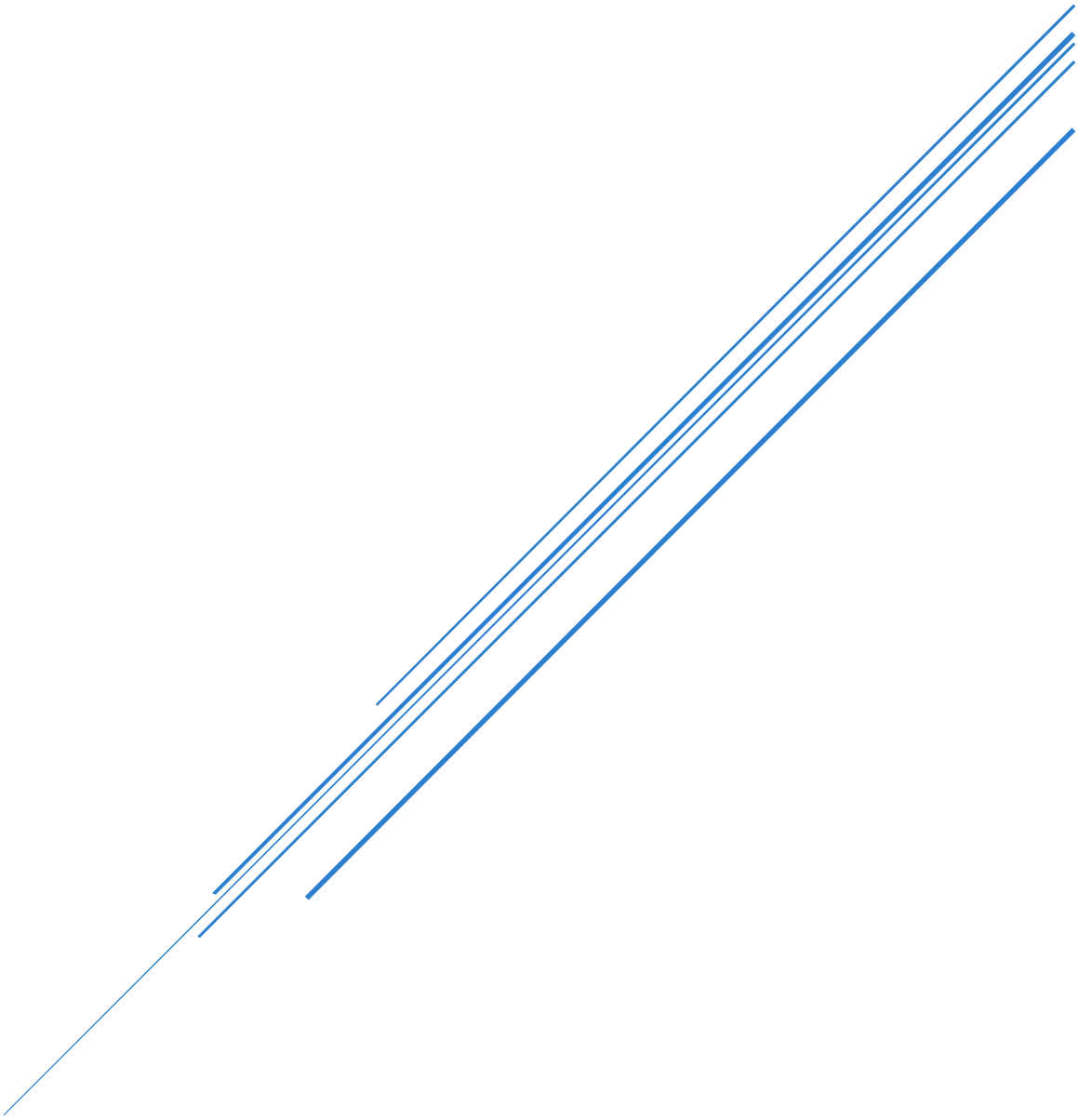
MANTOOTH REPORT

Report by Anthony Smithmyer

10/26/2025



Executive Summary

The main user on this Windows Vista computer is Wes Mantooth. This person is involved with various illegal activities such as check washing (which is the process of stealing checks and erasing details on the check with chemicals to be used by the criminal), ATM card skimming (which is the process of stealing bank account information digitally), and drug dealing, as shown through various emails, pictures, files, and Google searches on the computer. Wes has a more advanced understanding of computers because there are encrypted files on his computer, which means only people who know the password can view the file. These encrypted files are about stealing credit cards and dealing drugs to others. The computer is set to Mountain Time. There are deleted files on the computer that were recovered, some of which indicate involvement in suspicious activities. Other suspects may be accomplices of Wes Mantooth. They are known as John Washer, Mr. Smee, Rosco, and Skimmerman. His primary method of communicating with these people is through email.

Methods

Tools used:

- Autopsy 4.22.1 (The latest version)
- Windows Registry Explorer
- Windows Event Viewer
- PicPick Screenshot Tool
- Kali Linux

The process:

I downloaded the disk image of Precious's computer and started a new case in Autopsy 4.22.1. I selected the disk image as a data source. I began to look through the files on the image to find the essential flags. The flags are listed below:

1. Verify the MD5 hash of the image with the related Mantooth.E01.txt file.
2. User Account Discovery: What is the name of the main Windows user account?
3. User Account Discovery: What is the last login time of the main user?
4. Operating System Version: What operating system is installed?
5. Time Zone: What time zone is the computer set to?
6. USB Device History: Find one USB storage device that was connected to the computer and provide the make/model/serial number.
7. Browser History: Identify at least three websites the user has visited.
8. Browser History: Identify any suspicious search queries.
9. Email Attachments: Find at least one email attachment that the user sent.

10. Email Artifacts: Locate at least one email address used on the computer.
11. Pictures: Identify at least three images that could be meaningful.
12. Software: Identify at least three programs that are installed on the computer. Note
any suspicious applications and why.
13. Software: Identify any suspicious applications that the user has recently launched.
When were the applications last run?
14. Deleted Files: Identify and recover a deleted file.
15. Did you discover any other interesting evidence on the computer?

Verification:

I verified the flags and artifacts by using the built-in data artifacts section in Autopsy, finding the flags within the files on the disk image, and exploring the registry hives in Registry Explorer.

Findings

Before investigating the disk image for evidence of illegal activities, I found the first flag and verified the MD5 hash of the image to ensure that the image wasn't tampered with. The file hash listed in the Mantooth.E01.txt file is 31217210a1a69f272079a3bde3d9d8fc. Using Autopsy, I went to Data Sources > Mantooth.E01_1 Host and single-clicked on Mantooth.E01 in the right pane. The hash of the disk image is listed in the "File Metadata" section below. As shown in Figures 1 and 2, the file hash is the same.

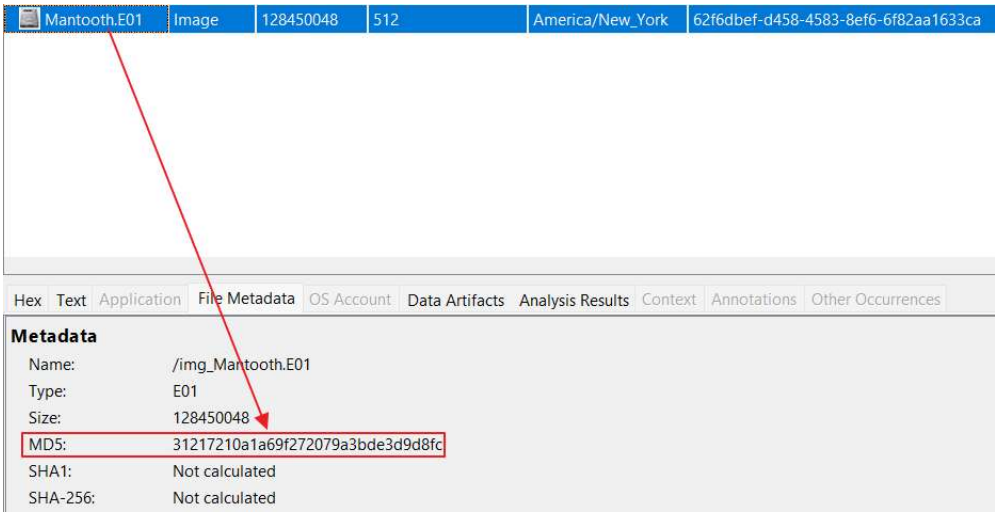


Figure 1: File hash of Mantooth.E01 in Autopsy

```
Information for C:\Documents and Settings\Ken\Desktop\ADSHARE\Mantooth32:

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
 Cylinders: 15
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 250,879
[Physical Drive Information]
 Drive Model: SanDisk Cruzer Mini USB Device
 Drive Interface Type: USB
 Source data size: 122 MB
 Sector count:    250879
[Computed Hashes]
 MD5 checksum:    31217210a1a69f272079a3bde3d9d8fc
 SHA1 checksum:   12e4ac047e328ca2bd63a4d65df25b3ecba55769
```

Figure 2: File hash of Mantooth.E01 in the associated text document

For the second flag, I discovered that Wes Mantooth is the main Windows user on this computer. This is because the Users folder for Wes Mantooth has the most subfolders and files compared to the other users on the computer, as shown in Figure 3. Additionally, the primary email address used on the computer, dollarhyde86@comcast.net belongs to Wes. This is shown below in Figure 4.

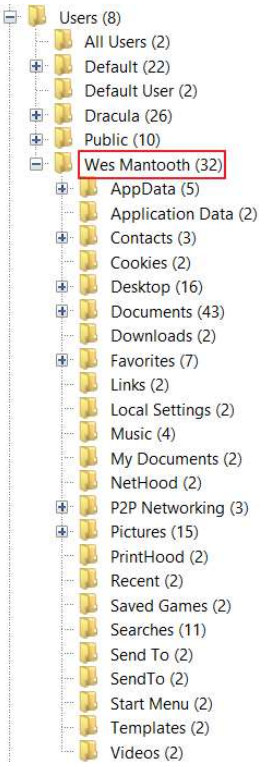


Figure 3: Wes Mantooth's Windows user folder

Data Source	E-Mail From	Date Received	Message (Plaintext)
Mantooth.E01	Outlook 2003 Team <olteam@microsoft.com>	2007-06-20 13:25:36 EDT	Thank you for using Microsoft® Office Outlook® 2003! .
Mantooth.E01	Rasco Badguy <txkidd@swbell.net>	2007-08-01 15:09:08 EDT	Guys, Been working on a letter that I think will get us so..
Mantooth.E01	Wes Mantooth <dollarhyde86@comcast.net>	2007-06-21 14:00:00 EDT	Sorry man. I have been a little under the weather lately.
Mantooth.E01	Wes Mantooth <dollarhyde86@comcast.net>	2007-06-21 17:06:00 EDT	Your crazy! You are going to blow your self up! I am sti
Mantooth.E01	Wes Mantooth <dollarhyde86@comcast.net>	2007-06-21 19:26:00 EDT	It works EXACTLY the same. I have been doing quit a bit

Figure 4: Wes Mantooth's email address shown in Autopsy

I discovered the third flag by looking at the security event logs found in System32. Using the Windows Event Viewer and filtering the log to only display login events, I found that Wes most recently logged onto the computer on 2/12/2008 at 3:11:02 PM. This is shown in Figure 5.

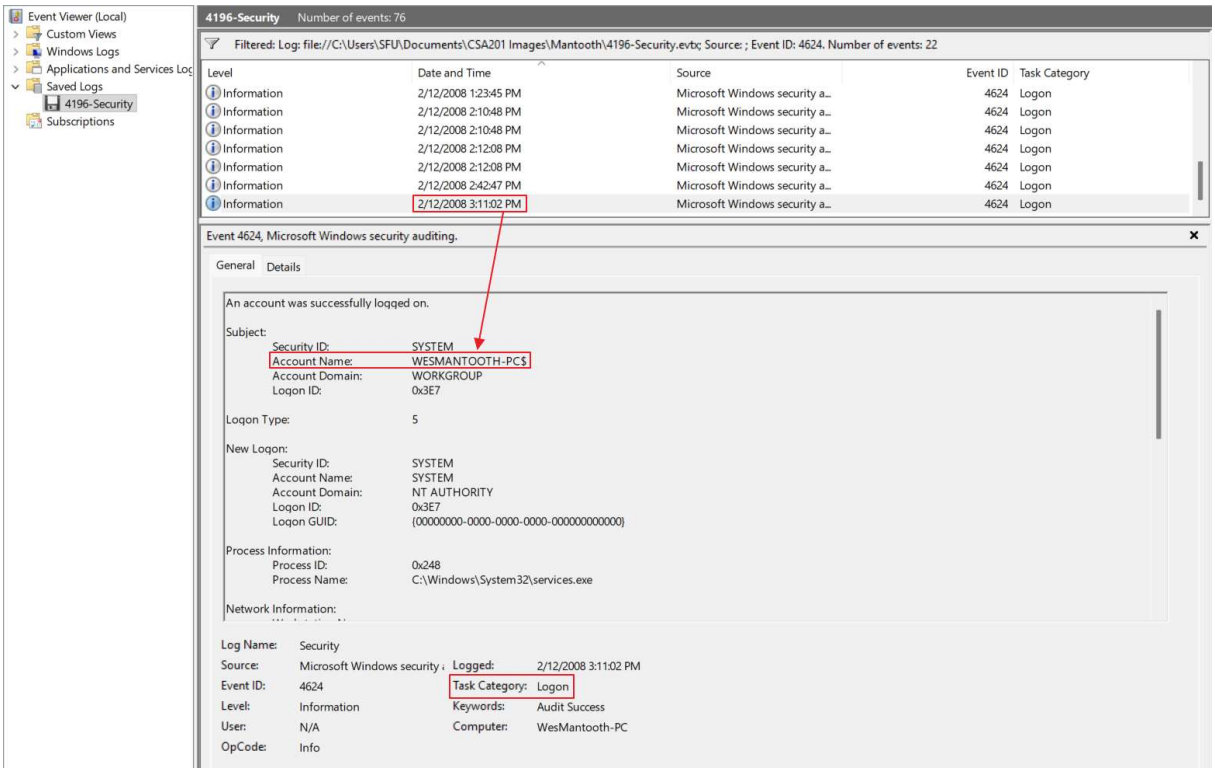


Figure 5: Wes Mantooth's most recent login

I found the fourth flag by looking at the Software hive in Windows Registry Explorer. By going to SOFTWARE\Microsoft\Windows NT\CurrentVersion, I discovered that Wes's computer is running Windows Vista Ultimate. This is shown below in Figure 6. Also note that the registered owner is listed as Wes Mantooth, which further proves that Wes is the main user on the computer.

RegisteredOwner	RegSz	Wes Mantooth
SystemRoot	RegSz	C:\Windows
ProductName	RegSz	Windows Vista (TM) Ultimate
ProductId	RegSz	89580-378-0753292-71704

Figure 6: Operating System version listed in Windows Registry Explorer

The fifth and sixth flags were found in the System hive in Windows Registry Explorer. For the fifth flag, I went to SYSTEM\CurrentControlSet\Control\TimeZoneInformation and saw that the computer was using Mountain Standard Time. This can be seen below in Figure 7.

Value Name	Value Data	Value Data Raw
Bias	420	420
StandardName	@tzres.dll,-192	@tzres.dll,-192
StandardBias	0	0
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-0B-00-01-00-02-00-00-00-00-00-00-00-00-00
DaylightName	@tzres.dll,-191	@tzres.dll,-191
DaylightBias	-60	4294967236
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-03-00-02-00-02-00-00-00-00-00-00-00-00-00
TimeZoneKeyName	Mountain Standard Time me	Mountain Standard Time me
ActiveTimeBias	360	360

Figure 7: Time zone information shown in Windows Registry Explorer

For the sixth flag, I went to SYSTEM\CurrentControlSet\Enum\USBSTOR and discovered a USB storage device that was plugged into the computer. This device was a SanDisk Cruzer Mini with the serial number SNDK4DB2A41B47901706. This information was also shown in Autopsy in the USB Device Attached tab. See Figures 8 and 9 for more information.

Value Name	Value Type	Data
DeviceDesc	RegSz	@disk.inf,%disk_devdesc%;Disk drive
Capabilities	RegDword	16
HardwareID	RegMultiSz	USBSTOR\DiskSanDisk_Cruzer_Mini__...
CompatibleIDs	RegMultiSz	USBSTOR\Disk USBSTOR\RAW
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002be1...
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002be1...
Class	RegSz	DiskDrive
Mfg	RegSz	@disk.inf,%genmanufacturer%;(Stan...
Service	RegSz	disk
ConfigFlags	RegDword	0
FriendlyName	RegSz	SanDisk Cruzer Mini USB Device

Figure 8: USB device in Registry Explorer

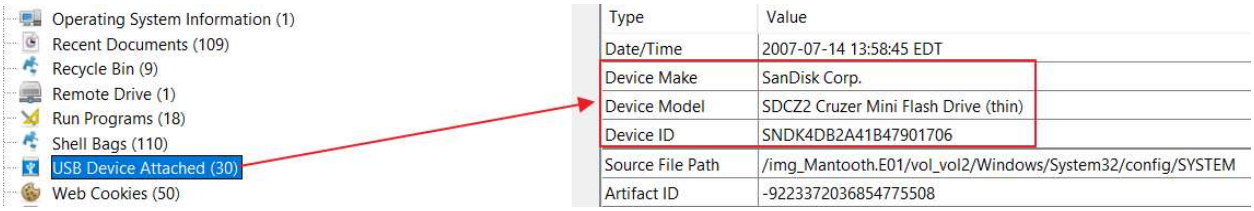


Figure 9: USB device in Autopsy

After finding the sixth flag, I began my search for the seventh flag. Using Autopsy, I went to Data Artifacts > Web History and found that Wes visited websites like http://67.19.222.106/crime/graphics/camera06.jpg, http://www.neonjoint.com/drug_recipes/chapter3.html, and http://www.herbalsmokeshops.com/images/herbs1-hawaiian-ruler.jpg. These websites indicate that Wes is involved in illegal activities like drug dealing, spying, and data stealing. While searching for the seventh flag, I also found the eighth flag. I discovered that Wes Mantooth searched for check washing, making meth, and atm card stealing on Google, which also indicates his interest in illegal activities. This is shown below in Figure 10.

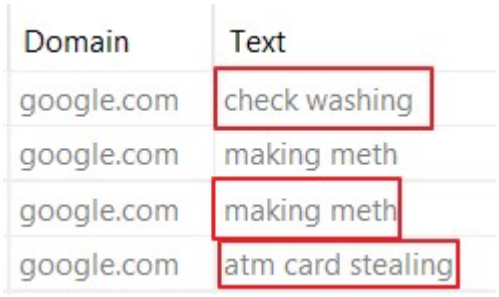


Figure 10: Suspicious search queries conducted by Wes Mantooth

I discovered the ninth and tenth flags while looking through the E-Mail Messages and the Communication Accounts tabs in Autopsy. Wes Mantooth sent an email that included a picture of his face. This is shown below in Figure 11. As for the tenth flag, recall that Figure 4

shows Wes's email address, dollarhyde86@comcast.net in Autopsy.

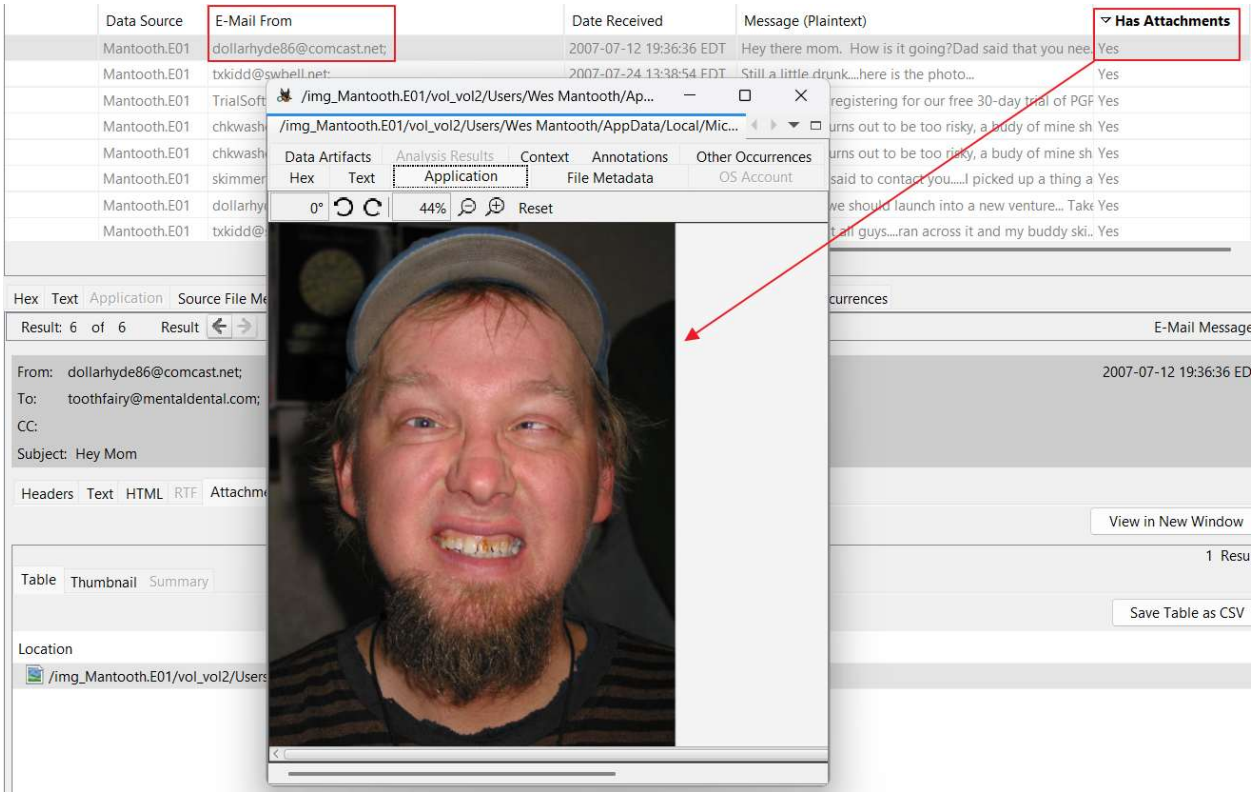


Figure 11: An email sent by Wes that includes a picture of his face attached

I searched for the eleventh flag by looking through the images on Wes Mantooth's computer in the File Views > File Types > By MIME Type > image tab in Autopsy. I found a picture called "Cover Plate.bmp", which shows a person installing a skimmer on an ATM. I also found an image called "Check1.png", which depicts a check that may have been stolen or washed. Additionally, I discovered an image called "meth_lab_small[1].jpg", which is a very blurry image of a meth lab. These pictures indicate Wes's involvement in illegal activities such as bank card theft, drug dealing, and check washing. These pictures

are shown below in Figures 12-14.

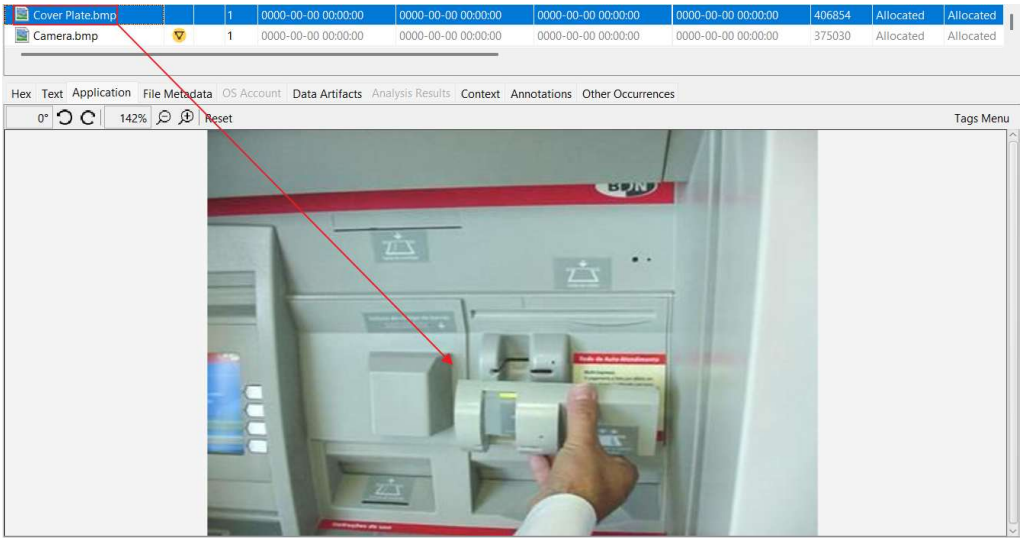


Figure 12: Picture of an ATM card skimmer

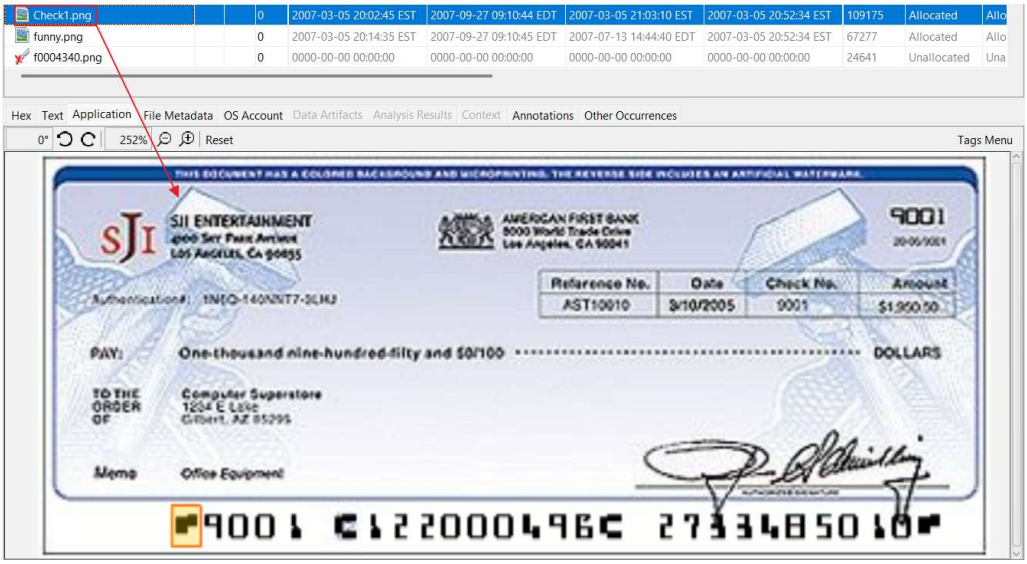


Figure 13: Picture of a check that may have been washed

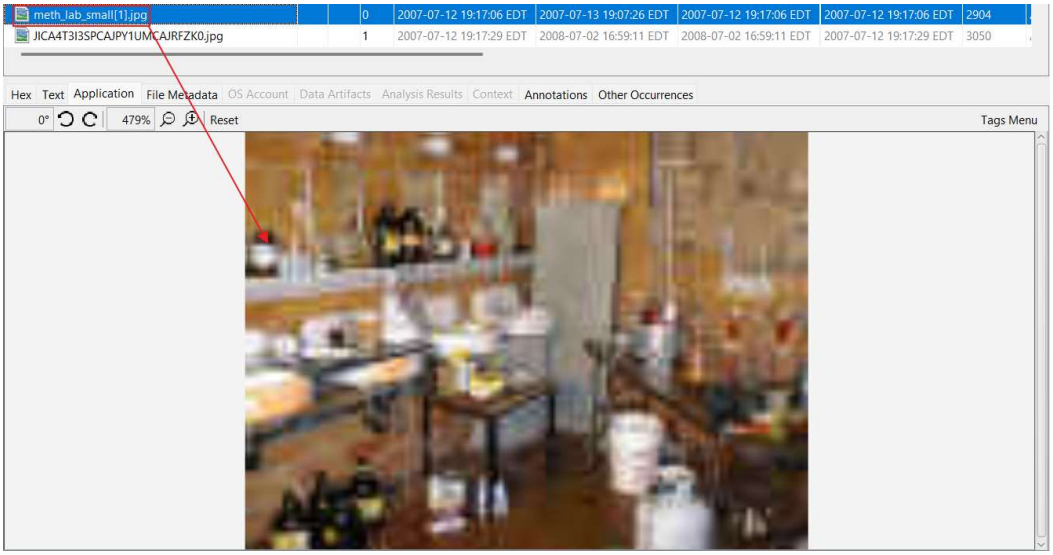


Figure 14: Picture of a meth lab

I discovered the twelfth flag shortly after finding the eleventh flag. I saw that TrueCrypt, FTK Imager, and Trillian were installed on the computer. TrueCrypt could have been used to encrypt files on Wes's computer. FTK Imager could have been used to understand how disk imaging works. Trillian, which is a messaging app, could have been used to talk with others. These apps are shown below in Figure 15.

Installed Programs

Table | Thumbnail | Summary

Source Name	S	C	O	Program Name
SOFTWARE			0	AccessData DNA 3 Worker v.3.3
SOFTWARE			0	AccessData Registry Viewer v.1.5
SOFTWARE			1	QuickTime
SOFTWARE			0	Adobe Reader 8 v.8.0.0
SOFTWARE			0	VNC Free Edition 4.1.2 v.4.1.2
SOFTWARE			0	TrueCrypt
SOFTWARE			0	Mozilla Firefox (2.0.0.3) v.2.0.0.3 (en-US)
SOFTWARE			0	AccessData FTK Imager v.2.5.1
SOFTWARE			1	Trillian

Figure 15: Programs installed on Wes Mantooth's computer

There was also a program called "junction.exe" on Wes Mantooth's desktop. This executable allows the user to create junction points, which allow alternate paths for a

directory to be accessed. This can be used for malicious intent, but it also shows Wes is a slightly more advanced computer user. This file is shown below in Figure 16.

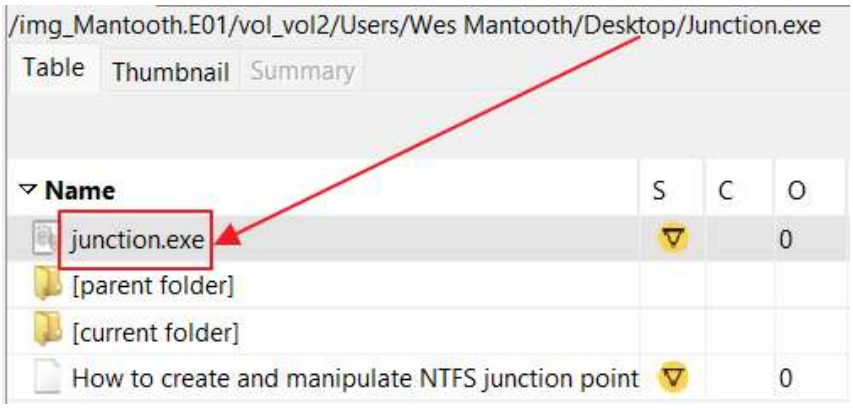


Figure 16: junction.exe file on Wes Mantooth's computer

I found the thirteenth flag by going to NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs in Windows Registry Explorer. I discovered that Wes opened the junction.exe program shown in Figure 16 on 8/24/2007 at 13:06:48.

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	88	Juncion.exe	Juncion.exe.lnk	31		
RecentDocs	89	Junction v1_04.mht	Junction v1_04.mht.lnk	32		2007-08-24 13:06:48

Figure 17: junction.exe file last opened timestamp

For the fourteenth flag, I went to File Views > Deleted Files > All (276) and found a deleted file called “My Confession.txt”. I was able to recover the text document, which says “This is my confession. I am a scum of the earth. I rob from the rich… and the poor too! I taketh away… and keepeth! I did it all… I am guilty Oh, by the way, I am deleting this so you will never find it! :)” This indicates that Wes knows he is guilty of his crimes but tried to hide it by deleting the file. However, the file was not overwritten, so it was easily recovered in Autopsy. This can be seen below in Figure 18. I also looked through the recycle bin on the computer and found an executable file called “CameraShy.exe” inside, as shown in Figure 19. I took the file hash and went to virustotal.com to see if the executable file was malicious. The file came back as malicious according to 25 out of 72 security vendors. It is also classified as a hacktool and a trojan. This is shown in Figure 20.

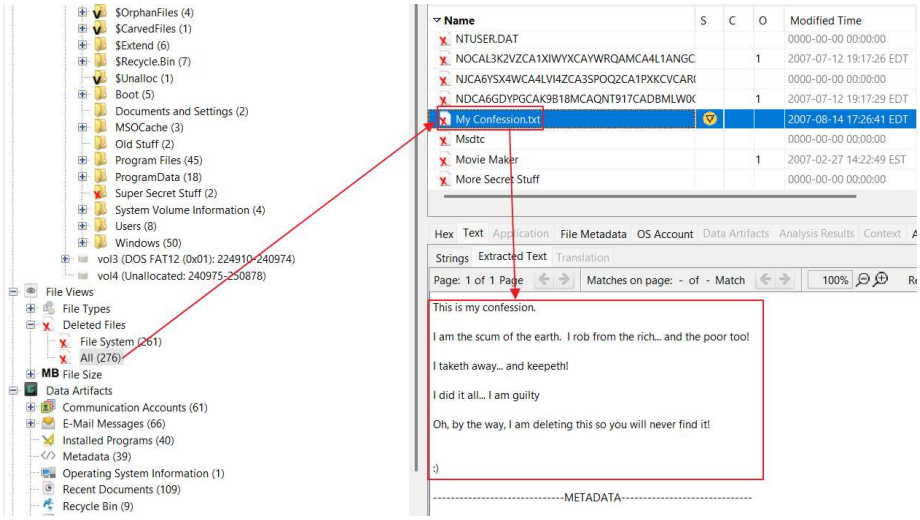


Figure 18: Deleted file containing Wes Mantooth's confession recovered in Autopsy

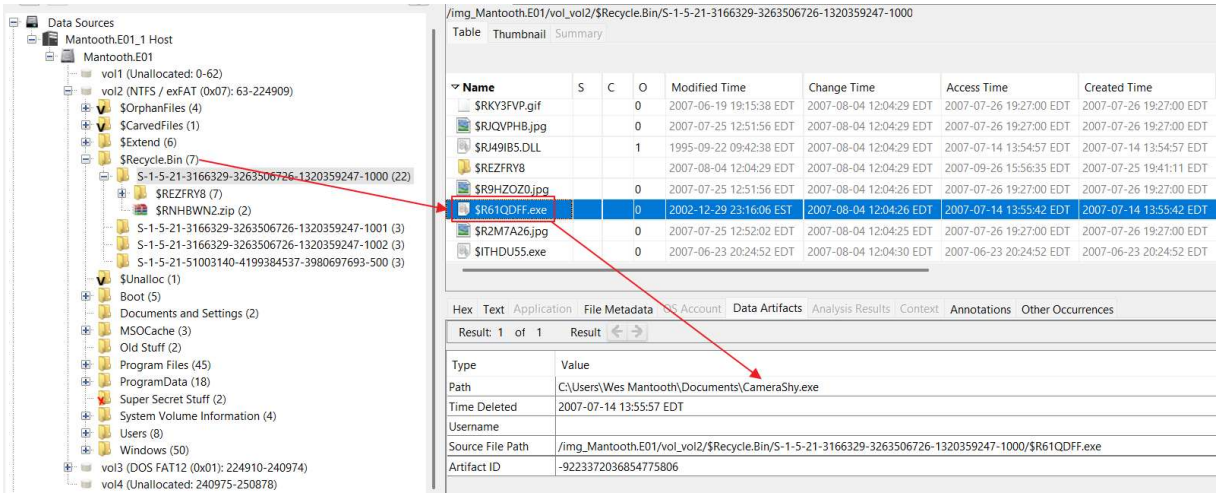


Figure 19: Possible malicious file inside the recycle bin

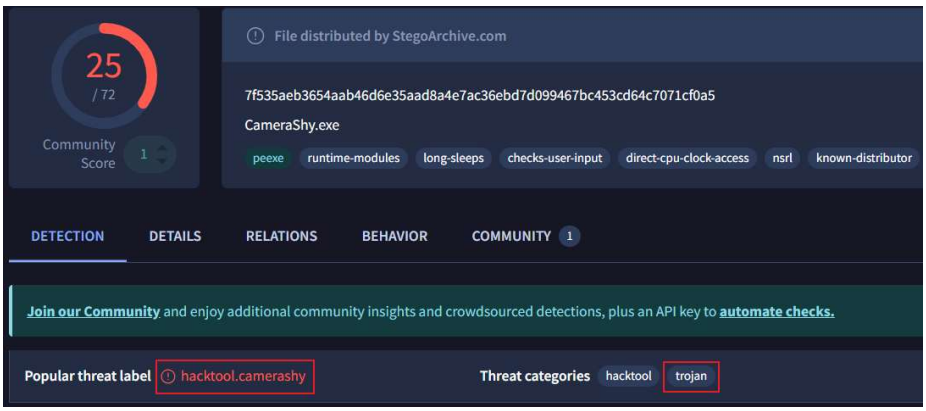


Figure 20: Malicious file results in virustotal.com

Finally, for the fifteenth flag, I discovered several interesting evidence on Wes Mantooth's computer. This includes a PowerPoint about installing ATM skimmers, a html with steps to make meth, an Excel spreadsheet with client names, drugs, and prices, and an email to Wes Mantooth and John Washer about other possible suspects getting caught by the police. John Washer (chkwasher@comcast.net) and Rosco (txkidd@swbell.net) are two of Wes Mantooth's accomplices. His other accomplices are known as Mr. Smee (smee.rox@gmail.com) and Skimmerman (skimmerman27@hotmail.com). These all indicate Wes's involvement with illegal activities. This is shown below in Figures 21-24. Note that in Figure 24, the news report states victims had spyware installed on their computers. The spyware involved could be the CameraShy.exe file that was in Wes's recycle bin, meaning he could have distributed it to the victims and deleted it to try to hide the evidence. There were also two encrypted files on the computer. One is a Word document about how to steal credit card numbers, and the other is an Excel spreadsheet about people who owe money to Wes. The Word document's password was unable to be cracked in Kali Linux, but the Excel spreadsheet's password was cracked. Its password is "smack", and the spreadsheet is the same as the one shown in Figure 23. See Figures 25 and 26 for more details about password cracking with John the Ripper. I also noticed that Wes cleared the security log at 11:35:01 AM on 2/12/2008, meaning that all prior data in the security log was deleted in an attempt to hide evidence and clear his tracks. This is shown in Figure 27.

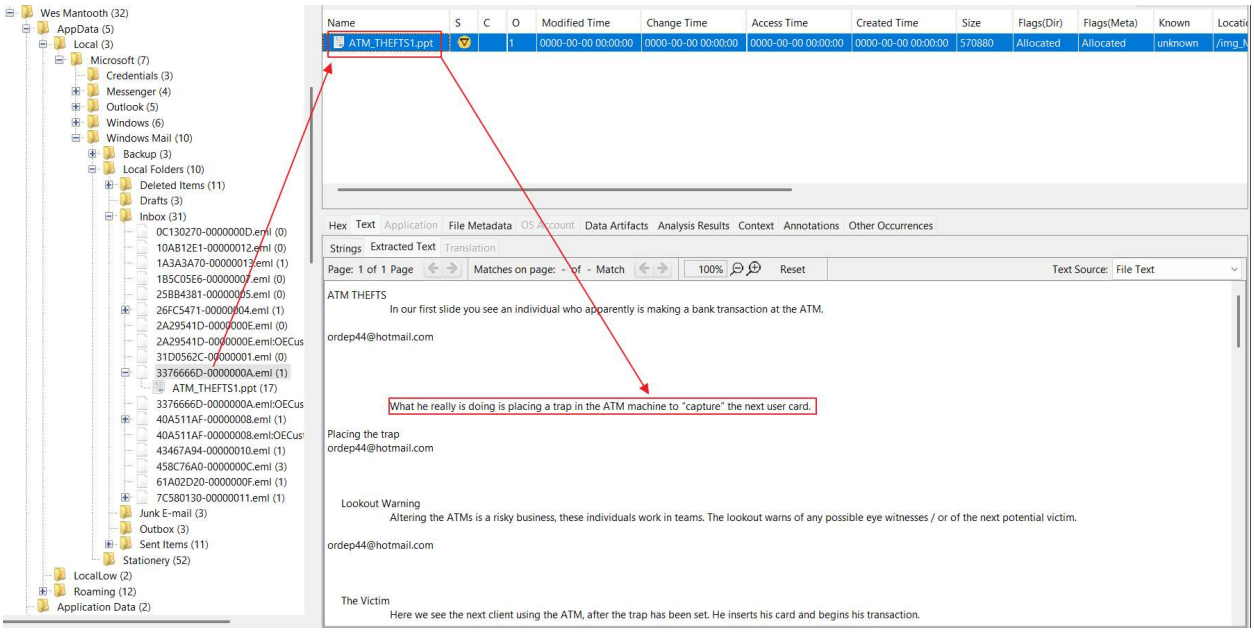


Figure 21: Email with a PowerPoint attached showing how to install ATM skimmers

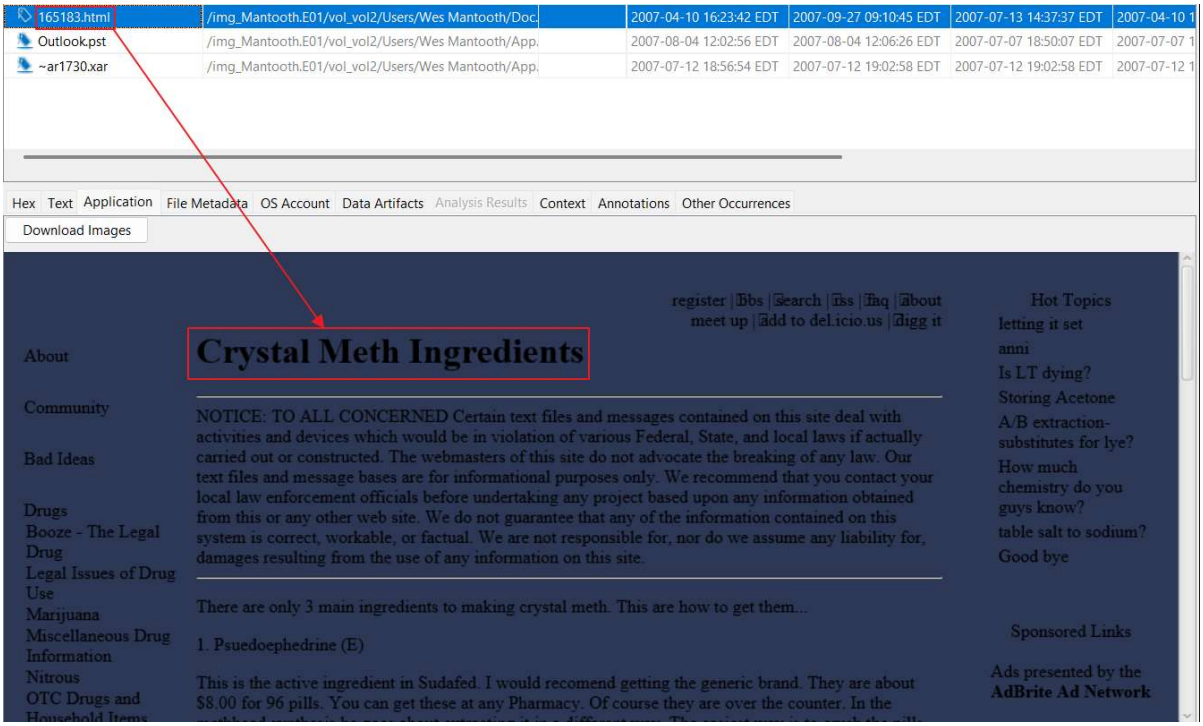


Figure 22: html file with the steps to make crystal meth

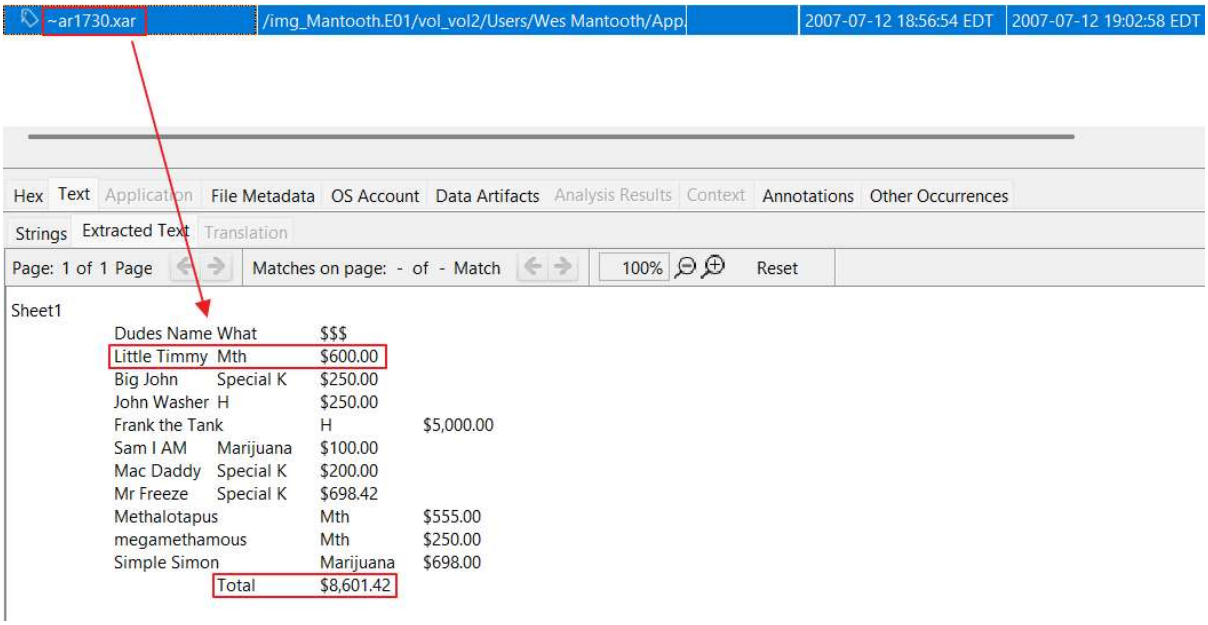


Figure 23: Excel spreadsheet with client names, drugs, and prices

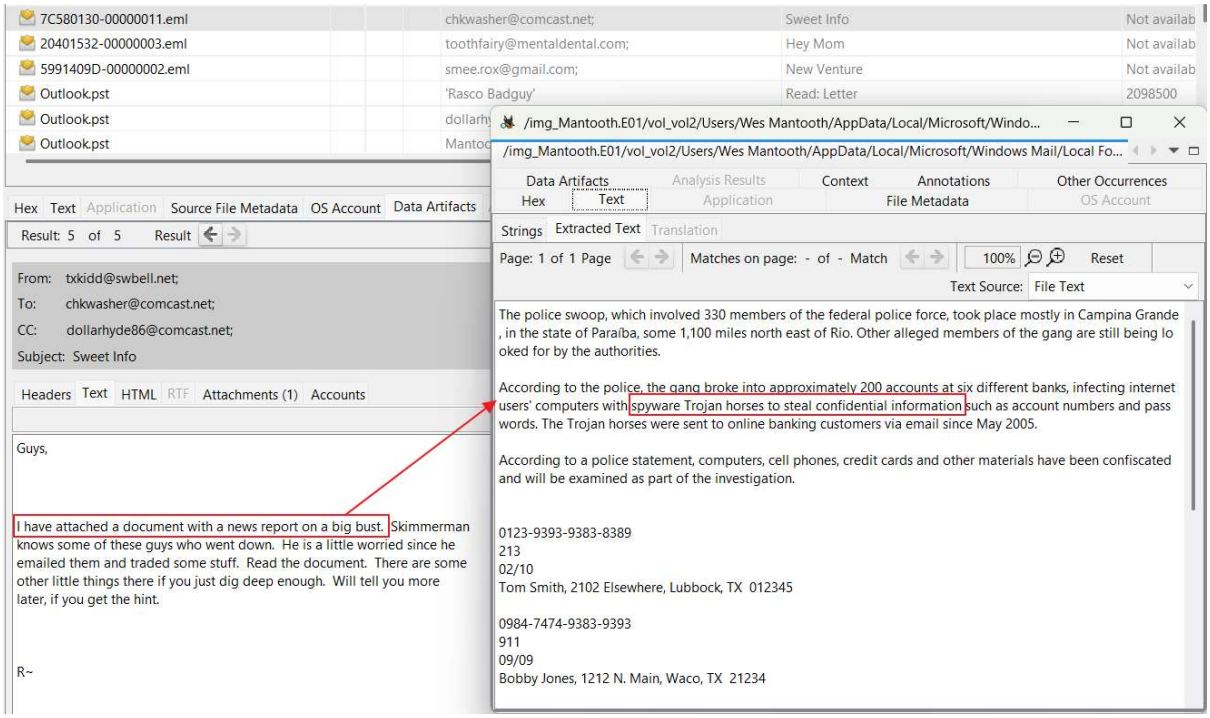


Figure 24: Email to Wes and John, an accomplice, about a bust involving other members of the crime group

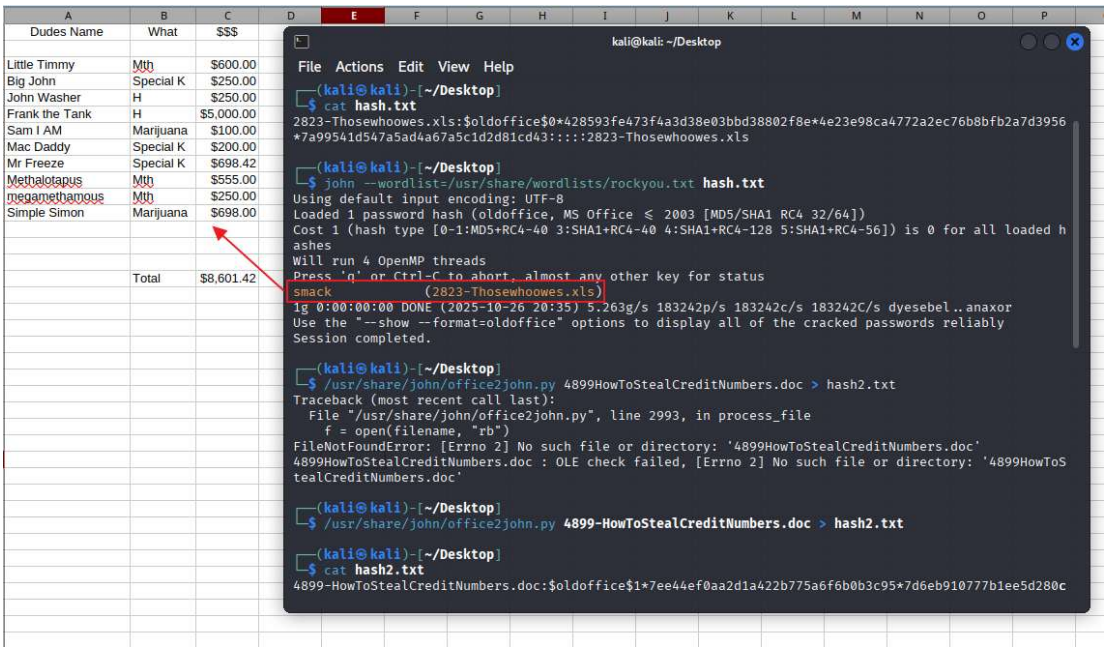


Figure 25: Cracked password for the Excel spreadsheet in Kali

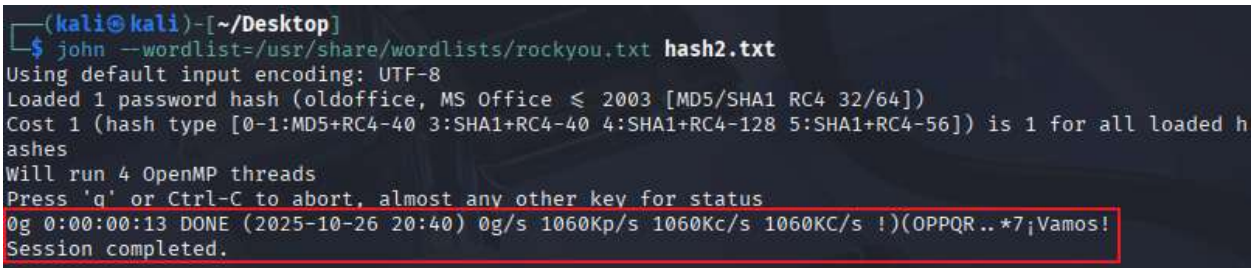


Figure 26: Unable to crack the password for the Word document in Kali

Figure 27: Cleared log event in the Windows Event Viewer

Timeline

Date/Time	Event	Relevance
7/11/2007 14:27:15 MDT	Wes receives an email from John Washer about how to install and use ATM skimmers	Indicates involvement with illegal activities.
7/12/2007 17:01:16 MDT	Wes creates the encrypted "Those who owes.xls" file	Shows higher expertise in computers, as well as possible evidence for drug dealing
7/12/2007 21:15:34 MDT	Wes searched for "atm card stealing" on the Internet	Shows interest in suspicious activities like card skimming
7/12/2007 21:15:52 MDT	Wes visited www.neonjoint.com, which is a drug site	Shows interest in drug dealing
7/12/2007 21:16:32 MDT	Wes searched for "making meth" on the Internet	Further indicates interest in drug dealing
7/14/2007 11:55:57 MDT	CameraShy.exe was moved to the recycle bin	Indicates attempted deletion of evidence
7/14/2007 11:58:45 MDT	USB storage device was inserted into the computer	Indicates possible transfer of data between the computer and the USB device
7/24/2007 9:39:54 MDT	Wes receives an email from Rosco about other accomplices getting busted	Shows involvement with other possible suspects
2/12/2008 11:35:01 MDT	Security log was cleared	Indicates an attempt to hide evidence

2/12/2008 15:11:02 MDT	Event logs indicate a successful login attempt	Wes Mantooth logged onto his computer
8/24/2008 13:06:48 MDT	Wes ran junction.exe	Indicates creation of a junction point, possibly for malicious intent

Conclusions

The main user on this Windows Vista computer is Wes Mantooth. This person is involved with various illegal activities such as check washing, ATM card skimming, and drug dealing, as shown through various emails, pictures, files, and search queries on the computer. Wes has a more advanced understanding of computers because there are encrypted files on his computer, which means only people who know the password can view the file. Cracking the passwords allows investigators to view the files. These encrypted files are about stealing credit cards and dealing drugs to others. The computer is set to Mountain Time. There are deleted files on the computer that were recovered, some of which indicate involvement in suspicious activities, such as a confession to committing crimes and a malicious executable file. Other individuals may be involved with Wes Mantooth's crimes. They are known as John Washer, Mr. Smee, Rosco, and Skimmerman, as shown through emails, which is Wes's primary method of communication.