Mantooth.E01

Digital Forensics Report

Prepared By:

**Brennen Yingling**

Professor:

**Mr. Michael Zambotti**

Class:

**CSA 201: Digital Forensics**

Date:

**October 12, 2025**

**Table of Contents**

1. Introduction ………………………………………………………..………………………… 2
   1. Executive Summary ………………………………………..………………………….... 2
   2. Tools Used …………………………………………………….………………………... 2
   3. Process ……………………………………………………….…………………….…… 3
2. Findings ……………………………………………………………………………………... 3
   1. Findings and Evidence – Day 1 ……………………………………………………….... 3
   2. Findings and Evidence – Day 2 …………………………………………......……….... 20
3. Conclusion ………………………………………………………….,.…………………….. 21
   1. Story ………………………………………………………………………………….... 21
   2. Timeline ……………………………………………………………………………….. 22
   3. Concluding Statement ……………………………………………………...………….. 22
4. **Introduction**

The purpose of this assessment is to review the Mantooth.E01 image and become familiar with using tools such as Autopsy, Windows Event Viewer, and FTK Imager, as well as any other digital forensics tools that may be needed. In this report, I will provide pictures of the fifteen flags I found during my investigation, along with a timeline of my findings, an overview of my process, and the various tools I used.

* 1. **Executive Summary**

On October 12, 2025, Professor Zambotti provided me with an image of the *Mantooth* computer hard drive. Professor Zambotti is requesting a forensic examination to see what information may have been deleted, and is requesting a full forensic examination and report for the image of this drive. From the information provided, the *Mantooth* image was collected in relation to a criminal investigation. I have searched for this drive to find evidence that shows the user is involved in illegal activity. After my investigation, the evidence I found suggests that the user could be related to buying, making, selling, or using drugs, as well as stealing credit card information by using a hidden camera beside an ATM.

* 1. **Tools Used**

Throughout my investigation, I used several different tools to analyze the image, document my findings, and show evidence, including:

|  |  |
| --- | --- |
| **Tool Name** | **What the Tool was used for** |
| Autopsy 4.22.1 (Latest Version) | I used this tool to examine the Mantooth.E01 image. |
| Exterro FTK Imager (Latest Version) | I used FTK Imager to verify the MD5 hash related to the Mantooth.E01 image. |
| Notepad | I used this tool to document my process and keep a timeline of when I found each flag. |
| Snipping Tool | I used this tool to screenshot and edit my findings. |

* 1. **Process**

Throughout my investigation period, my process involved first opening Notepad and documenting my start time for the day. Second, I would open the digital forensic tool that I had to use and load the Mantooth.E01 image. Following that, I searched for flags and documented what I found, took a screenshot, and stored that screenshot in a secure folder on my laptop. Whenever I finished for the day, I would document the end time for that investigation.

1. **Findings**

In this section of my report, I will include screenshots of any evidence I was able to locate, as well as a detailed description of what the evidence is, how I found it, and when I found it.

* 1. **Findings and Evidence – Day 1**

On 10/15/25 at 5:17 P.M. UTC, I began my investigation of the Mantooth.E01 image file. For flag #1, I was given a text document that had an MD5 hash of the Mantooth.E01 image, and I needed to verify the hash. I began by loading the image file into Exterro FTK Imager, left-clicked on the evidence item in the left pane, and clicked on “Verify Image.” Then, A box appeared showing relevant information, including the MD5 file hash. I then compared that hash to the hash provided in the text file to see if they matched. Figure 1 shows the text file as well as what I found in Exterro FTK Imager.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : MD5 Hash of Mantooth.E01 (Exterro FTK Imager).

Following that, I closed Exterro FTK Imager and opened Autopsy to begin looking for flag #2, which is to find the main Windows account user. At 5:41 P.M. UTC, in Autopsy, I clicked on the “Operating System Information” tab in the left-hand pane, then I navigated to the “NAME” column where it says WESMANTOOTH-PC. With this information, the evidence suggests that Wes Mantooth is the primary user. This can be seen in Figure 2.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Main Windows Account User (Autopsy).

At 5:48 P.M. UTC, I found Flag #3 by selecting the OS Accounts tab in the left-hand pane of Autopsy. After locating and clicking on the Wes Mantooth login, I determined that the last user login, as shown in Figure three, was on 2008-02-12 at 14:12:08 Mountain Standard Time.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Last User Log-in (Autopsy).

At 5:56 P.M. UTC, I found flag #4 by returning to the OS Information tab in the left-hand pane of Autopsy. Under “Program Name” in the right-hand pane, I identified the OS version as Windows Vista (TM) Ultimate, as shown in Figure 4.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : OS Version (Autopsy).

At 6:03 P.M. UTC, I discovered the Time Zone on this computer, or the answer to flag #5. I started by checking the SYSTEM registry hive, then going to Control Set 1, Control, and TimeZoneInformation. Then, as shown in Figure 5, I found that the time zone for this machine is Mountain Standard Time.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Time Zone Information (Autopsy).

Flag #6 is finding evidence that there has been a USB device attached to the computer. At 6:11 P.M. UTC, I found this flag by selecting the USB Device Attached tab in the left-hand pane of Autopsy, then clicking on one of the options. I determined the make of the device is Silicon Integrated Systems Corp., the model is Super Flash 1GB / GXT 64MB Flash Drive, and the serial number is 0000000000C80F, as shown in Figure 6.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : USB Item Attached (Autopsy).

I found flag #7 at 6:24 P.M. UTC, which is finding three websites visited by the user. First, I navigated to Web History in the left-hand pane of Autopsy. The three websites I found were *sccja.org/images/csid\_meth1.jpg,* which appears to be an image of methamphetamines, which can be seen in Figure 9. Then, I found two Google image results, one for drugs, specifically meth (Figure 7), and the other for stealing credit card information (Figure 8).

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Meth Image (Autopsy).

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Card Stealing Image (Autopsy).

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Meth Image (Autopsy).

At 6:41 P.M. UTC, I began investigating flag 8, which is any suspicious search queries. In the left-hand pane of Autopsy, I clicked on the Web History tab. Then, a bunch of searches that this user made appeared in the middle pane, so I looked through them, and as seen in Figure 10, the user made a search related to drug recipes.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Drug Recipe Search (Autopsy).

I then began my search for flag #9, which is finding an email with an attachment sent from the user. I discovered this at 6:49 P.M. UTC by going into the Email messages tab and then the default folder in the left-hand pane of Autopsy. In the middle pane, I sorted by “Has Attachment” and I picked an email sent by Wes Mantooth. Figure 11 shows where I found this message, and Figure 12 shows the attachment, which appears to be a prescription document.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : E-mail with Attachment (Autopsy)

A close-up of a prescription

AI-generated content may be incorrect.

Figure : Prescription Image (Snipping Tool).

I then found an email address that has been used on this computer, accomplishing flag #10. At 7:01 P.M. UTC, I navigated to the Communication Account and then Email in the left-hand pane of Autopsy. I then identified an email account being used as [dollarhyde86@comcast.net](mailto:dollarhyde86@comcast.net), which can be seen in Figure 13.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Email Address (Autopsy).

Then, for flag #11, I found three images that could be meaningful to this investigation. At 7:23 P.M. UTC, I selected File Types, then By MIME Type, then Image, and JPEG. The three images I found were of a hidden camera set up by an ATM (figure 14), a hand holding what appears to be drugs (figure 15), and a picture from a possible hidden camera by an ATM (figure 16).

A hand holding a box

AI-generated content may be incorrect.

Figure : Hidden Camera (Autopsy).

A computer screen shot of a hand holding a bag of food

AI-generated content may be incorrect.

Figure : Drugs (Autopsy).

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Picture from a Hidden Camera (Autopsy).

At 7:43 P.M. UTC, I investigated flag #12, which is at least three installed programs on the computer. I went to Installed Programs in the left-hand pane of Autopsy. In Figure 17, you can see the installed programs, including Adobe Reader (PDF viewer), VNC Free Edition (remote desktop application), and TrueCrypt (on-the-fly encryption software).

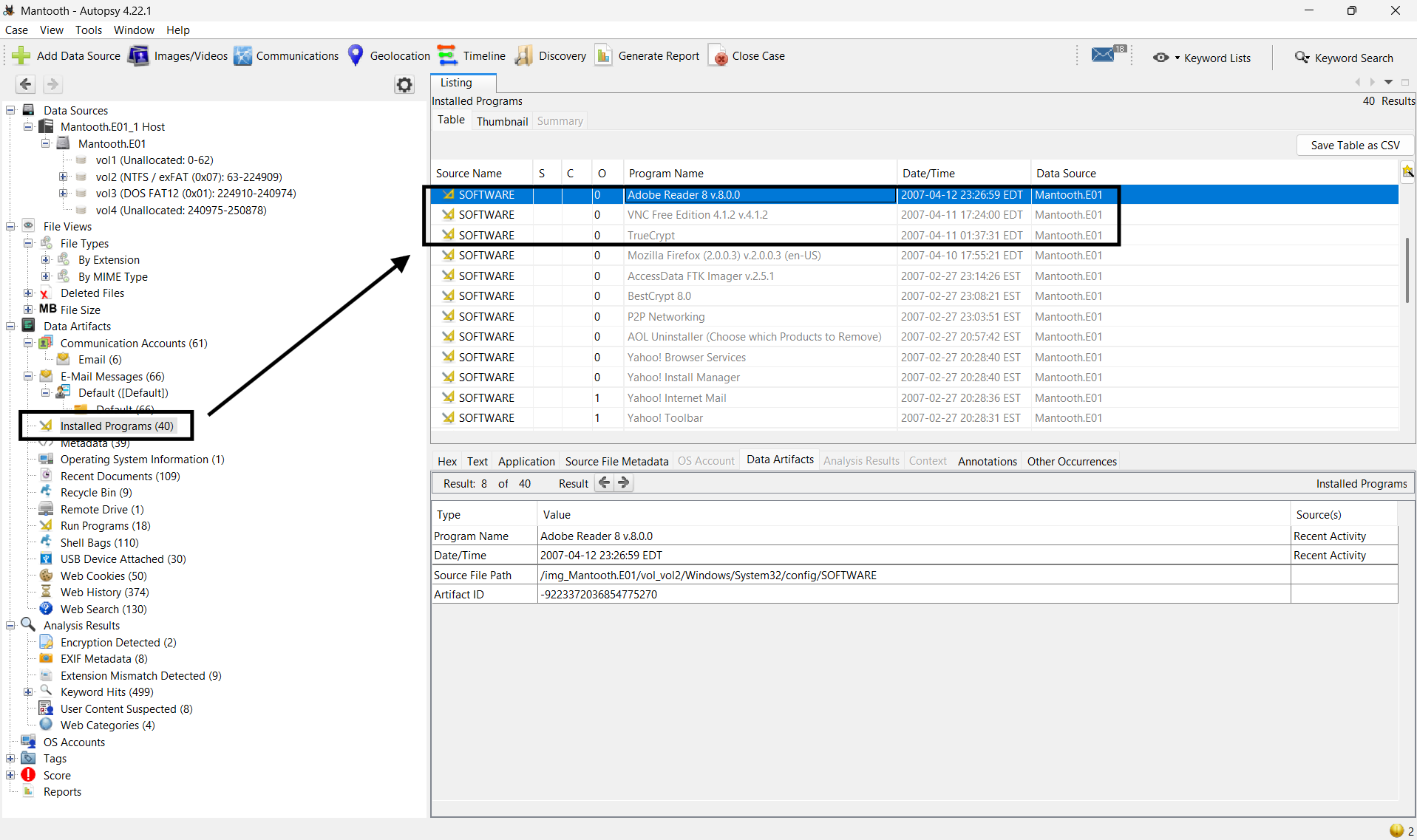


Figure : Installed Programs (Autopsy).

For flag # 13, I had to find any suspicious applications that the user has recently launched. At 8:07 P.M. UTC, I clicked the Run Programs tab in the left-hand pane. In Figure 18, it is shown that FTK Imager had been run on 2007-08-24 at 8:45:00 EDT, which suggests the user was familiar with forensic tools.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : FTK Imager was Run (Autopsy).

For flag #14, I had to identify and recover a deleted file. At 8:20 P.M. UTC, I navigated to Deleted Files, then the All folder, and searched through the entries. I found a deleted file labeled My Confession.txt, which can be seen in Figure 19. Then, I extracted the text file, which can be seen in Figure 20. Then at 8:27 P.M. UTC, I closed all related programs and wrapped up my investigation for the day.

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Deleted File (Autopsy).

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Extracted Text File (Notepad).

* 1. **Findings and Evidence – Day 2**

At 11:54 P.M. UTC on 10/17/2025, I reopened all of the programs and files and continued my investigation of the Mantooth.E01 image. Then at 12:17 A.M. UTC on 10/18/2025, I found flag #15, which is any other interesting evidence on the device. The first set of interesting things I was able to find is three .htm files, which were all related to drugs; a screenshot can be seen in Figure 21. Next, Figure 22 shows a password of some sort. This is not evidence of anything illegal, but it is still good information for us to know, just in case we come across anything password-protected. The last set of interesting things I was able to find is shown in Figure 23, which is a PowerPoint presentation and a document on ATM thefts and stealing credit card information. At 12:41 A.M. UTC, I concluded my investigation.

1. **Conclusion**
   1. **Story**

The story for this user is very interesting. I found lots of evidence that Wes Mantooth is involved in illegal activities, such as consuming, manufacturing, and or selling drugs, as well as stealing credit card information. I also found some evidence that suggests Wes Mantooth might be studying or planning to study Digital Forensics or Criminal Justice, for example, he had installed Exterro FTK imager, which is a common digital forensics tool used. Also, some of the websites he visited were from sccja.org, which is the South Carolina Criminal Justice Academy’s website. However, because of this user's messages to others as well as the fact that the user has his computer set to Mountain Standard Time, even though South Carolina is in Eastern Standard Time, the evidence suggests that Wes Mantooth is involved in these crimes.

* 1. **Timeline**

|  |  |  |
| --- | --- | --- |
| **Object** | **Open or Installed (UTC)** | **Significance** |
| Silicon Integrated Systems Corp. Super Flash 1GB / GXT 64MB Flash Drive | 2007-07-14 17:56.41 | This flash drive was plugged into the device and could have contained some of the evidence. |
| Google Images – “making meth” | 2007-7-13 03:17.08 | This is a search on Google Images for making meth. This is significant because making meth is illegal. |
| Google Images – “card stealing” | 2007-7-13 03:15.24 | This is a search on Google Images for stealing cards. This is significant because stealing cards is illegal. |
| sccja.org/images/csid\_meth1.jpg | 2007-7-13 03:17.02 | This link is to a website with images of meth. It is significant because meth is illegal. |
| Csid-methhand[1].jpg | 2007-7-12 23:17.01 | This is a picture of someone holding meth. It is significant because meth is an illegal drug. |
| FTK IMAGER.EXE | 2007-08-24 12:45.00 | The user has FTK Imager installed, meaning they have some familiarity with digital forensics tools. |

* 1. **Concluding Statement**

In conclusion, the forensic examination of the Mantooth.E01 image provided a clear and comprehensive image of the user's behavior and potential criminal involvement. Utilizing digital forensic tools such as Autopsy and Exterro FTK Imager, I was successful in discovering and verifying multiple pieces of evidence strongly pointing towards the involvement of the user, Wes Mantooth, in criminal activities involving drugs and credit card fraud. The existence of files, images, and browsing history related to methamphetamine production and ATM skimming confirms this conclusion. Further, the recovered deleted document entitled My Confession.txt and the installation of computer forensic software like FTK Imager indicate technical proficiency and probable intent to conceal or scrutinize incriminating evidence. The Mantooth.E01 file analysis was also a worthwhile experience at conducting methodical forensic analysis, verifying evidence integrity, authenticating hashes, submitting findings, and maintaining a thorough timeline of discovery. The case as a whole works to reinforce just how critical proper procedure is in digital investigation, especially when dealing with concealed data and tracing digital evidence back to real criminal activity. The evidence thus recovered would be admissible in court and demonstrates the value of digital forensics in today's investigations.