

ITIS 5250
Ruchira Pokhriyal
Semester Project
12/04/2018

Overview

A local group of criminals has been involved in check and credit card frauds, ATM scams and other financial crimes. These criminals are known to use a great deal of technology and hence, Detective Ketchum has asked me to process a desktop computer which belongs to a gang member called Wes Mantooth. For my examination, I have been provided with an EnCase format forensic image of this computer called Mantooth32.E01 by one of the. Therefore, for this project, I will be searching for evidence such as owner of the computer, specific software tools that are installed, recently run programs, user passwords, etc. Additionally, I will be looking for credit card numbers, checks, scam, browser history, information about the OS and other financial crimes.

Forensic Acquisition and Exam Preparation

I am provided with the forensic image '**Mantooth32.E01**', which was made by one of the lab techs of Detective Ketchum. I loaded this image to FTK Imager (Version 4.1.1.1) to verify the image integrity. Additionally, I used FTK (Version 6.3.0.186) for evidence processing.

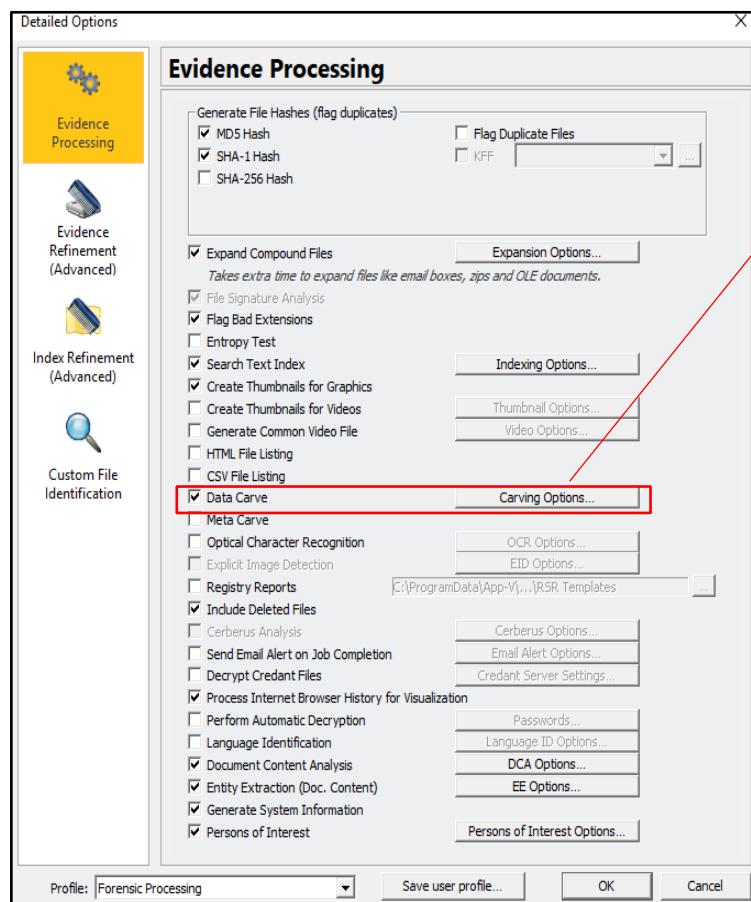
Hash Verification Results:

As seen below, both, the computed and stored hash values match:

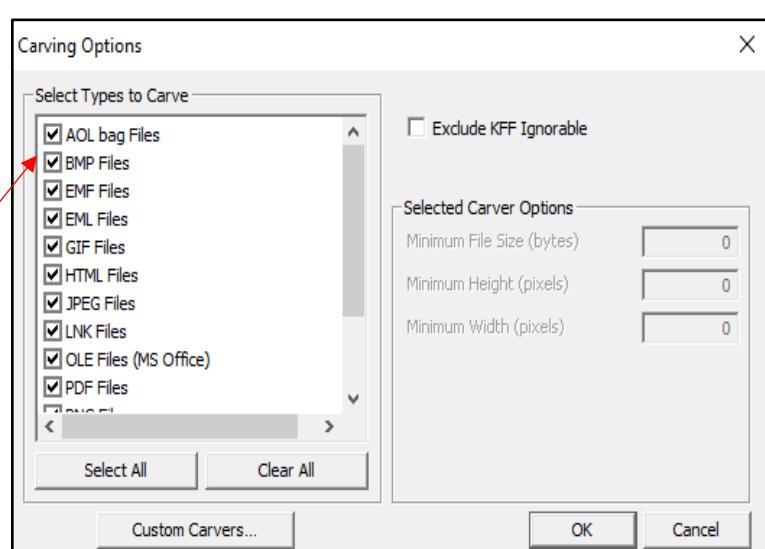
Drive/Image Verify Results	
<input type="checkbox"/>	
Name	Mantooth32.E01
Sector count	250879
MD5 Hash	
Computed hash	31217210a1a69f272079a3bde3d9d8fc
Stored verification hash	31217210a1a69f272079a3bde3d9d8fc
Verify result	Match
SHA1 Hash	
Computed hash	12e4ac047e328ca2bd63a4d65df25b3ecba55769
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image
<input type="button" value="Close"/>	

I customized the following options in FTK:

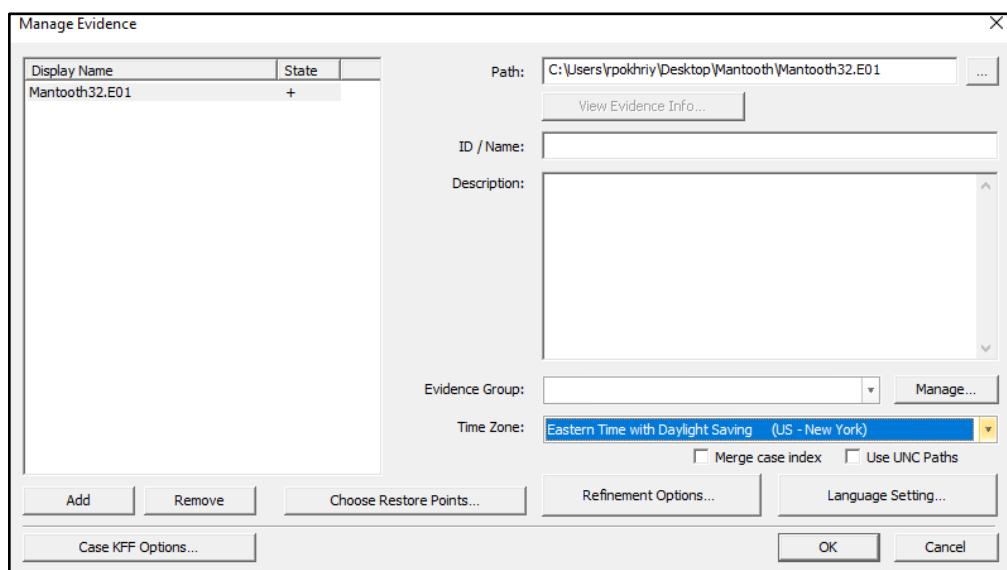
Evidence Processing using FTK:



Carving Options:

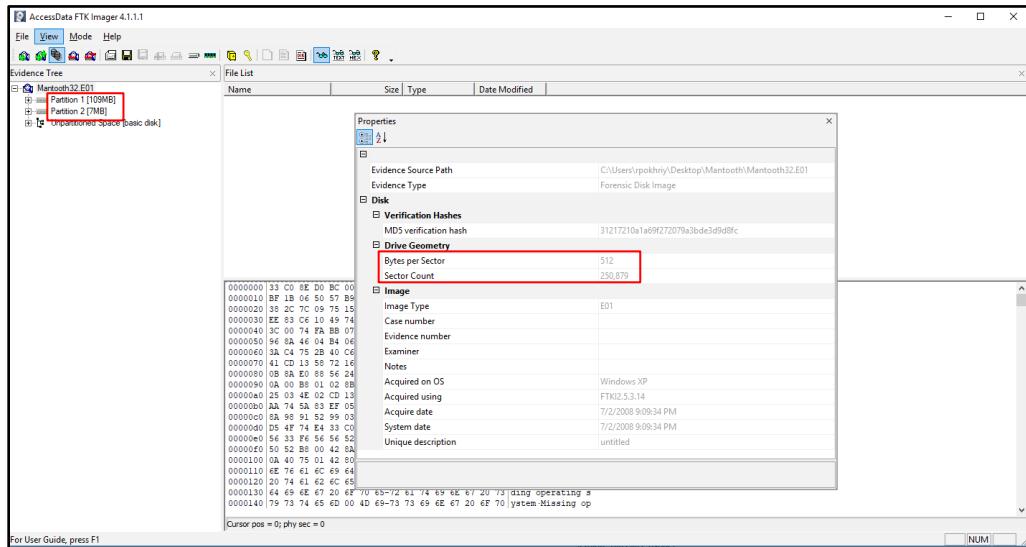


Adding Image:



Findings and Report

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



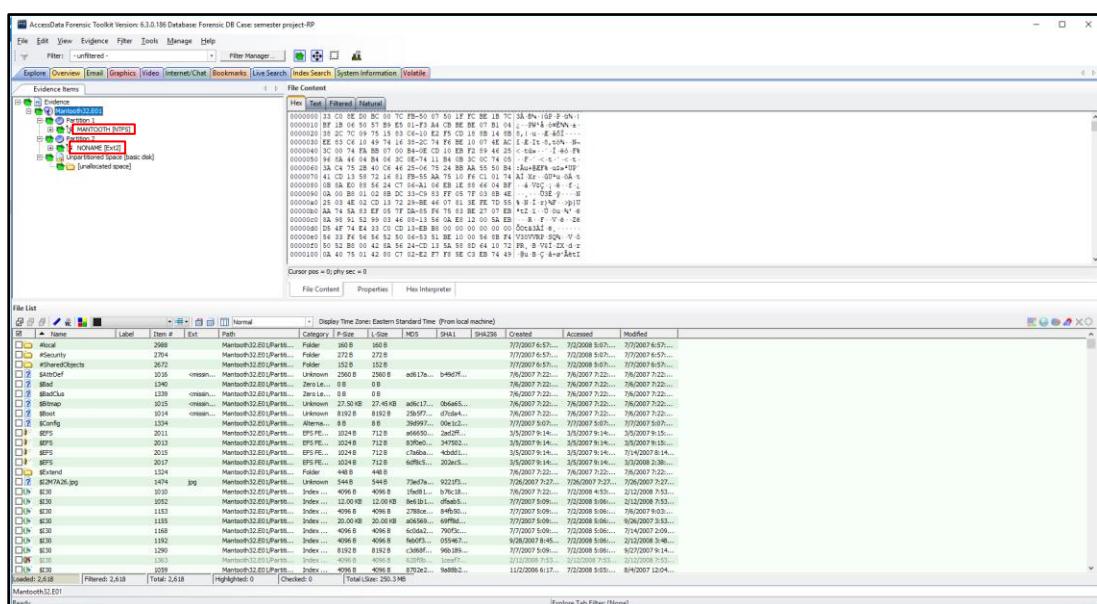
The space on the computer hard drive can be obtained by multiplying the **Bytes per Sector** and **Sector Count** values mentioned in the Drive Geometry.

Therefore, **512 * 250,897=128,450,048 bytes**.

Also, from FTK Imager, it can be seen that the total partition comprises of **109MB+7MB= 116MB (which is used)**

2. Identify the types of file systems in use.

As seen above, the two types of file systems in use are: **NTFS** and **Ext2**.



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

The ‘System Information’ in FTK shows the service pack of the Operating System is ‘Windows Vista Ultimate’ and the current version is **6.0**. And, as shown below, similar information is obtained upon exporting SOFTWARE file from FTK into the Registry Viewer.

The top window is titled "AccessData Forensic Toolkit Version 6.0.0.100 Database Forensic DB Case: semester project RP". It has tabs for "Evidence", "Overview", "Email", "HexView", "File Manager", "Disk", "Image", "Results", "Report", "Video", "InternetCache", "Bookmarks", "Live Search", "Index Search", and "System Information". The "System Information" tab is selected. The left pane shows a tree view of registry keys under "Windows NT\CurrentVersion\Run". The right pane shows a list of registry keys with their names, types, and data values. A red box highlights the "Windows Update" key under "Software\Microsoft\Windows\CurrentVersion\Run".

The bottom window is titled "AccessData Registry Viewer - [D:\02\Partition 3\HewiOCh\mpg]". It has tabs for "File", "Edit", "Report", "View", "Window", and "Help". The left pane shows a tree view of registry keys under "Windows NT\CurrentVersion\Run". The right pane shows a table of registry keys with columns "Name", "Type", and "Data". A red box highlights the "Windows Update" key under "Software\Microsoft\Windows\CurrentVersion\Run". The status bar at the bottom left shows "Last Written Time: 07/23/2009 11:53:52 UTC", "OS Install Date (UTC): Tue Feb 27 19:20:00 2007", and "OS Install Date (Local): Tue Feb 27 19:20:00 2007".

4. Find the date the OS was installed.

In FTK, the Windows NT Registry shows that the OS Install date is: **2/27/2007**. Additionally, the Owner Information in System Information and SOFTWARE file, when exported to registry viewer, shows the Install date as an epoch timestamp: **1172604123**. I converted this date to human readable format using epoch converter and the date was found to be: **2/27/2007**.

This screenshot is identical to the one above it, showing the AccessData Registry Viewer interface with the same registry keys and timestamp details in the status bar.

The top screenshot shows the AccessData Registry Viewer interface with the 'SYSTEM' file open. The 'Time Zone' key under 'CurrentControlSet\Control\TimeZoneInformation' is highlighted with a red box. The middle screenshot is a web-based timestamp converter from epochconverter.com. It shows the epoch time 1172604123 being converted to a human-readable date and time: Tuesday, February 27, 2007 7:22:03 PM GMT-05:00. The bottom screenshot shows the Windows registry viewer with the same 'Time Zone' key highlighted.

5. Identify the Time Zone information for the computer.

The time zone information can be found after exporting the **SYSTEM** file into the registry viewer from FTK, and under 'Terminal Server', the time zone is shown as 'Mountain Standard Time'.

This screenshot shows the AccessData Registry Viewer with the 'Windows' registry file open. The 'Time Zone' key under 'CurrentControlSet\Control\TimeZoneInformation' is highlighted with a red box. The right pane displays the key's properties and data values, including the 'Time Zone' value set to 'Mountain Standard Time'.

6. Show the owner of the computer.

In the Windows NT Registry under Overview tab in FTK, the owner of the computer was found to be 'Wes Mantooth'. Even the system information shows the registered owner of the computer to be 'Wes Mantooth'.

The screenshot displays two windows side-by-side. The top window is 'AccessData Registry Viewer - [Common Area]' showing the Windows NT registry keys. The bottom window is 'Microsoft(Windows NT)\CurrentVersion' showing the system properties. Both windows have a red box highlighting the 'RegisteredOwner' key, which is set to 'Wes Mantooth'.

AccessData Registry Viewer - [Common Area]

Name	Type	Data
CurrentVersion	REG_SZ	6.0
CurrentBuildNumber	REG_SZ	6000
CurrentBuild	REG_SZ	6000
SoftwareType	REG_SZ	System
CurrentType	REG_SZ	Multiprocessor Free
InstallDate	REG_DWORD	0x45E4B4DB (1172604123)
RegisteredOrganization	REG_SZ	Volturi Enterprises
RegisteredOwner	REG_SZ	Wes Mantooth
SystemRoot	REG_SZ	C:\Windows
ProductName	REG_SZ	Windows Vista (TM) Ultimate
ProductId	REG_SZ	8950-378-0753292-71704
DigitalProductId	REG_BINARY	A4 00 00 00 00 00 00 00 38 39 35 38 30 2D 33 37 38 2D ...
DigitalProductid	REG_BINARY	F8 04 00 00 00 00 00 30 38 39 00 35 00 38 00 30 00 ...
BuildNumber	REG_SZ	6000
BuildLab	REG_SZ	6000.vista_gdr.071009-1548
BuildLabEx	REG_SZ	6000.16575.0804.vista_gdr.071009-1548
BuildGUID	REG_SZ	86727b72-ee31-4d89-9d85-b0ec5d2da9c
CSDBuildNumber	REG_SZ	2
PathName	REG_SZ	C:\Windows

Microsoft(Windows NT)\CurrentVersion

Key Properties	Value
Last Written Time	2/12/2008 0:08:52 UTC
OS Install Date (UTC)	Tue Feb 27 19:22:03 200
OS Install Date (Local)	Tue Feb 27 14:22:03 200

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

All the Users of the computer are: Administrator, Laurent, Dracula, Wes Mantooth and Guest.

User	SID	User Name	Current LAN Hash	Previous LAN Hash	Current NT Hash	Previous NT Hash
S-1-5-21-3166329-3263506726-1320359247-1003		Laurent			D90D8508030C90473114BD90EFF3FE9E	
S-1-5-21-3166329-3263506726-1320359247-1002		Dracula			4F892A810F871BC64DOC1689322204E9	
S-1-5-21-3166329-3263506726-1320359247-1000		Wes Mantooth				
S-1-5-21-3166329-3263506726-1320359247-501		Guest				
S-1-5-21-3166329-3263506726-1320359247-500		Administrator			31D6CFE0D16AE931B73C59D7E0C089C0	

As seen in the screenshots below, following are the logon count of all the users:

Admin: 1

Guest: 0

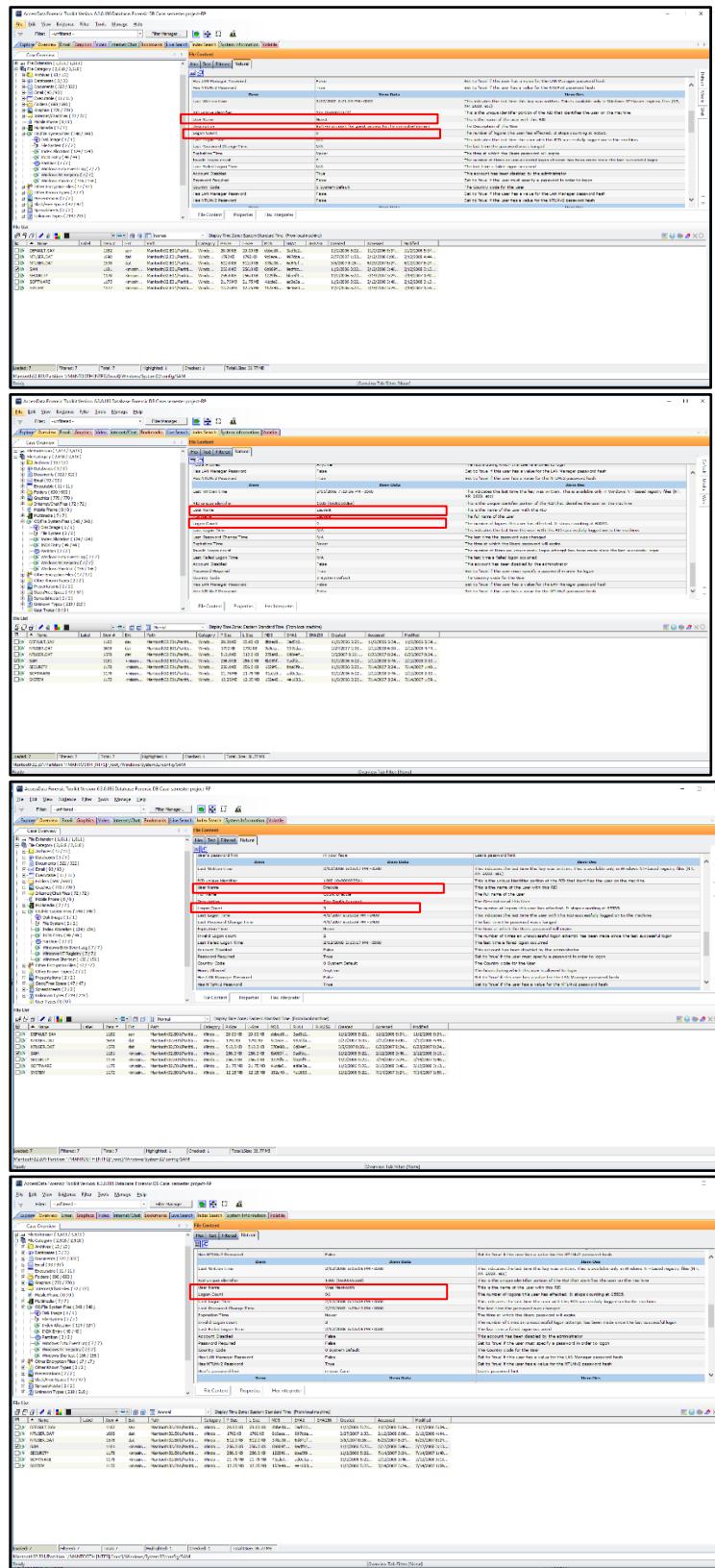
Laurent: 0

Dracula: 3

Wes Mantooth: 96

Thus, making 'Wes Mantooth' the most active user of the computer with a logon count of 96 times.

Item	Item Data	Item Desc
Last Written Time	3/27/2009 2:12:05 PM -0500	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, 2000, XP).
RID unique identifier	500 (0x0000014)	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.
Logon Count	1	The number of logons this user has effected. It stops counting at 43555.
Last Logon Time	3/27/2009 8:02:02 AM -0500	This indicates the last time user with this RID was successfully logged on to the machine.
Logon Count Change Time	3/27/2009 8:08:19 AM -0500	The last time the password was changed.
Expiration Time	Never	The time at which the user account will expire.
Invalid Logon Count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon.
Last Failed Logon Time	N/A	The last time a failed logon occurred.
Logon Count Maximum	True	Set to true if the user can log on as administrator.
Password Required	True	Set to true if the user must specify a password in order to logon.
Country Code	0 SystemDefault	The Country code for the user.
Hour Interval	Anytime	The hours during which the user is allowed to logon.
Has LAN Manager Password	False	Set to true if the user has a value for the LAN Manager password hash.
Has NTLMv2 Password	True	Set to true if the user has a value for the NTLMv2 password hash.



8. Identify user accounts and who uses the account.

Exporting SAM file into registry viewer through FTK, following user accounts are seen: **Wes Mantooth**, **Dracula** and **Laurent**. Their account disabled status is false. Amongst them, **Dracula** and **Wes Mantooth** use their account since their logon counts are 3 and 96 respectively.

Key Properties:

- Last Written Time: 2/12/2008 20:13:36 UTC
- SID unique identifier: 1000
- User Name: **Wes Mantooth**
- Logon Count: **96**
- Last Logon Time: 2/12/2008 20:13:36 UTC
- Last Password Change Time: 2/23/2008 18:29:13 UTC
- Expiration Time: Never
- Invalid Logon Count: 3
- Last Failed Logon Time: Never
- Account Disabled: **No**

Key Properties:

- Password Required: <need "SyKey" file>
- Country Code: 0 (System Default)
- Home Directory: <need "SyKey" file>
- LM Hash: <need "SyKey" file>
- NT Hash: <need "SyKey" file>
- Old NT Hash: <need "SyKey" file>
- Old LM Hash: <need "SyKey" file>

Key Properties:

- Last Written Time: 2/12/2008 20:13:37 UTC
- SID unique identifier: 1001
- User Name: **Dracula**
- Logon Count: **3**
- Last Logon Time: 4/2/2007 03:59:47 UTC
- Last Password Change Time: 4/2/2007 03:59:47 UTC
- Expiration Time: Never
- Invalid Logon Count: 2
- Last Failed Logon Time: Never
- Account Disabled: **No**

Key Properties:

- Password Required: <need "SyKey" file>
- Country Code: 0 (System Default)
- Home Directory: <need "SyKey" file>
- LM Hash: <need "SyKey" file>
- NT Hash: <need "SyKey" file>
- Old NT Hash: <need "SyKey" file>
- Old LM Hash: <need "SyKey" file>

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 Logon Time: Never
- Account Disabled: **No**

Key Properties:

- Password Required: <file>
- Country Code: 0 (System Default)
- Home Directory: <need "SyKey" file>
- LM Hash: <need "SyKey" file>
- NT Hash: <need "SyKey" file>
- Old NT Hash: <need "SyKey" file>
- Old LM Hash: <need "SyKey" file>

9. Acquire user passwords.

I exported SAM and SYSTEM files from FTK TO PRTK, and was able to crack the passwords for two user accounts, namely Dracula and Wes Mantooth.

Password for Dracula was found to be: **canine**

Password for Wes Mantooth was found to be: **tooth**

The screenshot shows the AccessData Forensic Toolkit interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, Help. The main window has tabs for Explorer, Overview, Email, Graphics, Video, Internet/Chat, Bookmarks, Live Search, Indexer, System Information, and Violate. The System Information tab is active, displaying 'Registry SYSTEM Information' with details like Active Control Set, Computer Name, Time Zone Bias, etc. Below it is a file list table:

Name	Label	Ext	Path	Category	File Size	MD5	SHA256	Created	Accessed	Last Modif.
CONSOLE.LOG	1.00				1.00 KB	9e0...d0	4f2...00	1/22/2008 9:24...	1/22/2008 9:24...	1/22/2008 9:24...
NTUSER.DAT	1.00		H:\Windows\...\ntuser.dat	File System	1,792 KB	1762 KB	997da...	2/27/2007 1:11...	2/22/2008 6:40...	2/22/2008 6:40...
NTUSER.DAT	1.00		H:\Windows\...\ntuser.dat	File System	512.0 KB	512.0 KB	378w9...	6d94ef...	3/23/2007 8:24...	6/13/2007 8:24...
SECURITY	1.00		H:\Windows\...\security	File System	256.0 KB	256.0 KB	bb459...	1/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 3:24...
SORTNAME	1.00		H:\Windows\...\sortname	File System	21.71 MB	21.71 MB	a3de1...	1/2/2006 5:22...	7/13/2007 8:46...	7/13/2007 8:46...
SYSTEM	1.00		H:\Windows\...\system	File System	1.00 KB	1.00 KB	4c47a...	1/2/2006 5:22...	7/14/2007 3:24...	7/14/2007 3:24...

At the bottom, it says 'Jobs: 7 Filtered: 7 Total: 7 Highlighted: 1 Checked: 2 Total User: 36.77 MB'.

The screenshot shows the AccessData Password Recovery Toolkit interface. The top menu bar includes File, Edit, View, Tools, Help. The main window has tabs for Explorer, Overview, Email, Graphics, Video, Internet/Chat, Bookmarks, Live Search, Indexer, System Information, and Violate. The System Information tab is active, displaying a list of cracked SAM entries:

Job Name	Attack Type	Status	Result
SAM	Windows account: Administrator [NT hash]	Finished	"canine"
SAM	Windows account: Dracula [NT hash]	Finished	"Empty"
SAM	Windows account: Guest [NT hash]	Finished	"Empty"
SAM	Windows account: Laurent [LM hash]	Finished	"Empty"
SAM	Windows account: Wes Mantooth [NT hash]	Finished	"tooth" [HEX=0D7ec8f00ef5274069]

On the left, there's an 'Add Job Wizard (Page 2 of 2)' dialog showing 'File Types' selected and 'SAM' chosen. On the right, there's a 'Properties' panel for the 'Sam' job.

10. Identify the last date Wes Mantooth logged on.

After exporting the SAM file from FTK to registry viewer, the last logon time of Wes Mantooth was found to be: **2/12/2008**.

The screenshot shows the AccessData Registry Viewer interface. On the left, the tree view displays the SAM file structure under 'SAM\11B1\Sam'. A selected node 'User' has its properties listed in the 'Key Properties' panel on the right. The 'Last Logon Time' field is highlighted in red and contains the value '2/12/2008 20:13:16 UTC'. Other properties shown include 'Last Written Time' (2/12/2008 20:13:16 UTC), 'SID Unique Identifier' (1000), and 'User Name' (Wes Mantooth). The 'Data' pane on the right shows binary data corresponding to the registry keys.

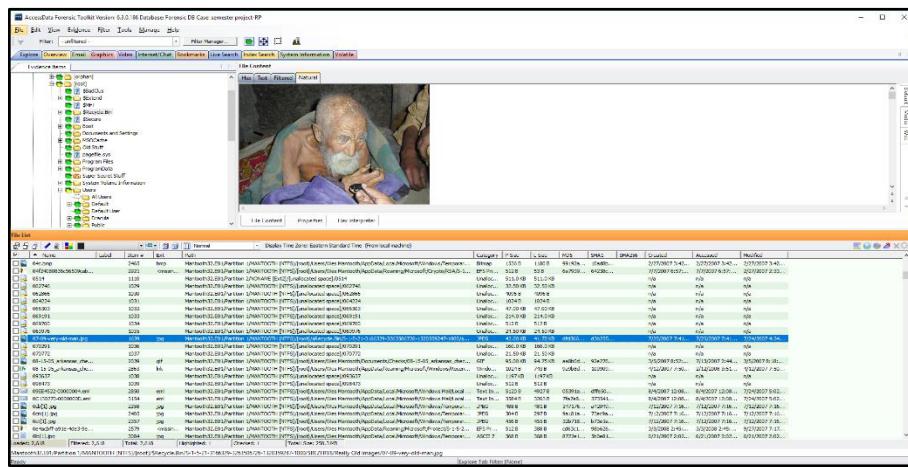
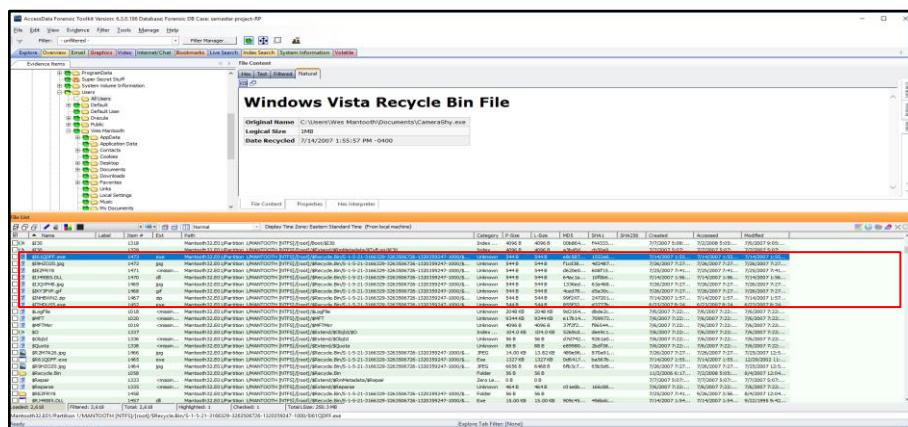
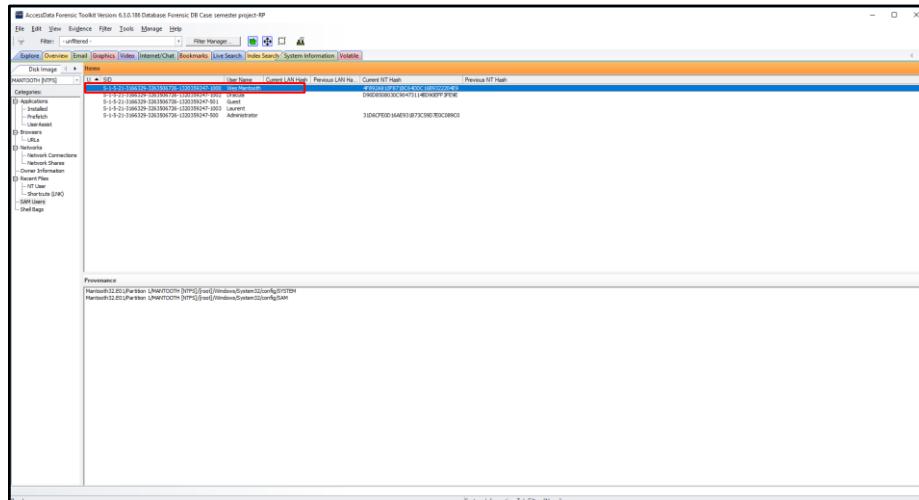
As shown below, the last date when Wes Mantooth logged on can also be seen in the SAM file in FTK:

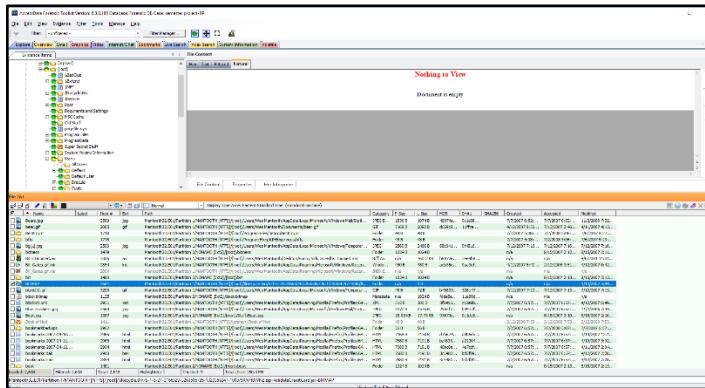
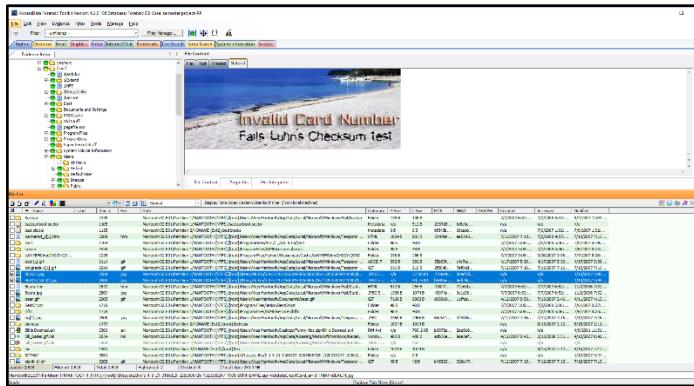
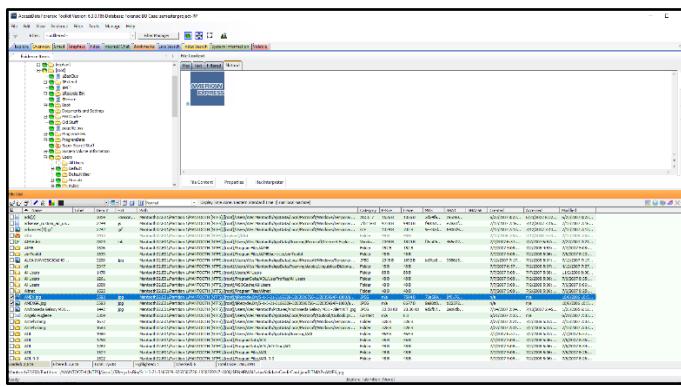
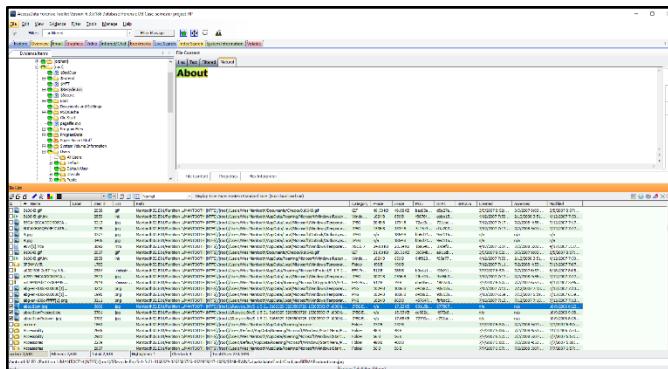
The screenshot shows the AccessData Forensic Toolkit interface. The 'Case Overview' pane on the left shows various forensic artifacts. The 'File Context' pane on the right displays the properties for the user 'Wes Mantooth'. The 'Last Logon Time' field is highlighted in red and contains the value '2/12/2008 20:13:16 UTC'. Below this, the 'Last Written Time' is also listed as '2/12/2008 20:13:16 UTC'. The 'Data' pane at the bottom shows the raw binary data of the SAM file.

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

In the 'System Information', under **SAM users**, the SID for Wes Mantooth is found to be:

'**S-1-5-21-3166329- 3263506726-1320359247-1000**'. The File Category in FTK hence, shows that the files shown in below screenshots were placed in the recycle bin by **Wes Mantooth**.





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

The exported **SAM** file in registry viewer, displays the location of the **user picture tile** for Wes Mantooth's account. Then, exploring the SAM file in FTK, under the graphics tab, I was able to find the mentioned picture (**Carved[28724].bmp**) as shown below:

13. Identify any pictures of Wes Mantooth.

In FTK, under the Email tab, I found an email with the subject '**Hey Mom**', which has an attachment called '**Wes.jpg**'. I then explored the graphics tab and found this picture of Wes Mantooth, named **Wes.jpg**.

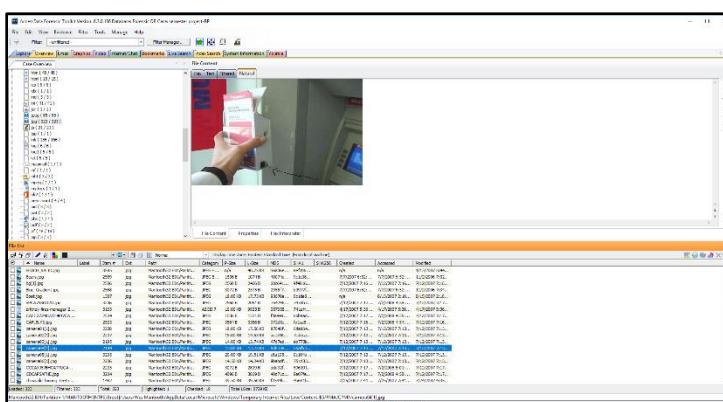
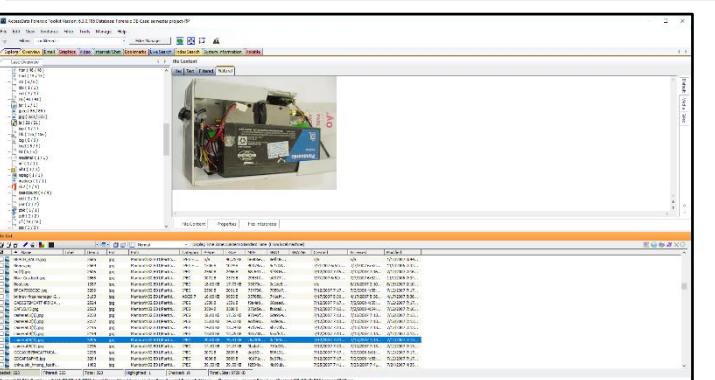
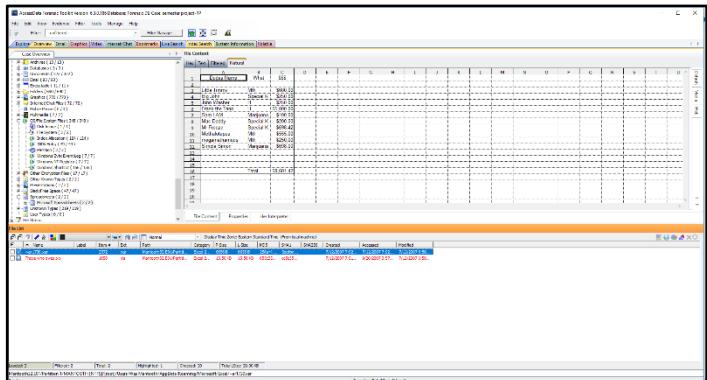
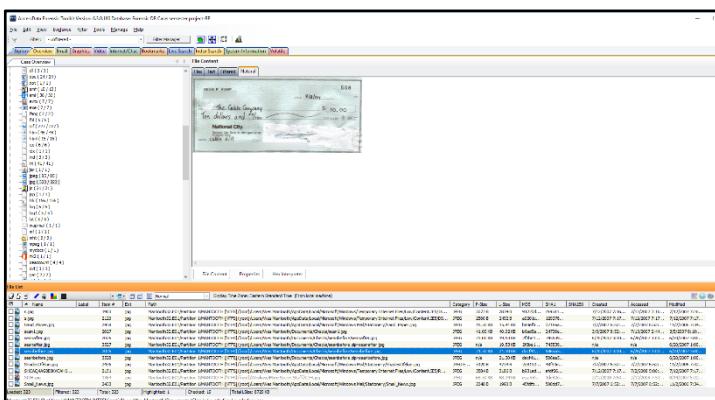
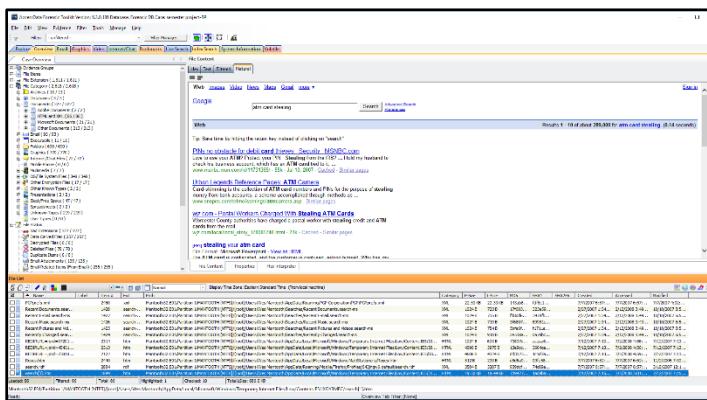
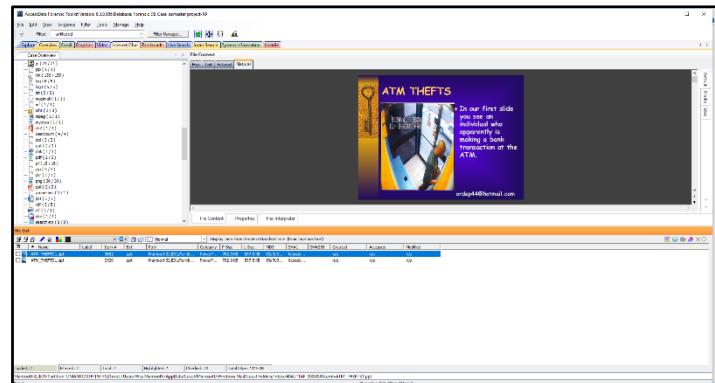
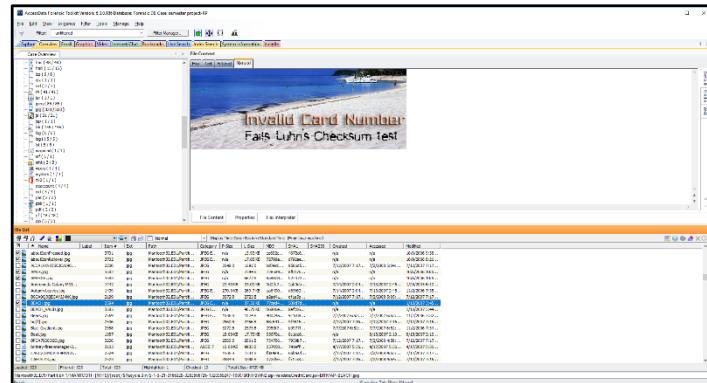
The screenshot shows the AccessData Forensic Toolkit interface with the following details:

- File Manager:** Shows a tree view of file types: Email (125), Email Attachments (125), Email Received Items (From Email) (255 / 255), and Forwarded Items (12).
- Email Items:** A list of emails from "Wes Mantooth" to himself, all sent on 7/12/2007 at 20:46. The subject is "sample test".
 - Attachment: "wes.jpg" (size 10KB)
 - Attachment: "wes part 1.gpg" (size 10KB)
 - Attachment: "wes part 2.gpg" (size 10KB)
 - Attachment: "wes part 3.gpg" (size 10KB)
 - Attachment: "wes part 4.gpg" (size 10KB)
 - Attachment: "wes part 5.gpg" (size 10KB)
 - Attachment: "wes part 6.gpg" (size 10KB)
 - Attachment: "wes part 7.gpg" (size 10KB)
 - Attachment: "wes part 8.gpg" (size 10KB)
 - Attachment: "wes part 9.gpg" (size 10KB)
 - Attachment: "wes part 10.gpg" (size 10KB)
- File Content:** Displays the email body, attachments, and a preview of the image.
- Email Conversation:** Shows the exchange between Wes Mantooth and himself.
- Email Attachments:** A list of attachments found in the email, including "10200F9F-00000004.eml" and "10200F9F-00000005.eml".
- File Content:** Shows the raw file content of the attachments.

A screenshot of the AccessData Forensic Toolkit version 5.0.2.180 Database Forensic DB Case viewer project-1-SP. The interface includes a top menu bar with File, Edit, View, Evidence, Filter, Tools, Manage, Help, and a toolbar with icons for Home, Filter, Index, Search, and Attachments. Below the menu is a navigation bar with tabs for Explorer, Overview, Email, Graphics, Video, Internet/Chat, Bookmarks, Live Search, Index Search, System Information, and Totals. A sidebar on the left lists 'Evidence Items' such as Media, Evidence, Hashes, and Forensics. The main area displays a grid of evidence items with preview thumbnails. One item, 'mcafee_00000000000000000000000000000000.jpg', is selected and shown in a large preview window at the bottom. This preview shows a man with a beard and mustache, looking slightly to the side. Below the preview are buttons for Edit Content, Properties, and Video Interpreter. At the bottom, a 'File List' table provides a detailed view of the selected file, including columns for Name, Type, Size, Path, Category, MD5, SHA1, and more. The file path is listed as 'mcafee_00000000000000000000000000000000.jpg'.

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

In FTK's Overview tab, I came across several pictures related to fraud and financial crimes. Few of these pictures are shown below:



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

I discovered the following software tools which were installed on the computer, after exporting the SOFTWARE file from FTK into registry viewer: AccessData FTK Imager, AccessData Registry Viewer, AccessData DNA3 Worker, TrueCrypt, BestCrypt etc. These software tools were also found in 'Installed Applications' under System Information.

The image shows two windows side-by-side. The left window is 'AccessData Registry Viewer Version 6.0.0.100' showing the registry keys for 'Software\Microsoft\Windows\CurrentVersion\Run'. Several entries are highlighted with red boxes, including 'AccessData FTK Imager', 'AccessData Registry Viewer', 'AccessData DNA3 Worker', 'TrueCrypt', 'BestCrypt', and 'WinRAR'. The right window is 'AccessData Forensic Toolkit Version 6.0.0.100 Database: Forensic DB Case: semester project-0F' showing the 'System Information' tab. It lists various installed applications with their publishers, install dates, and file paths. Notable entries include 'AccessData Registry Viewer' (Publisher: AccessData Incorporated, Install Date: 8/24/2008 8:43:08 AM), 'AccessData DNA3 Worker' (Publisher: Microsoft Corporation, Install Date: 8/27/2007 10:28 AM), 'TrueCrypt' (Publisher: TrueCrypt Development Team, Install Date: 8/27/2007 10:28 AM), and 'WinRAR' (Publisher: WinRAR Ltd, Install Date: 8/27/2007 10:28 AM).

16. Identify the most commonly opened programs.

Following is a screenshot of the **prefetch** tab under System Information in FTK, which shows the list of the most commonly opened programs.

The image shows the 'Prefetch' tab in the 'System Information' section of the AccessData Forensic Toolkit. It displays a table of prefetch files with columns for File Path, Run Count, and Last Run Time. The table is heavily redacted with a large red box. The first few rows show entries like 'DEVICEHARDISKVOLUME1\WINDOWS\EXPLORER.EXE' with a run count of 15 and last run time of 8/24/2007 8:47:34 AM, and 'DEVICEHARDISKVOLUME1\WINDOWS\SYSTEM32\XCOPY.EXE' with a run count of 68 and last run time of 9/27/2007 9:10:30 AM.

17. Provide total number of deleted files.

The total number of deleted files is 78. This information was found in the Overview Tab of FTK.

A screenshot of the AccessData Forensic Toolkit software interface. The window title is "AccessData Forensic Toolkit Version 6.3.0.186 Database Forensic DB Case semester project-RP". The "Overview" tab is selected. In the left sidebar, under "Case Overview", there is a section titled "Deleted Files (78 / 257)". Below this, there is a table with columns: Name, Label, Item #, Ext, Path, Category, I-size, L-size, MD5, SHA1, Created, Accessed, and Modified. The table lists numerous deleted files, including various file types like JPEG, PDF, and DOC. At the bottom of the table, it says "Deleted: 78 Filtered: 78 Highlighted: 1 Checked: 19 Total User: 526.7KB".

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

The total number of Carved files: 257 This information was found under the Overview tab of FTK

A screenshot of the AccessData Forensic Toolkit software interface, similar to the previous one but with different data. The window title is "AccessData Forensic Toolkit Version 6.3.0.186 Database Forensic DB Case semester project-RP". The "Overview" tab is selected. In the left sidebar, under "Case Overview", there is a section titled "Carved Files (257 / 257)". Below this, there is a table with columns: Name, Label, Item #, Ext, Path, Category, I-size, L-size, MD5, SHA1, Created, Accessed, and Modified. The table lists numerous carved files, including various file types like JPEG, PDF, and DOC. At the bottom of the table, it says "Carved: 257 Filtered: 257 Highlighted: 0 Checked: 19 Total User: 2404 KB".

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

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

Screenshot 1: Shows the full structure of the **MountedDevices** key. It includes numerous subkeys such as **ControlSet001**, **ControlSet002**, **LastKnownConfigRecovery**, and various **Volume** entries. A red box highlights the **USB** folder.

Screenshot 2: Another view of the **MountedDevices** key, similar to the first but with some differences in the list of subkeys. A red box highlights the **USB** folder.

Screenshot 3: A detailed view of the **USB** folder under **MountedDevices**. It lists several subkeys: **ACPI**, **DISPLAY**, **FDD**, **HKEY_CURRENT_USER**, **HKEY_LOCAL_MACHINE**, **HKEY_CLASSES_ROOT**, **HKEY_USERS**, **IDE**, **LPTENUM**, **PCIIDE**, **Power**, **Root**, **STORAGE**, **SMB**, **UMB**, and **USB**. A red box highlights the **DeviceDesc** key under **USB**.

Key Properties (Screenshot 3):

- Last Written Time: 7/14/2007 17:58:40 UTC

DeviceDesc Value Data (Screenshot 3):

```
REG_SZ: Canon PowerShot SD100
```

Key Properties (Screenshot 3):

- Last Written Time: 7/14/2007 17:58:40 UTC

The screenshot shows the AccessData Registry Viewer interface with the following details:

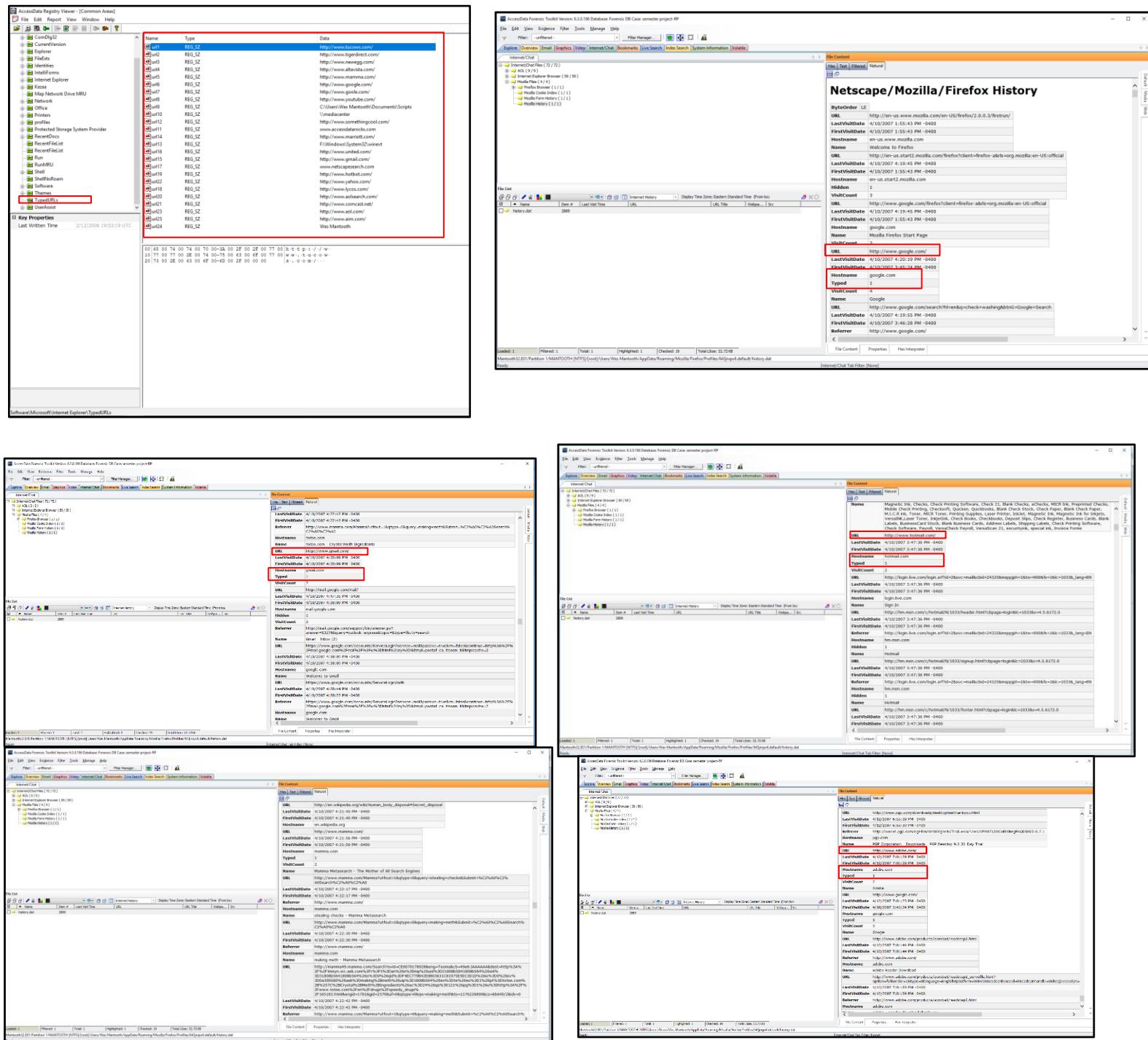
- File**, **Edit**, **Report**, **View**, **Window**, **Help**
- Name**: `\Device\HID`
- Type**: `REG_EXPAND_SZ` (Input and Output Devices\%USB Human Interface Device)
- Data**: `REG_EXPAND_SZ` (Input and Output Devices\%USB Human Interface Device)
- Subkeys**:
 - `\Device\HID`
 - `\Device\HID\DeviceInformation`
 - `\Device\HID\Capabilities`
 - `\Device\HID\HardwareD`
 - `\Device\HID\ControlHd`
 - `\Device\HID\Service`
 - `\Device\HID\Class`
 - `\Device\HID\Driver`
 - `\Device\HID\Class`
 - `\Device\HID\Hid`
- Properties**:
 - Key Properties**:
 - Last Written Time: 7/24/2009 17:08:41 UTC
 - Control**:
 - Control
 - Write
 - Query
 - File
 - Event
 - WaitForSingleObject
 - Hardware Profiles
 - Security**:
 - Full Control
 - Change My Logon Information
 - Read Control
 - Read Extended Security Information
 - Read Name Value
 - Write Extended Security Information
 - Write Name Value

20. Identify the most recently run programs

In the registry viewer, the **NTUSER.DAT** shows the most recently run programs on the computer. Similarly, ‘UserAssist’ in FTK shows which programs were run recently.

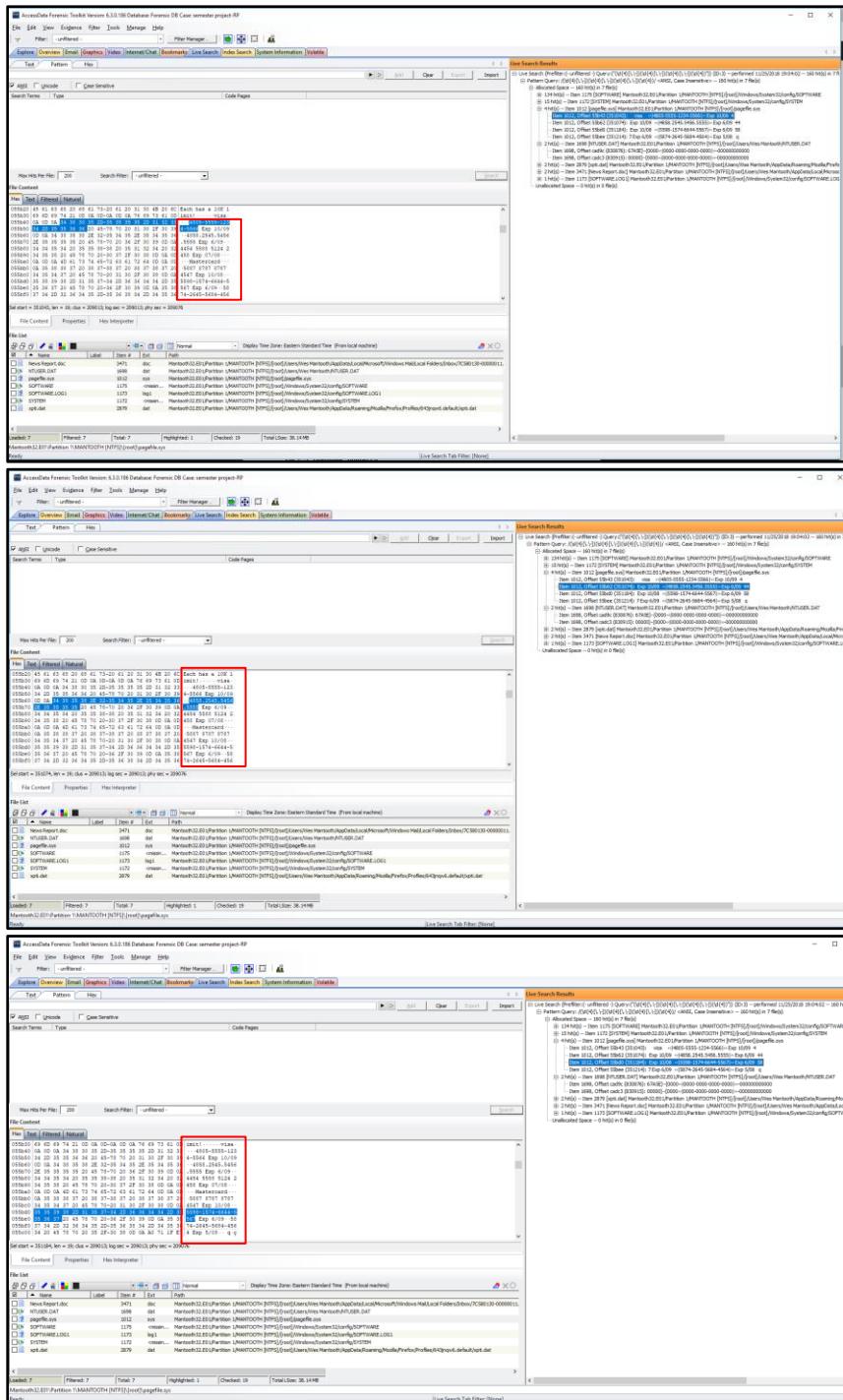
21. Identify any URLs that were visited by manually typing the address.

The following are the typed URLs that are visible in registry viewer after exporting **NTUSER.DAT**. Alternatively, 'Internet/Chat' files (history.dat under Mozilla files) in FTK, shows the URLs which were typed manually.



22. Identify any credit card numbers on the drive.

Performing Live Search and Index Search in FTK enabled me to recover the credit card numbers on the drive, as shown in below screenshots.

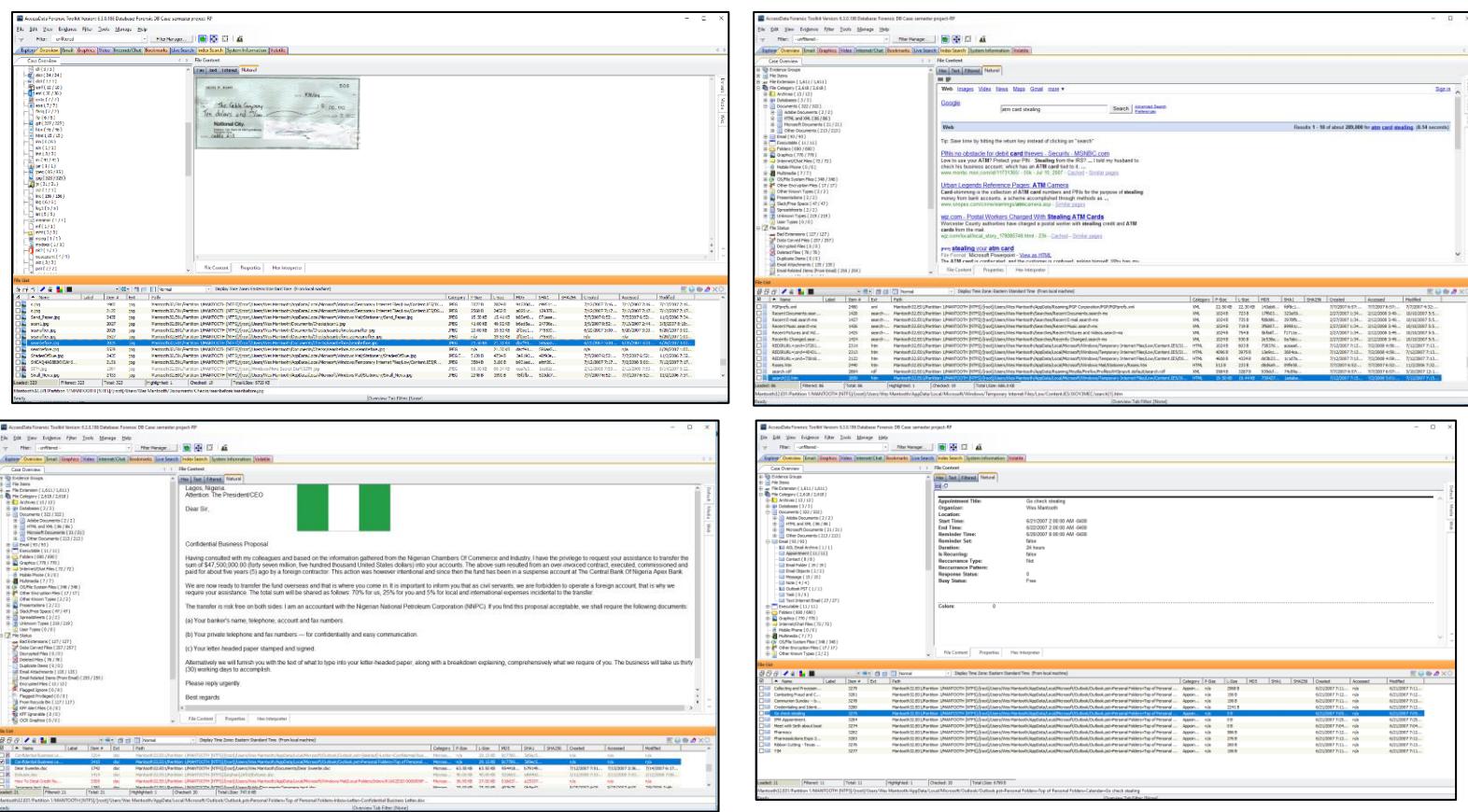


23. Provide a few examples of theft, title, checks, scam, and forensics.

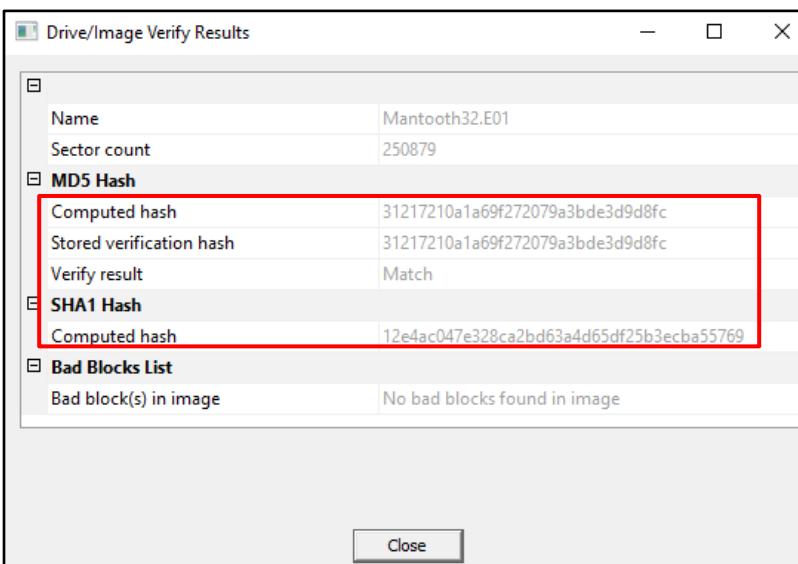
Following are the screen-shots of a few examples of theft, title, checks, and scam and forensics which I found in multiple locations of FTK.

The image displays nine screenshots of the AccessData FTK Forensic Toolkit interface, arranged in a 3x3 grid. Each screenshot shows a different aspect of forensic analysis:

- Top Left:** A file list view showing numerous log files and system artifacts.
- Top Middle:** A preview of a scanned document, likely a driver's license or identification card.
- Top Right:** A file list view showing log files and system artifacts.
- Middle Left:** A detailed analysis report with a large amount of text and code snippets.
- Middle Middle:** A preview of a check from "The City Company" for \$5.00.
- Middle Right:** A file list view showing log files and system artifacts.
- Bottom Left:** A preview of a cashier's check for \$8,000 DOLS 00 CTS.
- Bottom Middle:** A preview of a check from "The City Company" for \$5.00.
- Bottom Right:** A file list view showing log files and system artifacts.



Finally, after completing my examination of the provided image file I re-verified the image integrity using FTK Imager to ensure that the image was not altered in any way. Following hash results prove that both, the stored and the computed hash values match and that the image was not corrupted in any way during my examination.



Conclusion

In this project, I carefully securitized the provided image file and provided all the relevant information which was requested by Detective Ketchum and the UNCC Police Department. For my investigation, I used various forensic tools such as FTK, FTK Imager, Registry Viewer and PRTK to gather important evidence such as user passwords, scams and frauds, browser history, user account information, tools installed, browser history, deleted files, commonly run programs, etc. from multiple locations on the image file called Mantooth32.E01.