ITIS 5250
Sneha Rangari
Semester Project
12/04/2018

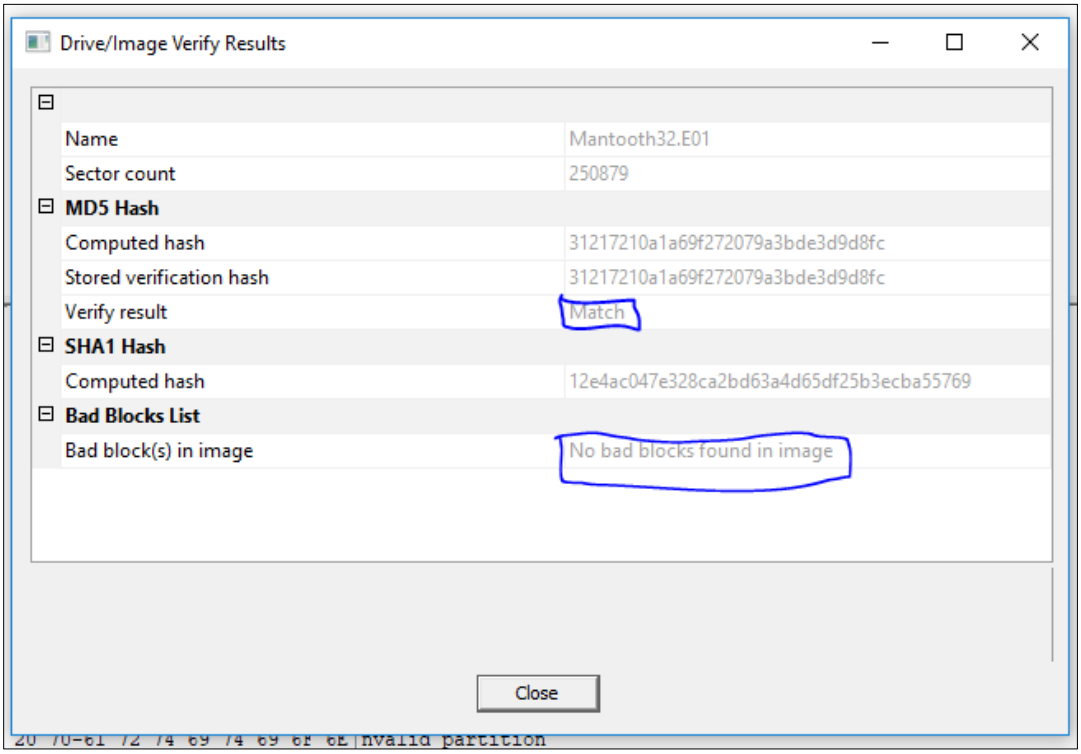
Overview:

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

Forensic Acquisition & Exam Preparation:

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

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

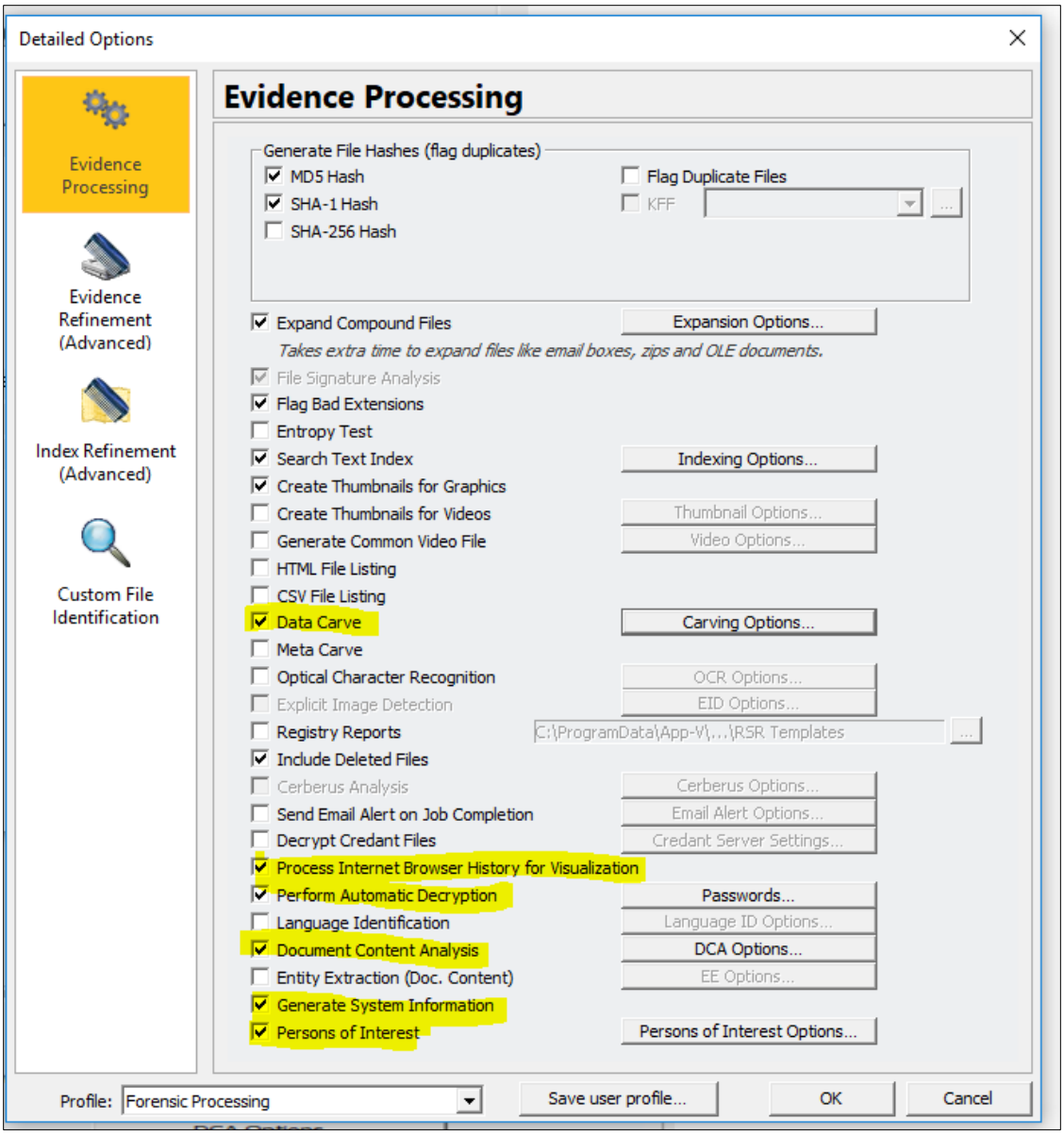


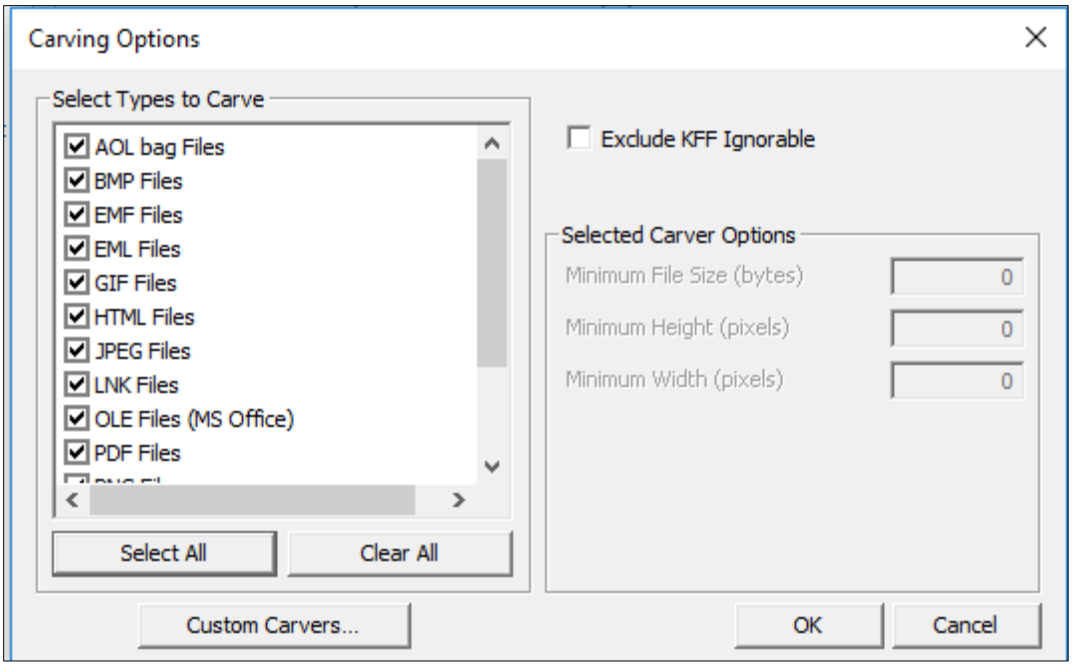
The above result show that this image was not tampered and then using FTK.
I customized processing profile by adding options:

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

In Carving options, I selected all types to Carve.

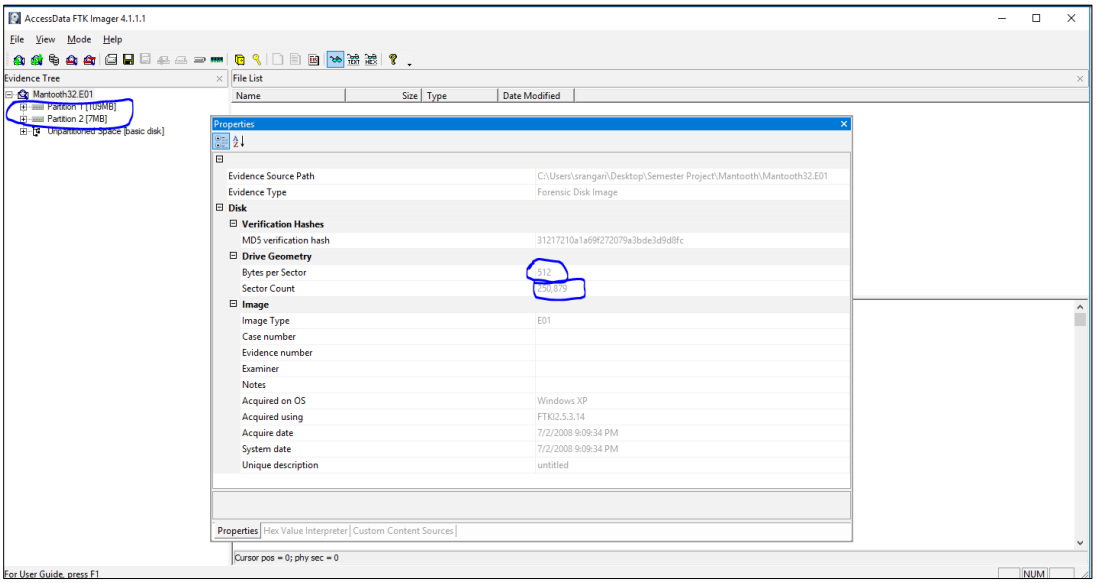
I processed them as shown:


Detailed Options
Evidence Processing
Evidence Refinement (Advanced)
Index Refinement (Advanced)
Custom File Identification
Evidence Processing
Generate File Hashes (flag duplicates)
MD5 Hash
SHA-1 Hash
SHA-256 Hash
Flag Duplicate Files
KFF
Expand Compound Files
Expansion Options...
Takes extra time to expand files like email boxes, zips and OLE documents.
File Signature Analysis
Flag Bad Extensions
Entropy Test
Search Text Index
Indexing Options...
Create Thumbnails for Graphics
Create Thumbnails for Videos
Thumbnail Options...
Generate Common Video File
Video Options...
HTML File Listing
CSV File Listing
Data Carve
Carving Options...
Meta Carve
Optical Character Recognition
OCR Options...
Explicit Image Detection
EID Options...
Registry Reports
C:\ProgramData\App-V\...\RSR Templates
Include Deleted Files
Cerberus Analysis
Cerberus Options...
Send Email Alert on Job Completion
Email Alert Options...
Decrypt Credant Files
Credant Server Settings...
Process Internet Browser History for Visualization
Perform Automatic Decryption
Passwords...
Language Identification
Language ID Options...
Document Content Analysis
DCA Options...
Entity Extraction (Doc. Content)
EE Options...
Generate System Information
Persons of Interest
Persons of Interest Options...
Profile:
Forensic Processing
Save user profile...
OK
Cancel



Findings and Report (Forensic Analysis)

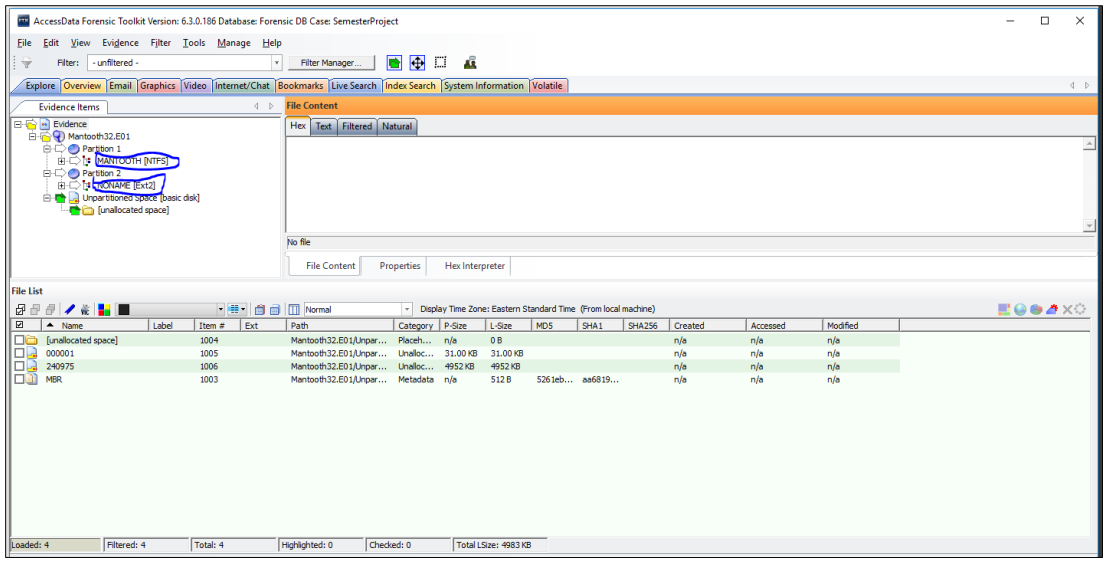
1. Account for how all the space on the computer hard drive was used (partitions, used/free).



The size of the computer hard drive is obtained by considering Drive Geometry in which Bytes per Sector are multiplied by Sector Count. i.e. 512x2,50,879 = 128,450,048 bytes.

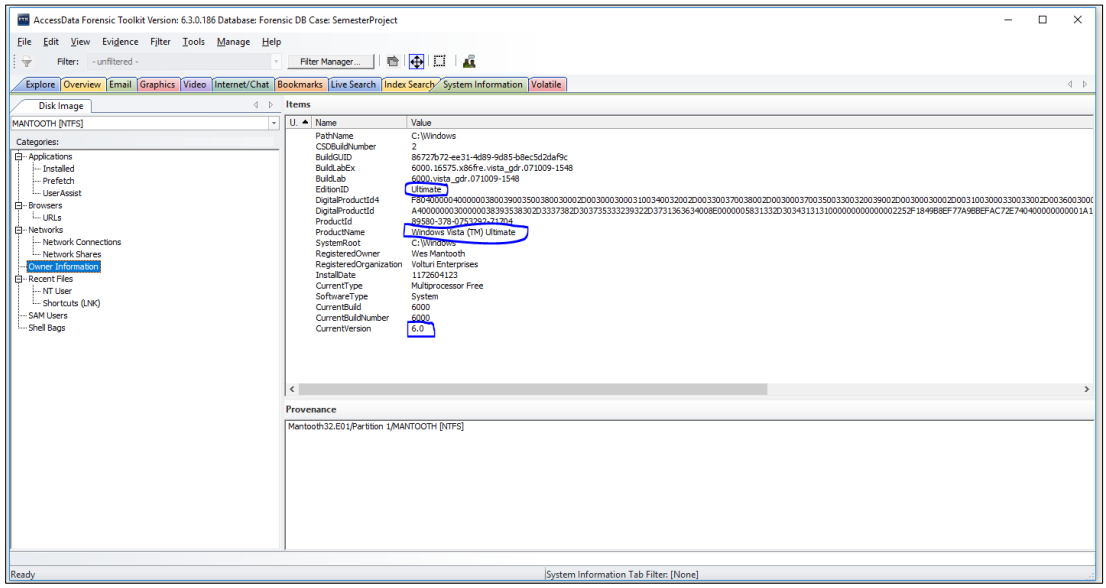
As shown in FTK Imager, total partition comprises of 109MB+7MB = 116 MB which is used.

2. Identify the types of file systems in use.



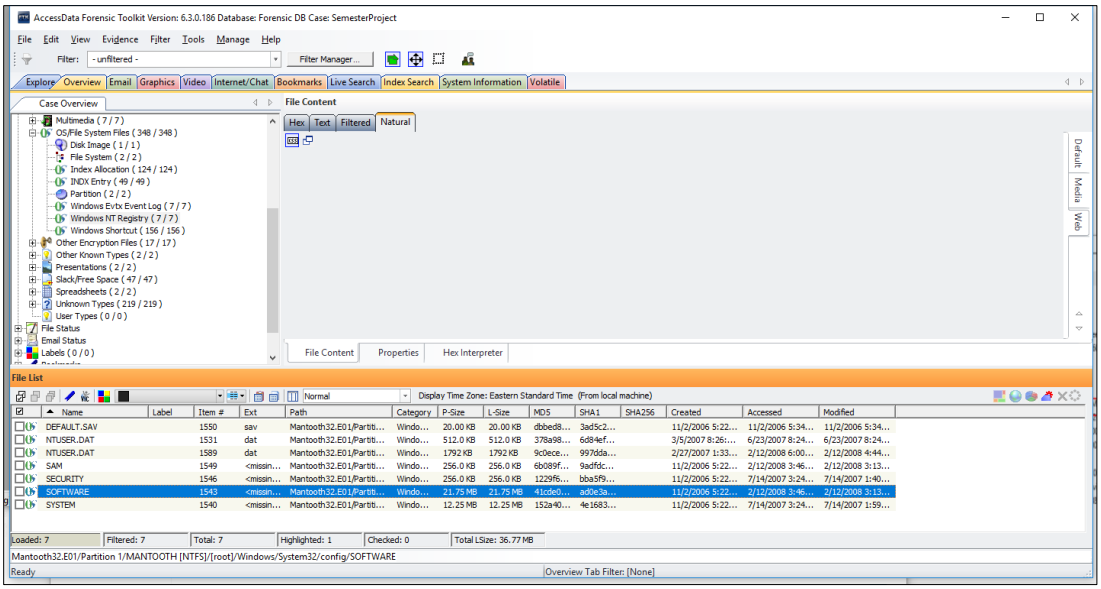
FTK shows two types of file systems in use, which are **NTFS** and **Ext2**.

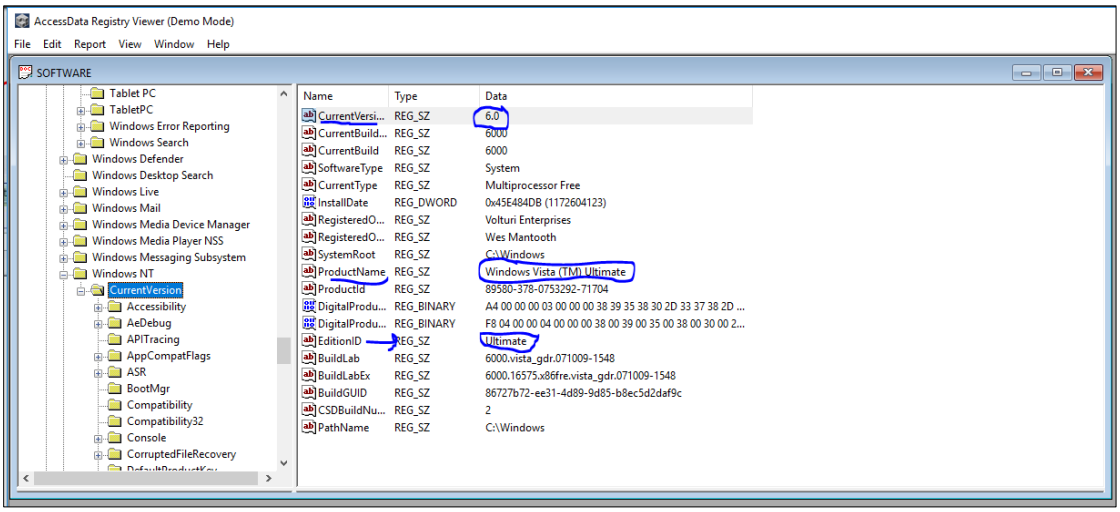
3. Identify the version and service pack of the operating system.



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

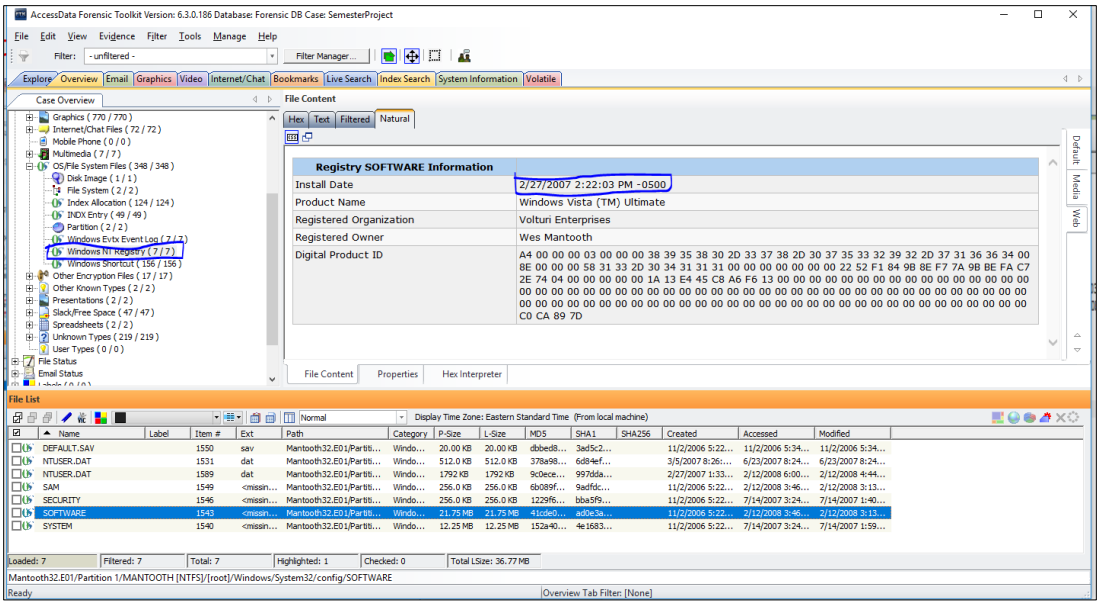
Similar information is evident when **SOFTWARE** file from FTK is exported into "**Registry viewer**" as shown above.

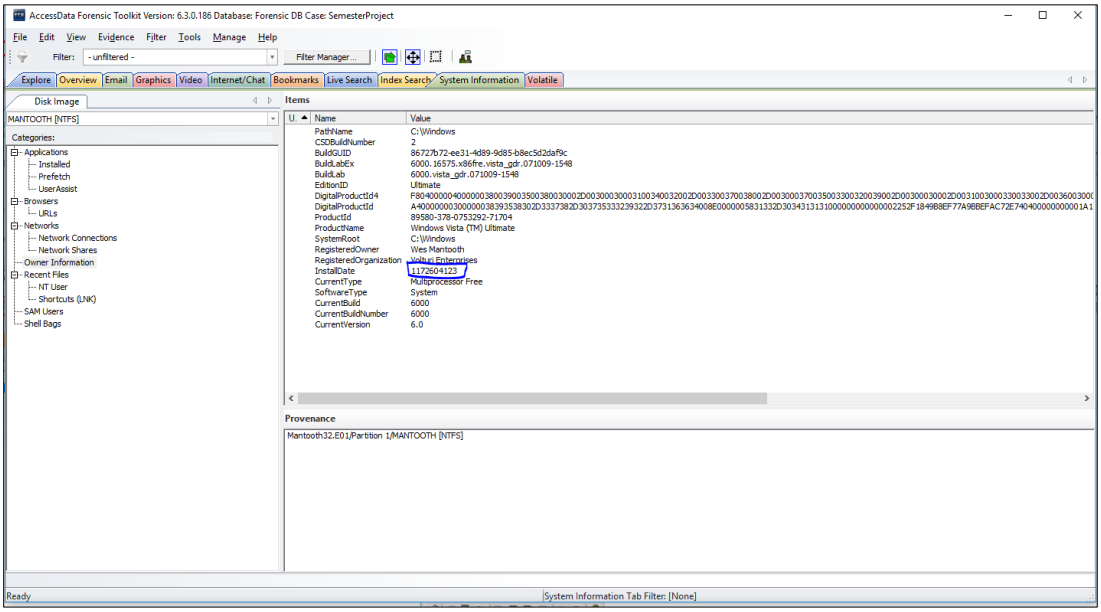




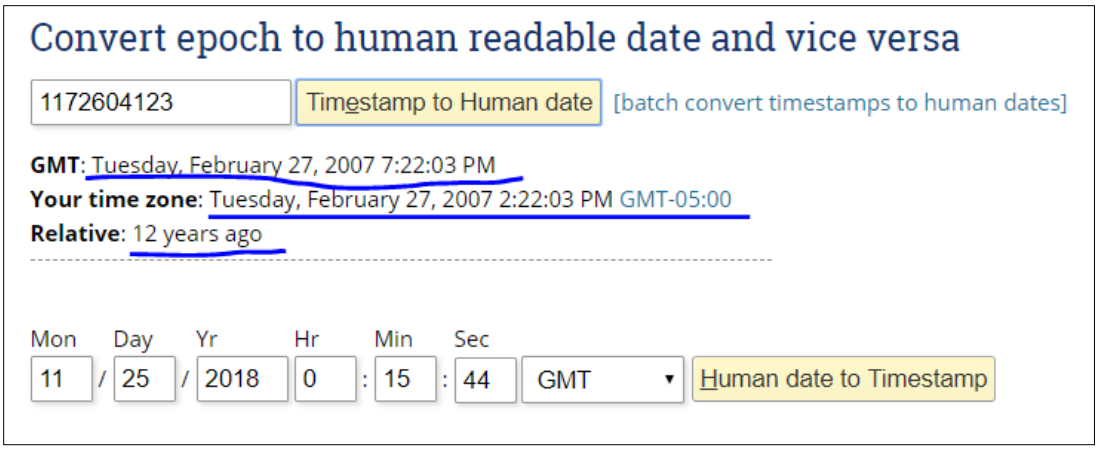
4. Find the date the OS was installed

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

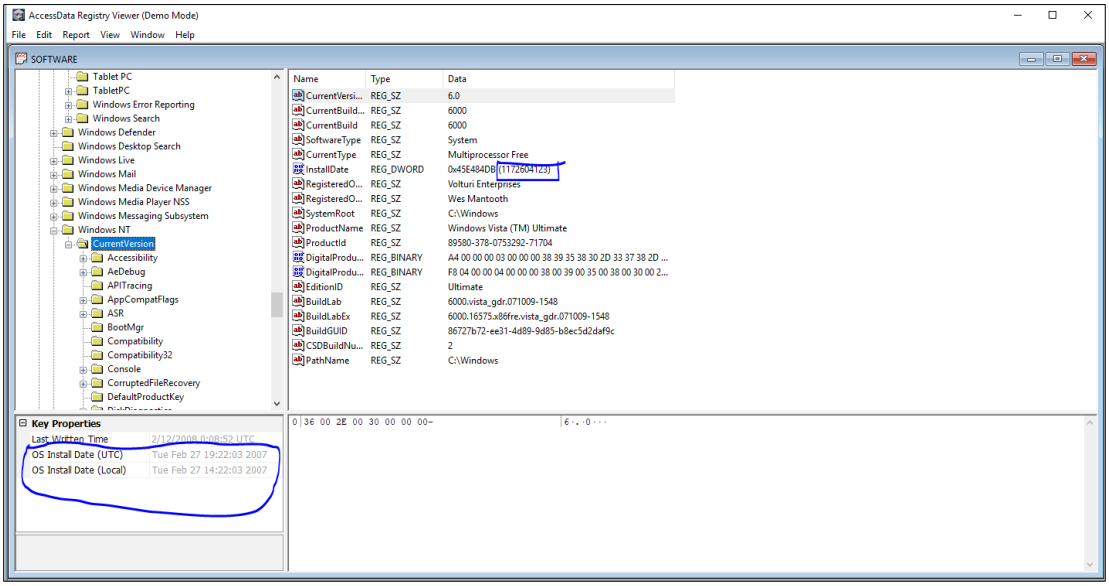




'System Information' in FTK shows epoch timestamp which I converted to human readable time format which also showed the OS was installed on **2/27/2007**

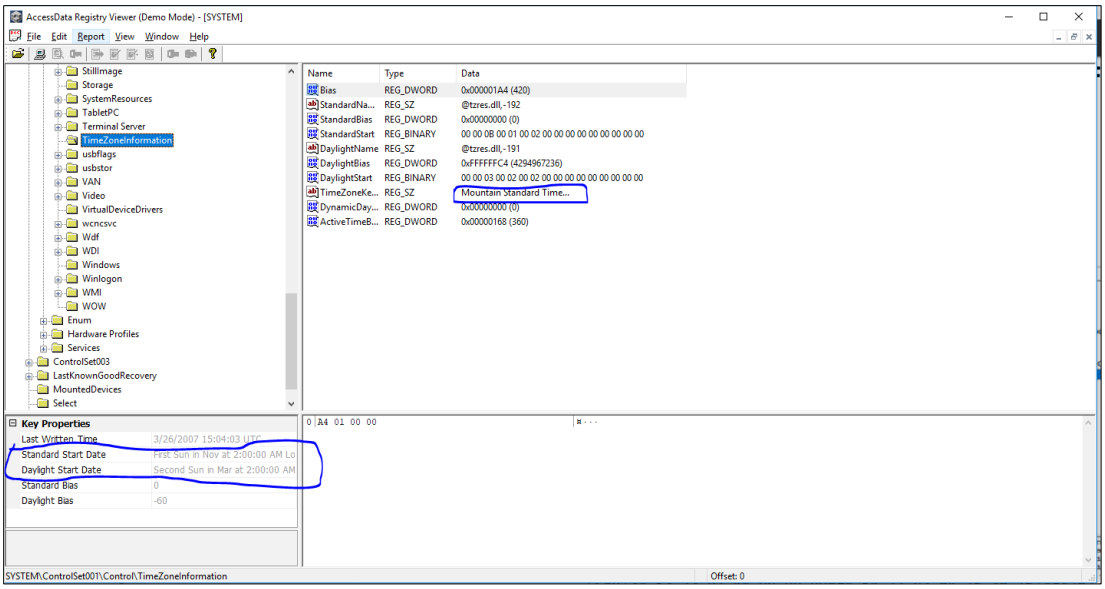


Likewise, when I exported **SOFTWARE** file from FTK into **Access Data's Registry Viewer**, I noticed installation date of the OS is **Tue Feb 27 19:22:03 2007** as shown.

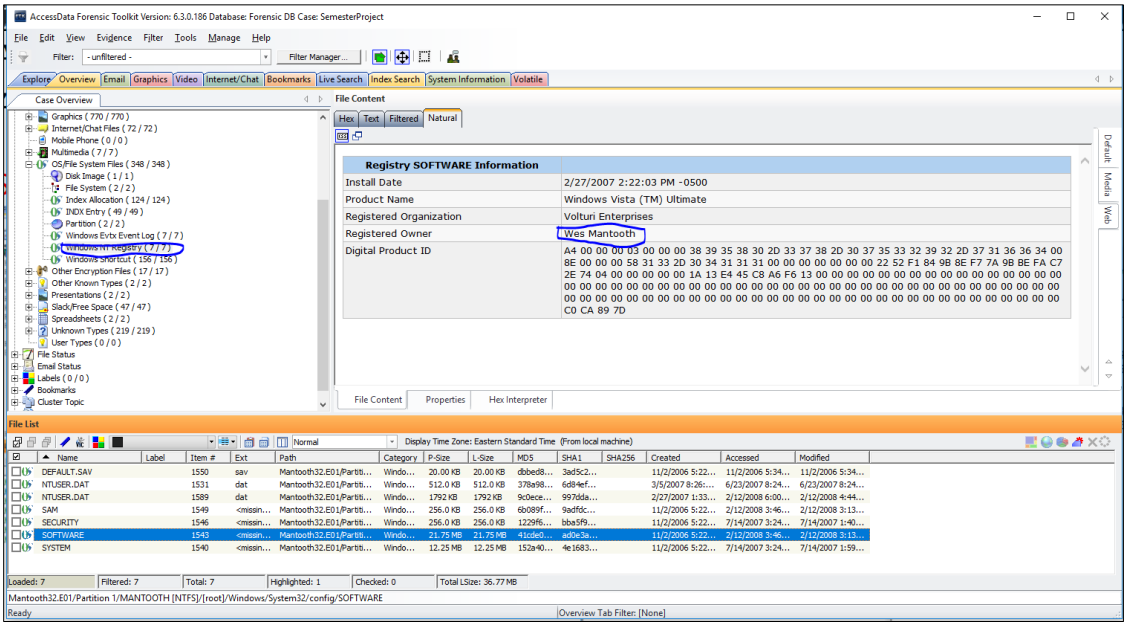


5. Identify the Time Zone information for the computer.

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

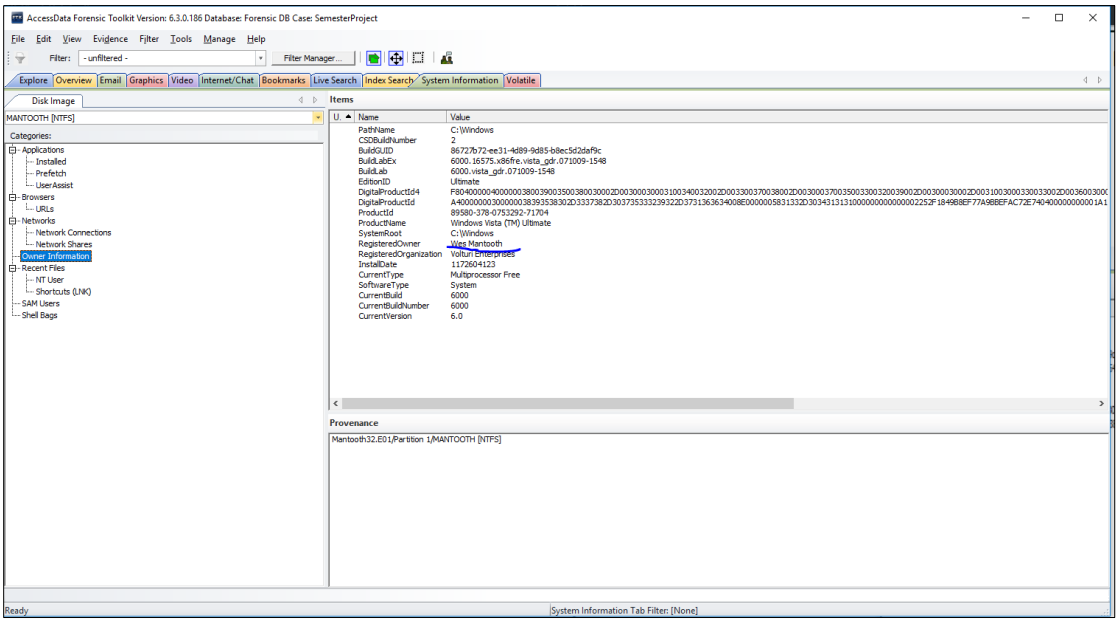


6. Show the owner of the computer.

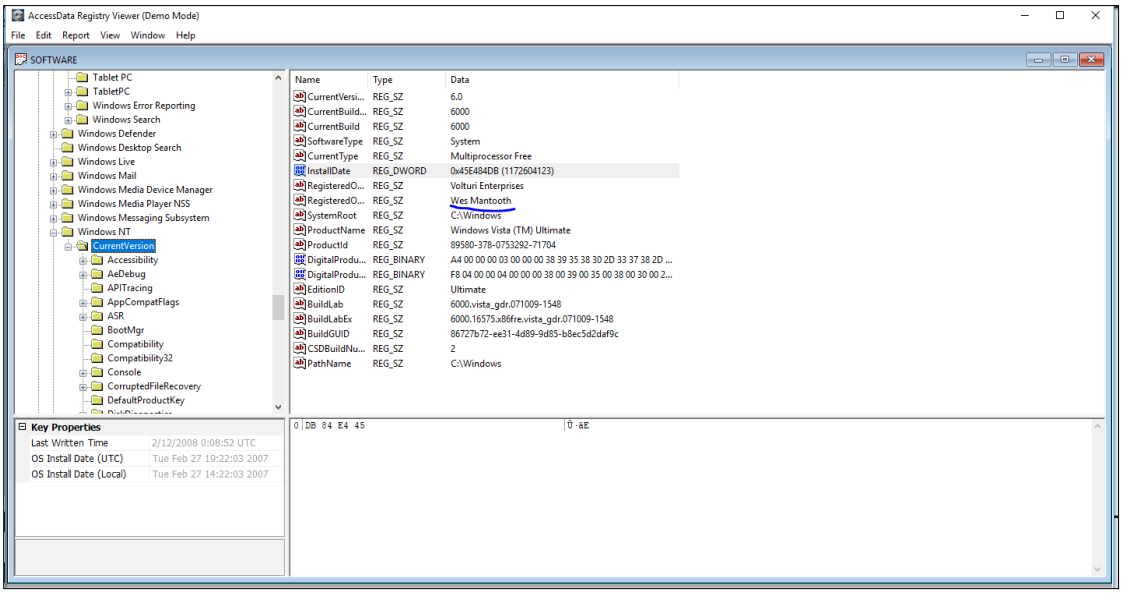


In FTK, the **SOFTWARE** file shows the registered owner of the computer is '**Wes Mantooth**'.

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

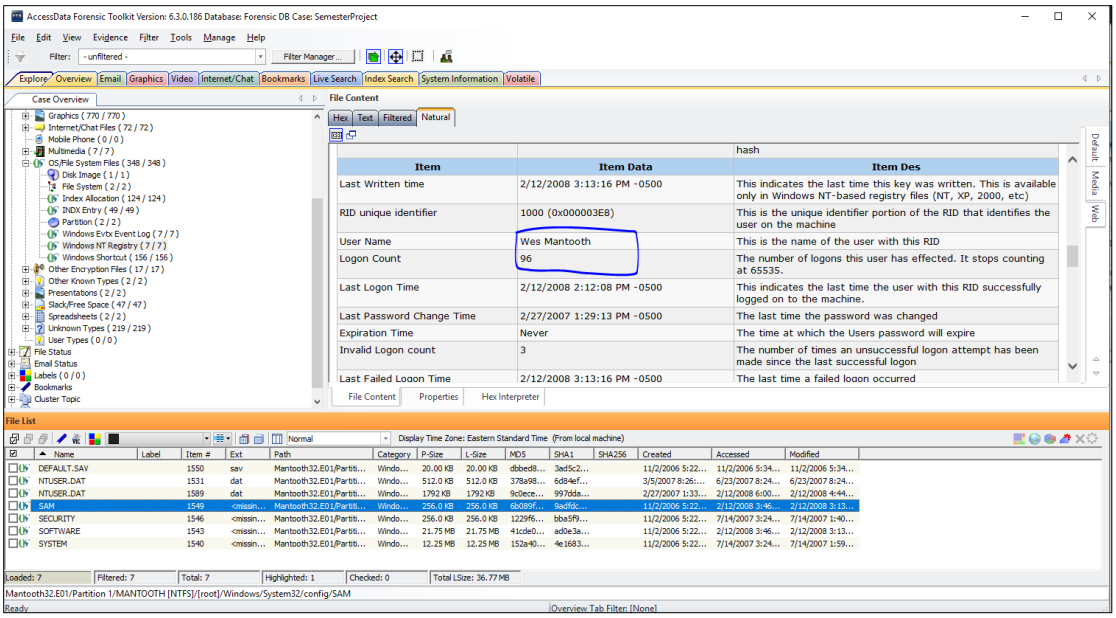


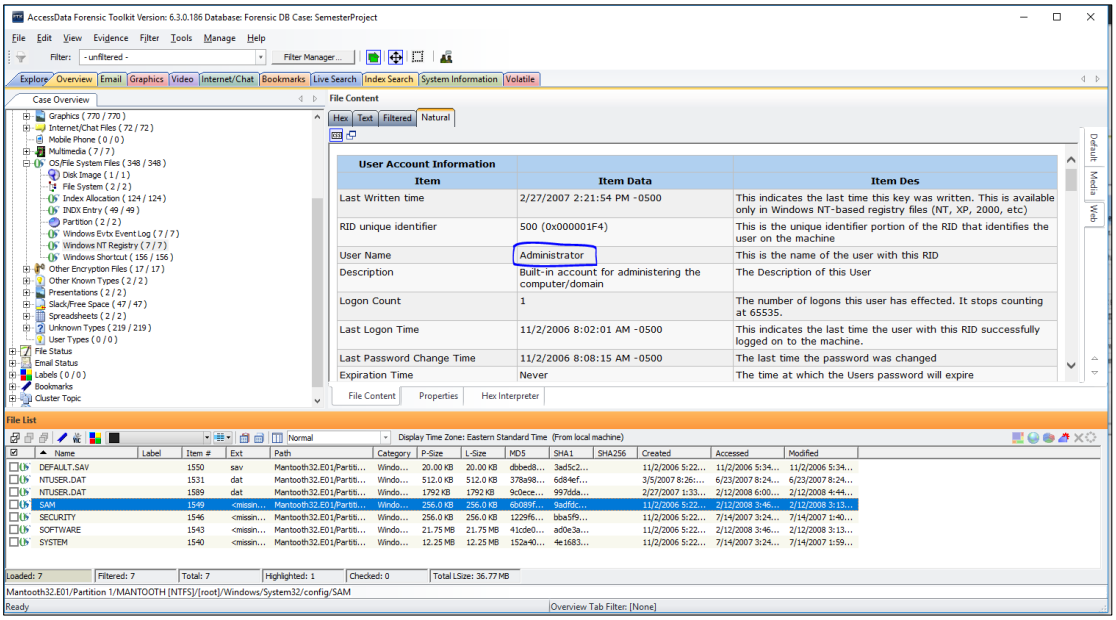
Also, when the SOFTWARE file is exported from FTK to the registry viewer, I noticed the registered owner is named as '**Wes Mantooth**'.

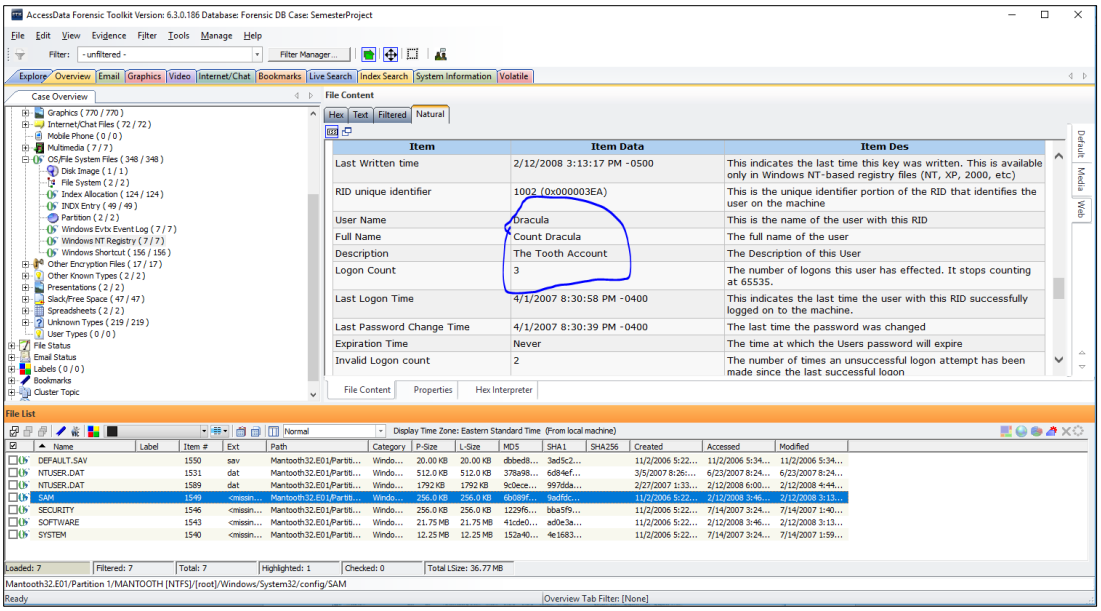


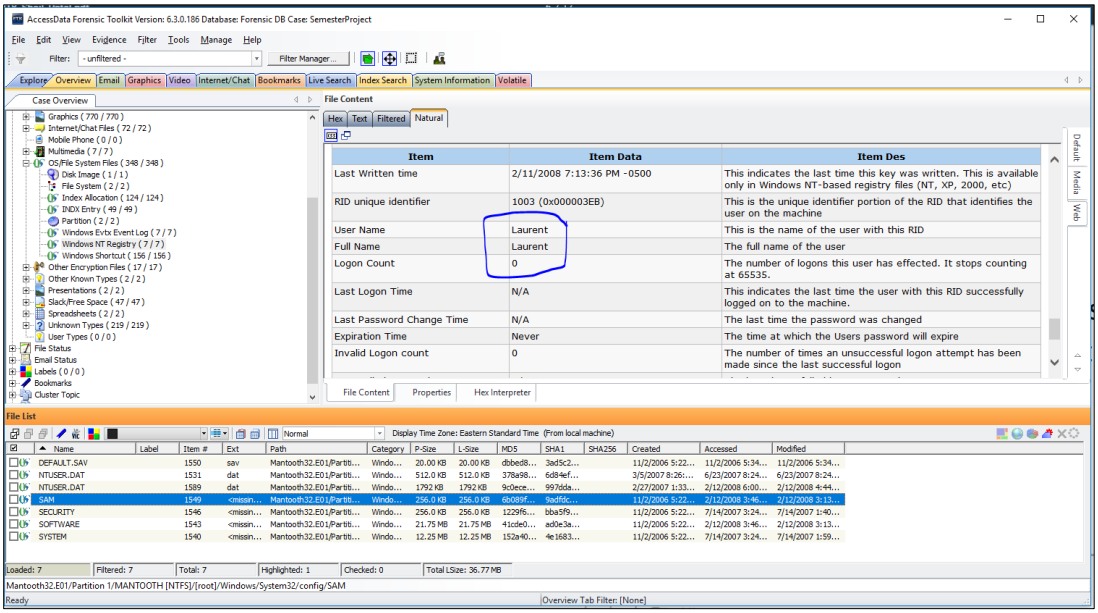
7. Show the most active user of the computer and list all users

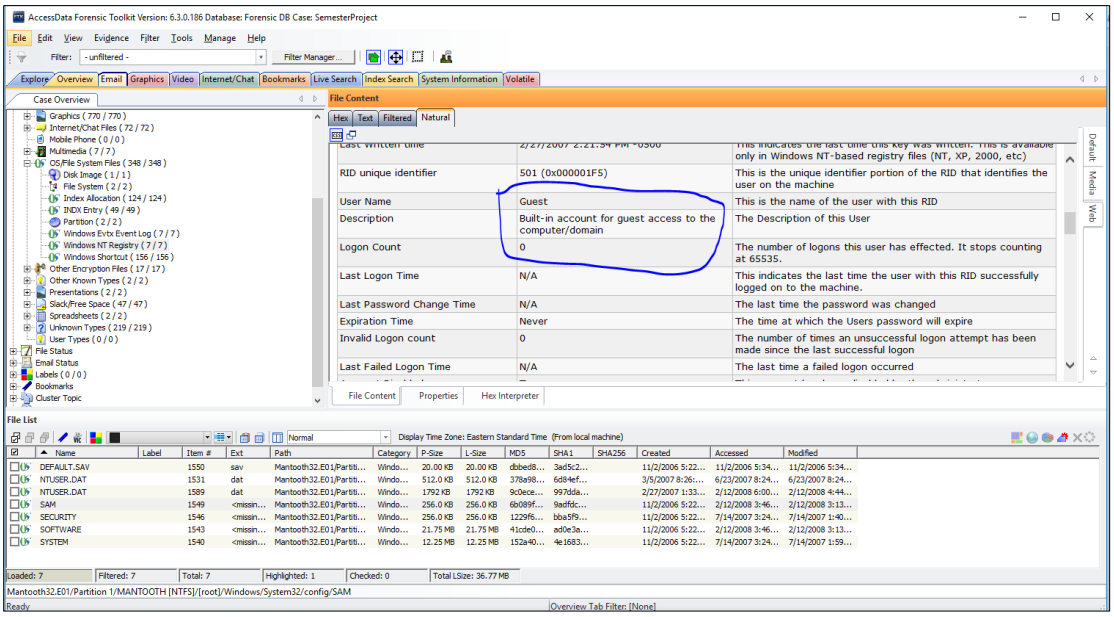
SAM file in FTK displays **Wes Mantooth** has logon count of **96** as compared to other users like Administrator, Guest, Laurent and Dracula whose logon count are 1, 0, 0 and 3 respectively and hence is the most active user as shown.


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
File Content
Hex Text Filtered Natural
hash
Item
Item Data
Item Des
Last Written time
2/12/2008 3:13:16 PM -0500
This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier
1000 (0x000003E8)
This is the unique identifier portion of the RID that identifies the user on the machine
User Name
Wes Mantooth
This is the name of the user with this RID
Logon Count
96
The number of logons this user has effected. It stops counting at 65535.
Last Logon Time
2/12/2008 2:12:08 PM -0500
This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time
2/27/2007 1:29:13 PM -0500
The last time the password was changed
Expiration Time
Never
The time at which the Users password will expire
Invalid Logon count
3
The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time
2/12/2008 3:13:16 PM -0500
The last time a failed logon occurred
File Content
Properties
Hex Interpreter
File List
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/SAM
Ready


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
File Content
Hex Text Filtered Natural
User Account Information
Item
Item Data
Item Des
Last Written time
2/27/2007 2:21:54 PM -0500
This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier
500 (0x000001F4)
This is the unique identifier portion of the RID that identifies the user on the machine
User Name
Administrator
This is the name of the user with this RID
Description
Built-in account for administering the computer/domain
The Description of this User
Logon Count
1
The number of logons this user has effected. It stops counting at 65535.
Last Logon Time
11/2/2006 8:02:01 AM -0500
This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time
11/2/2006 8:08:15 AM -0500
The last time the password was changed
Expiration Time
Never
The time at which the Users password will expire
File Content
Properties
Hex Interpreter
File List
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/SAM
Ready

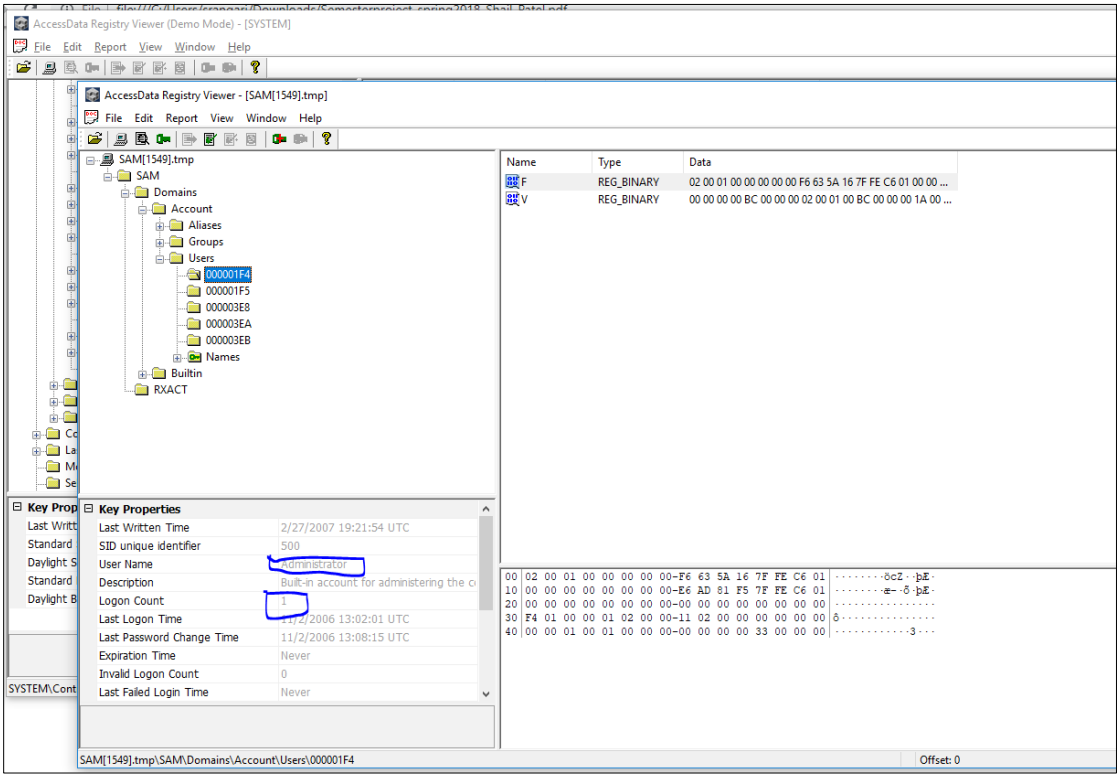

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
File Content
Hex Text Filtered Natural
Item | Item Data | Item Des
Last Written time | 2/12/2008 3:13:17 PM -0500 | This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier | 1002 (0x000003EA) | This is the unique identifier portion of the RID that identifies the user on the machine
User Name | Dracula | This is the name of the user with this RID
Full Name | Count Dracula | The full name of the user
Description | The Tooth Account | The Description of this User
Logon Count | 3 | The number of logons this user has effected. It stops counting at 65535.
Last Logon Time | 4/1/2007 8:30:58 PM -0400 | This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time | 4/1/2007 8:30:39 PM -0400 | The last time the password was changed
Expiration Time | Never | The time at which the Users password will expire
Invalid Logon count | 2 | The number of times an unsuccessful logon attempt has been made since the last successful logon
File Content Properties Hex Interpreter
File List
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/SAM
Ready
Overview Tab Filter: [None]

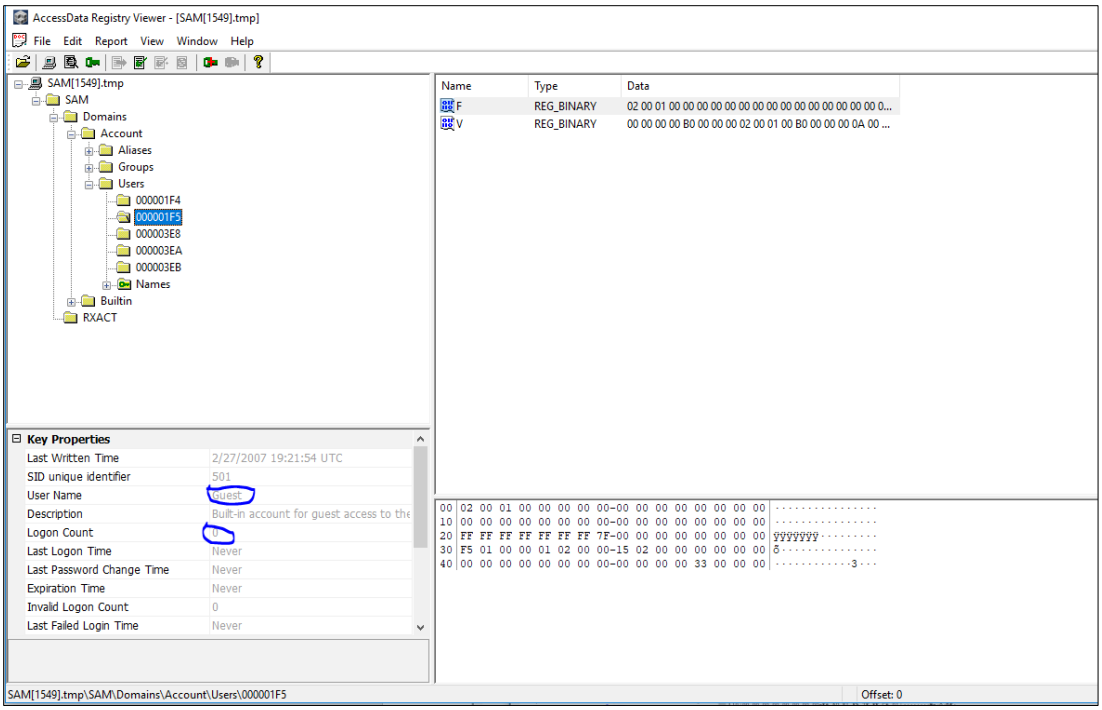

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
File Content
Hex Text Filtered Natural
Item | Item Data | Item Des
Last Written time | 2/11/2008 7:13:36 PM -0500 | This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier | 1003 (0x000003EB) | This is the unique identifier portion of the RID that identifies the user on the machine
User Name | Laurent | This is the name of the user with this RID
Full Name | Laurent | The full name of the user
Logon Count | 0 | The number of logons this user has effected. It stops counting at 65535.
Last Logon Time | N/A | This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time | N/A | The last time the password was changed
Expiration Time | Never | The time at which the Users password will expire
Invalid Logon count | 0 | The number of times an unsuccessful logon attempt has been made since the last successful logon
File Content Properties Hex Interpreter
File List
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/SAM
Ready
Overview Tab Filter: [None]

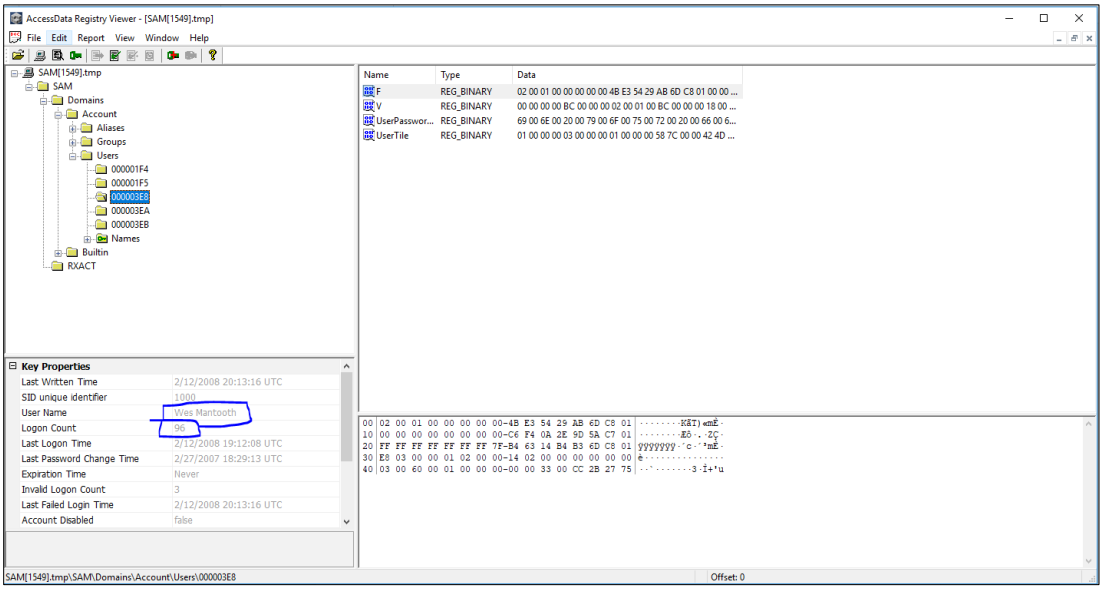


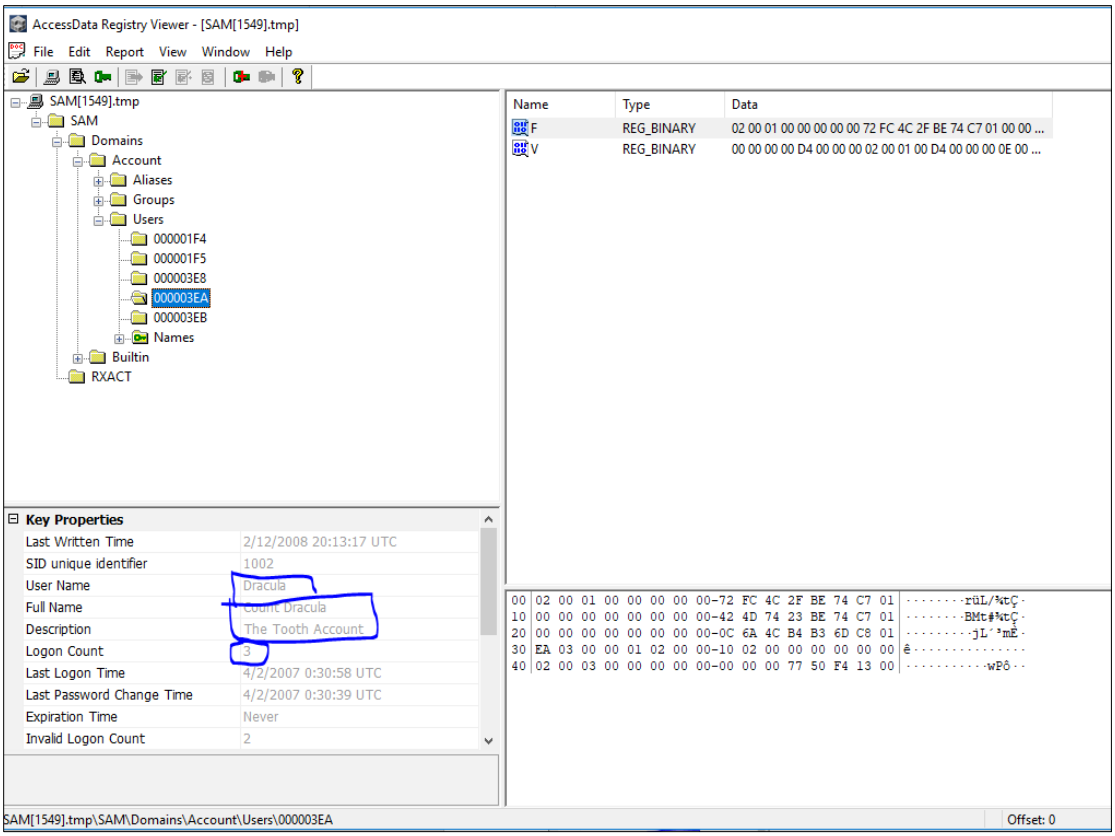
8. Identify user accounts and who uses the account.

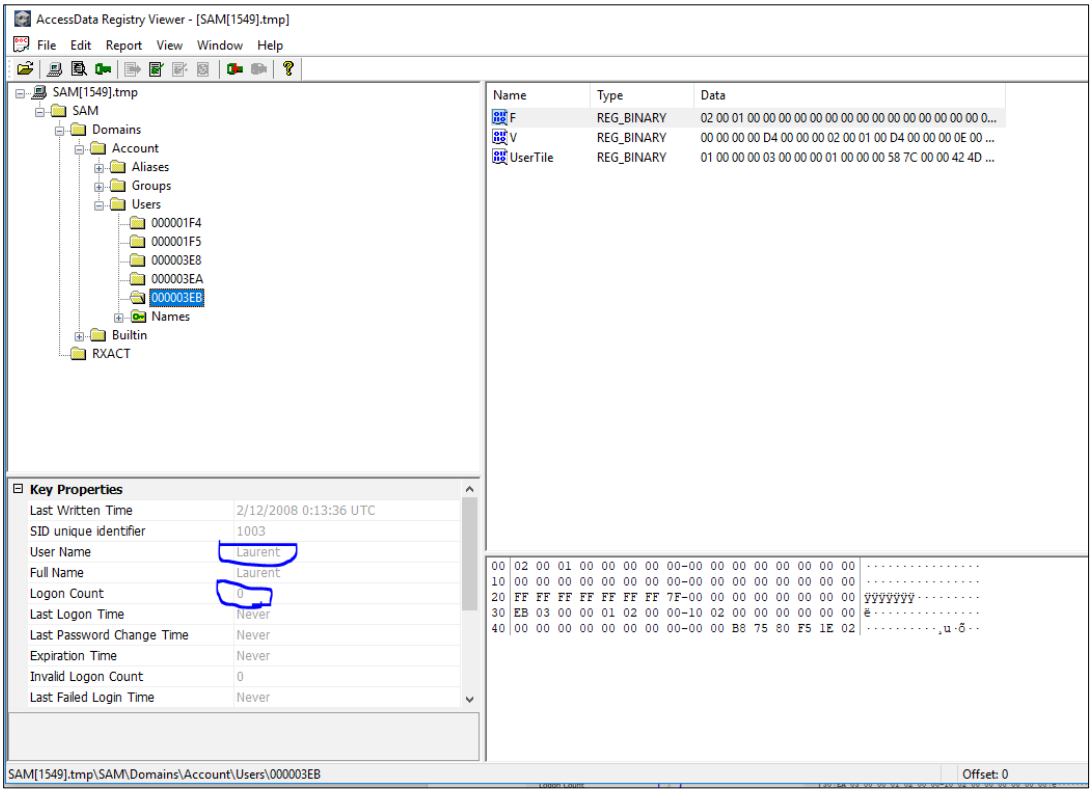
Exporting **SAM** file into registry viewer shows, user accounts are **Wes Mantooth, Dracula** and **Laurent, Administrator and Guest**. Their account disabled status is false. Amongst them, Wes Mantooth and Dracula uses their account since their logon count are 96 and 3 respectively as shown in “Key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




AccessData Registry Viewer - [SAM[1549].tmp]
File Edit Report View Window Help
SAM[1549].tmp
SAM
Domains
Account
Aliases
Groups
Users
000001F4
000001F5
000003E8
000003EA
000003EB
Names
Builtin
RXACT
Name Type Data
F REG_BINARY 02 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0...
V REG_BINARY 00 00 00 00 B0 00 00 00 02 00 01 00 B0 00 00 00 0A 00 ...
Key Properties
Last Written Time 2/27/2007 19:21:54 UTC
SID unique identifier 501
User Name Guest
Description Built-in account for guest access to the
Logon Count 0
Last Logon Time Never
Last Password Change Time Never
Expiration Time Never
Invalid Logon Count 0
Last Failed Login Time Never
SAM[1549].tmp\SAM\Domains\Account\Users\000001F5
Offset: 0

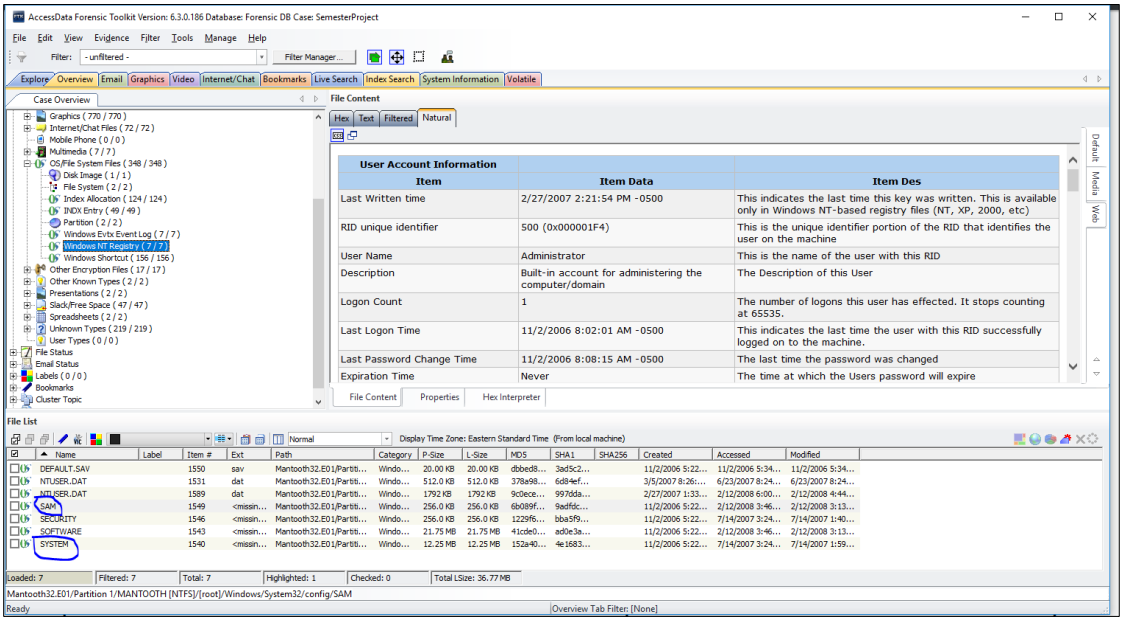

AccessData Registry Viewer - [SAM[1549].tmp]
File Edit Report View Window Help
SAM[1549].tmp
SAM
Domains
Account
Aliases
Groups
Users
000001F4
000001F5
000003E8
000003EA
000003EB
Names
Builtin
RXACT
Name Type Data
F REG_BINARY 02 00 01 00 00 00 00 00 4B E3 54 29 AB 6D C8 01 00 00 ...
V REG_BINARY 00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 18 00 ...
UserPasswor... REG_BINARY 69 00 6E 00 20 00 79 00 6F 00 75 00 72 00 20 00 66 00 6...
UserTile REG_BINARY 01 00 00 00 03 00 00 00 01 00 00 00 58 7C 00 00 42 4D ...
Key Properties
Last Written Time 2/12/2008 20:13:16 UTC
SID unique identifier 1000
User Name Wes Mantooth
Logon Count 96
Last Logon Time 2/12/2008 19:12:08 UTC
Last Password Change Time 2/27/2007 18:29:13 UTC
Expiration Time Never
Invalid Logon Count 3
Last Failed Login Time 2/12/2008 20:13:16 UTC
Account Disabled false
SAM[1549].tmp\SAM\Domains\Account\Users\000003E8
Offset: 0

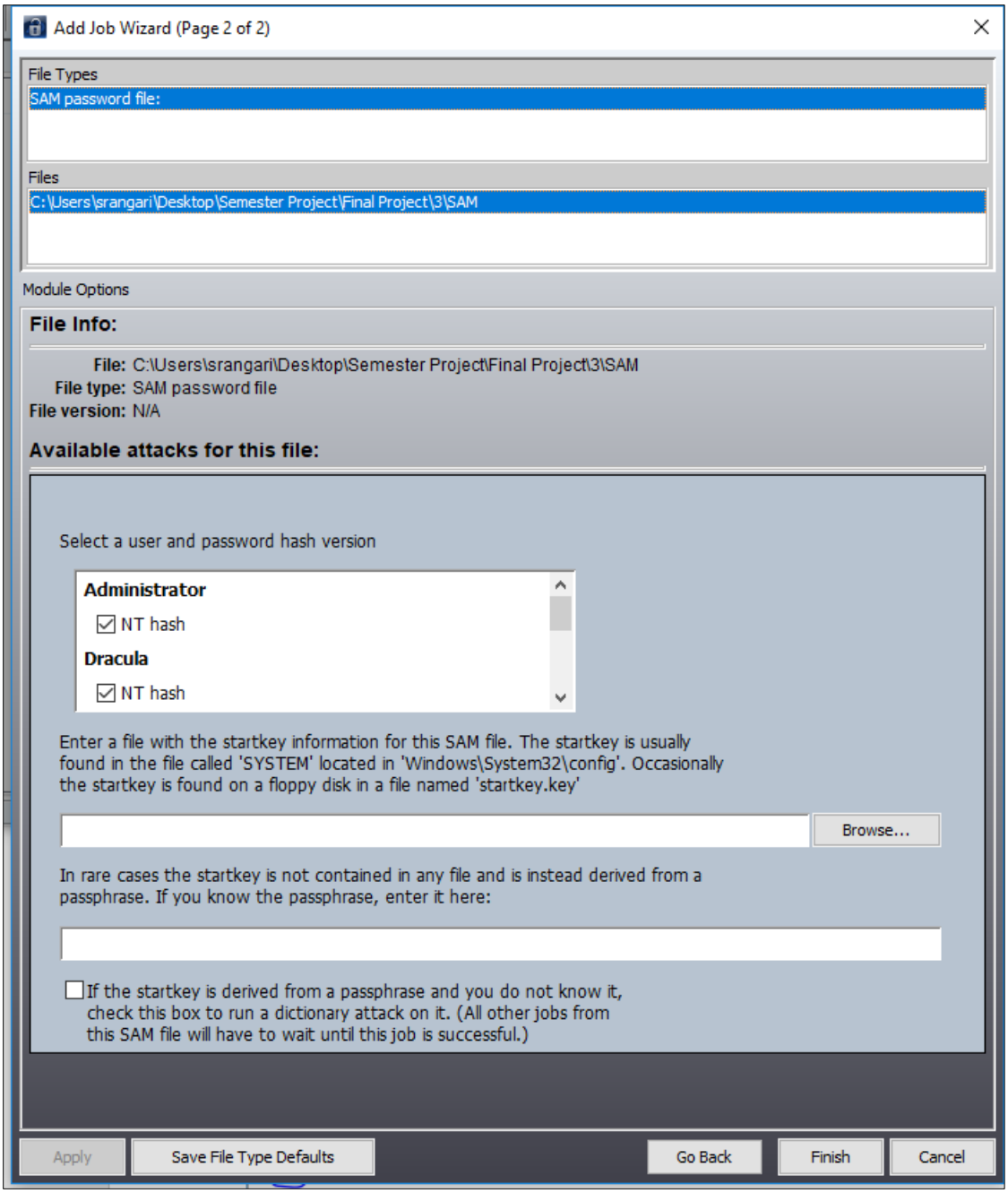

AccessData Registry Viewer - [SAM[1549].tmp]
File Edit Report View Window Help
SAM[1549].tmp
SAM
Domains
Account
Aliases
Groups
Users
000001F4
000001F5
000003E8
000003EA
000003EB
Names
Builtin
RXACT
Name Type Data
F REG_BINARY 02 00 01 00 00 00 00 00 72 FC 4C 2F BE 74 C7 01 00 00 ...
V REG_BINARY 00 00 00 00 D4 00 00 00 02 00 01 00 D4 00 00 00 0E 00 ...
Key Properties
Last Written Time 2/12/2008 20:13:17 UTC
SID unique identifier 1002
User Name Dracula
Full Name Count Dracula
Description The Tooth Account
Logon Count 3
Last Logon Time 4/2/2007 0:30:58 UTC
Last Password Change Time 4/2/2007 0:30:39 UTC
Expiration Time Never
Invalid Logon Count 2
00 02 00 01 00 00 00 00 00-72 FC 4C 2F BE 74 C7 01
10 00 00 00 00 00 00 00 00-42 4D 74 23 BE 74 C7 01
20 00 00 00 00 00 00 00 00-0C 6A 4C B4 B3 6D C8 01
30 EA 03 00 00 01 02 00 00-10 02 00 00 00 00 00 00
40 02 00 03 00 00 00 00 00-00 00 00 77 50 F4 13 00
SAM[1549].tmp\SAM\Domains\Account\Users\000003EA
Offset: 0

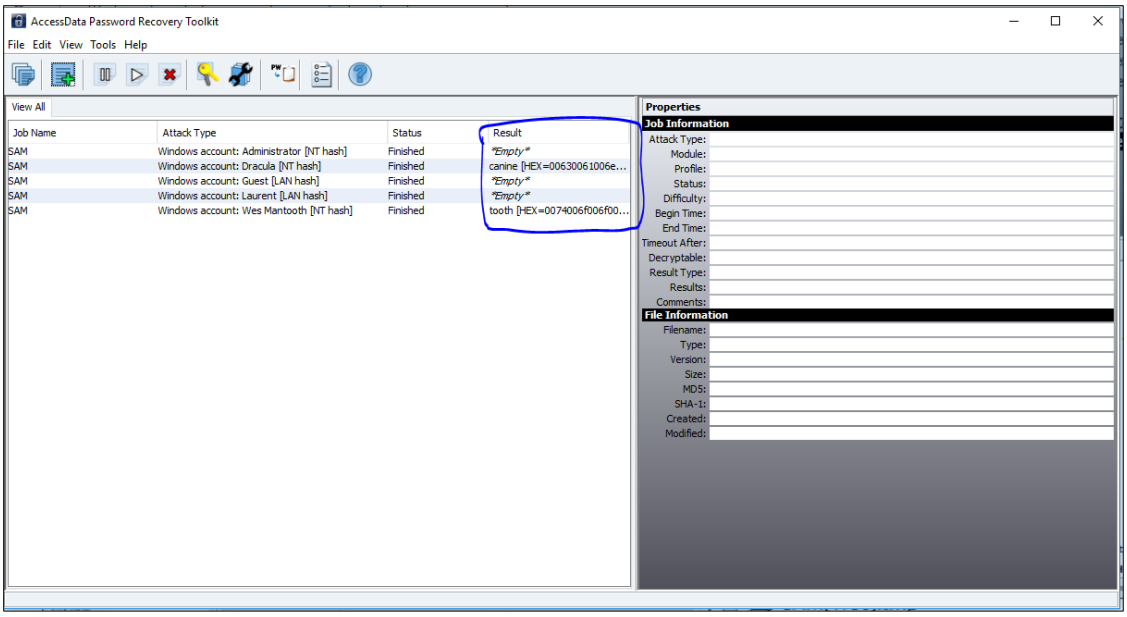

AccessData Registry Viewer - [SAM[1549].tmp]
File Edit Report View Window Help
SAM[1549].tmp
SAM
Domains
Account
Aliases
Groups
Users
000001F4
000001F5
000003E8
000003EA
000003EB
Names
Builtin
RXACT
Name Type Data
F REG_BINARY 02 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0...
V REG_BINARY 00 00 00 00 D4 00 00 00 02 00 01 00 D4 00 00 00 0E 00 ...
UserTile REG_BINARY 01 00 00 00 03 00 00 00 01 00 00 00 58 7C 00 00 42 4D ...
Key Properties
Last Written Time 2/12/2008 0:13:36 UTC
SID unique identifier 1003
User Name Laurent
Full Name Laurent
Logon Count 0
Last Logon Time Never
Last Password Change Time Never
Expiration Time Never
Invalid Logon Count 0
Last Failed Login Time Never
00 02 00 01 00 00 00 00 00-00 00 00 00 00 00 00 00
10 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
20 FF FF FF FF FF FF FF 7F-00 00 00 00 00 00 00 00
30 EB 03 00 00 01 02 00 00-10 02 00 00 00 00 00 00
40 00 00 00 00 00 00 00 00-00 00 B8 75 80 F5 1E 02
SAM[1549].tmp\SAM\Domains\Account\Users\000003EB
Offset: 0

9. Acquire user passwords.

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

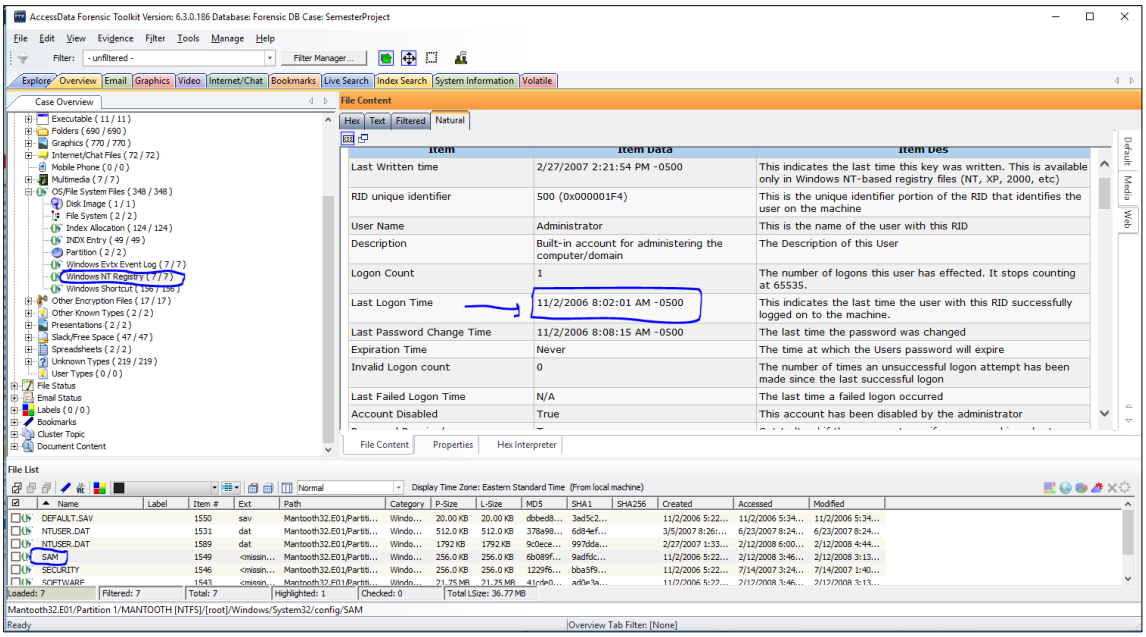



Add Job Wizard (Page 2 of 2)
File Types
SAM password file:
Files
C:\Users\srangari\Desktop\Semester Project\Final Project\3\SAM
Module Options
File Info:
File: C:\Users\srangari\Desktop\Semester Project\Final Project\3\SAM
File type: SAM password file
File version: N/A
Available attacks for this file:
Select a user and password hash version
Administrator
NT hash
Dracula
NT hash
Enter a file with the startkey information for this SAM file. The startkey is usually found in the file called 'SYSTEM' located in 'Windows\System32\config'. Occasionally the startkey is found on a floppy disk in a file named 'startkey.key'
Browse...
In rare cases the startkey is not contained in any file and is instead derived from a passphrase. If you know the passphrase, enter it here:
If the startkey is derived from a passphrase and you do not know it, check this box to run a dictionary attack on it. (All other jobs from this SAM file will have to wait until this job is successful.)
Apply
Save File Type Defaults
Go Back
Finish
Cancel

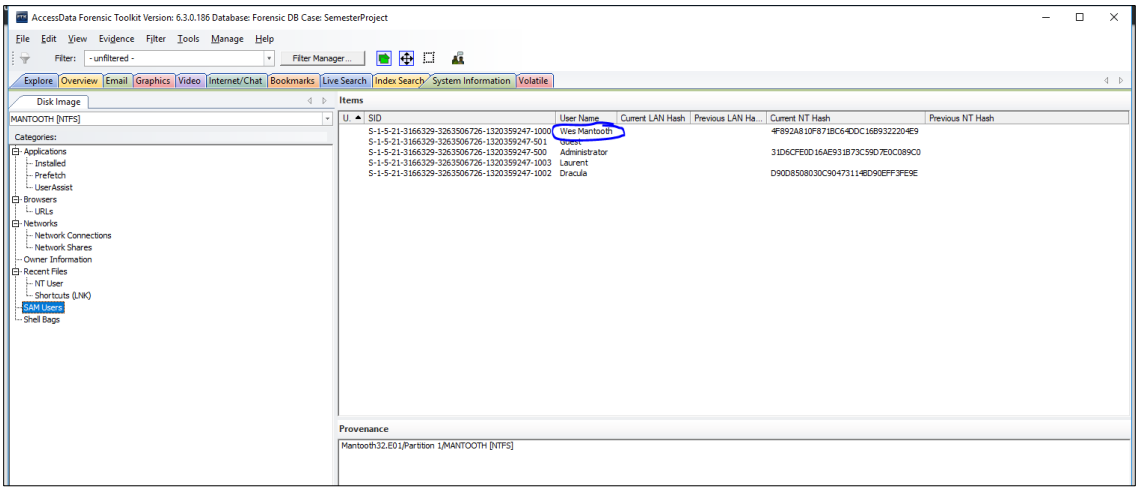


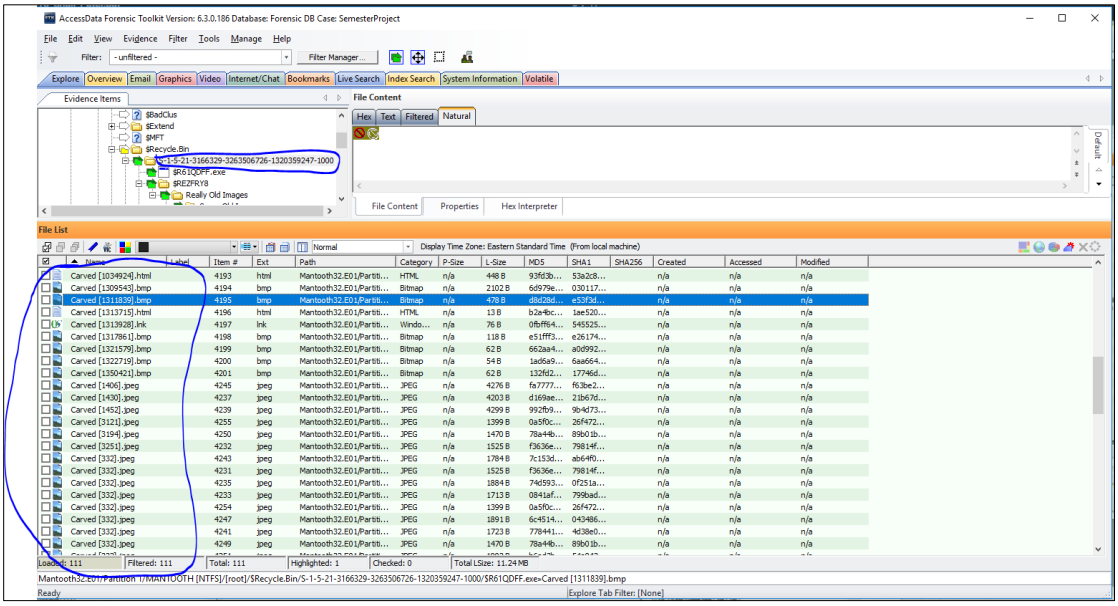
10. Identify the last date Wes Mantooth logged on.

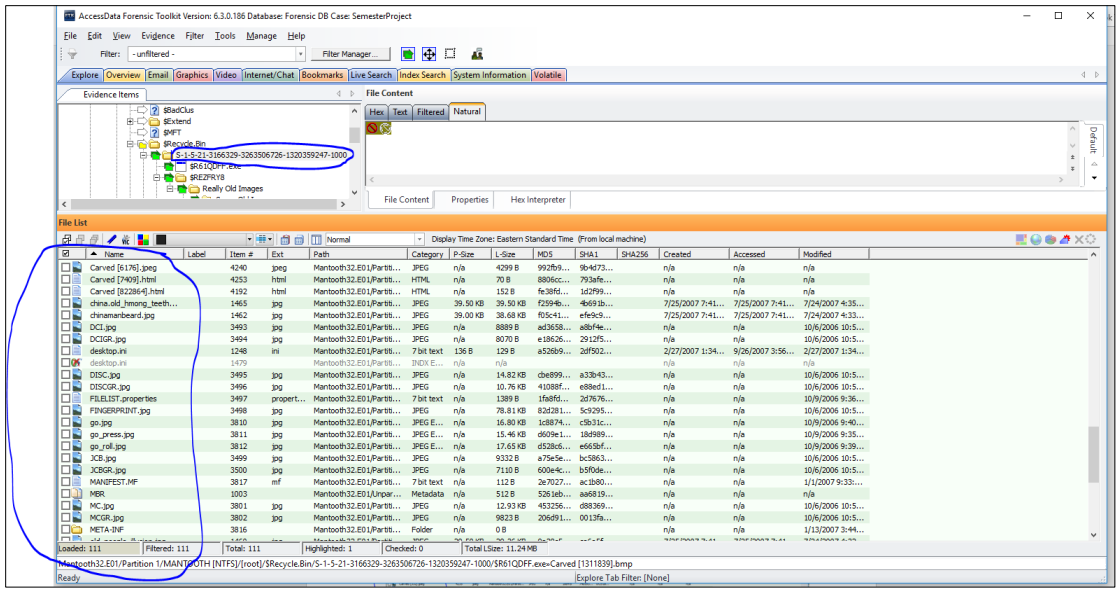
SAM file delineates last logon date of Wes Mantooth was **2/12/2008** as shown in below screenshot.

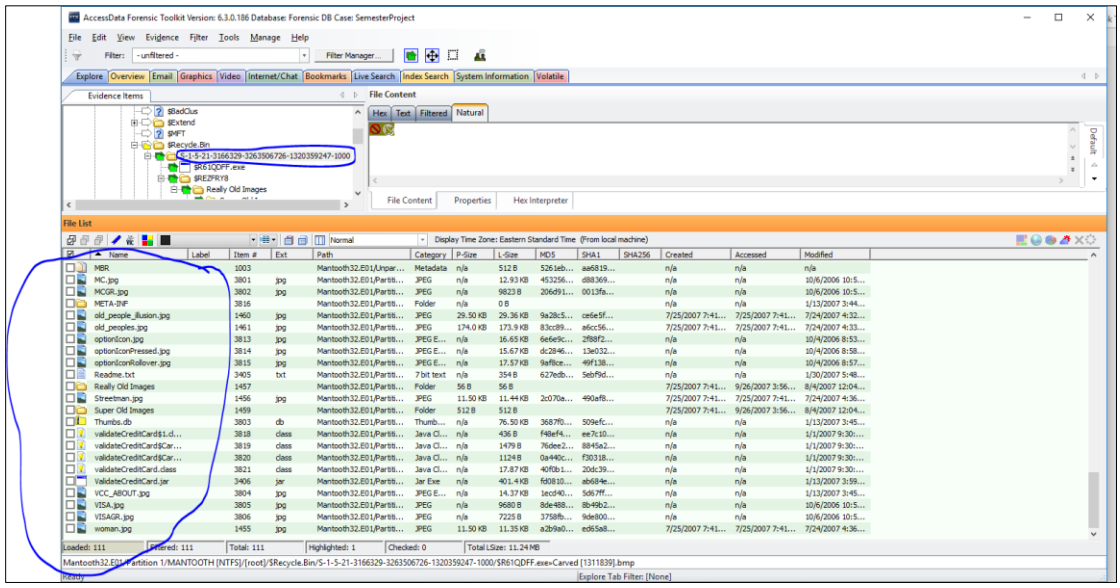


11. Identify files placed in the recycle bin by Wes Mantooth.


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Disk Image
MANTOOTH [NTFS]
Categories:
Applications
Installed
Prefetch
UserAssist
Browsers
URLs
Networks
Network Connections
Network Shares
Owner Information
Recent Files
NT User
Shortcuts (LNK)
SAM Users
Shell Bags
Items
U.
SID
User Name
Current LAN Hash
Previous LAN Ha...
Current NT Hash
Previous NT Hash
S-1-5-21-3166329-3263506726-1320359247-1000 Wes Mantooth 4F892A810F871BC64DDC16B9322204E9
S-1-5-21-3166329-3263506726-1320359247-501 Guest
S-1-5-21-3166329-3263506726-1320359247-500 Administrator 31D6CFE0D16AE931B73C59D7E0C089C0
S-1-5-21-3166329-3263506726-1320359247-1003 Laurent
S-1-5-21-3166329-3263506726-1320359247-1002 Dracula D90D8508030C90473114BD90EFF3FE9E
Provenance
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Evidence Items
$BadClus
$Extend
$MFT
$Recycle.Bin
S-1-5-21-3166329-3263506726-1320359247-1000
$R61QDFF.exe
$REZFRY8
Really Old Images
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Display Time Zone: Eastern Standard Time (From local machine)
Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256 Created Accessed Modified
Carved [1034924].html 4193 html Mantooth32.E01/Partiti... HTML n/a 448 B 93fd3b... 53a2c8... n/a n/a n/a
Carved [1309543].bmp 4194 bmp Mantooth32.E01/Partiti... Bitmap n/a 2102 B 6d979e... 030117... n/a n/a n/a
Carved [1311839].bmp 4195 bmp Mantooth32.E01/Partiti... Bitmap n/a 478 B d8d28d... e53f5f... n/a n/a n/a
Carved [1313715].html 4196 html Mantooth32.E01/Partiti... HTML n/a 13 B b2a4bc... 1ae520... n/a n/a n/a
Carved [1313928].lnk 4197 lnk Mantooth32.E01/Partiti... Windo... n/a 76 B 0fbff64... 545525... n/a n/a n/a
Carved [1317861].bmp 4198 bmp Mantooth32.E01/Partiti... Bitmap n/a 118 B e51fff3... e26174... n/a n/a n/a
Carved [1321579].bmp 4199 bmp Mantooth32.E01/Partiti... Bitmap n/a 62 B 662aa4... a0d992... n/a n/a n/a
Carved [1322719].bmp 4200 bmp Mantooth32.E01/Partiti... Bitmap n/a 54 B 1ad6a9... 6aa664... n/a n/a n/a
Carved [1350421].bmp 4201 bmp Mantooth32.E01/Partiti... Bitmap n/a 62 B 132fd2... 17746d... n/a n/a n/a
Carved [1406].jpeg 4245 jpeg Mantooth32.E01/Partiti... JPEG n/a 4276 B fa7777... f63be2... n/a n/a n/a
Carved [1430].jpeg 4237 jpeg Mantooth32.E01/Partiti... JPEG n/a 4203 B d169ae... 21b67d... n/a n/a n/a
Carved [1452].jpeg 4239 jpeg Mantooth32.E01/Partiti... JPEG n/a 4299 B 992fb9... 9b4d73... n/a n/a n/a
Carved [3121].jpeg 4255 jpeg Mantooth32.E01/Partiti... JPEG n/a 1399 B 0a5f0c... 26f472... n/a n/a n/a
Carved [3194].jpeg 4250 jpeg Mantooth32.E01/Partiti... JPEG n/a 1470 B 78a44b... 89b01b... n/a n/a n/a
Carved [3251].jpeg 4232 jpeg Mantooth32.E01/Partiti... JPEG n/a 1525 B f3636e... 79814f... n/a n/a n/a
Carved [332].jpeg 4243 jpeg Mantooth32.E01/Partiti... JPEG n/a 1784 B 7c153d... ab64f0... n/a n/a n/a
Carved [332].jpeg 4231 jpeg Mantooth32.E01/Partiti... JPEG n/a 1525 B f3636e... 79814f... n/a n/a n/a
Carved [332].jpeg 4235 jpeg Mantooth32.E01/Partiti... JPEG n/a 1884 B 74d593... 0f251a... n/a n/a n/a
Carved [332].jpeg 4233 jpeg Mantooth32.E01/Partiti... JPEG n/a 1713 B 0841af... 798bad... n/a n/a n/a
Carved [332].jpeg 4254 jpeg Mantooth32.E01/Partiti... JPEG n/a 1399 B 0a5f0c... 26f472... n/a n/a n/a
Carved [332].jpeg 4247 jpeg Mantooth32.E01/Partiti... JPEG n/a 1891 B 6c4514... 043486... n/a n/a n/a
Carved [332].jpeg 4241 jpeg Mantooth32.E01/Partiti... JPEG n/a 1723 B 778441... 4d38e0... n/a n/a n/a
Carved [332].jpeg 4249 jpeg Mantooth32.E01/Partiti... JPEG n/a 1470 B 78a44b... 89b01b... n/a n/a n/a
Loaded: 111 Filtered: 111 Total: 111 Highlighted: 1 Checked: 0 Total LSize: 11.24 MB
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/$R61QDFF.exe=Carved [1311839].bmp
Ready
Explore Tab Filter: [None]

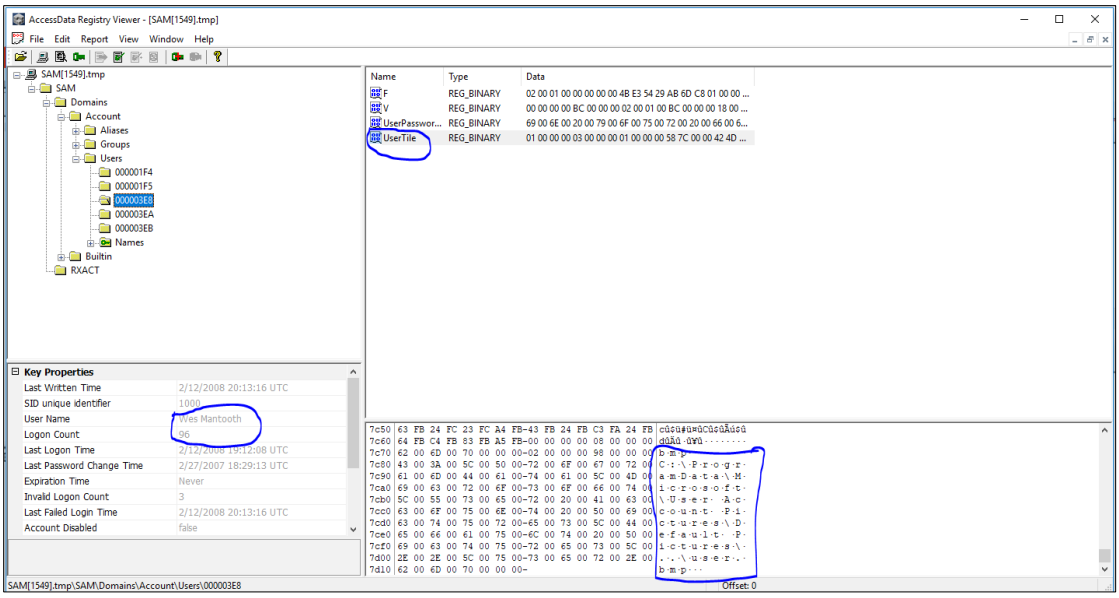


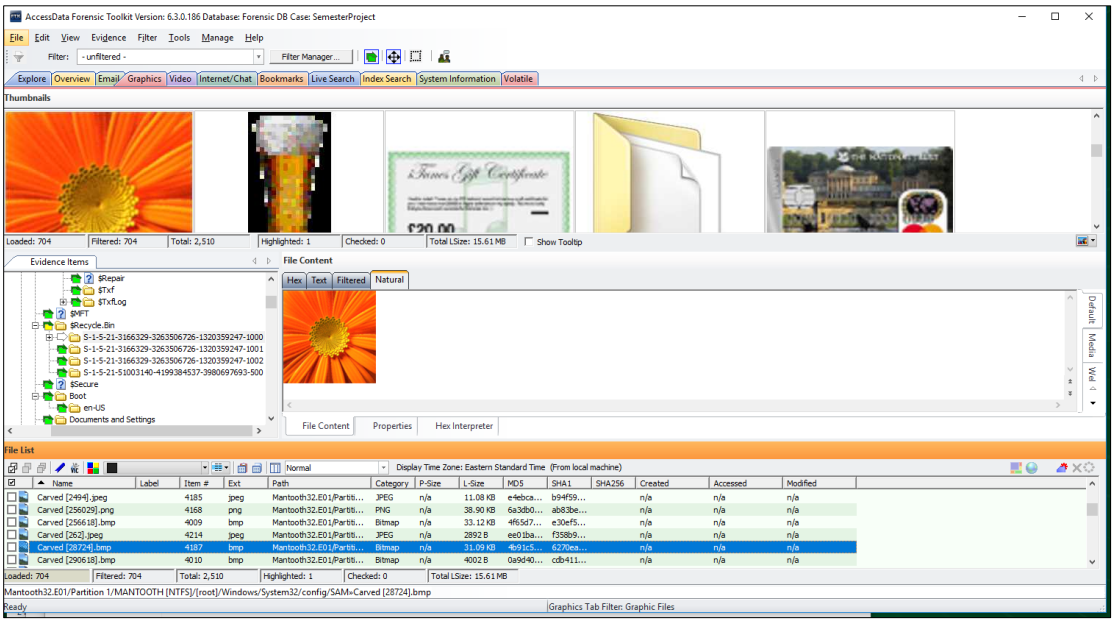


In ‘system information’ under SAM users, SID for Wes Mantooth is **‘S-1-5-21-3166329-3263506726-1320359247-1000’**. File Category in FTK shows these above files were placed in recycle bin by Wes Mantooth.

12. Recover the user picture tile for Wes Mantooth’s account.

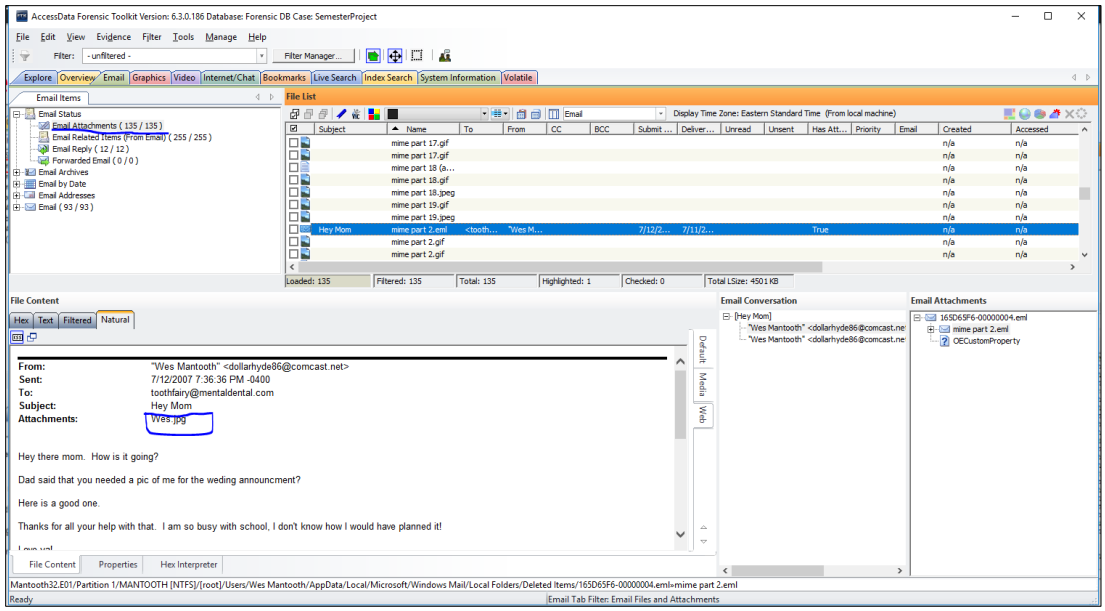
SAM file in registry viewer shows the **user picture tile** for Wes Mantooth’s account. Exploring the SAM file in graphics tab in FTK, we can see the following picture.

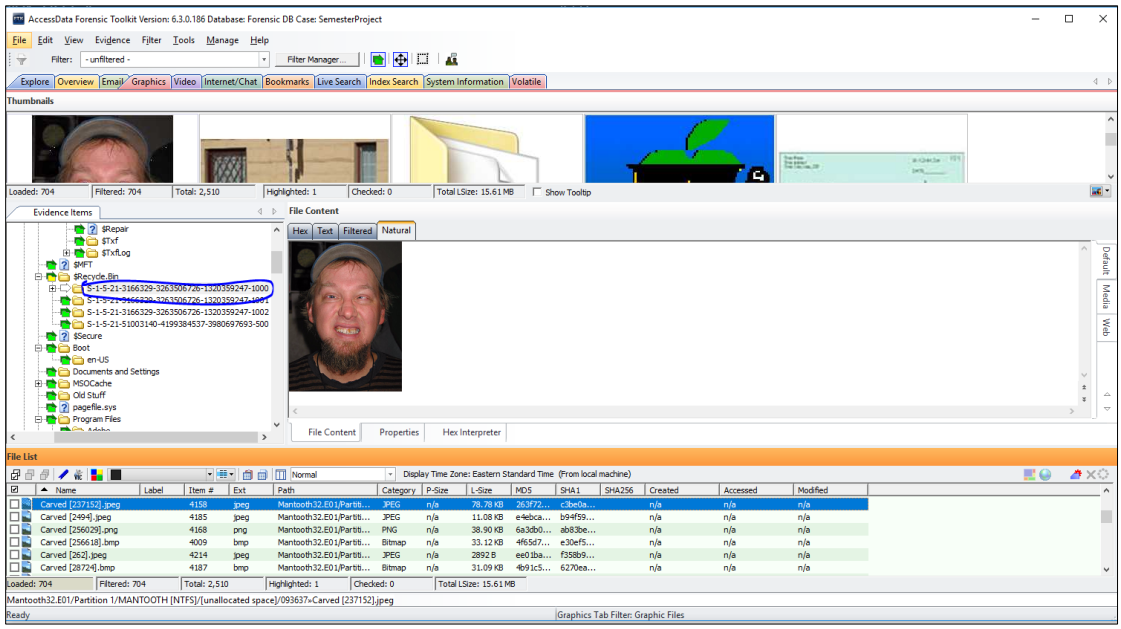


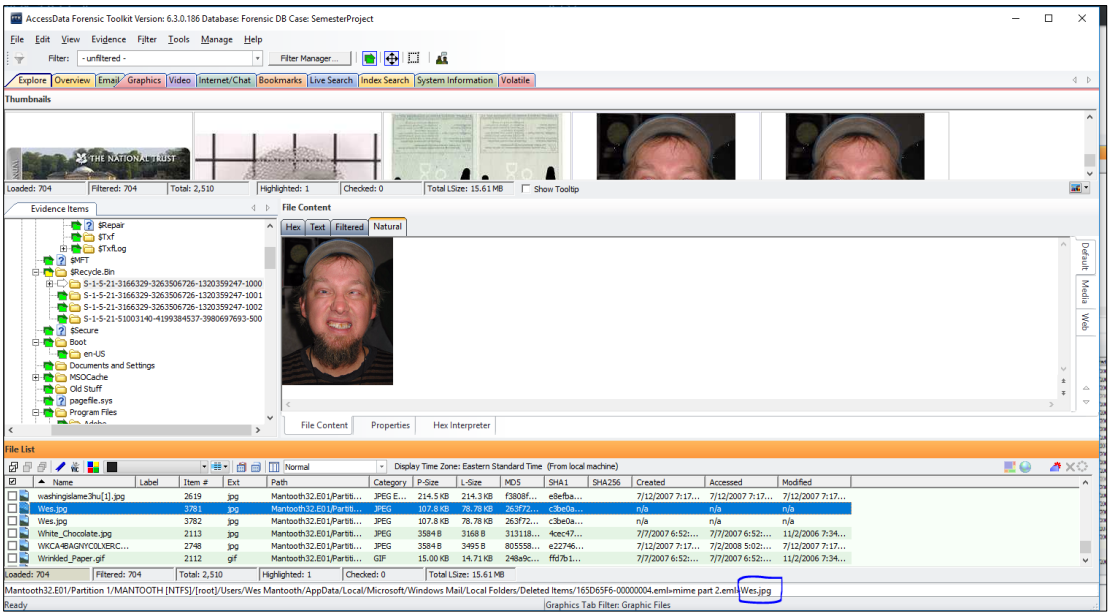


13. Identify any pictures of Wes Mantooth.

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

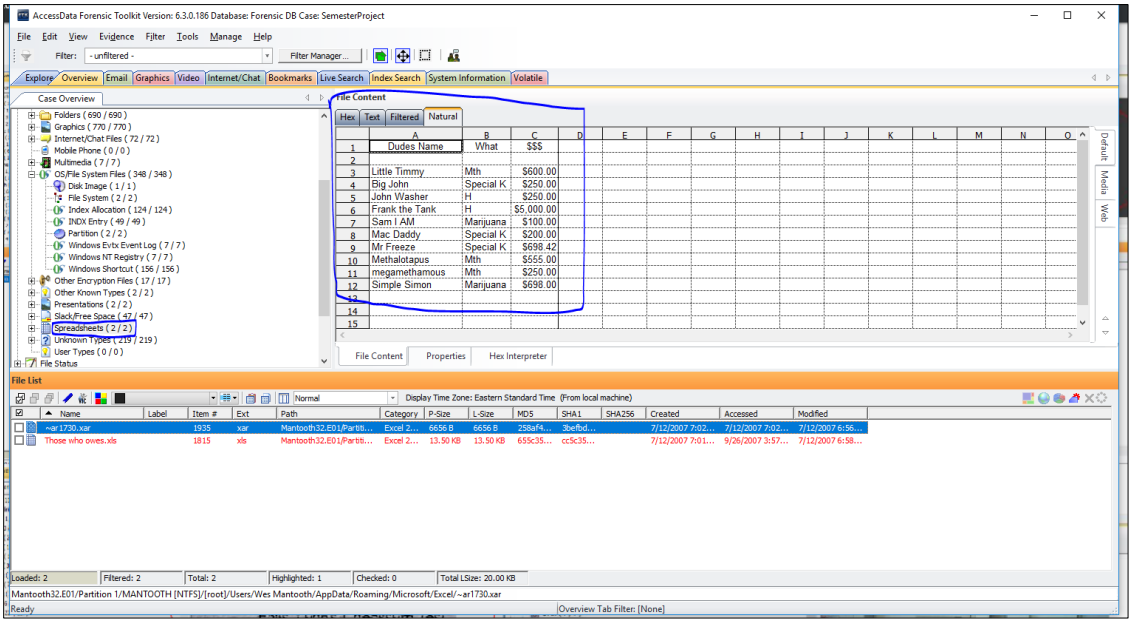

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Email Items
Email Status
Email Attachments (135 / 135)
Email Related Items (From Email) (255 / 255)
Email Reply (12 / 12)
Forwarded Email (0 / 0)
Email Archives
Email by Date
Email Addresses
Email (93 / 93)
File List
Display Time Zone: Eastern Standard Time (From local machine)
Subject To From CC BCC Unread Unsent Has Att... Priority Email Created Accessed
Hey Mom
File Content
Hex Text Filtered Natural
From: "Wes Mantooth" <dollarhyde86@comcast.net>
Sent: 7/12/2007 7:36:36 PM -0400
To: toothfairy@mentaldental.com
Subject: Hey Mom
Attachments: Wes.jpg
Hey there mom. How is it going?
Dad said that you needed a pic of me for the weding announcment?
Here is a good one.
Thanks for all your help with that. I am so busy with school, I don't know how I would have planned it!
Email Conversation
"Wes Mantooth" <dollarhyde86@comcast.ne
Email Attachments
165D65F6-00000004.eml
mime part 2.eml
OECustomProperty
File Content Properties Hex Interpreter
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows Mail/Local Folders/Deleted Items/165D65F6-00000004.eml=mime part 2.eml
Ready
Email Tab Filter: Email Files and Attachments

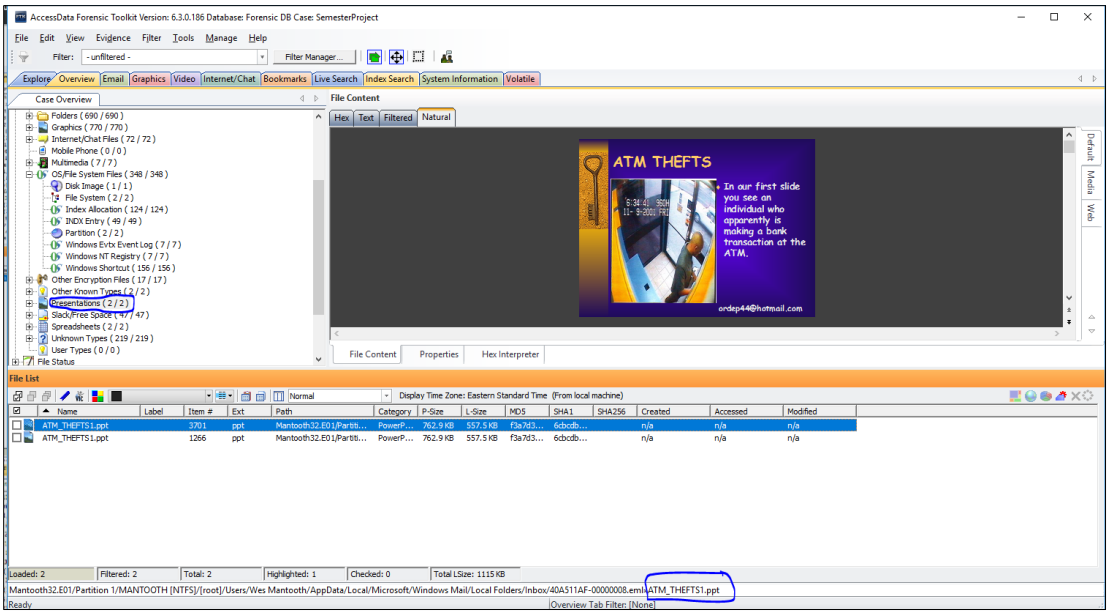

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Thumbnails
Loaded: 704 Filtered: 704 Total: 2,510 Highlighted: 1 Checked: 0 Total LSize: 15.61 MB Show Tooltip
Evidence Items
$Repair
$Txf
$TxfLog
$MFT
$Recycle.Bin
S-1-5-21-3166329-3263506726-1320359247-1000
S-1-5-21-3166329-3263506726-1320359247-1002
S-1-5-21-51003140-4199384537-3980697693-500
$Secure
Boot
en-US
Documents and Settings
MSOCache
Old Stuff
pagefile.sys
Program Files
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Display Time Zone: Eastern Standard Time (From local machine)
Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256 Created Accessed Modified
Carved [237152].jpeg 4158 jpeg Mantooth32.E01/Partiti... JPEG n/a 78.78 KB 263f72... c3be6a... n/a n/a n/a
Carved [2494].jpeg 4185 jpeg Mantooth32.E01/Partiti... JPEG n/a 11.08 KB e4ebca... b94f59... n/a n/a n/a
Carved [256029].png 4168 png Mantooth32.E01/Partiti... PNG n/a 38.90 KB 6a3db0... ab83be... n/a n/a n/a
Carved [256618].bmp 4009 bmp Mantooth32.E01/Partiti... Bitmap n/a 33.12 KB 4f65d7... e30ef5... n/a n/a n/a
Carved [262].jpeg 4214 jpeg Mantooth32.E01/Partiti... JPEG n/a 2892 B ee01ba... f358b9... n/a n/a n/a
Carved [28724].bmp 4187 bmp Mantooth32.E01/Partiti... Bitmap n/a 31.09 KB 4b91c5... 6270ea... n/a n/a n/a
Loaded: 704 Filtered: 704 Total: 2,510 Highlighted: 1 Checked: 0 Total LSize: 15.61 MB
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[unallocated space]/093637=Carved [237152].jpeg
Ready
Graphics Tab Filter: Graphic Files

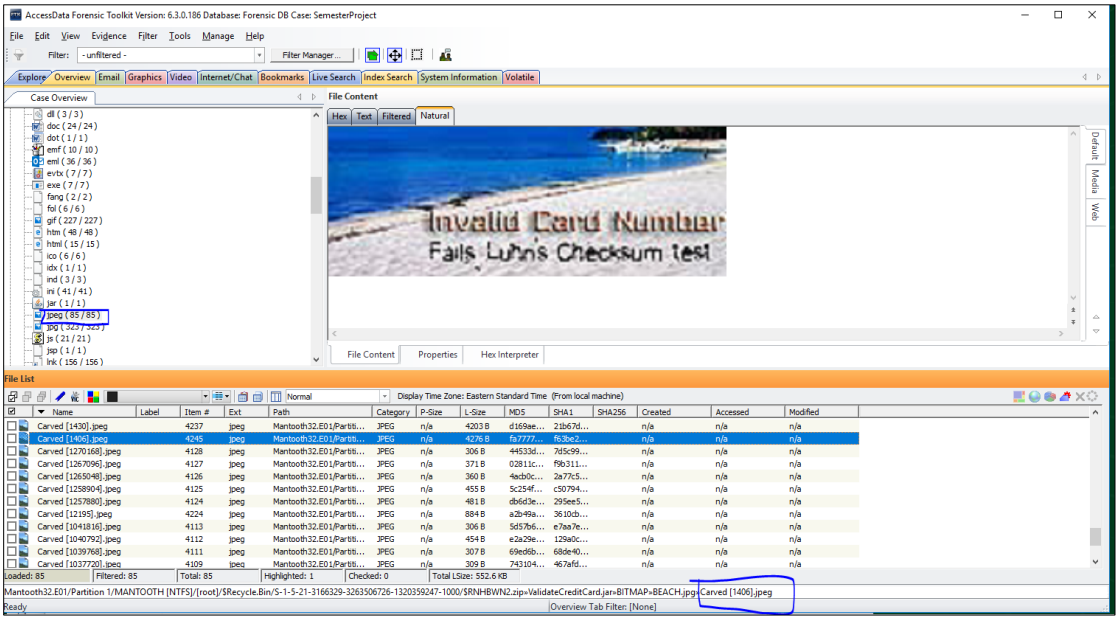


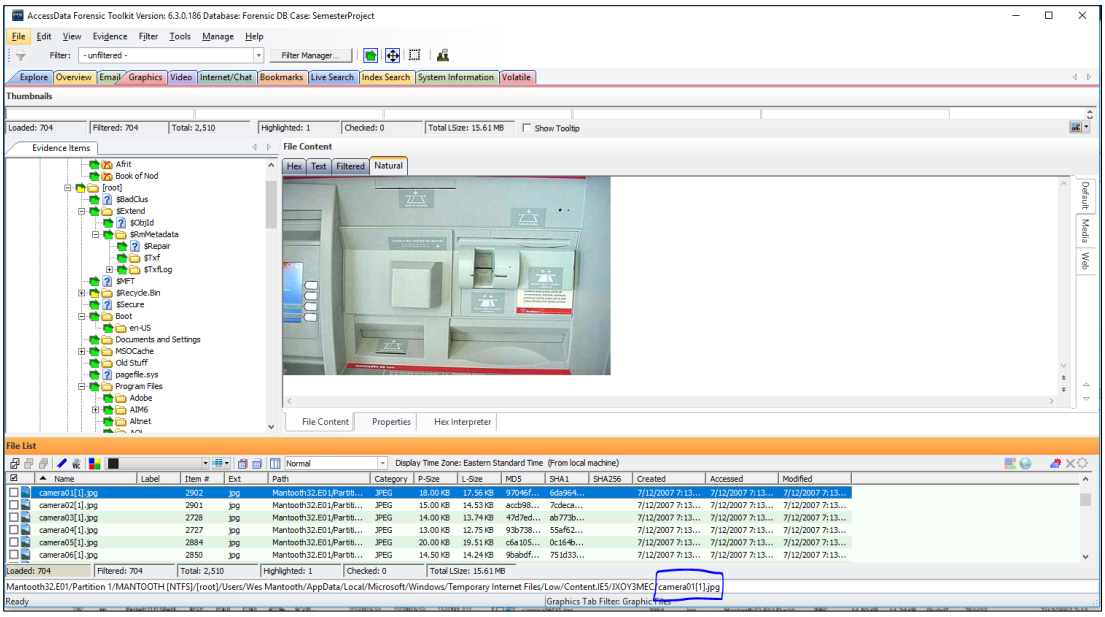
14. Identify any pictures related to the fraud or financial crimes.

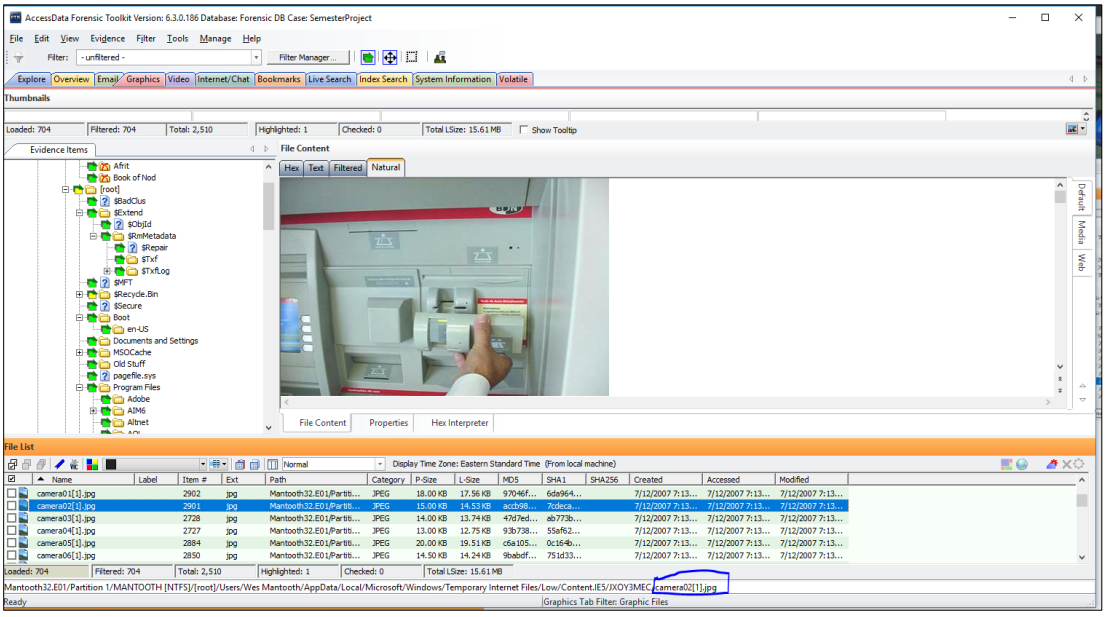
In the overview tab, I was able to find pictures related to the fraud or financial crimes as shown below.

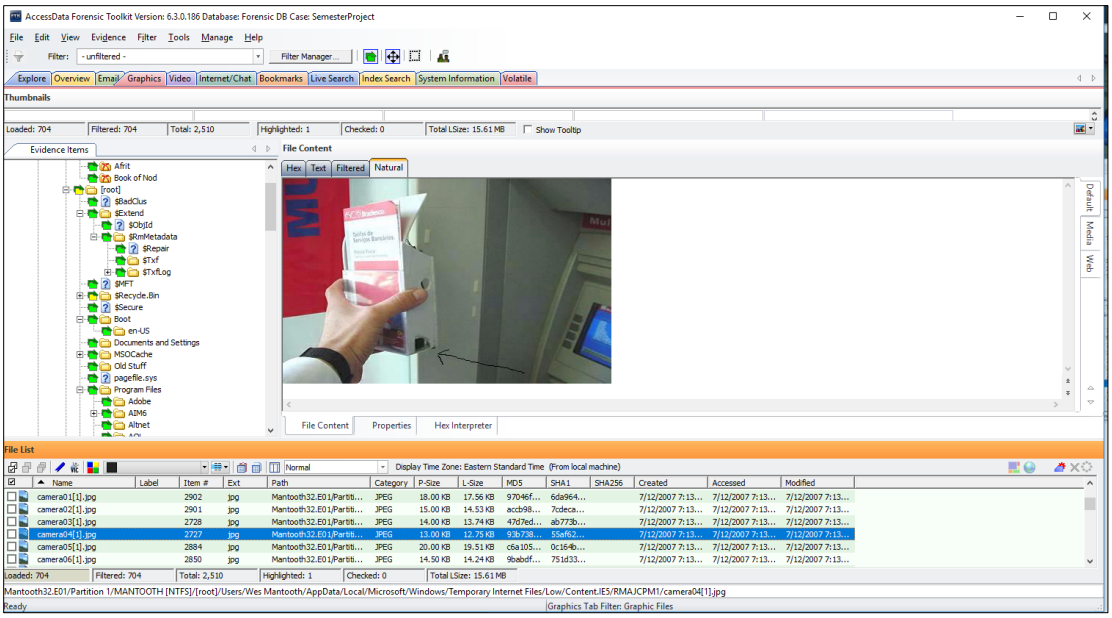


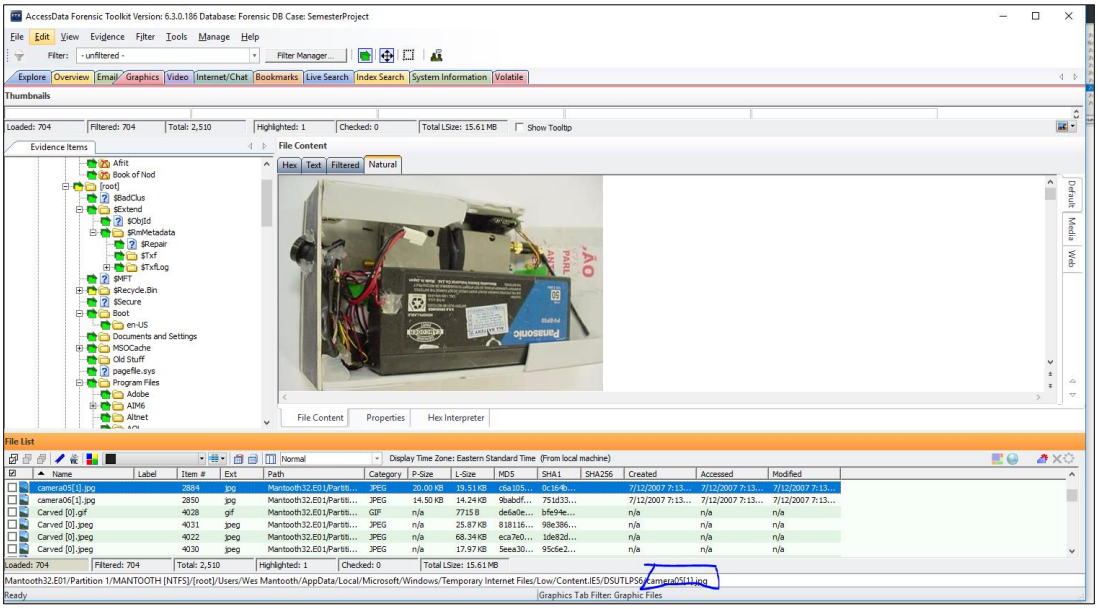

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
ATM THEFTS
In our first slide you see an individual who apparently is making a bank transaction at the ATM.
ordep44@hotmail.com
Presentations (2 / 2)
ATM_THEFTS1.ppt
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows Mail/Local Folders/Inbox/40A511AF-00000008.eml/ATM_THEFTS1.ppt


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
Invalid Card Number
Fails Luhn's Checksum test
jpeg (85 / 85)
Carved [1406].jpeg
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/$RNHBWN2.zip>ValidateCreditCard.jar>BITMAP>BEACH.jpg>Carved [1406].jpeg


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Thumbnails
Loaded: 704 Filtered: 704 Total: 2,510 Highlighted: 1 Checked: 0 Total LSize: 15.61 MB Show Tooltip
Evidence Items
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Normal Display Time Zone: Eastern Standard Time (From local machine)
Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256 Created Accessed Modified
camera01[1].jpg 2902 jpg Mantooth32.E01/Partiti... JPEG 18.00 KB 17.56 KB 97046f... 6da964... 7/12/2007 7:13... 7/12/2007 7:13... 7/12/2007 7:13...
camera02[1].jpg 2901 jpg Mantooth32.E01/Partiti... JPEG 15.00 KB 14.53 KB accb98... 7cdeca... 7/12/2007 7:13... 7/12/2007 7:13... 7/12/2007 7:13...
camera03[1].jpg 2728 jpg Mantooth32.E01/Partiti... JPEG 14.00 KB 13.74 KB 47d7ed... ab773b... 7/12/2007 7:13... 7/12/2007 7:13... 7/12/2007 7:13...
camera04[1].jpg 2727 jpg Mantooth32.E01/Partiti... JPEG 13.00 KB 12.75 KB 93b738... 55af62... 7/12/2007 7:13... 7/12/2007 7:13... 7/12/2007 7:13...
camera05[1].jpg 2884 jpg Mantooth32.E01/Partiti... JPEG 20.00 KB 19.51 KB c6a105... 0c164b... 7/12/2007 7:13... 7/12/2007 7:13... 7/12/2007 7:13...
camera06[1].jpg 2850 jpg Mantooth32.E01/Partiti... JPEG 14.50 KB 14.24 KB 9babdf... 751d33... 7/12/2007 7:13... 7/12/2007 7:13... 7/12/2007 7:13...
Loaded: 704 Filtered: 704 Total: 2,510 Highlighted: 1 Checked: 0 Total LSize: 15.61 MB
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/JXOY3MEC/camera01[1].jpg
Ready Graphics Tab Filter: Graphic Files

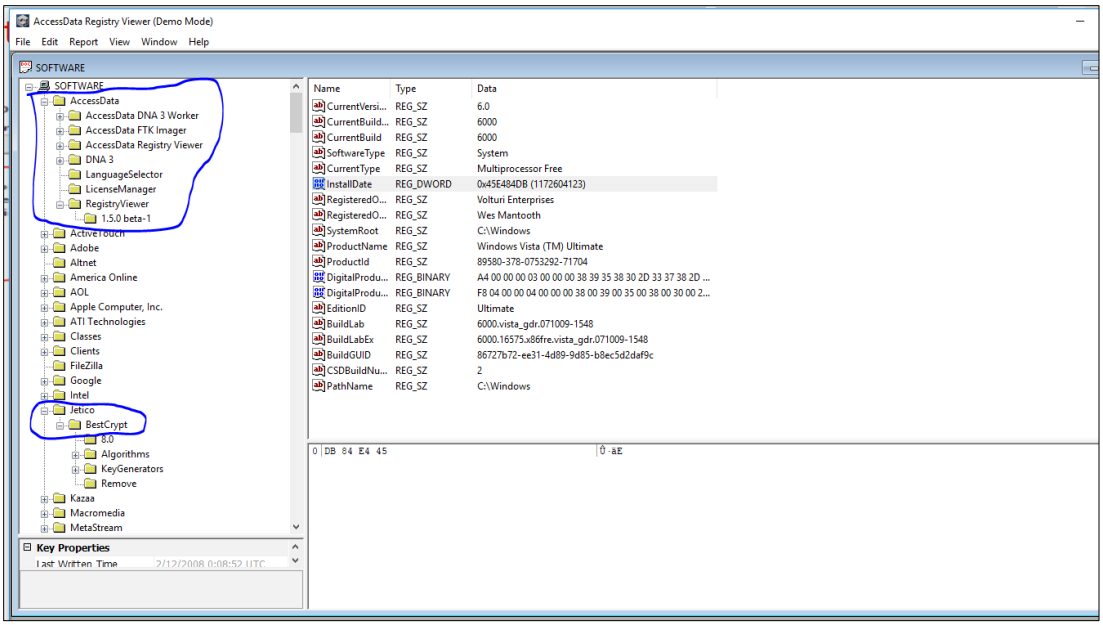

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Thumbnails
Loaded: 704 Filtered: 704 Total: 2,510 Highlighted: 1 Checked: 0 Total LSize: 15.61 MB Show Tooltip
Evidence Items
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Normal Display Time Zone: Eastern Standard Time (From local machine)
Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256 Created Accessed Modified
camera01[1].jpg 2902 jpg Mantooth32.E01/Partiti... JPEG 18.00 KB 17.56 KB 97046f... 6da964... 7/12/2007 7:13... 7/12/2007 7:13... 7/12/2007 7:13...
camera02[1].jpg 2901 jpg Mantooth32.E01/Partiti... JPEG 15.00 KB 14.53 KB accb98... 7cdeca... 7/12/2007 7:13... 7/12/2007 7:13... 7/12/2007 7:13...
camera03[1].jpg 2728 jpg Mantooth32.E01/Partiti... JPEG 14.00 KB 13.74 KB 47d7ed... ab773b... 7/12/2007 7:13... 7/12/2007 7:13... 7/12/2007 7:13...
camera04[1].jpg 2727 jpg Mantooth32.E01/Partiti... JPEG 13.00 KB 12.75 KB 93b738... 55af62... 7/12/2007 7:13... 7/12/2007 7:13... 7/12/2007 7:13...
camera05[1].jpg 2884 jpg Mantooth32.E01/Partiti... JPEG 20.00 KB 19.51 KB c6a105... 0c164b... 7/12/2007 7:13... 7/12/2007 7:13... 7/12/2007 7:13...
camera06[1].jpg 2850 jpg Mantooth32.E01/Partiti... JPEG 14.50 KB 14.24 KB 9babdf... 751d33... 7/12/2007 7:13... 7/12/2007 7:13... 7/12/2007 7:13...
Loaded: 704 Filtered: 704 Total: 2,510 Highlighted: 1 Checked: 0 Total LSize: 15.61 MB
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/JXOY3MEC/camera02[1].jpg
Ready Graphics Tab Filter: Graphic Files

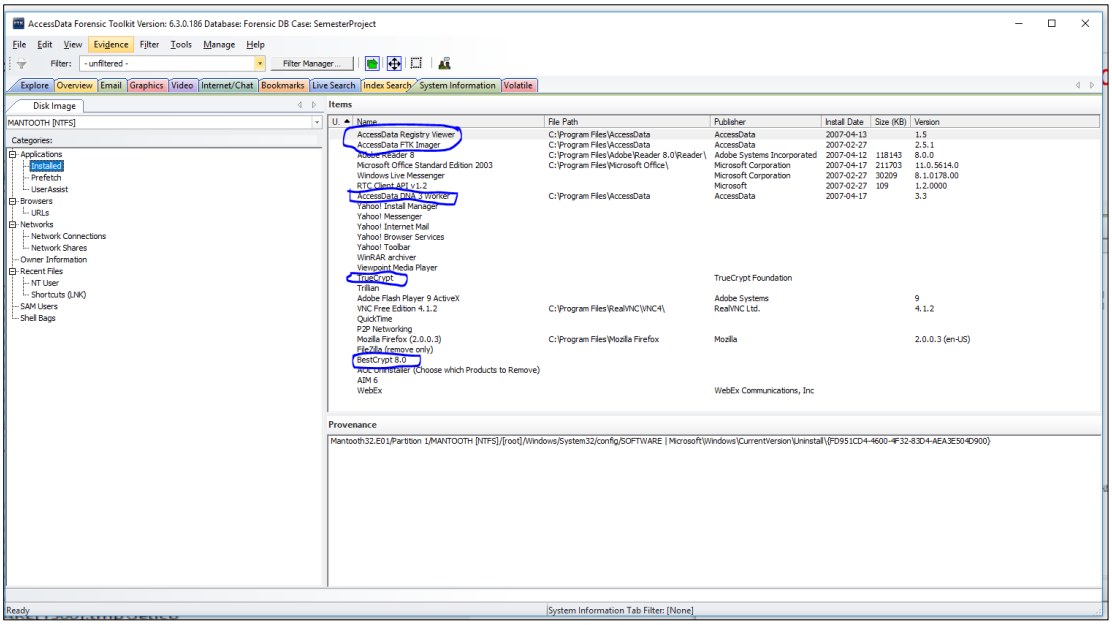




15. Identify any software that can be used to encrypt, obscure or forensically analyze data, or defeat forensics.

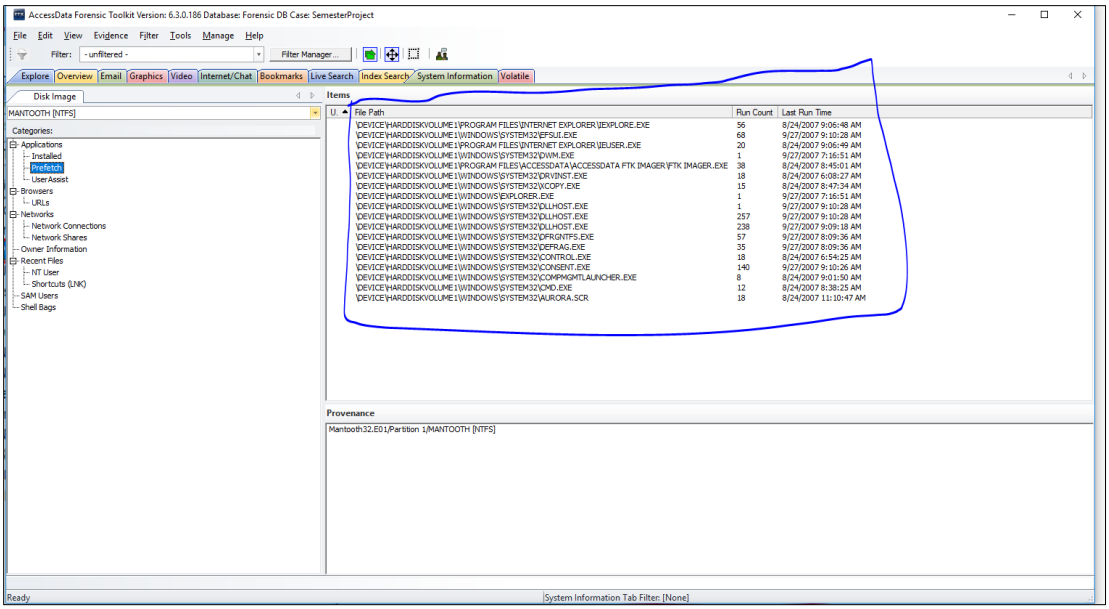
After exporting **SOFTWARE** file from FTK into registry viewer, I discovered these softwares. Additionally, in 'System Information' of FTK, I found these above highlighted softwares which were installed on the computer.





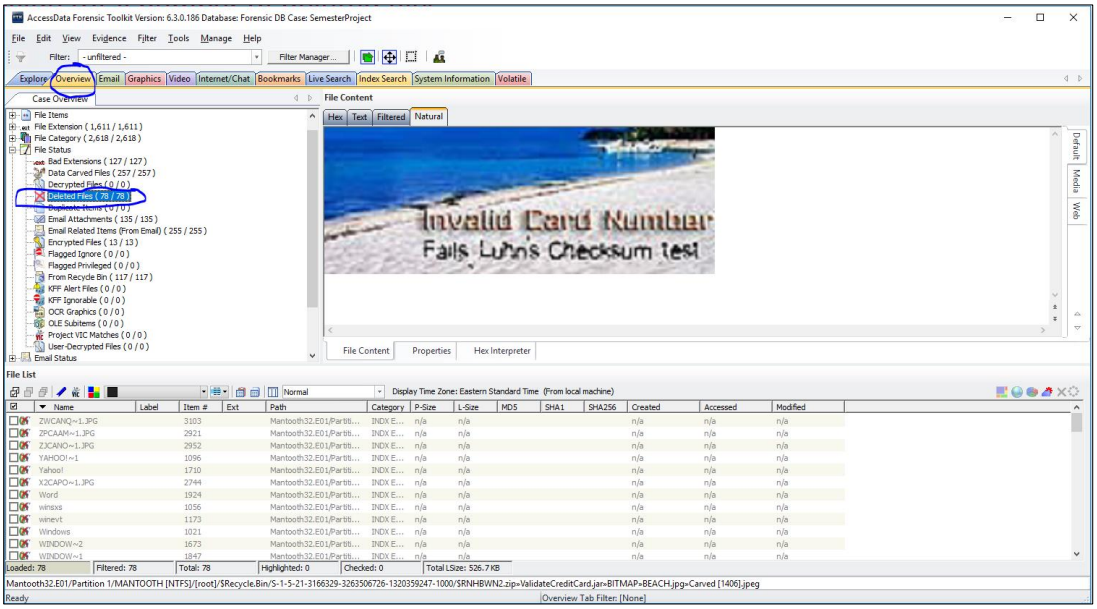
16. Identify the most commonly opened programs.

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

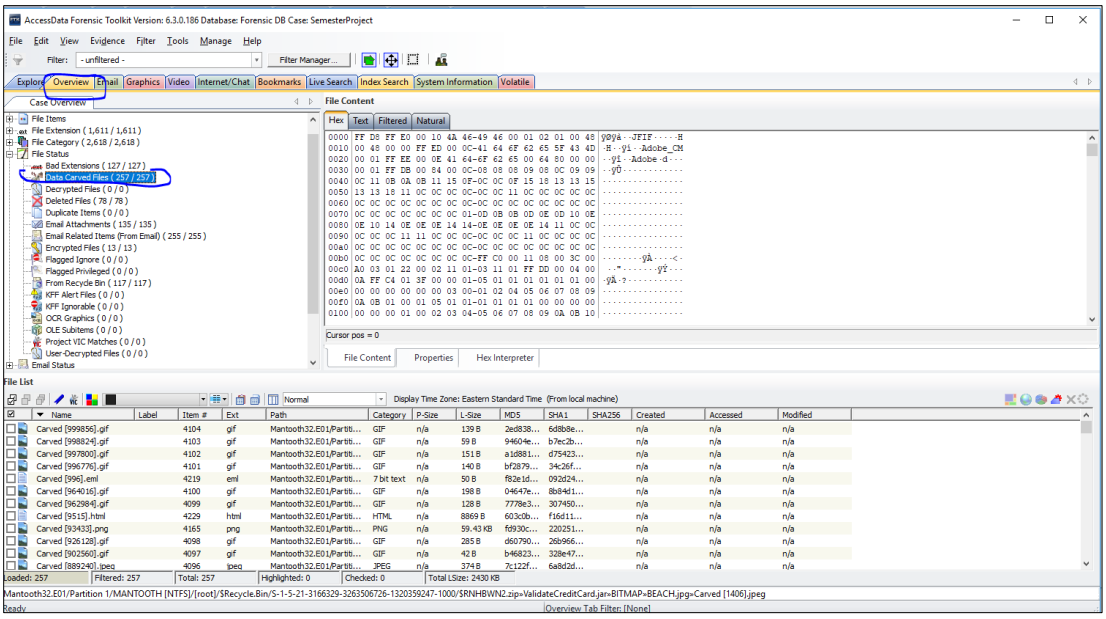


17. Provide total number of deleted files.

'Overview' tab shows **78** deleted files.



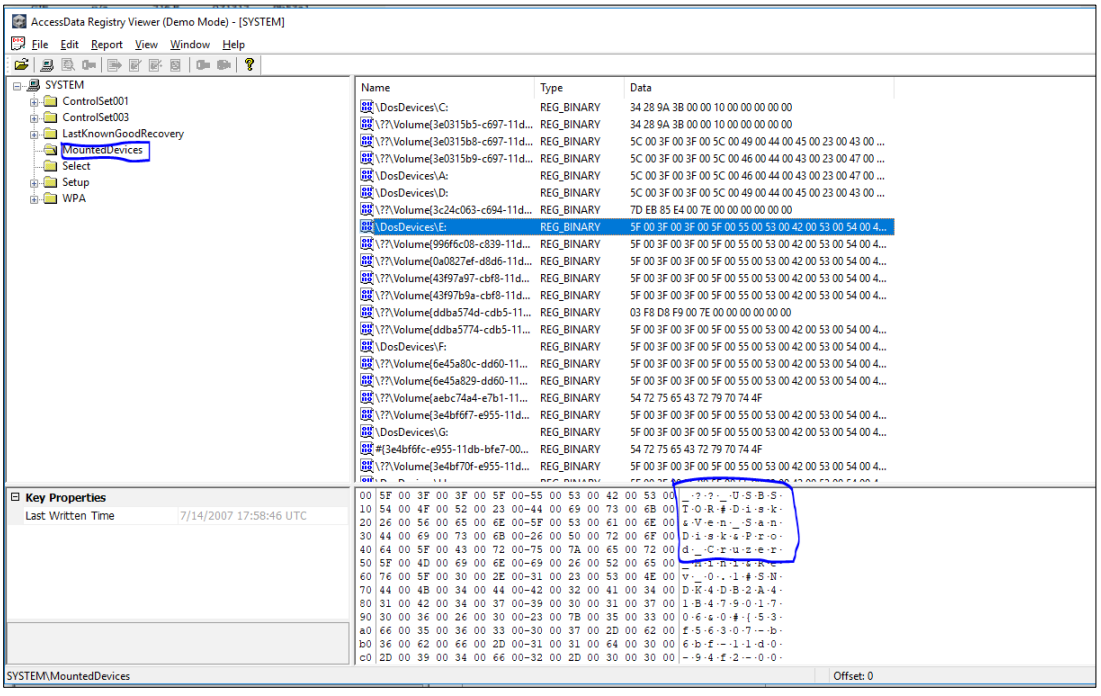
18. Perform file carving and find total number of carved files.

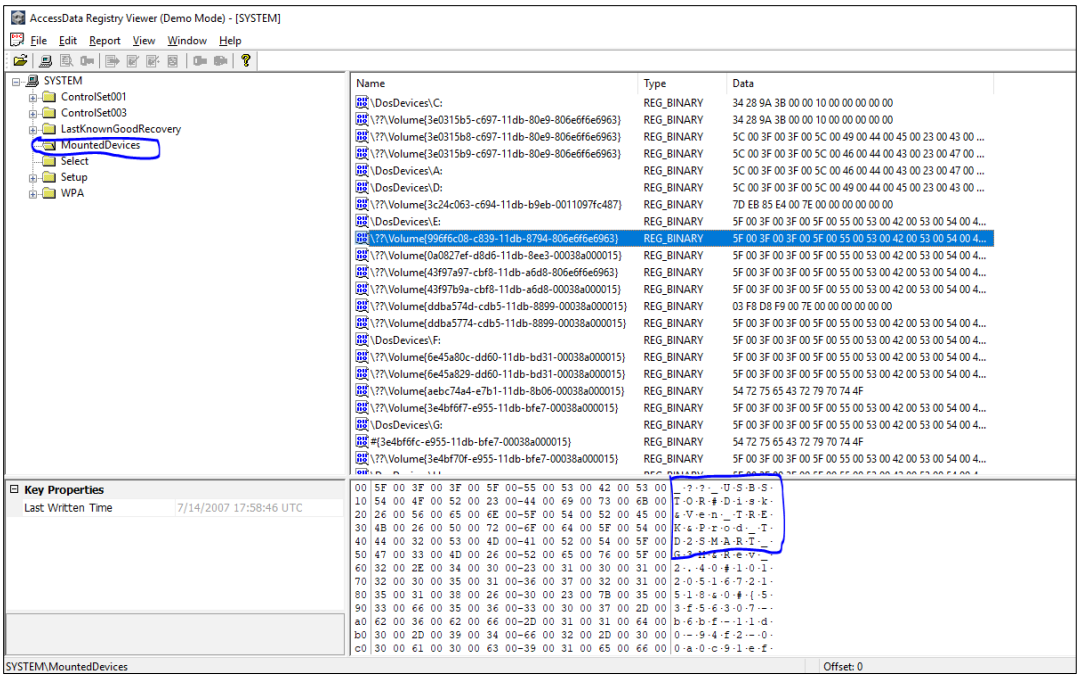


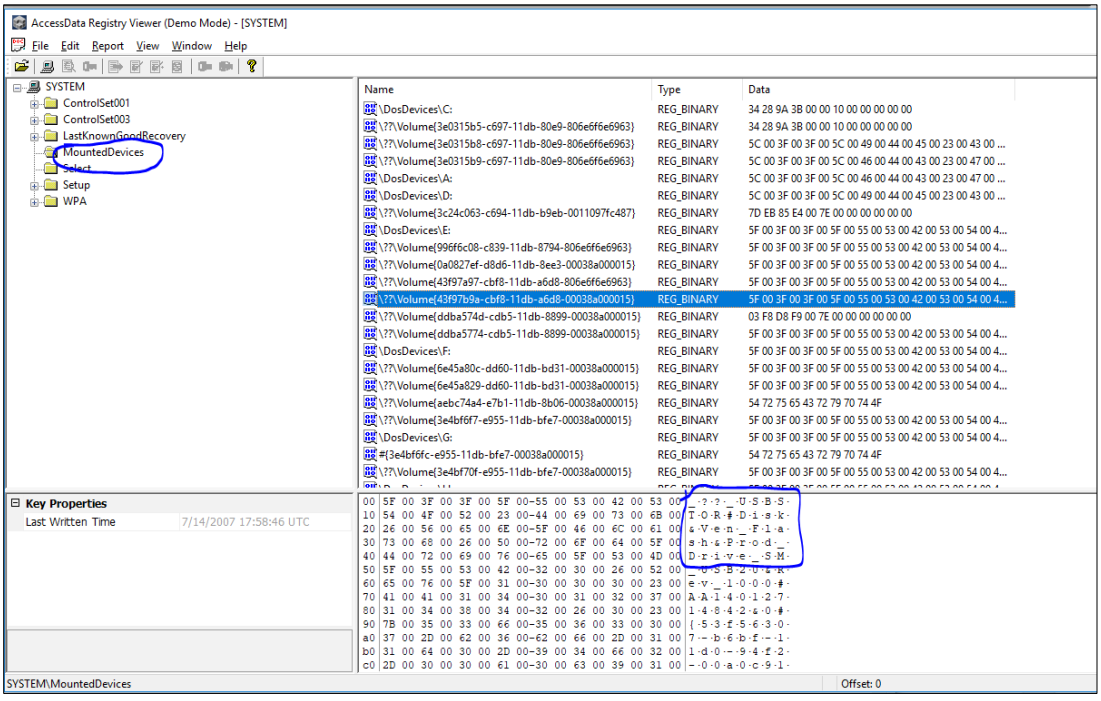
After carving operation, I found **257** data carved files.

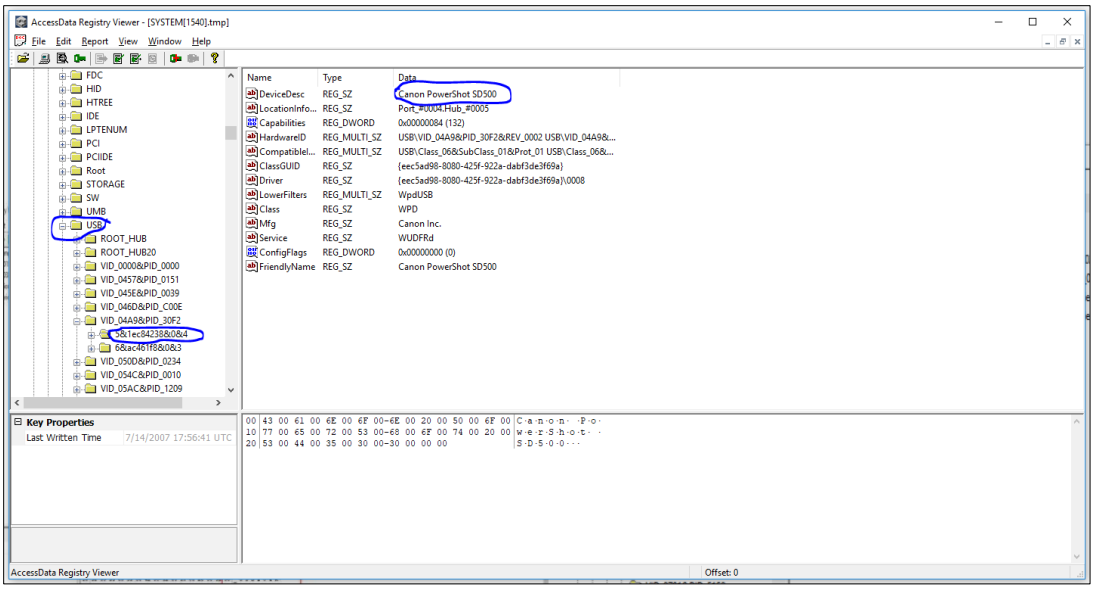
19. Identify any cameras, USB drives or other devices that have been attached to the computer.

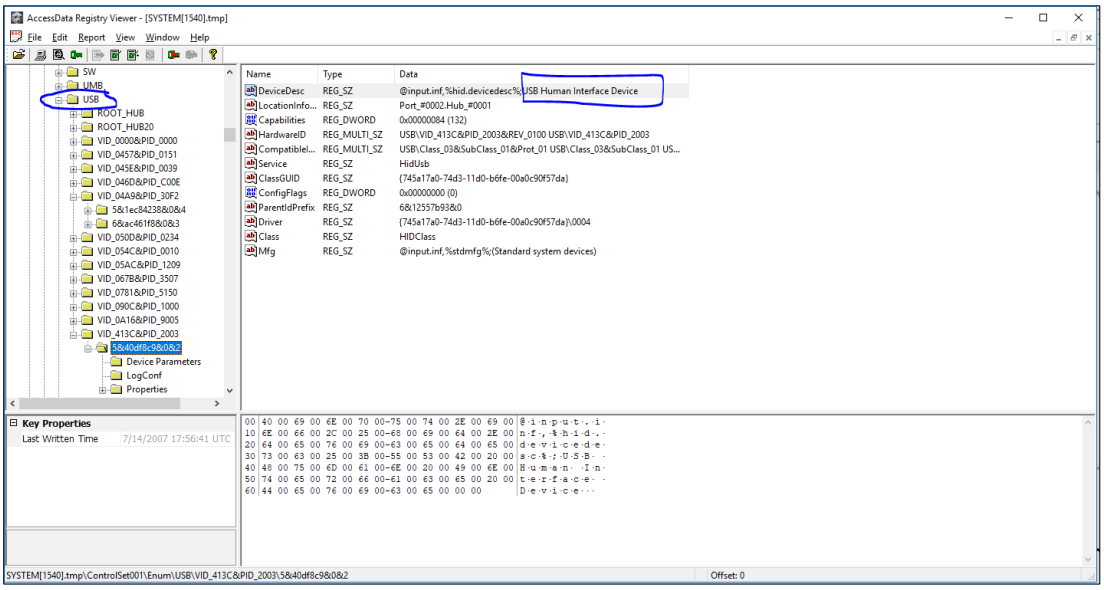
I exported SYSTEM file into registry viewer and found USB attachments under 'MountedDevices' as shown. Moreover, after exploring subfolders under 'USB' I found **USB drives, camera attachment and human interface device.**

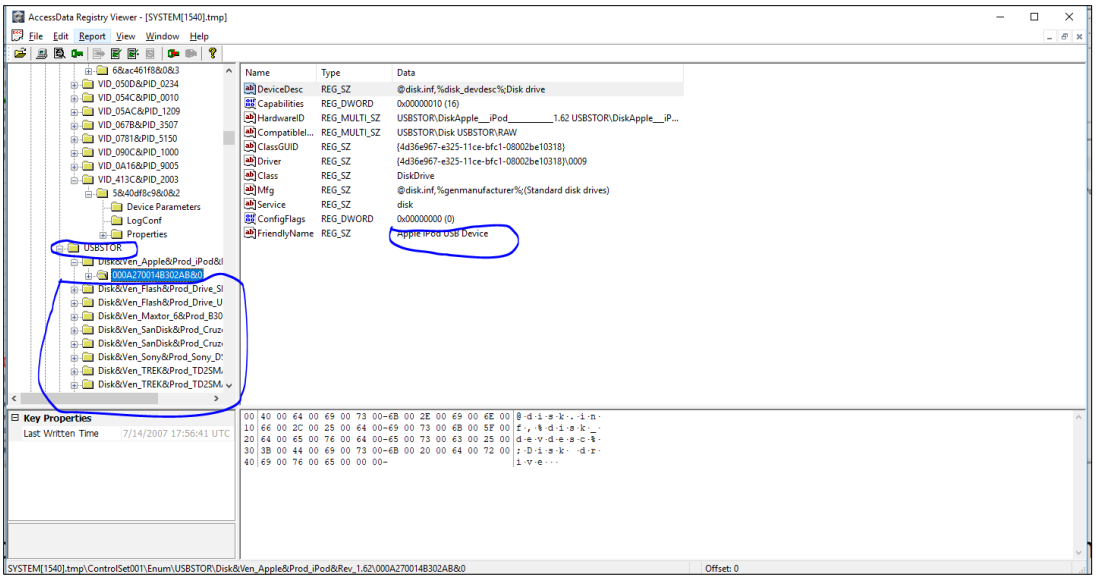



AccessData Registry Viewer (Demo Mode) - [SYSTEM]
File Edit Report View Window Help
SYSTEM
ControlSet001
ControlSet003
LastKnownGoodRecovery
MountedDevices
Select
Setup
WPA
Name
Type
Data
\DosDevices\C:
REG_BINARY
34 28 9A 3B 00 00 10 00 00 00 00 00
\??\Volume{3e0315b5-c697-11db-80e9-806e6f6e6963}
REG_BINARY
34 28 9A 3B 00 00 10 00 00 00 00 00
\??\Volume{3e0315b8-c697-11db-80e9-806e6f6e6963}
REG_BINARY
5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\??\Volume{3e0315b9-c697-11db-80e9-806e6f6e6963}
REG_BINARY
5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
\DosDevices\A:
REG_BINARY
5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
\DosDevices\D:
REG_BINARY
5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\??\Volume{3c24c063-c694-11db-b9eb-0011097fc487}
REG_BINARY
7D EB 85 E4 00 7E 00 00 00 00 00 00
\DosDevices\E:
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{996f6c08-c839-11db-8794-806e6f6e6963}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{0a0827ef-d8d6-11db-8ee3-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{43f97a97-cbf8-11db-a6d8-806e6f6e6963}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{43f97b9a-cbf8-11db-a6d8-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{ddba574d-cdb5-11db-8899-00038a000015}
REG_BINARY
03 F8 D8 F9 00 7E 00 00 00 00 00 00
\??\Volume{ddba5774-cdb5-11db-8899-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\DosDevices\F:
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{6e45a80c-dd60-11db-bd31-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{6e45a829-dd60-11db-bd31-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{aebc74a4-e7b1-11db-8b06-00038a000015}
REG_BINARY
54 72 75 65 43 72 79 70 74 4F
\??\Volume{3e4bf6f7-e955-11db-bfe7-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\DosDevices\G:
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
#{3e4bf6fc-e955-11db-bfe7-00038a000015}
REG_BINARY
54 72 75 65 43 72 79 70 74 4F
\??\Volume{3e4bf70f-e955-11db-bfe7-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
Key Properties
Last Written Time
7/14/2007 17:58:46 UTC
SYSTEM\MountedDevices
Offset: 0

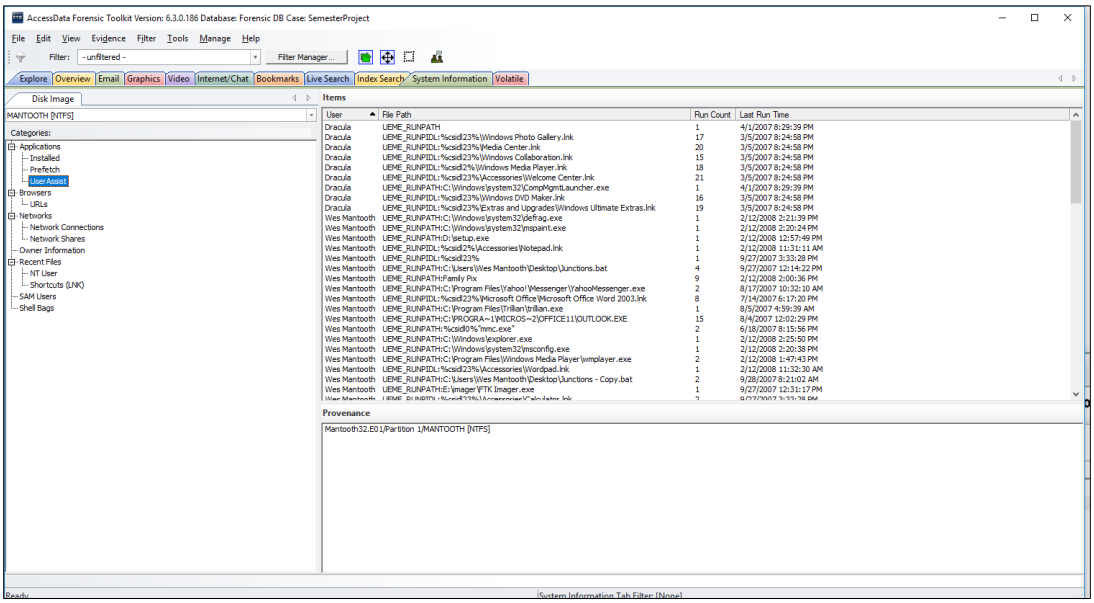

AccessData Registry Viewer (Demo Mode) - [SYSTEM]
File Edit Report View Window Help
SYSTEM
ControlSet001
ControlSet003
LastKnownGoodRecovery
MountedDevices
Select
Setup
WPA
Name
Type
Data
\DosDevices\C:
REG_BINARY
34 28 9A 3B 00 00 10 00 00 00 00 00
\??\Volume{3e0315b5-c697-11db-80e9-806e6f6e6963}
REG_BINARY
34 28 9A 3B 00 00 10 00 00 00 00 00
\??\Volume{3e0315b8-c697-11db-80e9-806e6f6e6963}
REG_BINARY
5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\??\Volume{3e0315b9-c697-11db-80e9-806e6f6e6963}
REG_BINARY
5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
\DosDevices\A:
REG_BINARY
5C 00 3F 00 3F 00 5C 00 46 00 44 00 43 00 23 00 47 00 ...
\DosDevices\D:
REG_BINARY
5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\??\Volume{3c24c063-c694-11db-b9eb-0011097fc487}
REG_BINARY
7D EB 85 E4 00 7E 00 00 00 00 00 00
\DosDevices\E:
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{996f6c08-c839-11db-8794-806e6f6e6963}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{0a0827ef-d8d6-11db-8ee3-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{43f97a97-cbf8-11db-a6d8-806e6f6e6963}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{43f97b9a-cbf8-11db-a6d8-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{ddba574d-cdb5-11db-8899-00038a000015}
REG_BINARY
03 F8 D8 F9 00 7E 00 00 00 00 00 00
\??\Volume{ddba5774-cdb5-11db-8899-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\DosDevices\F:
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{6e45a80c-dd60-11db-bd31-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{6e45a829-dd60-11db-bd31-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\??\Volume{aebc74a4-e7b1-11db-8b06-00038a000015}
REG_BINARY
54 72 75 65 43 72 79 70 74 4F
\??\Volume{3e4bf6f7-e955-11db-bfe7-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
\DosDevices\G:
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
#{3e4bf6fc-e955-11db-bfe7-00038a000015}
REG_BINARY
54 72 75 65 43 72 79 70 74 4F
\??\Volume{3e4bf70f-e955-11db-bfe7-00038a000015}
REG_BINARY
5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
Key Properties
Last Written Time
7/14/2007 17:58:46 UTC
SYSTEM\MountedDevices
Offset: 0


AccessData Registry Viewer - [SYSTEM[1540].tmp]
File Edit Report View Window Help
FDC
HID
HTREE
IDE
LPTENUM
PCI
PCIIDE
Root
STORAGE
SW
UMB
USB
ROOT_HUB
ROOT_HUB20
VID_0000&PID_0000
VID_0457&PID_0151
VID_045E&PID_0039
VID_046D&PID_C00E
VID_04A9&PID_30F2
5&1ec84238&0&4
68ac461f88&0&3
VID_050D&PID_0234
VID_054C&PID_0010
VID_05AC&PID_1209
Name Type Data
DeviceDesc REG_SZ Canon PowerShot SD500
LocationInfo... REG_SZ Port_#0004.Hub_#0005
Capabilities REG_DWORD 0x00000084 (132)
HardwareID REG_MULTI_SZ USB\VID_04A9&PID_30F2&REV_0002 USB\VID_04A9&...
Compatibilel... REG_MULTI_SZ USB\Class_06&SubClass_01&Prot_01 USB\Class_06&...
ClassGUID REG_SZ {eec5ad98-8080-425f-922a-dabf3de3f69a}
Driver REG_SZ {eec5ad98-8080-425f-922a-dabf3de3f69a}\0008
LowerFilters REG_MULTI_SZ WpdUSB
Class REG_SZ WPD
Mfg REG_SZ Canon Inc.
Service REG_SZ WUDFRd
ConfigFlags REG_DWORD 0x00000000 (0)
FriendlyName REG_SZ Canon PowerShot SD500
Key Properties
Last Written Time 7/14/2007 17:56:41 UTC
00 43 00 61 00 6E 00 6F 00-6E 00 20 00 50 00 6F 00 C·a·n·o·n· ·P·o·
10 77 00 65 00 72 00 53 00-68 00 6F 00 74 00 20 00 w·e·r·S·h·o·t· ·
20 53 00 44 00 35 00 30 00-30 00 00 00 S·D·5·0·0···
AccessData Registry Viewer
Offset: 0


AccessData Registry Viewer - [SYSTEM[1540].tmp]
File Edit Report View Window Help
SW
UMB
USB
ROOT_HUB
ROOT_HUB20
VID_0000&PID_0000
VID_0457&PID_0151
VID_045E&PID_0039
VID_046D&PID_C00E
VID_04A9&PID_30F2
5&1ec84238&0&4
68ac461f88&0&3
VID_050D&PID_0234
VID_054C&PID_0010
VID_05AC&PID_1209
VID_067B&PID_3507
VID_0781&PID_5150
VID_090C&PID_1000
VID_0A16&PID_9005
VID_413C&PID_2003
5&40df8c98&0&2
Device Parameters
LogConf
Properties
Name Type Data
DeviceDesc REG_SZ @input.inf,%hid.devicedesc%;USB Human Interface Device
LocationInfo... REG_SZ Port_#0002.Hub_#0001
Capabilities REG_DWORD 0x00000084 (132)
HardwareID REG_MULTI_SZ USB\VID_413C&PID_2003&REV_0100 USB\VID_413C&PID_2003
Compatibilel... REG_MULTI_SZ USB\Class_03&SubClass_01&Prot_01 USB\Class_03&SubClass_01 US...
Service REG_SZ HidUsb
ClassGUID REG_SZ {745a17a0-74d3-11d0-b6fe-00a0c90f57da}
ConfigFlags REG_DWORD 0x00000000 (0)
ParentIdPrefix REG_SZ 68&12557b93&0
Driver REG_SZ {745a17a0-74d3-11d0-b6fe-00a0c90f57da}\0004
Class REG_SZ HIDClass
Mfg REG_SZ @input.inf,%stdmfg%;(Standard system devices)
Key Properties
Last Written Time 7/14/2007 17:56:41 UTC
00 40 00 69 00 6E 00 70 00-75 00 74 00 2E 00 69 00 @·i·n·p·u·t·.·i·
10 6E 00 66 00 2C 00 25 00-68 00 69 00 64 00 2E 00 n·f·,·%·h·i·d·.·
20 64 00 65 00 76 00 69 00-63 00 65 00 64 00 65 00 d·e·v·i·c·e·d·e·
30 73 00 63 00 25 00 3B 00-55 00 53 00 42 00 20 00 s·c·%·;·U·S·B· ·
40 48 00 75 00 6D 00 61 00-6E 00 20 00 49 00 6E 00 H·u·m·a·n· ·I·n·
50 74 00 65 00 72 00 66 00-61 00 63 00 65 00 20 00 t·e·r·f·a·c·e· ·
60 44 00 65 00 76 00 69 00-63 00 65 00 00 00 D·e·v·i·c·e···
SYSTEM[1540].tmp\ControlSet001\Enum\USB\VID_413C&PID_2003\5&40df8c98&0&2
Offset: 0



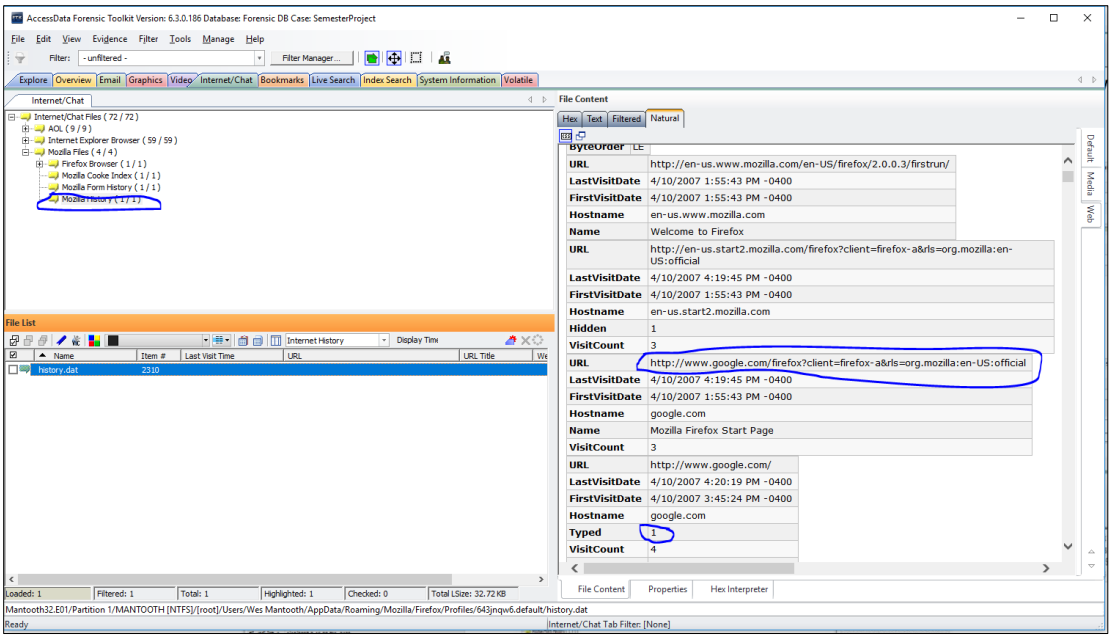
20. Identify the most recently run programs

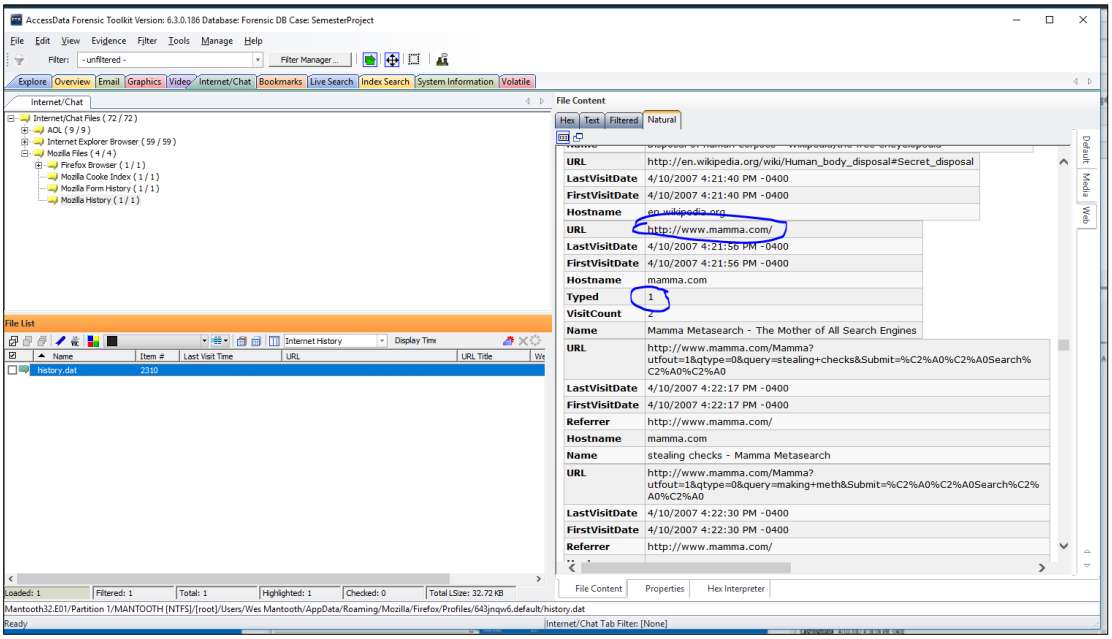


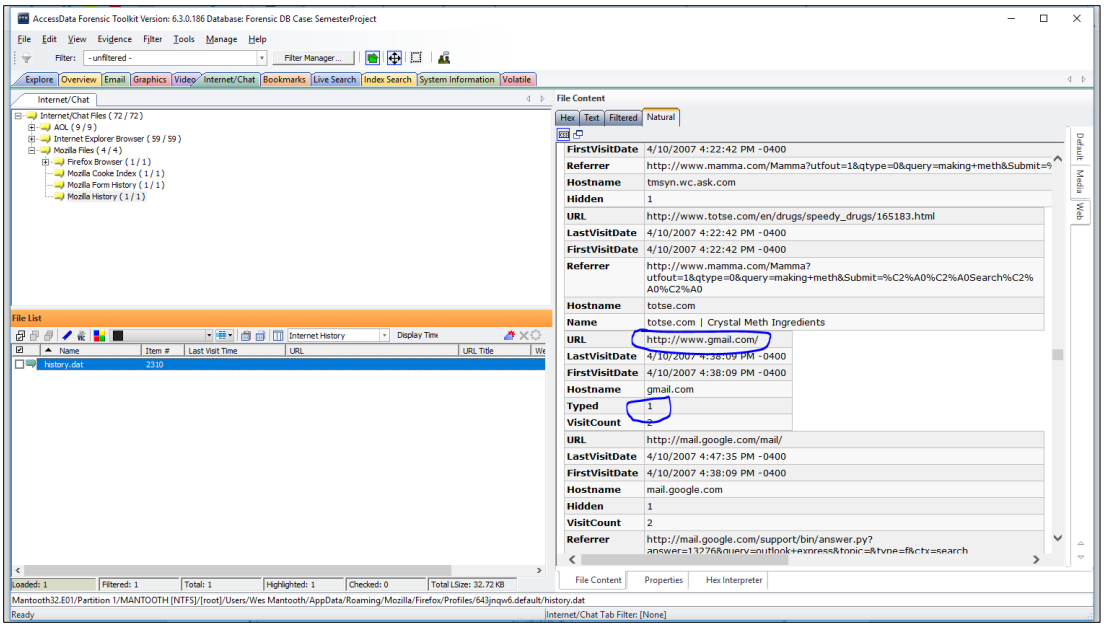
'**UserAssist**' in FTK explains which programs were recently run.

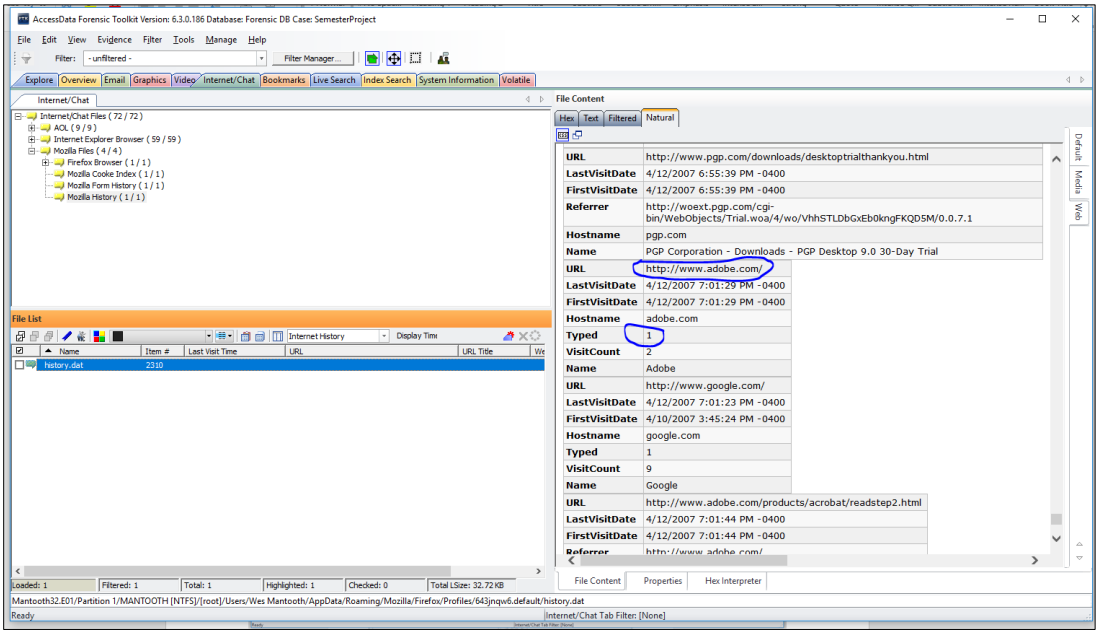
21. Identify any URLs that were visited by manually typing the address.

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


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Internet/Chat
Internet/Chat Files (72 / 72)
AOL (9 / 9)
Internet Explorer Browser (59 / 59)
Mozilla Files (4 / 4)
Firefox Browser (1 / 1)
Mozilla Cooke Index (1 / 1)
Mozilla Form History (1 / 1)
Mozilla History (1 / 1)
File List
Internet History
Display Tim
Name
Item #
Last Visit Time
URL
URL Title
history.dat
2310
Loaded: 1
Filtered: 1
Total: 1
Highlighted: 1
Checked: 0
Total LSize: 32.72 KB
File Content
Hex Text Filtered Natural
ByteOrder LE
URL http://en-us.www.mozilla.com/en-US/firefox/2.0.0.3/firstrun/
LastVisitDate 4/10/2007 1:55:43 PM -0400
FirstVisitDate 4/10/2007 1:55:43 PM -0400
Hostname en-us.www.mozilla.com
Name Welcome to Firefox
URL http://en-us.start2.mozilla.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official
LastVisitDate 4/10/2007 4:19:45 PM -0400
FirstVisitDate 4/10/2007 1:55:43 PM -0400
Hostname en-us.start2.mozilla.com
Hidden 1
VisitCount 3
URL http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official
LastVisitDate 4/10/2007 4:19:45 PM -0400
FirstVisitDate 4/10/2007 1:55:43 PM -0400
Hostname google.com
Name Mozilla Firefox Start Page
VisitCount 3
URL http://www.google.com/
LastVisitDate 4/10/2007 4:20:19 PM -0400
FirstVisitDate 4/10/2007 3:45:24 PM -0400
Hostname google.com
Typed 1
VisitCount 4
File Content
Properties
Hex Interpreter
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Roaming/Mozilla/Firefox/Profiles/643jnqw6.default/history.dat
Ready
Internet/Chat Tab Filter: [None]

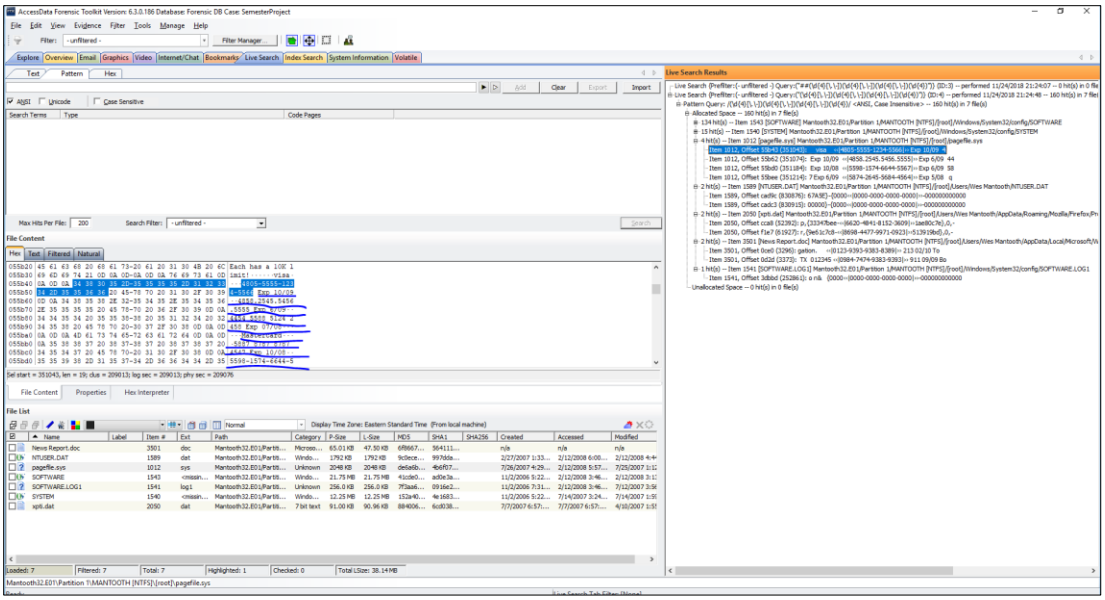

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: SemesterProject
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Internet/Chat
Internet/Chat Files (72 / 72)
AOL (9 / 9)
Internet Explorer Browser (59 / 59)
Mozilla Files (4 / 4)
Firefox Browser (1 / 1)
Mozilla Cooke Index (1 / 1)
Mozilla Form History (1 / 1)
Mozilla History (1 / 1)
File List
Internet History
Display Tim
Name
Item #
Last Visit Time
URL
URL Title
history.dat
2310
Loaded: 1
Filtered: 1
Total: 1
Highlighted: 1
Checked: 0
Total LSize: 32.72 KB
File Content
Hex Text Filtered Natural
URL http://en.wikipedia.org/wiki/Human_body_disposal#Secret_disposal
LastVisitDate 4/10/2007 4:21:40 PM -0400
FirstVisitDate 4/10/2007 4:21:40 PM -0400
Hostname en.wikipedia.org
URL http://www.mamma.com/
LastVisitDate 4/10/2007 4:21:56 PM -0400
FirstVisitDate 4/10/2007 4:21:56 PM -0400
Hostname mamma.com
Typed 1
VisitCount 2
Name Mamma Metasearch - The Mother of All Search Engines
URL http://www.mamma.com/Mamma?utfout=1&qtype=0&query=stealing+checks&Submit=%C2%A0%C2%A0Search%C2%A0%C2%A0
LastVisitDate 4/10/2007 4:22:17 PM -0400
FirstVisitDate 4/10/2007 4:22:17 PM -0400
Referrer http://www.mamma.com/
Hostname mamma.com
Name stealing checks - Mamma Metasearch
URL http://www.mamma.com/Mamma?utfout=1&qtype=0&query=making+meth&Submit=%C2%A0%C2%A0Search%C2%A0%C2%A0
LastVisitDate 4/10/2007 4:22:30 PM -0400
FirstVisitDate 4/10/2007 4:22:30 PM -0400
Referrer http://www.mamma.com/
File Content
Properties
Hex Interpreter
Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Roaming/Mozilla/Firefox/Profiles/643jnqw6.default/history.dat
Ready
Internet/Chat Tab Filter: [None]

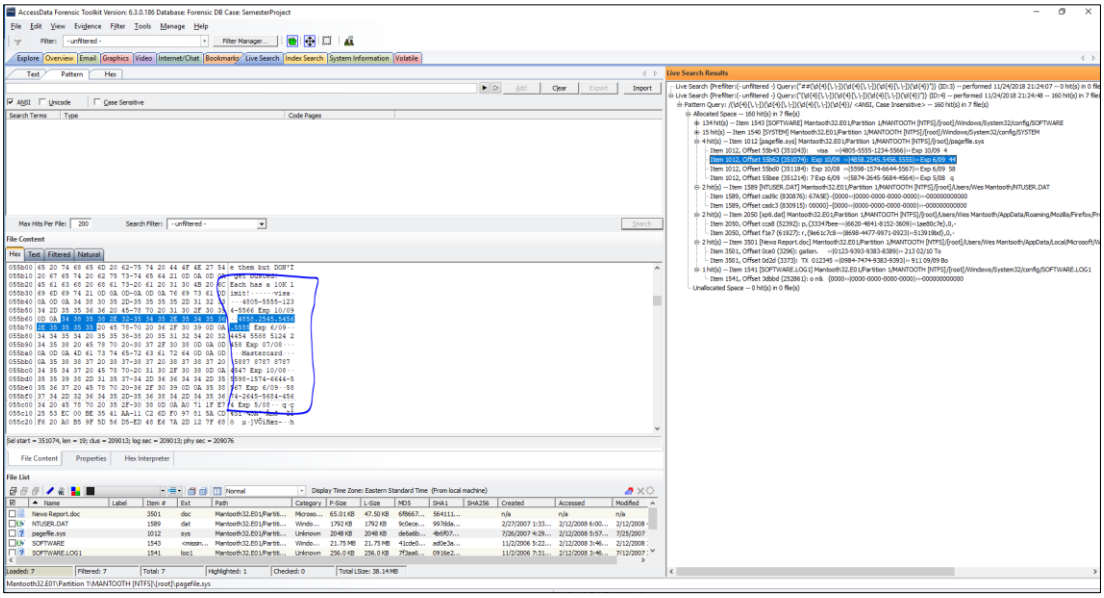


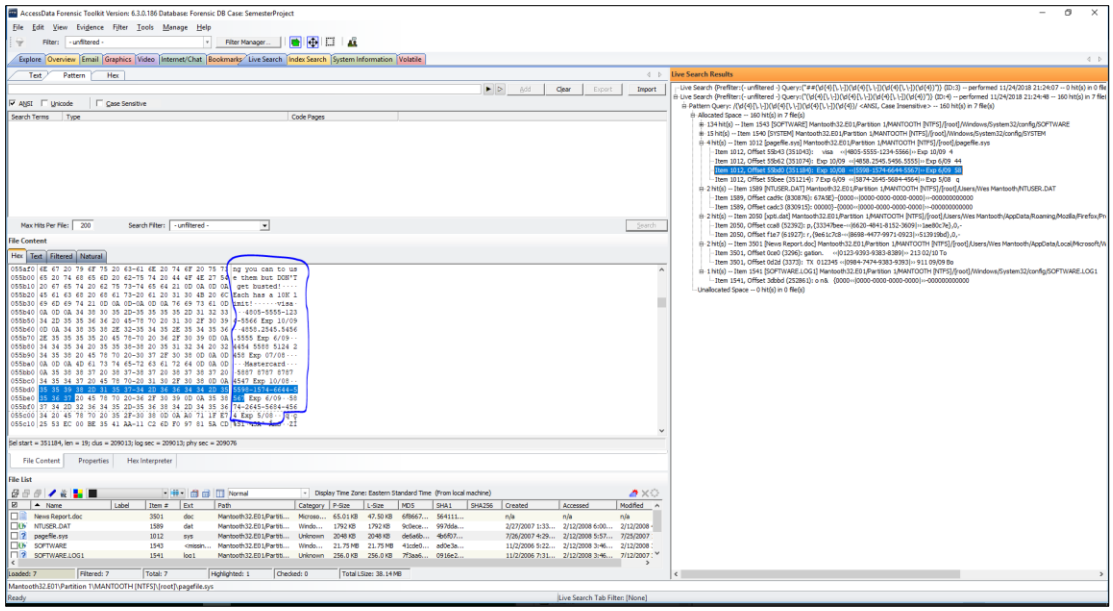


22. Identify any credit card numbers on the drive.

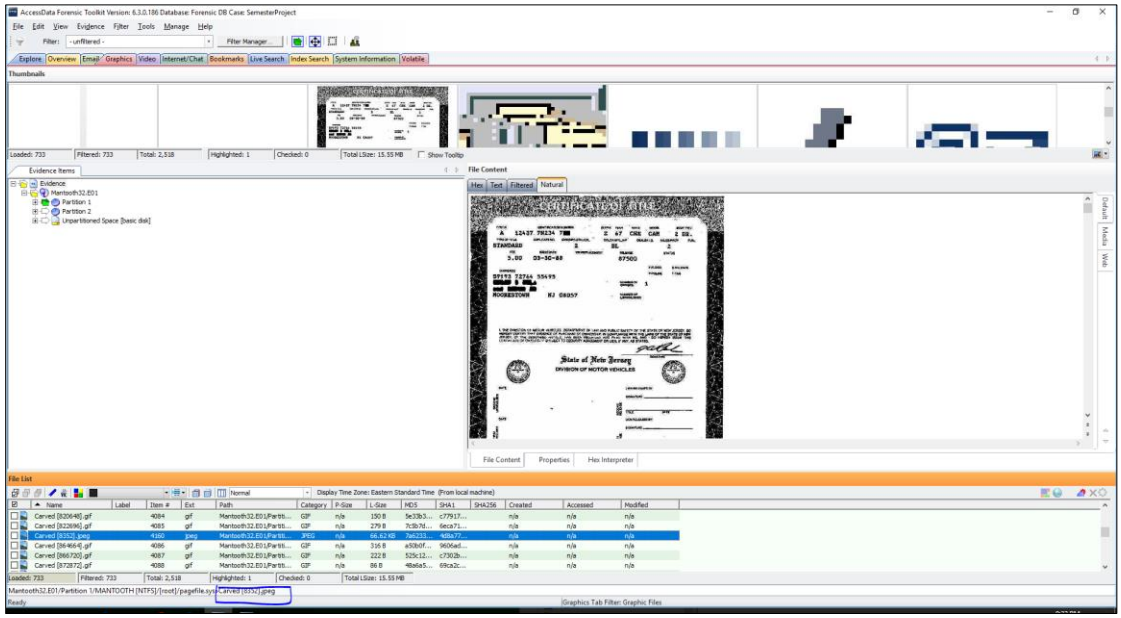
After performing **Live search** and **Index search** in FTK, I recovered these credit card numbers as shown.

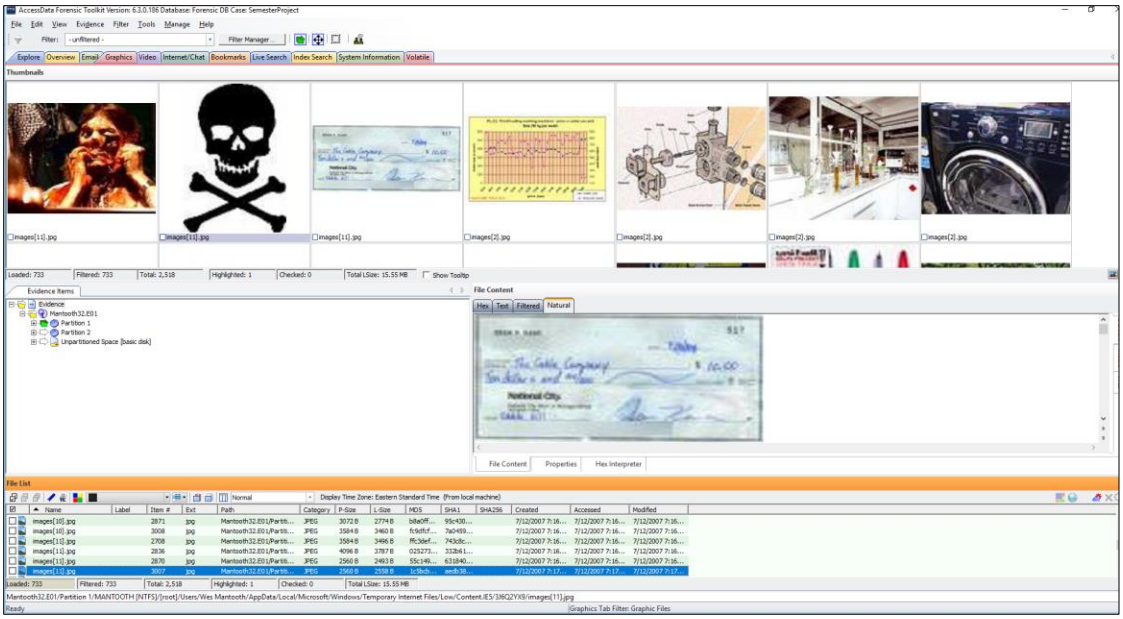


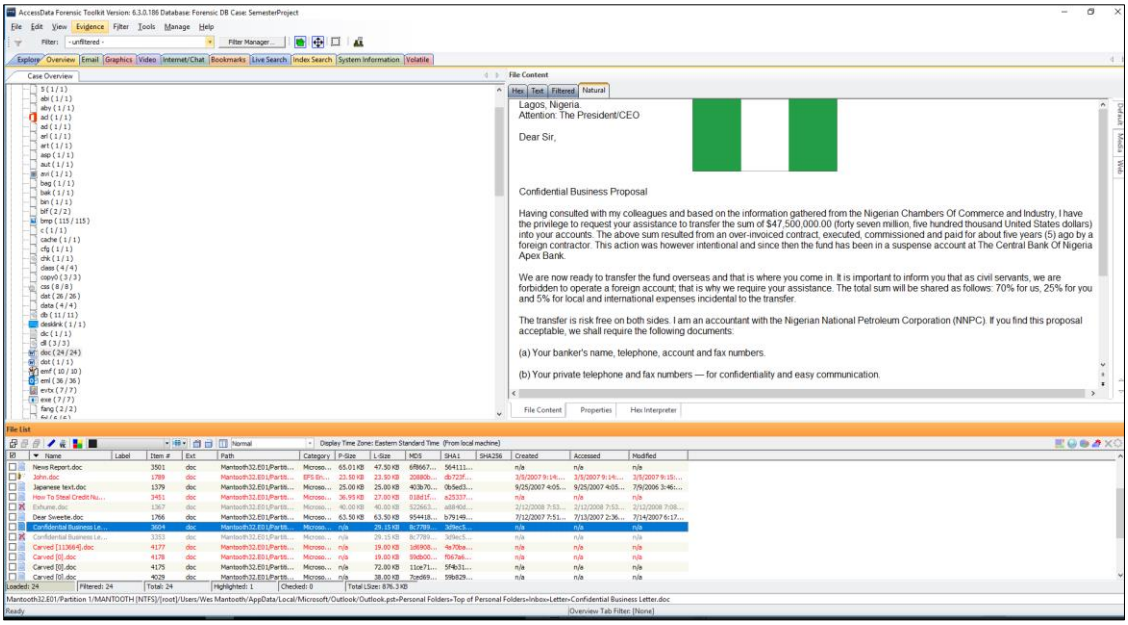


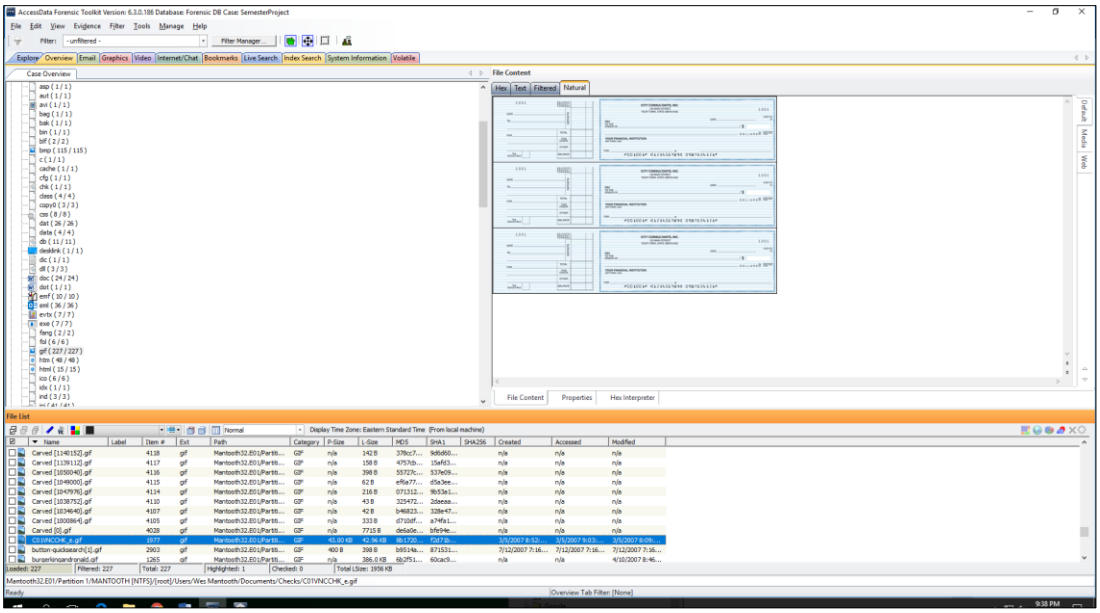


23. Provide a few examples of theft, title, checks, scam, and forensics.






Lagos, Nigeria.
Attention: The President/CEO
Dear Sir,
Confidential Business Proposal
Having consulted with my colleagues and based on the information gathered from the Nigerian Chambers Of Commerce and Industry, I have the privilege to request your assistance to transfer the sum of $47,500,000.00 (forty seven million, five hundred thousand United States dollars) into your accounts. The above sum resulted from an over-invoiced contract, executed, commissioned and paid for about five years (5) ago by a foreign contractor. This action was however intentional and since then the fund has been in a suspense account at The Central Bank Of Nigeria Apex Bank.
We are now ready to transfer the fund overseas and that is where you come in. It is important to inform you that as civil servants, we are forbidden to operate a foreign account; that is why we require your assistance. The total sum will be shared as follows: 70% for us, 25% for you and 5% for local and international expenses incidental to the transfer.
The transfer is risk free on both sides. I am an accountant with the Nigerian National Petroleum Corporation (NNPC). If you find this proposal acceptable, we shall require the following documents:
(a) Your banker's name, telephone, account and fax numbers.
(b) Your private telephone and fax numbers — for confidentiality and easy communication.



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

Conclusion

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

I figured out following:

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

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