 9:01:50 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\SYSTEM32\DHHOST.DLL	1	9/27/2007 10:28 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\EXPLORE.EXE	1	9/27/2007 9:16:51 AM
	[DEVICE]\HARDISKVOLUME1\WINDOWS\DHHOST.DLL	1	9/27/2007 9:10:28 AM

Provenance

Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Windows\Prefetch\SLIDER.EXE-0895AB54.pdf

Ready [System Information Tab Filter: [None]] 8:44 PM 12/3/2018

17. Provide total number of deleted files.

Using the FTK's Case Overview section, in the Deleted files, 79 files were found as listed in the screenshot below.

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Sem_Parag_Day3_39991

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager | Live Search Index Search System Information Volatile

Case Overview

File Items

- File Extension (.441 / 1,611)
- File Category (2,619 / 2,619)
- File Status

 - Bad Extensions (127 / 127)
 - Data Corrupted (272 / 272)
 - Deleted Files (79 / 79)
 - Duplicate Files (0 / 0)
 - Email Attachments (198 / 198)
 - Encrypted Files (255 / 255)
 - Encrypted Files (13 / 13)
 - Flagged Ignore (0 / 0)
 - Froggied Recycle Bin (0 / 0)
 - KPF Alert Files (0 / 0)
 - KPF Ignorable (0 / 0)
 - Large Files (0 / 0)
 - OLE Subtypes (0 / 0)
 - Project VNC Matches (0 / 0)
 - User Decrypted Files (0 / 0)
 - User Encrypted Files (0 / 0)
 - User Ignored Status

File List

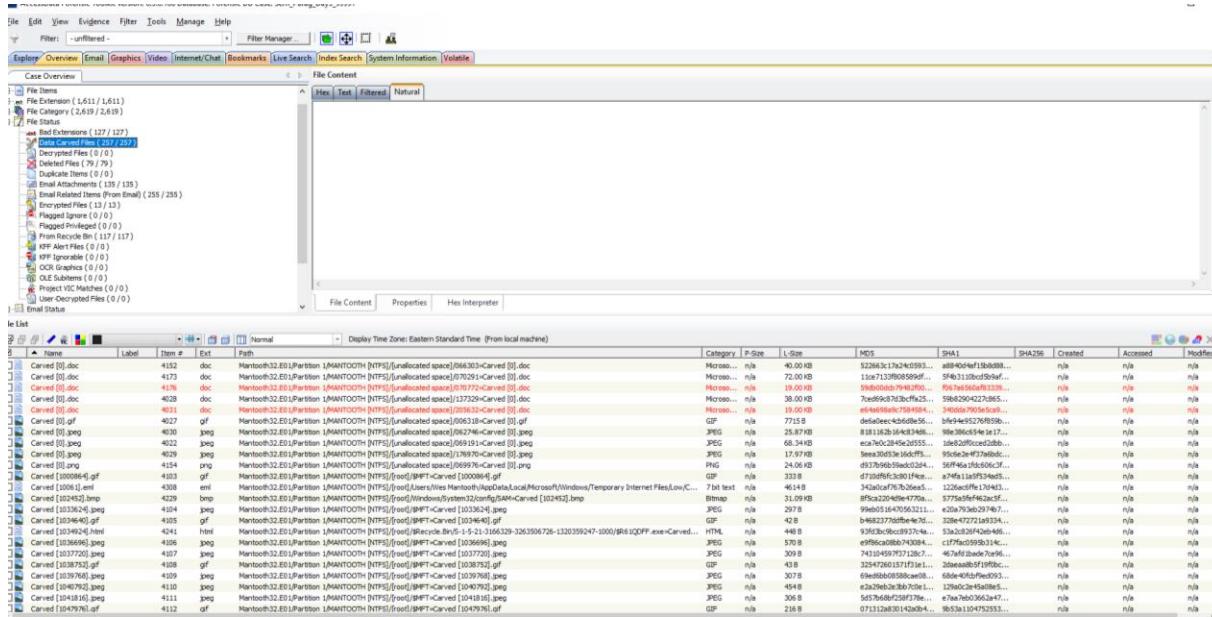
Name	Label	Item #	Ext	Path	Category	File Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified	
05		140		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Windows\Temporary Internet Files\Low\I...	INDEX E...	4096 B	4096 B	620fbfe891f77941...	108773d4e531d...	2/12/2008 7:53...	2/12/2008 7:53...	2/12/2008		
05		1965		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Users\Wes Mantooth\Desktop\secret\U230...	INDEX E...	4096 B	4096 B	620fbfe891f77941...	108773d4e531d...	2/12/2008 7:53...	2/12/2008 7:53...	2/12/2008		
05	[MetaCache]	4177		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Users\Wes Mantooth\[metaCache]	Planch...	n/a	n/a					n/a	n/a	
05	Audit	1451		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Users\Wes Mantooth\[audit]\Audit	Folder	48 B	48 B					2/12/2008 7:53...	2/12/2008 7:53...	
05	ar_test_nakui-doc	1969	doc	Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Users\Wes Mantooth\Desktop\secret\ar_test_nakui.doc	Microso...	19.00 KB	19.00 KB	e14a6f80cfc7984984...	340dd97905e5ca9...	2/12/2008 7:53...	2/12/2008 7:53...	2/12/2008		
05	ar_rec	1421	doc	Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Users\Wes Mantooth\Desktop\secret\ar_rec.doc	Microso...	38.10 KB	38.10 KB	7ed696c7d7bcfa25...	5962904227d365...	2/12/2008 7:53...	2/12/2008 7:53...	2/12/2008		
05	bill_Gates_of_Hk	2863		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Users\Wes Mantooth\[AppData\Roaming\Microsoft\Windows\Recent\Bill_Gates_of_Hk	INDEX E...	40 B	40 B					n/a	n/a	
05	Book of Nod	1420		Mantooth32.0\Partition 1\Partition [NTFS]\[organ]\Book of Nod	Folder	48 B	48 B					2/12/2008 7:53...	2/12/2008 7:53...	2/12/2008
05	com	1226		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Windows\System32\com	INDEX E...	n/a	n/a					n/a	n/a	n/a
05	Confidential Business Le...	3604	doc	Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Users\Wes Mantooth\[AppData\Local\Microsoft\Outlook\Outlook.pst]\[deleted].Letter+co...	Microso...	n/a	25.15 KB	8c77995b0cae1d93...	369ec5404e2736...			n/a	n/a	n/a
05	connection	1227		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Users\Wes Mantooth\[AppData\Local\Microsoft\Outlook\Outlook.pst]\[deleted].Connection	INDEX E...	n/a	n/a					n/a	n/a	n/a
05	connection	1878		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Program Files\ADMe\services\connection	INDEX E...	n/a	n/a					n/a	n/a	n/a
05	desktop.ini	1533		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\[filecycle.Bin\\$-1-3-166329-236305676-120339247-100]\desktop.ini	INDEX E...	n/a	n/a					n/a	n/a	n/a
05	DOWNLOD-1	1053		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Windows\DOWNLOD-1	INDEX E...	n/a	n/a					n/a	n/a	n/a
05	EPSS	1955		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Users\Wes Mantooth\[AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\EPSS.DOCX	INDEX E...	n/a	n/a					n/a	n/a	n/a
05	Exhume.docx	1452	doc	Mantooth32.0\Partition 1\Partition [NTFS]\[organ]\Exhume.docx	Microso...	40.40 KB	40.40 KB	522663c17a24d093...	a8b404af1b8db88...	2/12/2008 7:53...	2/12/2008 7:53...	2/12/2008		
05	FAVICOO-LICO	3095		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Users\Wes Mantooth\[AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\FAVICOO-LICO	INDEX E...	n/a	n/a					n/a	n/a	n/a
05	FightClub.jpg	1972	jpg	Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Users\Wes Mantooth\Desktop\secret\FightClub.jpg	JPEG	3584 B	3184 B	5d53e051864b33...	2e23872692914...	2/12/2008 7:53...	2/12/2008 7:53...	8/14/2000		
05	frogging.jpg	1416	jpg	Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Windows\Temporary Internet Files\Low\frogging.jpg	JPEG	39.00 KB	38.95 KB	52d0cff3d3047584...	d514b4b9c9c7b1...	2/12/2008 7:53...	2/12/2008 7:53...	8/14/2000		
05	group1.jpg	1417	jpg	Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Windows\Temporary Internet Files\Low\group1.jpg	JPEG	26.00 KB	25.87 KB	81b1161b1643b466...	98e386c54e1e17...	2/12/2008 7:53...	2/12/2008 7:53...	8/14/2000		
05	GROUP1-LHTM	1228		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Windows\System32\GRUPP1-2	INDEX E...	n/a	n/a					n/a	n/a	n/a
05	INGRES-LHTM	2788		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Users\Wes Mantooth\[AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\INGRES-LHTM	INDEX E...	n/a	n/a					n/a	n/a	n/a
05	INTERVIEW	1397		Mantooth32.0\Partition 1\Partition [NTFS]\[post]\Program Files\INTERVIEW	INDEX E...	n/a	n/a					n/a	n/a	n/a

Staged: 79 | Filtered: 79 | Total: 79 | Highlighted: 0 | Checked: 0 | Total LSize: 526.7 KB

Overview [Overview Tab Filter: [None]] 8:58 PM 12/3/2018

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

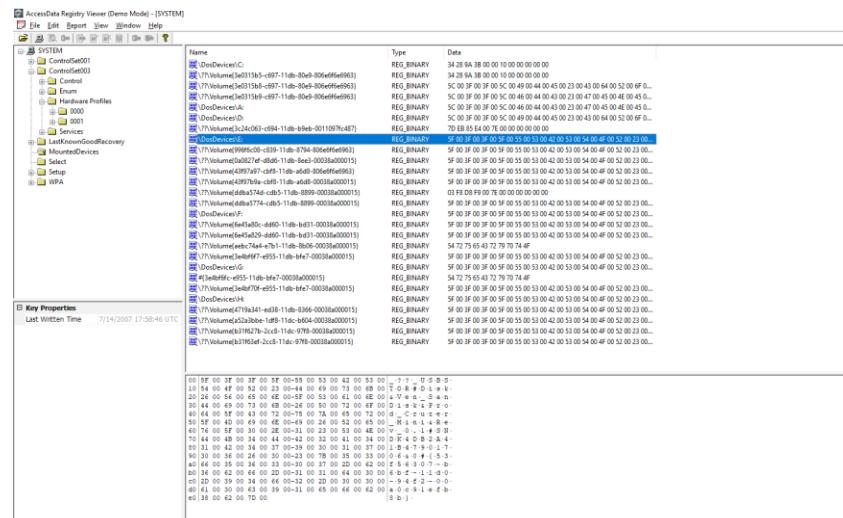
As seen in the screenshot below, FTK has carved 257 files, all of which are listed in the window.



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

After exporting the SYSTEM file from FTK and launching it in Registry viewer, you can find the Mounted Devices section where all the connected/disconnected devices are listed. Some of them are listed below with screenshots:

1. USBSTOR#Disk&Ven_SanDisk&Prod_Cruzer_Mini



2. USBSTOR#Disk&Ven_Flash&ProdDrive_UT

3. Apple iPod

4. USBSTOR#Disk&Ven_Sony_DSC

20. Identify the most recently run programs.

The prefetch can tell us the most recently run programs with their run count and when a particular executable was launched for the past 8 times. In the screenshot below, all the executables are in the descending order (most recently launched first in the list)

The screenshot shows the 'Items' tab in AccessData Forensic Toolkit. The left sidebar displays a tree view of categories such as Applications, Browsers, Networks, and Registry. The main pane lists files with columns for User, File Path, Run Count, and Last Run Time. A detailed table follows:

User	File Path	Run Count	Last Run Time
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\IIRULE.EXE	1	9/27/2007 9:10:28 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\IIRULE.EXE	257	9/27/2007 9:10:28 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\IFRULE.EXE	68	9/27/2007 9:10:28 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\ICONSENT.EXE	140	9/27/2007 9:10:26 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\ICONSENT.EXE	238	9/27/2007 9:10:26 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\DRIVERSFTFS.EXE	57	9/27/2007 8:09:36 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\DRIVERSFTFS.EXE	35	9/27/2007 8:09:36 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\DRVNTFNT.EXE	1	9/27/2007 8:09:35 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\DRVNTFNT.EXE	1	9/27/2007 7:16:51 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\DRVNTFNT.EXE	18	8/24/2007 11:10:47 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\DRVNTFNT.EXE	25	8/24/2007 11:10:47 AM
	\DEVICE\HARDISKVOLUME1\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE	56	8/24/2007 9:09:48 AM
	\DEVICE\HARDISKVOLUME1\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE	8	8/24/2007 9:09:48 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\WCOPY.EXE	15	8/24/2007 8:40:34 AM
	\DEVICE\HARDISKVOLUME1\PROGRAM FILES\ACCESSDATA FTK IMAGER\FTK IMAGER.EXE	38	8/24/2007 8:40:01 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\W3DFILTER.EXE	42	8/24/2007 8:39:20 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\CONTROLC.EXE	18	8/24/2007 8:39:23 AM
	\DEVICE\HARDISKVOLUME1\WINDOWS\SYSTEM32\DRVNTFNT.EXE	18	8/24/2007 6:08:27 AM

Below the table, the 'Provenance' section shows the path: Marboot32.E01\Partition 1\MANTOO1 [NTFS]\root\Windows\Prefetch\[EUSER.EXE-0B95A854].pf.

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

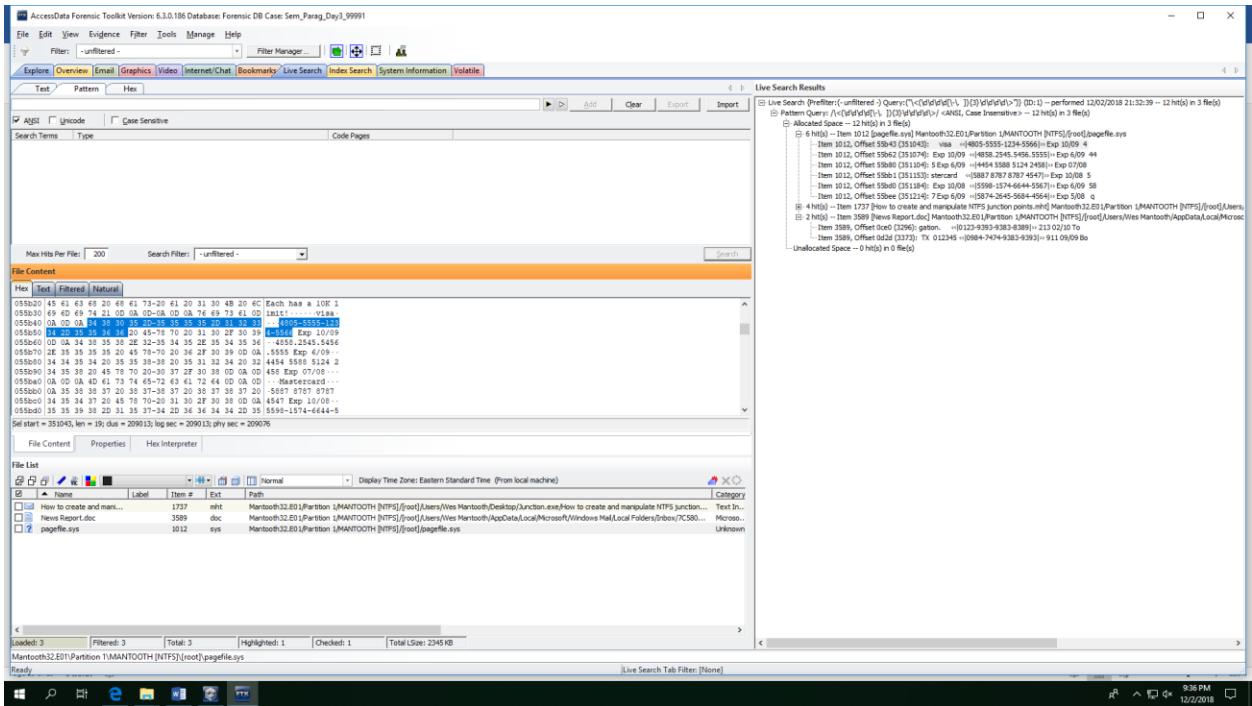
The NTUSER.dat has a section called “TypedURLs” where all the urls that were typed and entered into the browser are stored. Below is a screenshot of the same.

The screenshot shows the 'Key Properties' tab in AccessData Registry Viewer. The 'Last Written Time' is listed as 20/12/2008 10:53:19 UTC. The 'Data' column contains the following URLs:

Name	Type	Data
u1	REG_SZ	http://www.google.com/
u10	REG_SZ	http://www.tigerdirect.com/
u11	REG_SZ	http://www.newegg.com/
u12	REG_SZ	http://www.msn.com/
u13	REG_SZ	http://www.mamma.com/
u14	REG_SZ	http://www.yahoo.com/
u15	REG_SZ	http://www.google.com/
u16	REG_SZ	http://www.google.com/
u17	REG_SZ	http://www.youtube.com/
u18	REG_SZ	C:\Users\W...\My Documents\Scripts\\\mbedsacer
u19	REG_SZ	http://www.somethingsogood.com/
u20	REG_SZ	http://www.msnbc.msn.com/
u21	REG_SZ	F:\Windows\System32\inetat
u22	REG_SZ	http://www.united.com/
u23	REG_SZ	http://www.google.com/
u24	REG_SZ	http://www.google.com/
u25	REG_SZ	http://www.google.com/
u26	REG_SZ	http://www.hotbot.com/
u27	REG_SZ	http://www.yahoo.com/
u28	REG_SZ	http://www.lyrics.com/
u29	REG_SZ	http://www.concert.net/
u30	REG_SZ	http://www.aol.com/
u31	REG_SZ	http://www.arn.com/
u32	REG_SZ	Web Mantooth

22. Identify any credit card numbers on the drive. (This will require live search with a regular expression)

I made user of Live Search in FTK and used pattern search that is pre built with Credit Card query pattern to find Credit card information. Below are screenshots of the same.



AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Sem_Parag_Day3_99991

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager Import

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

Test Pattern Hex

Max Hits Per File: 200 Search Filters: -unfiltered -

File Content

Hex Test Filtered Natural

055b20 45 41 43 48 20 48 41 73>20 61 20 31 30 48 20 6C Each has a 10K 1
055b30 69 4D 69 74 21 0D 0A 0D>0A 0D 76 69 74 0D init.....vines
055b40 0A 0D 0A 34 38 30 35 2D>35 35 35 2D 31 32 35-4505-5555-123
055b50 34 35 38 20 45 78 70 20 36 2F 30 39 0D 0A 0D-4555-5555-123
055b60 0A 34 35 38 20 45 78 70 20 36 2F 30 39 0D 0A 0D-4555-5555-123
055b70 2E 35 35 35 35 20 45 78>70 20 36 2F 30 39 0D 0A 0D-4555-5555-123
055b80 0A 0D 0A 4D 61 73 74 65>72 63 61 72 64 0D 0D-Mastercard...
055b90 34 35 38 20 45 78 70 20 36 2F 30 39 0D 0A 0D-4555-5555-123
055ba0 35 35 39 20 31 35 37>34 2D 36 34 2D 35 5590-1574-6444-5
Set start = 351074 len = 19 due = 209013; log sec = 209013; phy sec = 209076

File Content Properties Hex Interpreter

File List

#	Name	Label	Item #	Ext	Path	Category
1	How to create and... 1737	mht	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\Desktop\Junction.exe			Text In...
2	News Report.doc 3598	doc	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox\7C580...			Microso...
3	pagefile.sys 1012	sys	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\root\pagefile.sys			Unknown

Loaded: 3 Filtered: 3 Total: 3 Highlighted: 1 Checked: 1 Total LSize: 2345 KB

Ready Live Search Tab Filter: [None]

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Sem_Parag_Day3_99991

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager Import

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

Test Pattern Hex

Max Hits Per File: 200 Search Filters: -unfiltered -

File Content

Hex Test Filtered Natural

055b20 45 41 43 48 20 48 41 73>20 61 20 31 30 48 20 6C Each has a 10K 1
055b30 69 4D 69 74 21 0D 0A 0D>0A 0D 76 69 74 0D init.....vines
055b40 0A 0D 0A 34 38 30 35 2D>35 35 35 2D 31 32 35-4505-5555-123
055b50 34 35 38 20 45 78 70 20 36 2F 30 39 0D 0A 0D-4555-5555-123
055b60 0A 34 35 38 20 45 78 70 20 36 2F 30 39 0D 0A 0D-4555-5555-123
055b70 2E 35 35 35 35 20 45 78>70 20 36 2F 30 39 0D 0A 0D-4555-5555-123
055b80 0A 0D 0A 4D 61 73 74 65>72 63 61 72 64 0D 0D-Mastercard...
055b90 34 35 38 20 31 35 37>34 2D 36 34 2D 35 5590-1574-6444-5
Set start = 351104 len = 19 due = 209013; log sec = 209013; phy sec = 209076

File Content Properties Hex Interpreter

File List

#	Name	Label	Item #	Ext	Path	Category
1	How to create and... 1737	mht	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\Desktop\Junction.exe			Text In...
2	News Report.doc 3598	doc	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox\7C580...			Microso...
3	pagefile.sys 1012	sys	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\root\pagefile.sys			Unknown

Loaded: 3 Filtered: 3 Total: 3 Highlighted: 1 Checked: 1 Total LSize: 2345 KB

Ready Live Search Tab Filter: [None]

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Sem_Parag_Day3_99991

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager Import

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

Test Pattern Hex

Max Hits Per File: 200 Search Filters: -unfiltered -

File Content

Hex Test Filtered Natural

055b20 45 41 43 48 20 48 41 73>20 61 20 31 30 48 20 6C Each has a 10K 1
055b30 69 4D 69 74 21 0D 0A 0D>0A 0D 76 69 74 0D init.....vines
055b40 0A 0D 0A 34 38 30 35 2D>35 35 35 2D 31 32 35-4505-5555-123
055b50 34 35 38 20 45 78 70 20 36 2F 30 39 0D 0A 0D-4555-5555-123
055b60 0A 34 35 38 20 45 78 70 20 36 2F 30 39 0D 0A 0D-4555-5555-123
055b70 2E 35 35 35 35 20 45 78>70 20 36 2F 30 39 0D 0A 0D-4555-5555-123
055b80 0A 0D 0A 4D 61 73 74 65>72 63 61 72 64 0D 0D-Mastercard...
055b90 34 35 38 20 31 35 37>34 2D 36 34 2D 35 5590-1574-6444-5
Set start = 351104 len = 19 due = 209013; log sec = 209013; phy sec = 209076

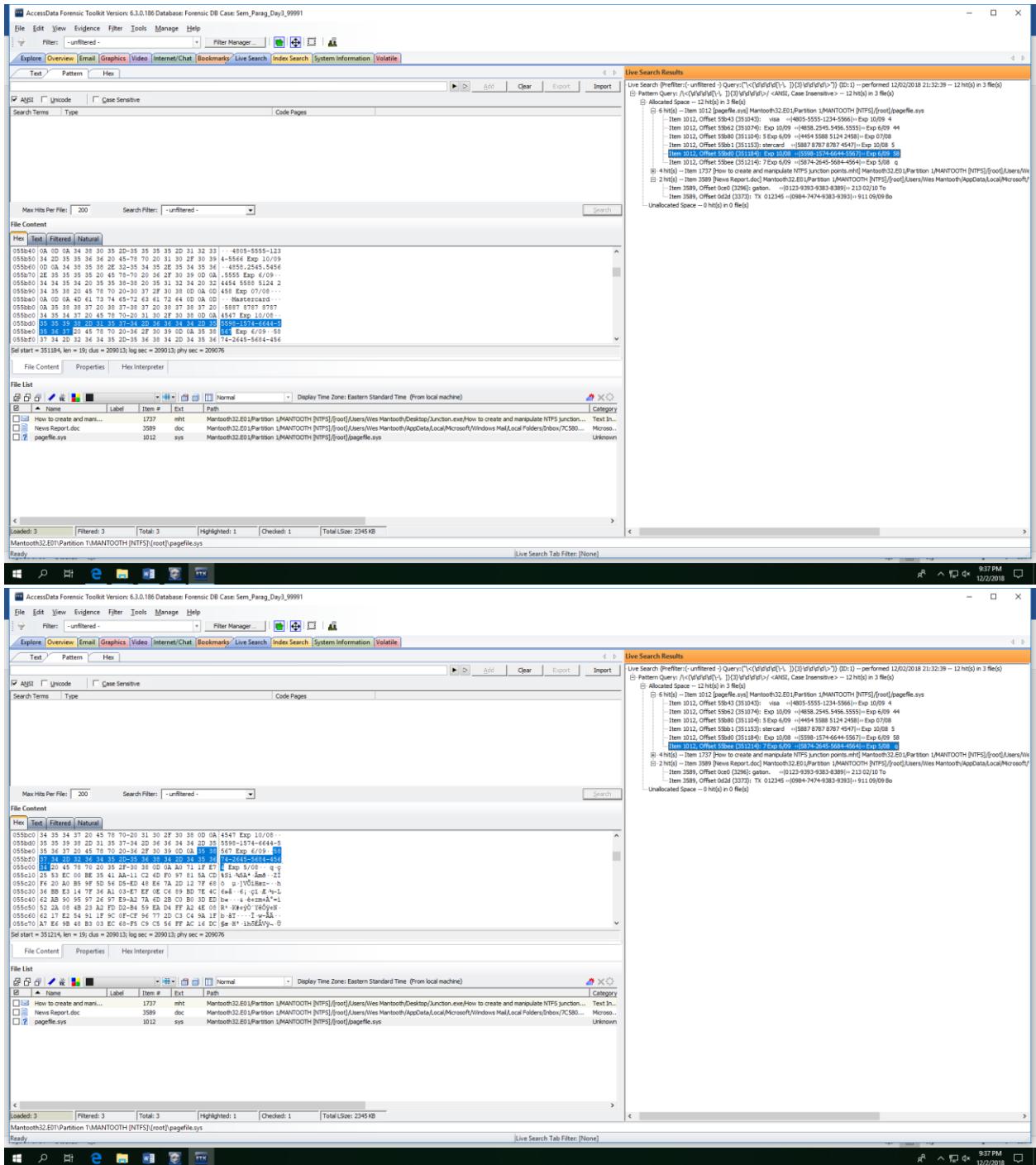
File Content Properties Hex Interpreter

File List

#	Name	Label	Item #	Ext	Path	Category
1	How to create and... 1737	mht	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\Desktop\Junction.exe			Text In...
2	News Report.doc 3598	doc	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox\7C580...			Microso...
3	pagefile.sys 1012	sys	Mantooth32.E01\Partition 1\MANTOOTH [NTFS]\root\pagefile.sys			Unknown

Loaded: 3 Filtered: 3 Total: 3 Highlighted: 1 Checked: 1 Total LSize: 2345 KB

Ready Live Search Tab Filter: [None]

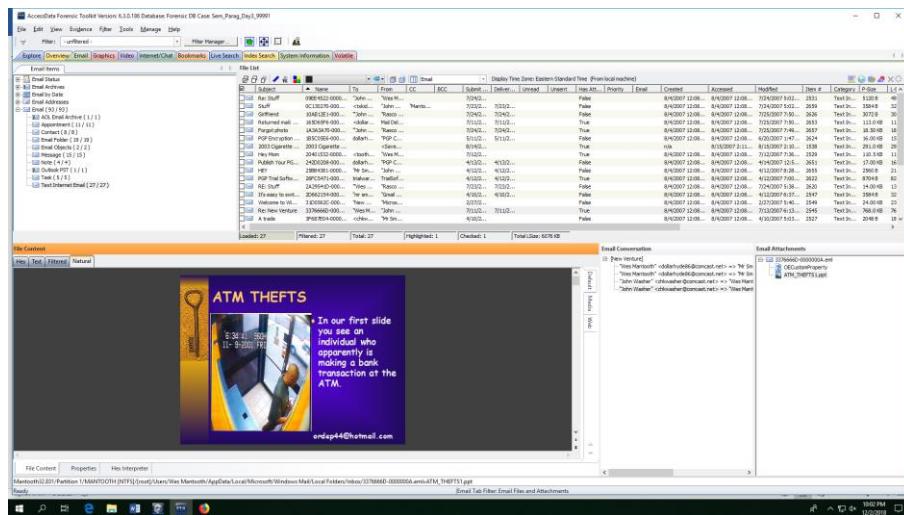
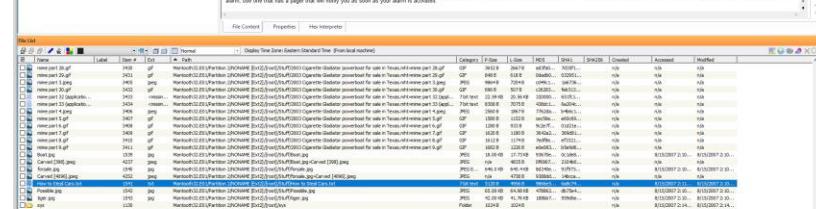
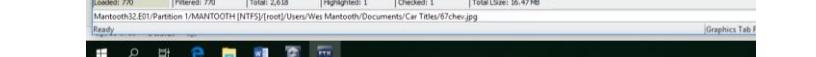
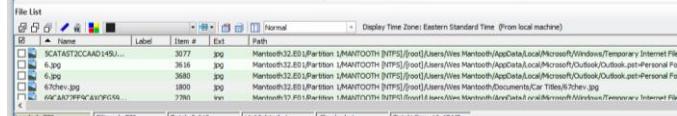
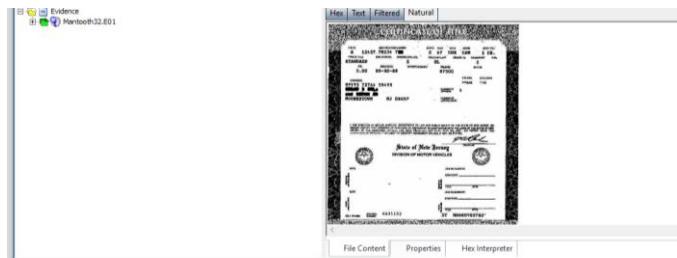


The screenshot displays the Access Data Forensic Toolkit interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, Help, and a Filter Manager button. Below the menu is a toolbar with icons for Text, Pattern, Hex, Filter, Add, Clear, Export, Import, and a magnifying glass icon. The main window has tabs for Explore, Overview, Email, Graphics, Video, Internet/Chat, Bookmarks, Live Search, Index Search, System Information, and Volatile. A search bar at the top allows filtering by ANSI, Unicode, and Case Sensitive, and includes a dropdown for Code Pages. The left pane shows 'File Content' with tabs for Hex, Text, Filtered, and Natural. The Hex tab displays binary data for several file types, including PDF, JPEG, and various document formats. The Text tab shows ASCII text, including a file named 'How to create and manipulate NTFS junction points.pdf'. The Filtered tab shows a subset of the data, and the Natural tab shows the data as it appears in the original file. The right pane is titled 'Live Search Results' and shows a list of search results for the query 'junction'. It lists items such as 'How to create and manipulate NTFS junction points.pdf' and 'News Report.doc', along with their file paths and offsets. The bottom status bar indicates loaded files (3), filtered files (3), total files (3), highlighted items (1), checked items (1), and a total size of 2045 KB. The bottom right corner shows the date and time as 9:37 PM on 12/2/2018.

23. Detective Ketchum has provided a list of search terms: Theft, Title, Checks, Scam, and Forensics. Provide ONLY (a few examples of) results of these that you believe may be relevant.

Some of the other evidence which I found relevant to the above terminologies are below:

THIS WARRANT VOID AFTER AUGUST 24, 2006
Auditor of State of Arkansas
To the State Treasurer, Little Rock, Ark
PMT TO THE ORDER OF:
[Redacted Address]
- PAY THIS AMOUNT -
*****2400.00
RECEIVED BY [Signature] Jim Tuck
TREASURER OF STATE
D 0942 07 24 2005 COB 200 76784 570614300# /0000000000✓



AccessData Forensic Toolkit Version 6.0.0.188 Database Forensic DB Case: Sem_Parag_Day_1_99991

Email Items

	Name	To	From	CC	BCC	Date	Subject	Unred.	Urgent	Time Att.	Priority	From	Opened	Modified	Item #	Category	Size	
...	Friend...	John...	Rasco...			7/24/0...	7042...					8/4/2007 12:08...	8/4/2007 12:08...	7/23/2007 7:50...	308	Text	3072 B	10
...	Retuned mail...	1650409...	...dolar...	Hai Del...		7/11/0...	7012...					8/4/2007 12:08...	8/4/2007 12:08...	7/23/2007 7:50...	363	Text	113.54 KB	11
...	Refund (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)																	
...	All AOL Email Archive (1/1)																	
...	All AOL Email Archive (1/1)																	
...	All Contact (8/8)																	
...	All Contact (8/8)				</td													

Finally, I hashed the image file again to verify if there was any tampering after we acquired the image.

Drive/Image Verify Results	
Name	Mantooth32.E01
Sector count	250879
MD5 Hash	
Computed hash	31217210a1a69f272079a3bde3d9d8fc
Stored verification hash	31217210a1a69f272079a3bde3d9d8fc
Verify result	Match
SHA1 Hash	
Computed hash	12e4ac047e328ca2bd63a4d65df25b3ecba55
Bad Blocks List	No bad blocks found in image
Close	

Conclusion:

In this case, I examined the forensic image given to me by Detective Ketchum and I performed various different tasks to find out the information for the report. I found the user passwords, understood which user logged on the most, also which OS and service pack is it running. I also, found evidence related to Mantooth's case. Moreover, I also identified recently run programs, recovered credit card info numbers, etc. I performed hash verification twice in this project to ensure the integrity during the acquisition and after performance.