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)

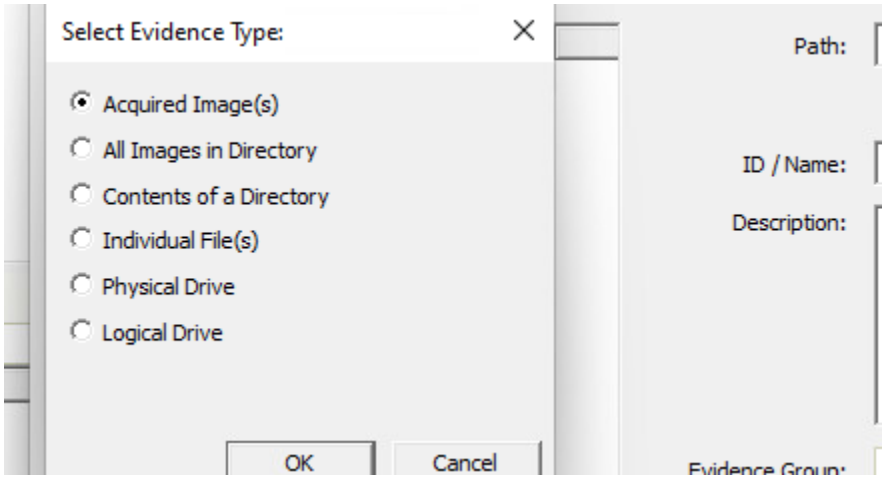
1. Include File Slack
2. Include Free Space
3. Ignore Status for all file status (Deleted, Encrypted, From Email)
4. All file types are selected by default
5. Include Message Headers by default

For Evidence Processing

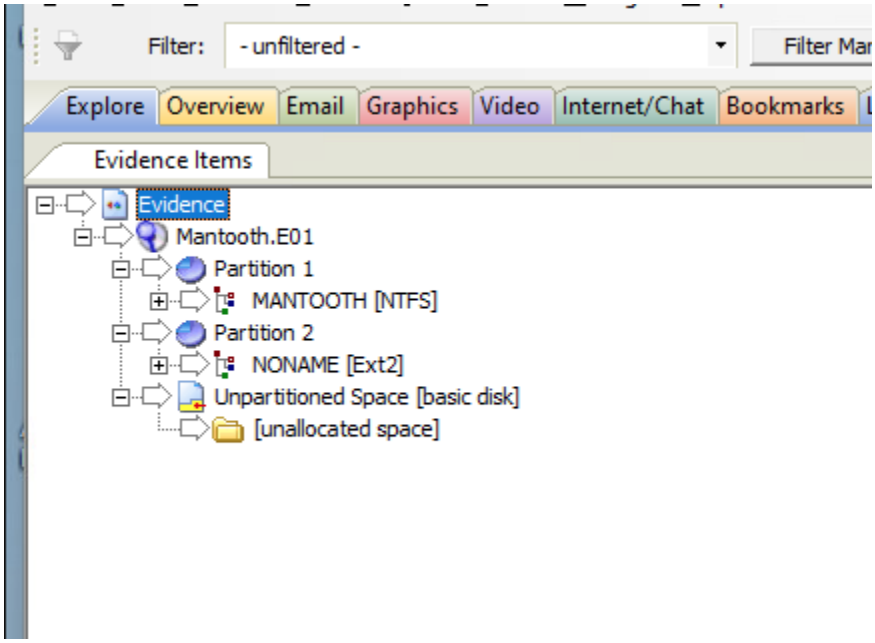
1. MD5 Hash
2. SHA-1 Hash
3. Expand Compound files
4. Flag Bad Extensions
5. Search Text Index
6. Create Thumbnails for Graphics
7. Include Deleted files

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?

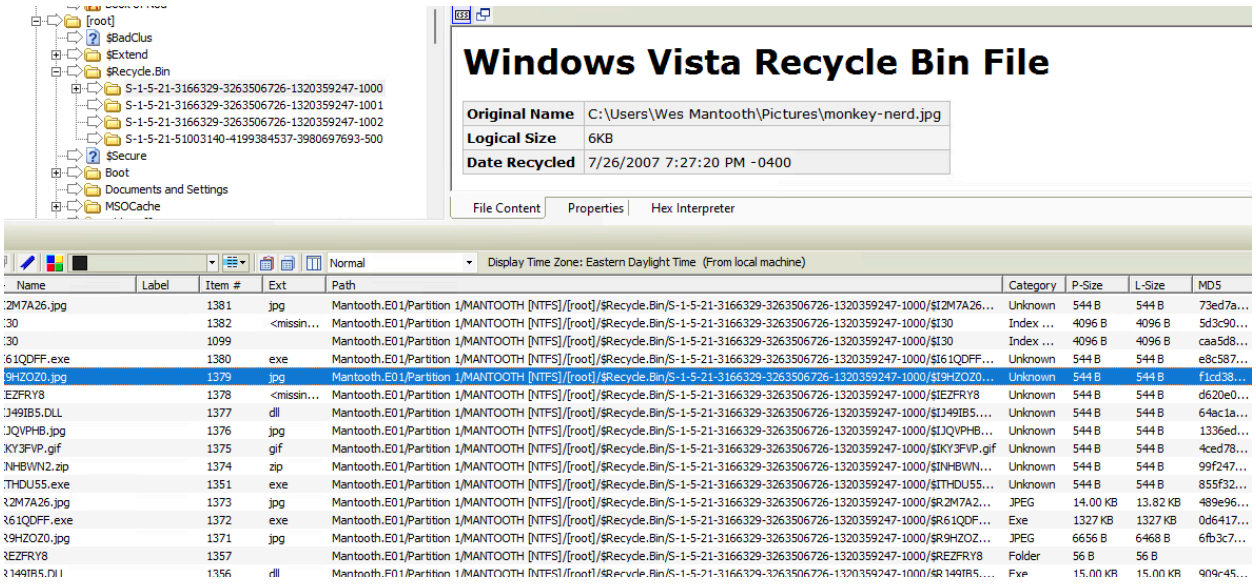


Two partitions

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?

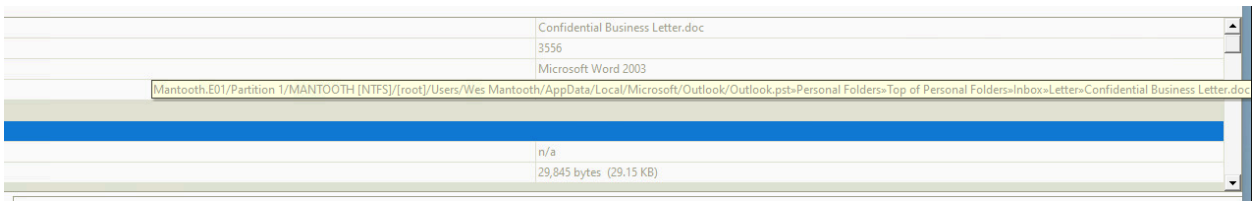
From this screenshot we can see that wes Mantooth user once owned these files and deleted it. We can say it belongs to Mantooth by seeing the path which says MANTOOTH[NTFS].

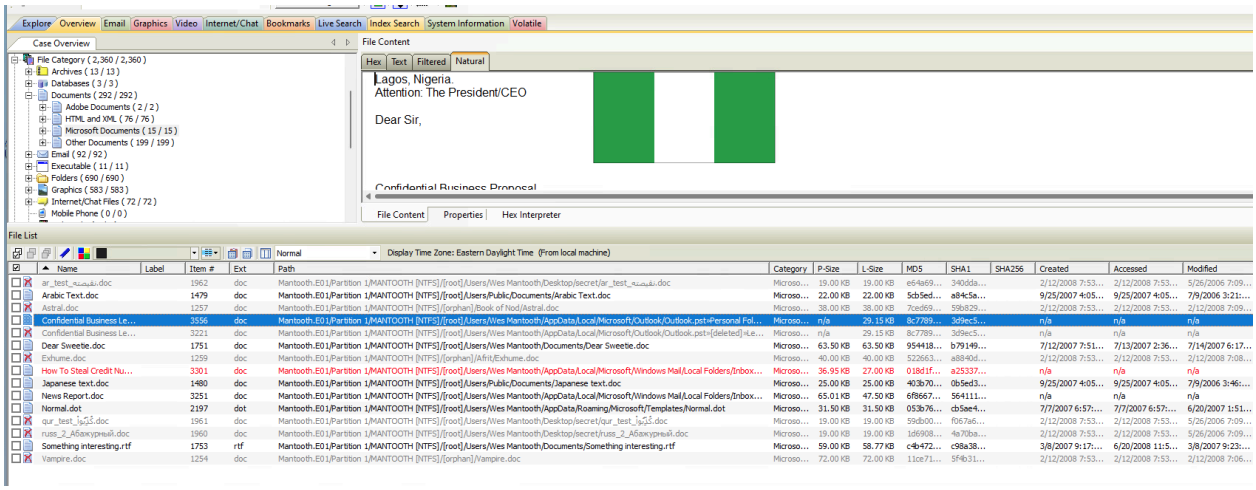


Question 5: Which file category (starting from File Category) does the file, *Confidential Business Letter.doc*, belong to? What is the file path for this file?

It belong to Documents > Microsoft Documents

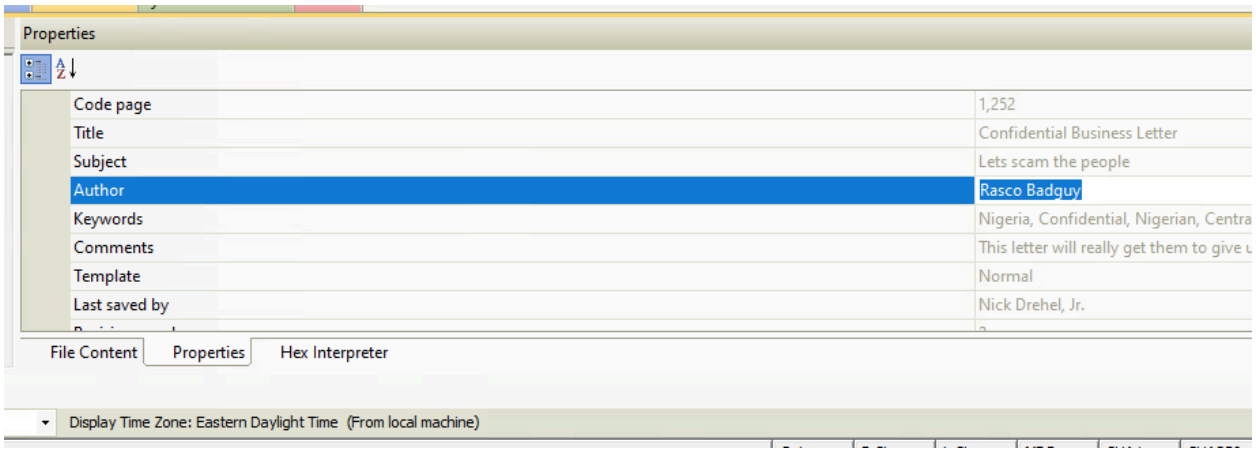
File Path for this file in below screenshot:

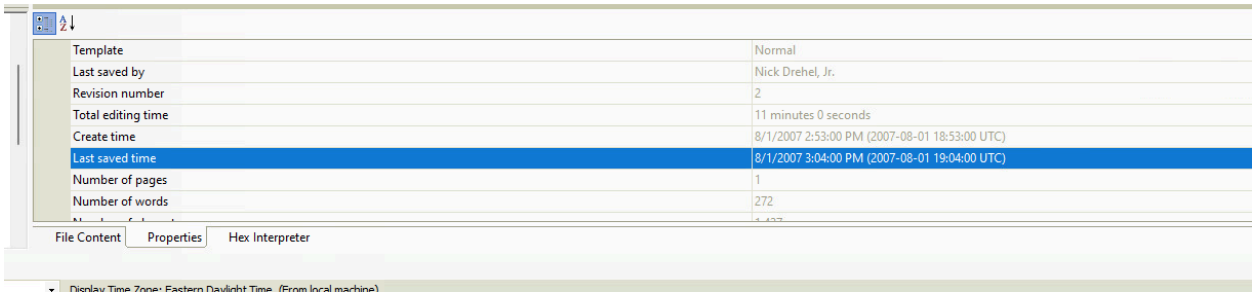




Question 6: Open the Confidential Business Letter.doc, check both File Content and Properties, who was the document author, when was this document last modified, and who modified at the last time?

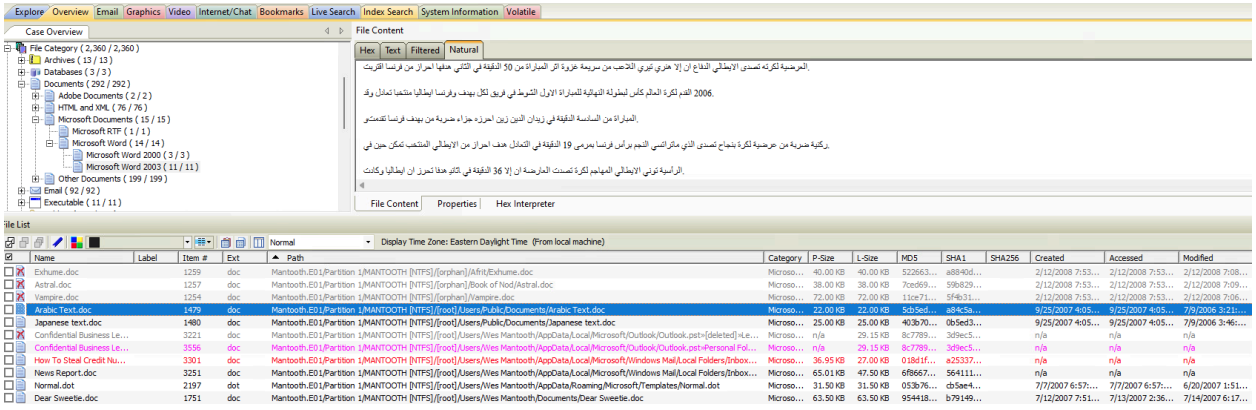
This file belongs to (Author) Rasco Badguy and last saved or modified by Nick Drehel, Jr. The Last time it is modified and saved is August 1 2007 3.04 pm.

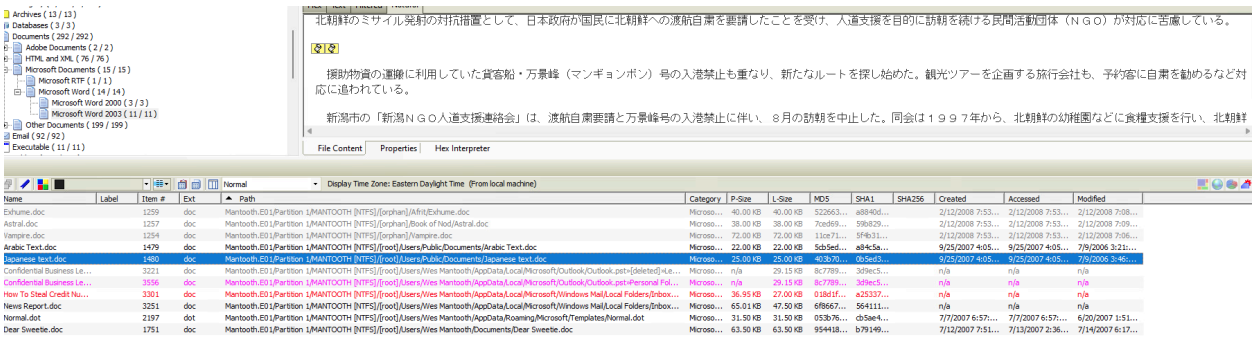




Question 7: What are the two documents that use foreign languages?

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

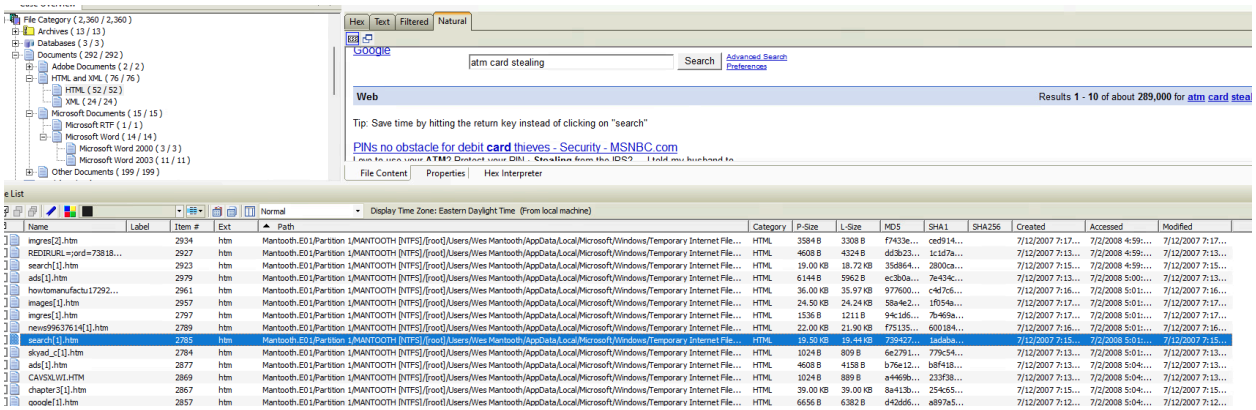




Go to File Category > Documents > HTML, and look for a Google search file that Mantooth searched “atm card stealing”.

Show a screenshot below.

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

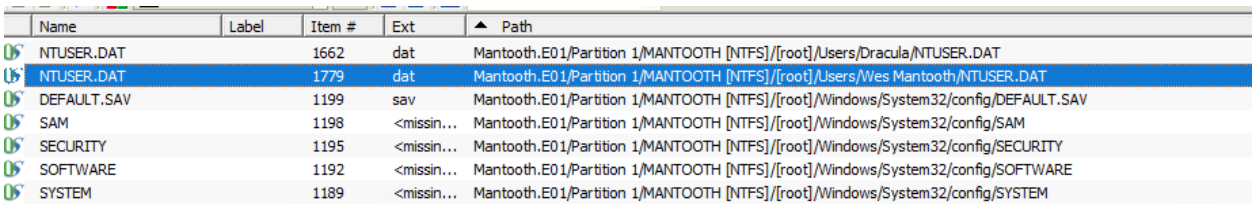


Question 8: Go to File Category > Multimedia > Video > MPEG 2.0 Video, watch happy.mpeg, what can you tell from the video?

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.

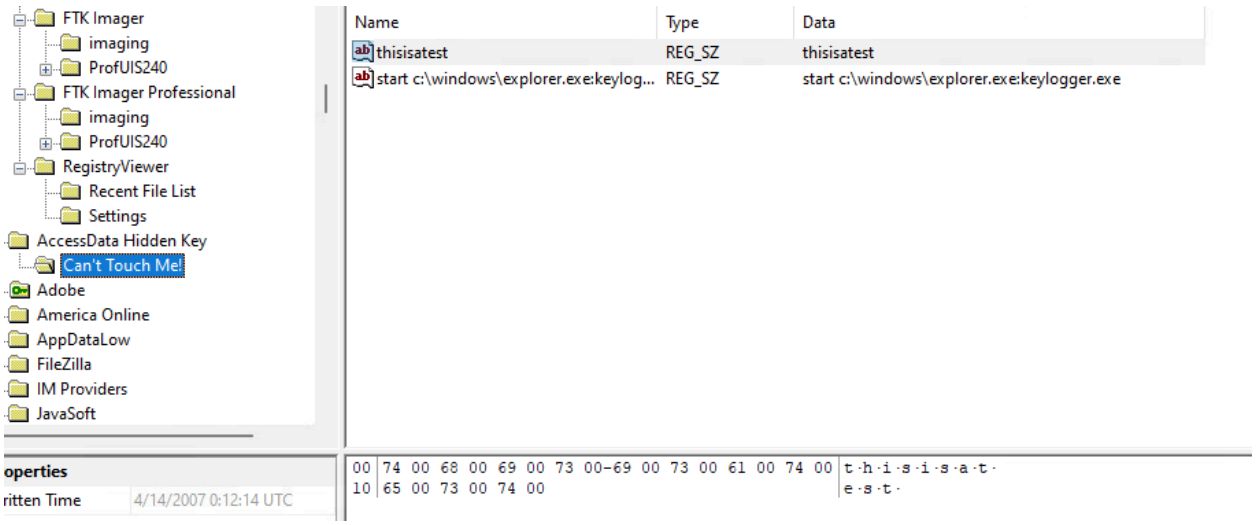
Path in screenshot below



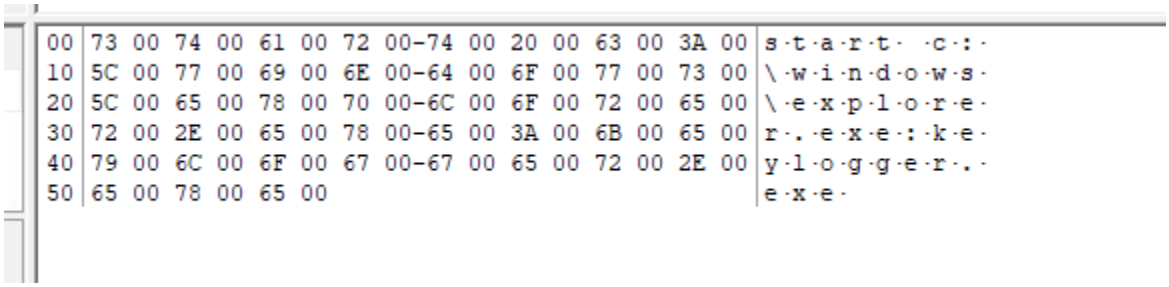
Name	Label	Item #	Ext	Path
NTUSER.DAT		1662	dat	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Dracula/NTUSER.DAT
NTUSER.DAT		1779	dat	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/NTUSER.DAT
DEFAULT.SAV		1199	sav	Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/DEFAULT.SAV
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

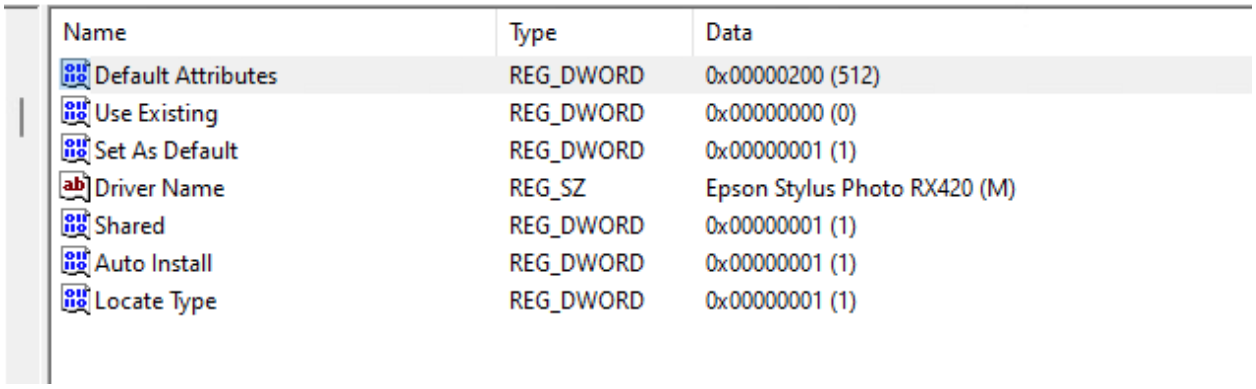
This NTUSER.DAT file is a hive file which has all the user-specific configuration settings and preferences of the WES MANTOOTH in this case. It also has lot of variables stored like environment variables, network configuration and personalized settings etc.

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.



I found a keylogger on this machine.

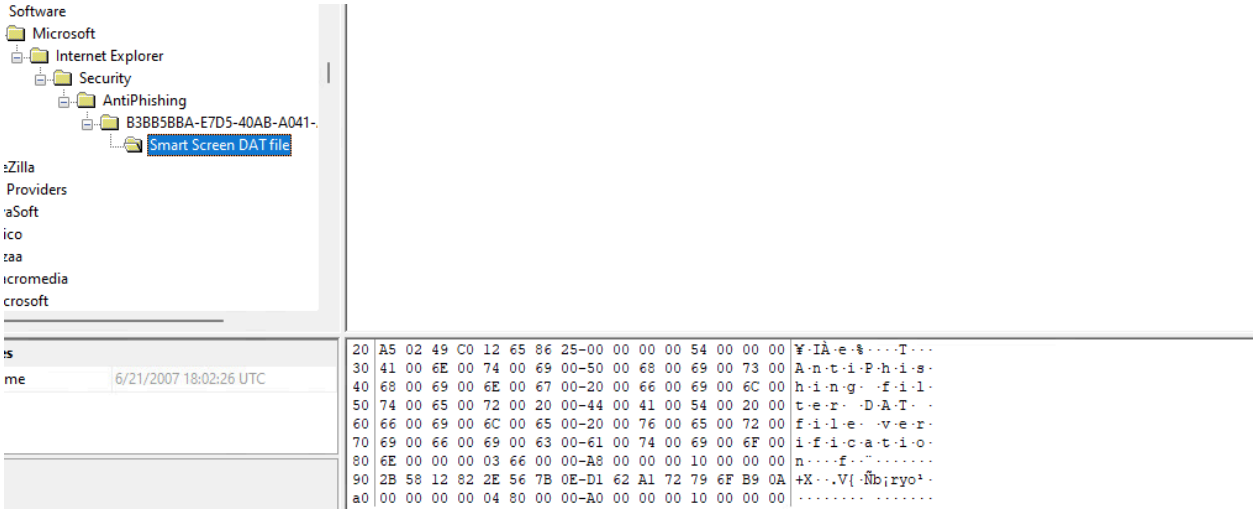




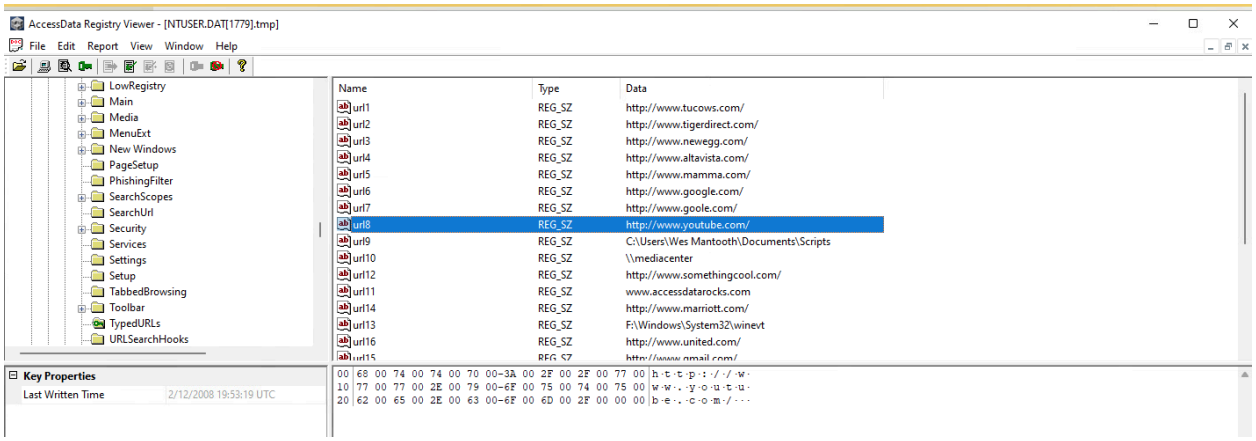
Driver used here is Epson Stylus Photo RX420 (Photo Printer)

Name	Type	Data
RemotePath	REG_SZ	\\mediacenter\My Internet Clearning 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)

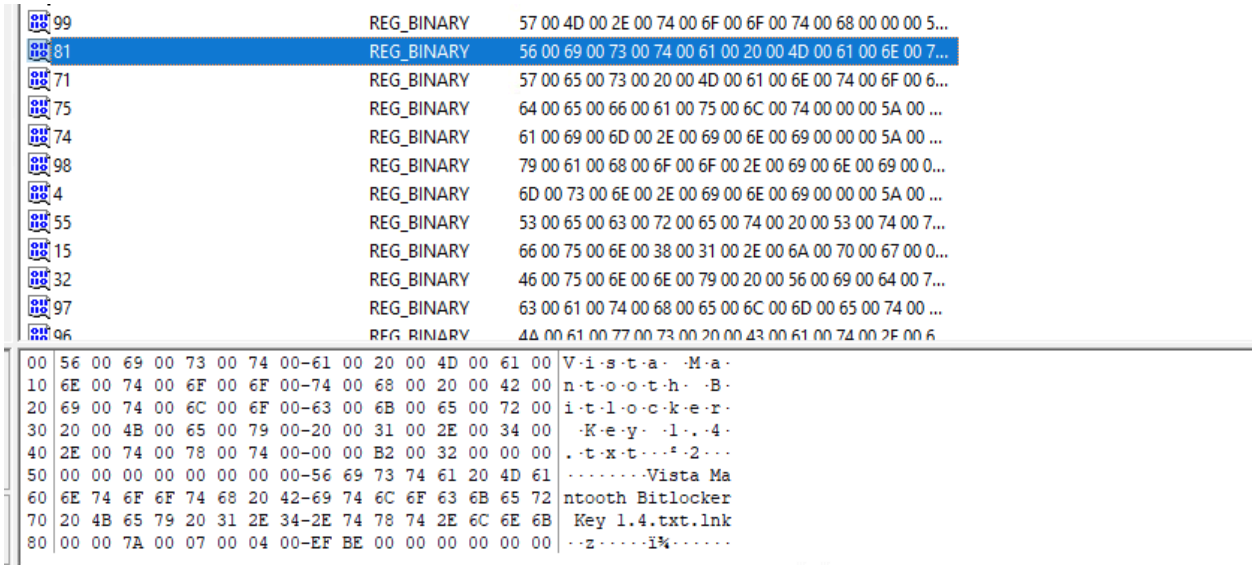
I searched what this clearning folder is and it said that other can access this folder.



AntiPhishing folder found.



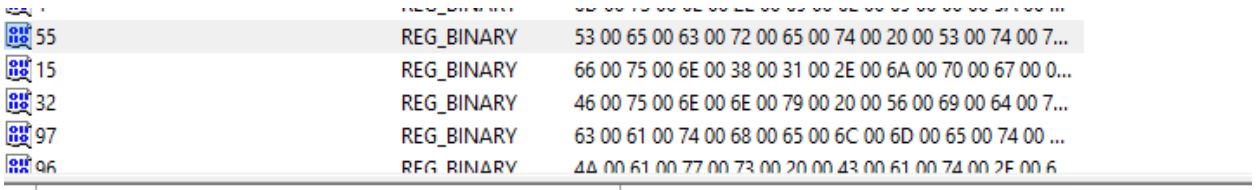
We found a Vista Mantooth Bitlocker Key.txt.lnk



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_BINARY	44 00 61 00 77 00 73 00 20 00 43 00 61 00 74 00 2E 00 6

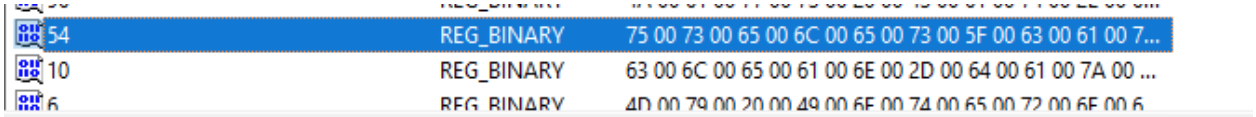
```
00 56 00 69 00 73 00 74 00-61 00 20 00 4D 00 61 00  V·i·s·t·a· ·M·a·
10 6E 00 74 00 6F 00 6F 00-74 00 68 00 20 00 42 00  n·t·o·o·t·h· ·B·
20 69 00 74 00 6C 00 6F 00-63 00 6B 00 65 00 72 00  i·t·l·o·c·k·e·r·
30 20 00 4B 00 65 00 79 00-20 00 31 00 2E 00 34 00   ·K·e·y· ·1·.·4·
40 2E 00 74 00 78 00 74 00-00 00 B2 00 32 00 00 00  .·t·x·t···²·2···
50 00 00 00 00 00 00 00 00-56 69 73 74 61 20 4D 61  ········Vista Ma
60 6E 74 6F 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-EF BE 00 00 00 00 00 00  ··z·····ï¾······
```

Secret Stuff.lnk



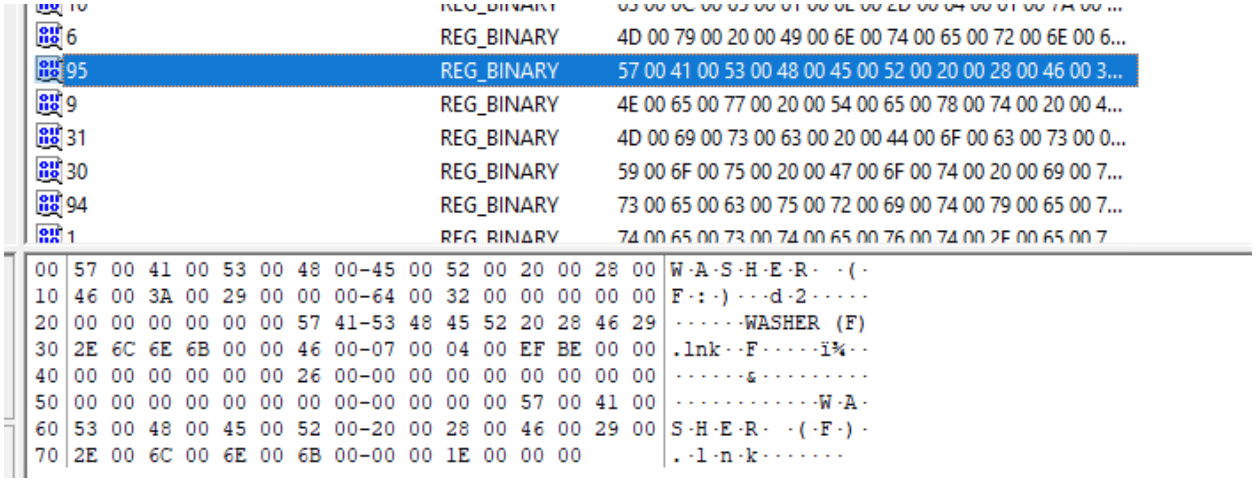
55	REG_BINARY	53 00 65 00 63 00 72 00 65 00 74 00 20 00 53 00 74 00 7...
15	REG_BINARY	66 00 75 00 6E 00 38 00 31 00 2E 00 6A 00 70 00 67 00 0...
32	REG_BINARY	46 00 75 00 6E 00 6E 00 79 00 20 00 56 00 69 00 64 00 7...
97	REG_BINARY	63 00 61 00 74 00 68 00 65 00 6C 00 6D 00 65 00 74 00 ...
96	REG_BINARY	44 00 61 00 77 00 73 00 20 00 43 00 61 00 74 00 2E 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 00-53 65 63 72 65 74 20 53  ·····Secret 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  ï¾··········&·····
50 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 20 00 00 00
```

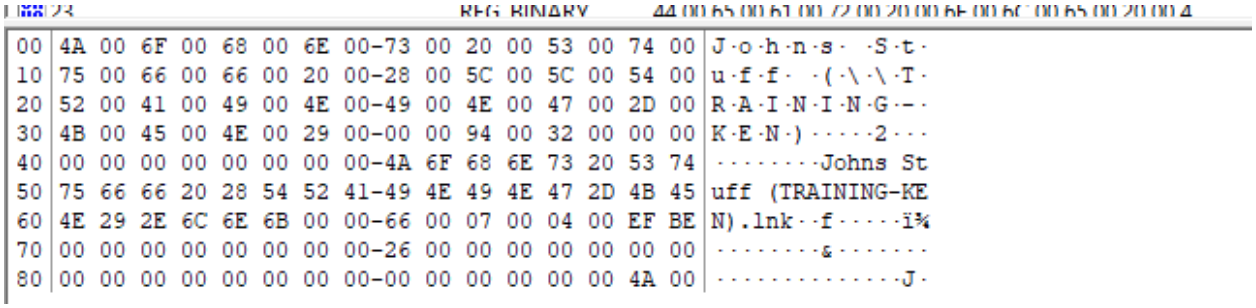


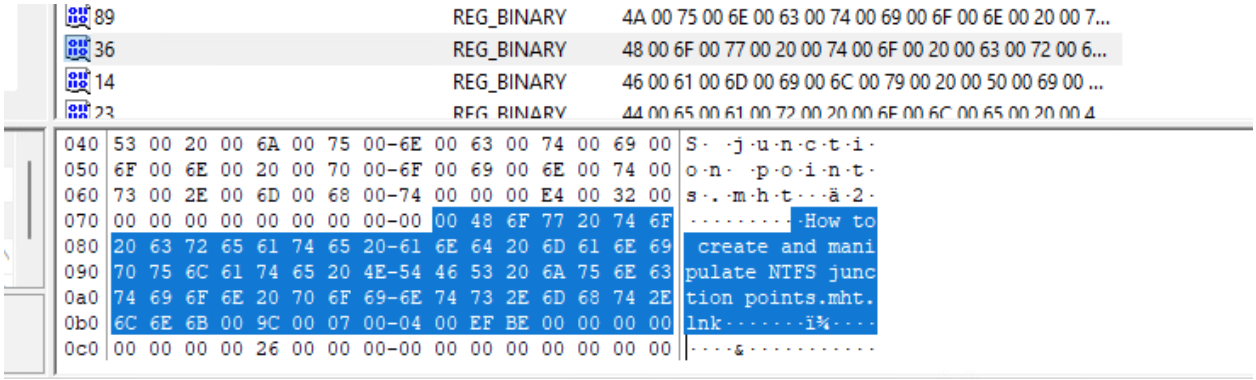
54	REG_BINARY	75 00 73 00 65 00 6C 00 65 00 73 00 5F 00 63 00 61 00 7...
10	REG_BINARY	63 00 6C 00 65 00 61 00 6E 00 2D 00 64 00 61 00 7A 00 ...
6	REG_BINARY	4D 00 79 00 20 00 49 00 6E 00 74 00 65 00 72 00 6E 00 6

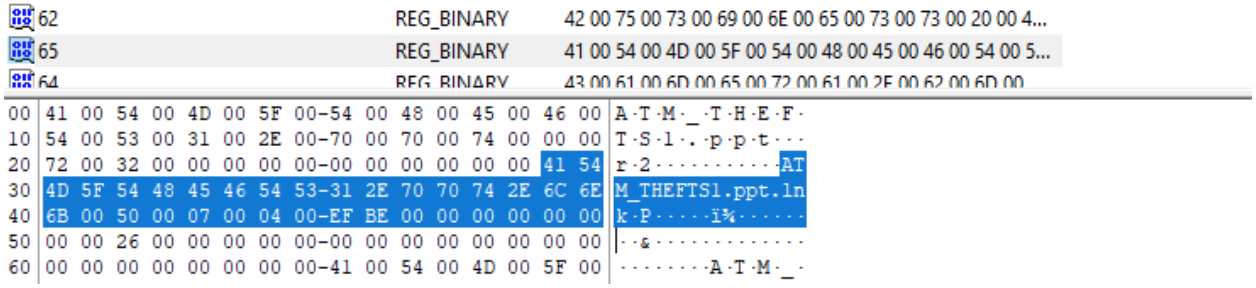
```
00 75 00 73 00 65 00 6C 00-65 00 73 00 5F 00 63 00  u·s·e·l·e·s·_·c·
10 61 00 74 00 2E 00 6A 00-70 00 67 00 00 00 70 00  a·t·.·j·p·g···p·
20 32 00 00 00 00 00 00 00-00 00 00 00 75 73 65 6C  2···········usel
30 65 73 5F 63 61 74 2E 6A-70 67 2E 6C 6E 6B 00 00  es_cat.jpg.lnk··
40 4E 00 07 00 04 00 EF BE-00 00 00 00 00 00 00 00  N·····ï¾········
50 26 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  &···············
60 00 00 00 00 00 00 75 00-73 00 65 00 6C 00 65 00  ·····u·s·e·l·e·
```

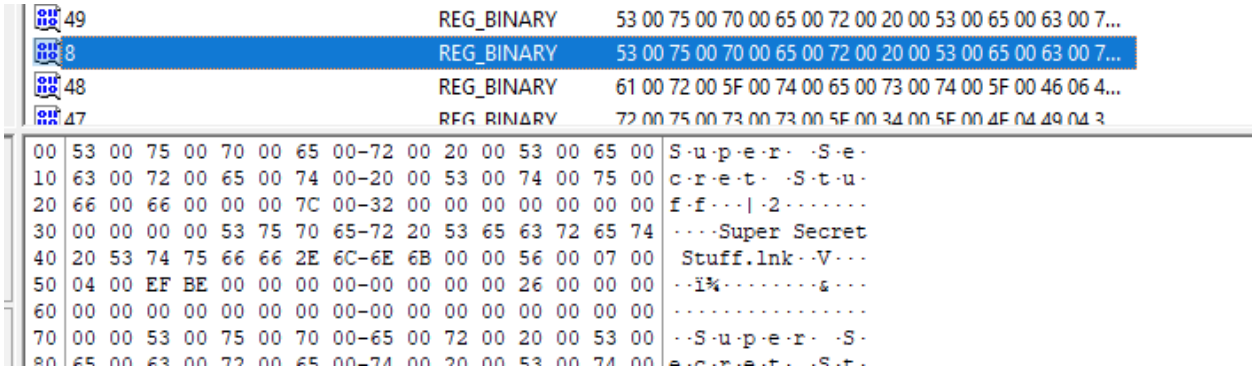


I feel John Stuff has important details to it.



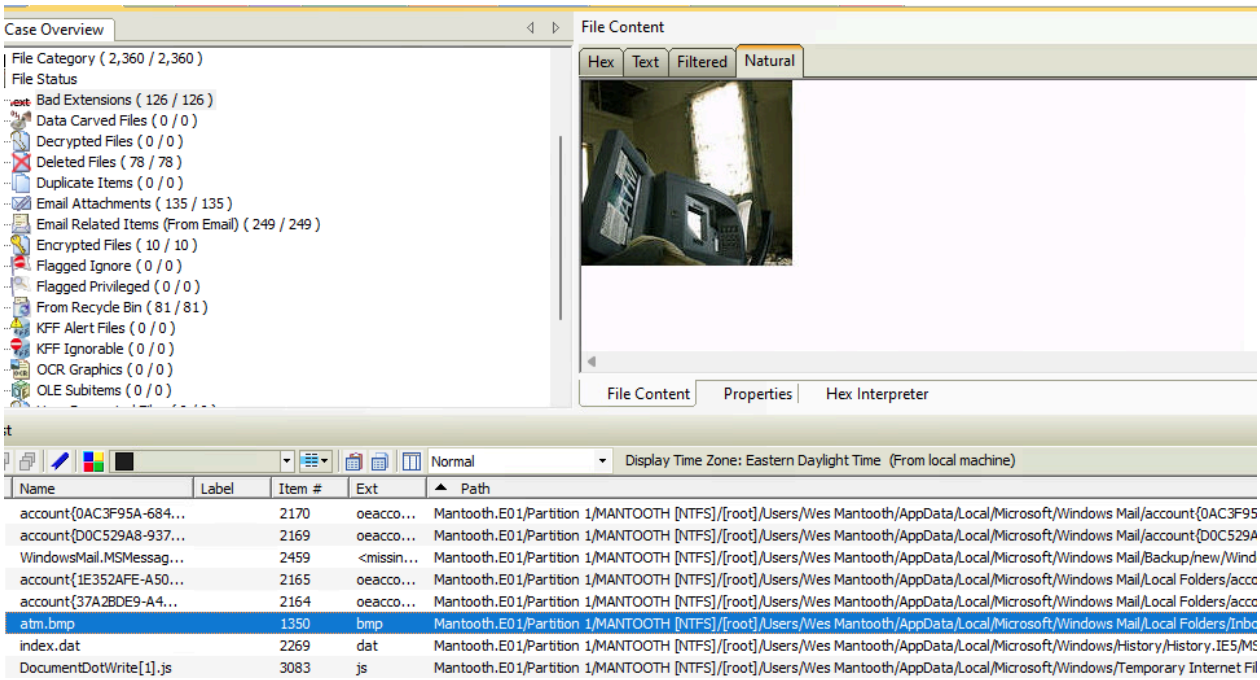


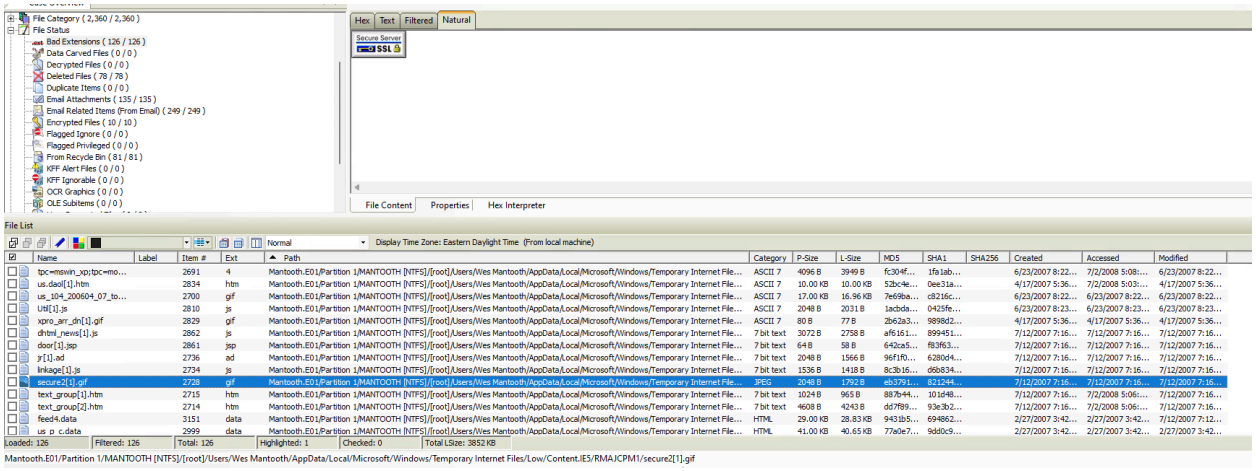




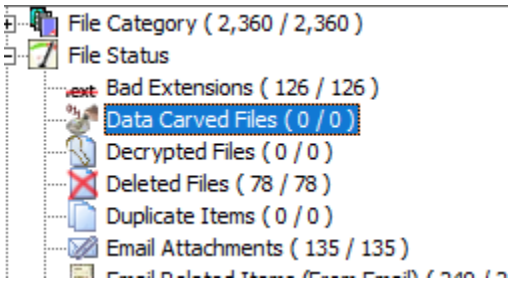
Lot of Cat images images and lot of secret stuff found here.

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.



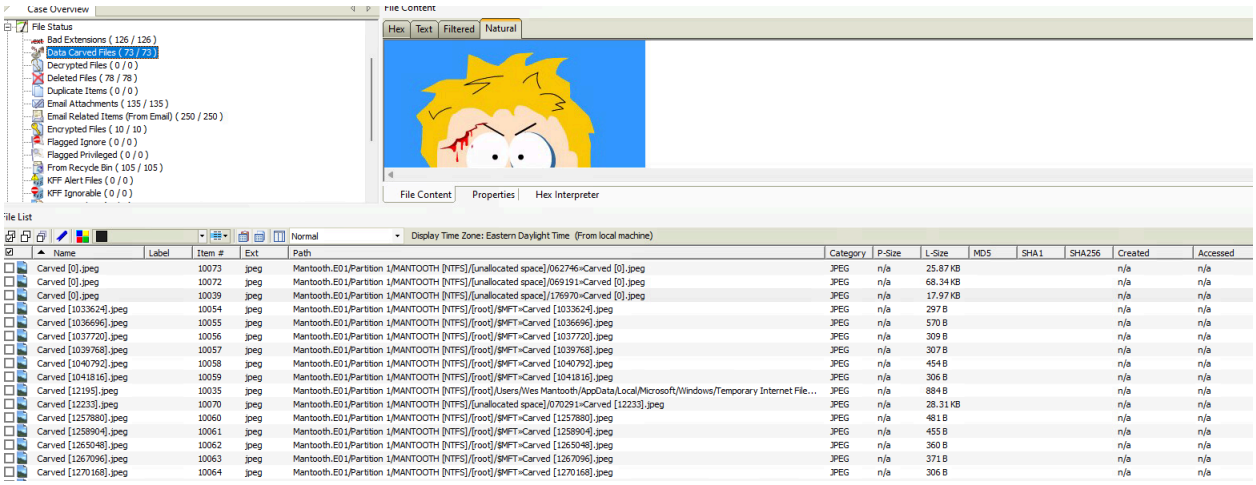


Question 12: Check the number of Data Carved Files from File Status, what is the number?



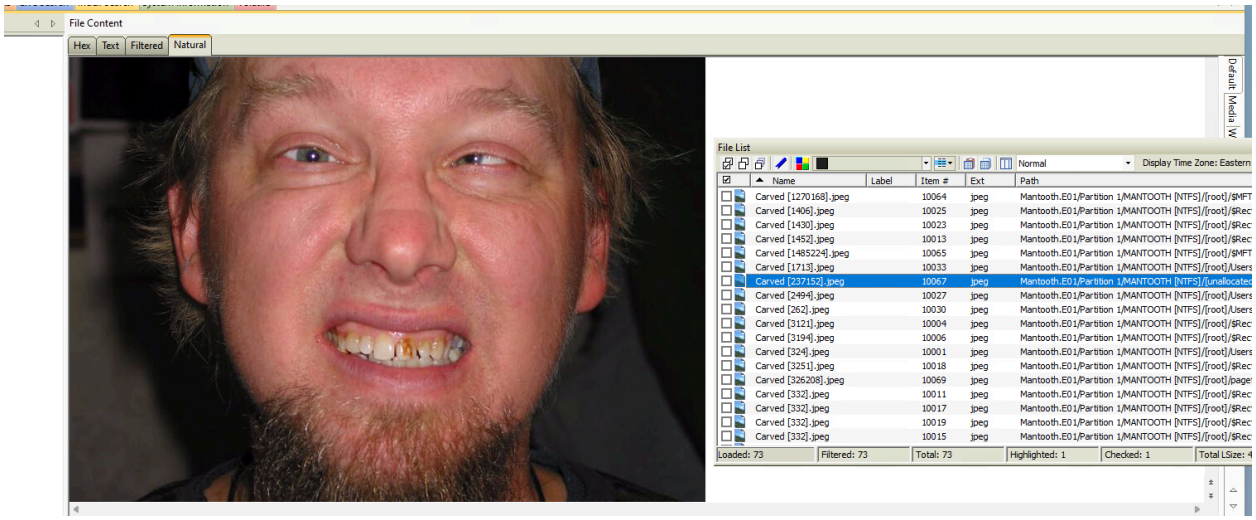
Initially Carved Files amount is 0.

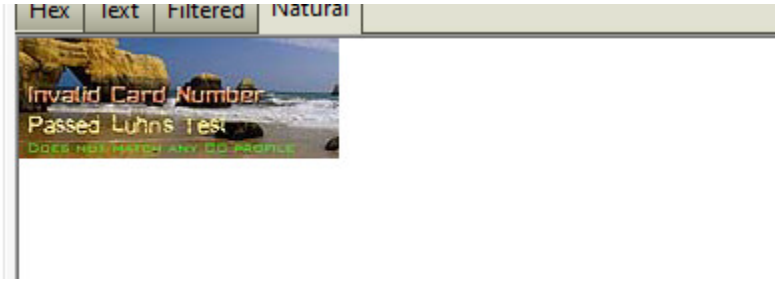
Question 13: Check the number of Data Carved Files again, have you carved out some files? Provide a screenshot.

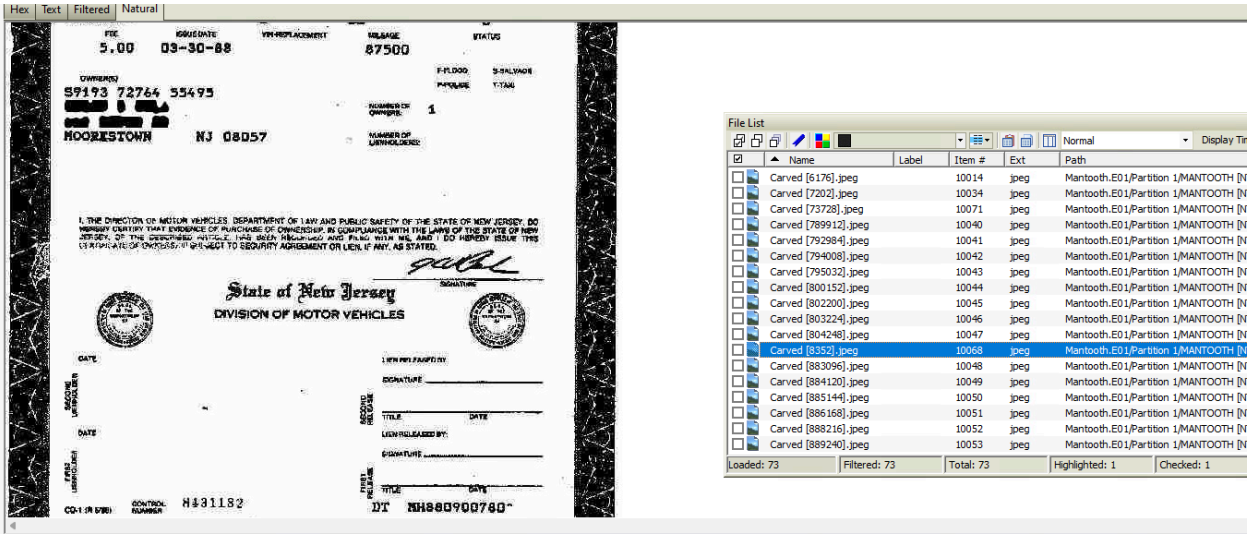


Yes, I carved out 73 jpeg images which may be crucial for our evidence.

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?

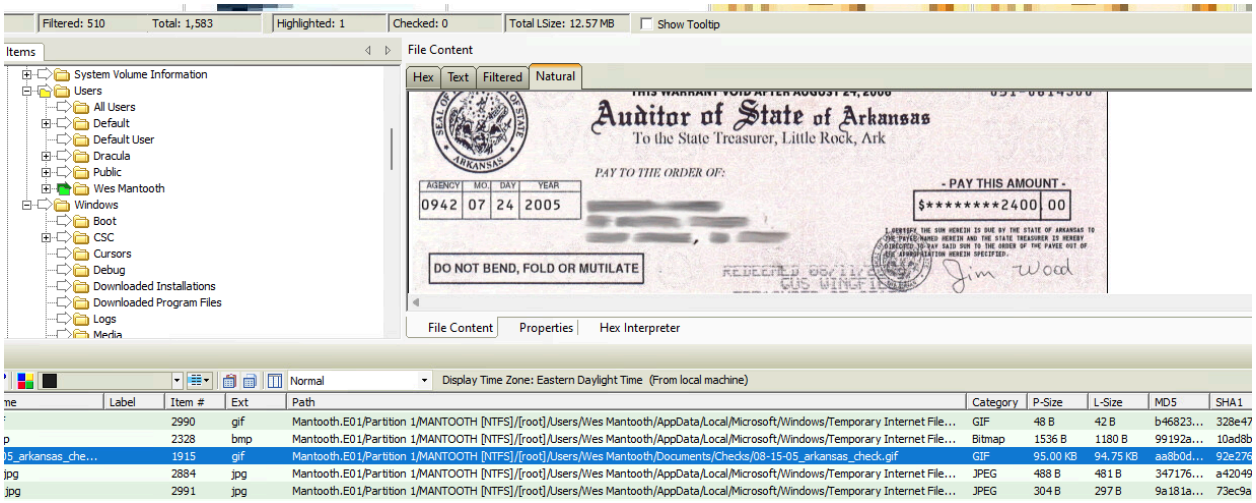






Data Carving is important because to extracted the deleted, fragmented and lost files along with their timelines which is very important for finding out crimes as for the forensics in concern.

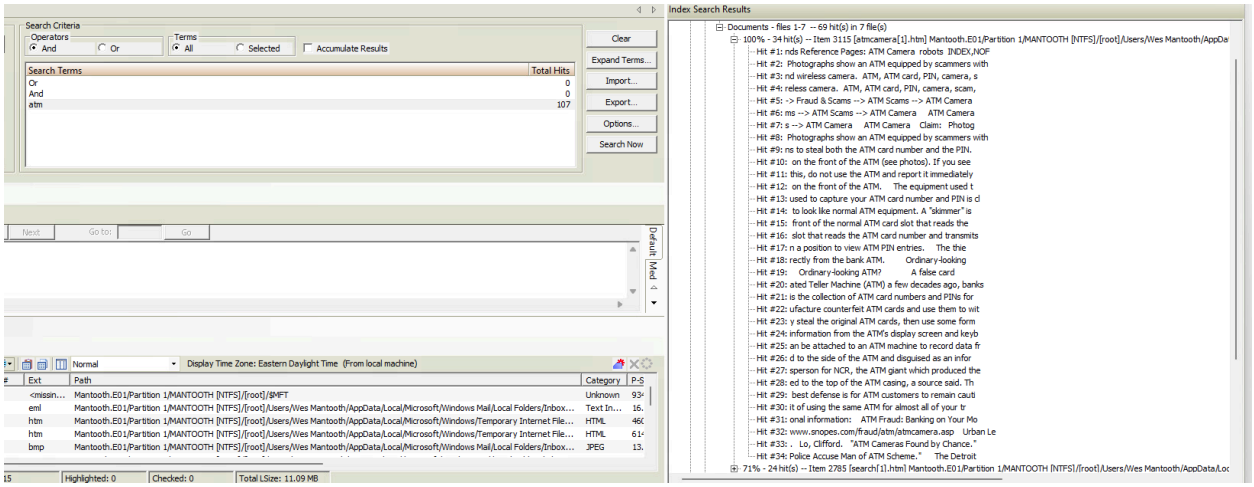
Question 15. Find one bank check image and bookmark it in Mantooth bookmark. What is the name of this image?

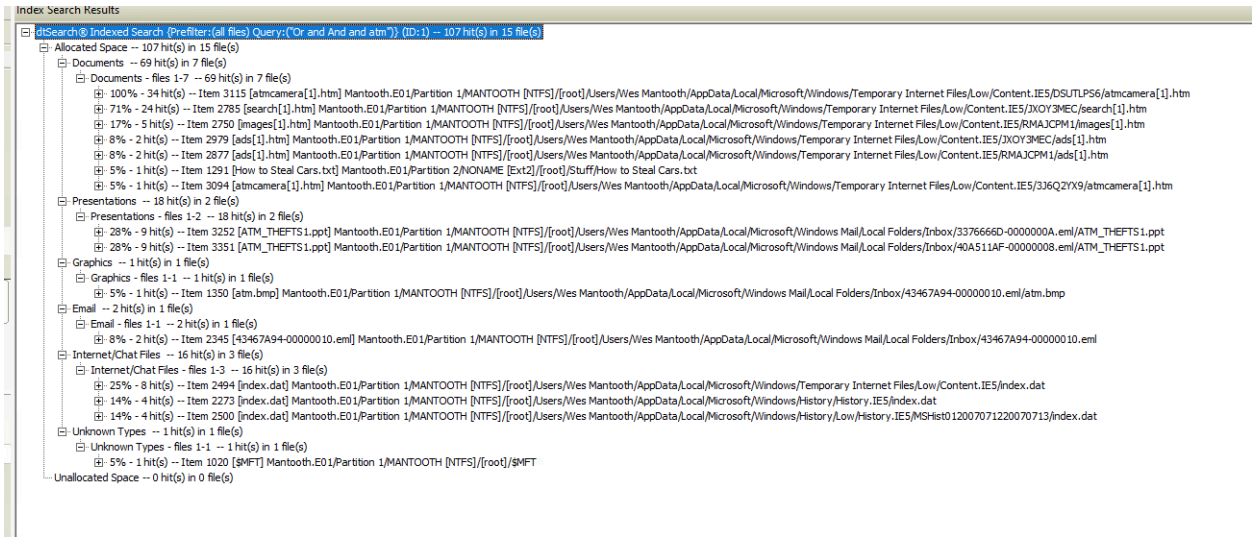


We found the check successfully and name we found on it is signed by “Jim Wood”

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

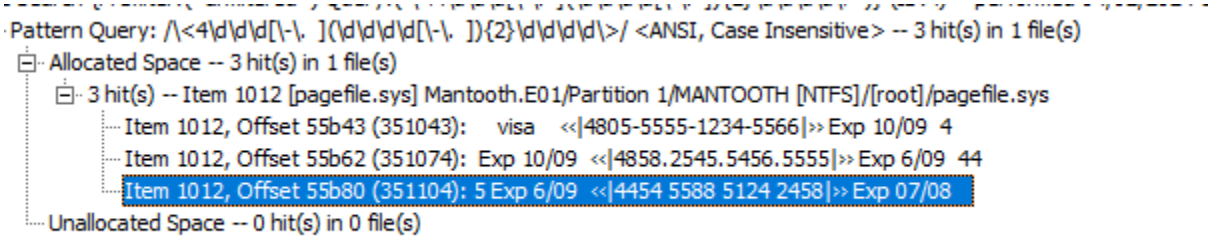
I got 107 hits in 15 files :

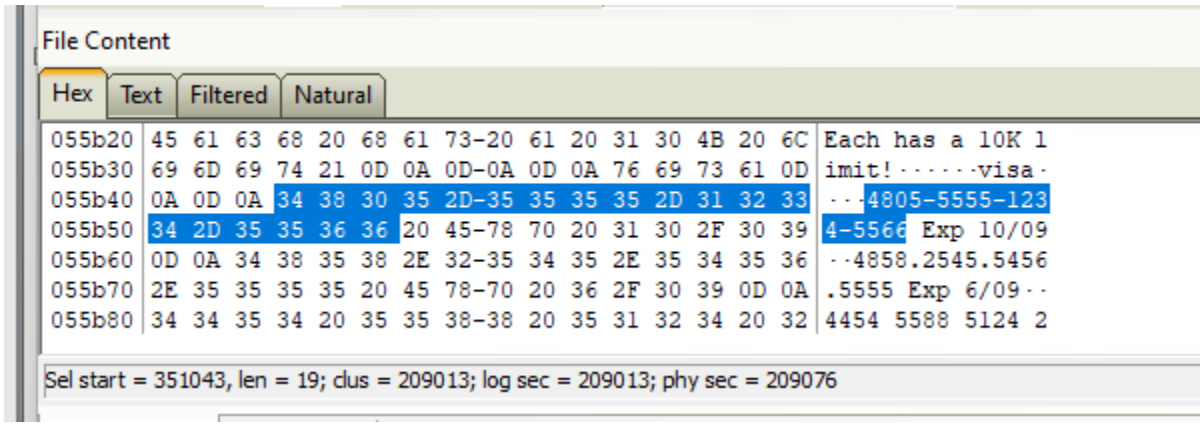


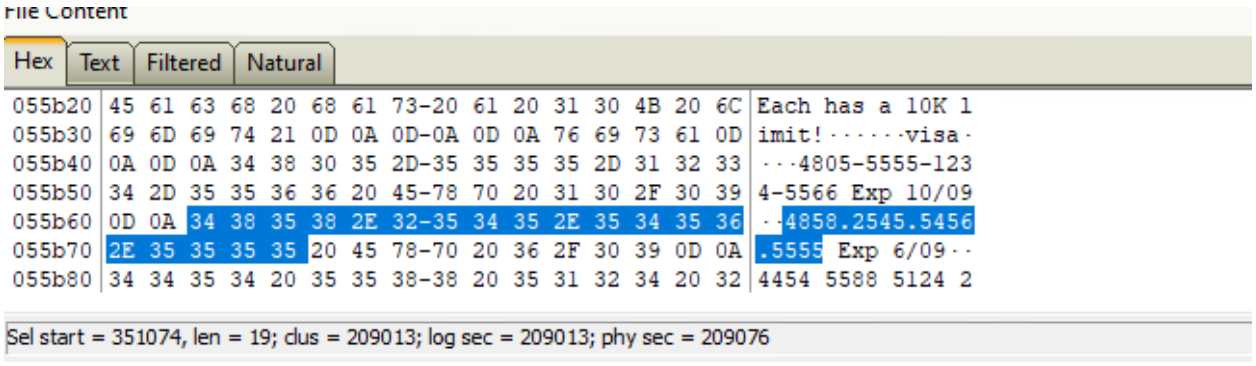


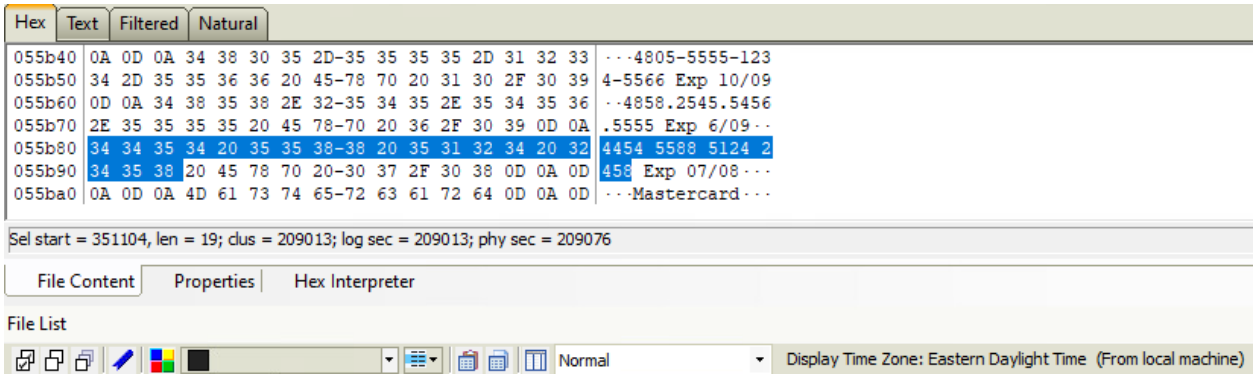
Question 17: Do you find any Visa numbers? list three Visa numbers along with the expiration date.

I got three visa numbers in this search





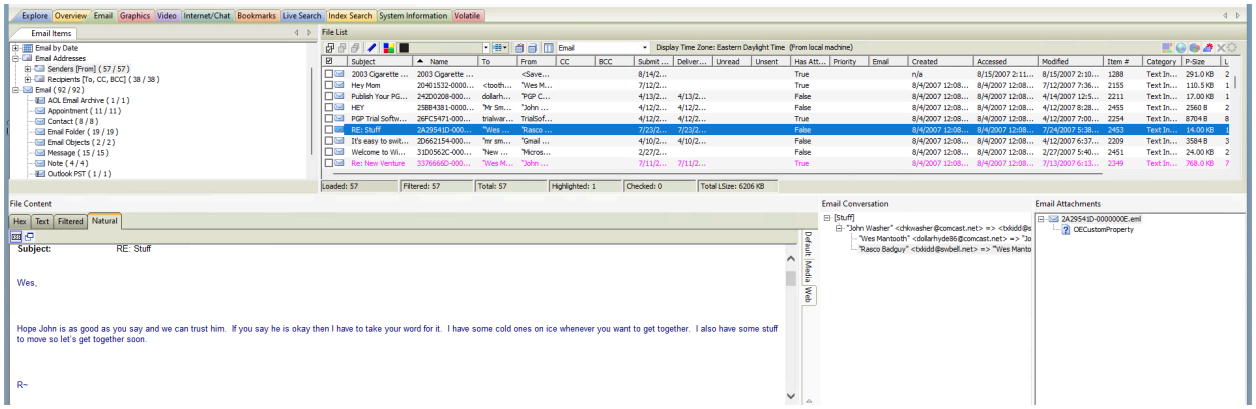




Question 18: What is the advantage of using indexed search vs. the live search?

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.



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

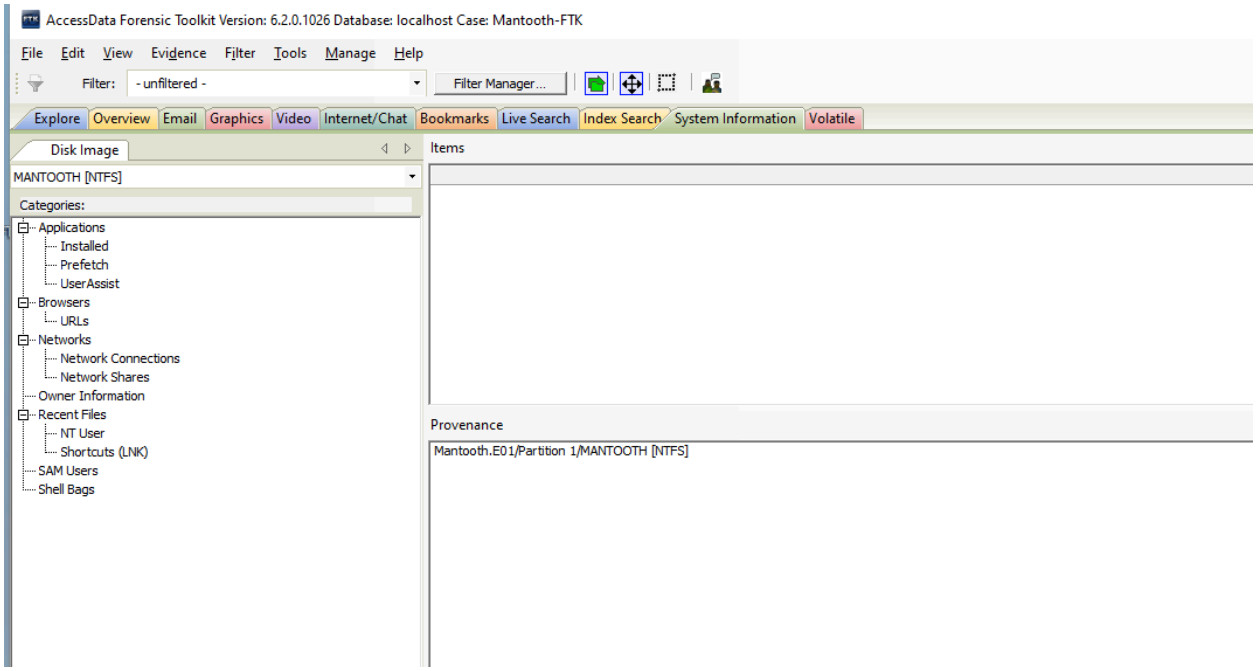
URL	:2007071220070713: Wes Mantooth@http://images.google.com/images?um=1&tab=wi&hl=en&q=atm card stealing
file:	
user name:	
response:	
accessed time:	7/12/2007 7:15:24 PM -0400
modified time:	7/12/2007 1:15:24 PM -0400
expiration time:	8/7/2007 7:15:26 PM -0400
hits:	1
use counts:	0

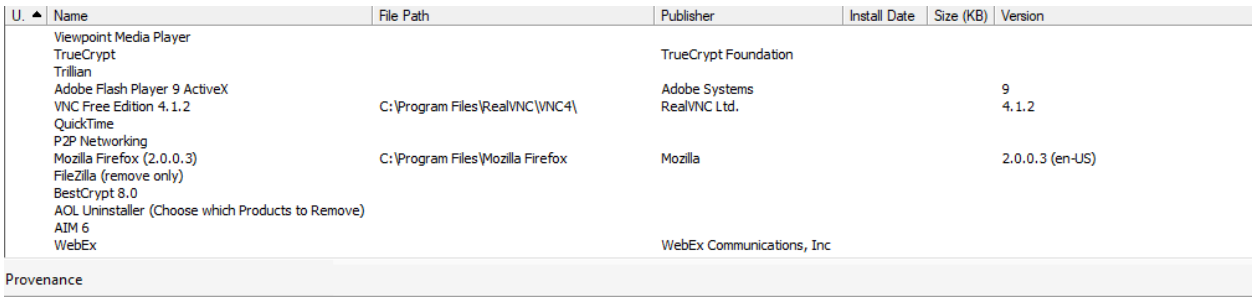
URL	:2007071220070713: Wes Mantooth@http://www.snopes.com/crime/warnings/atmcamera.asp
file:	
user name:	
response:	
accessed time:	7/12/2007 7:13:16 PM -0400
modified time:	7/12/2007 1:13:16 PM -0400
expiration time:	8/7/2007 7:13:18 PM -0400
hits:	1
use counts:	0

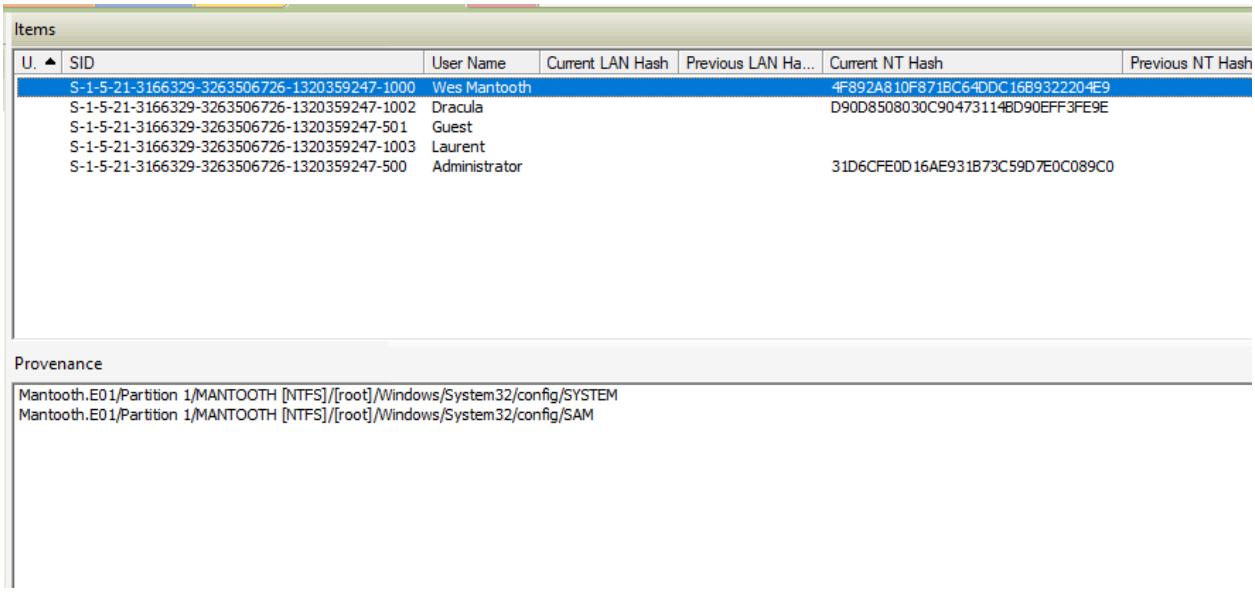
URL	:2007071220070713: Wes Mantooth@http://b.casalemedia.com/V2/44508/86958/index.html?www.snopes.com/fraud/atm/atmcamera.asp
file:	
user name:	
response:	
accessed time:	7/12/2007 7:15:00 PM -0400
modified time:	7/12/2007 1:15:00 PM -0400
expiration time:	8/7/2007 7:15:02 PM -0400
hits:	1
use counts: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

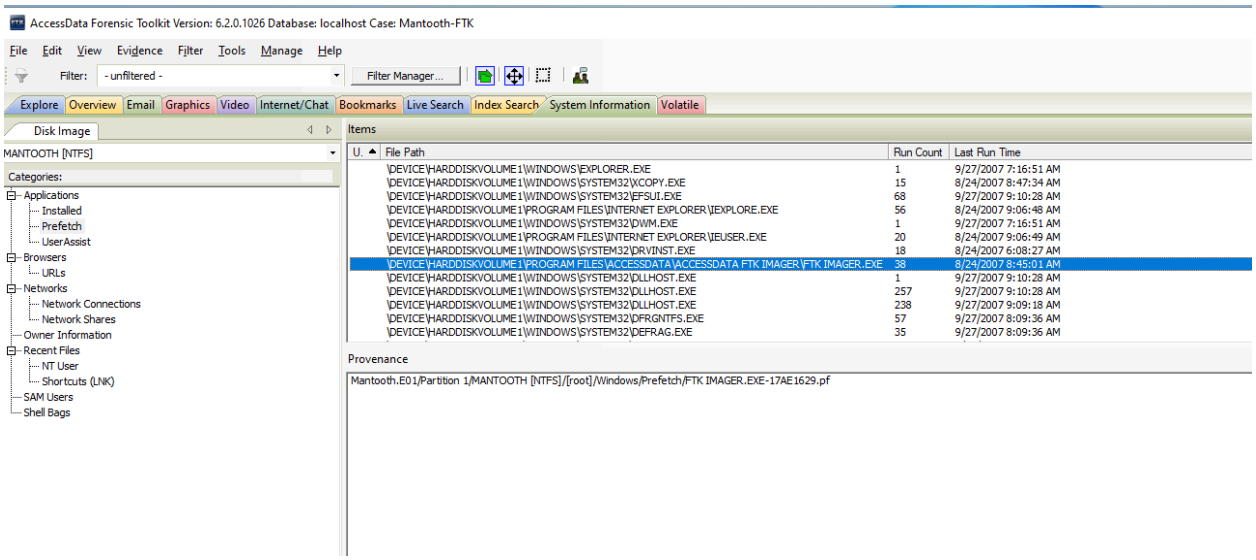
There are lot of important information were listed in this tab especially application prefetch and installed shows and give more information about the application ran by mantooth will us to know what's happened in his system for example he used BestCrypt to encrypt some of the files that is in the encrypted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







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.



Dracula	UEME_RUNPIDL:%csidl23%\Extras and Upgrades\Windows Ultimate Extras.lnk	19	3/5/2007 8:24:58 PM
Wes Mantooth	UEME_RUNPATH:C:\Windows\explorer.exe	1	2/12/2008 2:25:50 PM
Wes Mantooth	UEME_RUNPATH:C:\Windows\system32\defrag.exe	1	2/12/2008 2:21:39 PM
Wes Mantooth	UEME_RUNPATH:C:\Program Files\Windows Media Player\wmplayer.exe	2	2/12/2008 1:47:43 PM
Wes Mantooth	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
hose who owes	Microsoft Office 97/2000 Password Attack	Finished	*smack [HEX=48494a4...

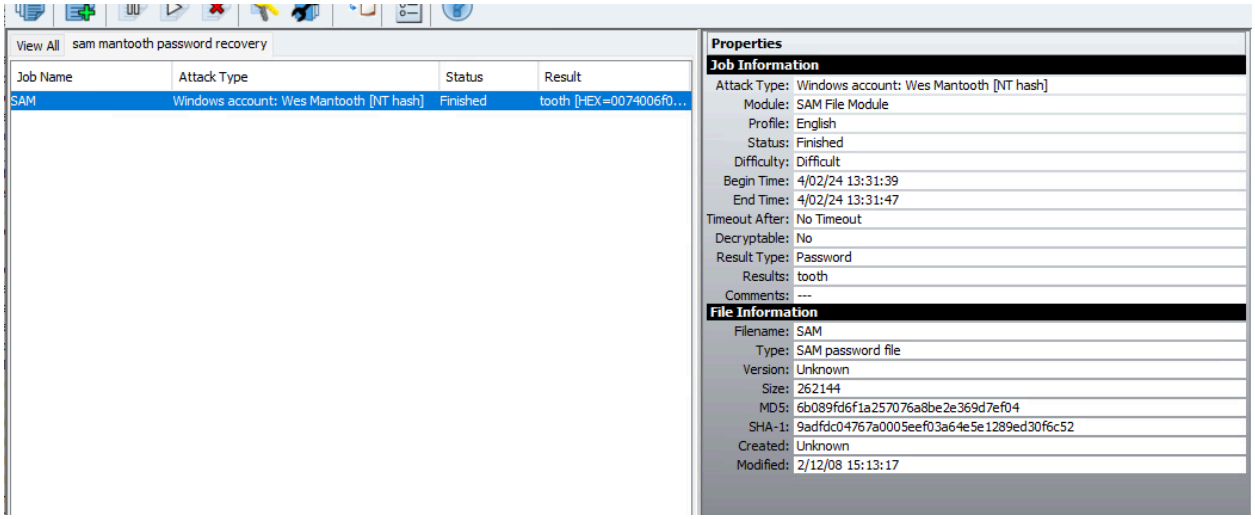
Properties

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:	cc5c3586d6555824c8f6711cc4b2dd7e3ba43fb4
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.

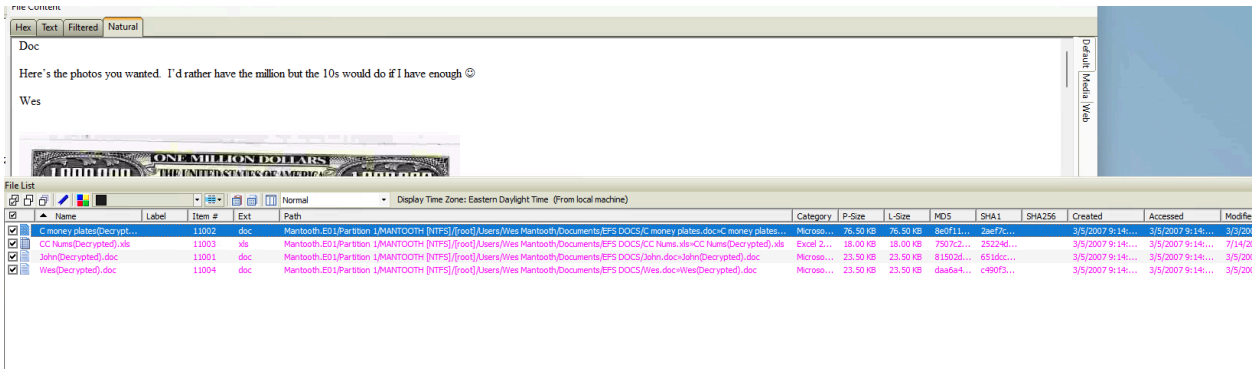


Password is tooth

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.



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

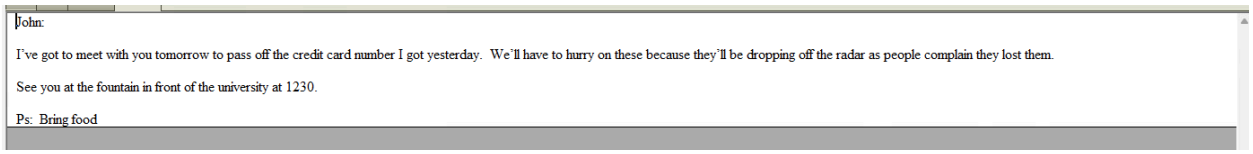
CC nums (Decrypted).xls

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



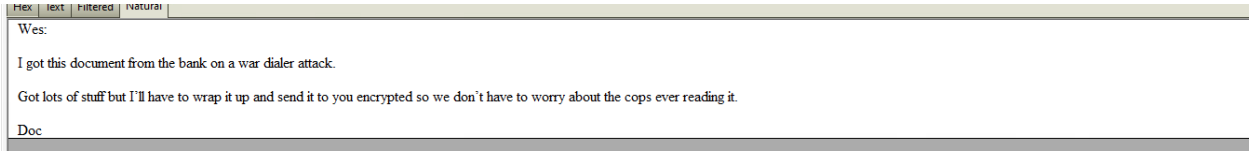
John:

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

Rosco,

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 budy 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.

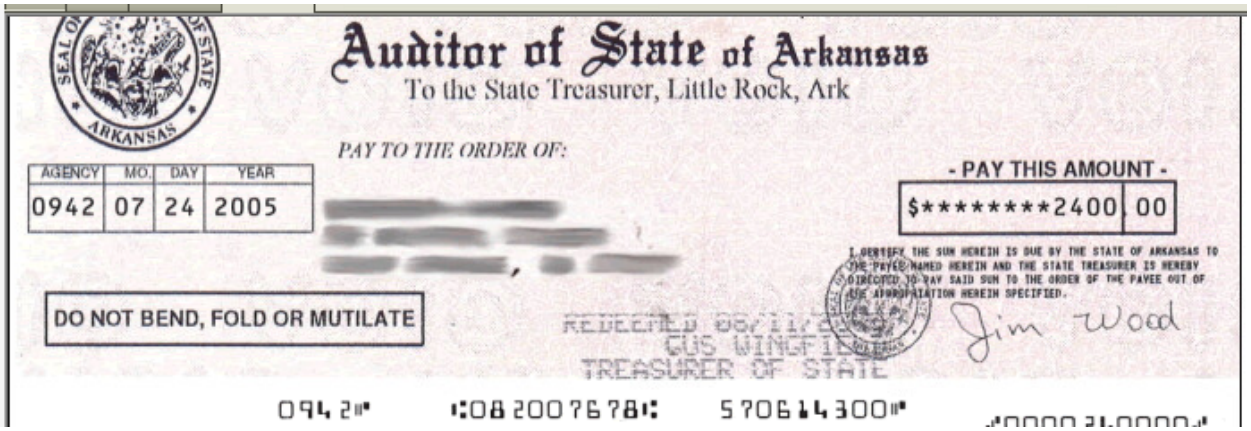
URL	:2007071220070713: Wes Mantooth@http://images.google.com/images?um=1&tab=wi&hl=en&q=atm card stealing
file:	
user name:	
response:	
accessed time:	7/12/2007 7:15:24 PM -0400
modified time:	7/12/2007 1:15:24 PM -0400
expiration time:	8/7/2007 7:15:26 PM -0400
hits:	1
use counts:	0

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 Iborders 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.

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			

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.