Mantooth Image Analysis

Report

Prepared By:

Jimmie Neese

Professor Zambotti

CSA 201: Digital Forensics I

23 Oct 2025

*Executive Summary*

Throughout this report, there will be information and evidence that was obtained from an exact copy of a hard drive from a computer named “Mantooth.e01”. The user of the computer being investigated has the name Wes Mantooth. There were multiple different tools that were used to investigate. All the tools being used are open-source tools. Open-source means that they are free for anyone to use. The hard drive was searched for multiple different flags, and many different forms of criminal evidence were found throughout the investigation. Wes Mantooth seemed to be a very low-key individual that could be incriminated against for multiple reasons. These reasons include credit card fraud, check fraud, ATM skimming, and making and selling multiple different kinds of drugs. All of the evidence included is explained referring to the corresponding screenshot. Throughout the report multiple forms of evidence backing up these claims will be mentioned. Included in the following report are the methods, findings and evidence, timeline of the user activity, and the conclusion.

*Methods*

Multiple resources were used to find the evidence in the “Mantooth.E01” image. These include:

-Forensic Toolkit (FTK) Imager

FTK Imager was used to make a bit-by-bit copy of the hard drive being examined.

-Autopsy

Autopsy was used to search through the bit-by-bit copy of the hard drive in order to find evidence within the drive.

-Windows Registry Explorer

Windows Registry Explorer was used to look through multiple different hives found within the image. These hives contained some of the evidence shown below.

-PrefetchWindows Event Viewer

PrefetchWindows Event Viewer was used to look through the event log found in the image. The event log was used to search for the last known shutdown of the drive.

-PicPick (Screenshot Tool)

PicPick was used to document the evidence found within the screenshots taken

*Findings*

While investigating the “Mantooth.e01” image, multiple forms of evidence brought up questions. (See below)

A screenshot of a computer

AI-generated content may be incorrect.

Figure 1 (Above): The MD5 hash of the file was verified with the MD5 of the “Mantooth.E01.txt” file.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 2 (Above): The main user of the computer was located and determined to be “Wes Mantooth”. This was determined because Mantooth had the highest number of logins into the computer with 96 logins (see above).

A screenshot of a computer

AI-generated content may be incorrect.

Figure 3 (Above): This screenshot was taken from PrefetchWindows Event Viewer and shows the last time the user logged in. The Event ID 6005 indicates the login.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4 (Above): The Windows Registry Explorer was used to examine the System hive found on Autopsy. The screenshot above shows the Current Version of Windows (Windows 6.0) that was used on the Mantooth.e01 image.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5 (Above): The screenshot above indicates that the computer's time zone was set to Mountain Standard Time. This was found using the System hive in the Windows Registry Explorer. The time zone indicates where the device was used.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 6 (Above): The screenshot above shows a USB drive that was connected to the computer. Autopsy was used to determine the Make, Model, and Serial of the drive. As you can see, the device is from Silicon Motion Inc. in Taiwan.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 7.1 (Above): The search made above was found in the Web History section of Autopsy. The website the user went to includes “speedy\_drugs” and “howtomanufactu.” This starts to form the question about the users possible interest in drugs.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 7.2 (Above): Another interesting search that the user made was found. This search seems to include information about the user wanting to learn how to steal credit cards. This was determined by the search query “atm%20card%20stealing”

A screenshot of a computer

AI-generated content may be incorrect.

Figure 7.3 (Above): The screenshot shows the web search made by Wes Mantooth that has the search query of “drug\_recipes”. This reinforces the idea that the user is involved in some drugs and other illegal activities.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 8 (Above): The email on the right side of the screenshot above was found with an attachment containing a prescription. From reading the email, it was determined that this was stolen from a Pharmacy. This reinforces more evidence that the user was in the drug scene.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 9 (Above): The screenshot above shows that the email address “dollarhyde86@comcast.net” is the user Wes Mantooth’s email address. The email above also reinforces Mantooth’s involvement in drugs.

A screen shot of a computer

AI-generated content may be incorrect.

Figure 10.1 (Above): The image found above shows what looks to be someone putting a credit card scanner on an atm. This brings the question and shows evidence that the user possibly has a background in some fraud.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 10.2 (Above): This image above is titled “csid\_meth1[1].jpg”. This type of evidence indicates that the user has been using meth and also reinforces the idea that the user is or has been involved in drugs.

A computer screen shot of a hand holding a candy

AI-generated content may be incorrect.

Figure 10.3 (Above): This image was found in the images section of Autopsy and depicts little bags filled with what looks to be cocaine and some other form of drug.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 11.1 (Above): The screenshot above shows that the software “TrueCrypt” was installed on the device used by Wes Mantooth. This could indicate that the user wanted to be able to encrypt some text or even some sort of file, which brings up some questions about why the user would want to encrypt text.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 11.2 (Above): This screenshot shows that FTK Imager was installed on the computer, which could indicate that the user could have some interest in Digital Forensics, or he could have been using it to try to look through his own computer to cover evidence.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 11.3 (Above): The screenshot above shows that “BestCrypt 8.0” was installed on the computer. This reinforces the idea that the user could have wanted to encrypt some text on his computer. This could be related to the drug trades or really any crime that we have seen the user commit.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 11.4 (Above): The screenshot above shows the metadata found in Autopsy for the “BestCrypt 8.0” software. The screenshot shows the last time the software was accessed, which proves that the user was trying to encrypt something.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 12 (Above): The screenshot above is an image that was deleted. The image was recovered and shows a South Park character that depicts the user Wes Mantooth’s lifestyle. The image was recovered by extracting it from Autopsy.

A computer screen shot of a person in a atm

AI-generated content may be incorrect.

Figure 13 (Above): The image above is a PowerPoint that was found on the “Mantooth.e01” image. This PowerPoint shows information on how to place an internal credit card skimmer into an ATM, reinforcing the previous evidence that shows the user could have been committing some fraud.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 14 (Above): The screenshot above shows that the user had a conversation containing him saying “go to jail. Do not pass go!” followed by some tasks. This could be information saying that if the user goes to jail, those are the tasks that the receiver of the message needs to do.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 15 (Above): The image above shows a file that was found on the “Mantooth.e01” image, containing information on how to make meth. This backs up the previous evidence indicating that the user is making drugs. The file was found using Autopsy.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 16 (Above): The screenshot above was taken from Autopsy. The image contains a .txt file titled “How to Steal Cars.txt”. The text document gives a step-by-step method on how to steal a car. This brings suspicion that the user could have been attempting to steal cars, along with the rest of the crimes he has committed.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 17: The right side of the screenshot above shows an email sent that talks about a huge bust of a credit card skimmer. The email has an attachment, which was extracted using Autopsy. The left side of the screenshot is the news report talked about in the email. This reinforces the idea that the user was involved in some credit card skimming and fraud.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 18 (Above): The image above shows a conversation between the user and someone else. The user says he has the “Special K” he has been looking for. This could be some sort of drug and reinforces the idea that the user makes and sells drugs. The conversation was found using Autopsy.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 19 (Above): The screenshot above shows an image of a check. This check is titled to “Tracy Smith”. Throughout the investigation, there was nothing found about Tracy Smith, which leads to the idea that the user is committing check fraud as well.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 20 (Above): The screenshot above shows a .zip file titled “ValidateCreditCard”. This reinforces the previous evidence that the user is skimming credit cards and validating them to make sure they work. This was also found in Autopsy.

*Timeline*

Below is a timeline created of the user Wes Mantooth’s suspicious activity on the computer:

|  |  |  |
| --- | --- | --- |
| Date: | Time: | Event: |
| 5 Mar. 2007 | 21:03:10 EDT | Check2.bmp was accessed by the user |
| 12 July 2007 | 19:16:43 EDT | An image of pills and cocaine was accessed by the user |
| 12 July 2007 | 19:16:43 EDT | An image of more drugs was accessed by the user |
| 12 July 2007 | 19:16:43 EDT | An image of more possibly drugs was accessed by the user |
| 12 July 2007 | 19:16:44 EDT | An image of crystal meth was accessed by the user |
| 12 July 2007 | 19:16:44 EDT | An image of bags full of white powder was accessed by the user |
| 12 July 2007 | 19:17:01 EDT | An image of bags of drugs was accessed by the user |
| 12 July 2007 | 19:17:01 EDT | An image that is titled “csid\_meth[1]” was accessed by the user |
| 13 July 2007 | 19:00:16 EDT | An image of a ATM skimmer was accessed by the user |
| 14 July 2007 | 13:56:55 EDT | A “ValidateCreditCard.zip” file was accessed by the user |
| 2 July 2008 | 16:56:42 EDT | A photo of a person smoking some sort of drug was accessed by the user |
| 2 July 2008 | 17:01:32 EDT | A file titled “How To Manufacture Meth” was accessed by the user |

Below is a timeline of the investigation taken place on the “Mantooth.E01” image:

|  |  |  |
| --- | --- | --- |
| Date: | Time: | Event: |
| 21 Oct 2025 | 3:22:21 PM EST | The Software hive was found and extracted |
| 21 Oct 2025 | 3:23:12 PM EST | The System hive was found and extracted |
| 21 Oct 2025 | 3:23:55 PM EST | The Security hive was found and extracted |
| 21 Oct 2025 | 3:26:45 PM EST | The time zone of the computer was found and documented |
| 21 Oct 2025 | 3:34:22 PM EST | The Current Version of the computer was found and documented |
| 21 Oct 2025 | 3:42:12 PM EST | The main user of the computer was found and documented |
| 23 Oct 2025 | 2:50:49 PM EST | A questionable USB device that was attached to the computer was found and documented |
| 23 Oct 2025 | 2:53:58 PM EST | Three suspicious websites that the user accessed were found and documented |
| 23 Oct 2025 | 2:56:58 PM EST | An email with an attachment was found and documented |
| 23 Oct 2025 | 3:07:43 PM EST | Three software that could have been used for Encrypting messages were found and documented |
| 23 Oct 2025 | 3:15:32 PM EST | A photo of a stolen check was found and documented |
| 23 Oct 2025 | 3:20:22 PM EST | A PowerPoint that displays how to put an ATM skimmer in was found and documented |
| 23 Oct 2025 | 3:29:12 PM EST | A file that teaches you how to manufacture Meth was found and documented |
| 23 Oct 2025 | 3:33:01 PM EST | A zip file named “ValidateCreditCards” was found and documented |
| 23 Oct 2025 | 3:36:53 PM EST | A file explaining how to steal a car was found and documented |
| 23 Oct 2025 | 3:42:44 PM EST | A png of a news report talking about how a credit card skimmer got busted was found and documented |
| 26 Oct 2025 | 2:56:21 PM EST | The System.evtx hive was found and extracted |
| 26 Oct 2025 | 2:58:55 PM EST | The last login of the user was found and documented |
| 26 Oct 2025 | 3:12:41 PM EST | The MD5 hash of the image was verified |

*Conclusion*

After the examination of “Mantooth.e01”, many different things can be taken into consideration. The investigation of the hard drive was done using multiple different online tools. These tools include FTK Imager, Autopsy, Windows Registry Explorer, PrefetchWindows Event Viewer, and PicPick. The tools were used in different ways and occurrences to help to find the flags and all the evidence included within the report. The main user of the computer was determined to be Wes Mantooth. Wes Mantooth seems to have a background in multiple different forms of drugs. This includes making and selling drugs like meth, cocaine, and some prescription drugs (Figure 7.1, 7.3, and Figure 8). It could be determined from the evidence that while selling the drugs, Mantooth was also committing multiple fraudulent acts. There is very concrete evidence in this report that can incriminate Wes Mantooth for multiple different types of fraud. There was evidence found that includes content that indicates Wes Mantooth using credit card skimmers (Figure 7.2). There is also evidence that Mantooth has a friend or multiple friends that are in with him in all of this. There was also evidence found that indicates that Wes Mantooth was interested in stealing cars (Figure 16). He also has pictures of checks on his hard drive that could also mean that Wes Mantooth was committing check fraud (Figure 19). Overall, Wes Mantooth could be determined to be a criminal in multiple different aspects including making and selling illegal drugs, fraud, and automobile theft.