ITIS 4250 / 5250

Gregory Ododa

Semester Project

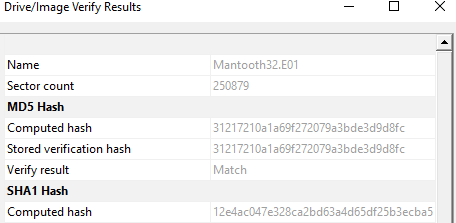
11/29/2017

**Overview:**

A local group of criminals has been involved in check fraud, credit card fraud, bad checks, ATM scams and other financial crimes. The objective of this lab is to process a desktop computer belonging to gang member Wes Mantooth for evidence of the financial crimes.

**Forensic Acquisition & Exam Preparation**

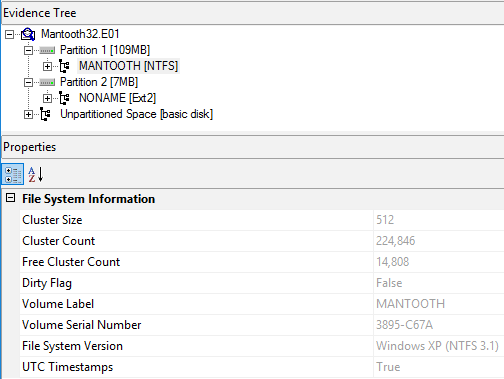
The image of the criminal’s computer named Mantooth32.E01 was provided by Detective Ketchum. To prepare the image I used the Access Data FTK (Forensic Toolkit) and FTK Imager. I began by using FTK Imager to verify the details of the Mantooth32.E01 image, below are the results and the geometry (found under the properties tab in FTK Imager:





**Findings and Report (Forensic Analysis)**

**The below image will be used to answer questions 1-5:**



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

**As shown above using FTK Imager, there are two partitions in the hard drive and their sizes are shown next to each partition.**

1. Identify the type of file systems in use.

**NTFS(New Technology File System) is used.**

1. Identify the version and service pack of the Operating System.

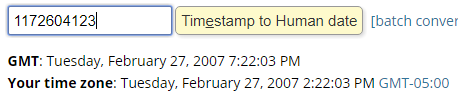
**Mantooth uses Windows XP (NTFS version 3.1).**

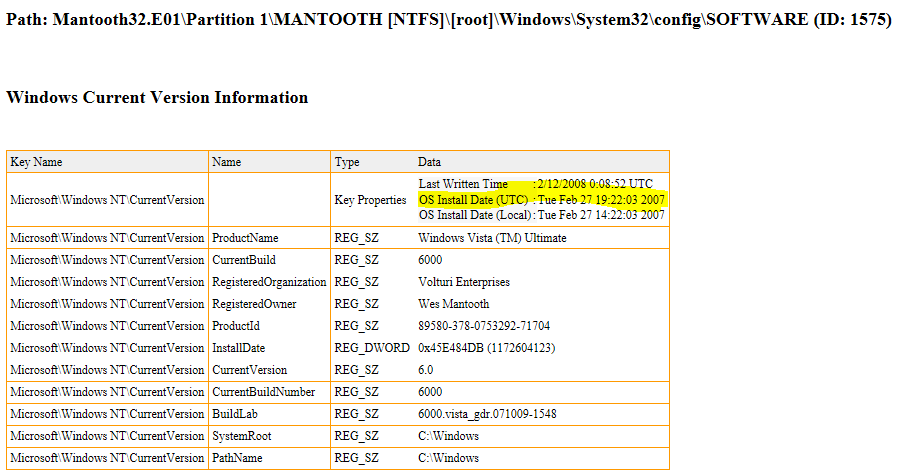
1. Find the date the OS was installed.

**The install date was found using FTK by doing an additional analysis to generate system information:**





**Below is the time converted to GMT:**



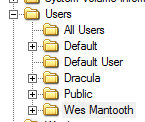
**The above information was found in the “MANTOOTH [NTFS],Software - OS Version,1575” file in my case registry file.**

1. Identify the Time Zone information for the computer.

**The Time Zone used is UTC. The screenshots above with a time show this.**

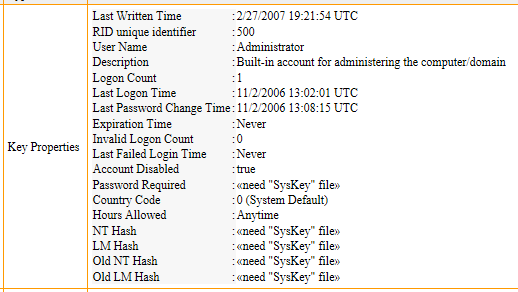
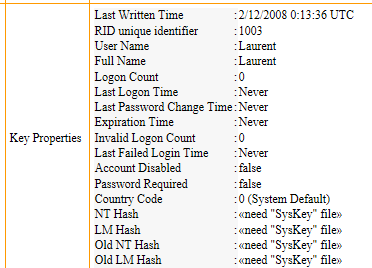
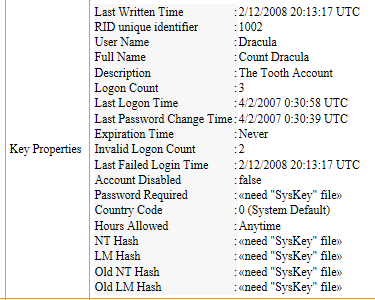
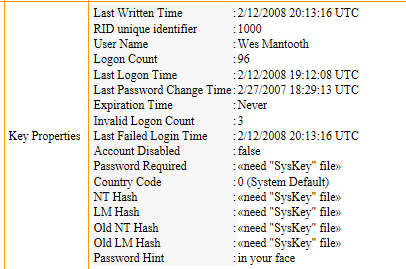
1. Show the owner of the computer.

**I found the owner in two locations, one is the first image displayed which was found using FTK Imager to search through the file system. The second image was found using FTK, I did an additional analysis to generate system information and the results give the actual registered owner of the computer:**



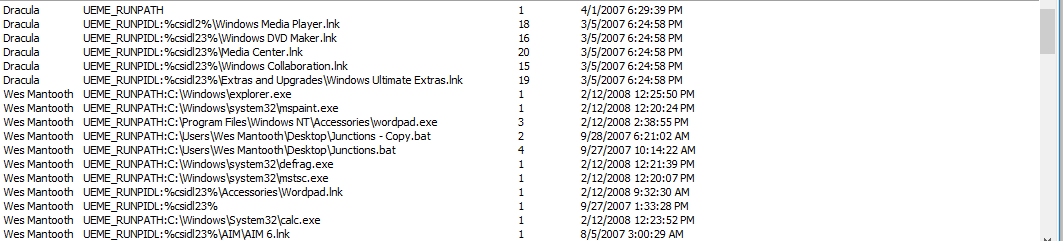


**The below images are found in my case registry folder under “1,MANTOOTH [NTFS],SAM - Users,1581”**

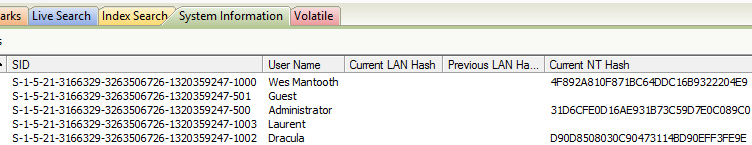


1. Show the most active user of the computer, and list all users.

**The first image on number 6 (above), shows all the users. Using the generated system information from FTK again I found that Dracula and Wes Mantooth have the most usage of the computer. Below shows the UserAssist information for applications installed on the computer and Dracula has the first six entries but Wes Mantooth has all of the rest:**



**Below are all the users found under SAM (Security Account Manager Registry file) Users in the FTK generation of system information:**



1. Identify user accounts and who uses the account.

**The images below were found in the SAM file:**

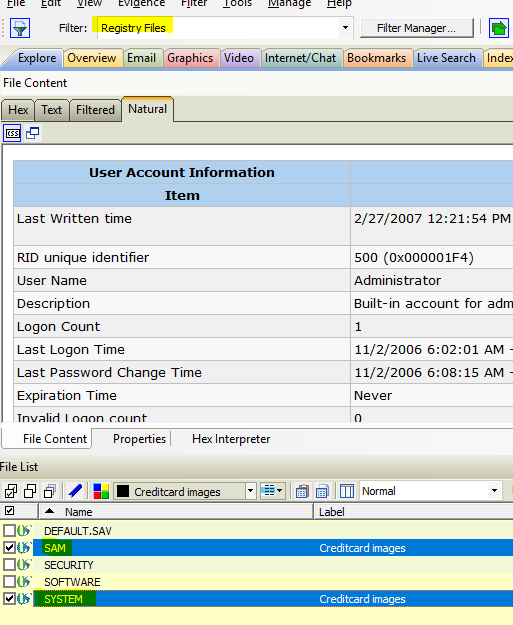


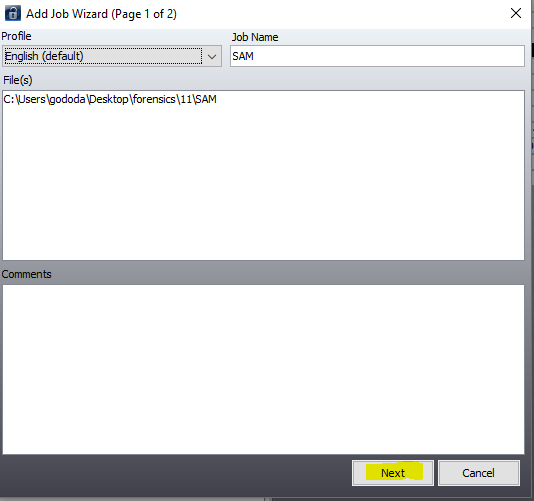




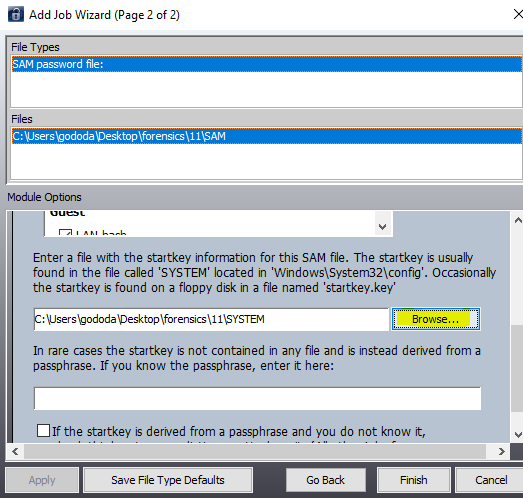
1. Acquire user passwords.

**First in FTK find the registry files SAM and SYSTEM and export them to a folder:**



**Next go to the password recovery tool to search the SAM file:**

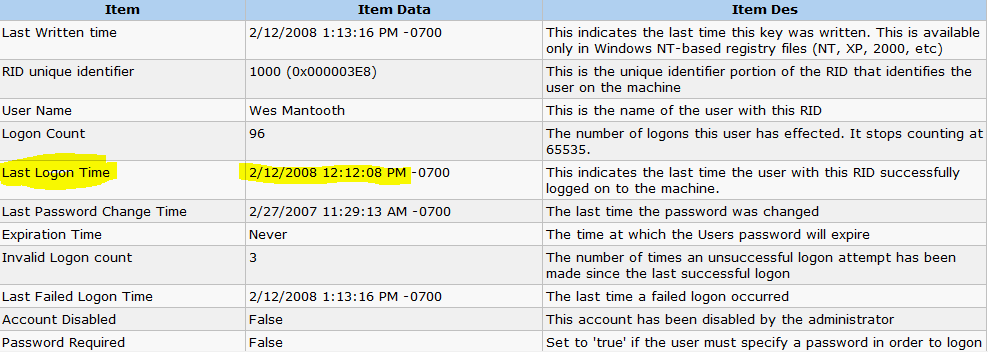
**Then choose SYSTEM:**



**All of the passwords came out empty except for Dracula and Wes Mantooth’s passwords. Below are the results:**

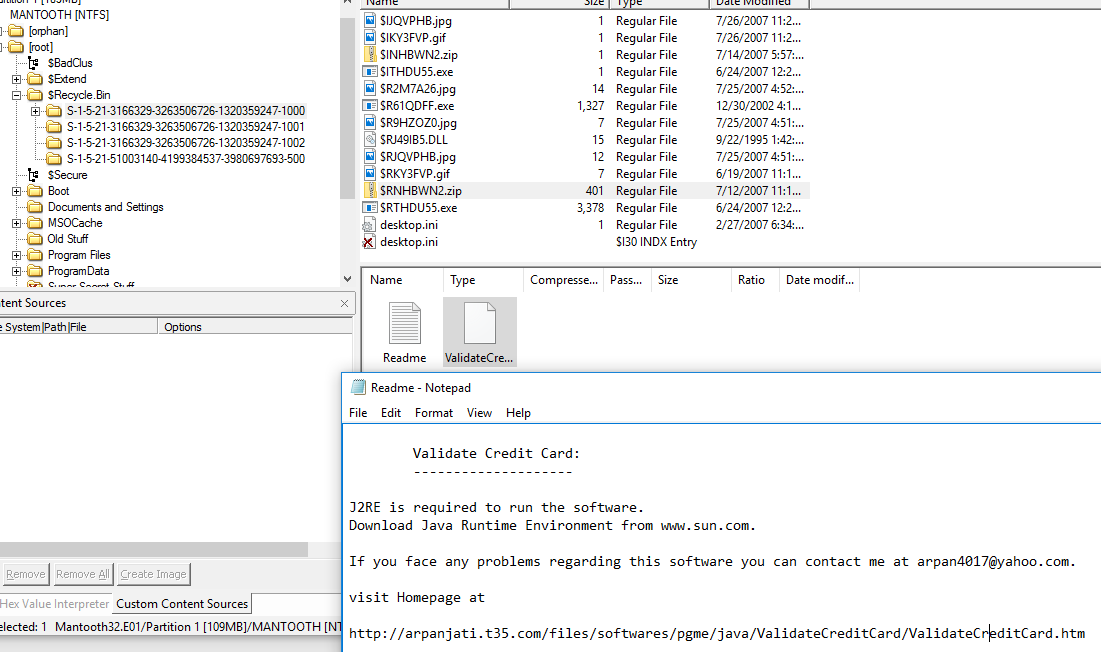


1. Identify the last date Wes Mantooth logged on.



**The image above was found in SAM file.**

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



**Above is a picture of Mantooth’s Recycle bin and a zip file for a file named ValidateCreditCard that might be of some use for the investigation.**

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

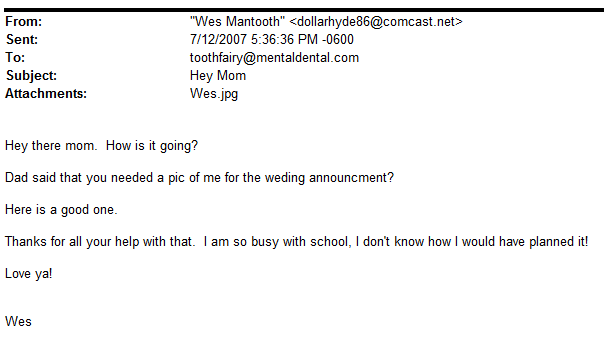
**The image should have been in the folder below:**



1. Identify any pictures of Wes Mantooth.



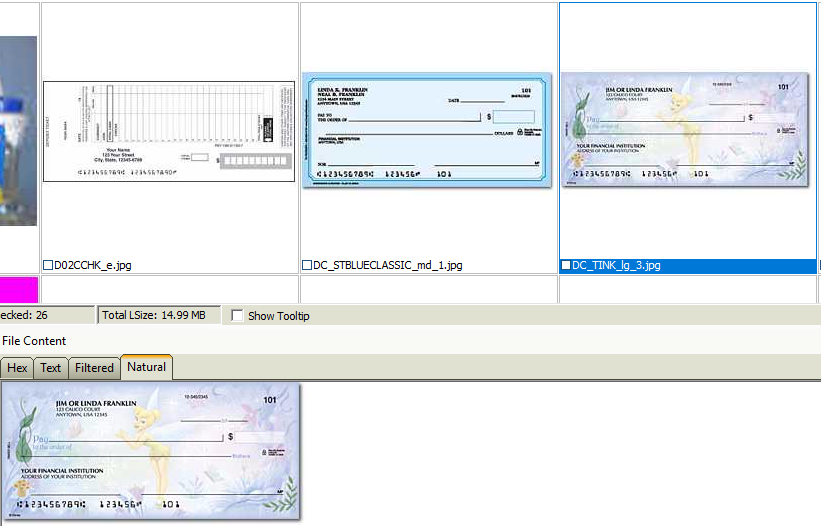
**This is a picture of Wes that he sent to his mother in the below email:**



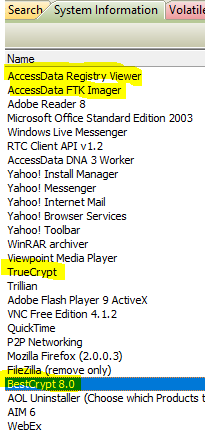
1. Identify any pictures related to the fraud or financial crimes mentioned above.

**The images below are from Wes Mantooths computer, showing several checks and a process where someone is tampering with an ATM.**





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



**AccessData programs are all forensic tools, also there is TrueCrypt, BestCrypt and PGP for encryption.**

1. Identify the most commonly opened programs.



**FTK Imager is the most commonly opened program. (Found in System Information)**

1. Provide ~~a list of all~~ deleted files. TOTAL NUMBER OF

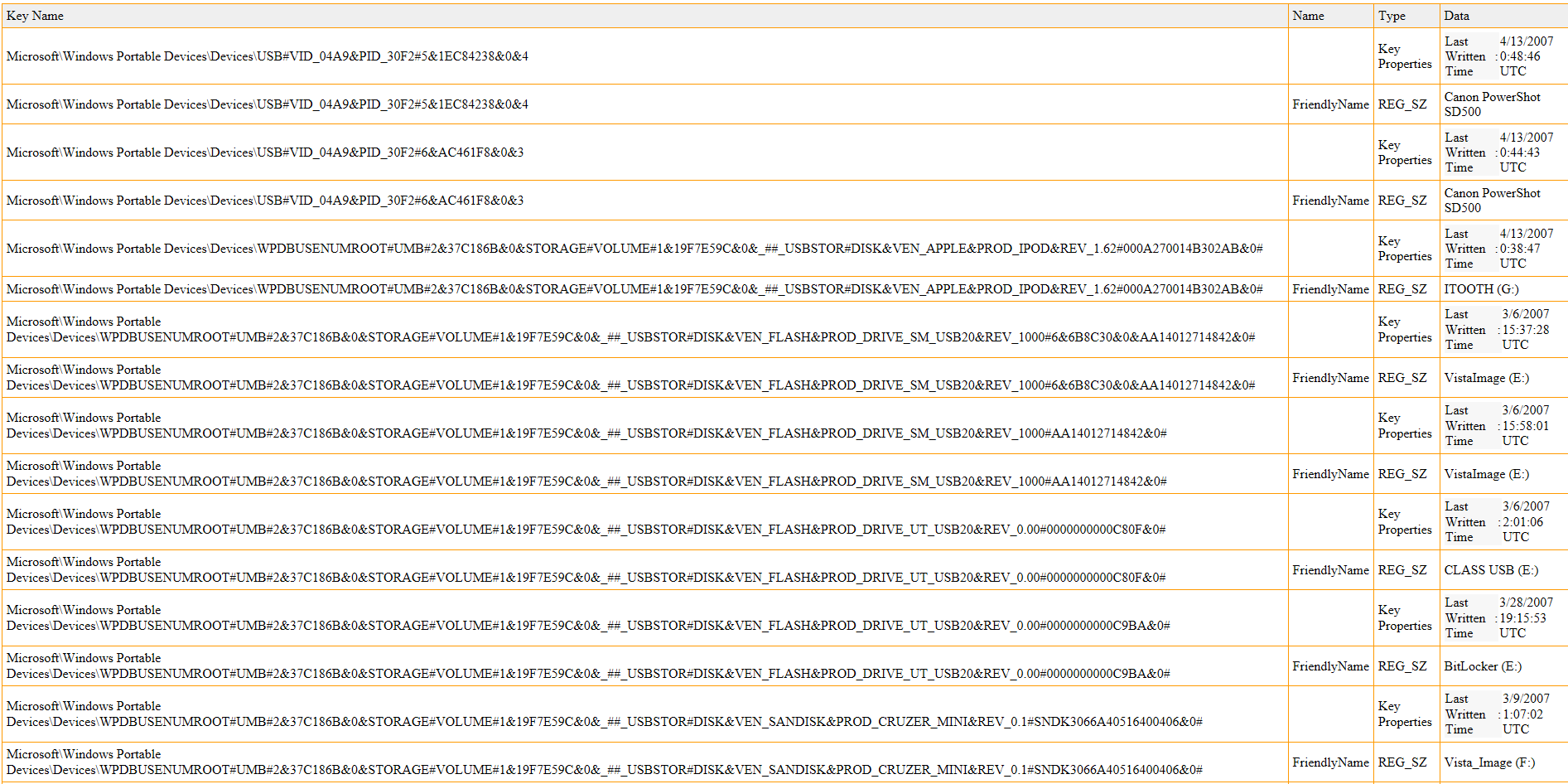
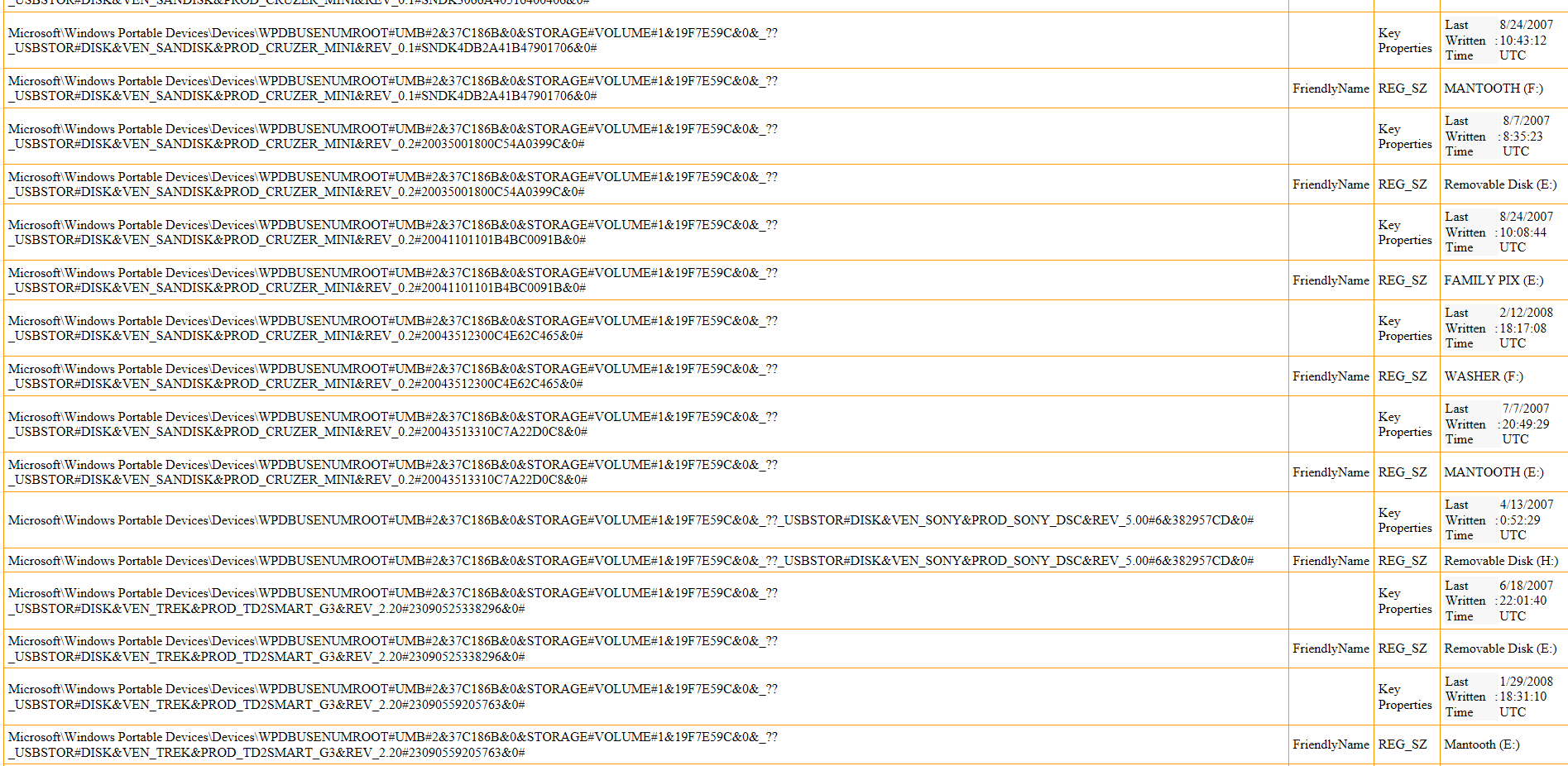
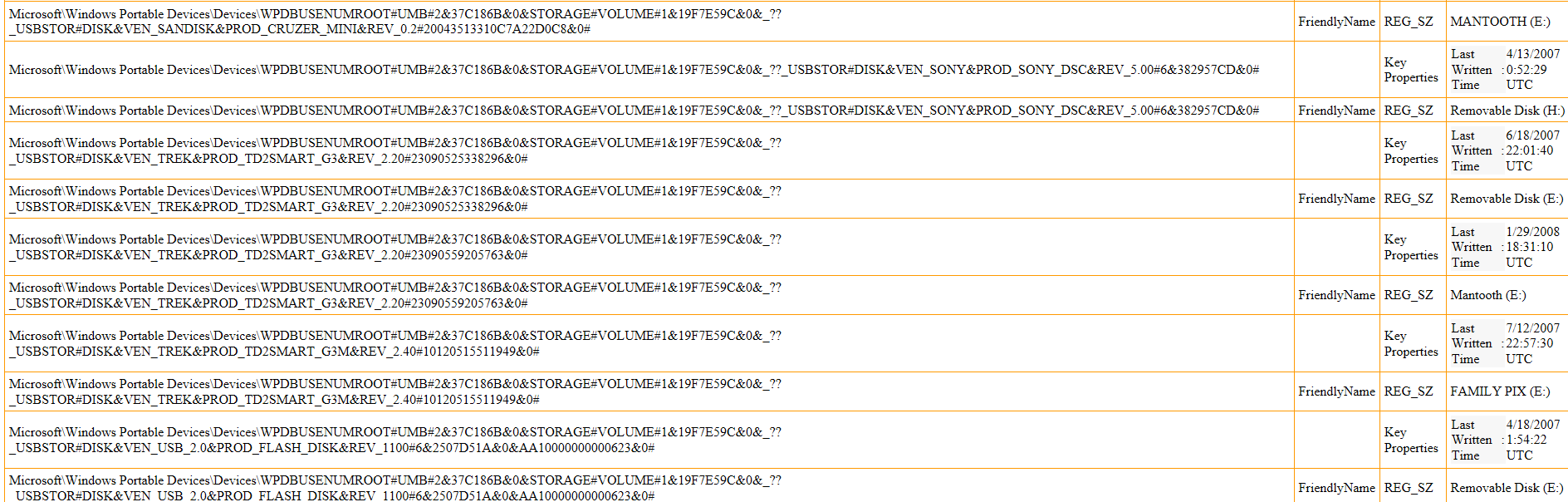
 **(Found under Overview in FTK)**

1. Perform a file carving ~~and list~~ carved files found. TOTAL NUMBER OF:

**(Found under Overview in FTK)**

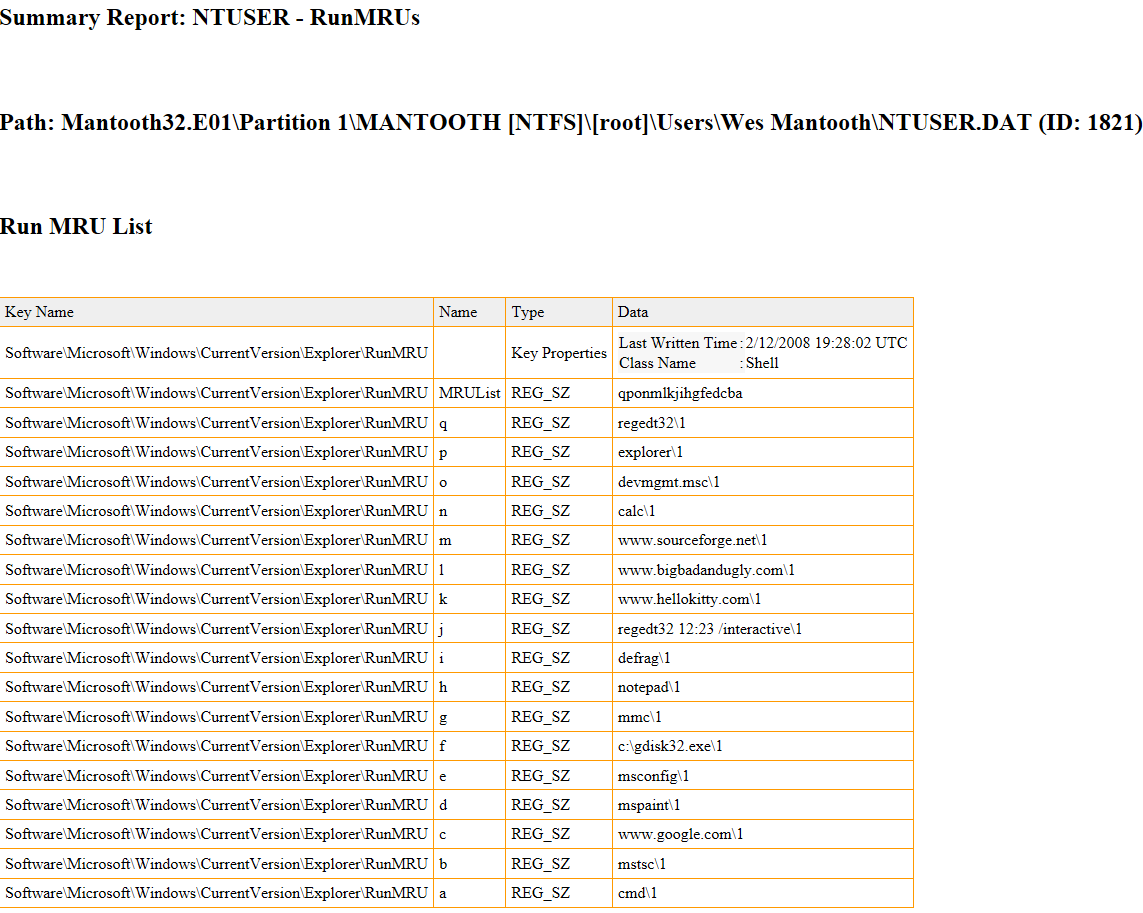
1. Identify any cameras, USB drives or other devices that have been attached to the computer.

**By using the Registry Report in my case folder (Semester\registry\_viewer\AutoRSR ) and selecting “1,MANTOOTH [NTFS],SOFTWARE - Installed Devices,1575” file it gave me the Cameras and USB files :**

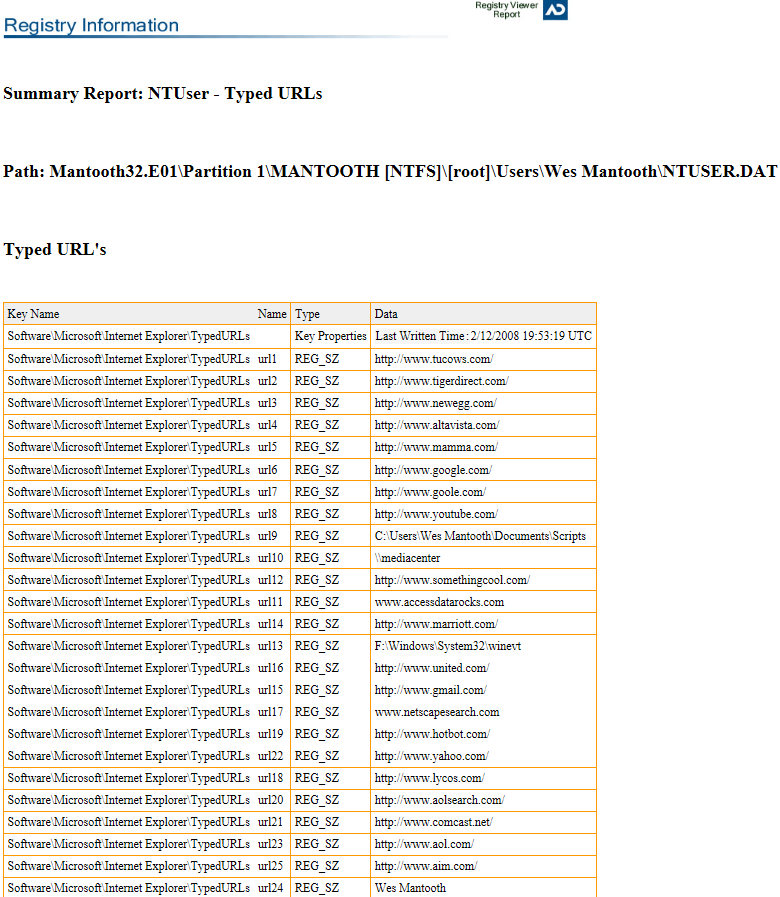
1. Identify the most recently run programs.

**The most recently ran programs are found in summary report: NTUSER –RunMRU’s in my “Semester\registry\_viewer\AutoRSR” case folder:**



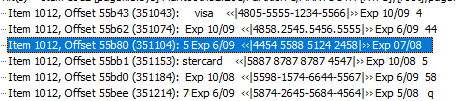
1. Identify any URLs that were visited by manually typing the address.

**In my case folder I used the “1,MANTOOTH [NTFS],Wes Mantooth,NTUser - Typed URLs,1821” File to view the typed URLs:**

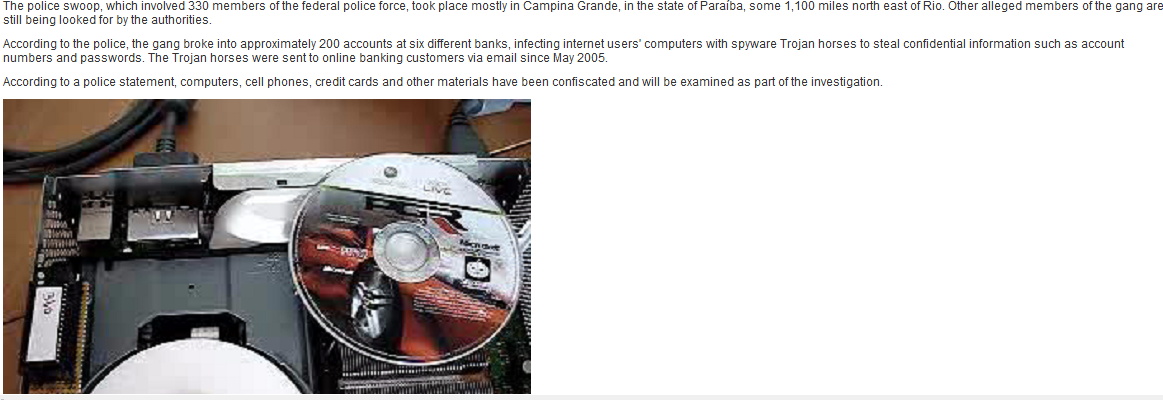


1. Identify any credit card numbers on the drive. (This will require live search with a regular expression)

**In the live search I went to the pattern section and selected credit cards and below are the results:**

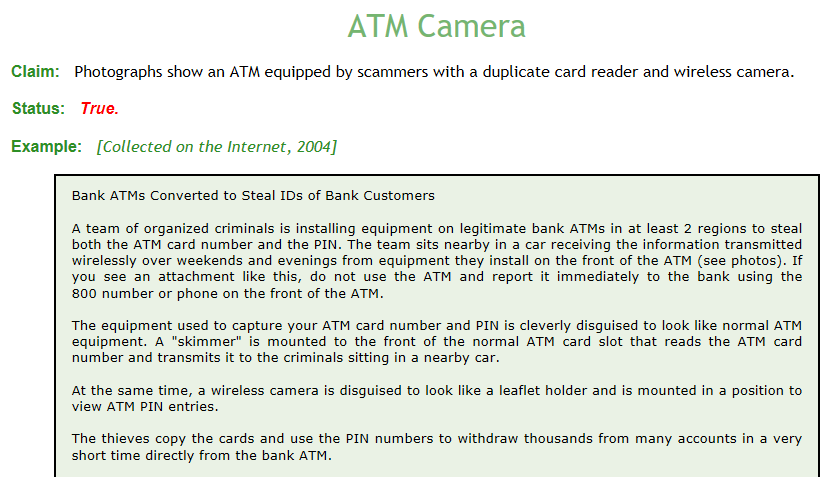


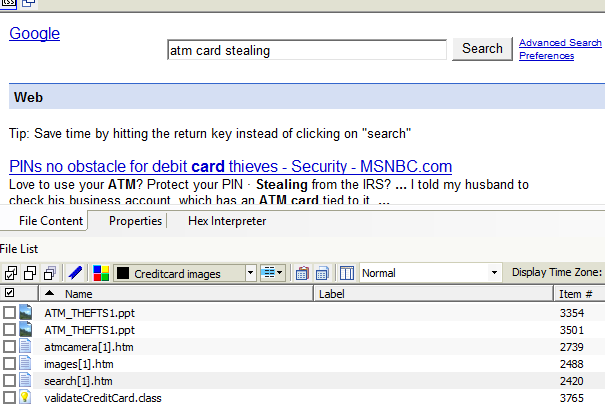
**In an email to John Washer there is an article about the theft of private information and credit card numbers below:**

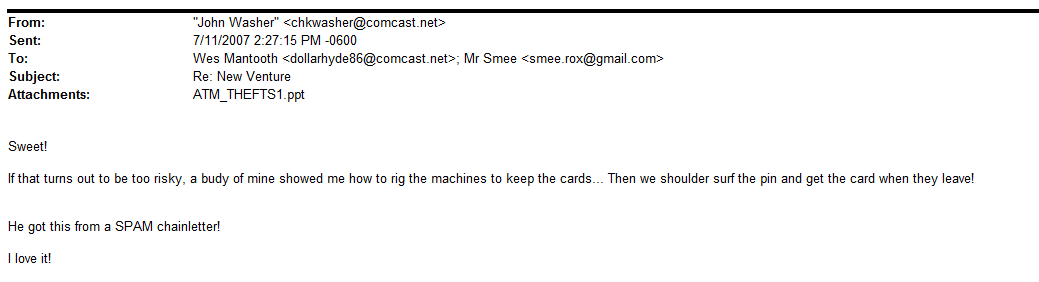


1. Detective Ketchum has provided a list of search terms: Theft, Title, Checks, Scam, Forensics. Provide ONLY (a few examples of) results of these that you believe may be relevant.

**There is a visited page that talks about theft using ATMs when Theft was searched:**



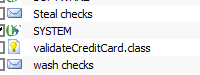


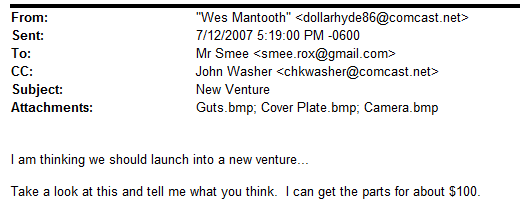


**(PowerPoint on ATM Theft attached in email)**

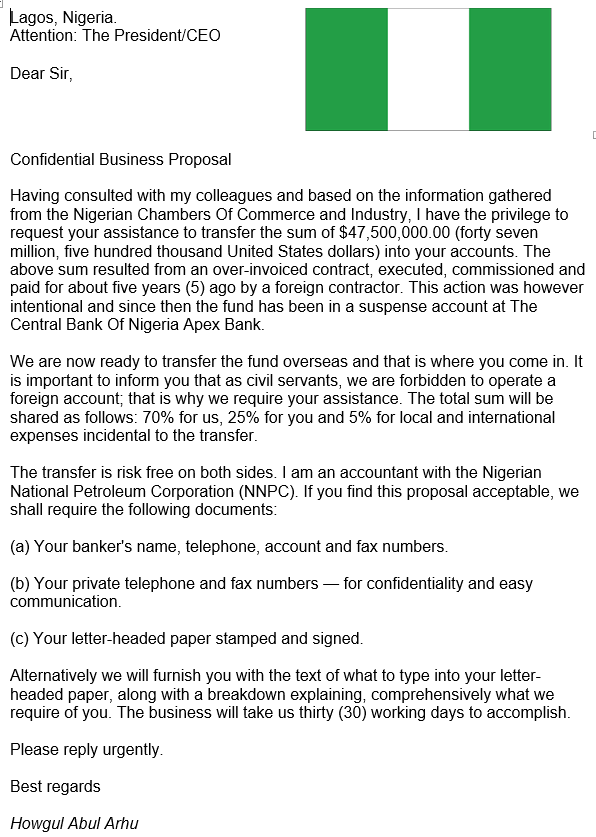


**(Program to validate Credit Cards)**



**There is also an email that link to the images above of the ATM tampering:** 





**(A scam letter to trick individuals to disclose private financial information)**

**Conclusion:**

There are several pieces of evidence proving intent to preform financial crimes. From the emails discussing tampering with ATMs, to the web searches for similar intentions, and even credit card numbers found in Wes Mantooth’s account, all of the evidence above can be used in deciding whether he is innocent or guilty.

**Below is the verified hash of the Mantooth image after examination (Unchanged from before beginning the investigation):**

