

CSEC 730 - Advanced Computer Forensics

Lab 2 - Forensic Toolkit (FTK) Lab

Questions 1: Read the default options of “Evidence Refinement” and “Index Refinement” and list 5 default settings from “Evidence Refinement” and 5 default settings from “Index Refinement.

For Evidence Refinement (ADVANCED)

1. Include File Slack
2. Include Free Space
3. Ignore Status for all file status (Deleted, Encrypted, From Email)
4. All file types are selected by default

For Index Refinement (ADVANCED)

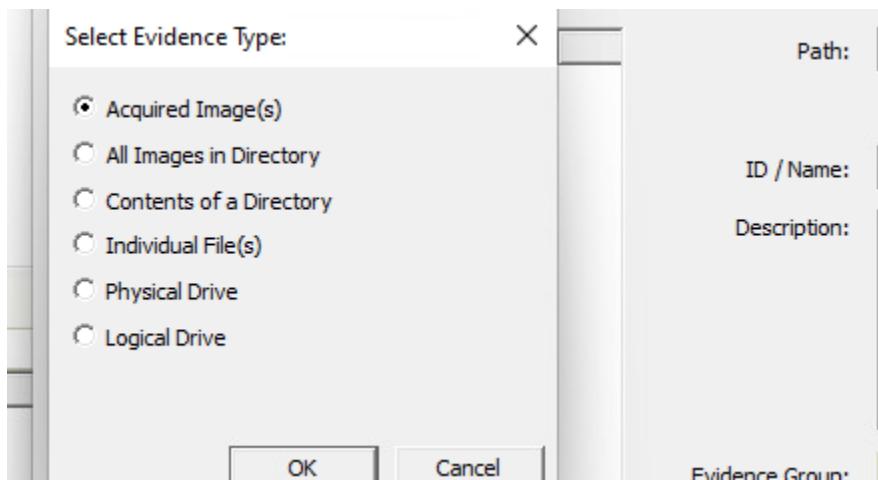
1. Include File Slack
2. Include Free Space
3. Ignore Status for all file status (Deleted, Encrypted, From Email)
4. All file types are selected by default
5. Include Message Headers by default

For Evidence Processing

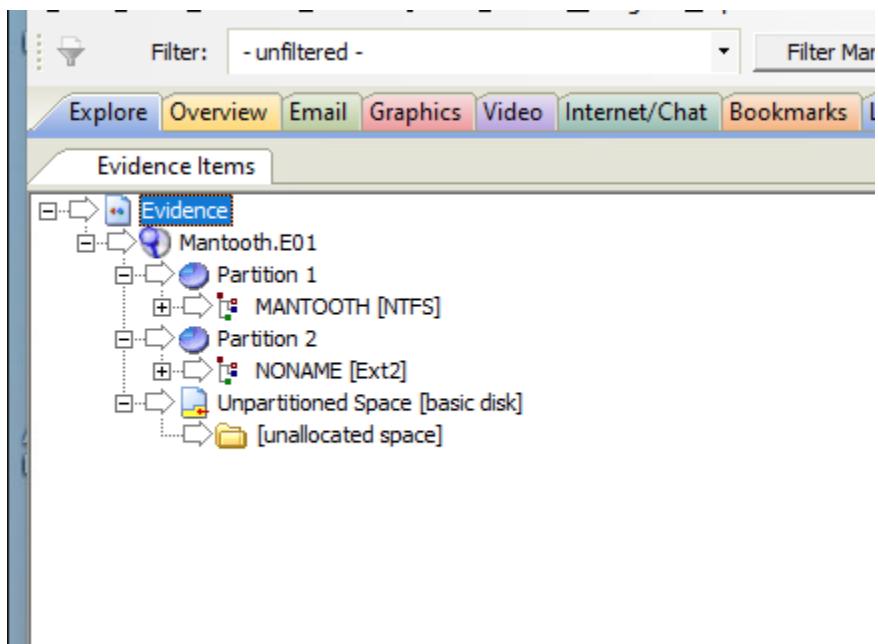
1. MD5 Hash
2. SHA-1 Hash
3. Expand Compound files
4. Flag Bad Extensions
5. Search Text Index
6. Create Thumbnails for Graphics
7. Include Deleted files

Question 2: What are the types of evidence that can be added to a case in FTK?

These are different types of evidence type we can add into the FTK



Question 3: Expand Mantooth.E01, how many partitions are in this image, and what are the filesystems?



Two partitions

1. NTFS
2. Ext 2 (Linux file system)

Question 4: Find \$Recycle.Bin from Partition 1, which user (user name) once owned and then deleted the files that belong to SID=1000? How do you know?

From this screenshot we can see that wes Mantooth user once owned these files and deleted it. We can say it belongs to Mantooth by seeing the path which says MANTOOTH[NTFS].

The screenshot shows a file viewer for the Windows Vista Recycle Bin. On the left is a tree view of the Recycle Bin structure:

```

    [root]
    +-- $BadClus
    +-- $Extend
    +-- $Recycle.Bin
        +-- S-1-5-21-3166329-3263506726-1320359247-1000
            +-- S-1-5-21-3166329-3263506726-1320359247-1001
                +-- S-1-5-21-3166329-3263506726-1320359247-1002
                    +-- S-1-5-21-51003140-4199384537-3980697693-500
    +-- $Secure
    +-- Boot
    +-- Documents and Settings
    +-- MSOCache

```

The main pane displays the details of a selected file:

Windows Vista Recycle Bin File	
Original Name	C:\Users\Wes Mantooth\Pictures\monkey-nerd.jpg
Logical Size	6KB
Date Recycled	7/26/2007 7:27:20 PM -0400

Below this is a table of deleted files:

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5
I2M7A26.jpg		1381	jpg	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$I2M7A26...	Unknown	544 B	544 B	73ed7a...
:30		1382	<missin...	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$:30	Index ...	4096 B	4096 B	5d3c90...
:30		1099		Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$:30	Index ...	4096 B	4096 B	caa5d8...
S61QDF.exe		1380	exe	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$S61QDF...	Unknown	544 B	544 B	e8c587...
R9HZOZO.jpg		1379	jpg	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R9HZOZO...	Unknown	544 B	544 B	f1cd3...
EZFRY8		1378	<missin...	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$EZFRY8...	Unknown	544 B	544 B	d620e0...
I49IB5.DLL		1377	dll	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$I49IB5...	Unknown	544 B	544 B	64ac1a...
JQVPHB.jpg		1376	jpg	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$JQVPHB...	Unknown	544 B	544 B	1336ed...
KY3FVP.gif		1375	gif	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$KY3FVP.gif	Unknown	544 B	544 B	4ced78...
NHBWN2.zip		1374	zip	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$NHBWN2...	Unknown	544 B	544 B	99f247...
THDUS5.exe		1351	exe	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$THDUS5...	Unknown	544 B	544 B	855f32...
R2M7A26.jpg		1373	jpg	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R2M7A2...	JPEG	14.00 KB	13.82 KB	489e96...
R61QDF.exe		1372	exe	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R61QDF...	Exe	1327 KB	1327 KB	0d6417...
R9HZOZO.jpg		1371	jpg	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R9HZOZO...	JPEG	6656 B	6468 B	6fb3c7...
REZFRY8		1357		Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$REZFRY8	Folder	56 B	56 B	
I49IB5.DLL		1356	dll	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$I49IB5...	Fxe	15.00 KR	15.00 KR	90945...

Question 5: Which file category (starting from File Category) does the file, Confidential Business Letter.doc, belong to? What is the file path for this file?

It belong to Documents > Microsoft Documents

File Path for this file in below screenshot:

The screenshot shows a file viewer with the following file path displayed in the status bar:

Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Outlook/Outlook.pst>Personal Folders>Top of Personal Folders>Inbox>Letter>Confidential Business Letter.doc

Screenshot of a digital forensics tool interface showing file analysis results.

File Overview:

- File Category (2,360 / 2,360)
- Databases (3 / 3)
- Documents (1,992 / 1,992)
- HTML and XML (76 / 76)
- Microsoft Documents (15 / 15)
- Other Documents (199 / 199)
- Email (92 / 92)
- Events (11 / 11)
- Icons (595 / 595)
- Graphics (582 / 582)
- Internet/Chat Files (72 / 72)
- Mobile Phone (0 / 0)

File Content:

Lagos, Nigeria.
Attention: The President/CEO
Dear Sir,

Confidential Business Proposal

File List:

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
ar_test_niubi.doc		1962	doc	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Desktop\secret\ar_test_niubi.doc	Microso...	19.00 KB	19.00 KB	e64a69...	340dd8...	n/a	2/12/2008 7:53...	2/12/2008 7:53...	5/26/2006 7:09...
Arabic.Text.doc		1479	doc	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Public\Documents\Arabic.Text.doc	Microso...	22.00 KB	22.00 KB	5cb5ed...	a845e5...	9/25/2007 4:05...	9/25/2007 4:05...	7/9/2006 3:21...	
Astral.doc		1257	doc	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[orphan]\Book of Hod\Astral.doc	Microso...	38.00 KB	38.00 KB	7ce891...	59b829...	2/12/2008 7:53...	2/12/2008 7:53...	2/12/2008 7:09...	
Confidential Business Le...		3556	doc	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Apodata\local\Microsoft\Outlook\Outlook.pst\Personal Folders\De...	Microso...	n/a	29.15 KB	82789...	3d3ec5...	n/a	n/a	n/a	n/a
Dear Sweetie.doc		3204	doc	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Apodata\local\Microsoft\Outlook\Outlook.pst\Personal Folders\De...	Microso...	25.00 KB	25.00 KB	53c9f1...	403700...	7/12/2007 7:51...	7/13/2007 2:36...	7/14/2007 6:17...	
Dear Sweetie.doc		1751	doc	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Documents\Dear Sweetie.doc	Microso...	63.50 KB	63.50 KB	9541b9...	b79149...	7/12/2007 7:51...	7/13/2007 2:36...	7/14/2007 6:17...	
Eduhome.doc		1289	doc	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[orphan]\ManfitEduhome.doc	Microso...	40.00 KB	40.00 KB	522663...	888404...	2/12/2008 7:53...	2/12/2008 7:53...	2/12/2008 7:08...	
How To Steal Credit Nu...		3301	doc	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Apodata\local\Microsoft\Windows Mail\Local Folders\inbox...	Microso...	36.95 KB	27.00 KB	0181f1...	a25332...	n/a	n/a	n/a	n/a
Japanese.text.doc		1480	doc	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Public\Documents\Japanese.text.doc	Microso...	25.00 KB	25.00 KB	40370...	048ed3...	9/25/2007 4:05...	9/25/2007 4:05...	7/9/2006 3:46...	
News Report.doc		3251	dot	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Apodata\Local\Microsoft\Windows Mail\Local Folders\inbox...	Microso...	65.01 KB	47.50 KB	6f8667...	564111...	n/a	n/a	n/a	n/a
Normal.dot		2197	dot	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Apodata\Roaming\Microsoft\Templates\Normal.dot	Microso...	31.50 KB	31.50 KB	05376...	db5ee4...	7/7/2007 6:57...	7/7/2007 6:57...	6/20/2007 1:51...	
qui_test_ls53.doc		1961	dot	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Desktop\secret\qui_test_ls53.doc	Microso...	19.00 KB	19.00 KB	59b800...	f0576f...	2/12/2008 7:53...	2/12/2008 7:53...	5/26/2006 7:09...	
russ_2_AxesKeypeak.doc		1960	dot	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Desktop\secret\russ_2_AxesKeypeak.doc	Microso...	19.00 KB	19.00 KB	169908...	4a70ba...	2/12/2008 7:53...	2/12/2008 7:53...	5/26/2006 7:09...	
Something interesting.rtf		1753	rtf	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Documents\Something interesting.rtf	Microso...	59.00 KB	58.77 KB	c4-472...	c96a38...	3/6/2007 9:17...	6/20/2008 11:5...	5/8/2007 9:23...	
Vampire.doc		1254	doc	Manooth.E01\Partition 1\MANTOOTH [NTFS]\[orphan]\Vampire.doc	Microso...	72.00 KB	72.00 KB	110e71...	5f4631...	2/12/2008 7:53...	2/12/2008 7:53...	2/12/2008 7:08...	

Question 6: Open the Confidential Business Letter.doc, check both File Content and Properties, who was the document author, when was this document last modified, and who modified at the last time?

This file belongs to (Author) Rasco Badguy and last saved or modified by Nick Drehel, Jr. The Last time it is modified and saved is August 1 2007 3.04 pm.

Screenshot of a digital forensics tool interface showing file properties and file details.

Properties:

Code page	1,252
Title	Confidential Business Letter
Subject	Lets scam the people
Author	Rasco Badguy
Keywords	Nigeria, Confidential, Nigerian, Central
Comments	This letter will really get them to give up their money.
Template	Normal
Last saved by	Nick Drehel, Jr.

File Content:

Display Time Zone: Eastern Daylight Time (From local machine)

File Details:

Keywords	Nigeria, Confidential, Nigerian, Central Bank, Apex, National Petroleum Corporation
Comments	This letter will really get them to give up their money. We need to get this out to any
Template	Normal
Last saved by	Nick Drehel, Jr.
Revision number	2
Total editing time	11 minutes 0 seconds
Create time	8/1/2007 2:53:00 PM (2007-08-01 18:53:00 UTC)

Template	Normal
Last saved by	Nick Drehel, Jr.
Revision number	2
Total editing time	11 minutes 0 seconds
Create time	8/1/2007 2:53:00 PM (2007-08-01 18:53:00 UTC)
Last saved time	8/1/2007 3:04:00 PM (2007-08-01 19:04:00 UTC)
Number of pages	1
Number of words	272

File Content Properties Hex Interpreter

Dienstau Time Zone: Eastern Daylight Time (From local machine)

Question 7: What are the two documents that use foreign languages?

Two documents are Arabic Text.doc which is in arabic and Japanese text.doc in Japanese.

Case Overview													
File Content													
Hex Text Filtered Natural													
<pre>العربية تكرر تصدى ابظلى الخاع ان لا هنرى نجزي الخص من سرعة خرة ان المدرا من 50 الثقة فى الثاني ملها اجاز من فرسا اقررت 2006. قدم تكر المعلم كالم لمسلمة اليمانية الميلاد الأول الشوط فى فريق كل بوب وفوسا ابظلى متملا بعد وف</pre>													
<pre>البرأ من المساحة النفعي في زيان الدين زيز احراز جراء خضراء من بيد فرسا اقتضى ركبة مدرية من عرضية لكرة ينبع تصدى الذي ملائى النم برس فرس بمعر 19 الثقة فى التعلم هذه اجاز من ابظلى المتسب تكين بيني في الراسية تزوي ابظلى المهام تكره تخصت العرضة ان لا 36 الثقة فى تذكر هذا تجز ان اصليا وكت</pre>													
File Content Properties Hex Interpreter													

File List													
Display Time Zone: Eastern Daylight Time (From local machine)													
Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Exhume.doc		1259	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[orphan]\Afr\Exhume.doc	Microso...	40.00 KB	40.00 KB	522653...	a8940d...	2/12/2008 7:53...	2/12/2008 7:08...	2/12/2008 7:08...	
Astral.doc		1257	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[orphan]\Book of Not\Astral.doc	Microso...	38.00 KB	38.00 KB	70ed69...	59b829...	2/12/2008 7:53...	2/12/2008 7:09...	2/12/2008 7:09...	
Vampire.doc		1254	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[orphan]\Vampire.doc	Microso...	1.00 KB	1.00 KB	13e1e0...	54e4b5...	2/12/2008 7:53...	2/12/2008 7:03...	2/12/2008 7:06...	
Arabic Text.doc		1479	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Public\Documents\Arabic Text.doc	Microso...	25.00 KB	25.00 KB	462b70...	0xb6ed3...	9/25/2007 4:05...	7/9/2006 3:21...	7/9/2006 3:21...	
Japanese text.doc		1480	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Public\Documents\Japanese text.doc	Microso...	25.00 KB	25.00 KB	8c7789...	3d8ec5...	9/25/2007 4:05...	7/9/2006 3:46...	7/9/2006 3:46...	
Confidential Business Le...		3221	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Outlook\Outlook.pst-[deleted].lve...	Microso...	n/a	29.15 KB	8c7789...	n/a	n/a	n/a	n/a	n/a
Confidential Business Le...		3556	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Outlook\Outlook.pst-Personal Fol...	Microso...	n/a	29.15 KB	8c7789...	3d8ec5...	n/a	n/a	n/a	n/a
How To Steal Credit Nu...		3301	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox...	Microso...	65.01 KB	27.00 KB	018d1f...	a25337...	n/a	n/a	n/a	n/a
News Report.doc		3251	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox...	Microso...	65.01 KB	47.50 KB	6b8667...	564111...	7/7/2007 6:57...	7/7/2007 6:57...	6/20/2007 1:51...	
Normal.dot		2197	dot	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Roaming\Microsoft\Templates\Normal.dot	Microso...	31.50 KB	31.50 KB	053b76...	cb58e4...	7/7/2007 6:57...	7/7/2007 6:57...	7/13/2007 2:36...	
Dear Sweetie.doc		1751	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Documents\Dear Sweetie.doc	Microso...	63.50 KB	63.50 KB	954418...	b79149...	7/12/2007 7:51...	7/13/2007 2:36...	7/14/2007 6:17...	

Archives (13 / 13)
Databases (3 / 3)
Desktop Icons (2 / 2)
Address Books (2 / 2)
HTML and XML (76 / 76)
Microsoft Documents (15 / 15)
Microsoft RTF (1 / 1)
Microsoft Word (14 / 14)
Microsoft Word 2000 (3 / 3)
Microsoft Word 2003 (11 / 11)
Other Documents (199 / 199)
Email (92 / 92)
Executable (11 / 11)

Archives (13 / 13)
Databases (3 / 3)
Desktop Icons (2 / 2)
Address Books (2 / 2)
HTML and XML (76 / 76)
Microsoft Documents (15 / 15)
Microsoft RTF (1 / 1)
Microsoft Word (14 / 14)
Microsoft Word 2000 (3 / 3)
Microsoft Word 2003 (11 / 11)
Other Documents (199 / 199)
Email (92 / 92)
Executable (11 / 11)

File List													
Display Time Zone: Eastern Daylight Time (From local machine)													
Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
Exhume.doc		1259	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[orphan]\Afr\Exhume.doc	Microso...	40.00 KB	40.00 KB	522653...	a8940d...	2/12/2008 7:53...	2/12/2008 7:08...	2/12/2008 7:08...	
Astral.doc		1257	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[orphan]\Book of Not\Astral.doc	Microso...	38.00 KB	38.00 KB	70ed69...	59b829...	2/12/2008 7:53...	2/12/2008 7:09...	2/12/2008 7:09...	
Vampire.doc		1254	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[orphan]\Vampire.doc	Microso...	1.00 KB	1.00 KB	13e1e0...	54e4b5...	2/12/2008 7:53...	2/12/2008 7:03...	2/12/2008 7:06...	
Arabic Text.doc		1479	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Public\Documents\Arabic Text.doc	Microso...	25.00 KB	25.00 KB	462b70...	0xb6ed3...	9/25/2007 4:05...	7/9/2006 3:21...	7/9/2006 3:21...	
Japanese text.doc		1480	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Public\Documents\Japanese text.doc	Microso...	25.00 KB	25.00 KB	8c7789...	3d8ec5...	9/25/2007 4:05...	7/9/2006 3:46...	7/9/2006 3:46...	
Confidential Business Le...		3221	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Outlook\Outlook.pst-[deleted].lve...	Microso...	n/a	29.15 KB	8c7789...	n/a	n/a	n/a	n/a	n/a
Confidential Business Le...		3556	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Outlook\Outlook.pst-Personal Fol...	Microso...	n/a	29.15 KB	8c7789...	3d8ec5...	n/a	n/a	n/a	n/a
How To Steal Credit Nu...		3301	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox...	Microso...	36.95 KB	27.00 KB	018d1f...	a25337...	n/a	n/a	n/a	n/a
News Report.doc		3251	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox...	Microso...	65.01 KB	47.50 KB	6b8667...	564111...	7/7/2007 6:57...	7/7/2007 6:57...	6/20/2007 1:51...	
Normal.dot		2197	dot	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Roaming\Microsoft\Templates\Normal.dot	Microso...	31.50 KB	31.50 KB	053b76...	cb58e4...	7/7/2007 6:57...	7/7/2007 6:57...	7/13/2007 2:36...	
Dear Sweetie.doc		1751	doc	Mantooth.E0\Partition_1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Documents\Dear Sweetie.doc	Microso...	63.50 KB	63.50 KB	954418...	b79149...	7/12/2007 7:51...	7/13/2007 2:36...	7/14/2007 6:17...	

Archives (13 / 13)
Databases (3 / 3)
Desktop Icons (2 / 2)
Address Books (2 / 2)
HTML and XML (76 / 76)
Microsoft Documents (15 / 15)
Microsoft RTF (1 / 1)
Microsoft Word (14 / 14)
Microsoft Word 2000 (3 / 3)
Microsoft Word 2003 (11 / 11)
Other Documents (199 / 199)
Email (92 / 92)
Executable (11 / 11)

Go to File Category > Documents > HTML, and look for a Google search file that Mantooth searched “atm card stealing”.

Show a screenshot below.

We can see from the screenshot that Mantooth searched for this html page “atm card stealing”

The screenshot shows a file browser interface with a sidebar navigation and a main search results area. The sidebar includes categories like Archives, Databases, Documents, Microsoft Office, and Other Documents. The search bar at the top contains the query "atm card stealing". Below the search bar, the results are displayed with a title "PINs no obstacle for debit card thieves - Security - MSNBC.com". The results table has columns for Name, Label, Item #, Ext, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, Accessed, and Modified. The results list several files, mostly HTML documents, with their respective details.

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
ingred[2].htm		2934	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	3534B	3308 B	F743... 0cd914...				7/12/2007 7:17...	7/2/2008 4:59...	7/12/2007 7:1...
REDIRURL=ord=73818...		2927	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	4608 B	4324 B	d43023... 1c1d7a...				7/12/2007 7:13...	7/2/2008 4:59...	7/12/2007 7:1...
search[1].htm		2928	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	16 B	16 B	3520ca... 2000ca...				7/12/2007 7:13...	7/2/2008 5:00...	7/12/2007 7:1...
ad[1].htm		2979	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	6,144 B	5962 B	4e342a... 5a26ca...				7/12/2007 7:13...	7/2/2008 5:00...	7/12/2007 7:1...
Chapter1.htm		2961	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	36,00 B	35,67 KB	977600... e4d7a6...				7/12/2007 7:16...	7/2/2008 5:01...	7/12/2007 7:1...
image[1].htm		2957	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	24,50 KB	24,24 KB	55a4e2... 1f05ab...				7/12/2007 7:17...	7/2/2008 5:01...	7/12/2007 7:1...
ingred[1].htm		2979	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	1536 B	1211 B	94e16... 79469a...				7/12/2007 7:17...	7/2/2008 5:01...	7/12/2007 7:1...
news995376[4].htm		2789	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	22,00 B	21,90 KB	F7153... 600184...				7/12/2007 7:16...	7/2/2008 5:01...	7/12/2007 7:1...
search[1].htm		2785	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	19,50 kB	19,44 KB	739427... 1ada8a...				7/12/2007 7:15...	7/2/2008 5:01...	7/12/2007 7:1...
slaved_c[1].htm		2784	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	1024 B	809 B	662791... 779554...				7/12/2007 7:13...	7/2/2008 5:01...	7/12/2007 7:1...
ad[1].htm		2877	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	4608 B	4158 B	b7612... b3f418...				7/12/2007 7:13...	7/2/2008 5:04...	7/12/2007 7:1...
Chapter1.htm		2869	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	1024 B	809 B	494000... 293000...				7/12/2007 7:13...	7/2/2008 5:04...	7/12/2007 7:1...
Chapter1.htm		2867	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	39,01 KB	39,00 KB	8a11b... c54e55...				7/12/2007 7:15...	7/2/2008 5:04...	7/12/2007 7:1...
code[1].htm		2857	htm	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/back/Webs/Mantooth/AppData/Local/Microsoft/Windows/Temporary Internet File... HTML	6556 B	6382 B	d42360... 8897a5...				7/12/2007 7:12...	7/2/2008 5:04...	7/12/2007 7:1...

Question 8: Go to File Category > Multimedia > Video > MPEG 2.0 Video, watch happy.mpeg, what can you tell from the video?

This video showcases the frustration of the guy handling the computer. It may be because of some software not being able to work properly, or somebody may have intentionally created this for him. The last reason he may be in a lot of blood pressure made him go mad for errors, bugs, or not handling the stress properly.

Question 9. Go to File Category > OS/File system Files > Windows NT Registry, what is the file path of Wes Mantooth's NTUSER.DAT? Explain what a NTUSER.DAT file is.

Path in screenshot below

Name	Label	Item #	Ext	Path
NTUSER.DAT		1662	dat	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Dracula/NTUSER.DAT
NTUSER.DAT		1779	dat	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/WesMantooth/NTUSER.DAT
DEFAULT.SAV		1199	sav	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/DEFAULT.SAV
SAM		1198	<missin...	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/SAM
SECURITY		1195	<missin...	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/SECURITY
SOFTWARE		1192	<missin...	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/SOFTWARE
SYSTEM		1189	<missin...	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/SYSTEM

This NTUSER.DAT file is a hive file which has all the user-specific configuration settings and preferences of the WES MANTOOOTH in this case. It also has lot of variables stored like environment variables, network configuration and personalized settings etc.

Question 10: List interesting results you found from TypedURLs, RecentDocs, and UserAssist. If you identified any other data from ntuser.dat, please also list here.

Name	Type	Data
thisisatest	REG_SZ	thisisatest
start c:\windows\explorer.exe:keylog...	REG_SZ	start c:\windows\explorer.exe:keylogger.exe

Properties

Written Time: 4/14/2007 0:12:14 UTC

I found a keylogger on this machine.

00	73 00 74 00 61 00 72 00-74 00 20 00 63 00 3A 00	s-t-a-r-t- -c-:-
10	5C 00 77 00 69 00 6E 00-64 00 6F 00 77 00 73 00	\w-i-n-d-o-w-s-
20	5C 00 65 00 78 00 70 00-6C 00 6F 00 72 00 65 00	\e-x-p-l-o-r-e-
30	72 00 2E 00 65 00 78 00-65 00 3A 00 6B 00 65 00	r- -e-x-e-: -k-e-
40	79 00 6C 00 6F 00 67 00-67 00 65 00 72 00 2E 00	y-l-o-g-g-e-r...-
50	65 00 78 00 65 00	e-x-e-

Name	Type	Data
Default Attributes	REG_DWORD	0x00000200 (512)
Use Existing	REG_DWORD	0x00000000 (0)
Set As Default	REG_DWORD	0x00000001 (1)
Driver Name	REG_SZ	Epson Stylus Photo RX420 (M)
Shared	REG_DWORD	0x00000001 (1)
Auto Install	REG_DWORD	0x00000001 (1)
Locate Type	REG_DWORD	0x00000001 (1)

Driver used here is Epson Stylus Photo RX420 (Photo Printer)

Name	Type	Data
RemotePath	REG_SZ	\mediacenter\My Internet Clearing Folder
UserName	REG_SZ	(value not set)
ProviderName	REG_SZ	Microsoft Windows Network
ProviderType	REG_DWORD	0x00020000 (131072)
ConnectionType	REG_DWORD	0x00000001 (1)
DeferFlags	REG_DWORD	0x00000004 (4)

I searched what this clearing folder is and it said that other can access this folder.

Software

- Microsoft
 - Internet Explorer
 - Security
 - AntiPhishing
 - B3BB5BBA-E7D5-40AB-A041-...
 - Smart Screen DAT file

zZilla

Providers

aSoft

ico

taa

icromedia

crossoft

me	6/21/2007 18:02:26 UTC	A5 02 49 C0 12 65 86 25-00 00 00 00 54 00 00 00	À·IÀ·e·%...·T...
		30 41 00 6E 00 74 00 69 00-50 00 68 00 69 00 73 00	À-n-t-i·P-h-i-s...
		40 68 00 69 00 6E 00 67 00-20 00 66 00 69 00 6C 00	h-i-n-g-·f-i-l-
		50 74 00 65 00 72 00 20 00-44 00 41 00 54 00 20 00	t-e-r- ·D-A-T- ·
		60 66 00 69 00 6C 00 65 00-20 00 76 00 65 00 72 00	f-i-l-e-·v-e-r-
		70 69 00 66 00 69 00 63 00-61 00 74 00 69 00 6F 00	i-f-i-c-a-t-i-o-
		80 6E 00 00 00 03 66 00 00-A8 00 00 00 10 00 00 00	n-...f-..."-.....
		90 2B 58 12 82 2E 56 7B 0E-D1 62 A1 72 79 6F B9 0A	+X-·.V(·Ñ;ryo!
		a0 00 00 00 00 04 80 00 00-A0 00 00 00 10 00 00 00

AntiPhishing folder found.

AccessData Registry Viewer - [NTUSER.DAT(1779).tmp]

File Edit Report View Window Help

LowRegistry	Name	Type	Data
Main	url1	REG_SZ	http://www.tucows.com/
Media	url2	REG_SZ	http://www.tigerdirect.com/
MenuExt	url3	REG_SZ	http://www.newegg.com/
New Windows	url4	REG_SZ	http://www.altavista.com/
PageSetup	url5	REG_SZ	http://www.mamma.com/
PhishingFilter	url6	REG_SZ	http://www.google.com/
SearchScopes	url7	REG_SZ	http://www.google.com/
SearchUrl	url8	REG_SZ	http://www.youtube.com/
Security	url9	REG_SZ	C:\Users\Wes Mantooth\Documents\Scripts
Services	url10	REG_SZ	\mediacenter
Settings	url11	REG_SZ	http://www.somethingcool.com/
Setup	url12	REG_SZ	www.accesdatarocks.com
TabbedBrowsing	url13	REG_SZ	http://www.marriott.com/
Toolbar	url14	REG_SZ	F:\Windows\System32\winevt
TypedURLs	url15	REG_SZ	http://www.united.com/
URLSearchHooks	url16	REG_SZ	http://www.gmail.com/

Key Properties

Last Written Time 2/12/2008 19:53:19 UTC

We found a Vista Mantooth Bitlocker Key.txt.lnk

99	REG_BINARY	57 00 4D 00 2E 00 74 00 6F 00 6F 00 74 00 68 00 00 00 5...
81	REG_BINARY	56 00 69 00 73 00 74 00 61 00 20 00 4D 00 61 00 6E 00 7...
71	REG_BINARY	57 00 65 00 73 00 20 00 4D 00 61 00 6E 00 74 00 6F 00 6...
75	REG_BINARY	64 00 65 00 66 00 61 00 75 00 6C 00 74 00 00 00 5A 00 ...
74	REG_BINARY	61 00 69 00 6D 00 2E 00 69 00 6E 00 69 00 00 00 5A 00 ...
98	REG_BINARY	79 00 61 00 68 00 6F 00 6F 00 2E 00 69 00 6E 00 69 00 0...
4	REG_BINARY	6D 00 73 00 6E 00 2E 00 69 00 6E 00 69 00 00 00 5A 00 ...
55	REG_BINARY	53 00 65 00 63 00 72 00 65 00 74 00 20 00 53 00 74 00 7...
15	REG_BINARY	66 00 75 00 6E 00 38 00 31 00 2E 00 6A 00 70 00 67 00 0...
32	REG_BINARY	46 00 75 00 6E 00 6E 00 79 00 20 00 56 00 69 00 64 00 7...
97	REG_BINARY	63 00 61 00 74 00 68 00 65 00 6C 00 6D 00 65 00 74 00 ...
96	REG_RINARV	4A 00 61 00 77 00 73 00 20 00 43 00 61 00 74 00 2F 00 6
00	56 00 69 00 73 00 74 00-61 00 20 00 4D 00 61 00	V-i-s-t-a- -M-a-
10	6E 00 74 00 6F 00 6F 00-74 00 68 00 20 00 42 00	n-t-o-o-t-h- -B-
20	69 00 74 00 6C 00 6F 00-63 00 6B 00 65 00 72 00	i-t-l-o-c-k-e-r-
30	20 00 4B 00 65 00 79 00-20 00 31 00 2E 00 34 00	-K-e-y- -l- -4-
40	2E 00 74 00 78 00 74 00-00 00 B2 00 32 00 00 00	.t-x-t- -z-2--
50	00 00 00 00 00 00 00 00-00-56 69 73 74 61 20 4D 61Vista Ma
60	6E 74 6F 74 68 20 42-69 74 6C 6F 63 6B 65 72	ntooth Bitlocker
70	20 4B 65 79 20 31 2E 34-2E 74 78 74 2E 6C 6E 6B	Key 1.4.txt.lnk
80	00 00 7A 00 07 00 04 00-00-EF BE 00 00 00 00 00 00	--z-----i%-----

Secret Stuff.lnk

55	REG_BINARY	53 00 65 00 63 00 72 00 65 00 74 00 20 00 53 00 74 00 7...
15	REG_BINARY	66 00 75 00 6E 00 38 00 31 00 2E 00 6A 00 70 00 67 00 0...
32	REG_BINARY	46 00 75 00 6E 00 6E 00 79 00 20 00 56 00 69 00 64 00 7...
97	REG_BINARY	63 00 61 00 74 00 68 00 65 00 6C 00 6D 00 65 00 74 00 ...
96	REG_RINARV	4A 00 61 00 77 00 73 00 20 00 43 00 61 00 74 00 2F 00 6
00	53 00 65 00 63 00 72 00-65 00 74 00 20 00 53 00	S-e-c-r-e-t- -S-
10	74 00 75 00 66 00 66 00-00 00 6A 00 32 00 00 00	t-u-f-f- -j-2--
20	00 00 00 00 00 00 00 00-00-53 65 63 72 65 74 20 53Secret S
30	74 75 66 66 2E 6C 6E 6B-00 00 4A 00 07 00 04 00	tuff.lnk- -J-----
40	EF BE 00 00 00 00 00 00-00-00 26 00 00 00 00 00 00	i%-----&-----
50	00 00 00 00 00 00 00 00-00-00 00 00 00 00 00 00 00	-----
60	53 00 65 00 63 00 72 00-65 00 74 00 20 00 53 00	S-e-c-r-e-t- -S-
70	74 00 75 00 66 00 66 00-2E 00 6C 00 6E 00 6B 00	t-u-f-f- -l-n-k-
80	00 00 00 00 00 00 00 00	-----
54	REG_BINARY	75 00 73 00 65 00 6C 00 65 00 73 00 5F 00 63 00 61 00 7...
10	REG_BINARY	63 00 6C 00 65 00 61 00 6E 00 2D 00 64 00 61 00 7A 00 ...
6	REG_RINARV	4D 00 79 00 20 00 49 00 6F 00 74 00 65 00 72 00 6F 00 6
00	75 00 73 00 65 00 6C 00-65 00 73 00 5F 00 63 00	u-s-e-l-e-s- -c-
10	61 00 74 00 2E 00 6A 00-70 00 67 00 00 00 70 00	a-t- -j-p-g- -p-
20	32 00 00 00 00 00 00 00-00-00 00 00 00 75 73 65 6C	2-----useL
30	65 73 5F 63 61 74 2E 6A-70 67 2E 6C 6E 6B 00 00	es_cat.jpg.lnk--
40	4E 00 07 00 04 00 EF BE-00 00 00 00 00 00 00 00 00	N-----i%-----
50	26 00 00 00 00 00 00 00-00-00 00 00 00 00 00 00 00 00	&-----
60	00 00 00 00 00 00 00 00-75 00-73 00 65 00 6C 00 65 00	-----u-s-e-l-e-

0x 10	REG_BINARY	00 00 00 00 00 01 00 00 00 2D 00 04 00 01 00 7A 00 ...
0x 6	REG_BINARY	4D 00 79 00 20 00 49 00 6E 00 74 00 65 00 72 00 6E 00 6...
0x 95	REG_BINARY	57 00 41 00 53 00 48 00 45 00 52 00 20 00 28 00 46 00 3...
0x 9	REG_BINARY	4E 00 65 00 77 00 20 00 54 00 65 00 78 00 74 00 20 00 4...
0x 31	REG_BINARY	4D 00 69 00 73 00 63 00 20 00 44 00 6F 00 63 00 73 00 0...
0x 30	REG_BINARY	59 00 6F 00 75 00 20 00 47 00 6F 00 74 00 20 00 69 00 7...
0x 94	REG_BINARY	73 00 65 00 63 00 75 00 72 00 69 00 74 00 79 00 65 00 7...
0x 1	REG_BINARY	74 00 65 00 73 00 74 00 65 00 76 00 74 00 2F 00 65 00 7...
00 57 00 41 00 53 00 48 00-45 00 52 00 20 00 28 00	W-A-S-H-E-R- -(-	
10 46 00 3A 00 29 00 00 00-64 00 32 00 00 00 00 00	F-:-)---d-2-----	
20 00 00 00 00 00 00 00 57 41-53 48 45 52 20 28 46 29WASHER (F)	
30 2E 6C 6E 6B 00 00 46 00-07 00 04 00 EF BE 00 00	.lnk--F----i%--	
40 00 00 00 00 00 00 26 00-00 00 00 00 00 00 00 00g-----	
50 00 00 00 00 00 00 00 00 00-00 00 00 00 57 00 41 00W-A-	
60 53 00 48 00 45 00 52 00-20 00 28 00 46 00 29 00	S-H-E-R- -(-F-) -	
70 2E 00 6C 00 6E 00 6B 00-00 00 1E 00 00 00	..-l-n-k-----	

I feel John Stuff has important details to it.

0x 23	REG_BINARY	44 00 65 00 61 00 12 00 20 00 6F 00 6C 00 65 00 20 00 4
00 4A 00 6F 00 68 00 6E 00-73 00 20 00 53 00 74 00	J-o-h-n-s- -S-t-	
10 75 00 66 00 66 00 20 00-28 00 5C 00 5C 00 54 00	u-f-f- -(\-\-\T-	
20 52 00 41 00 49 00 4E 00-49 00 4E 00 47 00 2D 00	R-A-I-N-I-N-G--	
30 4B 00 45 00 4E 00 29 00-00 00 94 00 32 00 00 00	K-E-N-)-----2---	
40 00 00 00 00 00 00 00 00-4A 6F 68 6E 73 20 53 74Johns St	
50 75 66 66 20 28 54 52 41-49 4E 49 4E 47 2D 4B 45	uff (TRAINING-KE	
60 4E 29 2E 6C 6E 6B 00 00-66 00 07 00 04 00 EF BE	N).lnk--f----i%	
70 00 00 00 00 00 00 00 00-26 00 00 00 00 00 00 00&-----	
80 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 4A 00J-	

0x 89	REG_BINARY	4A 00 75 00 6E 00 63 00 74 00 69 00 6F 00 6E 00 20 00 7...
0x 36	REG_BINARY	48 00 6F 00 77 00 20 00 74 00 6F 00 20 00 63 00 72 00 6...
0x 14	REG_BINARY	46 00 61 00 6D 00 69 00 6C 00 79 00 20 00 50 00 69 00 ...
0x 23	REG_BINARY	44 00 65 00 61 00 72 00 20 00 6F 00 6C 00 65 00 20 00 4
040 53 00 20 00 6A 00 75 00-6E 00 63 00 74 00 69 00	S- -j-u-n-c-t-i-	
050 6F 00 6E 00 20 00 70 00-6F 00 69 00 6E 00 74 00	o-n- -p-o-i-n-t-	
060 73 00 2E 00 6D 00 68 00-74 00 00 00 E4 00 32 00	s- -m-h-t- -ä-2-	
070 00 00 00 00 00 00 00 00-00 00 48 6F 77 20 74 6FHow to	
080 20 63 72 65 61 74 65 20-61 6E 64 20 6D 61 6E 69	create and mani	
090 70 75 6C 61 74 65 20 4E-54 46 53 20 6A 75 6E 63	pulate NTFS junc	
0a0 74 69 6F 6E 20 70 6F 69-6E 74 73 2E 6D 68 74 2E	tion points.mht.	
0b0 6C 6E 6B 00 9C 00 07 00-04 00 EF BE 00 00 00 00	lnk-----i%	
0c0 00 00 00 00 26 00 00 00-00 00 00 00 00 00 00 00&-----	

0x 62	REG_BINARY	42 00 75 00 73 00 69 00 6E 00 65 00 73 00 73 00 20 00 4...
0x 65	REG_BINARY	41 00 54 00 4D 00 5F 00-54 00 48 00 45 00 46 00 54 00 5...
0x 64	REG_BINARY	43 00 61 00 6D 00 65 00 72 00 61 00 2F 00 62 00 6D 00
00 41 00 54 00 4D 00 5F 00-54 00 48 00 45 00 46 00	A-T-M- _-T-H-E-F-	
10 54 00 53 00 31 00 2E 00-70 00 70 00 74 00 00 00	T-S-1- .p-p-t---	
20 72 00 32 00 00 00 00 00-00 00 00 00 00 00 41 54	r-2-----AT	
30 4D 5F 54 48 45 46 54 53-31 2E 70 70 74 2E 6C 6E	M_THEFTS1.ppt.ln	
40 6B 00 50 00 07 00 04 00-00 EF BE 00 00 00 00 00 00	k-P-----i%	
50 00 00 26 00 00 00 00 00-00 00 00 00 00 00 00 00 00&-----	
60 00 00 00 00 00 00 00 00-00 41 00 54 00 4D 00 5F 00A-T-M- _-	

49	REG_BINARY	53 00 75 00 70 00 65 00 72 00 20 00 53 00 65 00 63 00 7...
8	REG_BINARY	53 00 75 00 70 00 65 00 72 00 20 00 53 00 65 00 63 00 7...
48	REG_BINARY	61 00 72 00 5F 00 74 00 65 00 73 00 74 00 5F 00 46 06 4...
47	REG_BINARY	72 00 75 00 73 00 73 00 5F 00 34 00 5F 00 4F 04 49 04 3
00	53 00 75 00 70 00 65 00-72 00 20 00 53 00 65 00 S-u-p-e-r- -S-e-	
10	63 00 72 00 65 00 74 00-20 00 53 00 74 00 75 00 c-r-e-t- -S-t-u-	
20	66 00 66 00 00 00 7C 00-32 00 00 00 00 00 00 00 f-f--- -2-----	
30	00 00 00 00 53 75 70 65-72 20 53 65 63 72 65 74 ---Super Secret	
40	20 53 74 75 66 66 2E 6C-6E 6B 00 00 56 00 07 00 Stuff.lnk-V---	
50	04 00 EF BE 00 00 00 00-00 00 00 00 26 00 00 00 ..-i%-----&---	
60	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..-----	
70	00 00 53 00 75 00 70 00-65 00 72 00 20 00 53 00 --S-u-p-e-r- -S-	
80	65 00 63 00 72 00 65 00-74 00 20 00 53 00 74 00 e-c-m-e-t- -S+.	

Lot of Cat images images and lot of secret stuff found here.

Question 11: Examine the information listed under **File Status** to find out where FTK categorizes the files whose extension does not match the file type identified in the file header. List 2 Bad Extension files.

Case Overview

File Category (2,360 / 2,360)

File Status

- Bad Extensions (126 / 126)
 - Data Carved Files (0 / 0)
 - Decrypted Files (0 / 0)
 - Deleted Files (78 / 78)
 - Duplicate Items (0 / 0)
 - Email Attachments (135 / 135)
 - Email Related Items (From Email) (249 / 249)
 - Encrypted Files (10 / 10)
 - Flagged Ignore (0 / 0)
 - Flagged Privileged (0 / 0)
 - From Recycle Bin (81 / 81)
 - KFF Alert Files (0 / 0)
 - KFF Ignorable (0 / 0)
 - OCR Graphics (0 / 0)
 - OLE Subitems (0 / 0)

File Content

Hex Text Filtered Natural



File Content Properties Hex Interpreter

Normal

Display Time Zone: Eastern Daylight Time (From local machine)

Name	Label	Item #	Ext	Path
account{0AC3F95A-684...		2170	oearco...	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows Mail/account{0AC3F95
account{D0C529A8-937...		2169	oearco...	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows Mail/account{D0C529A
WindowsMail.MSMessag...		2459	<missin...	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows Mail/Backup/new/Wind
account{1E352AFE-A50...		2165	oearco...	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows Mail/Local Folders/acco
account{37A2BDE9-A4...		2164	oearco...	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows Mail/Local Folders/acco
atm.bmp		1350	bmp	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows Mail/Local Folders/lnbc
index.dat		2269	dat	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows/History/History.IE5/MS
DocumentDotWrite[1].js		3083	js	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows/Temporary Internet Fil

File Category (2,360 / 2,360)										
File Status										
<input checked="" type="checkbox"/> Bad Extensions (126 / 126)										
<input type="checkbox"/> Data Carved Files (0 / 0)										
<input type="checkbox"/> Decrypted Files (0 / 0)										
<input checked="" type="checkbox"/> Deleted Files (78 / 78)										
<input type="checkbox"/> Duplicate Items (0 / 0)										
<input checked="" type="checkbox"/> Email Attachments (135 / 135)										
<input type="checkbox"/> Email Related Items (From Email) (249 / 249)										
<input type="checkbox"/> Encrypted Files (10 / 10)										
<input type="checkbox"/> Flagged										
<input type="checkbox"/> Flagged Privileged (0 / 0)										
<input type="checkbox"/> From Recycle Bin (81 / 81)										
<input type="checkbox"/> KFF Alert Files (0 / 0)										
<input type="checkbox"/> KFF Ignorable (0 / 0)										
<input type="checkbox"/> OCR Graphics (9 / 9)										
<input type="checkbox"/> OLE Subitems (0 / 0)										

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed	Modified
toc-msswin_xp\bcmo...		2691	4	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	ASCII 7	4096 B	3949 B	fc304f...	1fa1ab...	6/23/2007 8:22...	7/2/2008 5:08...	6/23/2007 8:22...	
us.dsd[1].htm		2834	htm	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	ASCII 7	10.00 KB	10.00 KB	52b4e...	0ee31a...	4/17/2007 5:36...	7/2/2008 5:03...	4/17/2007 5:36...	
us_i04_200604_07_to...		2700	gif	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	ASCII 7	17.00 KB	16.96 KB	7e69ba...	a21216...	6/23/2007 8:22...	6/23/2007 8:22...	6/23/2007 8:22...	
UH[1].js		2810	js	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	ASCII 7	2048 B	2031 B	1acdbd...	0435fe...	6/23/2007 8:23...	6/23/2007 8:23...	6/23/2007 8:23...	
xpo_ar_dr[1].gif		2829	gif	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	ASCII 7	80 B	77 B	25d2a3...	989882...	4/17/2007 5:36...	4/17/2007 5:36...	4/17/2007 5:36...	
drive_neu[1].js		2862	js	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	7 bit text	3072 B	2758 B	a5f161...	899451...	7/12/2007 7:16...	7/12/2007 7:16...	7/12/2007 7:16...	
Y1[1].js		2861	js	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	7 bit text	96 B	96 B	941f25...	941f25...	7/12/2007 7:16...	7/12/2007 7:16...	7/12/2007 7:16...	
linkage[1].js		2736	ad	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	7 bit text	2048 B	1566 B	9e1fb9...	630844...	7/12/2007 7:16...	7/12/2007 7:16...	7/12/2007 7:16...	
us_p[1].htm		2734	htm	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	7 bit text	1536 B	1418 B	8c3b16...	989834...	7/12/2007 7:16...	7/12/2007 7:16...	7/12/2007 7:16...	
secure2[1].gif		2728	gif	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	JPEG	2048 B	1792 B	e83791...	821244...	7/12/2007 7:16...	7/12/2007 7:16...	7/12/2007 7:16...	
text_group[1].htm		2715	htm	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	7 bit text	1024 B	965 B	887b4...	101d48...	7/12/2007 7:16...	7/2/2008 5:06...	7/12/2007 7:16...	
text_group[2].htm		2714	htm	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	7 bit text	4608 B	4243 B	dd789...	93e32...	7/12/2007 7:16...	7/2/2008 5:06...	7/12/2007 7:16...	
feed4\data		3151	data	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	HTML	29.00 KB	28.83 KB	943b15...	694862...	2/27/2007 3:42...	2/27/2007 3:42...	2/27/2007 3:42...	
us_p.c\data		2999	data	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	HTML	41.00 KB	40.65 KB	77ae7...	96d9c9...	2/27/2007 3:42...	2/27/2007 3:42...	2/27/2007 3:42...	

Loaded: 126 Filtered: 126 Highlighted: 1 Checked: 0 Total Lsize: 3852 KB

Question 12: Check the number of Data Carved Files from File Status, what is the number?

File Category (2,360 / 2,360)										
File Status										
<input checked="" type="checkbox"/> Bad Extensions (126 / 126)										
<input type="checkbox"/> Data Carved Files (0 / 0)										
<input type="checkbox"/> Decrypted Files (0 / 0)										
<input checked="" type="checkbox"/> Deleted Files (78 / 78)										
<input type="checkbox"/> Duplicate Items (0 / 0)										
<input checked="" type="checkbox"/> Email Attachments (135 / 135)										

Initially Carved Files amount is 0.

Question 13: Check the number of Data Carved Files again, have you carved out some files? Provide a screenshot.

Case Overview										
File Status										
<input checked="" type="checkbox"/> Bad Extensions (126 / 126)										
<input type="checkbox"/> Data Carved Files (0 / 0)										
<input type="checkbox"/> Decrypted Files (0 / 0)										
<input checked="" type="checkbox"/> Deleted Files (78 / 78)										
<input type="checkbox"/> Duplicate Items (0 / 0)										
<input checked="" type="checkbox"/> Email Attachments (135 / 135)										
<input type="checkbox"/> Email Related Items (From Email) (250 / 250)										
<input type="checkbox"/> Encrypted Files (10 / 10)										
<input type="checkbox"/> Flagged										
<input type="checkbox"/> Flagged Privileged (0 / 0)										
<input type="checkbox"/> From Recycle Bin (81 / 81)										
<input type="checkbox"/> KFF Alert Files (0 / 0)										
<input type="checkbox"/> KFF Ignorable (0 / 0)										
<input type="checkbox"/> OCR Graphics (9 / 9)										
<input type="checkbox"/> OLE Subitems (0 / 0)										

File Content

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MDS	SHA1	SHA256	Created	Accessed
Carved[0].jpeg		10073	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[unallocated space]\062746\Carved[0].jpeg	JPEG	n/a	25.87 KB				n/a	n/a
Carved[0].htm		10072	htm	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[unallocated space]\069191\Carved[0].htm	JPEG	n/a	68.34 KB				n/a	n/a
Carved[0].jpg		10039	jpg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[unallocated space]\176970\Carved[0].jpg	JPEG	n/a	17.97 KB				n/a	n/a
Carved[1033624].jpeg		10054	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\#HTTP-Carved\[1033624].jpeg	JPEG	n/a	297 B				n/a	n/a
Carved[1036696].jpeg		10055	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\#HTTP-Carved\[1036696].jpeg	JPEG	n/a	570 B				n/a	n/a
Carved[1037720].jpeg		10056	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\#HTTP-Carved\[1037720].jpeg	JPEG	n/a	309 B				n/a	n/a
Carved[1039788].jpeg		10057	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\#HTTP-Carved\[1039788].jpeg	JPEG	n/a	307 B				n/a	n/a
Carved[1040792].jpeg		10058	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\#HTTP-Carved\[1040792].jpeg	JPEG	n/a	454 B				n/a	n/a
Carved[1041816].jpeg		10059	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\#HTTP-Carved\[1041816].jpeg	JPEG	n/a	306 B				n/a	n/a
Carved[121915].jpeg		10060	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet File...	JPEG	n/a	884 B				n/a	n/a
Carved[1257749].jpeg		10061	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\#HTTP-Carved\[1257749].jpeg	JPEG	n/a	28.51 KB				n/a	n/a
Carved[1258940].jpeg		10062	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\#HTTP-Carved\[1258940].jpeg	JPEG	n/a	455 B				n/a	n/a
Carved[1265048].jpeg		10063	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\#HTTP-Carved\[1265048].jpeg	JPEG	n/a	360 B				n/a	n/a
Carved[1267095].jpeg		10064	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\#HTTP-Carved\[1267095].jpeg	JPEG	n/a	371 B				n/a	n/a
Carved[1270168].jpeg		10064	jpeg	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\root\#HTTP-Carved\[1270168].jpeg	JPEG	n/a	306 B				n/a	n/a

Yes, I carved out 73 jpeg images which may be crucial for our evidence.

Question 14: What interesting files do you find by performing data carving process (if you did not find any pertinent information, that is fine)? Why is this process so important?

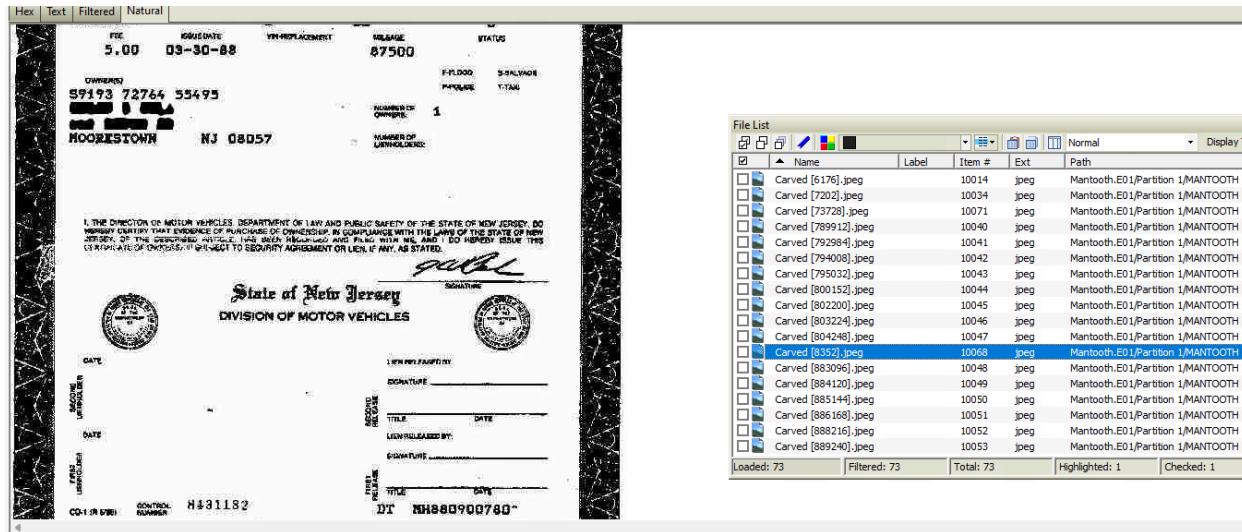


File Content

Hex Text Filtered Natural

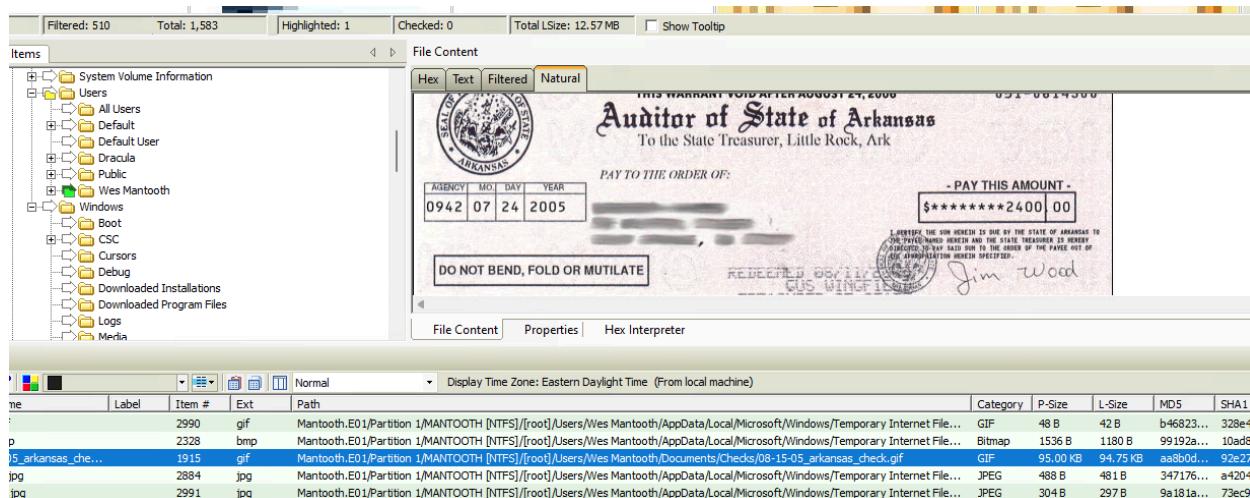
Name	Label	Item #	Ext	Path
Carved [1270168].jpeg		10064	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/.gmft
Carved [1406].jpeg		10025	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/.grec
Carved [1430].jpeg		10023	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/.grc
Carved [1452].jpeg		10013	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/.grc
Carved [1485224].jpeg		10065	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/.gmft
Carved [1713].jpeg		10033	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/Users
Carved [27152].jpeg		10067	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/unallocated
Carved [2494].jpeg		10027	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/Users
Carved [262].jpeg		10030	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/Users
Carved [3121].jpeg		10004	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/.grc
Carved [3194].jpeg		10006	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/.grc
Carved [324].jpeg		10001	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/Users
Carved [3251].jpeg		10018	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/.grc
Carved [326208].jpeg		10069	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/page
Carved [332].jpeg		10011	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/.grc
Carved [332].jpeg		10017	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/.grc
Carved [332].jpeg		10019	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/.grc
Carved [332].jpeg		10015	.jpeg	Mantooth.E01/partition 1/MANTOOOTH (NTFS)/root/.grc

Hex Text Filtered Natural



Data Carving is important because it extracts the deleted, fragmented and lost files along with their timelines which is very important for finding out crimes as for the forensics in concern.

Question 15. Find one bank check image and bookmark it in Mantooth bookmark. What is the name of this image?



We found the check successfully and name we found on it is signed by "Jim Wood"

Question 16: How many files contain “atm”, and how many hits of “atm” in total?

I got 107 hits in 15 files :

The screenshot shows a search interface with the following details:

Search Criteria:

- Operators: Or
- Terms: All
- Accumulate Results: Checked

Search Terms:

Search Term	Total Hits
Or	0
And	0
atm	107

Index Search Results:

Detailed list of hits (partial list shown):

- 100% - 34 hit(s) -- Item 3115 [atmcamera[1].htm] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\DSUTLPS6\atmcamera[1].htm
- Hit #1: nds Reference Pages: ATM Camera robots INDEX.HDF
- Hit #2: Photographs show an ATM equipped by scanners with
- Hit #3: nd wireless camera. ATM, ATM card, PIN, camera, scam,
- Hit #4: reless camera. ATM, ATM card, PIN, camera, scam,
- Hit #5: ms --> ATM Scans --> ATM Camera
- Hit #6: ms --> ATM Scans --> ATM Camera - ATM Camera
- Hit #7: ms --> ATM Camera --> ATM Camera
- Hit #8: ms --> ATM Camera --> ATM Camera
- Hit #9: Photographs show an ATM equipped by scanners with
- Hit #10: ns to steal both the ATM card number and the PIN.
- Hit #11: on the front of the ATM (see photos). If you see
- Hit #12: this, do not use the ATM and report it immediately
- Hit #13: on the front of the ATM. The equipment used t
- Hit #14: used to capture your ATM card number and PIN is d
- Hit #15: front of the normal ATM card slot that reads the
- Hit #16: slot that reads the ATM card number and transmits
- Hit #17: n a position to view ATM PIN entries. The the
- Hit #18: rectly from the bank ATM Ordinary-looking
- Hit #19: Ordinary-looking ATM? A false card
- Hit #20: ated Teller Machine (ATM) a few decades ago, banks
- Hit #21: in the collection of ATM card numbers and PINs for
- Hit #22: up to the ATM and copy them and then them out
- Hit #23: to steal the original ATM cards, then use them
- Hit #24: information from the ATM's display screen and keyboard
- Hit #25: be attached to an ATM machine to record data fr
- Hit #26: to the side of the ATM and disguised as an infor
- Hit #27: sponser for NCR, the ATM giant who produced the
- Hit #28: up to the top of the ATM case, a source said. Th
- Hit #29: best defense is for ATM owners to remain caud
- Hit #30: ATM cameras are installed in ATM for aler
- Hit #31: end information - ATM Fraud: Banking on Your Me
- Hit #32: www.snoops.com/fraud.htm/atmcamera.asp Urban Le
- Hit #33: Lo, Clifton "ATM Cameras Found by Chance."
- Hit #34: Police Accuse Man of ATM Scheme." The Detroit

The screenshot shows a detailed search results list with the following details:

Index Search Results:

dsSearch@ Indexed Search (Prefilter:(all files) Query:(“Or and And and atm”)) (ID:1) -- 107 hit(s) in 15 file(s)

Allocated Space: 107 hit(s) in 15 file(s)

Documents: 69 hit(s) in 7 file(s)

- Documents - files 1-7 -- 69 hit(s) in 7 file(s)
 - 100% - 34 hit(s) -- Item 3115 [atmcamera[1].htm] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\DSUTLPS6\atmcamera[1].htm
 - 71% - 24 hit(s) -- Item 2785 [search[1].htm] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\X0Y3MEC\search[1].htm
 - 17% - 5 hit(s) -- Item 2750 [images[1].htm] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\RMAJCPM1\images[1].htm
 - 8% - 2 hit(s) -- Item 2979 [ads[1].htm] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\X0Y3MEC\ads[1].htm
 - 8% - 2 hit(s) -- Item 2877 [ads[1].htm] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\RMAJCPM1\ads[1].htm
 - 5% - 1 hit(s) -- Item 1291 [How to Steal Cars.txt] Mantooth.E01\Partition 2\NONAME [Ext2]\[root]\Stuff\How to Steal Cars.txt
 - 5% - 1 hit(s) -- Item 3094 [atmcamera[1].htm] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\3J6Q2YX9\atmcamera[1].htm
- Presentations - 18 hit(s) in 2 file(s)
 - Presentations - files 1-2 -- 18 hit(s) in 2 file(s)
 - 28% - 9 hit(s) -- Item 3252 [ATM_THEFTS1.ppt] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox\337666D0-0000000A.eml/ATM_THEFTS1.ppt
 - 28% - 9 hit(s) -- Item 3351 [ATM_THEFTS1.ppt] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox\40A511AF-00000008.eml/ATM_THEFTS1.ppt
- Graphics - 1 hit(s) in 1 file(s)
 - Graphics - files 1-1 -- 1 hit(s) in 1 file(s)
 - 5% - 1 hit(s) -- Item 1350 [atm.bmp] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox\43467A94-00000010.eml/atm.bmp
- Email - 2 hit(s) in 1 file(s)
 - Email - files 1-1 -- 2 hit(s) in 1 file(s)
 - 8% - 2 hit(s) -- Item 2345 [42467A94-00000010.eml] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows Mail\Local Folders\Inbox\43467A94-00000010.eml
- Internet/Chat Files - 16 hit(s) in 3 file(s)
 - Internet/Chat Files - files 1-3 -- 16 hit(s) in 3 file(s)
 - 25% - 8 hit(s) -- Item 2494 [index.dat] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\Index.dat
 - 14% - 4 hit(s) -- Item 2373 [index.dat] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
 - 14% - 4 hit(s) -- Item 2500 [index.dat] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012007071220070713\index.dat
- Unknown Types - files 1-1 -- 1 hit(s) in 1 file(s)
 - Unknown Types - files 1-1 -- 1 hit(s) in 1 file(s)
 - 5% - 1 hit(s) -- Item 1020 [SMFT] Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\SMFT

Unallocated Space: 0 hit(s) in 0 file(s)

Question 17: Do you find any Visa numbers? list three Visa numbers along with the expiration date.

I got three visa numbers in this search

```
-----  
Pattern Query: /\<4\d\d\d[\-\.\ ](\d\d\d\d[\-\.\ ]){2}\d\d\d\d\>/ <ANSI, Case Insensitive> -- 3 hit(s) in 1 file(s)  
└ Allocated Space -- 3 hit(s) in 1 file(s)  
  └ 3 hit(s) -- Item 1012 [pagefile.sys] Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/pagefile.sys  
    └ Item 1012, Offset 55b43 (351043): visa <<4805-5555-1234-5566|>> Exp 10/09 4  
    └ Item 1012, Offset 55b62 (351074): Exp 10/09 <<4858.2545.5456.5555|>> Exp 6/09 44  
    └ Item 1012, Offset 55b80 (351104): 5 Exp 6/09 <<4454 5588 5124 2458|>> Exp 07/08  
└ Unallocated Space -- 0 hit(s) in 0 file(s)
```

File Content	
	Hex Text Filtered Natural
055b20	45 61 63 68 20 68 61 73-20 61 20 31 30 4B 20 6C Each has a 10K 1
055b30	69 6D 69 74 21 0D 0A 0D-0A 0D 0A 76 69 73 61 0D imit!.....visa-
055b40	0A 0D 0A 34 38 30 35 2D-35 35 35 35 2D 31 32 33 ...4805-5555-123
055b50	34 2D 35 35 36 36 20 45-78 70 20 31 30 2F 30 39 4-5566 Exp 10/09
055b60	0D 0A 34 38 35 38 2E 32-35 34 35 2E 35 34 35 36 ..4858.2545.5456
055b70	2E 35 35 35 35 20 45 78-70 20 36 2F 30 39 0D 0A .5555 Exp 6/09 ..
055b80	34 34 35 34 20 35 35 38-38 20 35 31 32 34 20 32 4454 5588 5124 2

Sel start = 351043, len = 19; clus = 209013; log sec = 209013; phy sec = 209076

File Content	
	Hex Text Filtered Natural
055b20	45 61 63 68 20 68 61 73-20 61 20 31 30 4B 20 6C Each has a 10K 1
055b30	69 6D 69 74 21 0D 0A 0D-0A 0D 0A 76 69 73 61 0D imit!.....visa-
055b40	0A 0D 0A 34 38 30 35 2D-35 35 35 35 2D 31 32 33 ...4805-5555-123
055b50	34 2D 35 35 36 36 20 45-78 70 20 31 30 2F 30 39 4-5566 Exp 10/09
055b60	0D 0A 34 38 35 38 2E 32-35 34 35 2E 35 34 35 36 ..4858.2545.5456
055b70	2E 35 35 35 35 20 45 78-70 20 36 2F 30 39 0D 0A .5555 Exp 6/09 ..
055b80	34 34 35 34 20 35 35 38-38 20 35 31 32 34 20 32 4454 5588 5124 2

Sel start = 351074, len = 19; clus = 209013; log sec = 209013; phy sec = 209076

Sel start = 351104, len = 19; clus = 209013; log sec = 209013; phy sec = 209076

File Content Properties Hex Interpreter

File List

Display Time Zone: Eastern Daylight Time (From local machine)

Hex	Text	Filtered	Natural
055b40	0A 0D 0A 34 38 30 35 2D-35 35 35 35 2D 31 32 33		... 4805-5555-123
055b50	34 2D 35 35 36 36 20 45-78 70 20 31 30 2F 30 39		4-5566 Exp 10/09
055b60	0D 0A 34 38 35 38 2E 32-35 34 35 2E 35 34 35 36		.4858.2545.5456
055b70	2E 35 35 35 35 20 45 78-70 20 36 2F 30 39 0D 0A		.5555 Exp 6/09..
055b80	34 34 35 34 20 35 35 38-38 20 35 31 32 34 20 32	4454 5588 5124 2	
055b90	34 35 38 20 45 78 70 20-30 37 2F 30 38 0D 0A 0D	458	Exp 07/08...
055ba0	0A 0D 0A 4D 61 73 74 65-72 63 61 72 64 0D 0A 0D		...Mastercard...

Question 18: What is the advantage of using indexed search vs. the live search?

I felt Index search was quick as it was searching based on the index “atm”, but the live search goes through the queuing process like data carving method and took time to carve out the information about the visa as uses brute force approach rather than matching the index. But live search is very useful in rigorous matching the file to take out the needed file, rather than grouping a lot of files in index search.

Question 19: Check emails in Senders and Recipients under the Display Name of “wes mantooth”, do you find any important information? If so, what kind of information have you got? Bookmark some important messages to support your final report.

Email Items

File List

Display Time Zone: Eastern Daylight Time (From local machine)

Subject	To	From	CC	BCC	Submit...	Deliver...	Unread	Unsent	Has Att...	Priority	Email	Created	Accessed	Modified	Item #	Category	Size	L
2003 Cigarette ...	<Sever...				8/14/2...				True		n/a	8/15/2007 2:11...	8/15/2007 2:10...	1288	Text In...	29.1 KB	2	
Hey Mom	20415132-0000...	<tooth...	"Wes M...		7/12/2...				True			8/14/2007 12:08...	7/12/2007 7:36...	2155	Text In...	110.5 KB	1	
Publish Your PG...	24200008-0000...	Sophie...	"RGP C...		4/13/2...	4/13/2...			False			8/14/2007 12:08...	4/14/2007 12:5...	2211	Text In...	17.0 KB	1	
Appointment (11/11)	20415132-0000...	John W...	"John W...		4/12/2...	4/12/2...			False			8/14/2007 12:08...	8/14/2007 12:08...	2212	Text In...	1.8 KB	2	
PGP Trial Softwa...	20PC1471-0000...	tralkey ...	"TrialSoft...		4/12/2...	4/12/2...			True			8/14/2007 12:08...	4/12/2007 7:00...	2254	Text In...	8794 B	8	
RBC-Offices	2A29541D-0000...	"Rasco ...	"Rasco ...		7/23/2...	7/23/2...			False			8/4/2007 12:08...	8/4/2007 12:08...	2453	Text In...	(4.00 KB)	1	
It's easy to swit...	2D652154-0000...	"Mr Smee...	"Mr Smee...		4/10/2...	4/10/2...			False			8/4/2007 12:08...	8/4/2007 12:08...	2209	Text In...	3584 B	3	
Welcome to Vil...	31D0562C-0000...	New ...	"Moros...		2/27/2...				False			8/4/2007 12:08...	8/4/2007 12:08...	2451	Text In...	24.00 KB	2	
Re: New Venture	33D98603-0000...	"Wes M...	"John ...		7/11/2...	7/11/2...			True			8/4/2007 12:08...	8/4/2007 12:08...	2349	Text In...	788.0 KB	7	

So three people were involved John Washer, Wes Mantooth and Rasco Badguy, initially and got help from Mr. Smee, also it goes like Rasco Badguy is a buddy for Mr. Smee who used this technique of stealing card many times. John Washer and Mantooth and Rasco mails has potential information which we can use to frame the information.

I noticed lot of emails with potential information and bookmarked it to Mantooth folder.

Question 20: What is an index.dat file? List some pertinent information from this file.

Index.dat file is a storage or a database for the internet explorer where it stores information about URLs, visited sites with appropriate times. Internet Explorer uses it to retrieve pages faster that are already been visited.

There are lot of potential URLs been recorded in this file and I listed the screenshot below, like visited URLs based on the word ATM and computer

URL	:2007071220070713: Wes Mantooth@file:///E:/Business Ideas/ATM_THEFTS1.ppt
file:	
user name:	
response:	
accessed time:	7/12/2007 7:29:42 PM -0400
modified time:	7/12/2007 1:29:42 PM -0400
expiration time:	8/7/2007 7:29:44 PM -0400
hits:	3
use counts:	0

URL	:2007071220070713: Wes Mantooth@file:///C:/Users/Wes Mantooth/Desktop/ATM_THEFTS1.ppt
file:	
user name:	
response:	
accessed time:	7/12/2007 7:28:14 PM -0400
modified time:	7/12/2007 1:28:14 PM -0400
expiration time:	8/7/2007 7:28:16 PM -0400
hits:	2
use counts:	0

URL	:2007071220070713: Wes Mantooth@file:///C:/Users/Wes Mantooth/Desktop/Ape_20shoot.gif
file:	
user name:	
response:	
accessed time:	7/12/2007 7:31:25 PM -0400
modified time:	7/12/2007 1:31:25 PM -0400
expiration time:	8/7/2007 7:24:18 PM -0400
hits:	2
use counts:	0

URL	Visited: Wes Mantooth@http://www.snopes.com/crime/warnings/atmcamera.asp
file:	
user name:	
response:	
accessed time:	7/12/2007 7:13:16 PM -0400
modified time:	7/12/2007 7:13:16 PM -0400
expiration time:	8/7/2007 7:13:18 PM -0400
hits:	1
use counts:	0

URL	Visited: Wes Mantooth@http://www.snopes.com/fraud/atm/atmcamera.asp
file:	
user name:	
response:	
accessed time:	7/12/2007 7:13:19 PM -0400
modified time:	7/12/2007 7:13:19 PM -0400
expiration time:	8/7/2007 7:13:20 PM -0400
hits:	1
use counts:	0

URL	Visited: Wes Mantooth@http://images.google.com/images?um=1&tab=wi&hl=en&q=atm card stealing
file:	
user name:	
response:	
accessed time:	7/12/2007 7:15:24 PM -0400
modified time:	7/12/2007 7:15:24 PM -0400
expiration time:	8/7/2007 7:15:26 PM -0400
hits:	1
use counts:	0

URL	Visited: Wes Mantooth@http://www.google.com/search?hl=en&q=atm+card+stealing&btnG=Google+Search
file:	
user name:	
response:	
accessed time:	7/12/2007 7:15:34 PM -0400
modified time:	7/12/2007 7:15:34 PM -0400
expiration time:	8/7/2007 7:15:36 PM -0400
hits:	3
use counts:	0

URL	Visited: Wes Mantooth@http://www.google.com/search?hl=en&q=I+am+searching+for+bad+stuff+on+Google&btnG=Google+Search
file:	
user name:	
response:	
accessed time:	8/5/2007 5:10:14 AM -0400
modified time:	8/5/2007 5:10:14 AM -0400
expiration time:	8/31/2007 5:10:16 AM -0400
hits:	7
use counts:	0

URL	:2007071220070713: Wes Mantooth@http://images.google.com/images?um=1&tab=wi&hl=en&q=atm card stealing
file:	
user name:	
response:	
accessed time:	7/12/2007 7:15:24 PM -0400
modified time:	7/12/2007 1:15:24 PM -0400
expiration time:	8/7/2007 7:15:26 PM -0400
hits:	1
use counts:	0

URL	:2007071220070713: Wes Mantooth@http://www.snopes.com/crime/warnings/atmcamera.asp
file:	
user name:	
response:	
accessed time:	7/12/2007 7:13:16 PM -0400
modified time:	7/12/2007 1:13:16 PM -0400
expiration time:	8/7/2007 7:13:18 PM -0400
hits:	1
use counts:	0

URL	:2007071220070713: Wes Mantooth@http://b.casalemedia.com/V2/44508/86958/index.html?www.snopes.com/fraud/atm/atmcamera.asp
file:	
user name:	
response:	
accessed time:	7/12/2007 7:15:00 PM -0400
modified time:	7/12/2007 1:15:00 PM -0400
expiration time:	8/7/2007 7:15:02 PM -0400
hits:	1
use counts:	0

Question 21: Choose two pieces of evidences (for example, Prefetch and SAM Users). Describe the information, and also explain why they are important for forensic investigation.

There are lot of important information were listed in this tab especially application prefetch and installed shows and give more information about the application ran by mantooth will us to know what's happened in his system for example he used BestCrypt to encrypt some of the files that is in the encrypted folder.

The screenshot shows the AccessData Forensic Toolkit interface. The title bar indicates Version: 6.2.0.1026 Database: localhost Case: Mantooth-FTK. The menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, and Help. The toolbar has a filter dropdown (-unfiltered -), Filter Manager, and other icons. The tabs at the top are Explore (selected), Overview, Email, Graphics, Video, Internet/Chat, Bookmarks, Live Search, Index Search, System Information, and Volatile. The left pane shows a tree view of the 'Disk Image' MANTOOOTH [NTFS] with categories: Applications (Installed, Prefetch, UserAssist), Browsers (URLs), Networks (Network Connections, Network Shares, Owner Information), Recent Files (NT User, Shortcuts (.LNK), SAM Users, Shell Bags). The right pane has sections for 'Items' and 'Provenance' (Mantooth.E01/Partition 1/MANTOOOTH [NTFS]). Below is a table of installed applications:

Name	File Path	Publisher	Install Date	Size (KB)	Version
Viewpoint Media Player					
TrueCrypt		TrueCrypt Foundation			
Trillian					
Adobe Flash Player 9 ActiveX					
VNC Free Edition 4.1.2	C:\Program Files\RealVNC\VNC4\	Adobe Systems RealVNC Ltd.	9 4.1.2		
QuickTime					
P2P Networking					
Mozilla Firefox (2.0.0.3)	C:\Program Files\Mozilla Firefox	Mozilla			2.0.0.3 (en-US)
FileZilla (remove only)					
BestCrypt 8.0					
AOL Uninstaller (Choose which Products to Remove)					
AIM 6					
WebEx		WebEx Communications, Inc			

Provenance

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			4F892A810F871B64DDC16B9322204E9	
	S-1-5-21-3166329-3263506726-1320359247-1002	Dracula			D90D8508030C90473114BD90EFF3FE9E	
	S-1-5-21-3166329-3263506726-1320359247-501	Guest				
	S-1-5-21-3166329-3263506726-1320359247-1003	Laurent				
	S-1-5-21-3166329-3263506726-1320359247-500	Administrator			31D6CFE0D16AE931B73C59D7E0C089C0	

Provenance

Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/SYSTEM
Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/SAM

For Sam we got the hash for the wes mantooth which can be used to crack his password and SAM and system are very important for password cracking so that we recover the password to decrypt the files those are encrypted by the mantooth.

Disk Image

MANTOOTH [NTFS]

File Path	Run Count	Last Run Time
\DEVICE\HARDISK\SYSTEM1\WINDOWS\EXPLORER.EXE	1	9/27/2007 7:16:51 AM
\DEVICE\HARDISK\SYSTEM1\WINDOWS\SYSTEM32\VCOPY.EXE	15	8/24/2007 8:47:34 AM
\DEVICE\HARDISK\SYSTEM1\WINDOWS\SYSTEM32\FSJU.EXE	68	9/27/2007 9:10:28 AM
\DEVICE\HARDISK\SYSTEM1\PROGRAM FILES\INTERNET EXPLORER\EXPLORE.EXE	56	8/24/2007 9:06:48 AM
\DEVICE\HARDISK\SYSTEM1\WINDOWS\SYSTEM32\DWIM.EXE	1	9/27/2007 7:16:51 AM
\DEVICE\HARDISK\SYSTEM1\PROGRAM FILES\INTERNET EXPLORER\IUSER.EXE	20	8/24/2007 9:06:49 AM
\DEVICE\HARDISK\SYSTEM1\WINDOWS\SYSTEM32\DRVINST.EXE	18	8/24/2007 6:08:27 AM
\DEVICE\HARDISK\SYSTEM1\PROGRAM FILES\ACCESSDATA\ACCESSDATA FTK IMAGER\FTK IMAGER.EXE	38	8/24/2007 8:45:01 AM
\DEVICE\HARDISK\SYSTEM1\WINDOWS\SYSTEM32\DLLHOST.EXE	1	9/27/2007 9:10:28 AM
\DEVICE\HARDISK\SYSTEM1\WINDOWS\SYSTEM32\DLLHOST.EXE	257	9/27/2007 9:10:28 AM
\DEVICE\HARDISK\SYSTEM1\WINDOWS\SYSTEM32\DLLHOST.EXE	238	9/27/2007 9:09:18 AM
\DEVICE\HARDISK\SYSTEM1\WINDOWS\SYSTEM32\DRGNFTS.EXE	57	9/27/2007 8:09:36 AM
\DEVICE\HARDISK\SYSTEM1\WINDOWS\SYSTEM32\DEFRAG.EXE	35	9/27/2007 8:09:36 AM

Provenance

Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Windows\Prefetch\FTK IMAGER.EXE-17AE1629.pf

Dracula	UEME_RUNPIDL:%csid 23%\Extras and Upgrades\Windows Ultimate Extras.lnk	19	3/5/2007 8:24:58 PM
Wes Mantooh	UEME_RUNPATH:C:\Windows\explorer.exe	1	2/12/2008 2:25:50 PM
Wes Mantooh	UEME_RUNPATH:C:\Windows\system32\defrag.exe	1	2/12/2008 2:21:39 PM
Wes Mantooh	UEME_RUNPATH:C:\Program Files\Windows Media Player\wmplayer.exe	2	2/12/2008 1:47:43 PM
Wes Mantooh	UEME_RUNPATH:C:\gdisk32.exe	1	2/12/2008 2:21:02 PM

Provenance

Mantooth.E01/Partition 1/MANTOOTH [NTFS]
--

DECRYPT ENCRYPTED FILES USING PRTK.

Question 22: What are the passwords for the “Those who owes.xls” file? Show a screenshot of your PRTK with the passwords.

View All			
Job Name	Attack Type	Status	Result
Those who owes	Microsoft Office 97/2000 Password Attack	Finished	*smack [HEX=48494a4...

Properties

Job Information

Attack Type: Microsoft Office 97/2000 Password Attack
Module: Microsoft Office Encryption Module
Profile: English
Status: Finished
Difficulty: Difficult
Begin Time: 4/02/24 13:18:51
End Time: 4/02/24 13:18:57
Timeout After: No Timeout
Decryptable: Yes
Result Type: Password
Results: *smack
Comments: ---

File Information

Filename: Those who owes.xls
Type: Excel
Version: 97/2000
Size: 13824
MD5: 655c3528129b43a3267c27f23507a3b3
SHA-1: cc5c3586d6555824c8f671cc4b2dd7e3ba43fb4
Created: Unknown
Modified: 7/12/07 18:58:45

The password we recovered is *smack

Part II. Attempt to recover Mantooth's logon password to recover EFS files.

Question 23: What is Mantooth's logon password? Show a screenshot of your PRTK with the password.

The screenshot shows a software interface for password recovery. On the left, a table lists a single job named 'SAM' with an attack type of 'Windows account: Wes Mantooth [NT hash]'. The status is 'Finished' and the result is 'tooth [HEX=0074006f...]' (partially visible). On the right, the 'Properties' window is open under the 'Job Information' tab. It contains detailed information about the attack, including the attack type ('Windows account: Wes Mantooth [NT hash]'), module ('SAM File Module'), profile ('English'), status ('Finished'), difficulty ('Difficult'), begin time ('4/02/24 13:31:39'), end time ('4/02/24 13:31:47'), and timeout after ('No Timeout'). The result type is 'Password' and the result value is 'tooth'. The 'File Information' tab is also visible, showing details like filename ('SAM'), type ('SAM password file'), version ('Unknown'), size ('262144'), MD5 ('6b089fd6f1a257076a8be2e369d7ef04'), SHA-1 ('9adfdc04767a0005eeff03a64e5e1289ed30f6c52'), creation date ('Unknown'), and modification date ('2/12/08 15:13:17').

Password is tooth

Part III. Attempt to decrypt files

Question 24: How many files you have decrypted? Show a screenshot of “Decrypted Files”. Include all decrypted files in your Mantooth bookmark.

I found total of 4 decrypted files.

The screenshot shows a file viewer interface with a preview pane displaying a one-million-dollar bill. The file list table shows four decrypted files:

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modif
C money plates[Decrypt..		11002	doc	Mantooth.ED1\Partition_1\MANTOOOTH [NTFS]\root\Users\Wes Mantooth\Documents\EFS DOCS\C money plates.doc-C money plates..	Microso...	76.50 KB	76.50 KB	8e0f11...	2ae7fc...		3/5/2007 9:14:...	3/5/2007 9:14:...	3/3/200
CC Name[Decrypted].xls	xls	11003	xls	Mantooth.ED1\Partition_1\MANTOOOTH [NTFS]\root\Users\Wes Mantooth\Documents\EFS DOCS\CC Name[Decrypted].xls	Excel 2...	18.00 KB	18.00 KB	7907c...	2522d...		3/5/2007 9:14:...	3/5/2007 9:14:...	7/14/2
John[Decrypted].doc	doc	11001	doc	Mantooth.ED1\Partition_1\MANTOOOTH [NTFS]\root\Users\Wes Mantooth\Documents\EFS DOCS\John.doc-John[Decrypted].doc	Microso...	23.50 KB	23.50 KB	81502d...	651dc...		3/5/2007 9:14:...	3/5/2007 9:14:...	3/5/200
Wes[Decrypted].doc	doc	11004	doc	Mantooth.ED1\Partition_1\MANTOOOTH [NTFS]\root\Users\Wes Mantooth\Documents\EFS DOCS\Wes.doc-Wes[Decrypted].doc	Microso...	23.50 KB	23.50 KB	daa6a4...	c490f3...		3/5/2007 9:14:...	3/5/2007 9:14:...	3/5/200

C money Plated.doc

Hex Text Filtered Natural

Doc

Here's the photos you wanted. I'd rather have the million but the 10s would do if I have enough 😊

Wes



File List

- Cm
- CC1
- John
- Wes

CC nums (Decrypted).xls

File Content

Hex Text Filtered Natural

	A	B	C	D	E	F	G	H
1	Credit Card Numbers	Name	Bank	Type	Exp	ID		
2	1234-1234-1234-1344	Red Skelton	BOA	Visa	9/10	123		
3	9877-1434-6543-2145	Jim Carrey	Wells Fargo	Visa	3/09	765		
4	37987-123458-13454	Buster Keaton	BOA	Amex	12/07			
5	123-123-123-1-2	Chris Rock		JC Penny	1/08			
6	6878-9876-9876-9876	Eddie Murphy	Bank of Panama	MC	4/09			
7	6789-2435-5464-6554	Robin Williams	Bank of American Forks	Visa	6/11	345		
8	543-345-567-1-1	Adam Sandler		Mervyns	9/11			
9								
10								
11								

John.doc

John
I've got to meet with you tomorrow to pass off the credit card number I got yesterday. We'll have to hurry on these because they'll be dropping off the radar as people complain they lost them.
See you at the fountain in front of the university at 1230.
Ps: Bring food

Wes.doc

Hex | Text | Filtered | Natural |
Wes:
I got this document from the bank on a war dialer attack.
Got lots of stuff but I'll have to wrap it up and send it to you encrypted so we don't have to worry about the cops ever reading it.
Doc

Step 3: Case Report (See FTK User Guide)

Question 25: Based on your investigation using FTK, provide your statement about this case regarding Wes Mantooth. Provide 3-5 evidence to support your statement.

We got lot of crucial information and evidences in this case, like emails, graphics, images, and documents and excel sheets. The crucial evidence I feel are listed below.

Initial Emails explains the conversion between John Washer, Rasco Badguy and Mantooth. We can get grasp that they involved in something which is dangerous as "venture". So we need to find what they could be involved by seeing Mantooth html files about what he is searching for.

From: "John Washer" <chkwasher@comcast.net>
Sent: 7/23/2007 1:59:09 PM -0400
To: txkidd@swbell.net
CC: Mantooth <dollarhyde86@comcast.net>
Subject: Stuff

Rasco,

I got your name from Wes. He says that you are the GOTO guy for the kinda stuff I am into.

:) DIDN'T YOU WES!

Anywaze... We should get together sometime and I can show you my "goods". I am getting pretty good at my trade.

In the meantime, we will keep our new relationship on the QT via Email.

Let me know if I can help you in any way with your ventures.

John

From: "Rasco Badguy" <txkidd@swbell.net>
Sent: 7/23/2007 2:27:11 PM -0400
To: Wes Mantooth <dollarhyde86@comcast.net>
Subject: RE: Stuff

Wes,

Hope John is as good as you say and we can trust him. If you say he is okay then I have to take your word for it. I have some cold ones on ice whenever you want to get together. I also have some stuff to move so let's get together soon.

From: "John Washer" <chkwasher@comcast.net>
Sent: 7/11/2007 4:27:15 PM -0400
To: Wes Mantooth <dollarhyde86@comcast.net>; Mr Smee <smee.rox@gmail.com>
Subject: Re: New Venture
Attachments: ATM_THEFTS1.ppt

Sweet!

If that turns out to be too risky, a bud of mine showed me how to rig the machines to keep the cards... Then we shoulder surf the pin and get the card when they leave!

He got this from a SPAM chainletter!

From: "Wes Mantooth" <dollarhyde86@comcast.net>
Sent: 7/12/2007 7:19:00 PM -0400
To: Mr Smee <smee.rox@gmail.com>
CC: John Washer <chkwasher@comcast.net>
Subject: New Venture
Attachments: Guts.bmp; Cover Plate.bmp; Camera.bmp

I am thinking we should launch into a new venture...

Take a look at this and tell me what you think. I can get the parts for about \$100.

Word

From: "Rasco Badguy" <txkidd@swbell.net>
Sent: 7/23/2007 5:26:10 PM -0400
To: John Washer <chkwasher@comcast.net>
CC: Wes Mantooth <dollarhyde86@comcast.net>
Subject: You will love this....
Attachments: How To Steal Credit Numbers.doc

This doc says it all guys.....ran across it and my buddy skimmerman used it a few times.....worked like a charm.....

From: "Rasco Badguy" <txkidd@swbell.net>
Sent: 7/24/2007 11:39:54 AM -0400
To: John Washer <chkwasher@comcast.net>
CC: Wes Mantooth <dollarhyde86@comcast.net>
Subject: Sweet Info
Attachments: News Report.doc

Guys,

I have attached a document with a news report on a big bust. Skimmerman knows some of these guys who went down. He is a little worried since he emailed them and traded some stuff. Read the document. There are some other little things there if you just dig deep enough. Will tell you more later, if you get the hint.

From: John Washer <chkwasher@comcast.net>
Sent: 6/20/2007 1:56:23 PM -0400
To: Mantooth <dollarhyde86@comcast.net>
Subject: Whats up in D town?

Dude!

You been laying a little low these days?

I have been trying to call you almost daily and we can't hook up!

I have the "Special K" your looking for... but it is going to cost you!

Below URLs says about the URLs he been searching for involves stealing atm card and bypassing atm camera and having lot of ppts about the stealing the atm card.

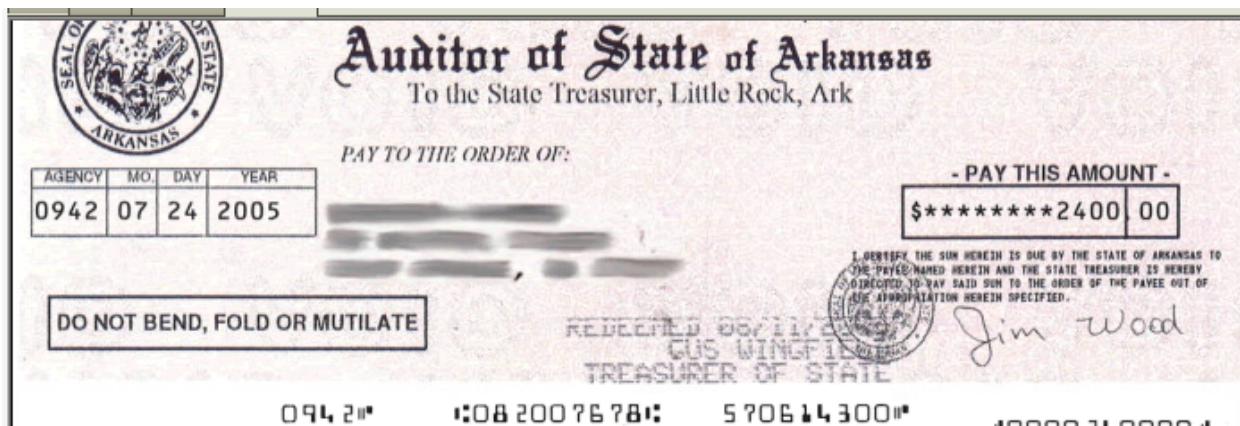
URL	:2007071220070713: Wes Mantooth@http://images.google.com/images?um=1&tab=wi&hl=en&q=atm card stealing
file:	
user name:	
response:	
accessed time:	7/12/2007 7:15:24 PM -0400
modified time:	7/12/2007 1:15:24 PM -0400
expiration time:	8/7/2007 7:15:26 PM -0400
hits:	1
use counts:	0

URL	:2007071220070713: Wes Mantooth@http://www.snopes.com/crime/warnings/atmcamera.asp
file:	
user name:	
response:	
accessed time:	7/12/2007 7:13:16 PM -0400
modified time:	7/12/2007 1:13:16 PM -0400
expiration time:	8/7/2007 7:13:18 PM -0400
hits:	1
use counts:	0

URL	Visited: Wes Mantooth@http://www.snopes.com/fraud/atm/atmcamera.asp
file:	
user name:	
response:	
accessed time:	7/12/2007 7:13:19 PM -0400
modified time:	7/12/2007 7:13:19 PM -0400
expiration time:	8/7/2007 7:13:20 PM -0400
hits:	1
use counts:	0

URL	http://tbn0.google.com/images?q=tbn:6Vi5Ho2kXz2B3M:http://www.diebold.com/atmsecurity/images/atm_trapping.jpg
file:	RMAJCPM1\images[3].jpg
user name:	wes mantooth
response:	HTTP/1.1 200 OK Content-Type: image/jpeg Content-Length: 1652
accessed time:	7/12/2007 7:15:23 PM -0400
modified time:	
expiration time:	

Found the check which has someone's name on it. This Arkansas located at borders Missouri to the north, Tennessee and Mississippi to the east, Louisiana to the south, Texas. It has been evident that they are stealing checks and planning to steal atm cards too.



So we can say that Mantooth and other guys are involved in stealing the atm cards and bunch of visa card numbers are seen. So they have been involving in this venture together.

After successfully decrypting the file we can clearly see that they are actively stealing the credit card numbers and trying to steal money at the end.

	A	B	C	D	E	F	G	H
1	Credit Card Numbers	Name	Bank	Type	Exp	ID		
2	1234-1234-1234-1344	Red Skelton	BOA	Visa	9/10	123		
3	9877-1434-6543-2145	Jim Carrey	Wells Fargo	Visa	3/09	765		
4	37987-123458-13454	Buster Keaton	BOA	Amex	12/07			
5	123-123-123-1-2	Chris Rock		JC Penny	1/08			
6	6878-9876-9876-9876	Eddie Murphy	Bank of Panama	MC	4/09			
7	6789-2435-5464-6554	Robin Williams	Bank of American Forks	Visa	6/11	345		
8	543-345-567-1-1	Adam Sandler		Mervyns	9/11			

John:

I've got to meet with you tomorrow to pass off the credit card number I got yesterday. We'll have to hurry on these because they'll be dropping off the radar as people complain they lost them.

See you at the fountain in front of the university at 1230.

Ps: Bring food

Wes:

I got this document from the bank on a war dialer attack.

Got lots of stuff but I'll have to wrap it up and send it to you encrypted so we don't have to worry about the cops ever reading it.

Doc

Doc

Here's the photos you wanted. I'd rather have the million but the 10s would do if I have enough ☺

Wes



These are the evidences and still more to it are collected and shows that these guys are on stealing money using credit card and atm card numbers and stealing those cards to drain the money out of it. Lot of different computer based evidence we got from this analysis.