ITIS 5250
Ruchira Pokhriyal
Semester Project
12/04/2018

Overview

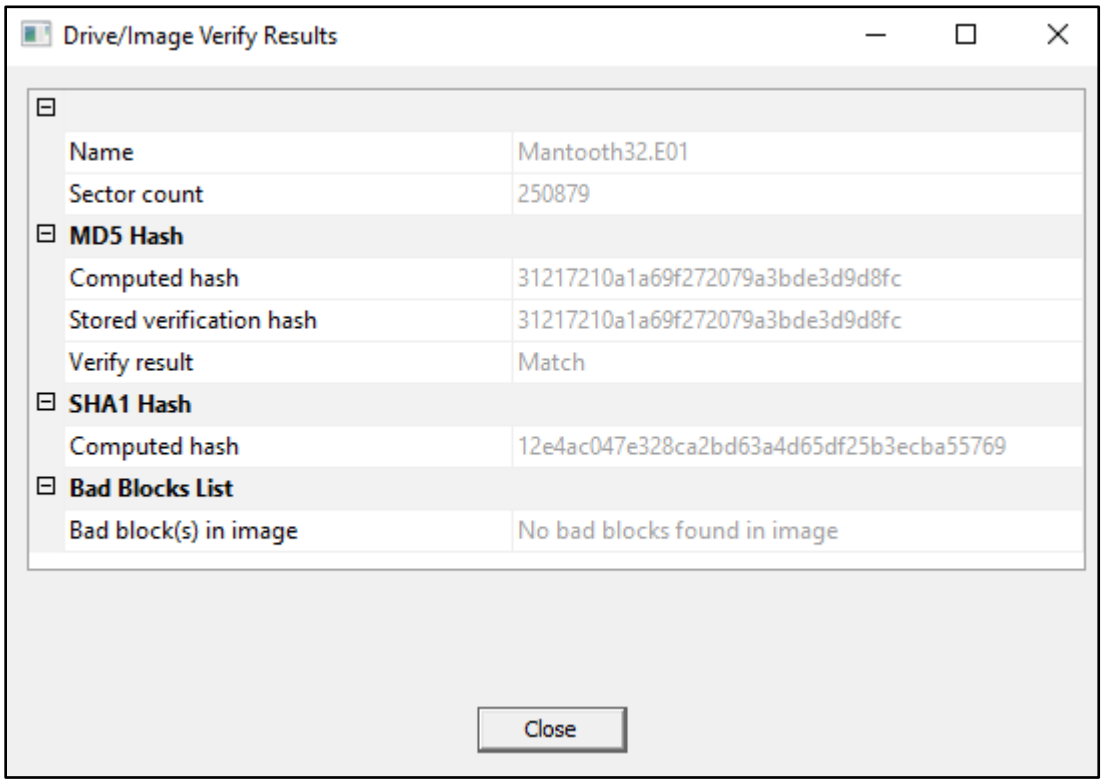
A local group of criminals has been involved in check and credit card frauds, ATM scams and other financial crimes. These criminals are known to use a great deal of technology and hence, Detective Ketchum has asked me to process a desktop computer which belongs to a gang member called Wes Mantooth. For 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.

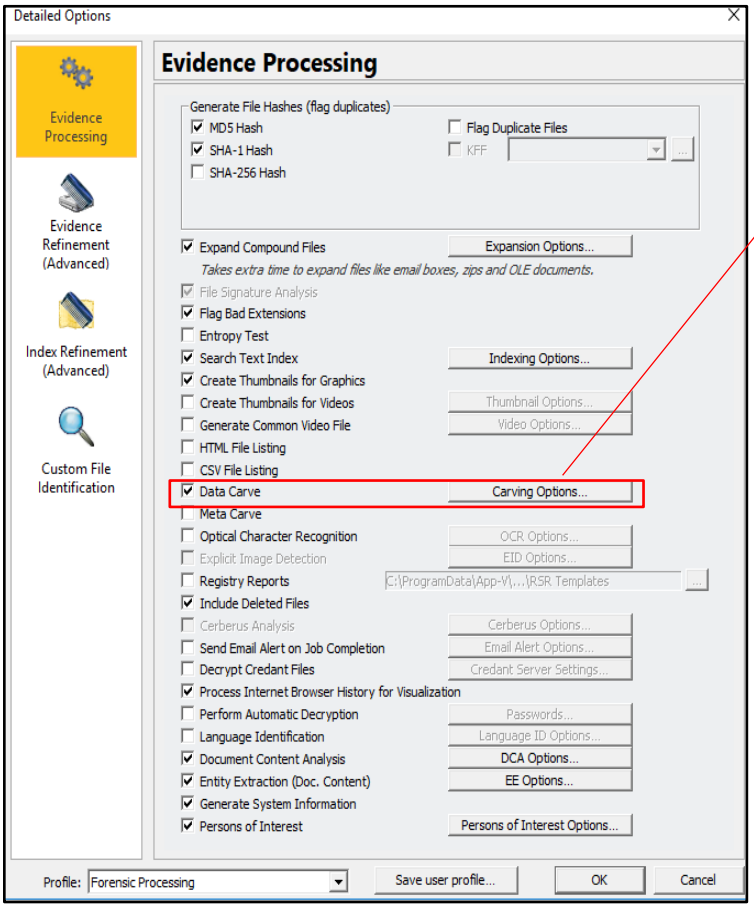
Hash Verification Results:

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

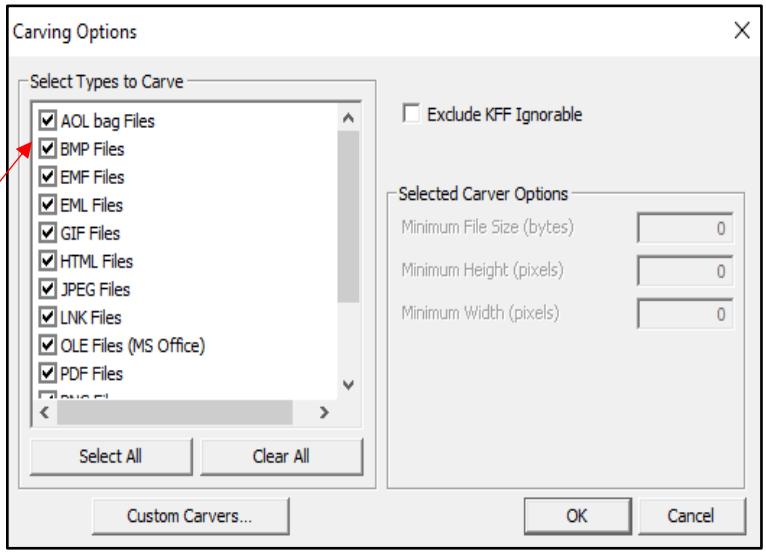


I customized the following options in FTK:

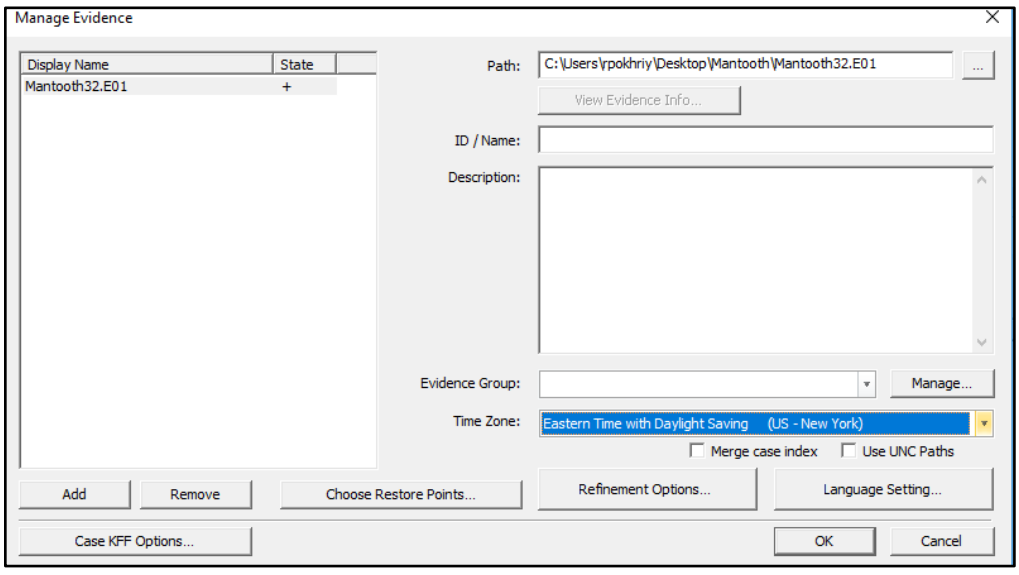
Evidence Processing using FTK:



Carving Options:

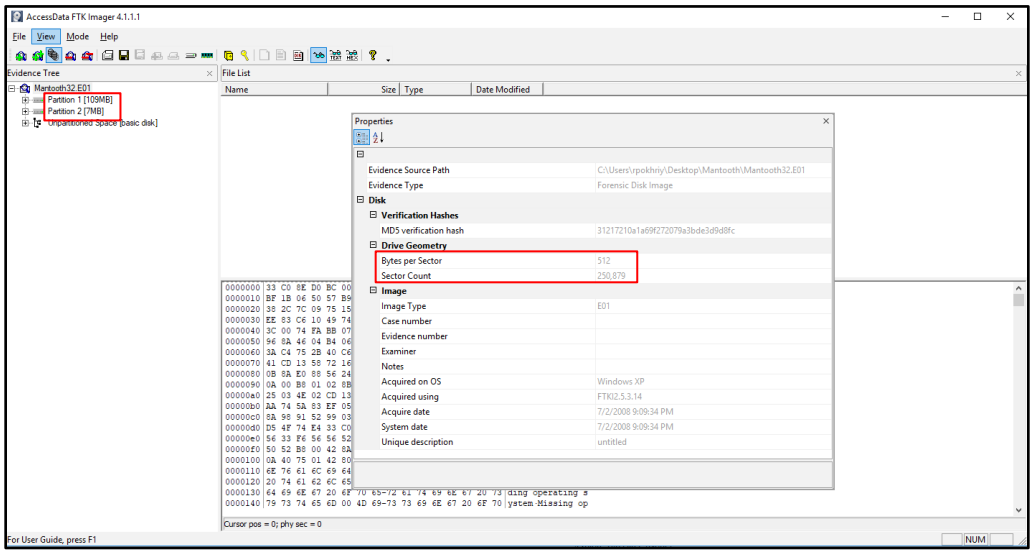


Adding Image:



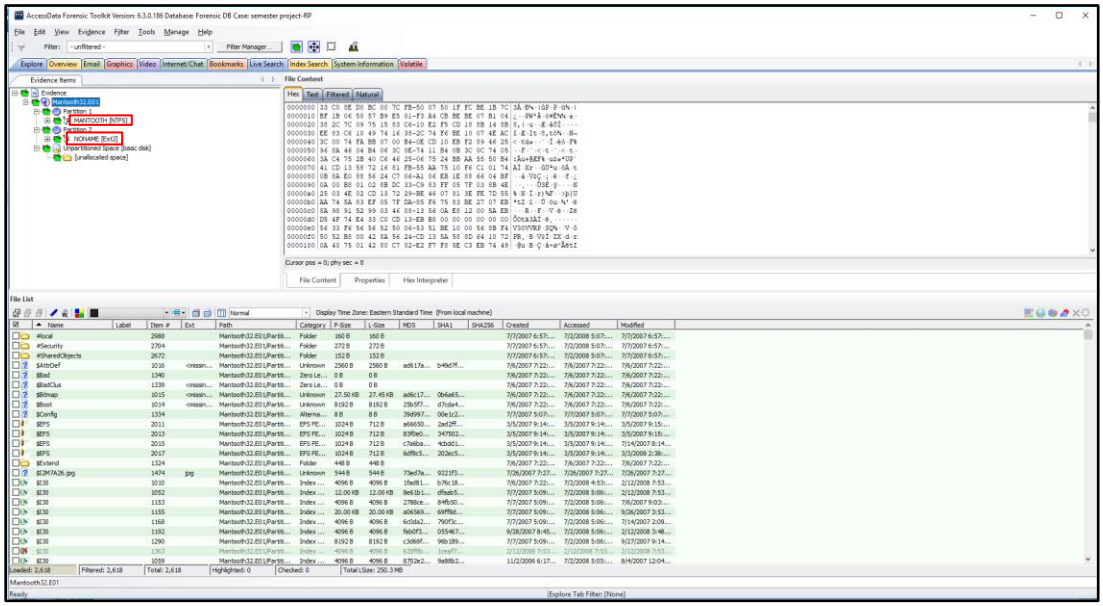
Findings and Report

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



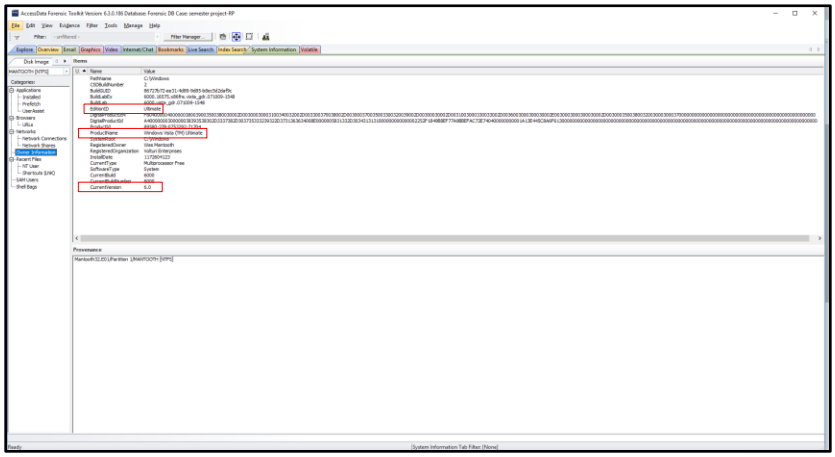
The space on the computer hard drive can be obtained by multiplying the **Bytes per Sector** and **Sector Count** values mentioned in the Drive Geometry.
Therefore, **512 * 250,897=128,450,048 bytes.**
Also, from FTK Imager, it can be seen that the total partition comprises of **109MB+7MB= 116MB (which 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.**



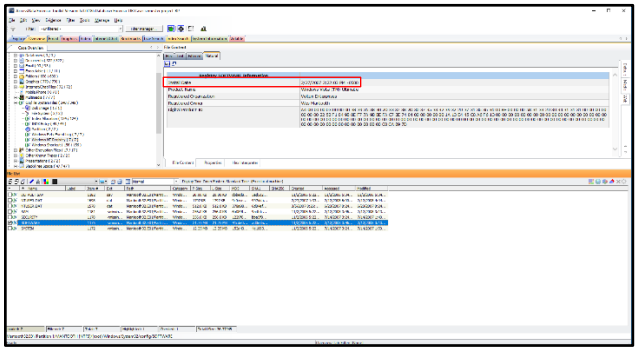
3. Identify the version and service pack of the operating system.

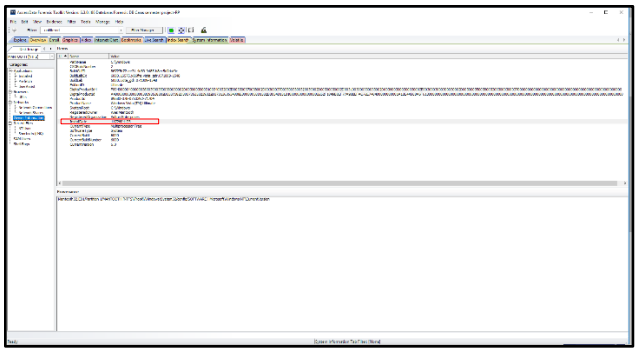
The **'System Information'** in FTK shows the service pack of the Operating System is **'Windows Vista Ultimate'** and the current version is **6.0.** And, as shown below, similar information is obtained upon exporting **SOFTWARE** file from FTK into the **Registry Viewer.**

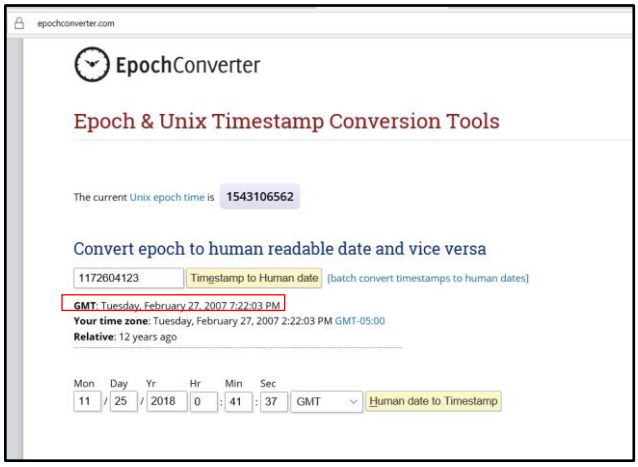


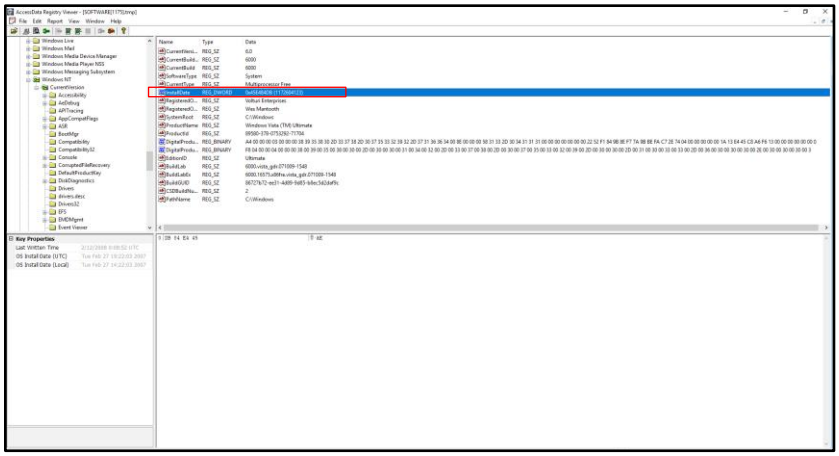
4. Find the date the OS was installed.

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**.



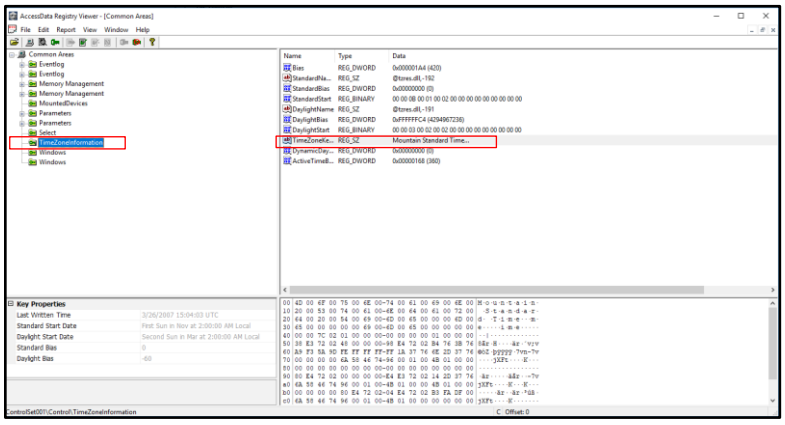






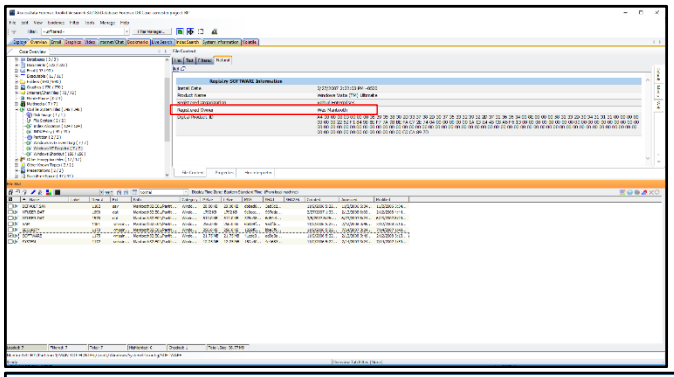
5. Identify the Time Zone information for the computer.

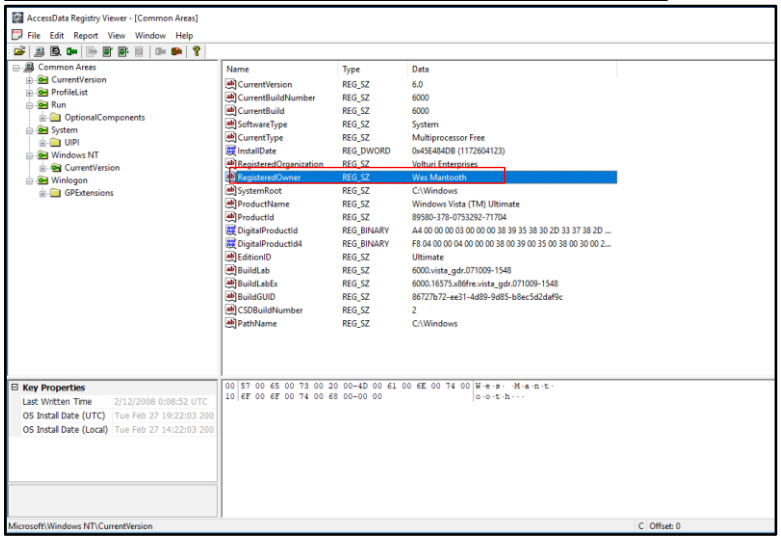
The time zone information can be found after exporting the **SYSTEM** file into the registry viewer from FTK, and under 'Terminal Server', the time zone is shown as '**Mountain Standard Time'.**



6. Show the owner of the computer.

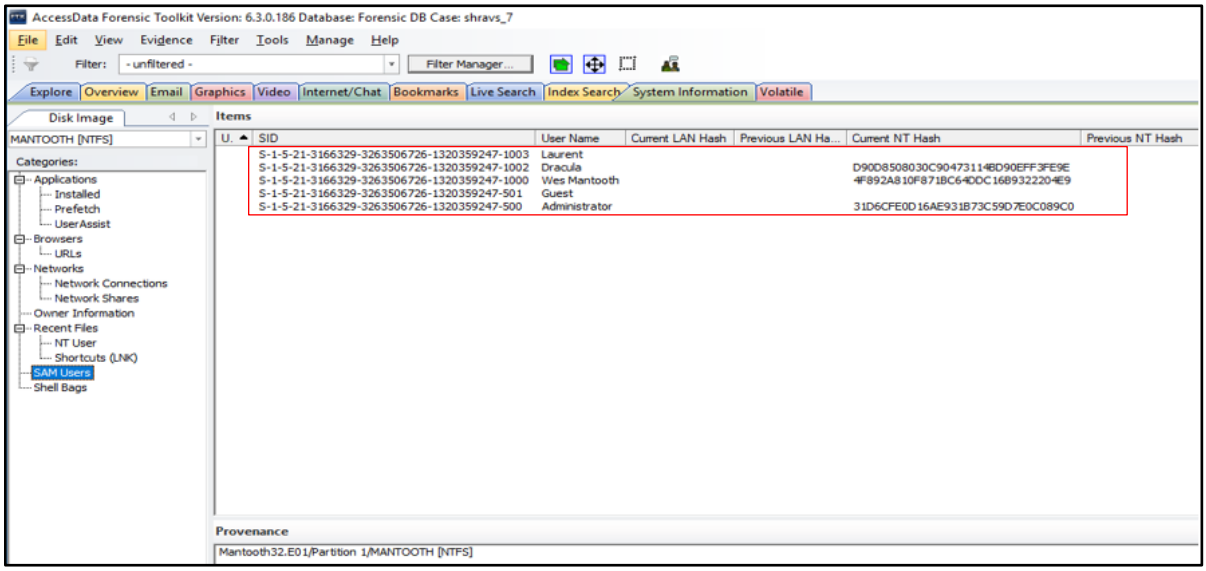
In the Windows NT Registry under Overview tab in FTK, the owner of the computer was found to be ‘Wes Mantooth’. Even the system information shows the registered owner of the computer to be ‘Wes Mantooth’.





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.



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

Admin: 1

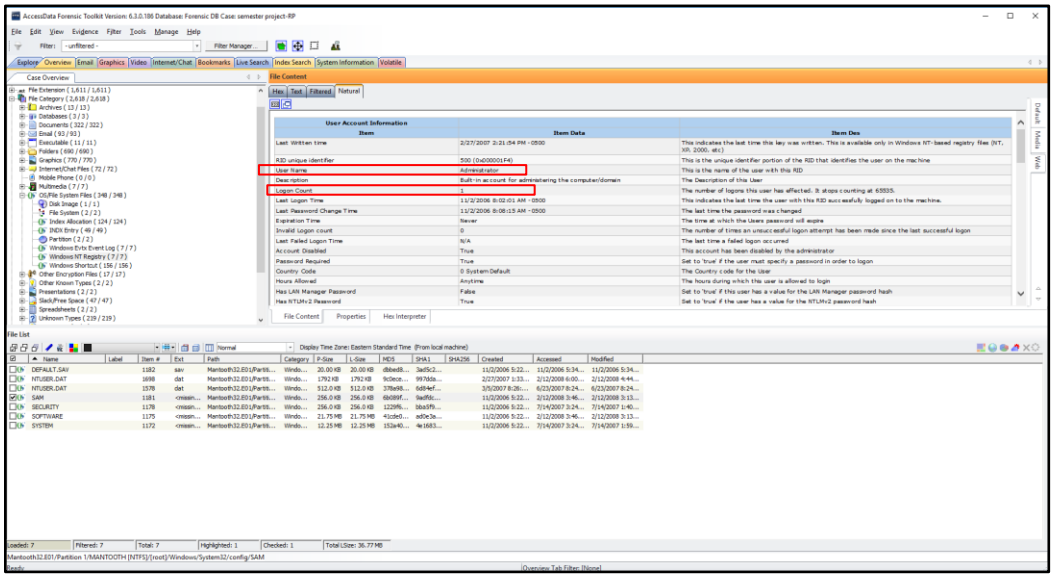
Guest: 0

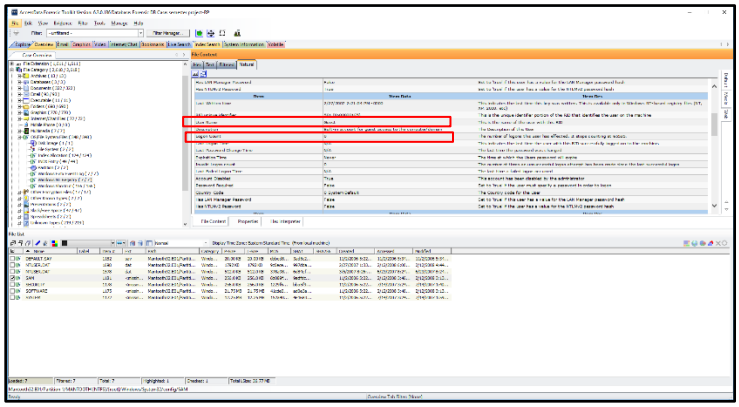
Laurent: 0

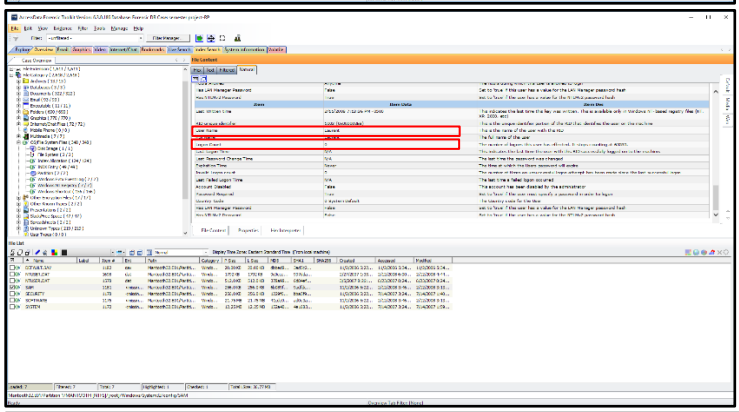
Dracula: 3

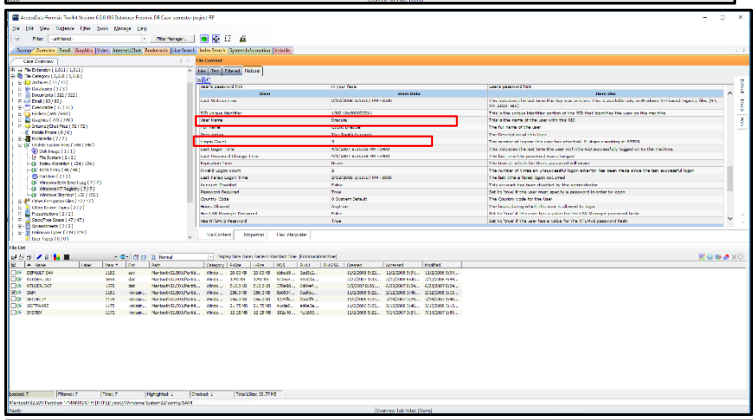
Wes Mantooth: 96

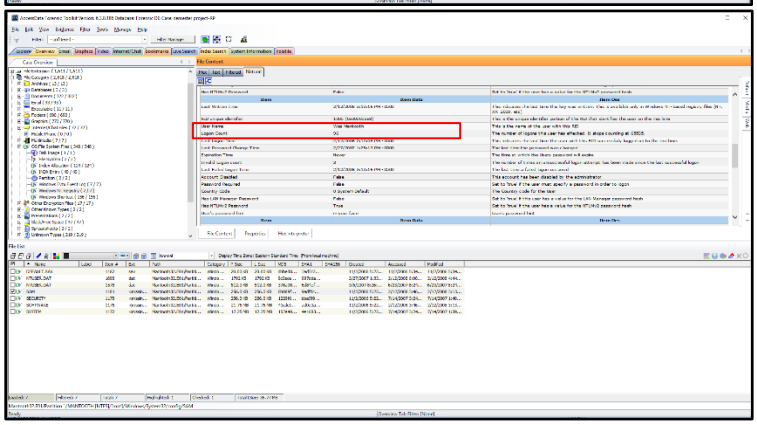
Thus, making 'Wes Mantooth' the most active user of the computer with a logon count of 96 times.





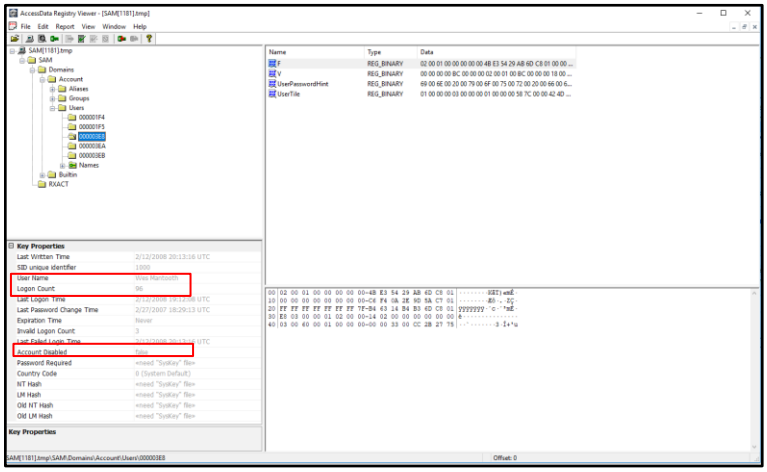


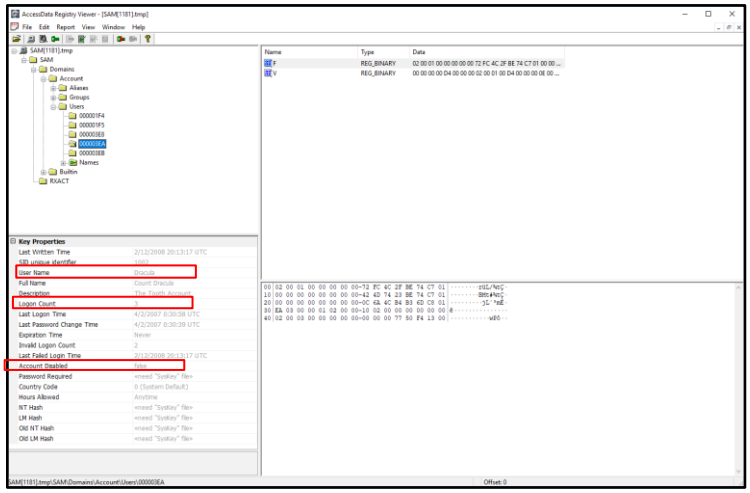


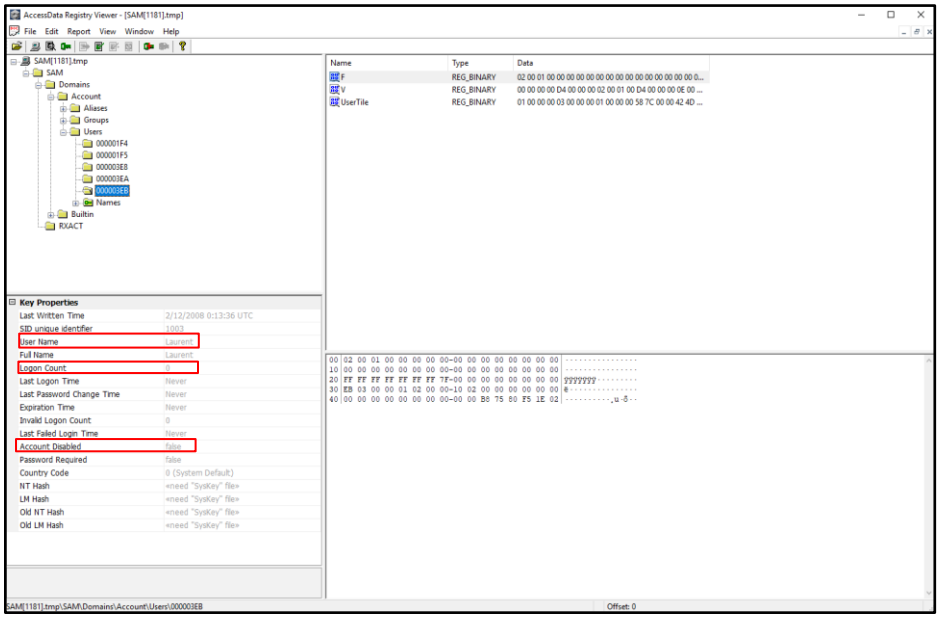


8. Identify user accounts and who uses the account.

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.





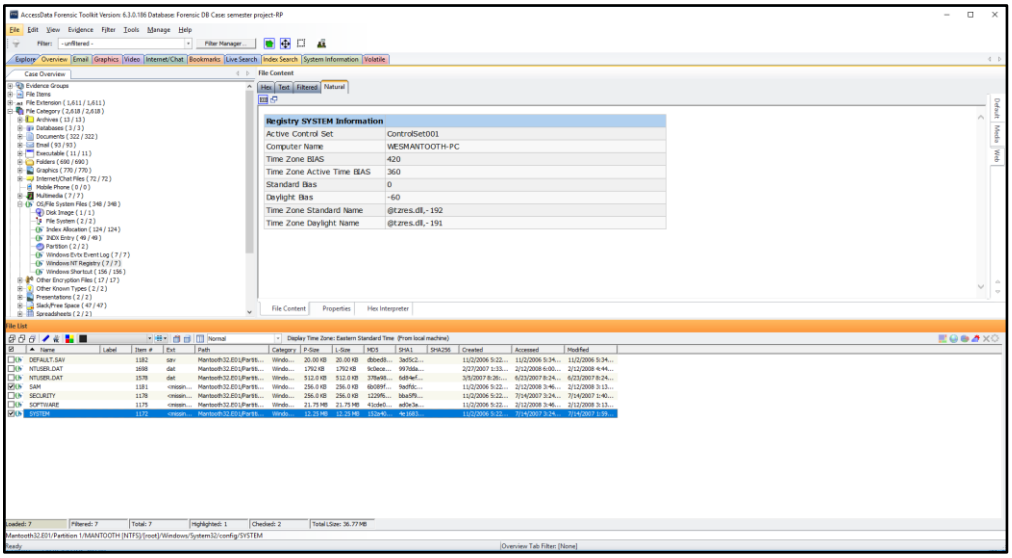


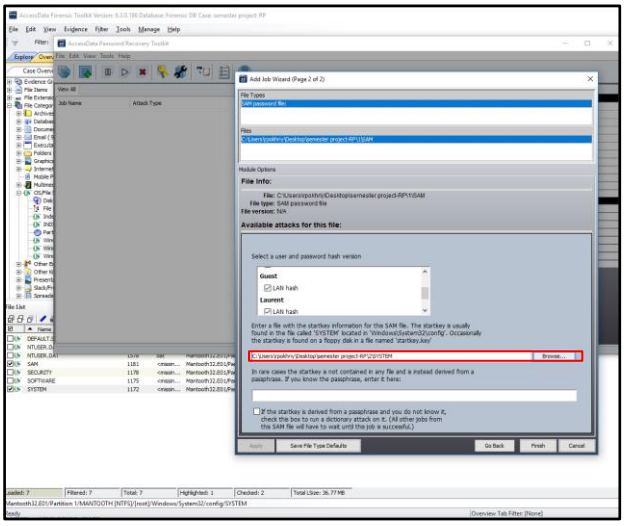
9. Acquire user passwords.

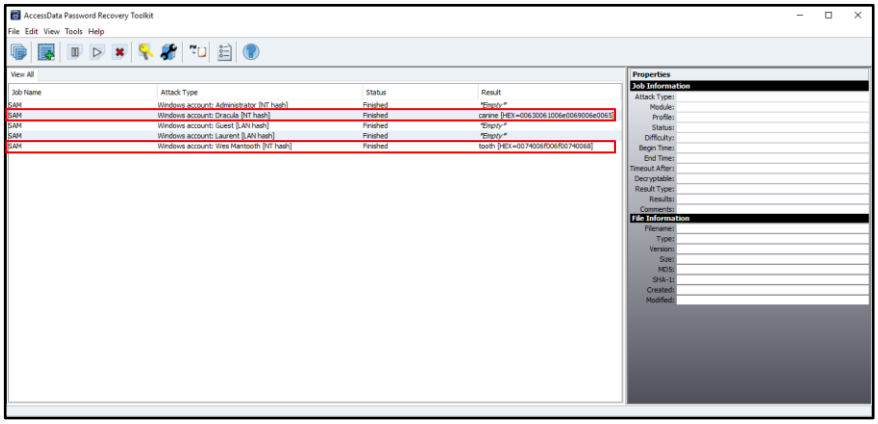
I exported SAM and SYSTEM files from FTK TO PRTK, and was able to crack the passwords for two user accounts, namely Dracula and Wes Mantooth.

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

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

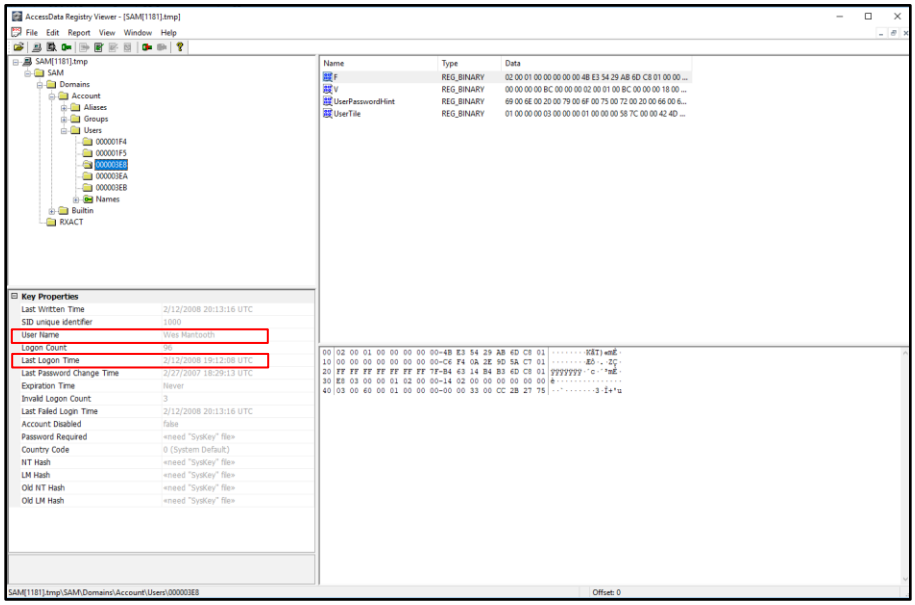




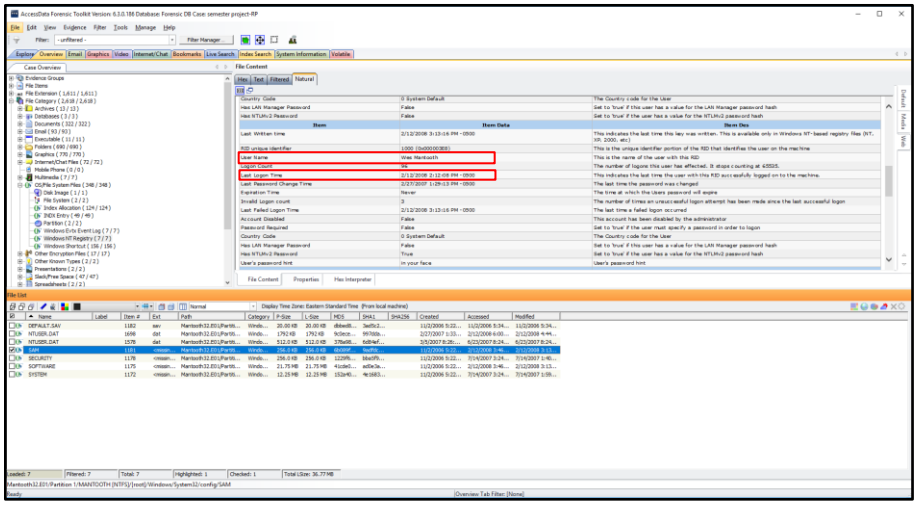


10. Identify the last date Wes Mantooth logged on.

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

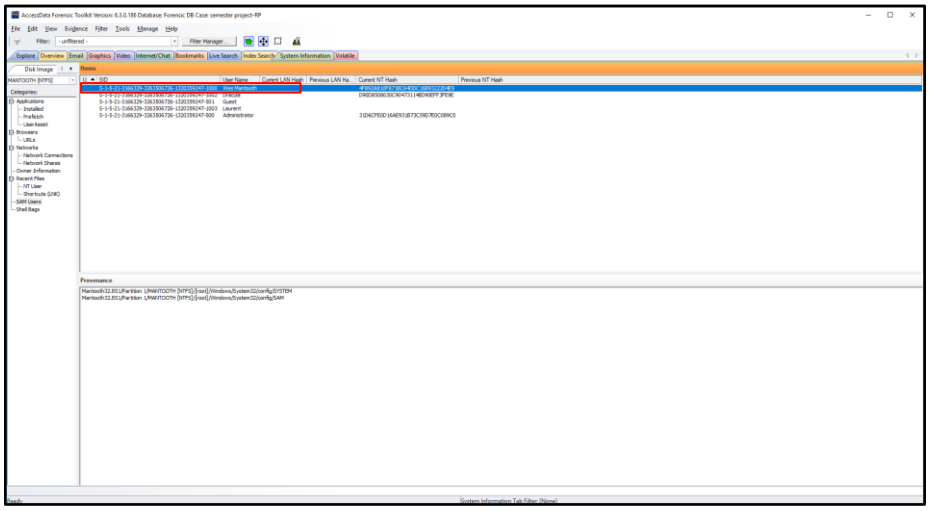


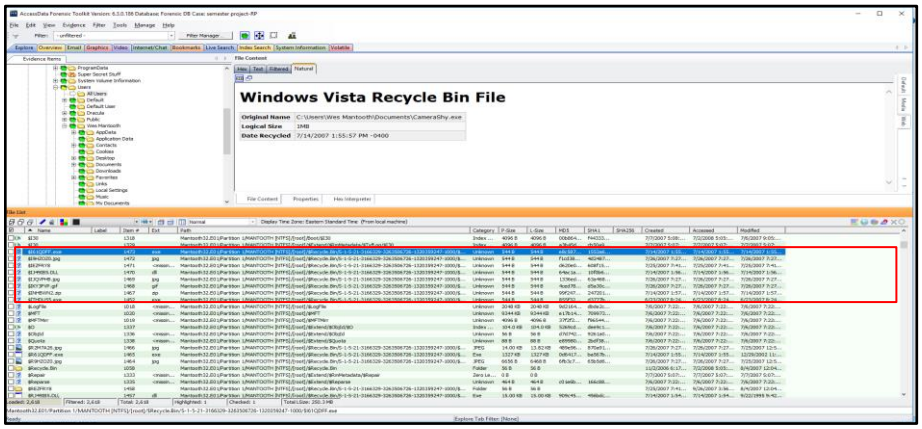
As shown below, the last date when Wes Mantooth logged on can also be seen in the SAM file in FTK:

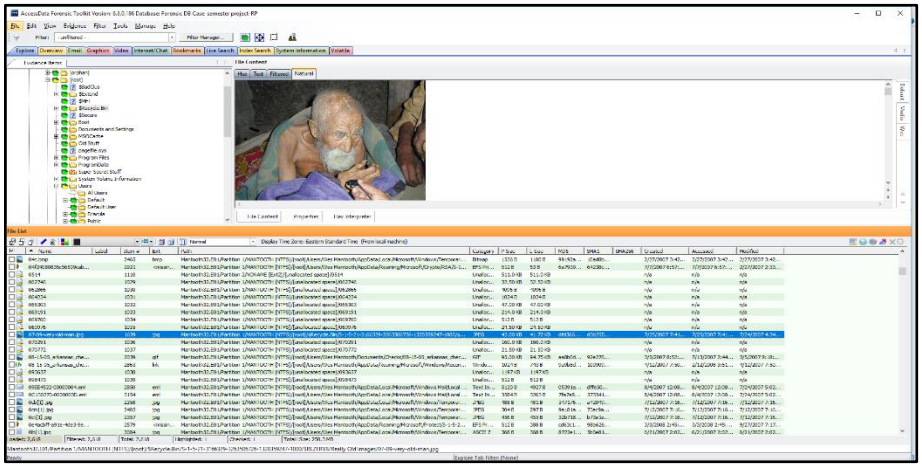


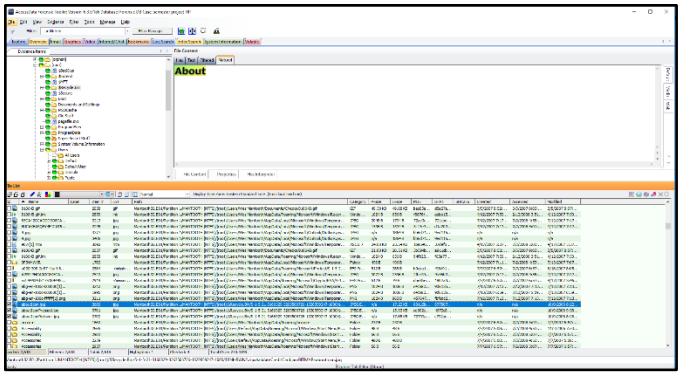
11. Identify files placed in the recycle bin by Wes Mantooth.

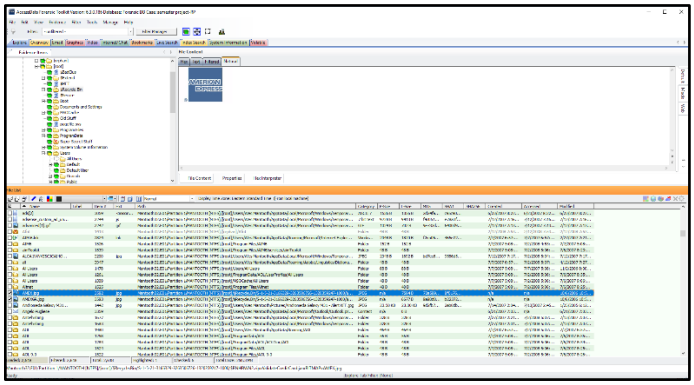
In the **'System Information'**, under **SAM users**, the SID for Wes Mantooth is found to be: **'S-1-5-21-3166329- 3263506726-1320359247-1000**'. The File Category in FTK hence, shows that the files shown in below screenshots were placed in the recycle bin by **Wes Mantooth**.

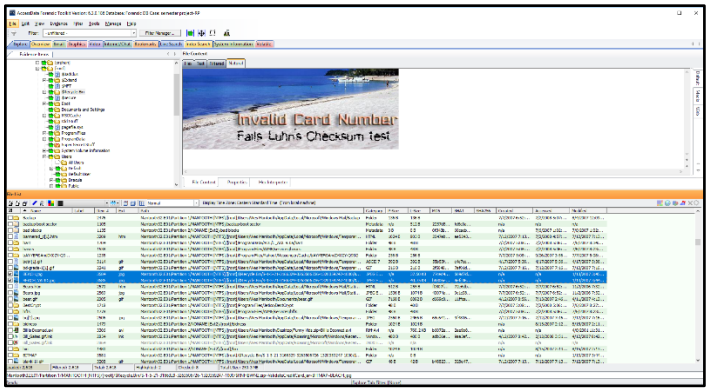


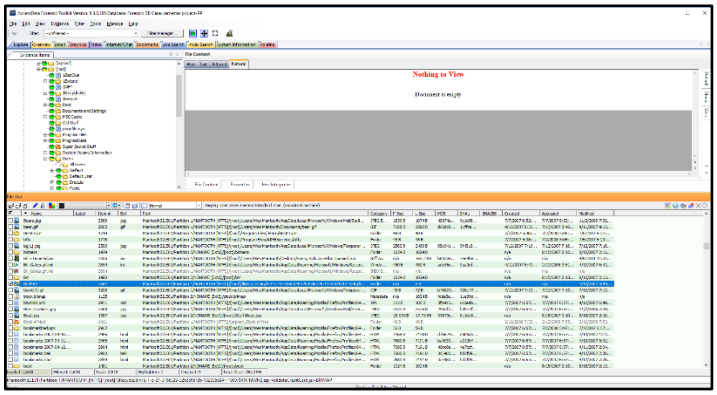








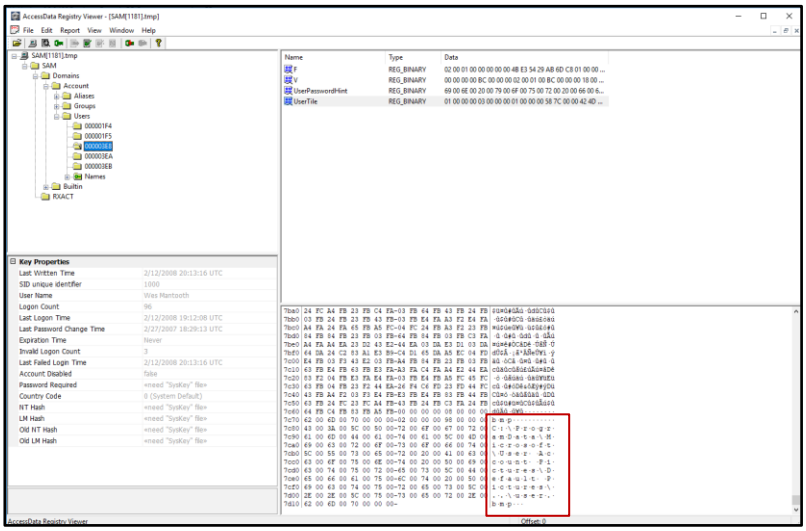


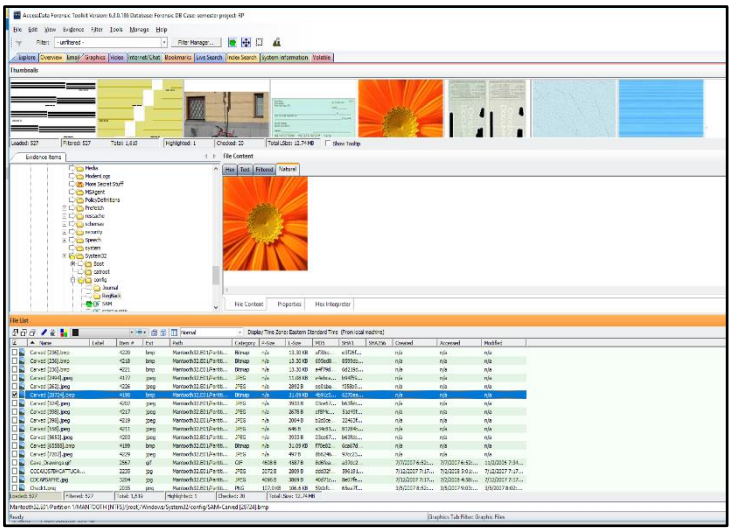


12. Recover the user picture tile for Wes Mantooth's account.

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:

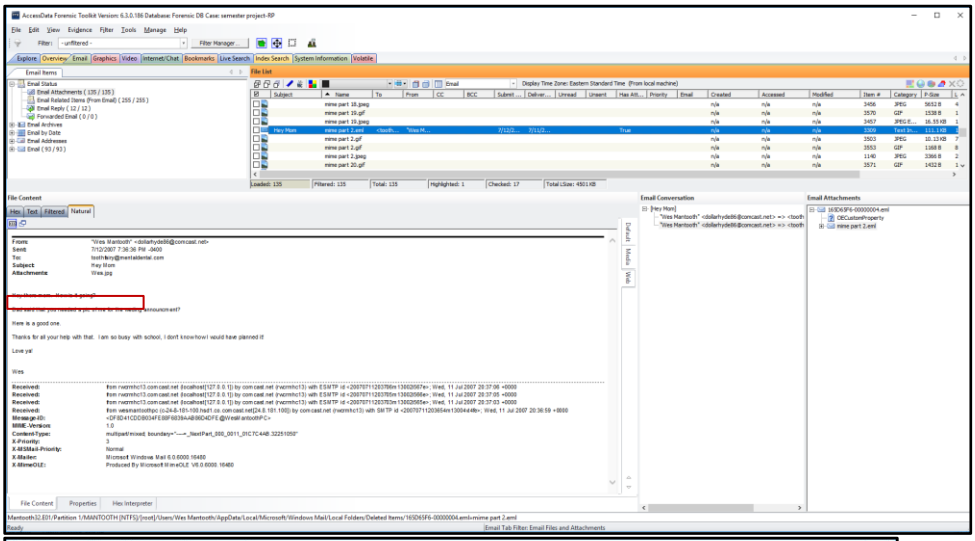
.

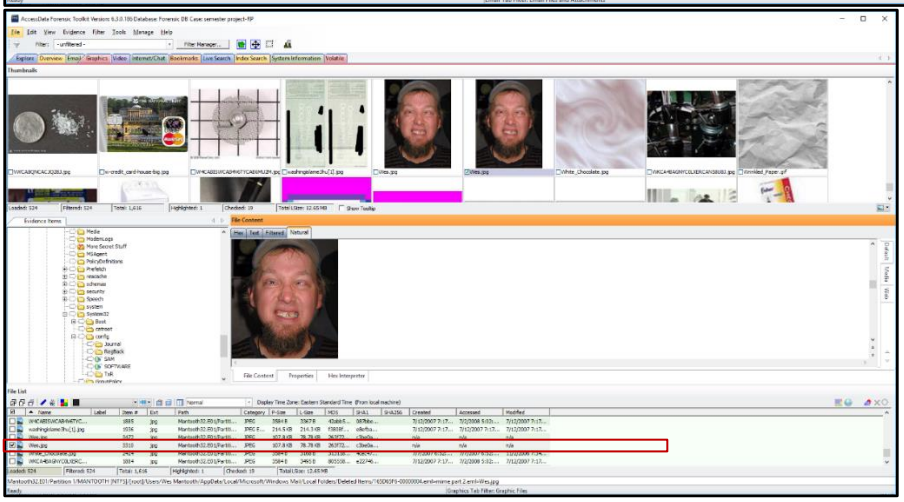




13. Identify any pictures of Wes Mantooth.

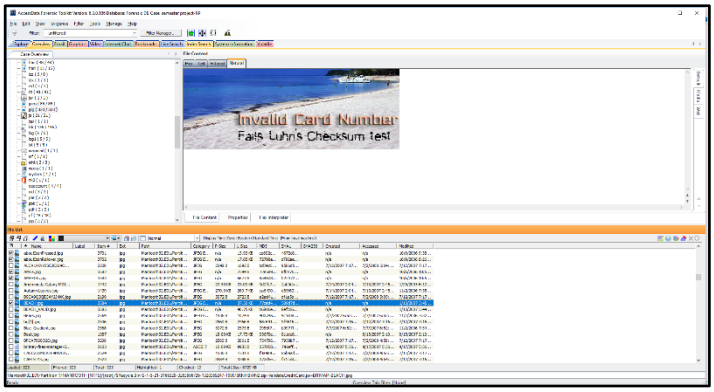
In FTK, under the Email tab, I found an email with the subject **'Hey Mom',** which has an attachment called **'Wes.jpg'**. I then explored the graphics tab and found this picture of Wes Mantooth, named **Wes.jpg**.

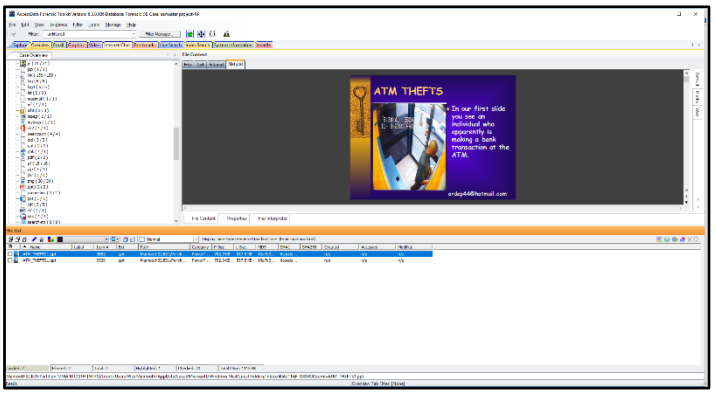


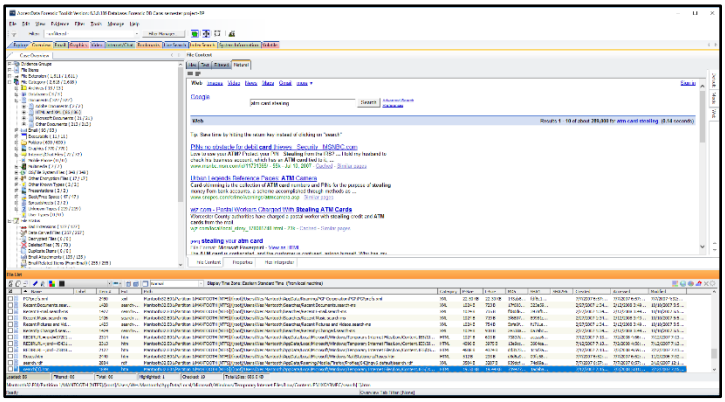


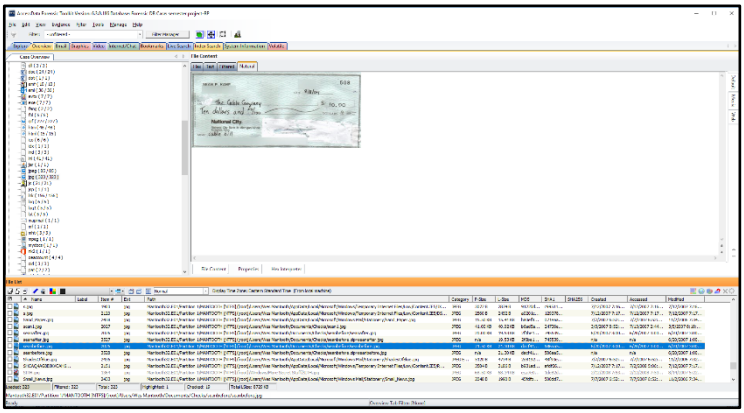
14. Identify any pictures related to the fraud or financial crimes.

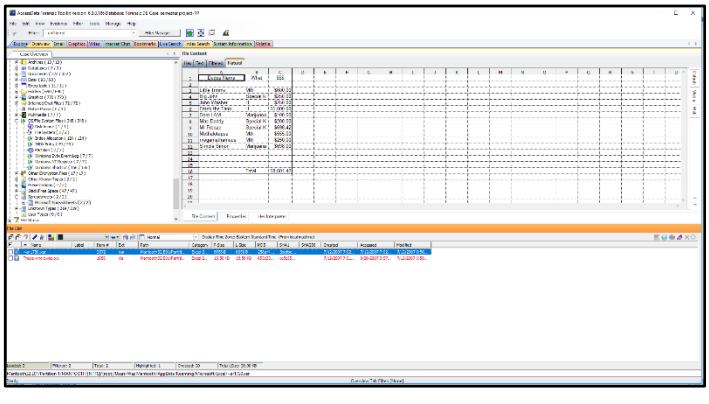
In FTK's Overview tab, I came across several pictures related to fraud and financial crimes. Few of these pictures are shown below:

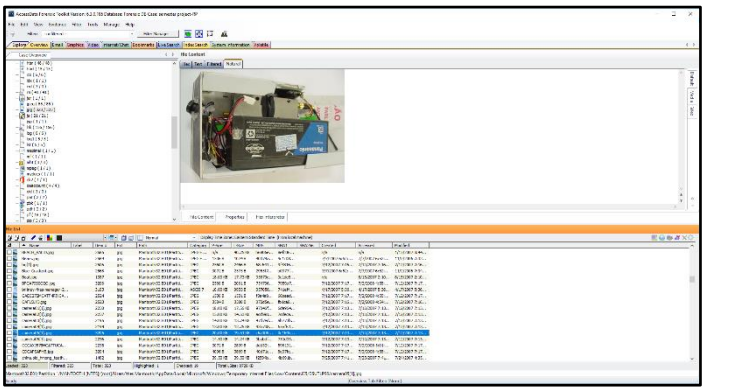


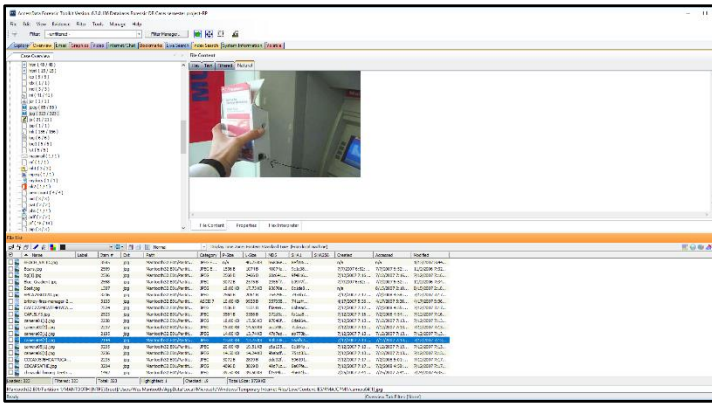






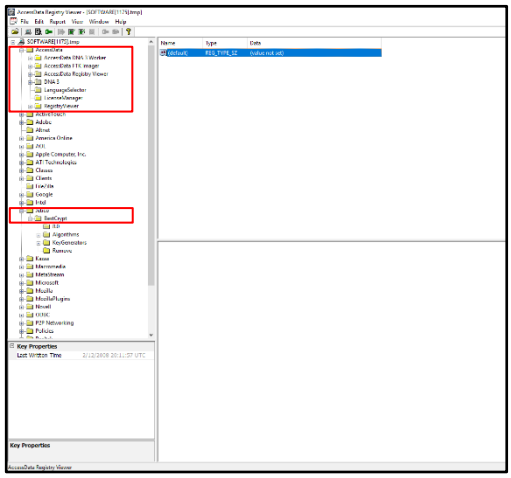


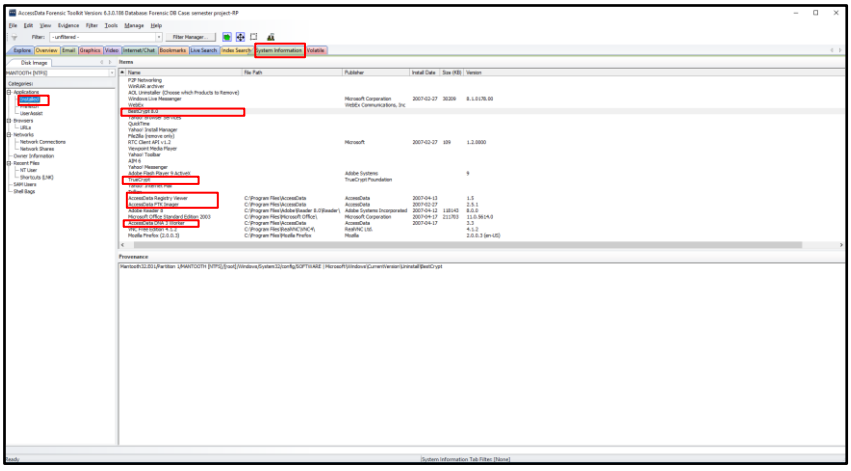




15. Identify any software that can be used to encrypt, obscure or forensically analyze data, or defeat forensics.

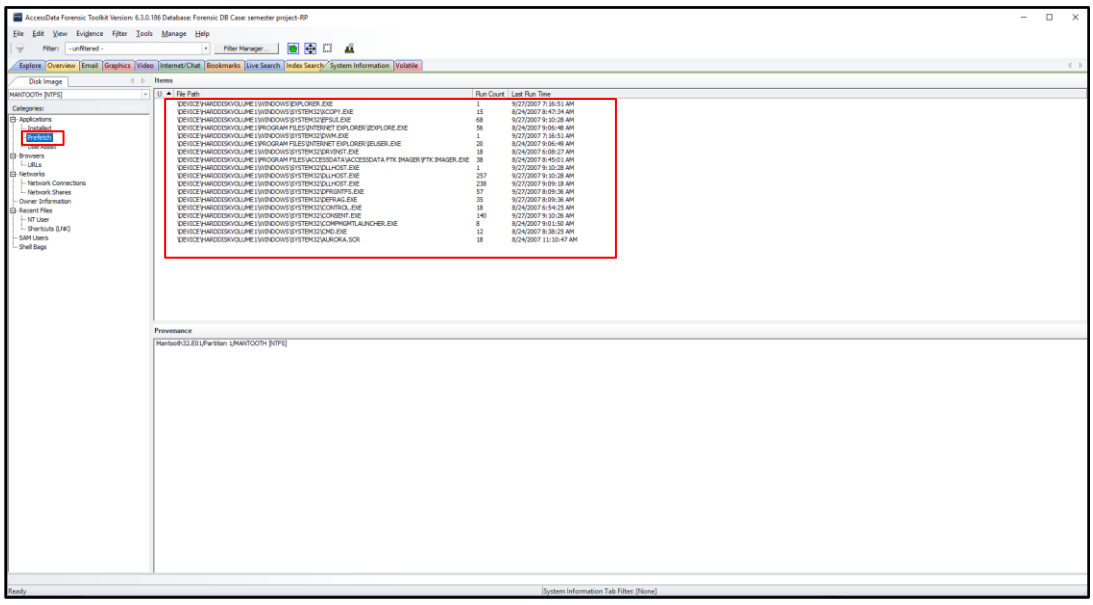
I discovered the following software tools which were installed on the computer, after exporting the SOFTWARE file from FTK into registry viewer: AccessData FTK Imager, AccessData Registry Viewer, AccessData DNA3 Worker, TrueCrypt, BestCryt etc. These software tools were also found in **'Installed Applications'**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





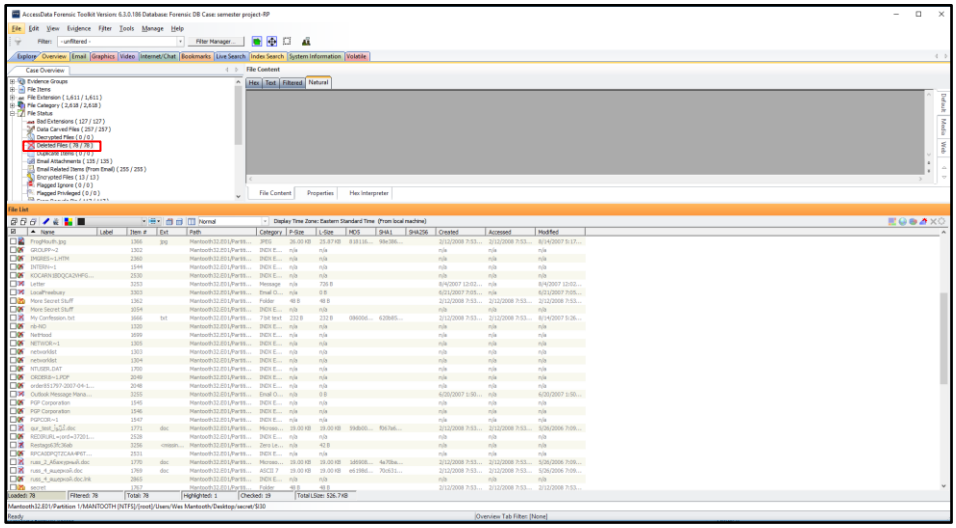
16. Identify the most commonly opened programs.

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



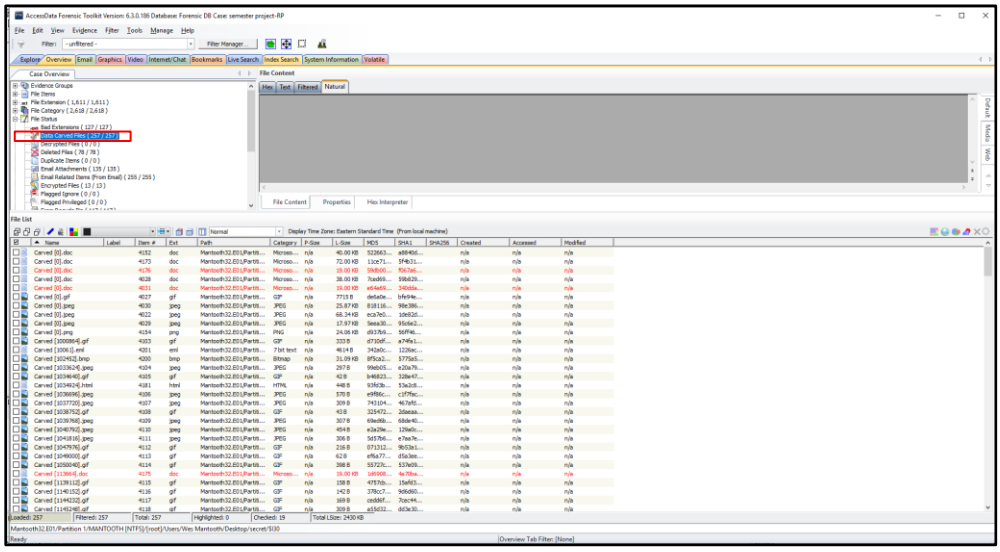
17. Provide total number of deleted files.

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



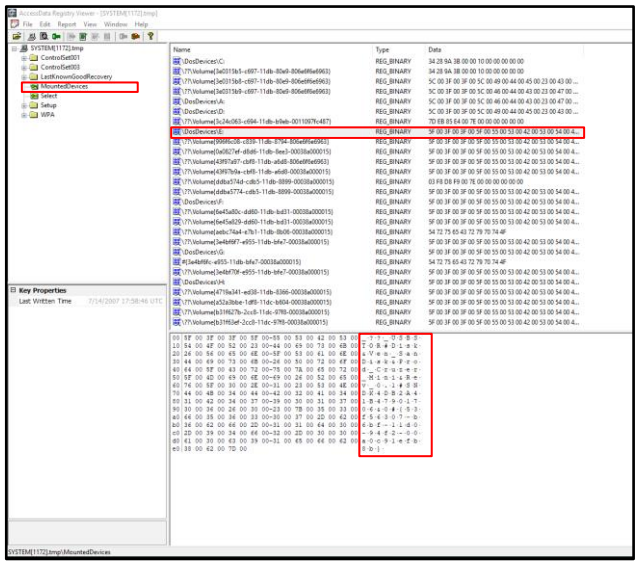
18. file carving and find total number of carved files.

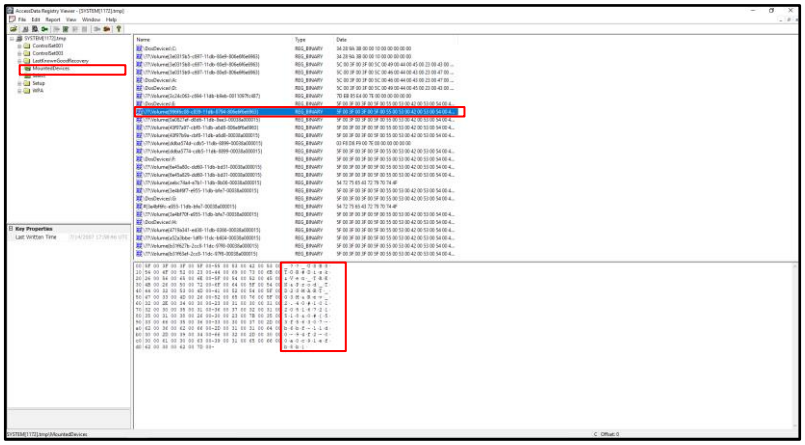
The total number of Carved files: 257 This information was found under the Overview tab of FTK

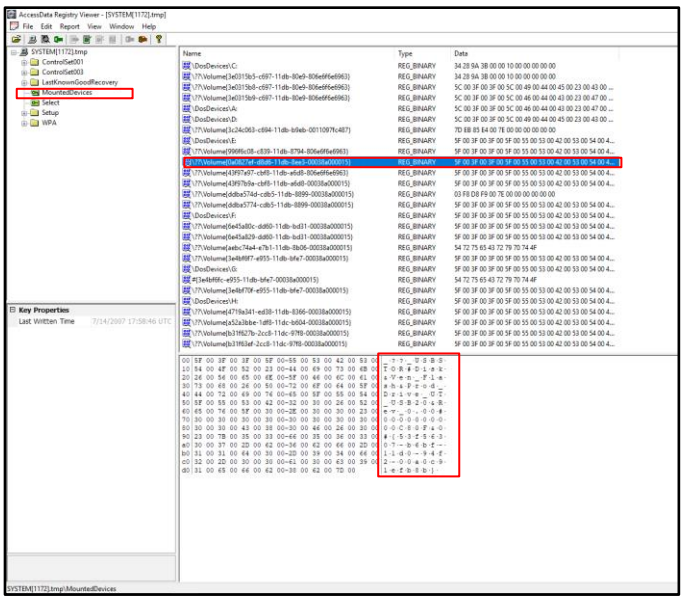


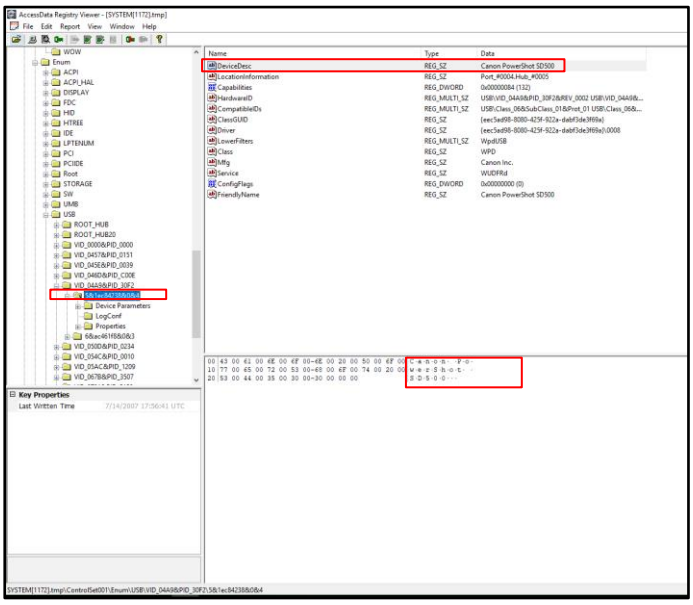
19. Identify any cameras, USB drives or other devices that have been attached to the computer.

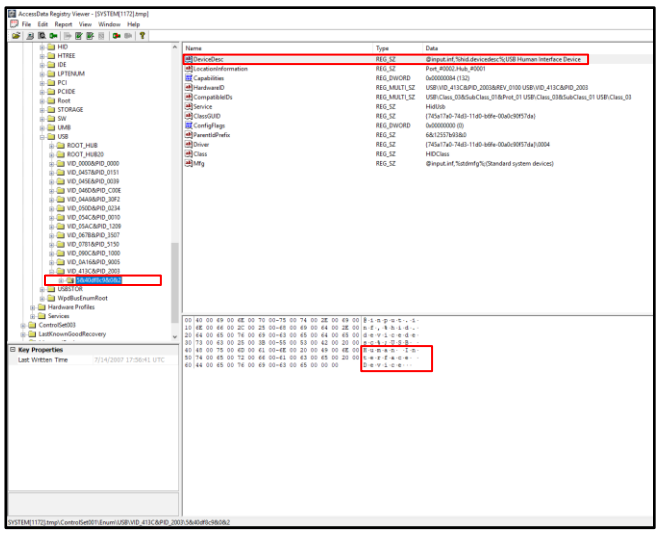
I exported SYSTEM file from FTK into the registry viewer and found the USB attachments under **'MountedDevices'** as shown below. Furthermore, after exploring subfolders under **'USB'**, I found camera attachment, USB drives and human interface device.

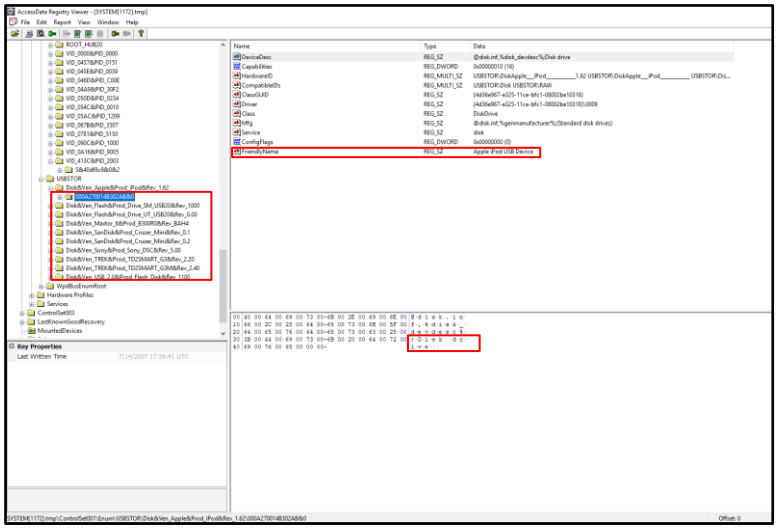






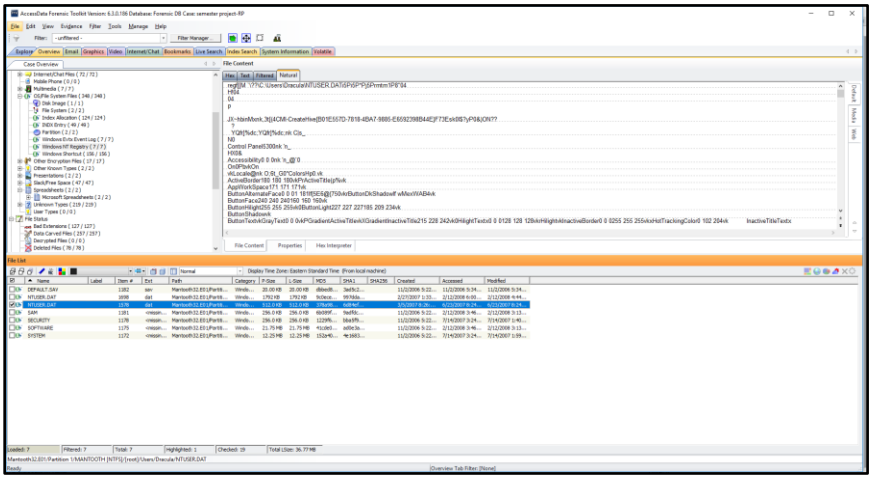


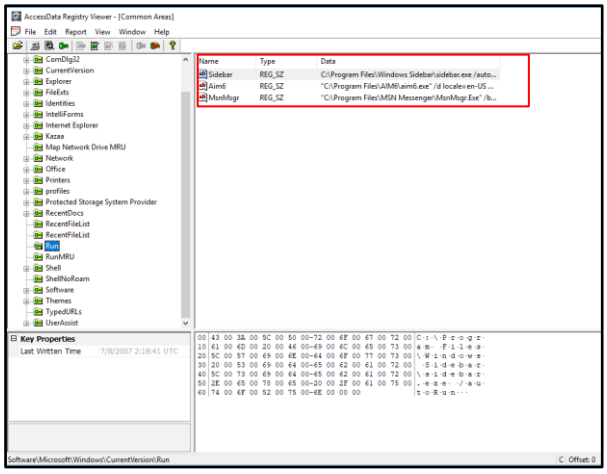


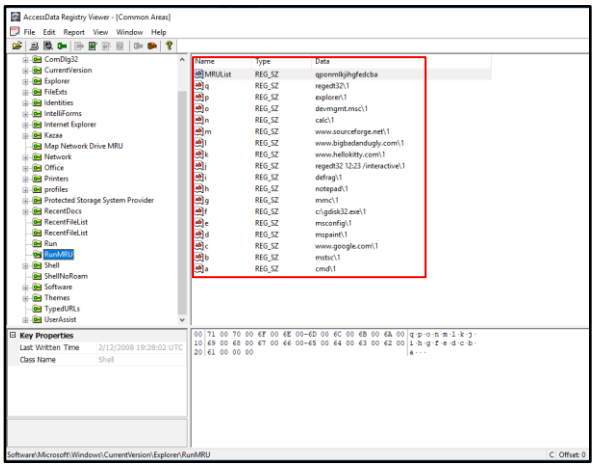


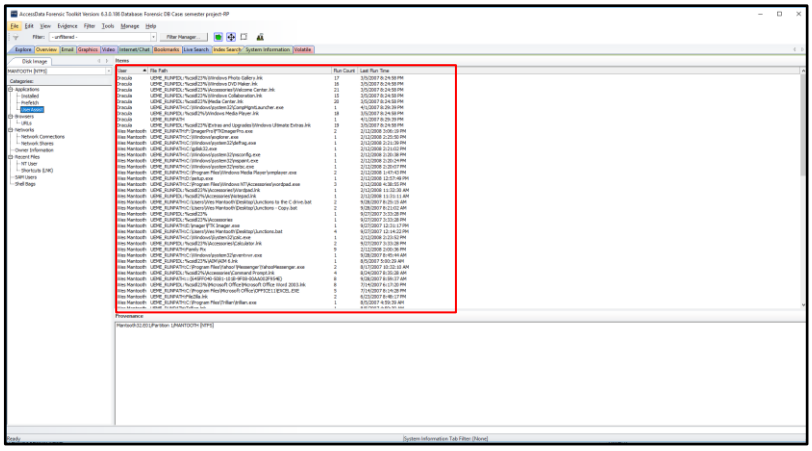
20. Identify the most recently run programs.

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.



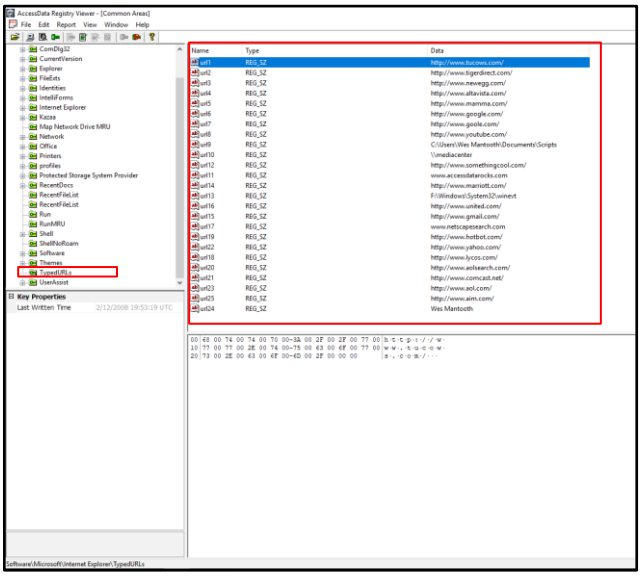


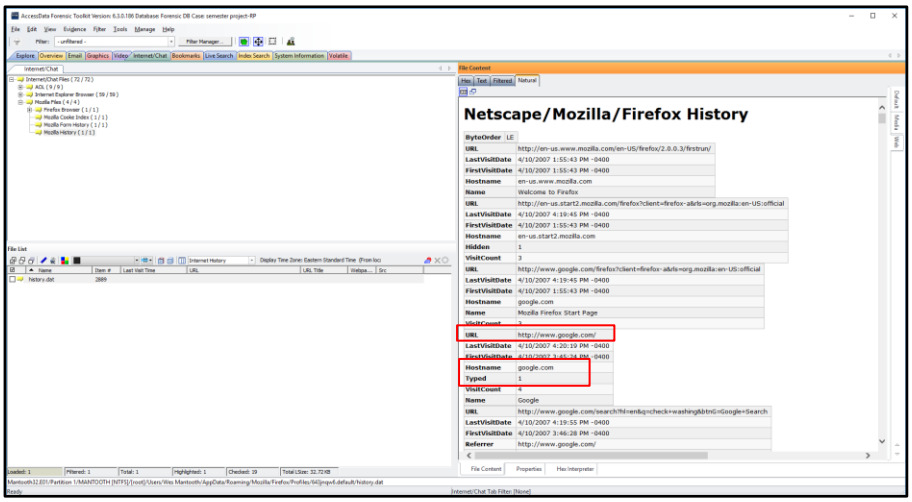


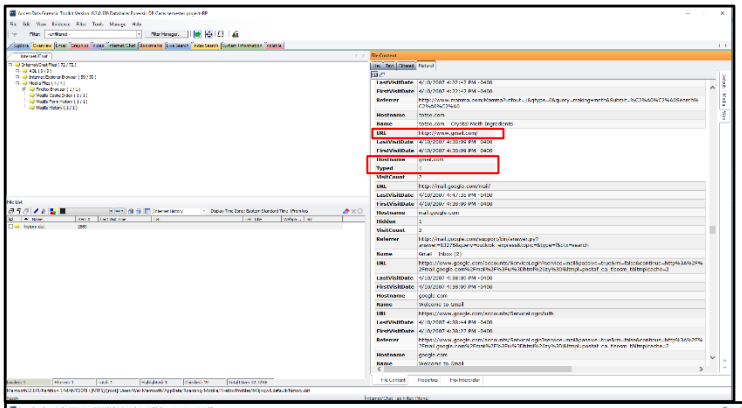


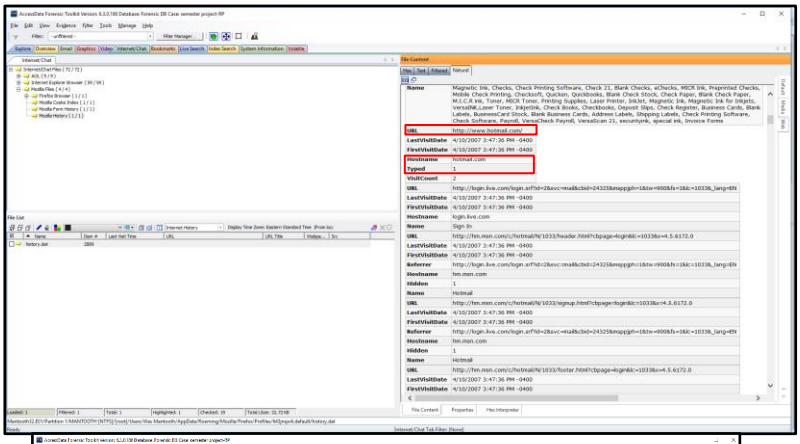
21. Identify any URLs that were visited by manually typing the address.

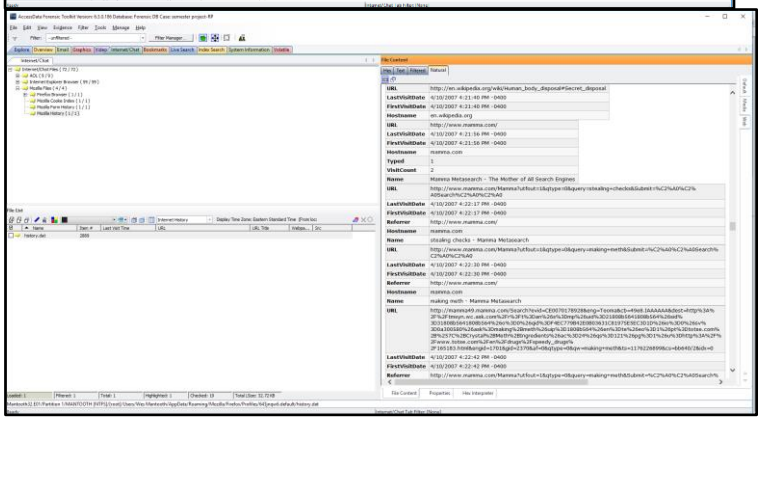
The following are the typed URLs that are visible in registry viewer after exporting **NTUSER.DAT**. Alternatively, 'Internet/Chat' files (history.dat under Mozilla files) in FTK, shows the URLs which were typed manually.

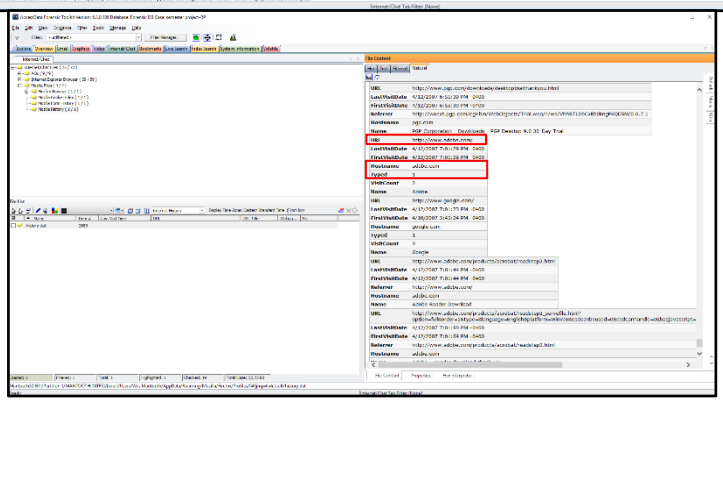






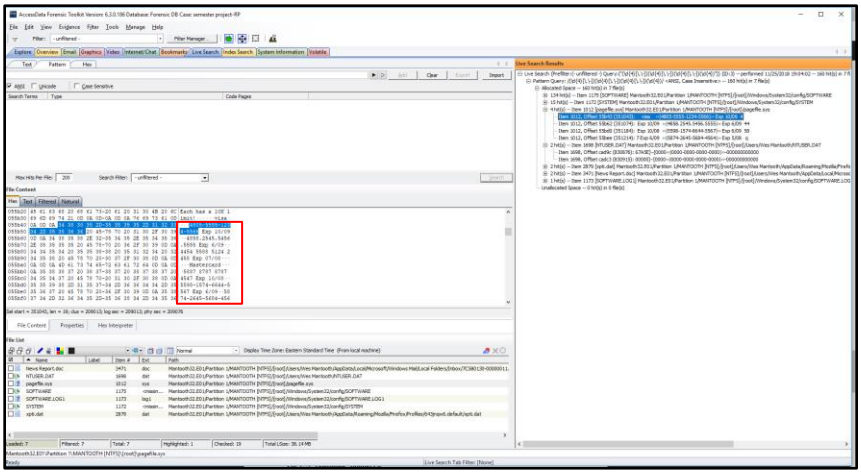


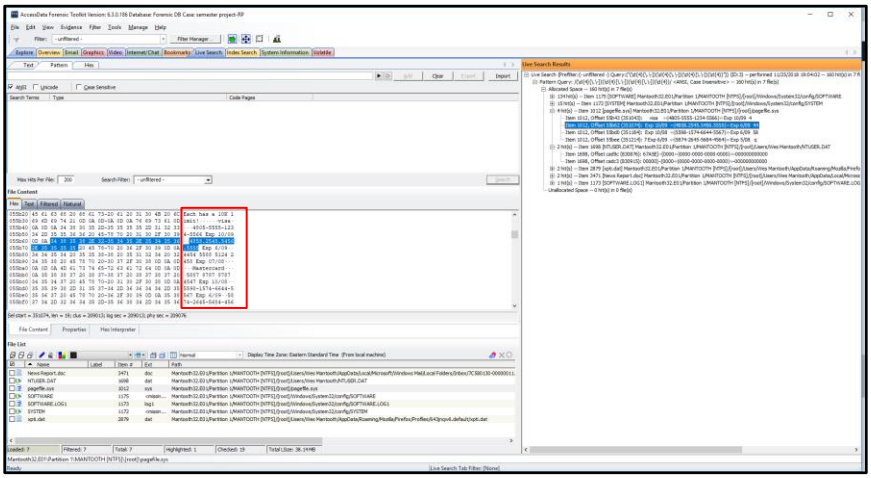


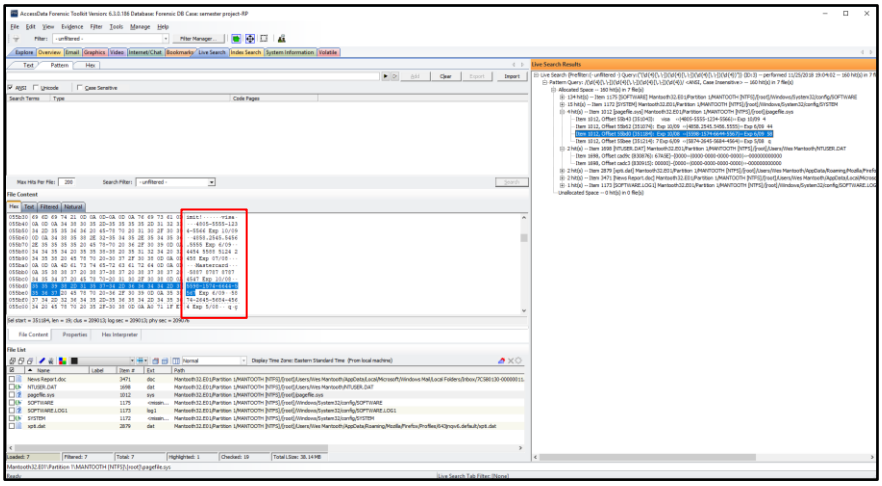


22. Identify any credit card numbers on the drive.

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

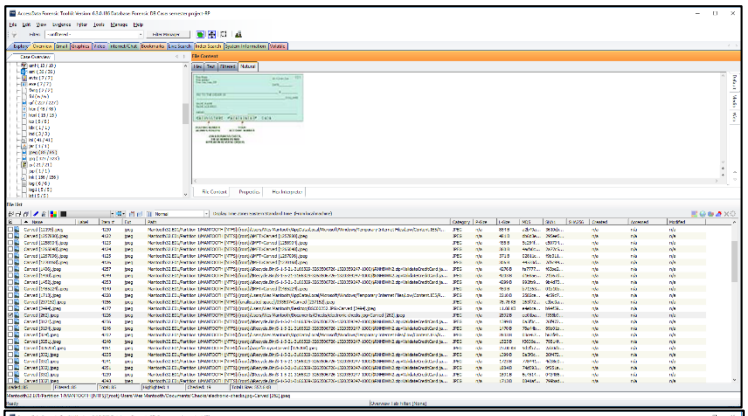


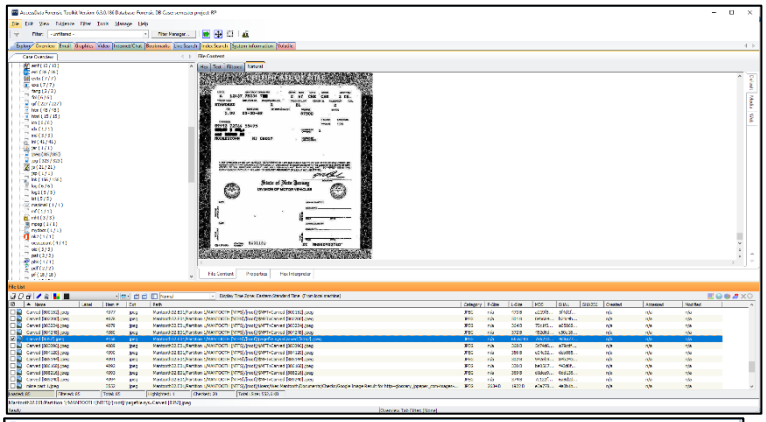


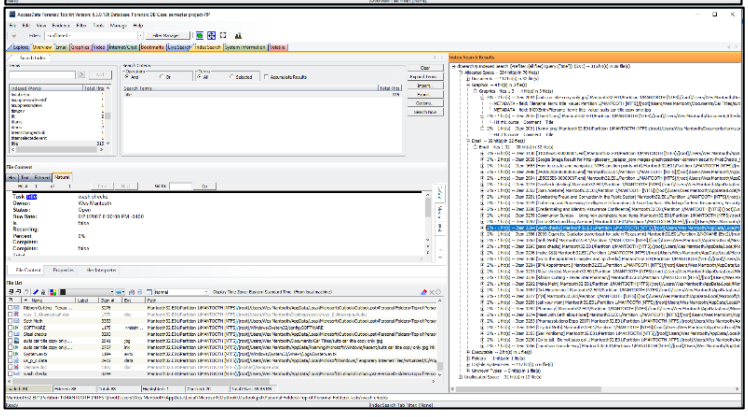


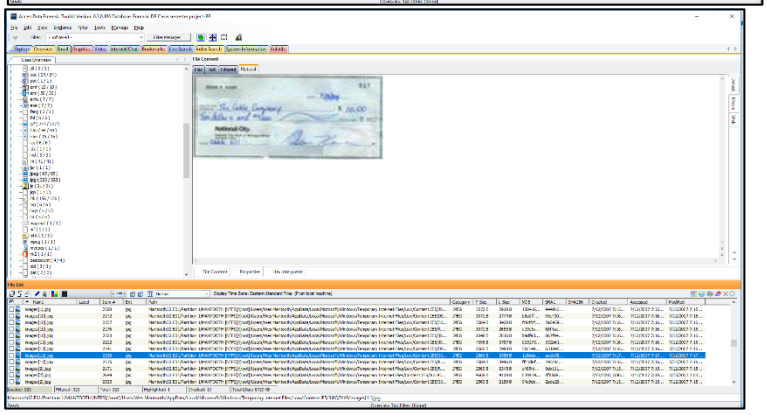
23. Provide a few examples of theft, title, checks, scam, and forensics.

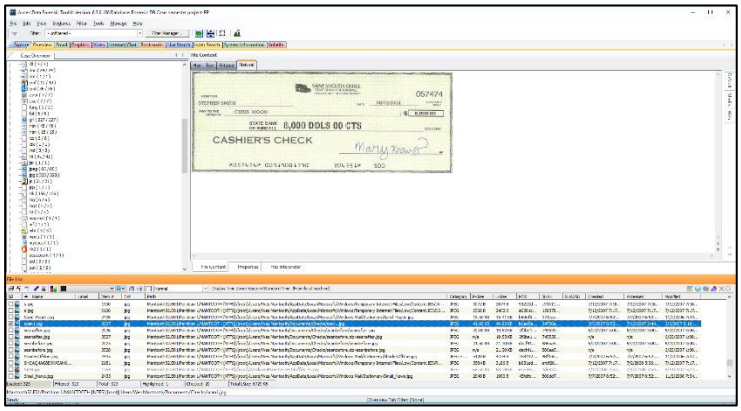
Following are the scrren-shots of a few examples of theft, title, checks, and scam and forensics which I found in multiple locations of FTK.

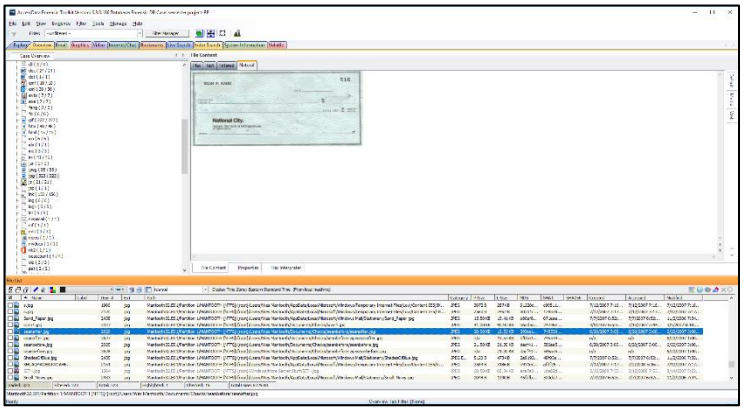


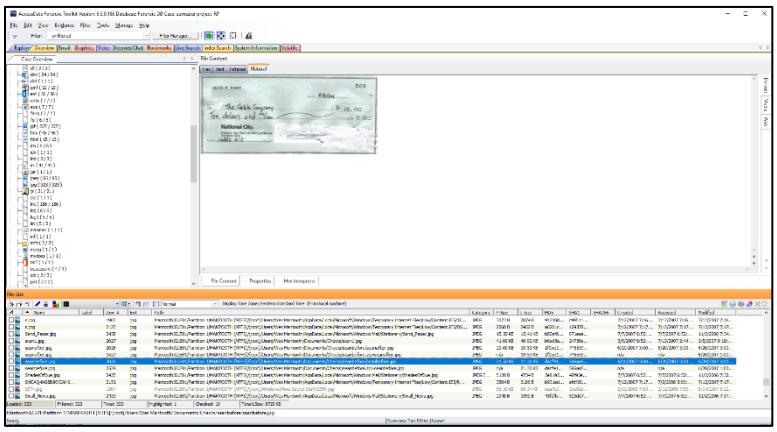


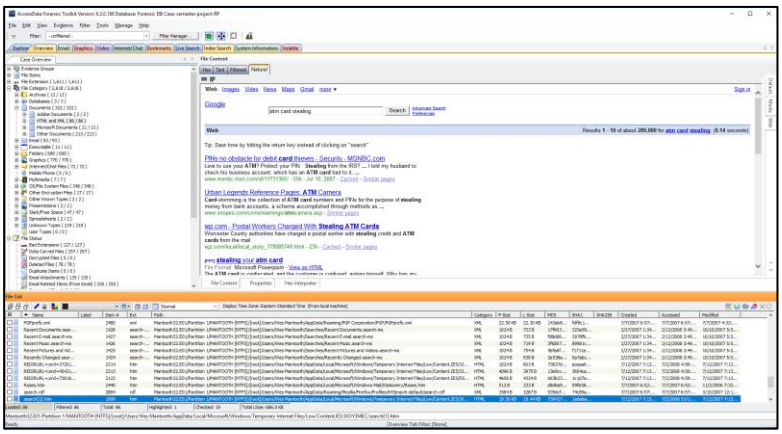


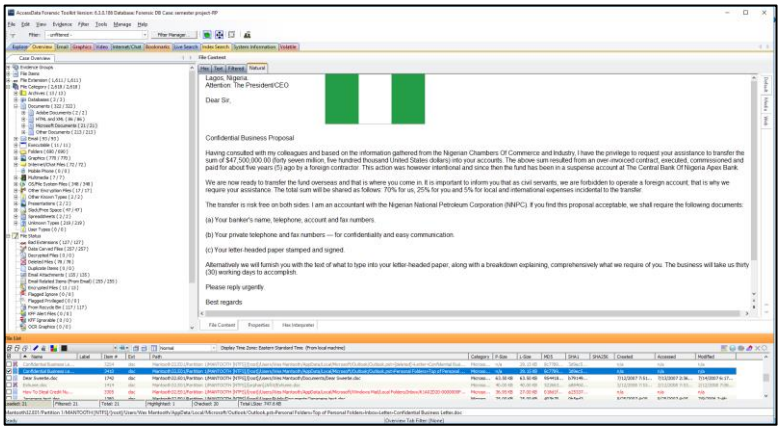


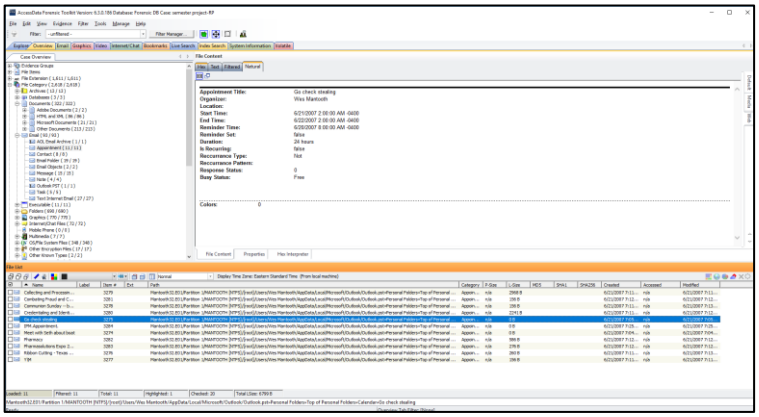




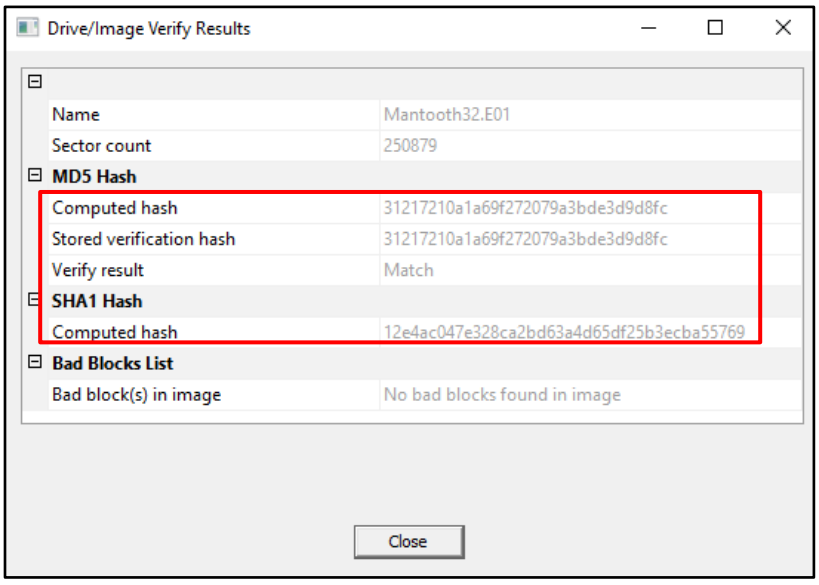








Finally, after completing my examination of the provided image file I re-verified the image integrity using FTK Imager to ensure that the image was not altered in any way. Following hash results prove that both, the stored and the computed hash values match and that the image was not corrupted in any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