Czyryca Corp

Wes Mantooth vs The State

October 21, 2022
Prepared by: Aidan Czyryca
Czyryca Corp
400 E 2nd St, Bloomsburg
PA 17815

Table of Contents

Case Background

Defendant Wes Mantooth was pulled over by a local police officer during a recent traffic stop and was questioned by the officer. During the questioning, Mantooth began to act unusual and the police officer requested to search Mantooth's vehicle. After getting consent to the search, the police officer found a small amount of marijuana along with a thumb drive in Mantooth's clothing. After the traffic stop, police officers also siezed a computer taken from the home of Wes Mantooth. Along with this possesion of marijuana, Mantooth has had other previous incidents with the police.

The state police department has received permission to examine both the hard drive found in Mantooth's home computer and the thumb drive found in his vehicle. The state police's forensic lab cannot currently take this case so forensic examiner Aidan Czyryca has been hired to do the examination on behalf of the state police department. Copies of the forensic images of both the hard drive from Mantooth's home computer and the thumb drive from his vehicle has been turned over to forensic examiner Aidan Czyryca. The judge is expecting a full report on any illegal activity found on both of these pieces of evidence.

Shortly after handing the evidence to the forensic examiner, the initial findings led to the search of any potential accomplices of Wes Mantooth in this case. John Washer was found to be connected to Mantooth's illegal activity in the preliminary report and was questioned by police officers in his residence. Police officers were able to get permission to sieze a computer in Washer's possession and proceeded to send a copy of the forensic image of the computer's hard drive to the forensic examiner. With this new evidence, the judge is now expecting an analysis of the hard drive found in the computer in Washer's possession and anything that ties the two men together in illegal activity.

Executive Summary

In this examination, I believe that the forensic images provided for analysis contain sufficient information to strongly support that Wes Mantooth was involved in criminal activity, John Washer was involved in criminal activity, and that the two men were accomplices in the shared illegal actions of drug possession, drug creation, and credit card fraud.

In the investigation of Wes Mantooth's forensic images, there is strong evidence to support the claims that he participated in:

- Drug Possession
  - Personal documents recorded the sale of illegal drugs through a personal excel database that recorded the business of selling the drugs. Emails belonging to accounts in his control recorded the possession of illegal drugs.
  - Personally gathering prescription drugs using pre-signed and unused doctor's prescription notes which was revealed through personal images about the prescription notes and emails about the collection of the drugs.
  - Creation of illegal drugs which was revealed by a document found in his user profile and an admission that he was creating drugs in an email to an accomplice.
- Financial Fraud
  - Possession of stolen credit cards and all accompanying information found in an excel file located in the user profile of Mantooth.
  - Gathering of stolen credit cards through the use of card skimmers on ATM machines as revealed by images found in Mantooth's user profile.
  - Preparation for check washing as revealed by many images of checks and calendar reminders set found in Mantooth's user profile showing the intent to wash checks.
  - Gathered car titles in other people's names as revealed by images of whole car titles found in Mantooth's user profile.
  - Confession that plead guilty to theft found as a deleted text file that was

recovered from Mantooth's user profile.

The records used to determine suspicion of these illegal activities are reasonably thought to belong to Wes Mantooth due to files being on his person at the time of his arrest were also found on the Wes Mantooth user profile on his computer. Wes Mantooth would to have access to the account called Wes Mantooth and subsequently the files used to support the claims.

In the investigation of John Washer's forensic images, there is enough evidence to support the claims that he participated in:

- Drug Possession
    - Purchase for illegal drugs as found in Mantooth's excel database of his illegal business operations. This is in turn supported by: An email with Washer from a third part suggesting a trade in illegal substances, and a personal file documenting an invitation from Mantooth to create illegal drugs.
- Financial Fraud
    - Owning and viewing a guide on how to steal credit card numbers which was found in the user account linked to Washer's illegal activities.
    - Owning and viewing a guide on printing credit cards that was found in the user account linked to Washer.
    - Showing intent to do these actions by owning software that activates credit cards and by writing the intention to confess to the police.

The files used in this were determined to be under Washer's possession because they were either shared between Mantooth and himself, under the password protected administrator account of his own office computer, or connected to an email that is supported to be under Washer's control.

Lastly, the two suspects were certainly knowledgable of and supported each other's illegal activities due to a large number of emails between the two from email addresses under their control, reasonable suspicion of in-person contact during illegal activity, and shared matching files pertaining to illegal activity.

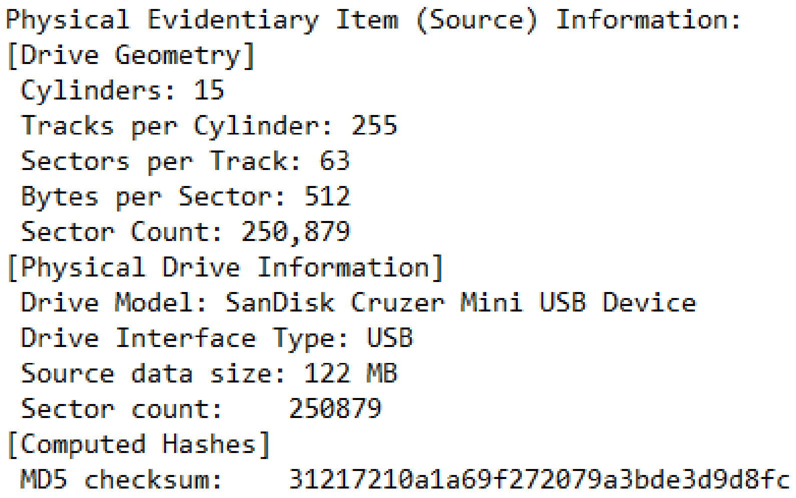
Examiner Credentials

The forensic examiner hired by the state police department to analyze the evidence in this case is Aidan Czyryca. Aidan Czyryca recently graduated from Bloomsburg University of Pennsylvania with a Bachelor of Science in Digital Forensics and Cybersecurity in the Spring of 2022. He is now employed at Czyryca Corporation as a Junior Analyst as of June 2022. Aidan Czyryca has been handling cases of personal lawsuits and of the local and state police departments for Czyryca Corporation. The examiner has been trained to be able to collect and handle evidence, conduct forensic examinations, prepare comprehensive reports, and give expert testimony through the company and his education.

Scope

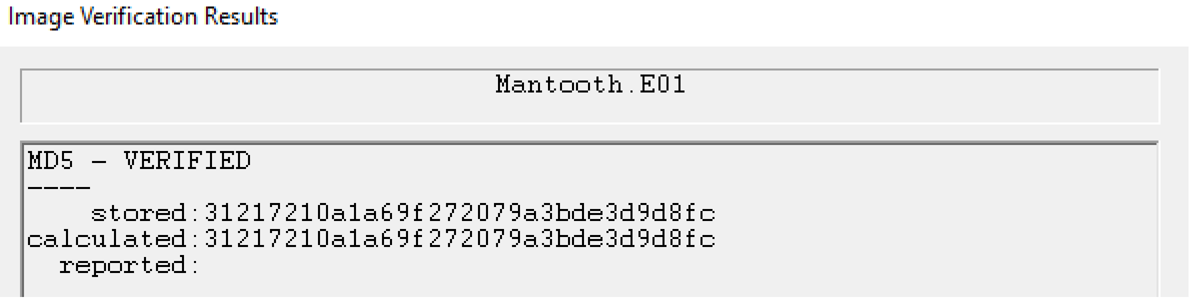
The forensic examiner has been tasked to provide all evidence of illegal activity on the forensic images provided and any evidence linking John Washer and Wes Mantooth as accomplices in illegal activity.

Forensic image “Mantooth.E01” is of Wes Mantooth’s hard drive found inside of his home computer.



```
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
```

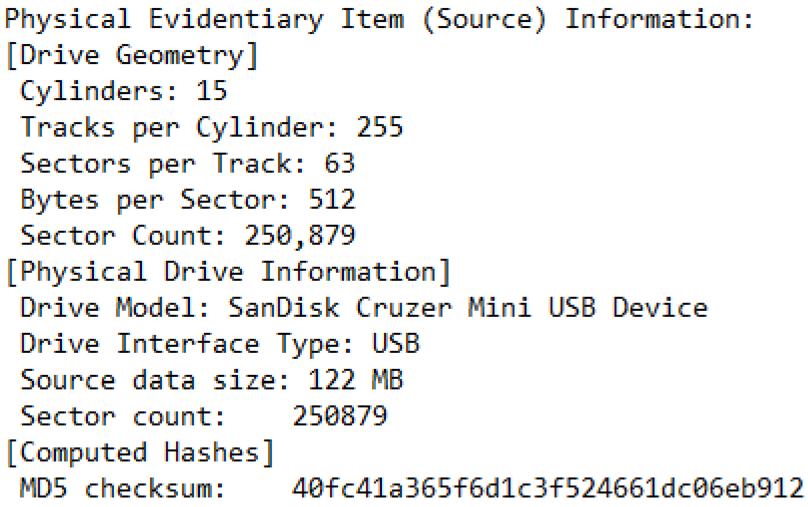
Figure 1: Image of the properties of the physical hard drive[Mantooth.E01] in Mantooth's home computer.



```
Image Verification Results

Mantooth.E01

MD5 - VERIFIED
----
    stored:31217210a1a69f272079a3bde3d9d8fc
calculated:31217210a1a69f272079a3bde3d9d8fc
  reported:
```

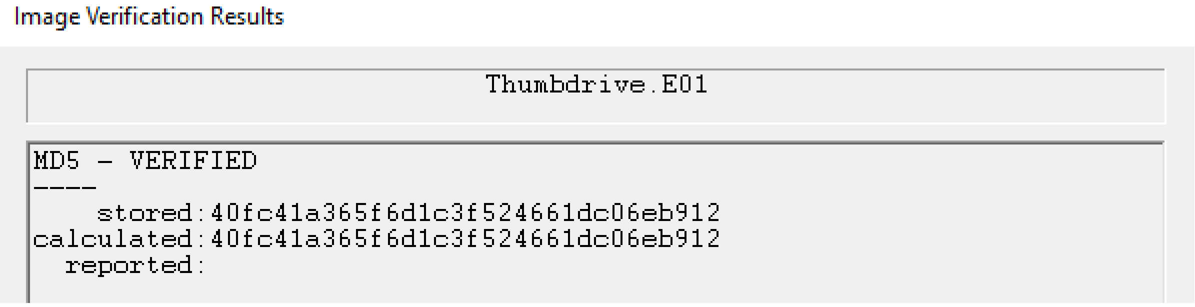
Figure 2: Image verifying that the image received is the same as the image being examined.

Forensic image “Thumbdrive.E01” is of Wes Mantooth’s thumb drive found on his person during the traffic stop.



```
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:    40fc41a365f6d1c3f524661dc06eb912
```

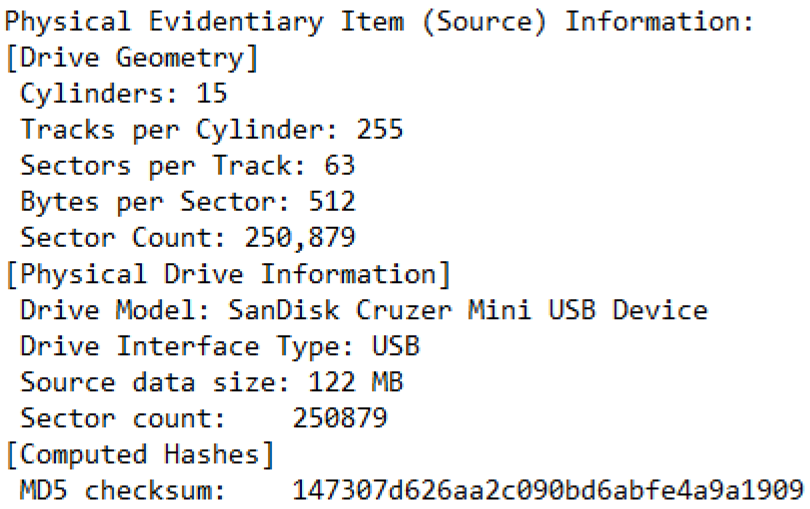
Figure 3: Image of the properties of the physical thumb drive[Thumbdrive.E01] in Mantooth's person during the traffic stop.



```
Image Verification Results

Thumbdrive.E01

MD5 - VERIFIED
----
    stored:40fc41a365f6d1c3f524661dc06eb912
calculated:40fc41a365f6d1c3f524661dc06eb912
  reported:
```

Figure 4: Image verifying that the image received is the same as the image being examined.

Forensic image “Washer.E01” is of John Washer’s hard drive found in a computer found in Washer’s residence.



```
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:    147307d626aa2c090bd6abfe4a9a1909
```

Figure 5: Image of the properties of the physical hard drive[Washer.E01] found in a computer in Washer's residence.

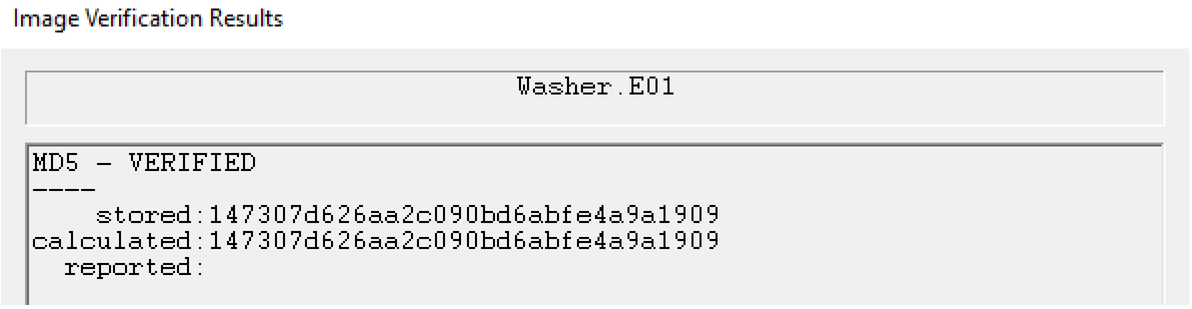


Image Verification Results

Washer.E01

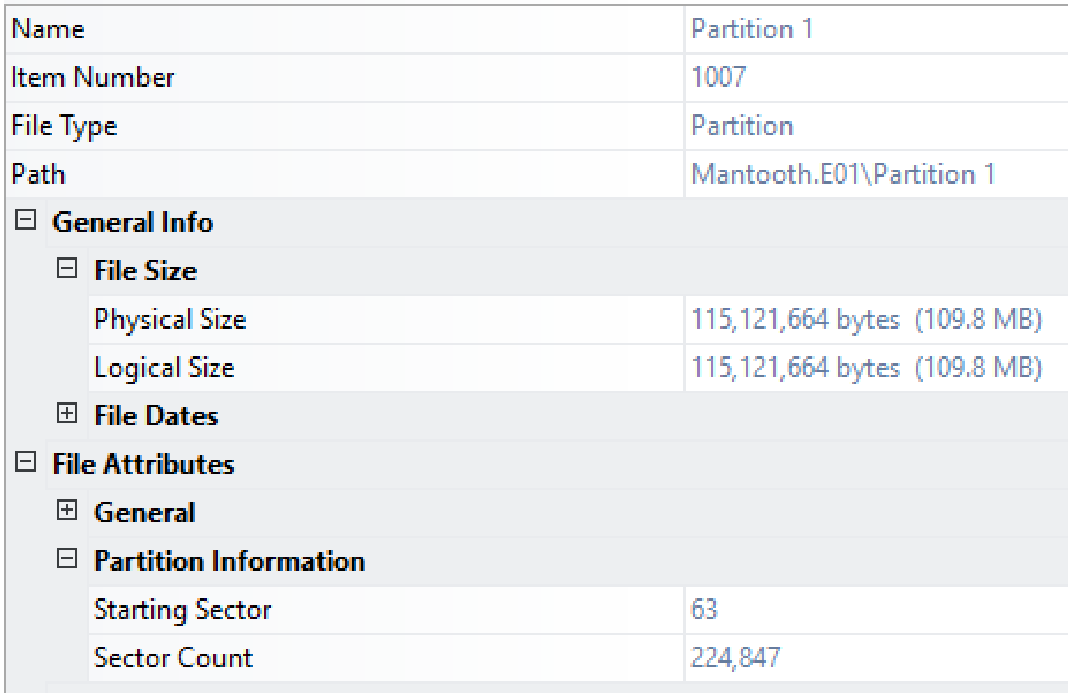
```
MD5 - VERIFIED
----
    stored:147307d626aa2c090bd6abfe4a9a1909
calculated:147307d626aa2c090bd6abfe4a9a1909
  reported:
```

Figure 6: Image verifying that the image received is the same as the image being examined.

Basic Computer Information

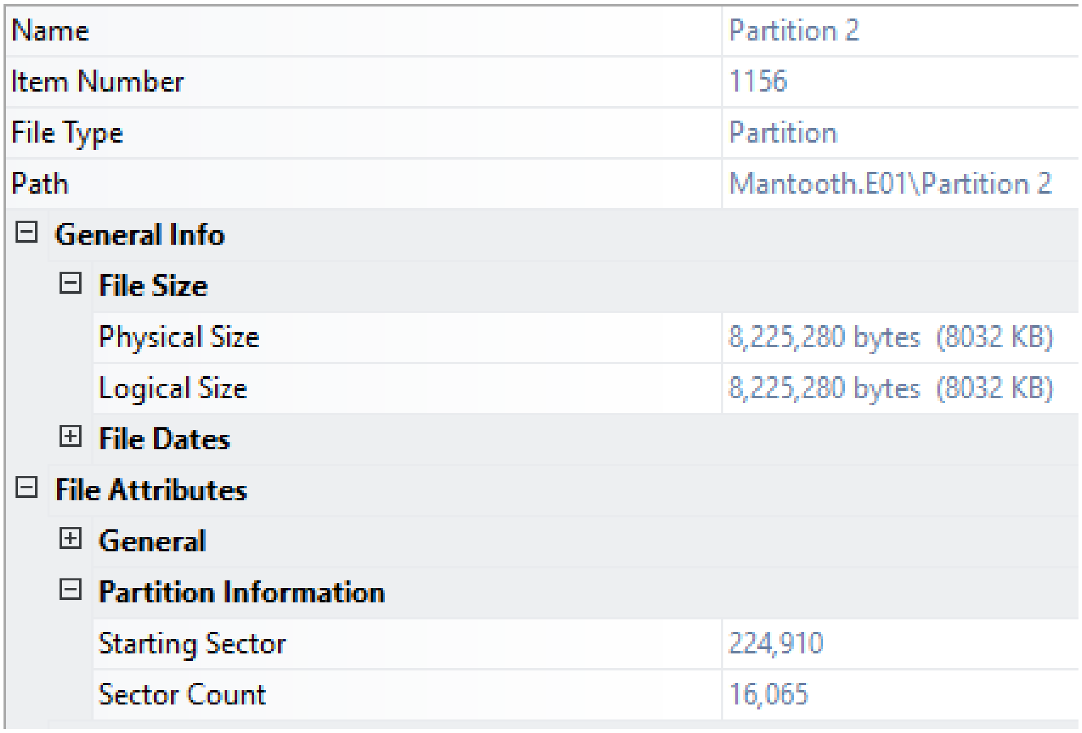
Mantooth Hard Drive

Mantooth's Hard Drive contains two partitions. The first partition uses the majority of the space on the drive and contains the Windows Vista operating system. The second partition is a small storage partition containing personal images and documents. There are also 4983 kilobytes of unallocated space which is all empty. The image of this drive was acquired on September 2nd, 2008.



Name	Partition 1
Item Number	1007
File Type	Partition
Path	Mantooth.E01\Partition 1
⊟ **General Info**	
⊟ **File Size**	
Physical Size	115,121,664 bytes (109.8 MB)
Logical Size	115,121,664 bytes (109.8 MB)
⊞ **File Dates**	
⊟ **File Attributes**	
⊞ **General**	
⊟ **Partition Information**	
Starting Sector	63
Sector Count	224,847

Figure 7: Image contains information about the first partition.

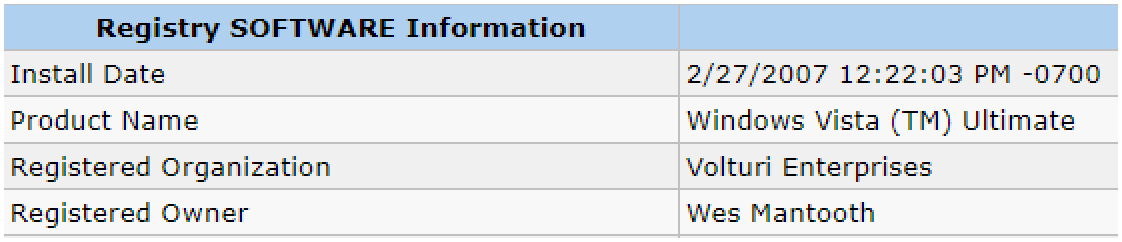


Name	Partition 2
Item Number	1156
File Type	Partition
Path	Mantooth.E01\Partition 2
⊟ **General Info**	
⊟ **File Size**	
Physical Size	8,225,280 bytes (8032 KB)
Logical Size	8,225,280 bytes (8032 KB)
⊞ **File Dates**	
⊟ **File Attributes**	
⊞ **General**	
⊟ **Partition Information**	
Starting Sector	224,910
Sector Count	16,065

Figure 8: Image contains information about the second partition.

Windows Vista Partition

The first partition is solely occupied by the Windows Vista operating system and is registered under Wes Mantooth's name. The file system for the operating system is NTFS. This information is found in the registry file named SOFTWARE found at "Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Windows/System32/config/SOFTWARE".

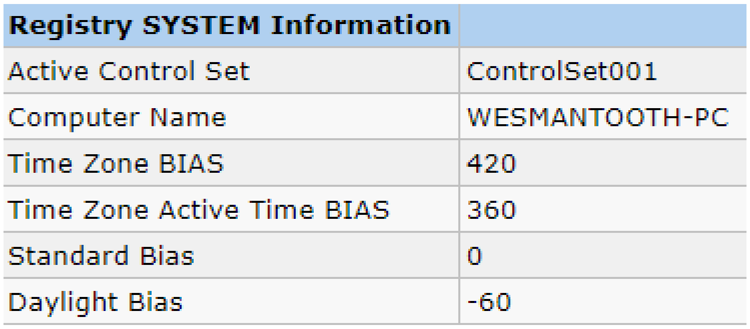


Registry SOFTWARE Information	
Install Date	2/27/2007 12:22:03 PM -0700
Product Name	Windows Vista (TM) Ultimate
Registered Organization	Volturi Enterprises
Registered Owner	Wes Mantooth

Figure 9: Image of the information provided by the SOFTWARE registry file.

Within the operating system, the computer is named WESMANTOOTH-PC and runs on the time zone of Mountain Standard Time with daylight savings. This information can be found in the SYSTEM registry file found at "Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\

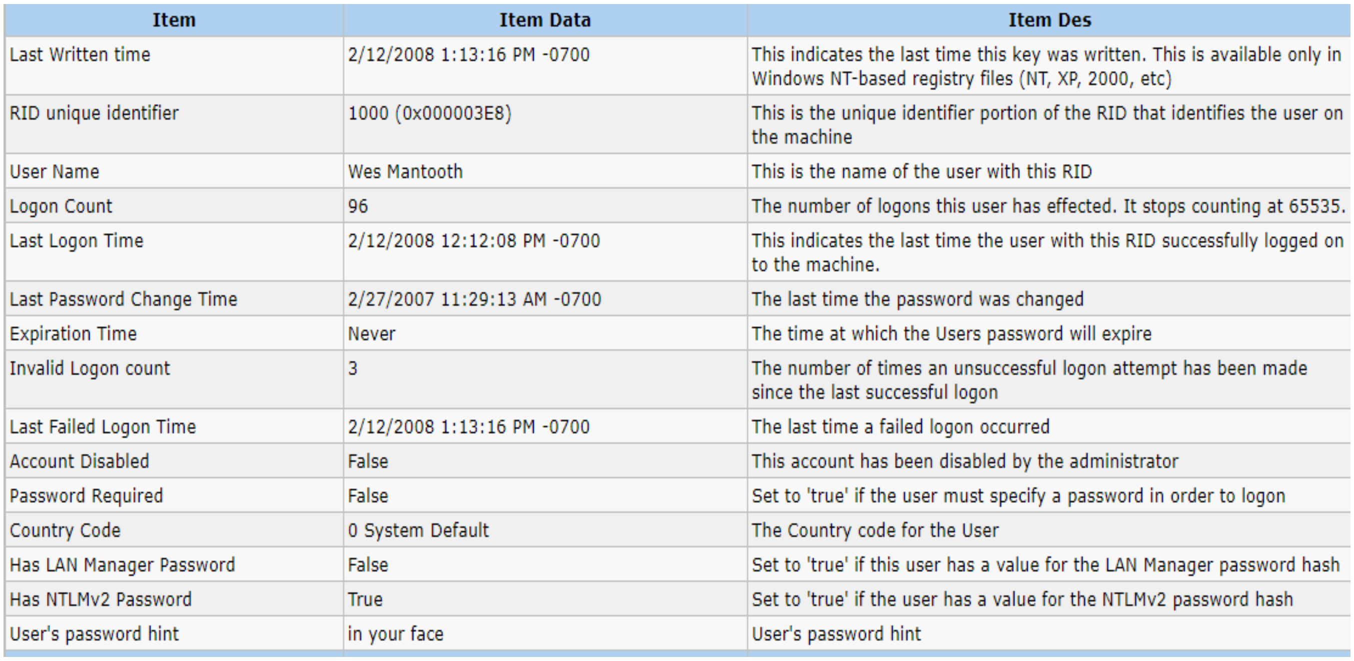
Windows\System32\config\SYSTEM”. This information can also be backed up by looking in the Active Control Set, ControlSet001, where the same time zone information is conveyed.



Registry SYSTEM Information	
Active Control Set	ControlSet001
Computer Name	WESMANTOOTH-PC
Time Zone BIAS	420
Time Zone Active Time BIAS	360
Standard Bias	0
Daylight Bias	-60

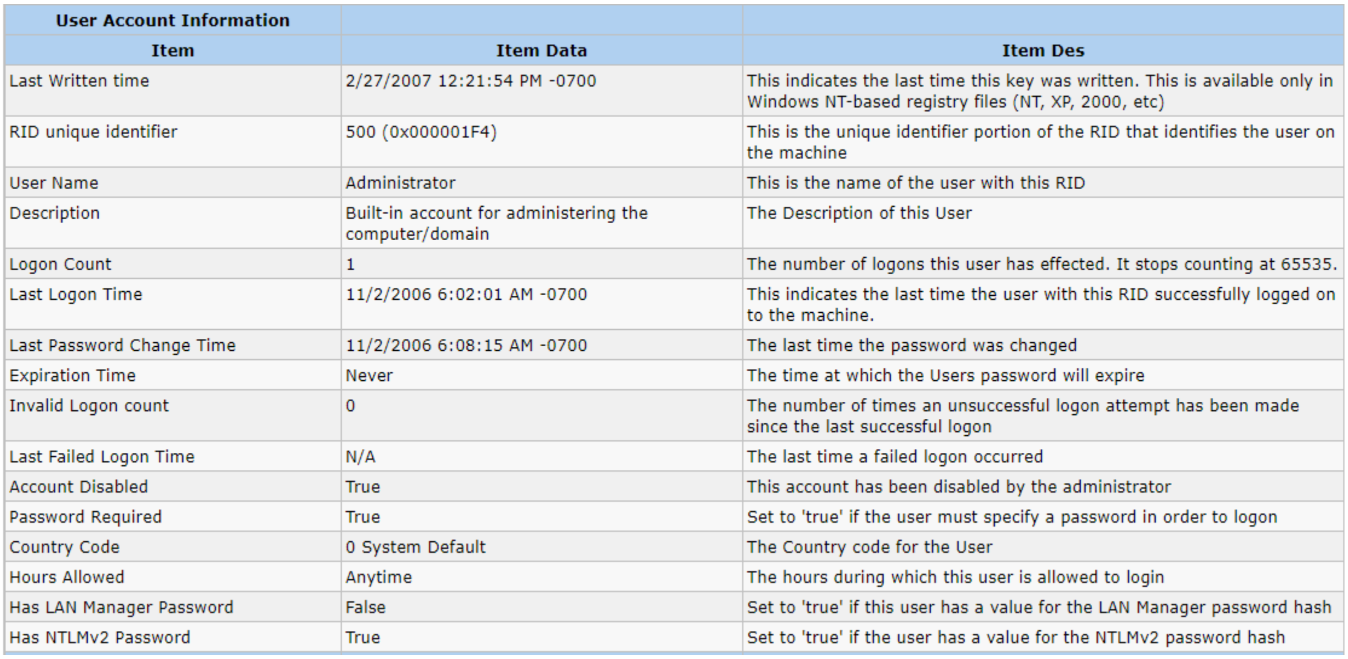
Figure 10: Image shows information from SYSTEM registry file.

There are five user accounts set up on this operating system: Wes Mantooth, Administrator, Count Dracula, Laurent, and Guest. In the SAM registry file, crucial data on each user is stored. The SAM registry file is found at “Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Windows\System32\config\SAM”. The most important to note are the User Name, Last Logon Time, the Unique Identifier, and whether the account is enabled. Specifically, note the following: The Administrator and Guest and Laurent accounts are disabled, the accounts for Dracula and Administrator have not been logged in to since April 1st, 2007 and November 2nd, 2006 respectively; the Guest and Laurent accounts have never been logged in to; the Wes Mantooth account has the password “tooth” despite not being required to have a password, and the Count Dracula account has the password “canine”.



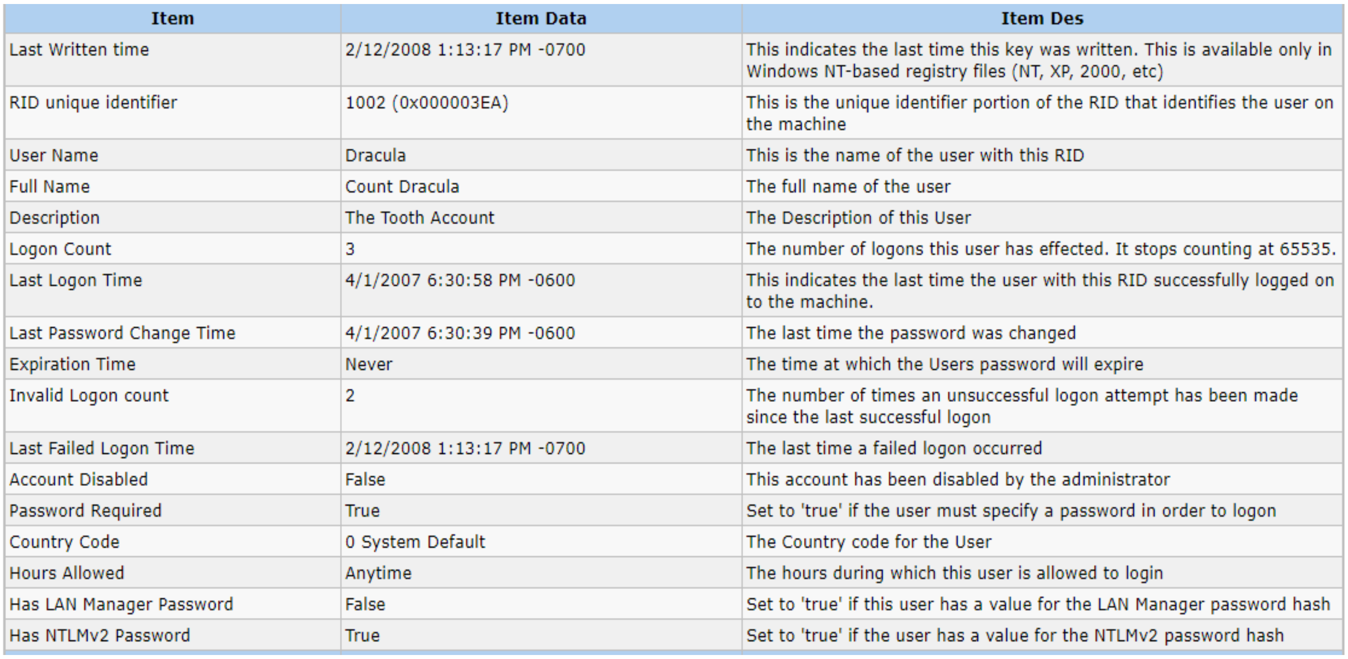
Item	Item Data	Item Des
Last Written time	2/12/2008 1:13:16 PM -0700	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1000 (0x000003E8)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Wes Mantooth	This is the name of the user with this RID
Logon Count	96	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	2/12/2008 12:12:08 PM -0700	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	2/27/2007 11:29:13 AM -0700	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	3	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	2/12/2008 1:13:16 PM -0700	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	False	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash
User's password hint	in your face	User's password hint

Figure 11: Wes Mantooth user account information.



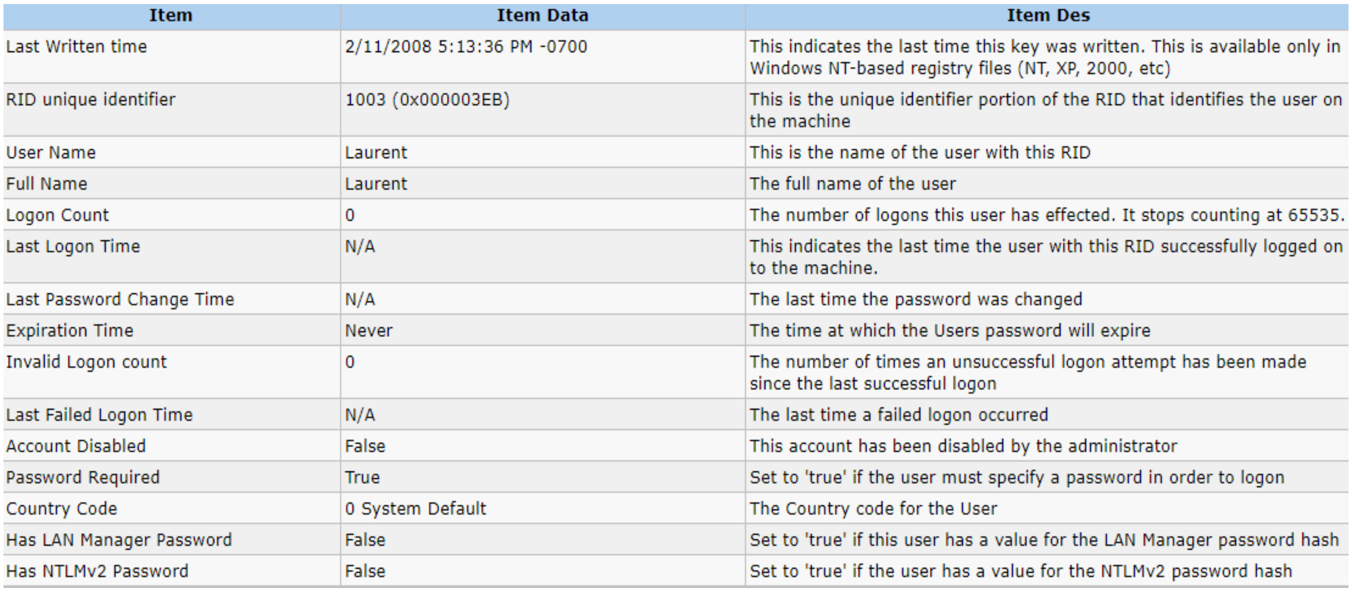
User Account Information		
Item	**Item Data**	**Item Des**
Last Written time	2/27/2007 12:21:54 PM -0700	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	500 (0x000001F4)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Administrator	This is the name of the user with this RID
Description	Built-in account for administering the computer/domain	The Description of this User
Logon Count	1	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	11/2/2006 6:02:01 AM -0700	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	11/2/2006 6:08:15 AM -0700	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	True	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Hours Allowed	Anytime	The hours during which this user is allowed to login
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 12: Administrator user account information.



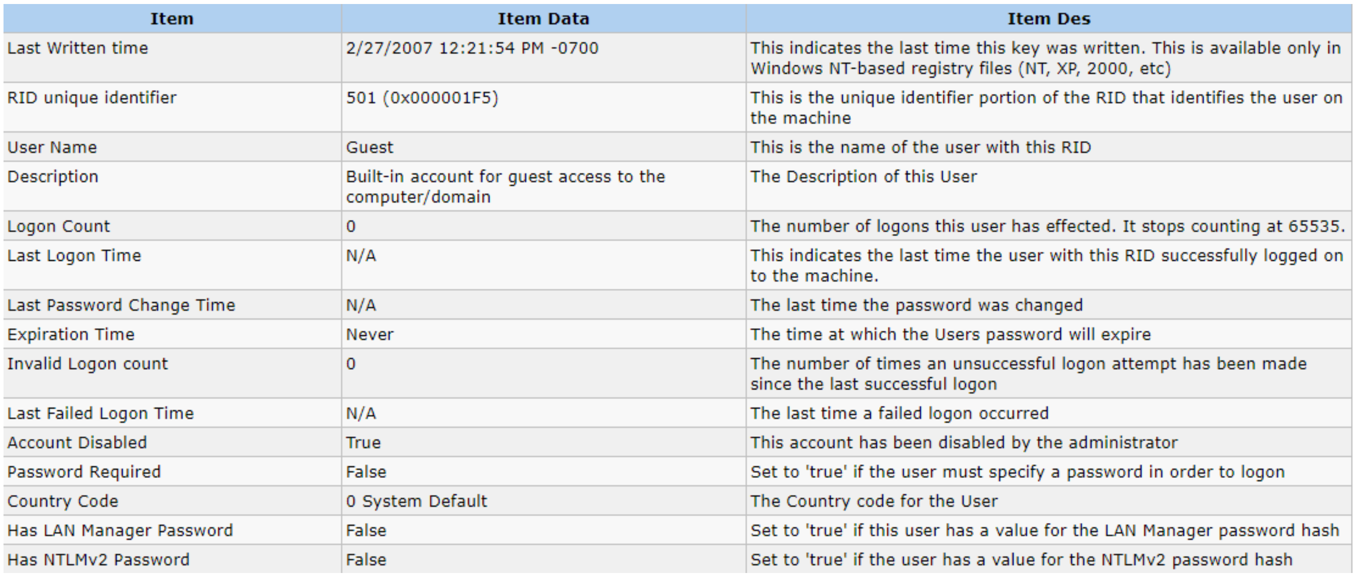
Item	Item Data	Item Des
Last Written time	2/12/2008 1:13:17 PM -0700	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1002 (0x000003EA)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Dracula	This is the name of the user with this RID
Full Name	Count Dracula	The full name of the user
Description	The Tooth Account	The Description of this User
Logon Count	3	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	4/1/2007 6:30:58 PM -0600	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	4/1/2007 6:30:39 PM -0600	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	2	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	2/12/2008 1:13:17 PM -0700	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Hours Allowed	Anytime	The hours during which this user is allowed to login
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 13: Count Dracula user account information.



Item	Item Data	Item Des
Last Written time	2/11/2008 5:13:36 PM -0700	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1003 (0x000003EB)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Laurent	This is the name of the user with this RID
Full Name	Laurent	The full name of the user
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	False	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 14: Laurent user account information.

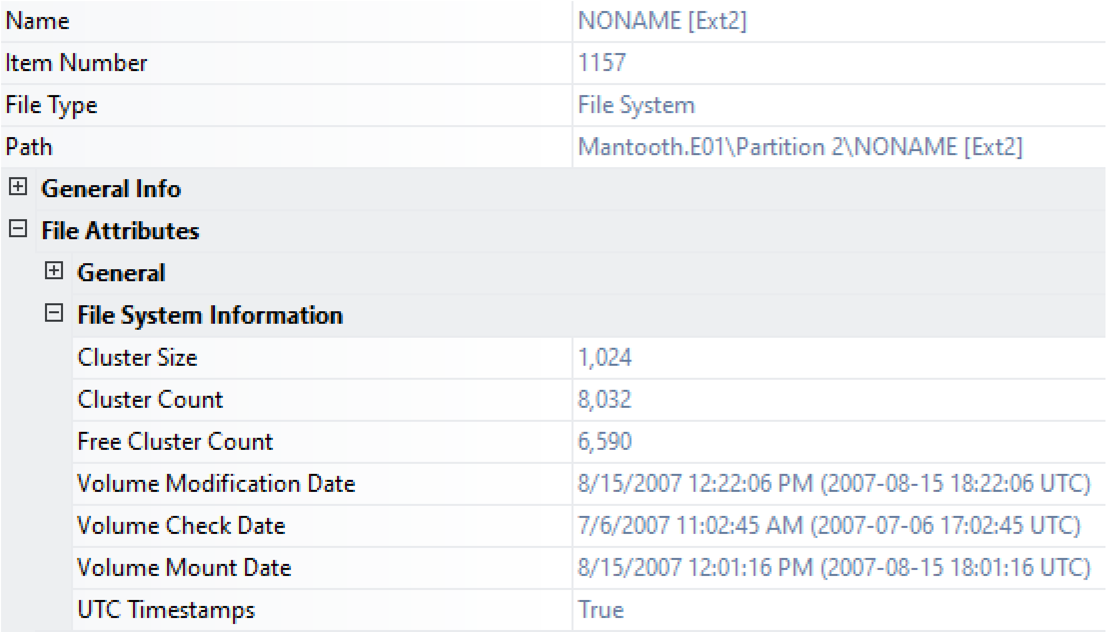


Item	Item Data	Item Des
Last Written time	2/27/2007 12:21:54 PM -0700	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	501 (0x000001F5)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Guest	This is the name of the user with this RID
Description	Built-in account for guest access to the computer/domain	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	True	This account has been disabled by the administrator
Password Required	False	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	False	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 15: Guest user account information.

NONAME Partition

The second partition is a small EXT2 file system that contains personal images and documents. The name of this file system is “NONAME”. It has not been modified since August 15th, 2007 which is months before this hard drive was seized by police.

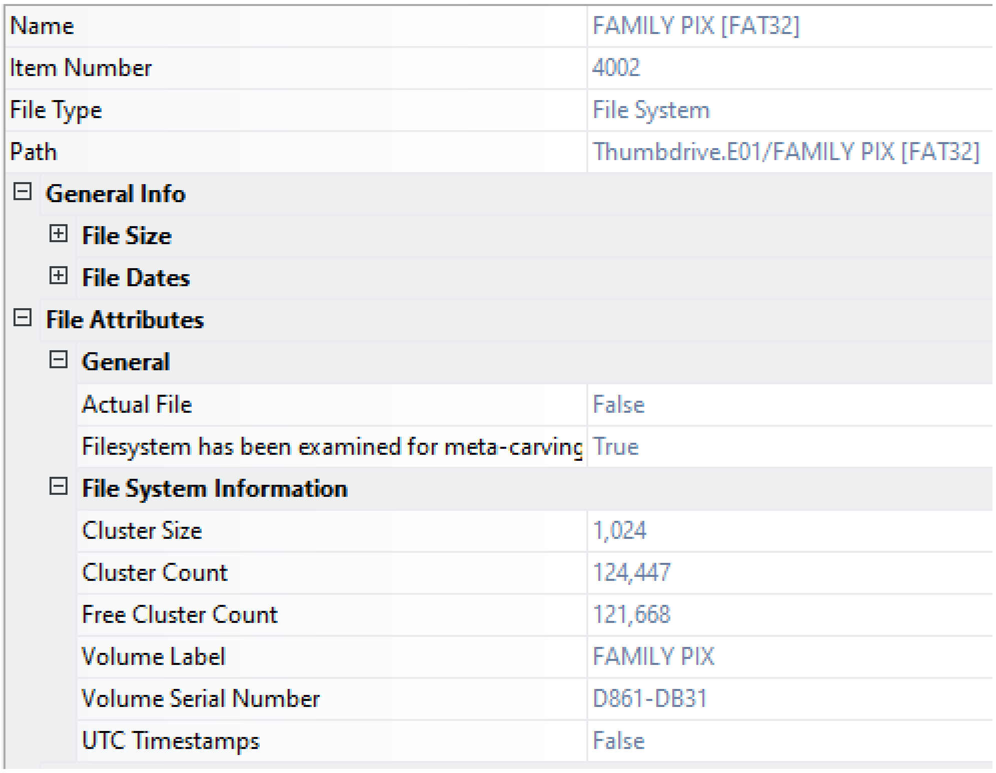


Name	NONAME [Ext2]
Item Number	1157
File Type	File System
Path	Mantooth.E01\Partition 2\NONAME [Ext2]
⊞ **General Info**	
⊟ **File Attributes**	
⊞ **General**	
⊟ **File System Information**	
Cluster Size	1,024
Cluster Count	8,032
Free Cluster Count	6,590
Volume Modification Date	8/15/2007 12:22:06 PM (2007-08-15 18:22:06 UTC)
Volume Check Date	7/6/2007 11:02:45 AM (2007-07-06 17:02:45 UTC)
Volume Mount Date	8/15/2007 12:01:16 PM (2007-08-15 18:01:16 UTC)
UTC Timestamps	True

Figure 16: Image contains information on the NONAME file system.

Mantooth Thumb Drive

Mantooth's thumb drive is a single partition made up of a FAT32 file system called "FAMILY PIX". The thumb drive contains roughly 4 megabytes of images and personal documents. The rest of the Thumbdrive.E01 image is made up of empty space. The thumb drive was imaged on March 3rd, 2008.

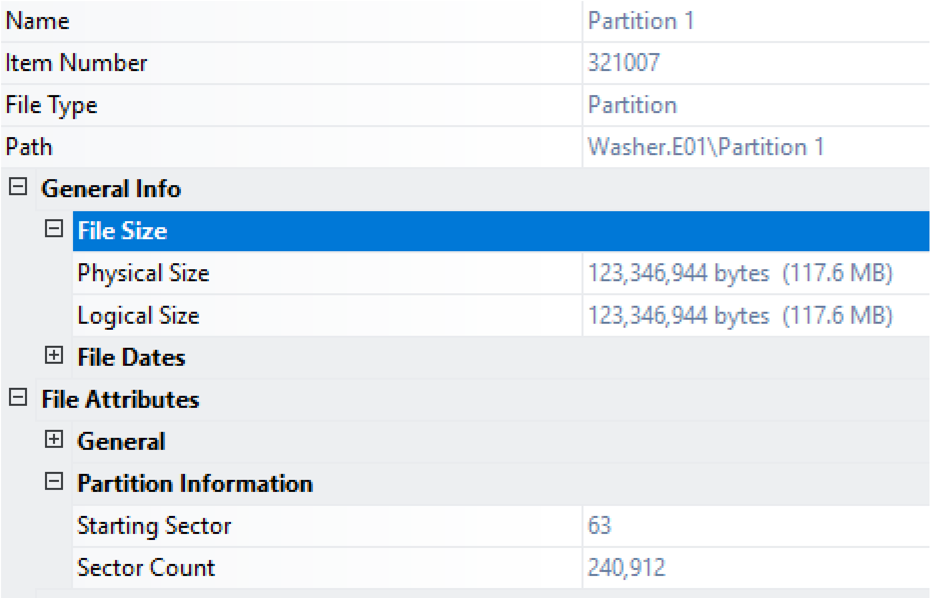


Name	FAMILY PIX [FAT32]
Item Number	4002
File Type	File System
Path	Thumbdrive.E01/FAMILY PIX [FAT32]
⊟ **General Info**	
⊞ **File Size**	
⊞ **File Dates**	
⊟ **File Attributes**	
⊟ **General**	
Actual File	False
Filesystem has been examined for meta-carving	True
⊟ **File System Information**	
Cluster Size	1,024
Cluster Count	124,447
Free Cluster Count	121,668
Volume Label	FAMILY PIX
Volume Serial Number	D861-DB31
UTC Timestamps	False

Figure 17: Image contains information on the FAMILY PIX file system.

Washer Hard Drive

The forensic image of the hard drive confiscated from the computer in Washer’s residence contains one partition. The partition solely contains the Windows XP operating system which uses the NTFS file system. There are also 4983 kilobytes of empty space not contained by the partition. There is also a broken master boot record of 512 bytes found outside of the partition. The image of the drive was acquired on March 10th, 2008.

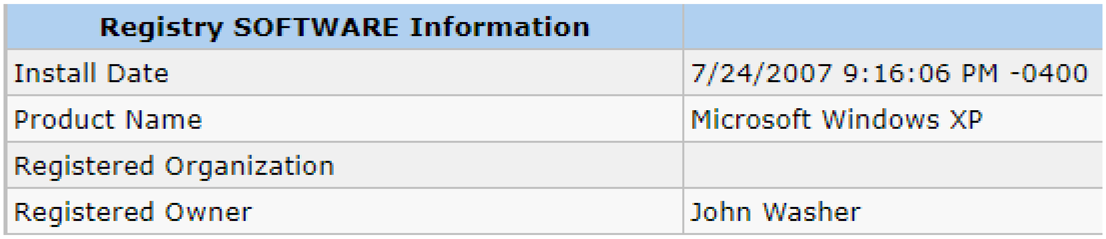


Name	Partition 1
Item Number	321007
File Type	Partition
Path	Washer.E01\Partition 1
⊟ **General Info**	
⊟ **File Size**	
Physical Size	123,346,944 bytes (117.6 MB)
Logical Size	123,346,944 bytes (117.6 MB)
⊞ **File Dates**	
⊟ **File Attributes**	
⊞ **General**	
⊟ **Partition Information**	
Starting Sector	63
Sector Count	240,912

Figure 18: Image contains information about the only partition on Washer's hard drive.

Windows XP Partition

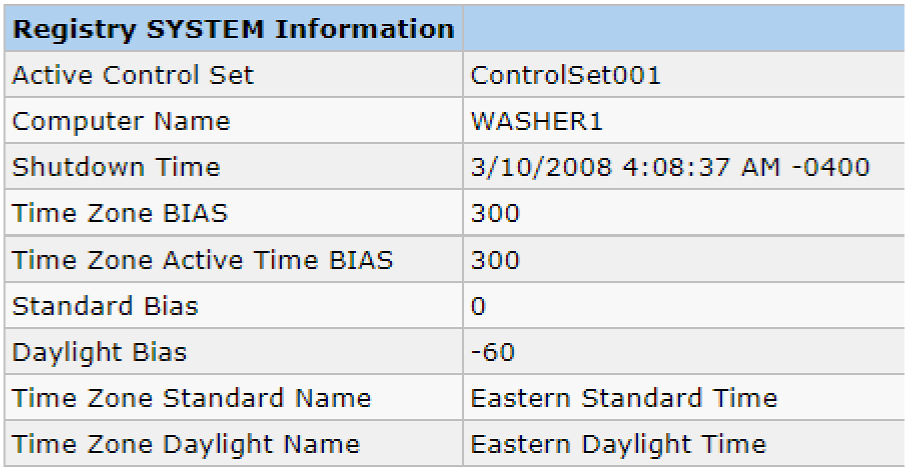
The partition is solely occupied by the Windows XP operating system and is registered under John Washer's name. The file system for the operating system is NTFS. This information is found in the registry file named SOFTWARE found at "Washer.E01\Partition 1\WASHER [NTFS]\[root]\WINDOWS\system32\config\software".



Registry SOFTWARE Information	
Install Date	7/24/2007 9:16:06 PM -0400
Product Name	Microsoft Windows XP
Registered Organization	
Registered Owner	John Washer

Figure 19: Image contains information about the SOFTWARE registry file.

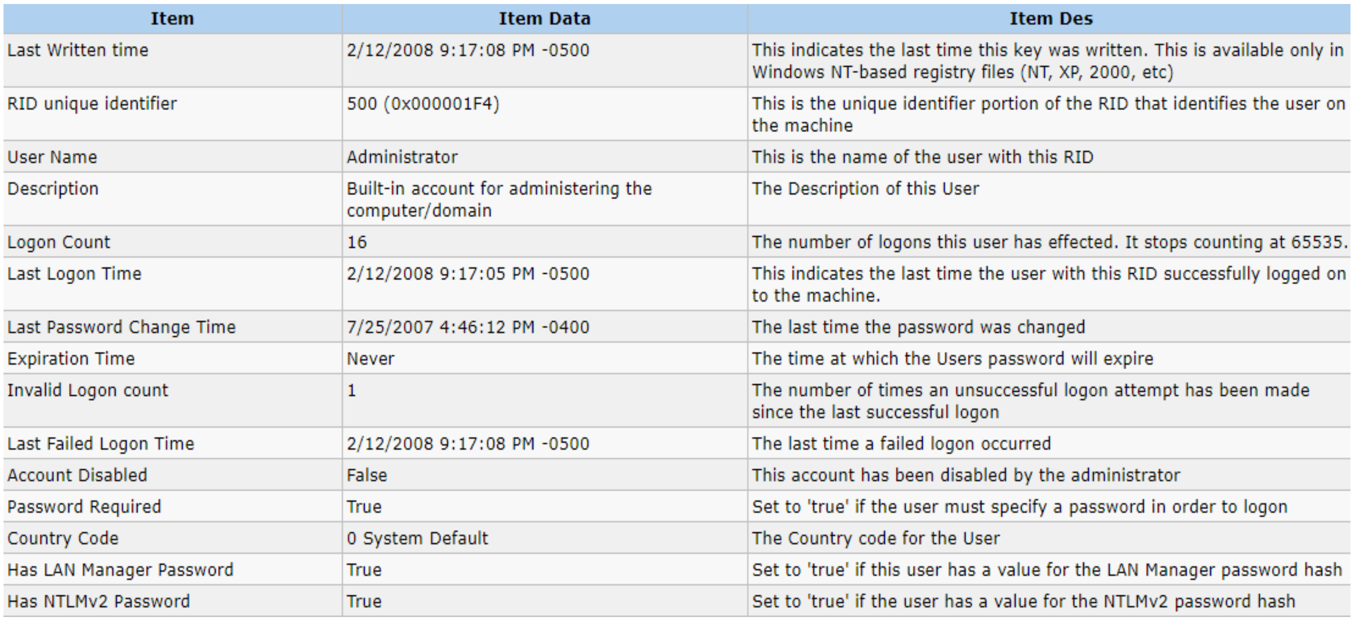
Within the operating system, the computer is name "WASHER1" and runs on the time zone of Eastern Standard Time with daylight savings. This information can be found in the SYSTEM registry file found at "Washer.E01\Partition 1\WASHER [NTFS]\[root]\WINDOWS\system32\config\system". This information can also be backed up by looking in the Active Control Set, ControlSet001, where the same time zone information is conveyed.



Registry SYSTEM Information	
Active Control Set	ControlSet001
Computer Name	WASHER1
Shutdown Time	3/10/2008 4:08:37 AM -0400
Time Zone BIAS	300
Time Zone Active Time BIAS	300
Standard Bias	0
Daylight Bias	-60
Time Zone Standard Name	Eastern Standard Time
Time Zone Daylight Name	Eastern Daylight Time

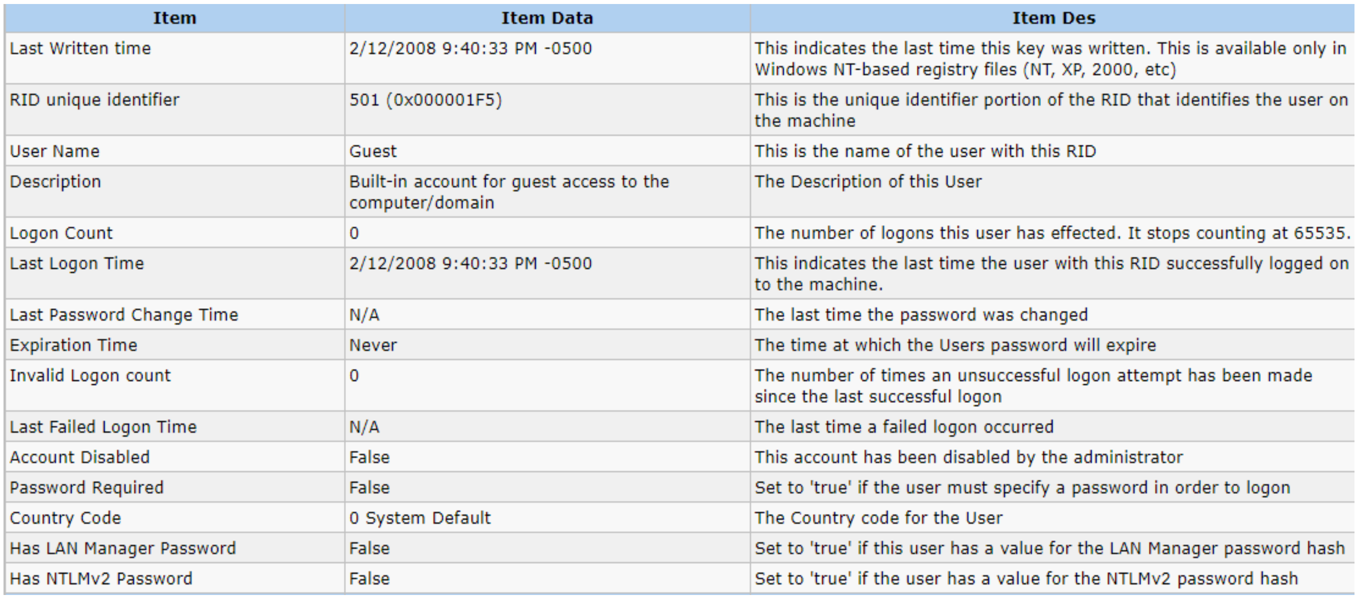
Figure 20: Image contains information about the SYSTEM registry file.

There are eight user accounts set up on this operating system: Administrator, Guest, Remote Desktop Help Assistant Account, SUPPORT_388945a0, Billy Bob Brubeck, The Wolf, Mr Smee, Captian Hook, and Artimus the Aardvark. In the SAM registry file, crucial data on each user is stored. This SAM registry file is found at “Washer.E01\Partition 1\WASHER [NTFS]\[root]\WINDOWS\system32\config\SAM”. The most important to note are the User Name, Last Logon Time, the Unique Identifier, and whether the account is enabled. Specifically, note the following: The Administrator account has the password “meth”; the Guest account has never been logged on to; the Help Assistant account has never been logged on to and has the description of “Account for Providing Remote Assistance”; the Support account has never been logged on to and is disabled; and the Artimus the Aardvark account has never been logged on to and has the account description of “Account for generating bad debt”.



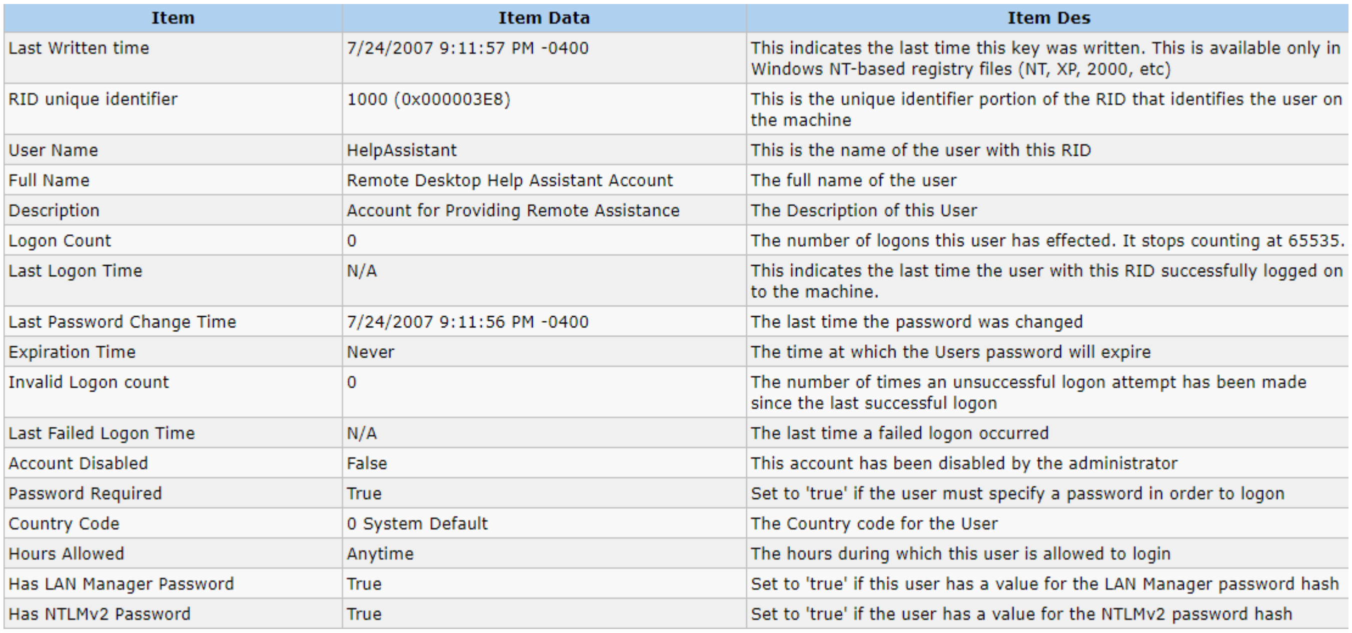
Item	Item Data	Item Des
Last Written time	2/12/2008 9:17:08 PM -0500	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	500 (0x000001F4)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Administrator	This is the name of the user with this RID
Description	Built-in account for administering the computer/domain	The Description of this User
Logon Count	16	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	2/12/2008 9:17:05 PM -0500	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	7/25/2007 4:46:12 PM -0400	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	1	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	2/12/2008 9:17:08 PM -0500	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	True	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 21: Administrator account information.



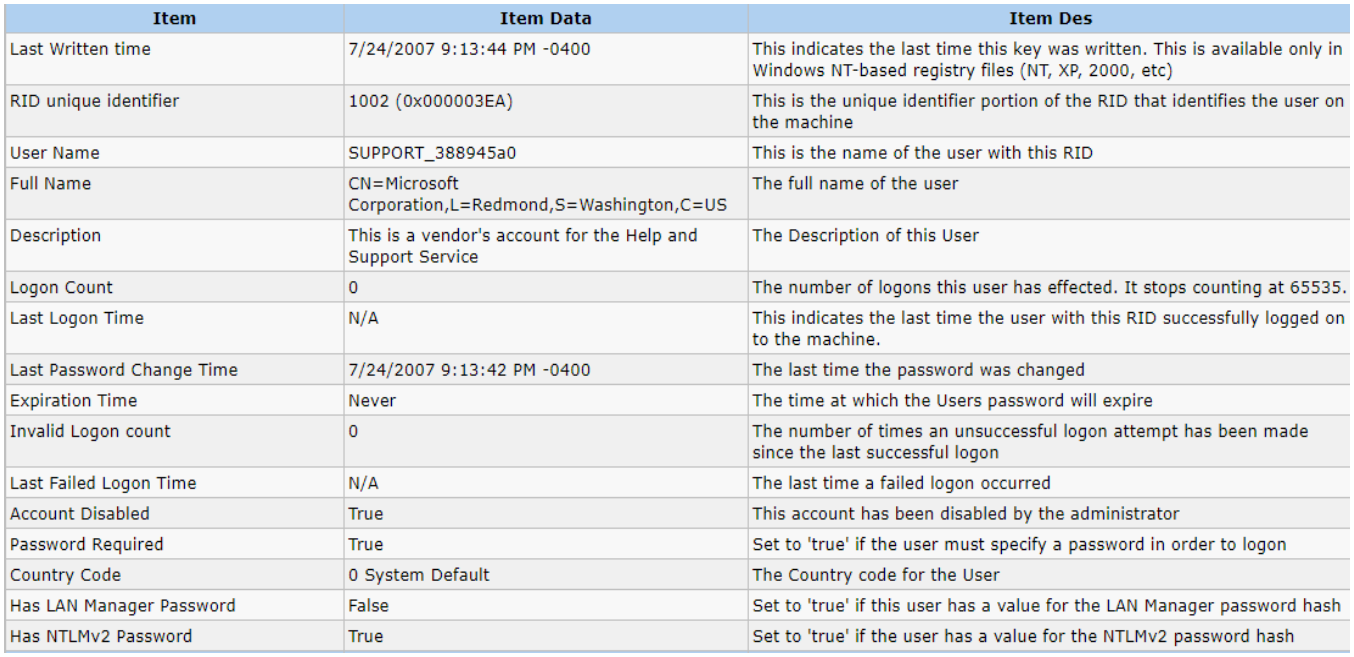
Item	Item Data	Item Des
Last Written time	2/12/2008 9:40:33 PM -0500	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	501 (0x000001F5)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Guest	This is the name of the user with this RID
Description	Built-in account for guest access to the computer/domain	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	2/12/2008 9:40:33 PM -0500	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	False	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	False	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 22: Guest account information.



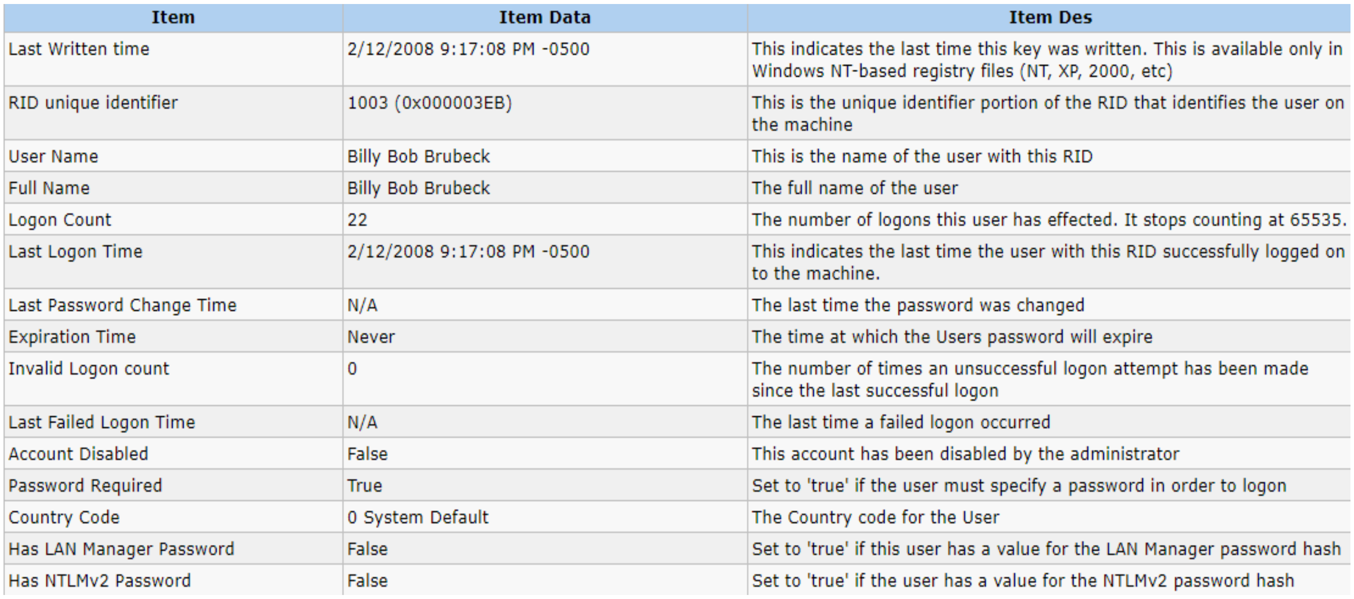
Item	Item Data	Item Des
Last Written time	7/24/2007 9:11:57 PM -0400	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1000 (0x000003E8)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	HelpAssistant	This is the name of the user with this RID
Full Name	Remote Desktop Help Assistant Account	The full name of the user
Description	Account for Providing Remote Assistance	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	7/24/2007 9:11:56 PM -0400	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Hours Allowed	Anytime	The hours during which this user is allowed to login
Has LAN Manager Password	True	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 23: HelpAssistant account information.



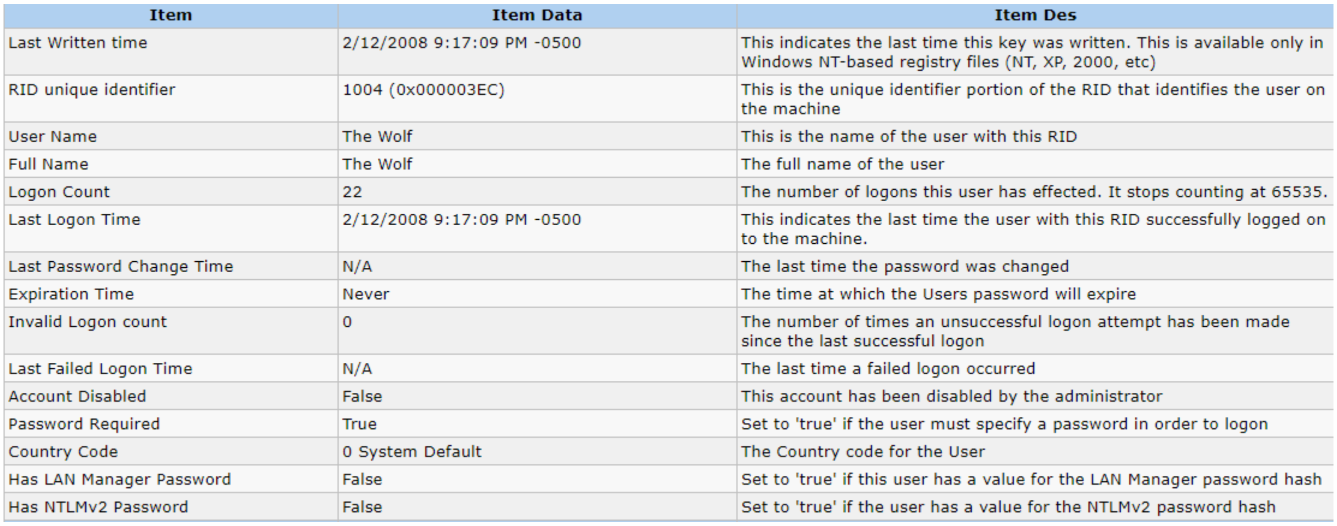
Item	Item Data	Item Des
Last Written time	7/24/2007 9:13:44 PM -0400	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1002 (0x000003EA)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	SUPPORT_388945a0	This is the name of the user with this RID
Full Name	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	The full name of the user
Description	This is a vendor's account for the Help and Support Service	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	7/24/2007 9:13:42 PM -0400	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	True	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	True	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 24: SUPPORT_388945a0 account information.



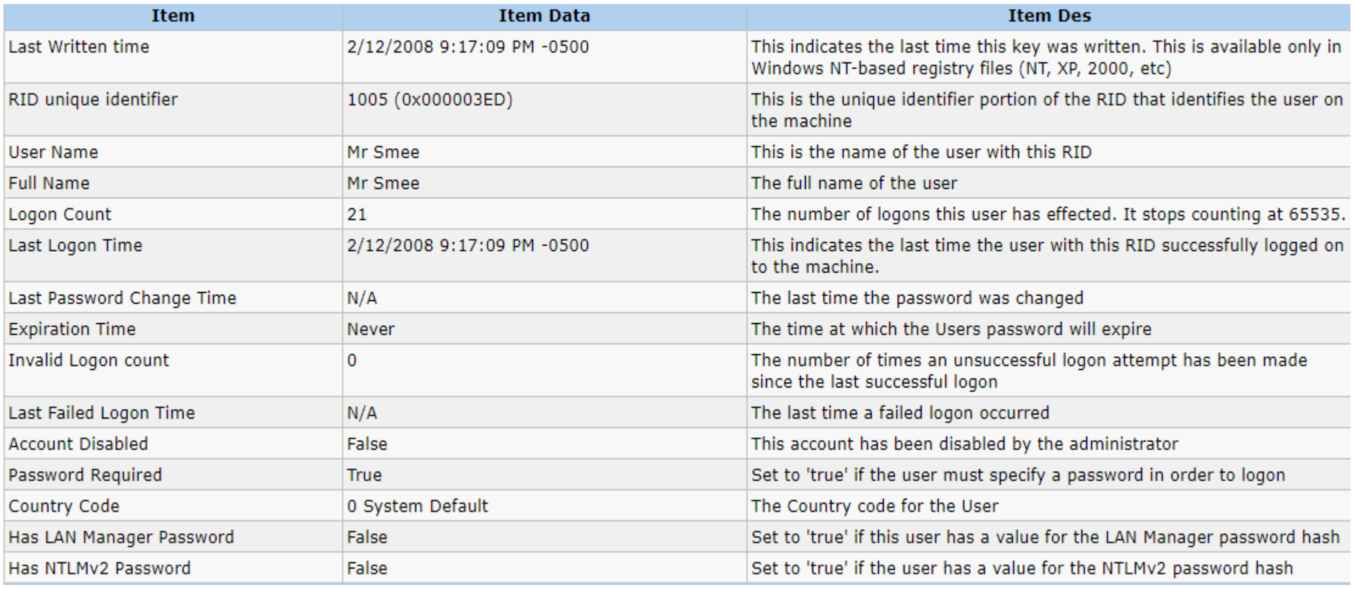
Item	Item Data	Item Des
Last Written time	2/12/2008 9:17:08 PM -0500	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1003 (0x000003EB)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Billy Bob Brubeck	This is the name of the user with this RID
Full Name	Billy Bob Brubeck	The full name of the user
Logon Count	22	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	2/12/2008 9:17:08 PM -0500	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	False	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 25: Billy Bob Brubeck account information.



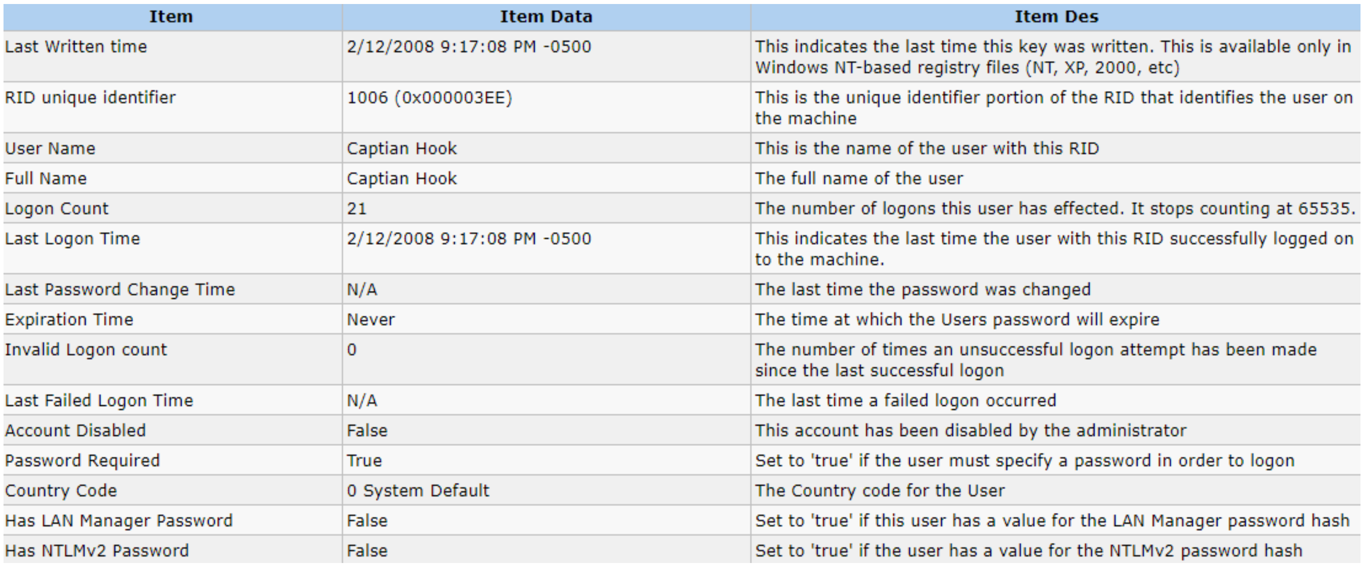
Item	Item Data	Item Des
Last Written time	2/12/2008 9:17:09 PM -0500	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1004 (0x000003EC)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	The Wolf	This is the name of the user with this RID
Full Name	The Wolf	The full name of the user
Logon Count	22	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	2/12/2008 9:17:09 PM -0500	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	False	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 26: The Wolf account information.



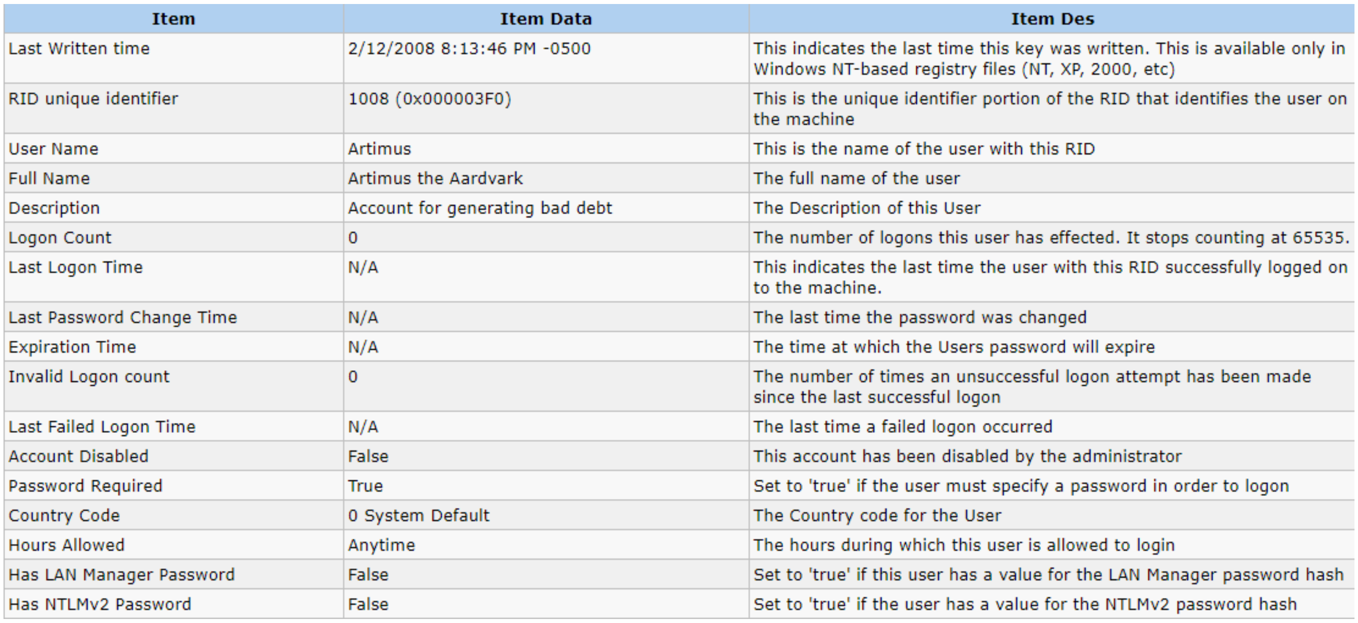
Item	Item Data	Item Des
Last Written time	2/12/2008 9:17:09 PM -0500	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1005 (0x000003ED)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Mr Smee	This is the name of the user with this RID
Full Name	Mr Smee	The full name of the user
Logon Count	21	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	2/12/2008 9:17:09 PM -0500	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	False	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 27: Mr Smee account information.



Item	Item Data	Item Des
Last Written time	2/12/2008 9:17:08 PM -0500	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1006 (0x000003EE)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Captian Hook	This is the name of the user with this RID
Full Name	Captian Hook	The full name of the user
Logon Count	21	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	2/12/2008 9:17:08 PM -0500	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	Never	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	False	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 28: Captian Hook account information.



Item	Item Data	Item Des
Last Written time	2/12/2008 8:13:46 PM -0500	This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)
RID unique identifier	1008 (0x000003F0)	This is the unique identifier portion of the RID that identifies the user on the machine
User Name	Artimus	This is the name of the user with this RID
Full Name	Artimus the Aardvark	The full name of the user
Description	Account for generating bad debt	The Description of this User
Logon Count	0	The number of logons this user has effected. It stops counting at 65535.
Last Logon Time	N/A	This indicates the last time the user with this RID successfully logged on to the machine.
Last Password Change Time	N/A	The last time the password was changed
Expiration Time	N/A	The time at which the Users password will expire
Invalid Logon count	0	The number of times an unsuccessful logon attempt has been made since the last successful logon
Last Failed Logon Time	N/A	The last time a failed logon occurred
Account Disabled	False	This account has been disabled by the administrator
Password Required	True	Set to 'true' if the user must specify a password in order to logon
Country Code	0 System Default	The Country code for the User
Hours Allowed	Anytime	The hours during which this user is allowed to login
Has LAN Manager Password	False	Set to 'true' if this user has a value for the LAN Manager password hash
Has NTLMv2 Password	False	Set to 'true' if the user has a value for the NTLMv2 password hash

Figure 29: Artimus the Aardvark account information.

Procedure

Antivirus Scan

Before examining the evidence, every forensic image was scanned for viruses. The antivirus program used during this examination is called ClamWin. Each forensic image is mounted and scanned for viruses. This process does not damage the integrity of the original forensic image as the information mounted is a copy of the image and is also not allowed to be written to.

The Mantooth Hard Drive was mounted to the forensic machine, in a read only method, physically as a simulated hard drive and logically as two distinct read only file systems. Each partition of the hard drive was scanned independently. One dangerous file was detected in the first partition of Wes Mantooth's Hard Drive and was recognized as "Win.Tool.Snadboy-6". This file is an executable that leads to a program called Snadboy which is allegedly used to reveal passwords hidden by asterisks in any circumstance. The file should not have an adverse effect on the examination computer or the analysis of the evidence.

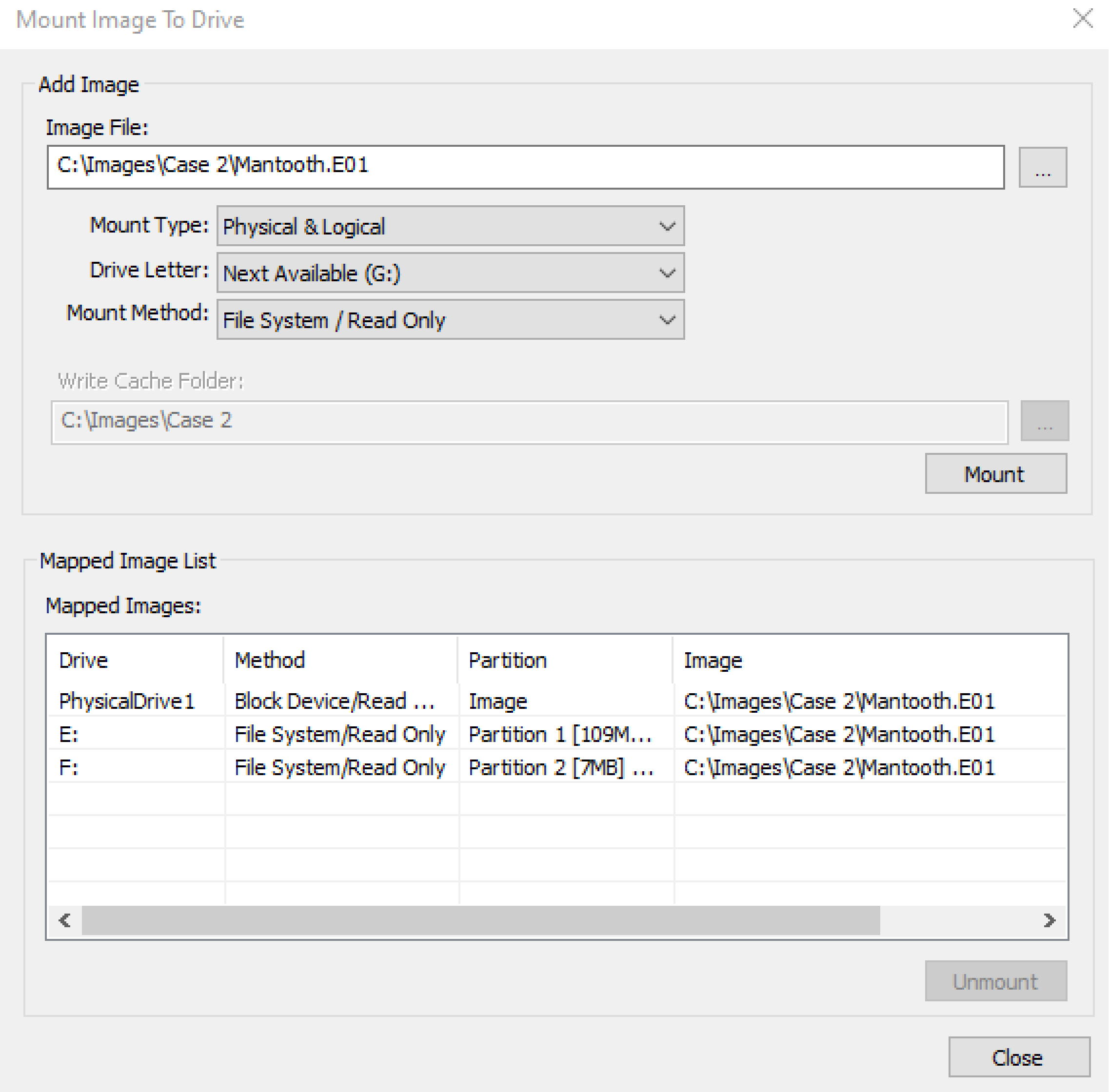


Image File: C:\Images\Case 2\Mantooth.E01

Mount Type: Physical & Logical

Drive Letter: Next Available (G:)

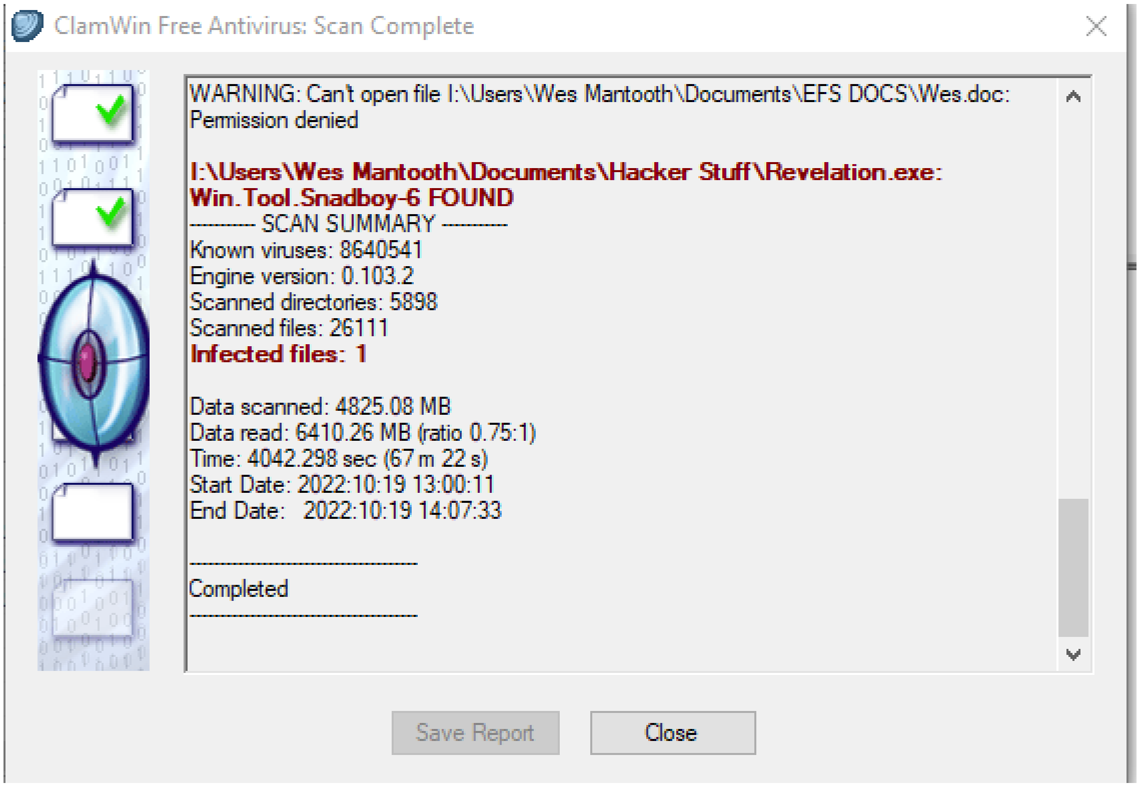
Mount Method: File System / Read Only

Write Cache Folder: C:\Images\Case 2

Mapped Images:

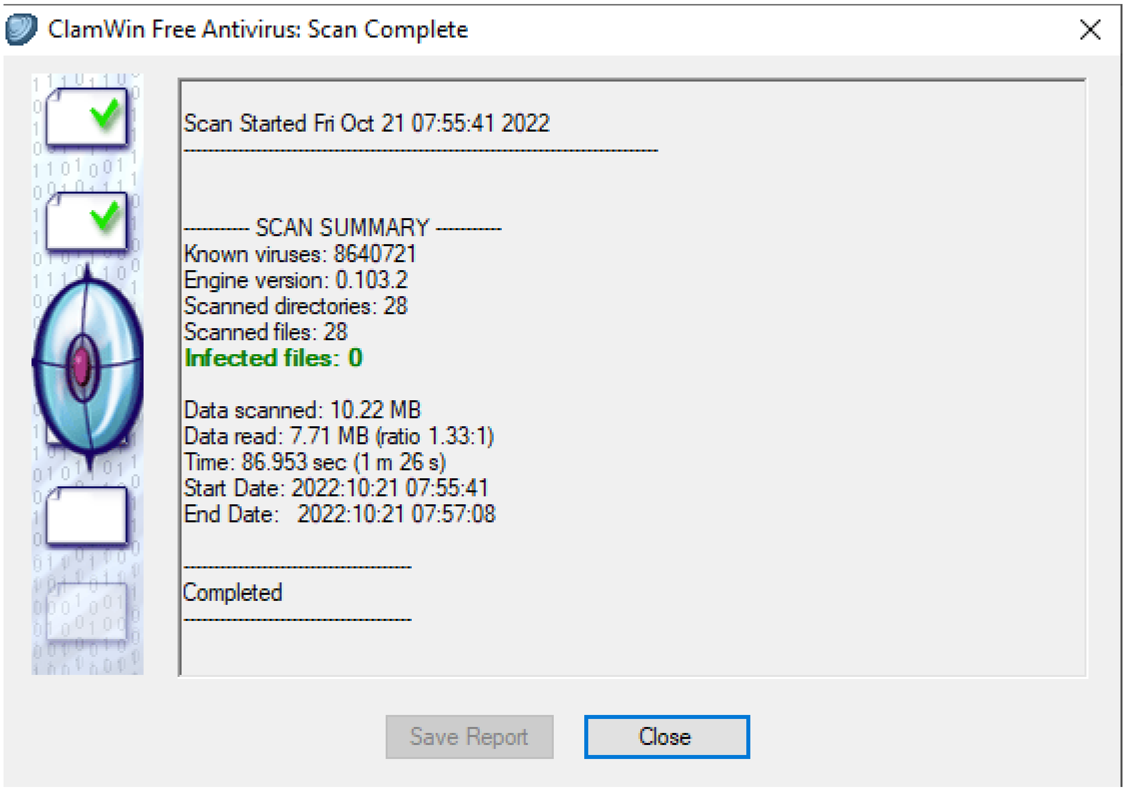
Drive	Method	Partition	Image
PhysicalDrive1	Block Device/Read ...	Image	C:\Images\Case 2\Mantooth.E01
E:	File System/Read Only	Partition 1 [109M...	C:\Images\Case 2\Mantooth.E01
F:	File System/Read Only	Partition 2 [7MB] ...	C:\Images\Case 2\Mantooth.E01

Figure 30: Image about the mounting of the Mantooth Hard Drive.



```
WARNING: Can't open file I:\Users\Wes Mantooth\Documents\EFS DOCS\Wes.doc:
Permission denied

I:\Users\Wes Mantooth\Documents\Hacker Stuff\Revelation.exe:
Win.Tool.Snadboy-6 FOUND
---------- SCAN SUMMARY ----------
Known viruses: 8640541
Engine version: 0.103.2
Scanned directories: 5898
Scanned files: 26111
Infected files: 1

Data scanned: 4825.08 MB
Data read: 6410.26 MB (ratio 0.75:1)
Time: 4042.298 sec (67 m 22 s)
Start Date: 2022:10:19 13:00:11
End Date:   2022:10:19 14:07:33

--------------------------------
Completed
--------------------------------
```

Figure 31: Image about the virus scanning of the first partition of Mantooth's Hard Drive.



```
Scan Started Fri Oct 21 07:55:41 2022
-------------------------------------------------------------------


---------- SCAN SUMMARY ----------
Known viruses: 8640721
Engine version: 0.103.2
Scanned directories: 28
Scanned files: 28
Infected files: 0

Data scanned: 10.22 MB
Data read: 7.71 MB (ratio 1.33:1)
Time: 86.953 sec (1 m 26 s)
Start Date: 2022:10:21 07:55:41
End Date:   2022:10:21 07:57:08

--------------------------------
Completed
--------------------------------
```

Figure 32: Image about the virus scanning of the second partition of Mantooth's Hard Drive.

The Mantooth Thumb Drive was mounted to the forensic machine, in a ready only method, physically as a simulated hard drive and logically as the FAMILY PIX partition. The virus scan detected no dangerous files on the thumb drive.

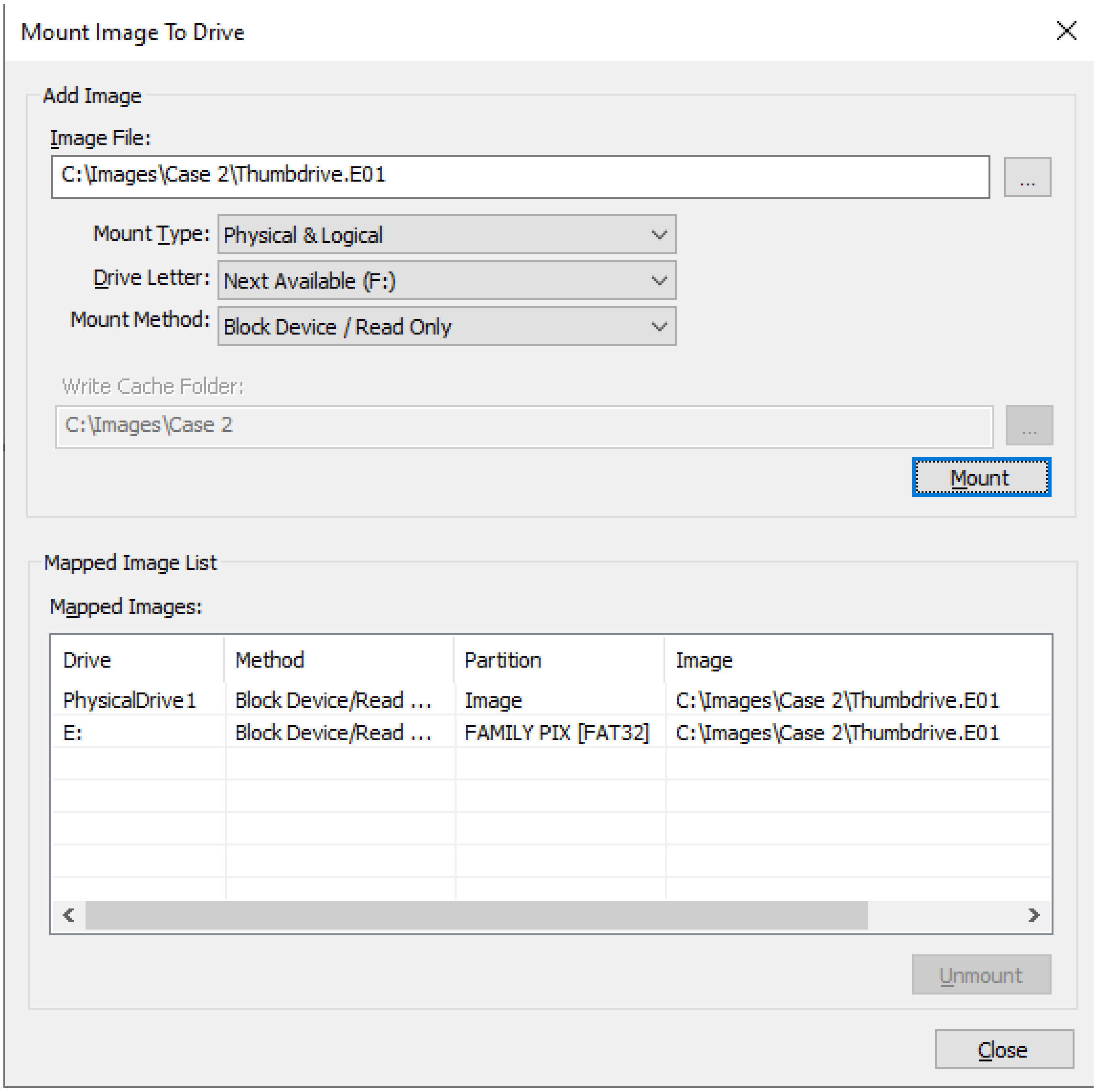


Image File: C:\Images\Case 2\Thumbdrive.E01

Mount Type: Physical & Logical

Drive Letter: Next Available (F:)

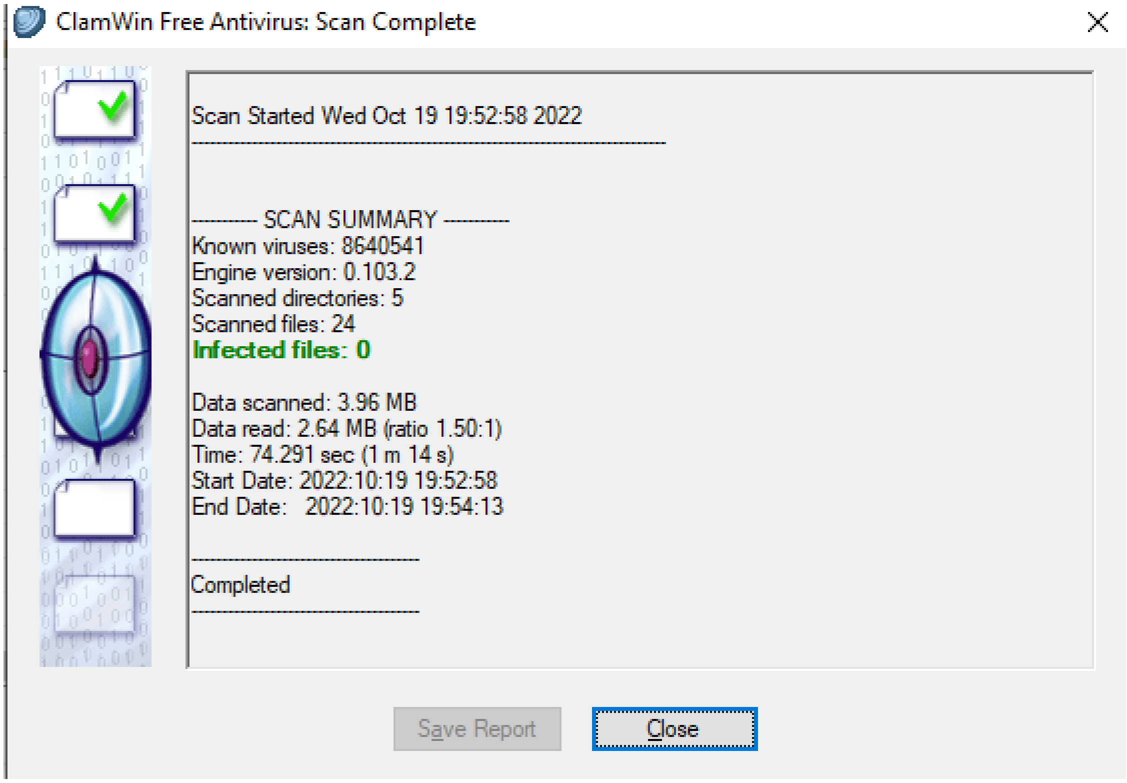
Mount Method: Block Device / Read Only

Write Cache Folder: C:\Images\Case 2

Mapped Images:

Drive	Method	Partition	Image
PhysicalDrive1	Block Device/Read ...	Image	C:\Images\Case 2\Thumbdrive.E01
E:	Block Device/Read ...	FAMILY PIX [FAT32]	C:\Images\Case 2\Thumbdrive.E01

Figure 33: Image about the mounting of Mantooth's Thumb Drive.



```
Scan Started Wed Oct 19 19:52:58 2022
--------------------------------------------------------------------


----------- SCAN SUMMARY -----------
Known viruses: 8640541
Engine version: 0.103.2
Scanned directories: 5
Scanned files: 24
Infected files: 0

Data scanned: 3.96 MB
Data read: 2.64 MB (ratio 1.50:1)
Time: 74.291 sec (1 m 14 s)
Start Date: 2022:10:19 19:52:58
End Date:   2022:10:19 19:54:13

--------------------------------------
Completed
--------------------------------------
```

Figure 34: Image about the virus scanning of Mantooth's Thumb Drive.

The Washer Hard Drive was mounted to the forensic machine, in a ready only method, physically as a simulated hard drive and logically as one file system. The virus scan detected no dangerous files on the hard drive.

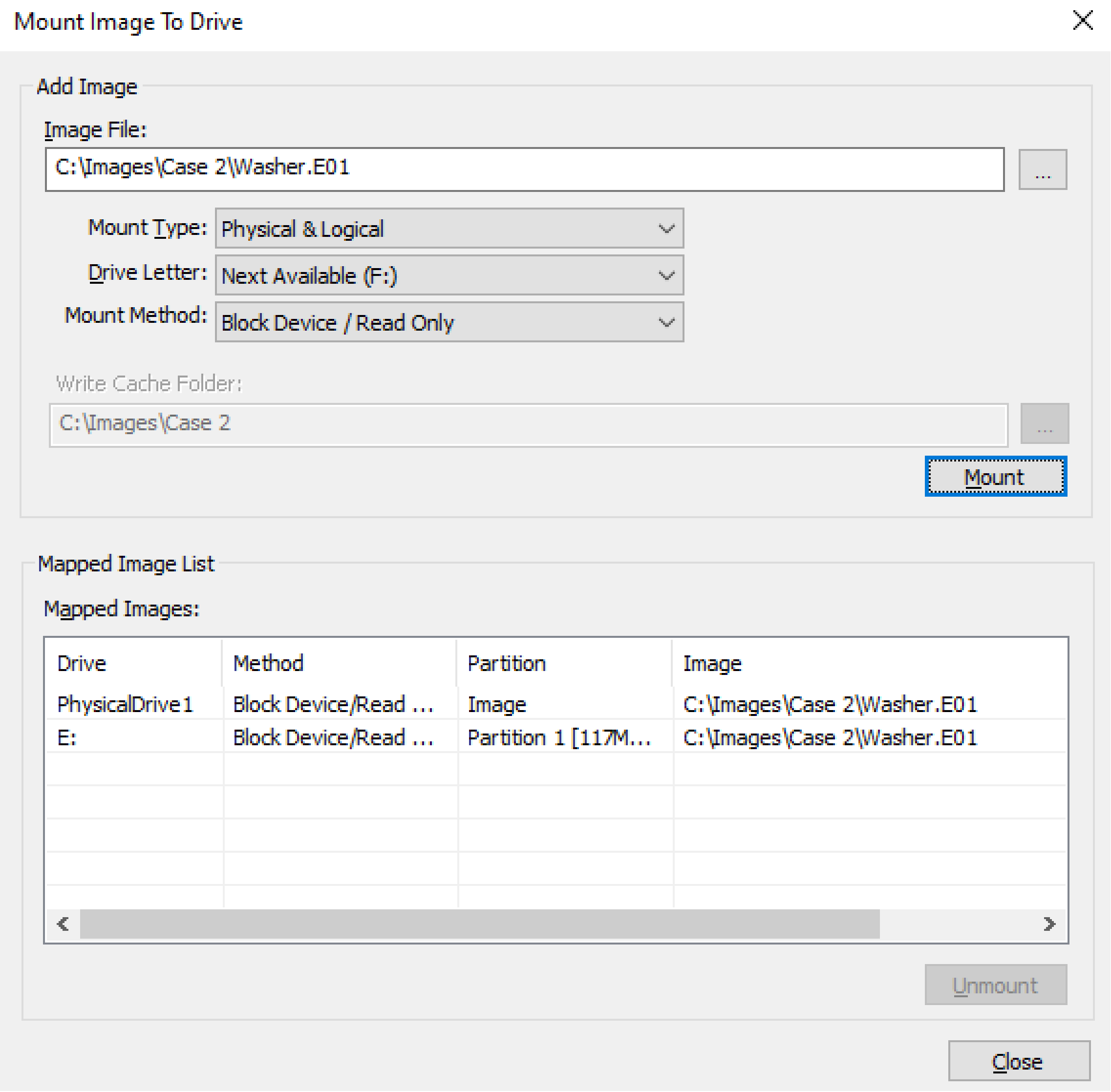


Image File: C:\Images\Case 2\Washer.E01

Mount Type: Physical & Logical

Drive Letter: Next Available (F:)

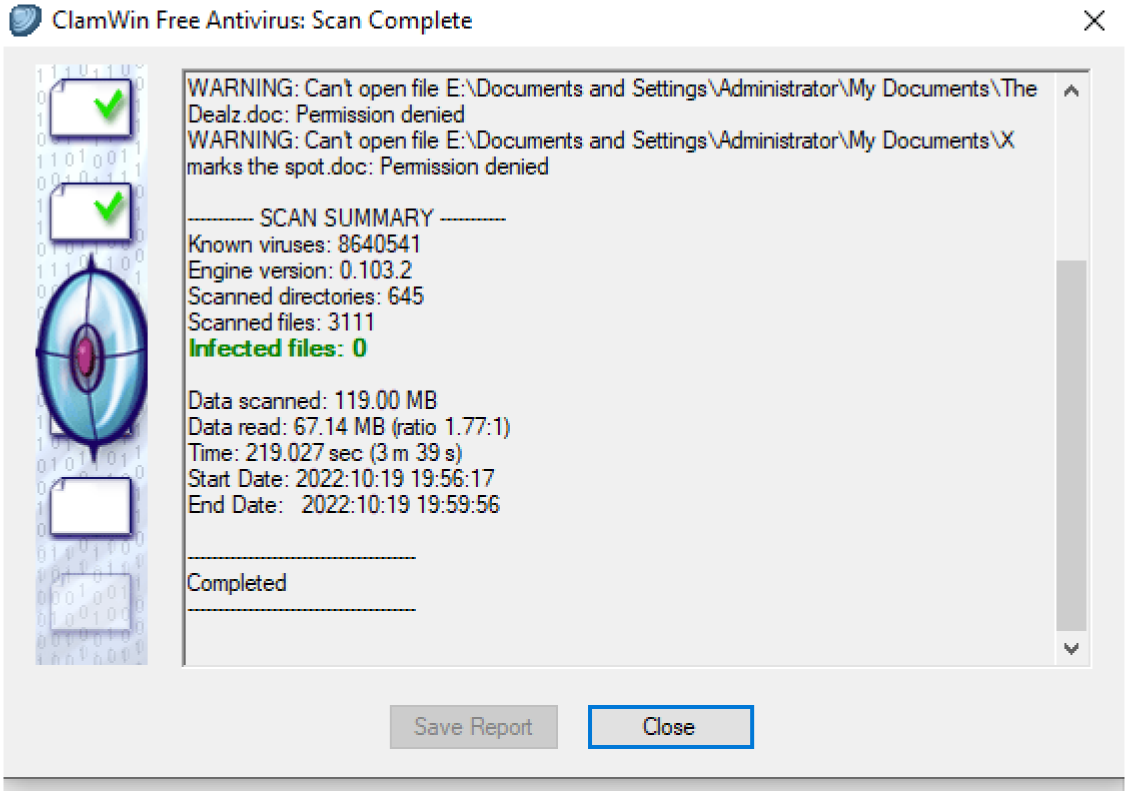
Mount Method: Block Device / Read Only

Write Cache Folder: C:\Images\Case 2

Mapped Images:

Drive	Method	Partition	Image
PhysicalDrive1	Block Device/Read ...	Image	C:\Images\Case 2\Washer.E01
E:	Block Device/Read ...	Partition 1 [117M...	C:\Images\Case 2\Washer.E01

Figure 35: Image about mounting the Washer Hard Drive.

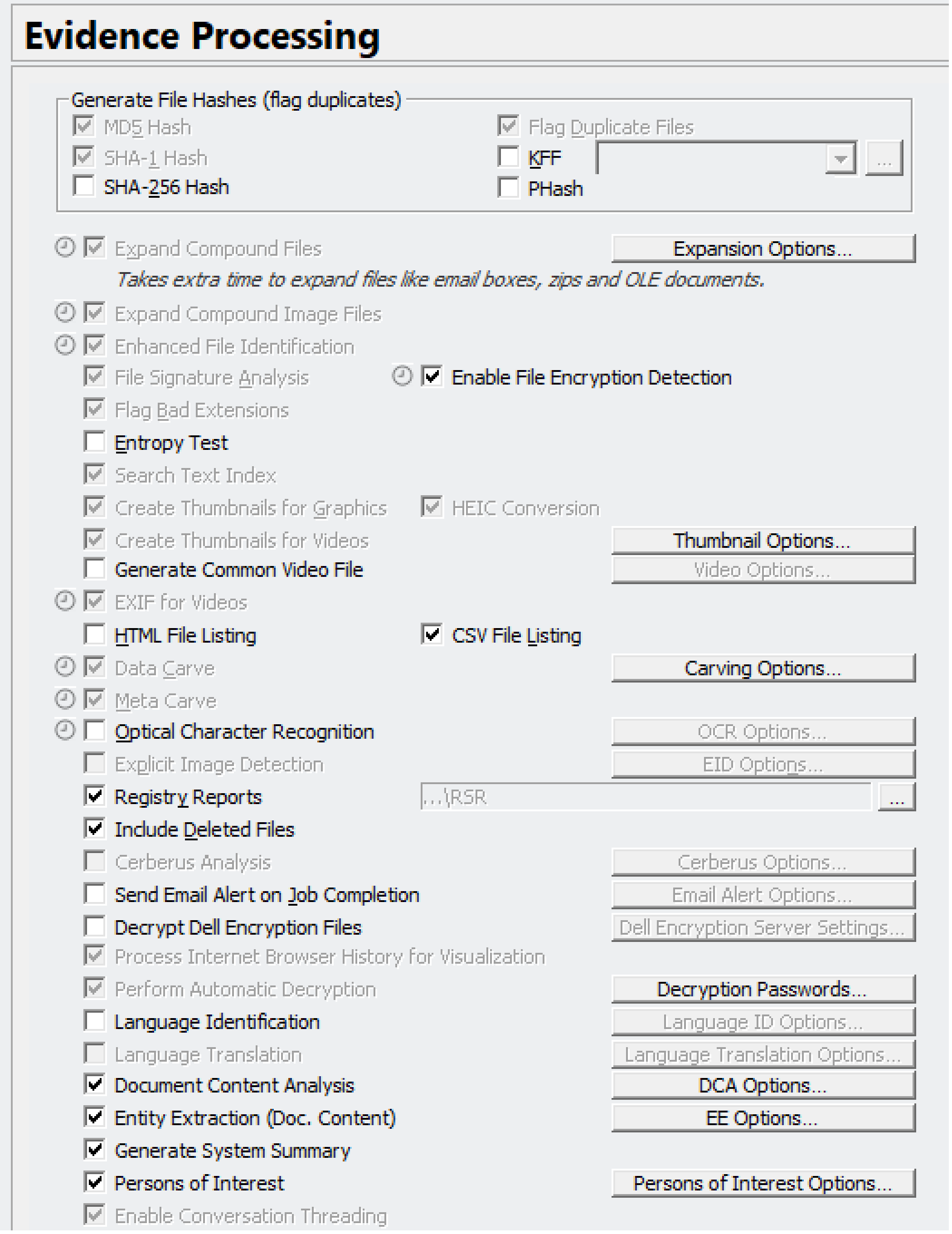


```
WARNING: Can't open file E:\Documents and Settings\Administrator\My Documents\The
Dealz.doc: Permission denied
WARNING: Can't open file E:\Documents and Settings\Administrator\My Documents\X
marks the spot.doc: Permission denied

----------- SCAN SUMMARY -----------
Known viruses: 8640541
Engine version: 0.103.2
Scanned directories: 645
Scanned files: 3111
Infected files: 0

Data scanned: 119.00 MB
Data read: 67.14 MB (ratio 1.77:1)
Time: 219.027 sec (3 m 39 s)
Start Date: 2022:10:19 19:56:17
End Date:   2022:10:19 19:59:56

--------------------------------------
Completed
--------------------------------------
```

Figure 36: Image about the virus scanning of the Washer Hard Drive.

Processing

The processing and analysis of the forensic images was handled in the forensic program FTK from the company AccessData. The processing automatically indexes and hashes every file found, carves out deleted files from free space, sorts common files by categories, and other processes that make the forensic analysis less time consuming and more consistent. All of these processes could be done by hand but automating them makes the forensic analysis more consistent and understandable to more people.



Evidence Processing

Generate File Hashes (flag duplicates)

☑ MD5 Hash
☑ SHA-1 Hash
□ SHA-256 Hash
☑ Flag Duplicate Files
□ KFF
□ PHash

☑ Expand Compound Files

Takes extra time to expand files like email boxes, zips and OLE documents.

☑ Expand Compound Image Files
☑ Enhanced File Identification
☑ File Signature Analysis
☑ Enable File Encryption Detection
☑ Flag Bad Extensions
□ Entropy Test
☑ Search Text Index
☑ Create Thumbnails for Graphics
☑ HEIC Conversion
☑ Create Thumbnails for Videos
□ Generate Common Video File
☑ EXIF for Videos
□ HTML File Listing
☑ CSV File Listing
☑ Data Carve
☑ Meta Carve
□ Optical Character Recognition
□ Explicit Image Detection
☑ Registry Reports ...\RSR
☑ Include Deleted Files
□ Cerberus Analysis
□ Send Email Alert on Job Completion
□ Decrypt Dell Encryption Files
☑ Process Internet Browser History for Visualization
☑ Perform Automatic Decryption
□ Language Identification
□ Language Translation
☑ Document Content Analysis
☑ Entity Extraction (Doc. Content)
☑ Generate System Summary
☑ Persons of Interest
☑ Enable Conversation Threading

Figure 37: Image showing specifically what processes were selected during the forensic analysis.

Decryption

There were many files found in all three of the evidence items which were decrypted by either the built in Microsoft encryption protocol called EFS or by other encryption means. Over the course of the examination, many passwords were found which led to the examiner being able to access some of these encrypted files. The following collected passwords were gathered by AccessData's Password Recovery Tool Kit and from files found inside the forensic image: canine, tooth, meth, smack, HIJIL03016KNMLM, molar, acetone1, camp, mojo, supercallifragilistic. These passwords were used to automatically decrypt files that were detected to have been encrypted. Most of the files encrypted were personal documents and images many of which will be presented as decrypted files in the findings section of this report.

Gathering Pertinent Information

Once the forensic images were scanned for viruses, processed, and several passwords were found, the forensic analysis proceeded with the gathering of frequently useful artifacts. These artifacts include: Pictures, videos, email, calendar dates, user logon credentials, time zone information, language settings, browser history, browser cookies, browser cache, file shortcuts, personal documents, and message databases.

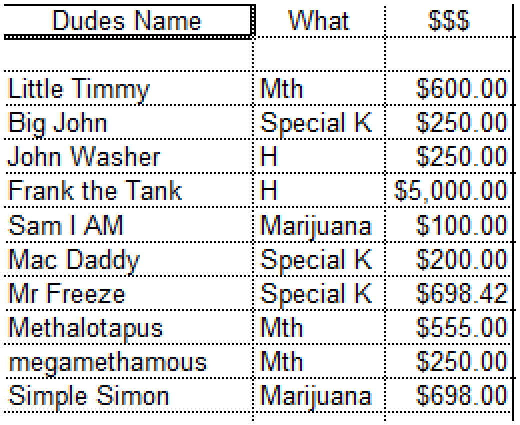
Findings

Wes Mantooth

Drug Possession

There are multiple pieces of evidence linking Wes Mantooth to the possession of illegal drugs. There is the document "Those who owes.xls" which specifies how much different people owe him for various different drugs, his collection of various scanned prescriptions, and a document detailing how to make meth found in the user under Mantooth's control.

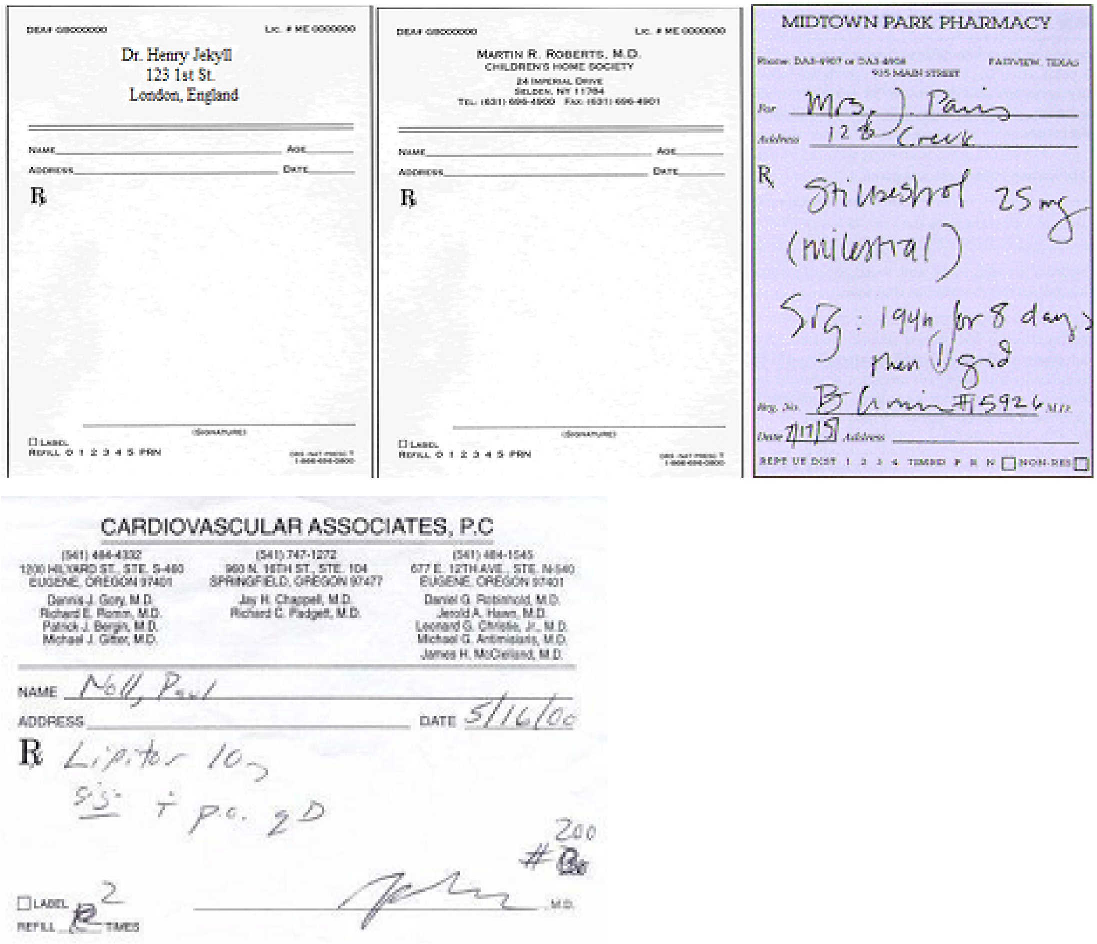
First, the excel file "Those who owes.xls" contains details of the names of buyers, what they are buying, and how much the buyers owe Mantooth. This file has credibility of being owned by Mantooth because this file was found on his person at the time of the traffic stop and an exact copy is also in the Wes Mantooth user of his computer. Due to files being on Mantooth at the time of his arrest also being on the Mantooth user on his computer, Wes Mantooth has to have access to the account called Wes Mantooth. A copy of the file can be found under "Thumbdrive.E01/FAMILY PIX [FAT32]/[root]/Bidness Docs/Those who owes.xls" and on the Desktop of the Wes Mantooth user. This file also has a shortcut located in the Recent folder of the same user at "Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Roaming/Microsoft/Windows/Recent/Those who owes.xls.lnk". This shows the intent for Wes Mantooth to frequently access and modify the information found within the excel document.



Dudes Name	What	$$$
Little Timmy	Mth	$600.00
Big John	Special K	$250.00
John Washer	H	$250.00
Frank the Tank	H	$5,000.00
Sam I AM	Marijuana	$100.00
Mac Daddy	Special K	$200.00
Mr Freeze	Special K	$698.42
Methalotapus	Mth	$555.00
megamethamous	Mth	$250.00
Simple Simon	Marijuana	$698.00

Figure 38: Image containing the full “Those who owes.xls” document.

Secondly, the Wes Mantooth user contains four images of scanned prescriptions. Two of the prescriptions are already pre-signed by a doctor and have the potential to be used to acquire prescription drugs via a forged prescription. Because of the previously established link between Wes Mantooth the person and Wes Mantooth the user, it can be said that Wes gathered these images himself in some capacity. All four images are found under the Wes Mantooth user in a dedicated folder for fake prescriptions at “Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Documents\Scripts”.



DEA# G8000000 Lic. # ME 0000000

Dr. Henry Jekyll
123 1st St.
London, England

NAME________ AGE____
ADDRESS________ DATE____

℞

(SIGNATURE)

□ LABEL
REFILL 0 1 2 3 4 5 PRN

DEA# G8000000 Lic. # ME 0000000

MARTIN R. ROBERTS, M.D.
CHILDREN'S HOME SOCIETY
24 IMPERIAL DRIVE
SELDEN, NY 11784
TEL: (631) 696-4900 FAX: (631) 696-4901

NAME________ AGE____
ADDRESS________ DATE____

℞

(SIGNATURE)

□ LABEL
REFILL 0 1 2 3 4 5 PRN

MIDTOWN PARK PHARMACY

Phone: DA3-4907 or DA3-4908 FAIRVIEW, TEXAS
935 MAIN STREET

For Mrs. J. Paris
Address 12 Creek

R Stilbestrol 25 mg
(milestral)

S/G: 1 q4h for 8 days
then 1 qid

Reg. No. B Lamin #15926 M.D.
Date 7/17/5 Address

REPT UP DIST 1 2 3 4 TIMED P R N □ NON-RES □

CARDIOVASCULAR ASSOCIATES, P.C

(541) 484-4332
1200 HILYARD ST., STE. S-480
EUGENE, OREGON 97401
Dennis J. Gory, M.D.
Richard E. Romm, M.D.
Patrick J. Bergin, M.D.
Michael J. Gitter, M.D.

(541) 747-1272
960 N. 16TH ST., STE. 104
SPRINGFIELD, OREGON 97477
Jay H. Chappell, M.D.
Richard C. Padgett, M.D.

(541) 484-1545
677 E. 12TH AVE., STE. N-540
EUGENE, OREGON 97401
Daniel G. Robinhold, M.D.
Jerold A. Hawn, M.D.
Leonard G. Christie, Jr., M.D.
Michael G. Antimisiaris, M.D.
James H. McClelland, M.D.

NAME Noll, Paul
ADDRESS________ DATE 5/16/00

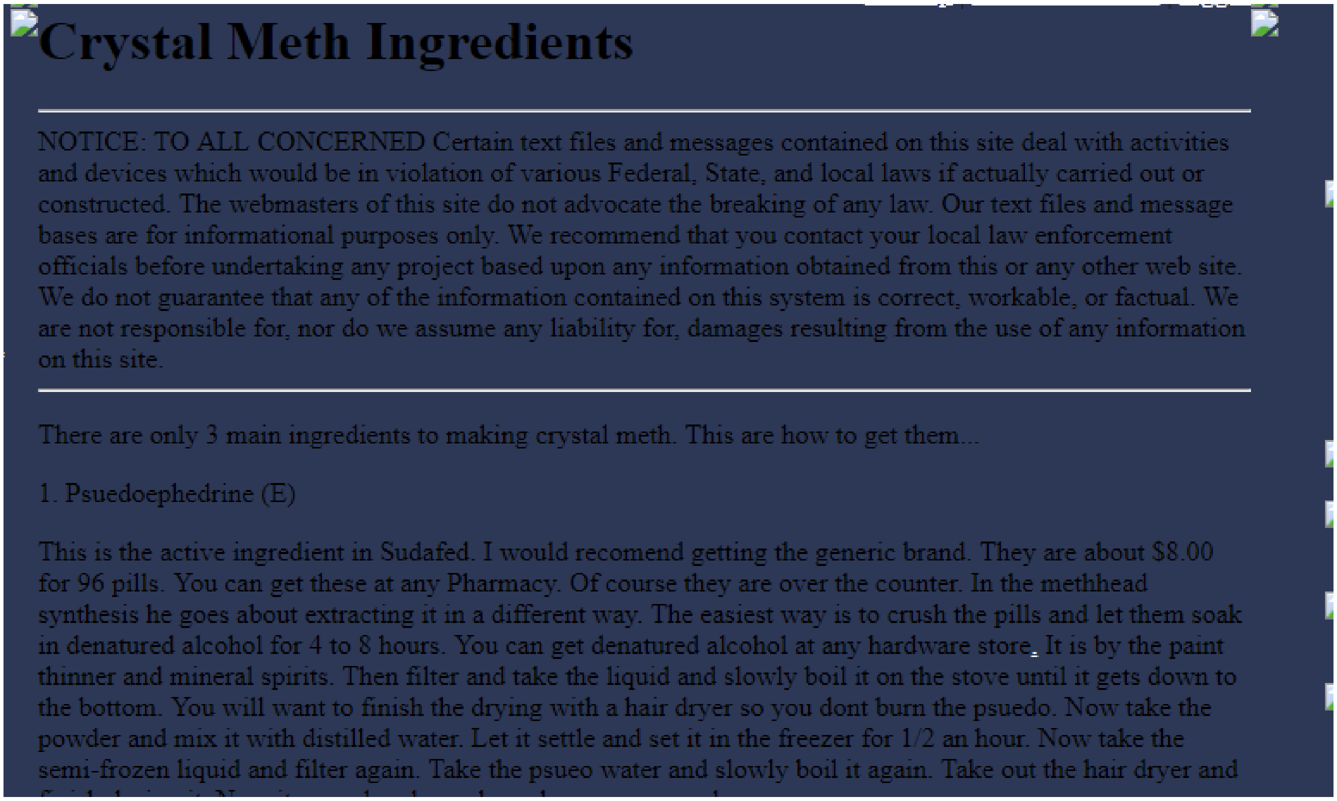
℞ Lipitor 10mg
S.S. i p.o. qD

#200

□ LABEL
REFILL 2 TIMES
M.D.

Figure 39: Contains a collection of images that are fraudulent prescription notes.

The third piece of evidence linking Wes Mantooth to drug possession is the html file of a website that teaches readers how to make meth in great detail. This meth making guide is found in a folder called “Mr Smee” inside of the user under the control of Mantooth. This file can be found specifically at “Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Documents/Mr Smee/165183.html”.



Crystal Meth Ingredients

NOTICE: TO ALL CONCERNED Certain text files and messages contained on this site deal with activities and devices which would be in violation of various Federal, State, and local laws if actually carried out or constructed. The webmasters of this site do not advocate the breaking of any law. Our text files and message bases are for informational purposes only. We recommend that you contact your local law enforcement officials before undertaking any project based upon any information obtained from this or any other web site. We do not guarantee that any of the information contained on this system is correct, workable, or factual. We are not responsible for, nor do we assume any liability for, damages resulting from the use of any information on this site.

There are only 3 main ingredients to making crystal meth. This are how to get them...

1. Psuedoephedrine (E)

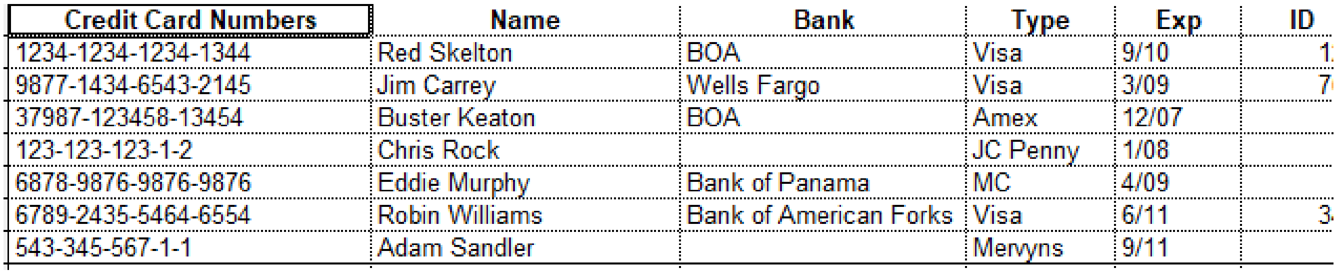
This is the active ingredient in Sudafed. I would recomend getting the generic brand. They are about $8.00 for 96 pills. You can get these at any Pharmacy. Of course they are over the counter. In the methhead synthesis he goes about extracting it in a different way. The easiest way is to crush the pills and let them soak in denatured alcohol for 4 to 8 hours. You can get denatured alcohol at any hardware store. It is by the paint thinner and mineral spirits. Then filter and take the liquid and slowly boil it on the stove until it gets down to the bottom. You will want to finish the drying with a hair dryer so you dont burn the psuedo. Now take the powder and mix it with distilled water. Let it settle and set it in the freezer for 1/2 an hour. Now take the semi-frozen liquid and filter again. Take the psueo water and slowly boil it again. Take out the hair dryer and

Figure 40: Image contains an excerpt from a PDF containing direction on how to make meth.

Financial Fraud

There are many pieces of evidence connecting Wes Mantooth to active fraud regarding credit cards, check washing, as well as car title fraud. Mantooth can be linked to credit card fraud and check washing due to the large amount of information regarding how to commit the fraud and information about past fraud found on the user under Mantooth's control.

The first piece of evidence linking Mantooth to credit card fraud is the excel file called "CC Nums.xls" in which collected credit cards have all of their information stored. This file is stored in the user under Mantooth's control at "Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Documents/EFS DOCS/CC Nums.xls".



Credit Card Numbers	Name	Bank	Type	Exp	ID
1234-1234-1234-1344	Red Skelton	BOA	Visa	9/10	1
9877-1434-6543-2145	Jim Carrey	Wells Fargo	Visa	3/09	7
37987-123458-13454	Buster Keaton	BOA	Amex	12/07	
123-123-123-1-2	Chris Rock		JC Penny	1/08	
6878-9876-9876-9876	Eddie Murphy	Bank of Panama	MC	4/09	
6789-2435-5464-6554	Robin Williams	Bank of American Forks	Visa	6/11	3
543-345-567-1-1	Adam Sandler		Mervyns	9/11	

Figure 41: Image contains a section of the excel database containing stolen credit card information.

The second piece of evidence linking Mantooth to credit card fraud is a pair of images depicting credit card skimmers being applied to an ATM and a view of a skimmer’s inner mechanism. Both of these images can be found on the thumb drive on Mantooth at the time of the arrest at “Thumbdrive.E01/FAMILY PIX [FAT32]/[root]/Business Ideas” and are named “Cover Plate.bmp” and “Guts.bmp”.

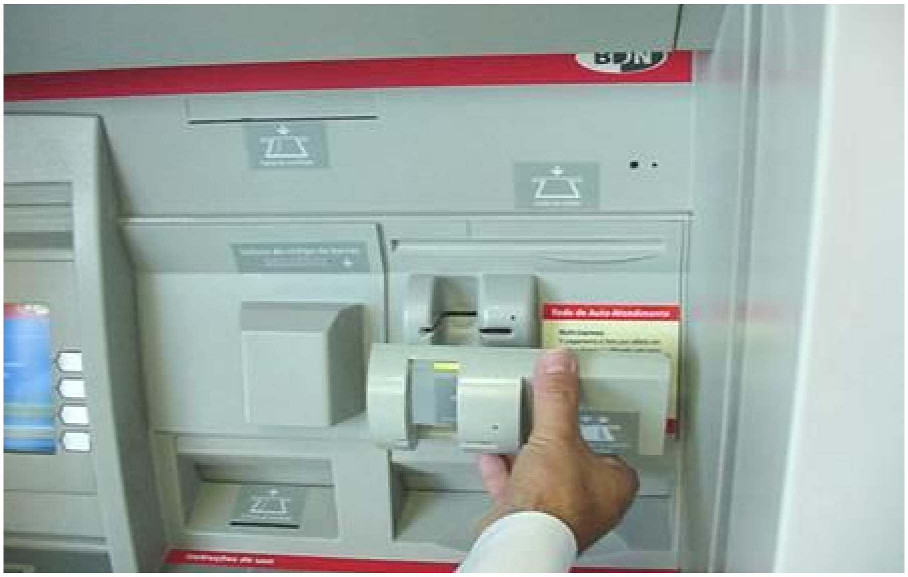


Figure 42: Image details a card skimmer being installed on an ATM.

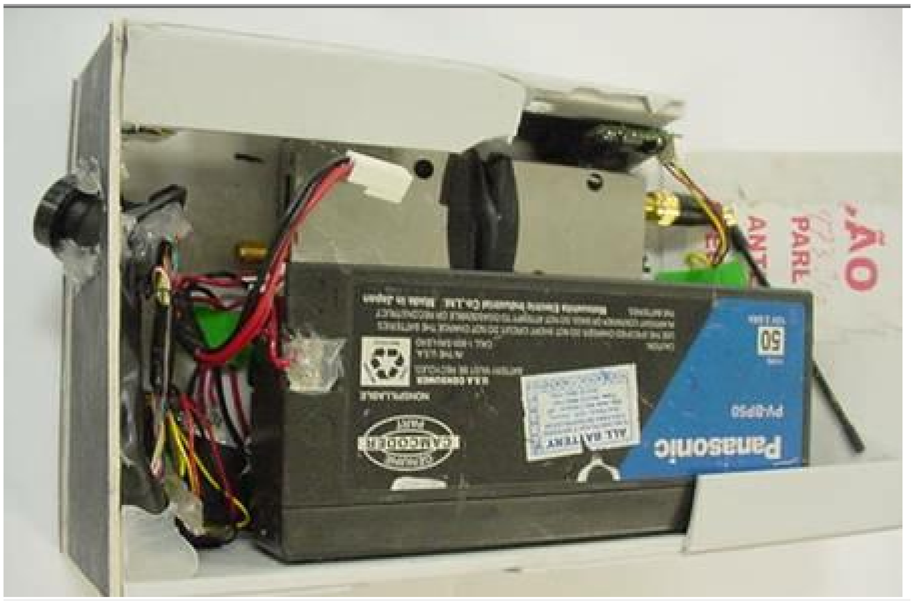
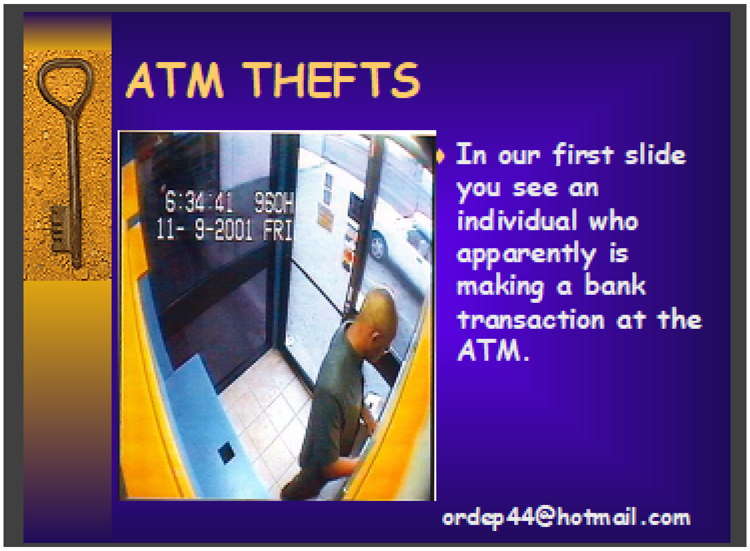


Figure 43: Image contains a view of the inner mechanism of a card skimmer.

The next pieces of evidence links Mantooth to check fraud. The first image is of the first slide of a PowerPoint presentation taken from Mantooth’s thumb drive on how to steal from people using a bank’s ATM located at “Thumbdrive.E01/FAMILY PIX [FAT32]/[root]/Business Ideas/ATM_THEFTS1.ppt”. The second image is of a calendar reminder that is set to remind Wes Mantooth to “Go check stealing”. The third image is of another calendar reminder set to “wash checks”. These reminders show a clear intention to commit more acts of fraud than have already been committed by acquiring full credit card information. The file to the reminder can be found at “Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Outlook/Outlook.pst»Personal Folders»Top of Personal Folders»Calendar»Go check stealing”.

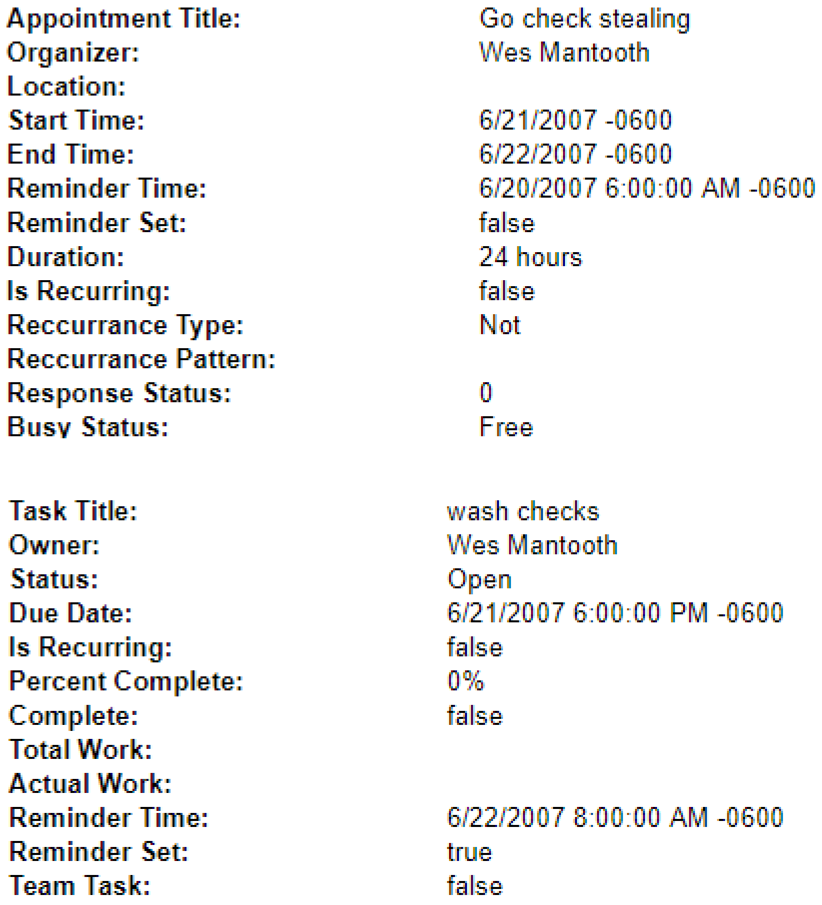


ATM THEFTS

- In our first slide you see an individual who apparently is making a bank transaction at the ATM.

ordep44@hotmail.com

Figure 44: Image depicts one slide from a presentation about ATM theft.



Appointment Title:	Go check stealing
Organizer:	Wes Mantooth
Location:	
Start Time:	6/21/2007 -0600
End Time:	6/22/2007 -0600
Reminder Time:	6/20/2007 6:00:00 AM -0600
Reminder Set:	false
Duration:	24 hours
Is Recurring:	false
Reccurrance Type:	Not
Reccurrance Pattern:	
Response Status:	0
Busy Status:	Free

Task Title:	wash checks
Owner:	Wes Mantooth
Status:	Open
Due Date:	6/21/2007 6:00:00 PM -0600
Is Recurring:	false
Percent Complete:	0%
Complete:	false
Total Work:	
Actual Work:	
Reminder Time:	6/22/2007 8:00:00 AM -0600
Reminder Set:	true
Team Task:	false

Figure 45: Collection of just two images about the reminders in the calendar.

The third piece of evidence is the folder called “Checks” Inside the folder contains many blank or pre-signed checks. Below are a few of the images of checks stored in that folder which is located at “Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Documents/Checks/Check1.png”.

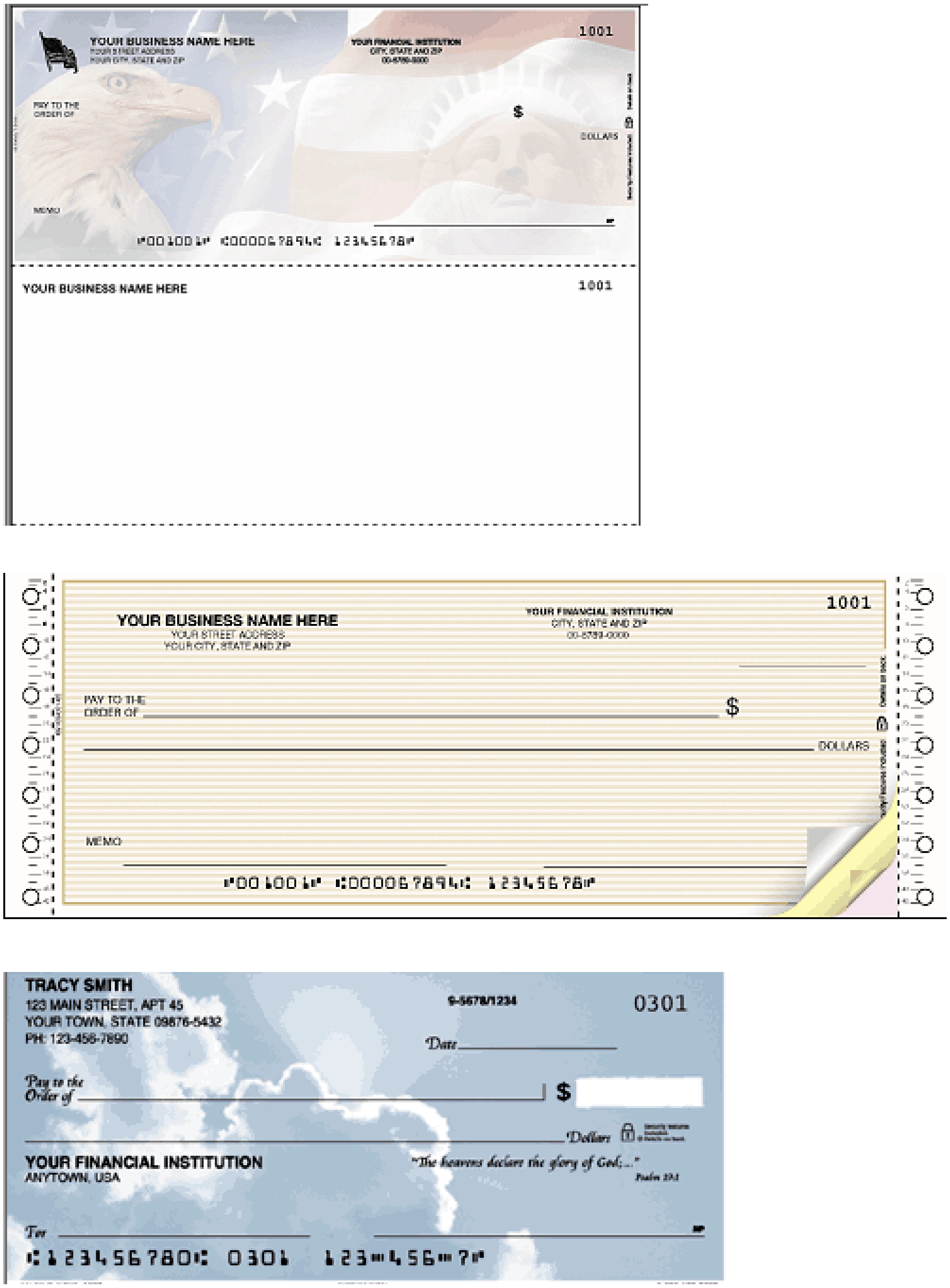
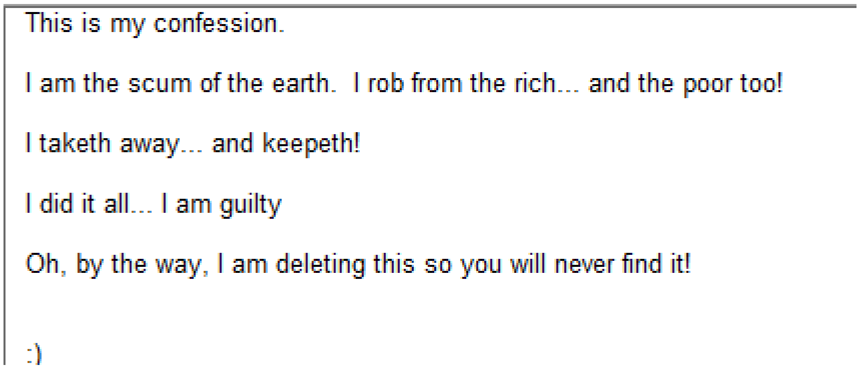


Figure 46: Contains a collection of images depicting three blank checks.

Next, Mantooth confesses that he is guilty of theft in a deleted text file found on his desktop called “My Confession.txt” which is pictured below. The file with the confession is found at “Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Desktop/Stuff to Delete/My Confession.txt”.



This is my confession.

I am the scum of the earth. I rob from the rich... and the poor too!

I taketh away... and keepeth!

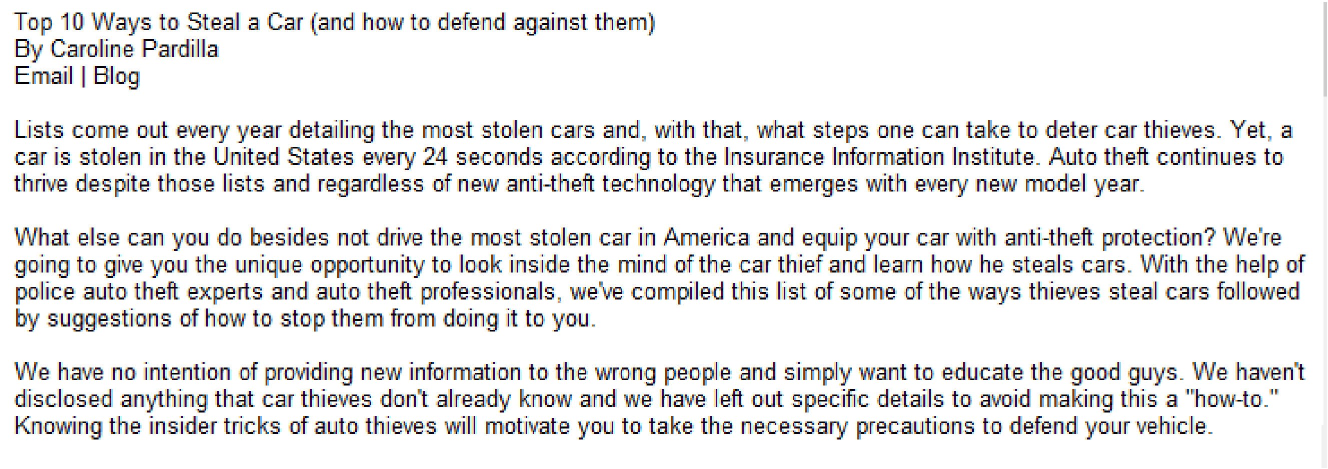
I did it all... I am guilty

Oh, by the way, I am deleting this so you will never find it!

:)

Figure 47: Image showing the text file of Wes Mantooth's confession.

Lastly, Mantooth is shown to have interest in stealing cars and carrying car titles in other people’s names. The following image contains a long text file, found in the storage partition of Mantooth’s Hard Drive, about an article on how to steal cars. The text of the article can be found at “Mantooth.E01/Partition 2/NONAME [Ext2]/[root]/Stuff/How to Steal Cars.txt”. The image following the article is of one of the car titles found at “Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Documents/Car Titles” called “67chev.jpg”. This Car Titles folder is found in the user profile under Wes Mantooth’s control.



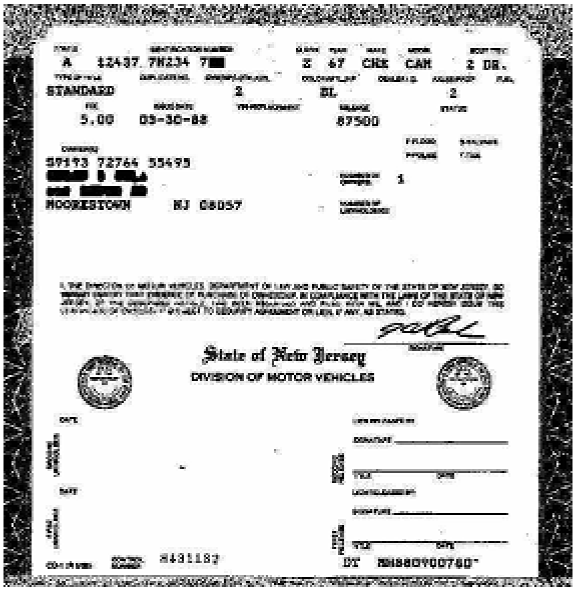
Top 10 Ways to Steal a Car (and how to defend against them)
By Caroline Pardilla
Email | Blog

Lists come out every year detailing the most stolen cars and, with that, what steps one can take to deter car thieves. Yet, a car is stolen in the United States every 24 seconds according to the Insurance Information Institute. Auto theft continues to thrive despite those lists and regardless of new anti-theft technology that emerges with every new model year.

What else can you do besides not drive the most stolen car in America and equip your car with anti-theft protection? We're going to give you the unique opportunity to look inside the mind of the car thief and learn how he steals cars. With the help of police auto theft experts and auto theft professionals, we've compiled this list of some of the ways thieves steal cars followed by suggestions of how to stop them from doing it to you.

We have no intention of providing new information to the wrong people and simply want to educate the good guys. We haven't disclosed anything that car thieves don't already know and we have left out specific details to avoid making this a "how-to." Knowing the insider tricks of auto thieves will motivate you to take the necessary precautions to defend your vehicle.

Figure 48: Image showing an excerpt from the article 'Top 10 Ways to Steal a Car'.



A 12437 7H234 7[redacted] Z 67 CHE CAM 2 DR.

STANDARD 2 BL 2

5.00 03-30-88 87500

S7173 72764 55493

[redacted]

MOORESTOWN NJ 08057

1

I, THE DIRECTOR OF MOTOR VEHICLES, DEPARTMENT OF LAW AND PUBLIC SAFETY OF THE STATE OF NEW JERSEY, DO HEREBY CERTIFY THAT EVIDENCE OF PURCHASE OF OWNERSHIP, IN COMPLIANCE WITH THE LAWS OF THE STATE OF NEW JERSEY, OF THE DESCRIBED VEHICLE, HAS BEEN RECEIVED AND FILED WITH ME, AND I DO HEREBY ISSUE THIS CERTIFICATE OF OWNERSHIP SUBJECT TO SECURITY AGREEMENT OR LIEN, IF ANY, AS STATED.

State of New Jersey

DIVISION OF MOTOR VEHICLES

DATE

DATE

8431182

DT NH880900780

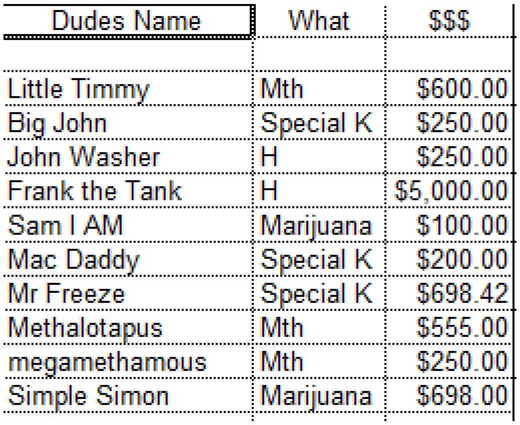
Figure 49: Image showing a fraudulent car title.

John Washer

Drug Possession

There are a few files that point to John Washer being in the possession of illegal drugs. These files led to John Washer acquiring these drugs by purchasing them from Wes Mantooth, creating them, and trading for them.

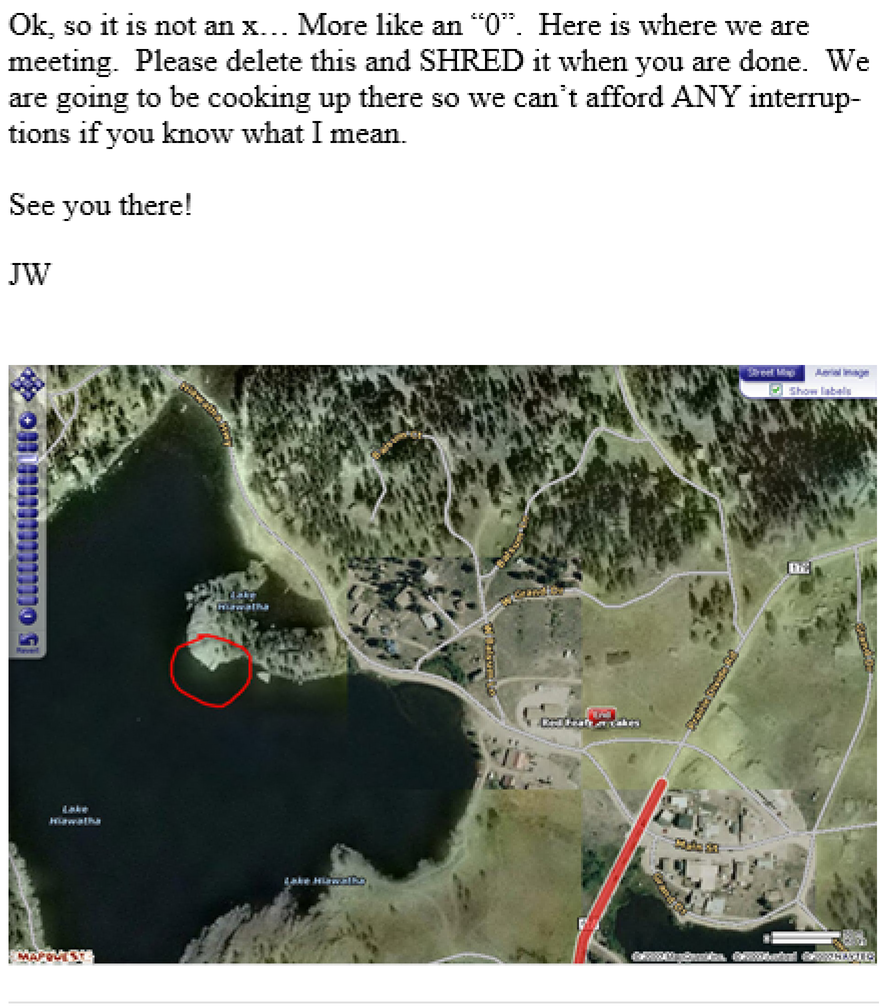
The first example of drug possession is from purchasing heroin from Wes Mantooth as detailed in the document “Those who owes.xls” found in Mantooth’s thumb drive. The file details that Wes Mantooth sold John Washer heroin and that Washer owes Mantooth $250 for the sale. The document itself can be found at “Thumbdrive.E01/FAMILY PIX [FAT32]/[root]/Bidness Docs/Those who owes.xls”.



Dudes Name	What	$$$
Little Timmy	Mth	$600.00
Big John	Special K	$250.00
John Washer	H	$250.00
Frank the Tank	H	$5,000.00
Sam I AM	Marijuana	$100.00
Mac Daddy	Special K	$200.00
Mr Freeze	Special K	$698.42
Methalotapus	Mth	$555.00
megamethamous	Mth	$250.00
Simple Simon	Marijuana	$698.00

Figure 50: Image showing to contents of the excel database called 'Those who owes.xls'.

The second example of drug possession by Washer comes from the document title “X marks the spot.doc”. The document shows an email message to Wes Mantooth inviting him to partake in “cooking” some substance. This substance could be Meth as Wes Mantooth had acquired a document teaching readers how to create the drug. The document itself can be found at “Washer.E01/Partition 1/WASHER [NTFS]/[root]/Documents and Settings/Administrator/My Documents/X marks the spot.doc”.



Ok, so it is not an x… More like an "0". Here is where we are meeting. Please delete this and SHRED it when you are done. We are going to be cooking up there so we can't afford ANY interruptions if you know what I mean.

See you there!

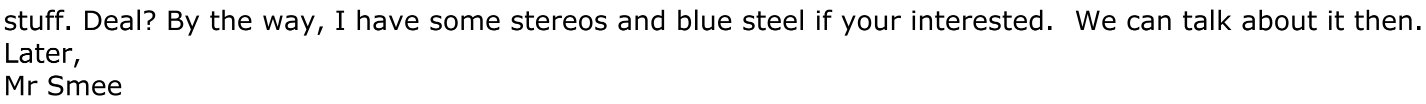
JW

Figure 51: Image depicts an aerial view of the meeting location discovered in file 'X marks the spot.doc'.

The third way John Washer could be in possession of illegal drugs is from a conversation with someone named "Mr Smee" over email in which Mr Smee suggests trading substances. This file can be found at "Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Windows Mail/Local Folders/Sent Items/3F687E04-00000001.eml".

From:	"Mr Smee" <smee.rox@gmail.com>
Sent:	4/10/2007 3:03:28 PM -0600
To:	chkwasher@comcast.net
Subject:	A trade

So, what do you say we trade a few blanks for some of the good stuff? I am going to be in your town next week and we could hook up for the trade. Don't bother sending me the ones with security. I want the easy



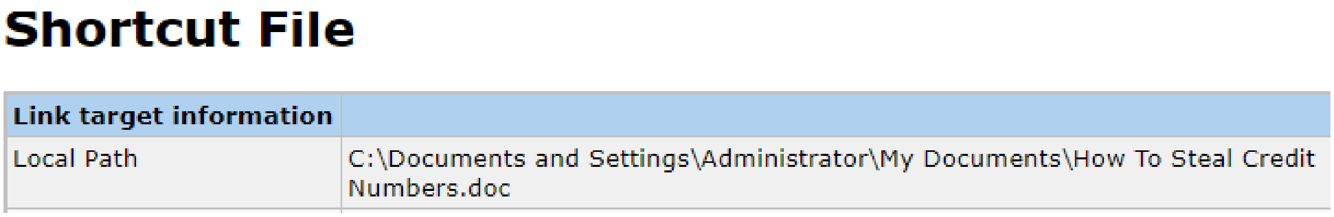
stuff. Deal? By the way, I have some stereos and blue steel if your interested. We can talk about it then.
Later,
Mr Smee

Figure 52: Image depicts an aerial view of the meeting location discovered in file 'X marks

Financial Fraud

There are also files supporting that Washer is in on the same credit fraud scheme as Mantooth is and can be supported by files pertaining to credit card printing and guides on how to steal credit cards.

The following image is taken of the shortcut file of a document called "How to Steal Credit Numbers.doc" which was retrieved from the Recent folder of the Administrator account. This supports that this file is regularly accessed by the user. This link file is seen at "Washer.E01/Partition 1/WASHER [NTFS]/[root]/Documents and Settings/Administrator/Recent/How To Steal Credit Numbers.doc.lnk".



Shortcut File

Link target information	
Local Path	C:\Documents and Settings\Administrator\My Documents\How To Steal Credit Numbers.doc

Figure 53: Image depiction of the link file created for 'How To Steal Credit Number.doc".

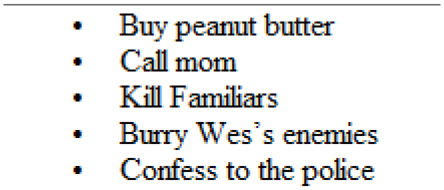
The following image is taken from a document called "Card_Printing_101.pdf" and can be found at "Washer.E01/Partition 1/WASHER [NTFS]/[root]/Documents and Settings/Administrator/Local Settings/Application Data/Identities/{6B6FD541-F2AF-4EFB-AF50-EC531BF02474}/Microsoft/Outlook Express/Sent Items.dbx»Re: Me and my woman.eml»Card_Printing_101.pdf".

Introduction

Photo Identification Cards

Figure 54: Image depicts a single page excerpt for the file 'Card_Printing_101.pdf"

Just like in Mantooth's computer, there is also a confession of guilt found in Washer's computer. The following image is of a document called "Washers To Do List.doc" and details a list of five tasks to be done with the fifth task being "Confess to the police". This document can be viewed at "Washer.E01/Partition 1/WASHER [NTFS]/[root]/Documents and Settings/Administrator/Desktop/Stuff/Washers To Do List.doc.doc".



- Buy peanut butter
- Call mom
- Kill Familiars
- Burry Wes's enemies
- Confess to the police

Figure 55: Image depicting the whole "To Do List.doc"

Other Ties between Mantooth and Washer

The following email chain supports that Mantooth and Washer frequently trade with each other for illegal substances such as prescription drugs and ketamine. Email chain can be found at "Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Outlook/Outlook.pst»Personal Folders»Top of Personal Folders»Sent Items»RE: Whats up in D town?".

From:	Wes Mantooth <dollarhyde86@comcast.net>
Sent:	6/21/2007 3:06:36 PM -0600
To:	'John Washer' <chkwasher@comcast.net>
Subject:	RE: Whats up in D town?
Attachments:	doc-prescription.jpg

Your crazy! You are going to blow your self up! I am sticking with my method…

I horked another today from the pharm counter… this lady is a mess. She just leaves this stuff lying around! ☺

From: John Washer [mailto:chkwasher@comcast.net]
Sent: Thursday, June 21, 2007 12:02 PM
To: Wes Mantooth
Subject: Re: Whats up in D town?

Very nice... forget percriptions... This is the way to go!

http://www.totse.com/en/drugs/speedy_drugs/howtomanufactu172921.html

----- Original Message -----

From: Wes Mantooth

To: 'John Washer'

Sent: Thursday, June 21, 2007 12:00 PM

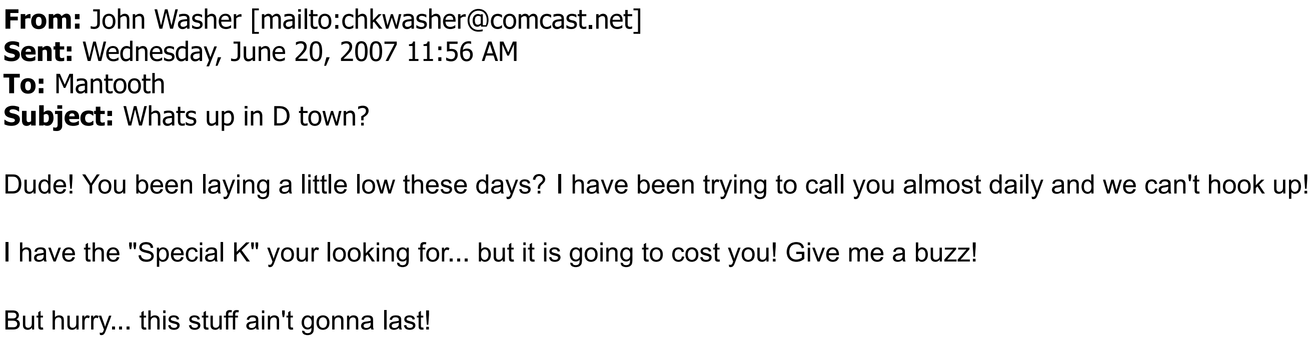
Subject: RE: Whats up in D town?

Sorry man. I have been a little under the weather lately. Too much party!

Yea, I am good to go… same time and place. I am hot on the trail of some good scripts…

Check this one out! I need to do a little editing on the type and quantity… but it shouldn't be a problem

Later



From: John Washer [mailto:chkwasher@comcast.net]
Sent: Wednesday, June 20, 2007 11:56 AM
To: Mantooth
Subject: Whats up in D town?

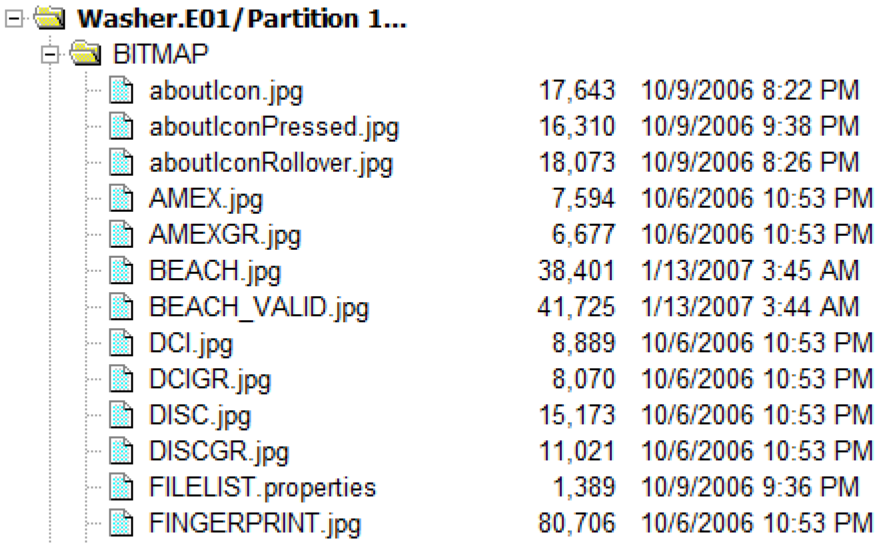
Dude! You been laying a little low these days? I have been trying to call you almost daily and we can't hook up!

I have the "Special K" your looking for... but it is going to cost you! Give me a buzz!

But hurry... this stuff ain't gonna last!

Figure 56: Image depicts email exchange between John Washer and Wes Mantooth.

The exact same file of a credit card validating program can be found on both Washer’s computer under the user Administrator and the recycling bin of Wes Mantooth’s user on his own computer. The file can be found at “Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/$RNHBWN2.zip” on Mantooth’s computer and at “Washer.E01/Partition 1/WASHER [NTFS]/[root]/Documents and Settings/Administrator/Desktop/Stuff/ValidateCreditCard.jar” on Washer’s computer.

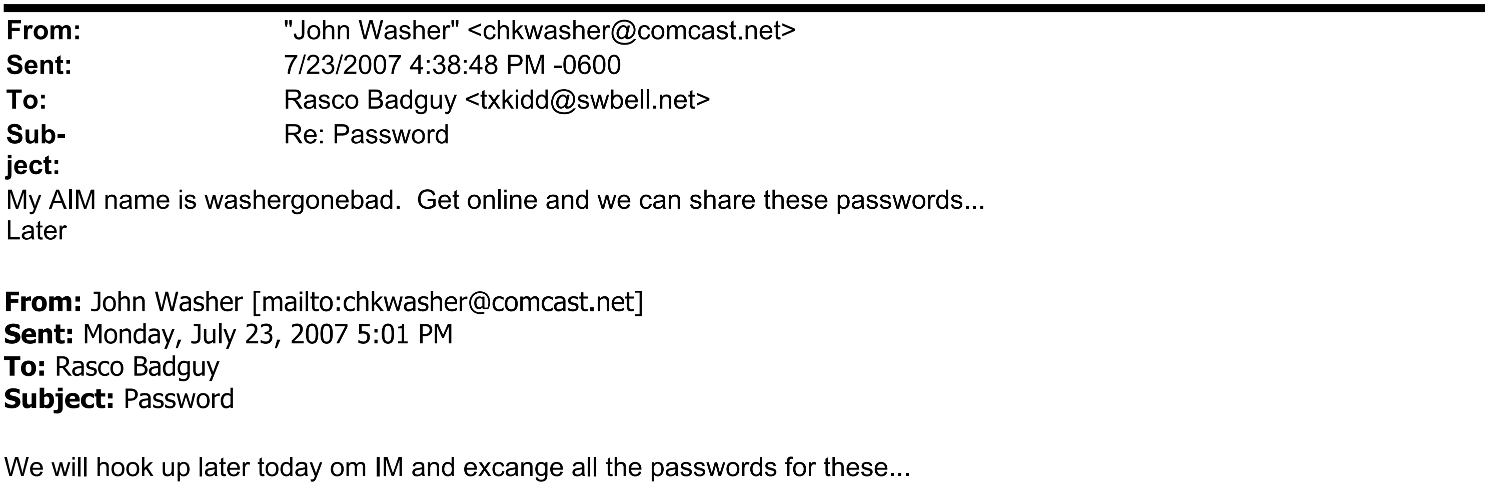


```
Washer.E01/Partition 1...
  BITMAP
    aboutIcon.jpg              17,643   10/9/2006 8:22 PM
    aboutIconPressed.jpg       16,310   10/9/2006 9:38 PM
    aboutIconRollover.jpg      18,073   10/9/2006 8:26 PM
    AMEX.jpg                    7,594   10/6/2006 10:53 PM
    AMEXGR.jpg                  6,677   10/6/2006 10:53 PM
    BEACH.jpg                  38,401   1/13/2007 3:45 AM
    BEACH_VALID.jpg            41,725   1/13/2007 3:44 AM
    DCI.jpg                     8,889   10/6/2006 10:53 PM
    DCIGR.jpg                   8,070   10/6/2006 10:53 PM
    DISC.jpg                   15,173   10/6/2006 10:53 PM
    DISCGR.jpg                 11,021   10/6/2006 10:53 PM
    FILELIST.properties         1,389   10/9/2006 9:36 PM
    FINGERPRINT.jpg            80,706   10/6/2006 10:53 PM
```

Figure 57: Image contains a piece of the ZIP file that is found on both hard drives.

It is also likely that Washer and Mantooth have ties outside of what is recorded on their computers as Mantooth has had two programs called FileZilla and Kazaa installed on his computer which are peer-to-peer file sharing programs and Washer has an AOL Instant

Messenger account and has been spreading his contact info. Traces of these two programs having been installed before can be found in “”. The following email shows that Washer has been using his AIM account. This email chain can be found at “Washer.E01/Partition 1/WASHER [NTFS]/[root]/Documents and Settings/Administrator/Local Settings/Application Data/Identities/{6B6FD541-F2AF-4EFB-AF50-EC531BF02474}/Microsoft/Outlook Express/Sent Items.dbx»Re: Password.eml”.



From:	"John Washer" <chkwasher@comcast.net>
Sent:	7/23/2007 4:38:48 PM -0600
To:	Rasco Badguy <txkidd@swbell.net>
Subject:	Re: Password

My AIM name is washergonebad. Get online and we can share these passwords...
Later

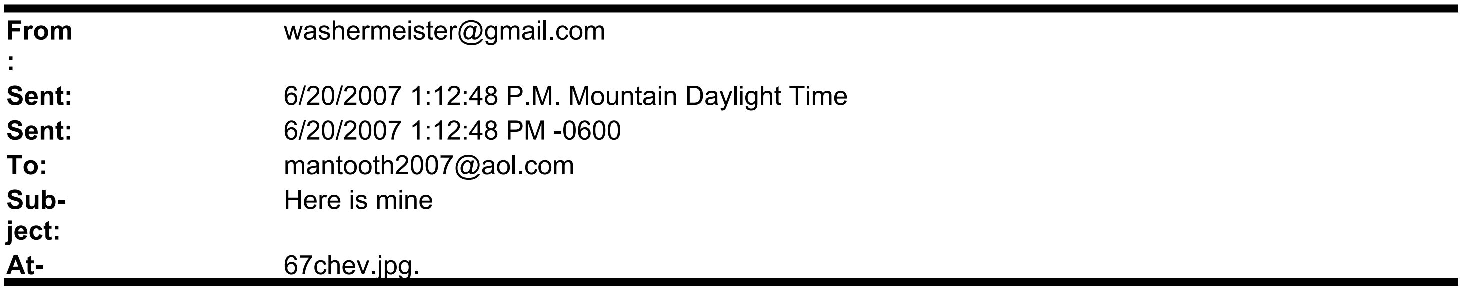
From: John Washer [mailto:chkwasher@comcast.net]
Sent: Monday, July 23, 2007 5:01 PM
To: Rasco Badguy
Subject: Password

We will hook up later today om IM and excange all the passwords for these...

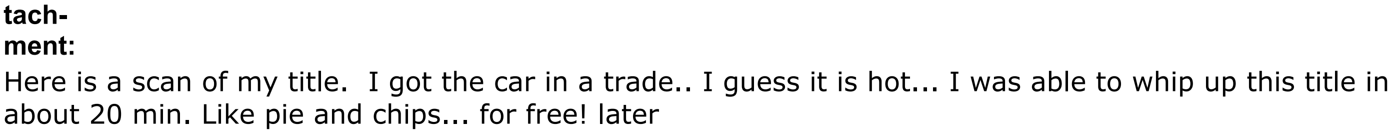
Figure 58: Image contains an email exchange between Rasco and John Washer.

Supporting Personal Emails

This email supports that Wes Mantooth has access to the email address “mantooth2007@aol.com” because a copy of 67chev.jpg can be found on the Wes Mantooth user profile. Email found at “Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/ProgramData/AOL/C_AOL 9.0a/organize/mantooth2007»mantooth2007»Mail»Incoming⁄Saved Mail»6⁄20⁄2007 washermeister@gm Here is mine”



From:	washermeister@gmail.com
Sent:	6/20/2007 1:12:48 P.M. Mountain Daylight Time
Sent:	6/20/2007 1:12:48 PM -0600
To:	mantooth2007@aol.com
Subject:	Here is mine
At-	67chev.jpg.



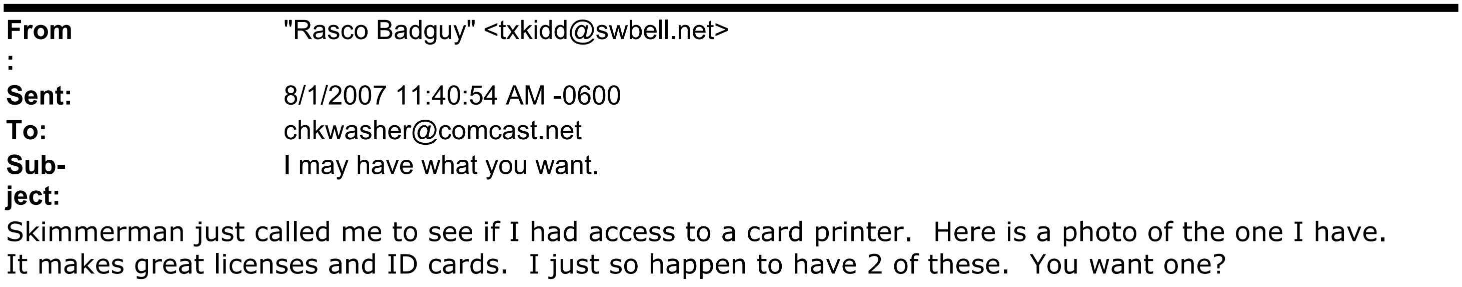
tachment:

Here is a scan of my title. I got the car in a trade.. I guess it is hot... I was able to whip up this title in about 20 min. Like pie and chips... for free! later

Figure 59: Image contains an email that contains a JPG attachment.

The calendar found at “Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Outlook/Outlook.pst»Personal Folders»Top of Personal Folders»Calendar” has three reminders for the user Wes Mantooth set by the email “Wes Mantooth <dollarhyde86@comcast.net>". This supports that Wes Mantooth has access to this email address.

This email supports that “chkwasher@comcast.net” is accessible by John Washer as a credit card printer would be useless to someone who didn’t have a credit card activator program. Therefore, expressing interest to have a card printer supports that the email chkwasher@comcast.net is accessible by John Washer. Email found at “Washer.E01/Partition 1/WASHER [NTFS]/[root]/Documents and Settings/Administrator/Local Settings/Application Data/Identities/{6B6FD541-F2AF-4EFB-AF50-EC531BF02474}/Microsoft/Outlook Express/Inbox.dbx»I may have what you want.”

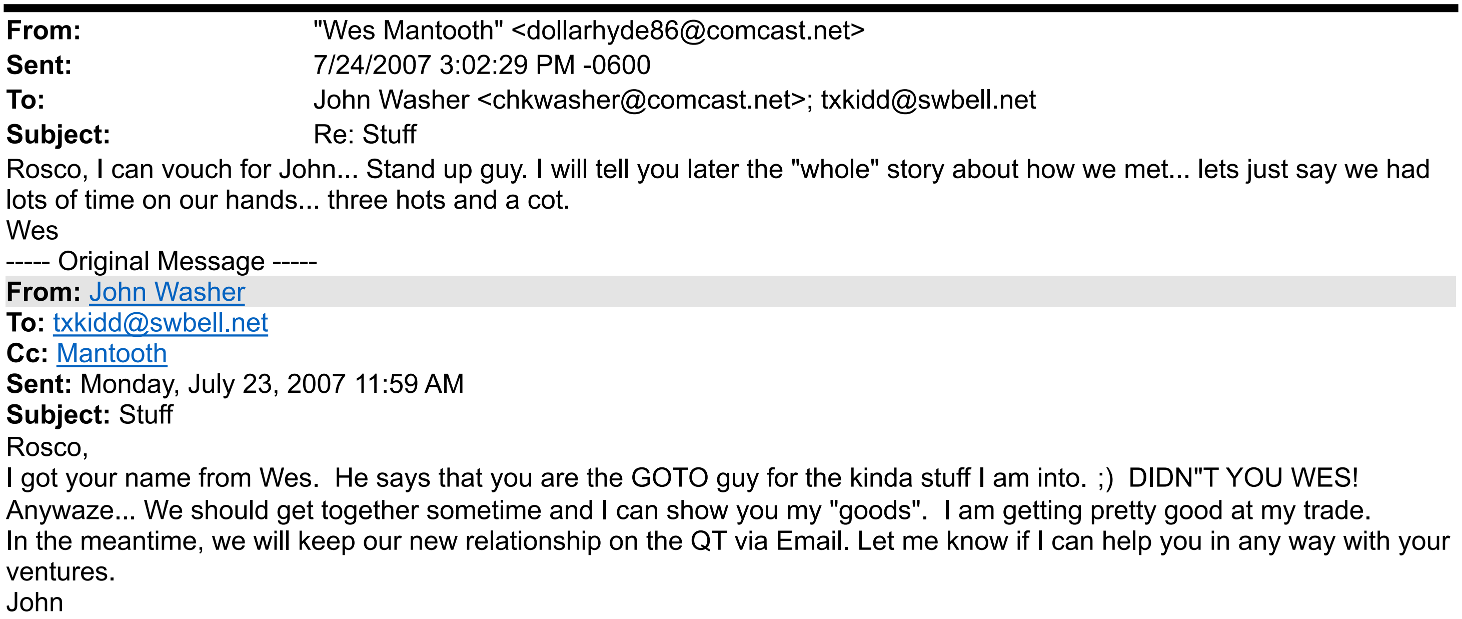


From:	"Rasco Badguy" <txkidd@swbell.net>
Sent:	8/1/2007 11:40:54 AM -0600
To:	chkwasher@comcast.net
Subject:	I may have what you want.

Skimmerman just called me to see if I had access to a card printer. Here is a photo of the one I have. It makes great licenses and ID cards. I just so happen to have 2 of these. You want one?

Figure 60: Image contains a piece of the ZIP file that is found on both hard drives.

This email implicates that “dollarhyde86@comcast.net” is Wes Mantooth and chkwasher@comcast.net is John Washer because the two are calling each other by their first names and are acting as if they are friends in person. “Washer.E01/Partition 1/WASHER [NTFS]/[root]/Documents and Settings/Administrator/Local Settings/Application Data/Identities/{6B6FD541-F2AF-4EFB-AF50-EC531BF02474}/Microsoft/Outlook Express/Inbox.dbx»Re: Stuff”.



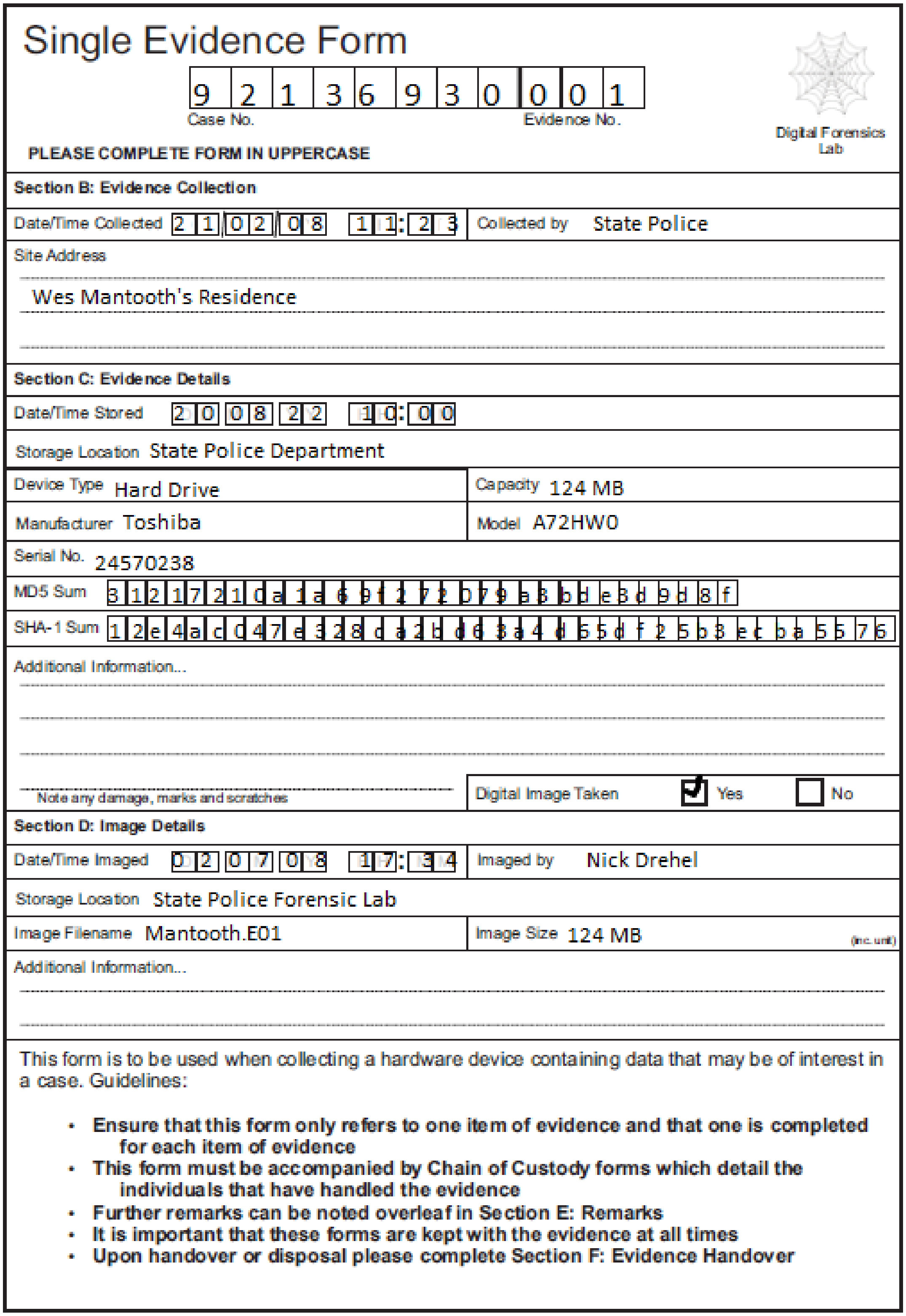
From: "Wes Mantooth" <dollarhyde86@comcast.net>
Sent: 7/24/2007 3:02:29 PM -0600
To: John Washer <chkwasher@comcast.net>; txkidd@swbell.net
Subject: Re: Stuff

Rosco, I can vouch for John... Stand up guy. I will tell you later the "whole" story about how we met... lets just say we had lots of time on our hands... three hots and a cot.
Wes
----- Original Message -----
From: John Washer
To: txkidd@swbell.net
Cc: Mantooth
Sent: Monday, July 23, 2007 11:59 AM
Subject: Stuff

Rosco,
I got your name from Wes. He says that you are the GOTO guy for the kinda stuff I am into. ;) DIDN"T YOU WES!
Anywaze... We should get together sometime and I can show you my "goods". I am getting pretty good at my trade.
In the meantime, we will keep our new relationship on the QT via Email. Let me know if I can help you in any way with your ventures.
John

Figure 61: Image depicting an email conversion between Wes Mantooth and John Washer.

Chain of Custody



Single Evidence Form

Case No.	9 2 1 3 6 9 3 0
Evidence No.	0 0 1

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 21/02/08 11:23	Collected by State Police

Site Address

Wes Mantooth's Residence

Section C: Evidence Details

Date/Time Stored 20/08/22 10:00

Storage Location State Police Department

Device Type Hard Drive	Capacity 124 MB
Manufacturer Toshiba	Model A72HW0

Serial No. 24570238

MD5 Sum 3 1 2 1 7 2 1 0 a 1 a 6 9 f 2 7 2 0 7 9 a 3 b d e 3 d 9 d 8 f

SHA-1 Sum 1 2 e 4 a c 0 4 7 e 3 2 8 c a 2 b d 6 3 a 4 d 5 5 d f 2 5 b 3 e c b a 5 5 7 6

Additional Information...

Note any damage, marks and scratches	Digital Image Taken ☑ Yes □ No

Section D: Image Details

Date/Time Imaged 02/07/08 17:34	Imaged by Nick Drehel

Storage Location State Police Forensic Lab

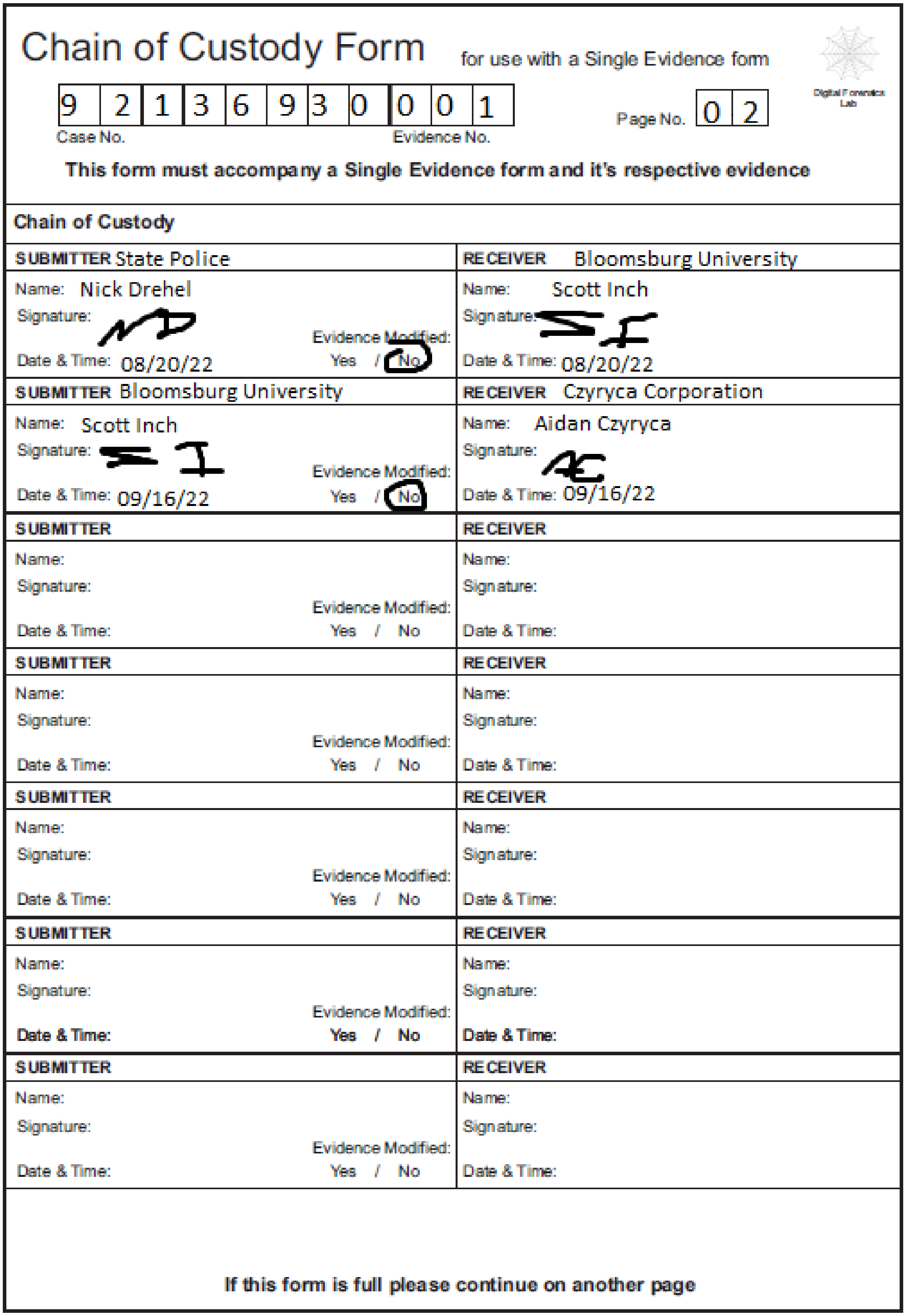
Image Filename Mantooth.E01	Image Size 124 MB (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Figure 62: Single Evidence Form for Mantooth Hard Drive.



Chain of Custody Form

for use with a Single Evidence form

Digital Forensics Lab

Case No. 9 2 1 3 6 9 3 0   Evidence No. 0 0 1

Page No. 0 2

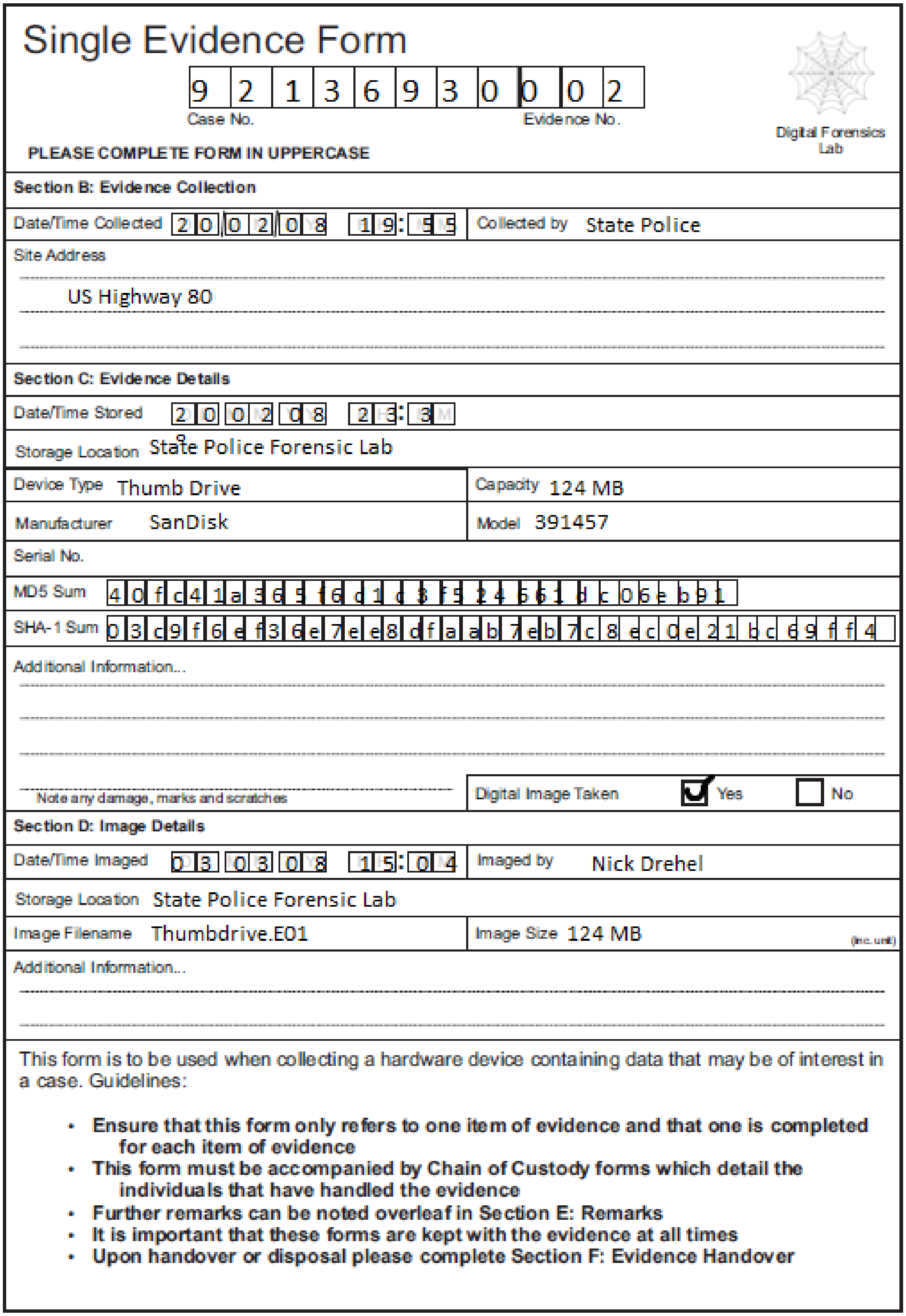
This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER State Police	**RECEIVER** Bloomsburg University
Name: Nick Drehel Signature: ND Evidence Modified: Date & Time: 08/20/22 Yes / [✓ No]	Name: Scott Inch Signature: SI Date & Time: 08/20/22
SUBMITTER Bloomsburg University	**RECEIVER** Czyryca Corporation
Name: Scott Inch Signature: SI Evidence Modified: Date & Time: 09/16/22 Yes / [✓ No]	Name: Aidan Czyryca Signature: AC Date & Time: 09/16/22
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: **Date & Time: Yes / No**	Name: Signature: **Date & Time:**
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:

If this form is full please continue on another page

Figure 63: Chain of Custody Form for Mantooth Hard Drive.



Single Evidence Form

9 2 1 3 6 9 3 0 0 0 2

Case No. Evidence No.

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 2 0 0 2 0 8 1 9 : 5 5

Collected by State Police

Site Address

US Highway 80

Section C: Evidence Details

Date/Time Stored 2 0 0 2 0 8 2 3 : 3

Storage Location State Police Forensic Lab

Device Type Thumb Drive

Capacity 124 MB

Manufacturer SanDisk

Model 391457

Serial No.

MD5 Sum 4 0 f c 4 1 a 3 6 5 f 6 d 1 c 3 f 5 2 4 6 6 1 d c 0 6 e b 9 1

SHA-1 Sum 0 3 c 9 f 6 e f 3 6 e 7 e e 8 d f a a b 7 e b 7 c 8 e c 0 e 2 1 b c 6 9 f f 4

Additional Information...

Note any damage, marks and scratches

Digital Image Taken ☑ Yes □ No

Section D: Image Details

Date/Time Imaged 0 3 0 3 0 8 1 5 : 0 4

Imaged by Nick Drehel

Storage Location State Police Forensic Lab

Image Filename Thumbdrive.E01

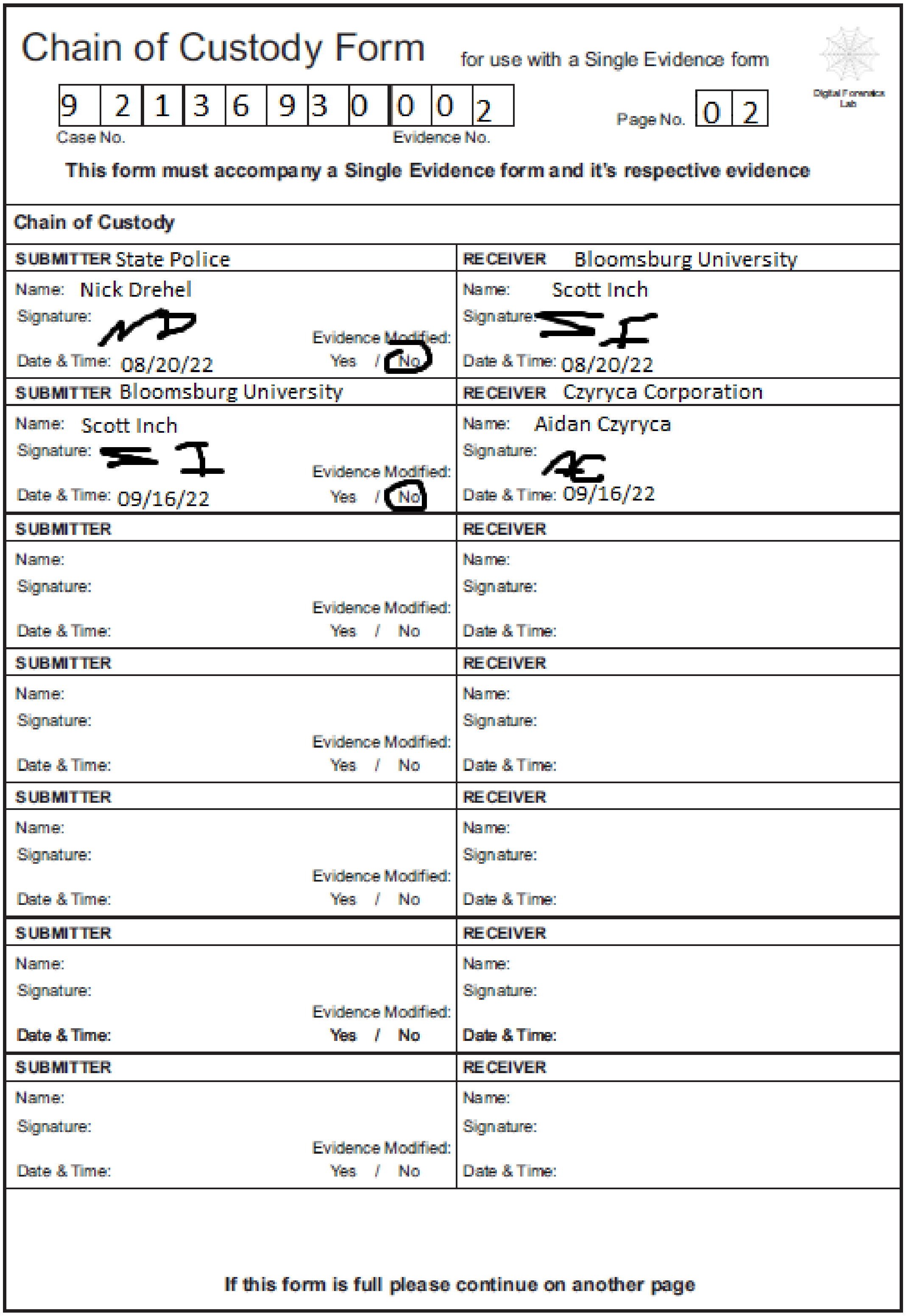
Image Size 124 MB (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Figure 64: Single Evidence Form for Mantooth Thumb Drive.



Chain of Custody Form for use with a Single Evidence form

Digital Forensics Lab

9	2	1	3	6	9	3	0	0	0	2

Case No. Evidence No.

Page No. 0 2

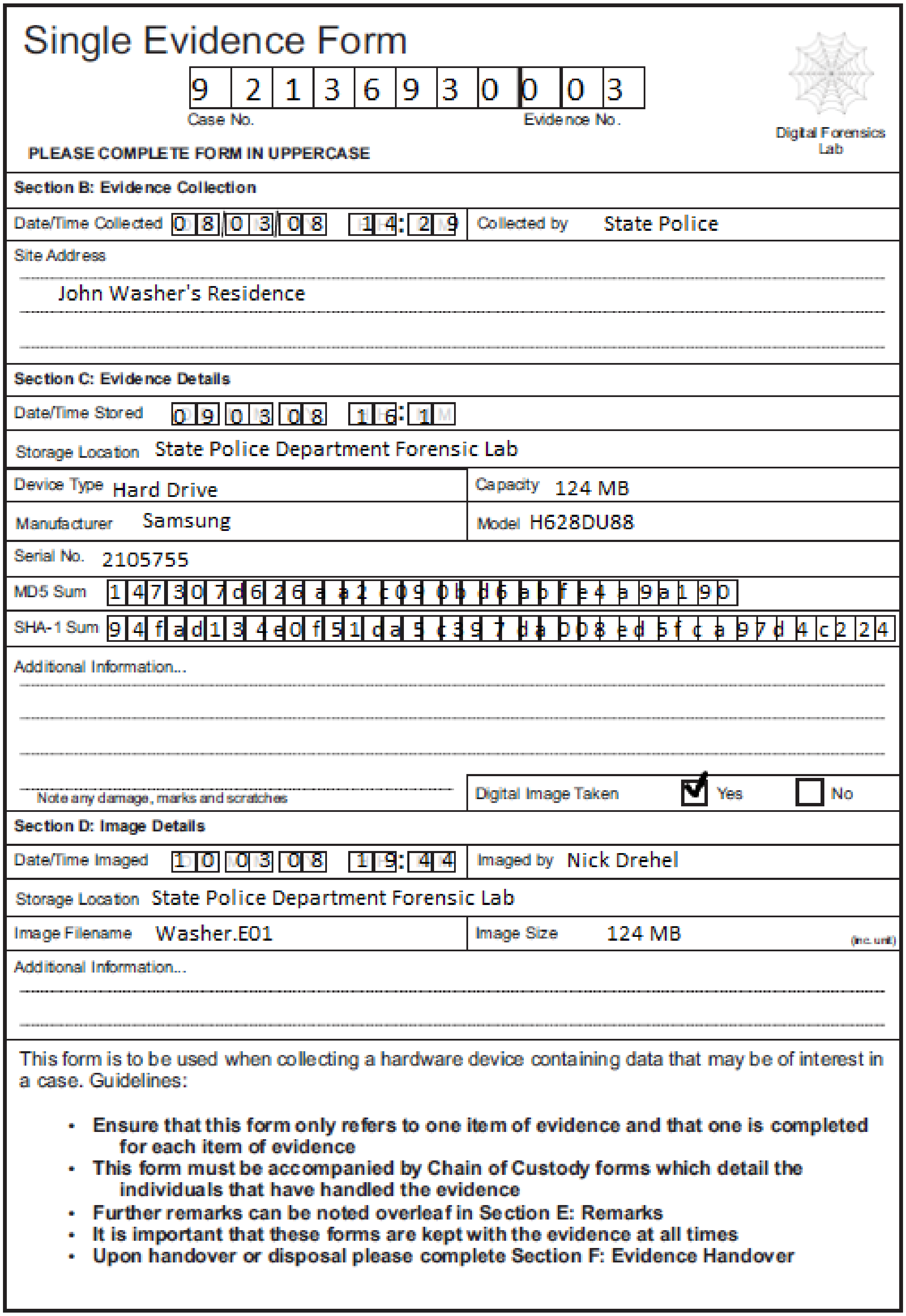
This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER State Police	**RECEIVER** Bloomsburg University
Name: Nick Drehel Signature: ND Evidence Modified: Date & Time: 08/20/22 Yes / [✓ No]	Name: Scott Inch Signature: SI Date & Time: 08/20/22
SUBMITTER Bloomsburg University	**RECEIVER** Czyryca Corporation
Name: Scott Inch Signature: SI Evidence Modified: Date & Time: 09/16/22 Yes / [✓ No]	Name: Aidan Czyryca Signature: AC Date & Time: 09/16/22
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: **Date & Time:** **Yes / No**	Name: Signature: **Date & Time:**
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:

If this form is full please continue on another page

Figure 65: Chain of Custody Form for Mantooth Thumb Drive.



Single Evidence Form

Case No. 9 2 1 3 6 9 3 0 Evidence No. 0 0 3

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 08/03/08 14:29 Collected by State Police

Site Address

John Washer's Residence

Section C: Evidence Details

Date/Time Stored 09/03/08 16:1

Storage Location State Police Department Forensic Lab

Device Type Hard Drive Capacity 124 MB

Manufacturer Samsung Model H628DU88

Serial No. 2105755

MD5 Sum 147307d626aa2c090bd6abfe4a9a190

SHA-1 Sum 94fad134e0f51da5c397da008ed5fca97d4c224

Additional Information...

Note any damage, marks and scratches

Digital Image Taken ☑ Yes □ No

Section D: Image Details

Date/Time Imaged 10/03/08 19:44 Imaged by Nick Drehel

Storage Location State Police Department Forensic Lab

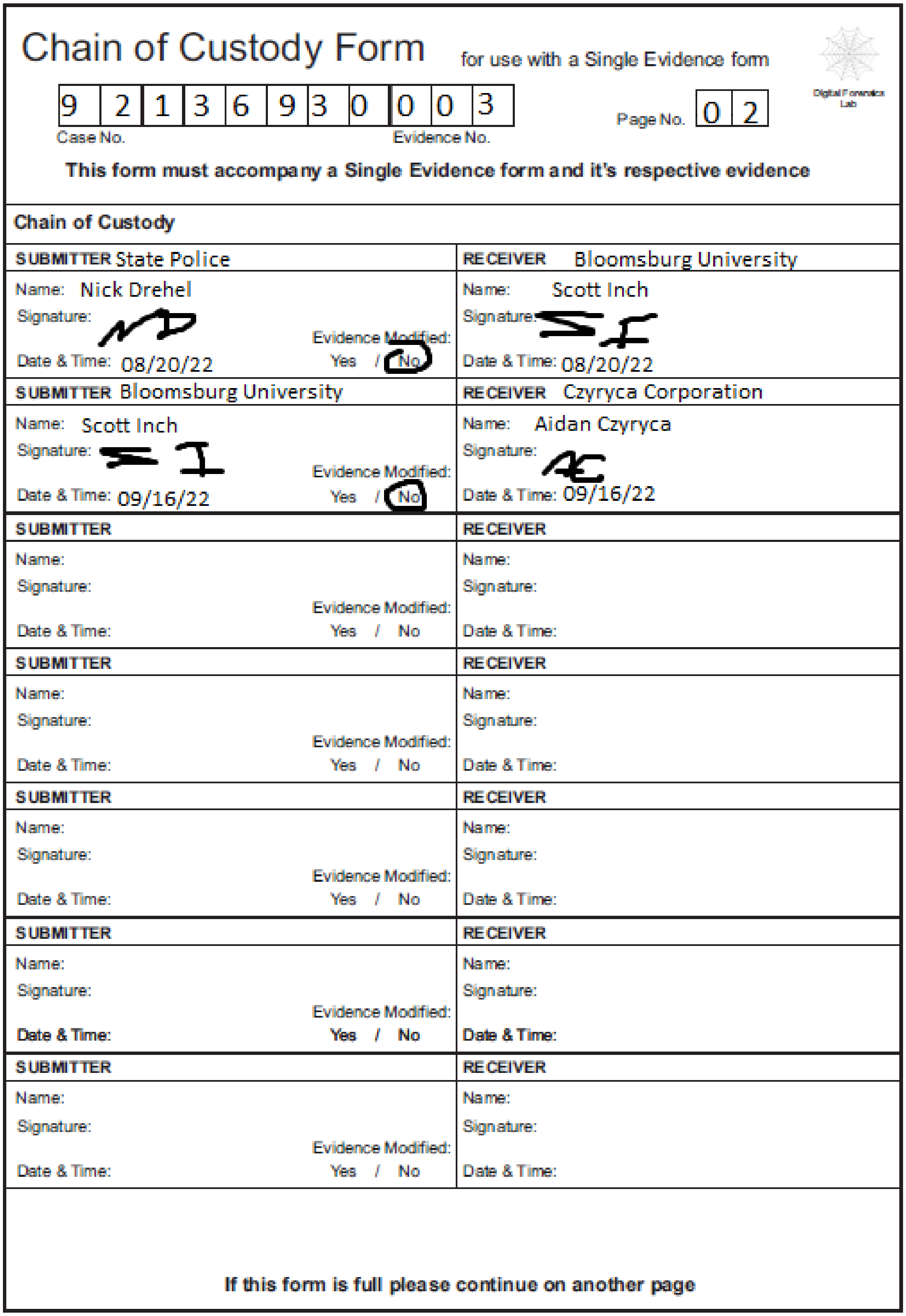
Image Filename Washer.E01 Image Size 124 MB (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Figure 66: Single Evidence Form for Washer Hard Drive.



Chain of Custody Form

for use with a Single Evidence form

Digital Forensics Lab

9	2	1	3	6	9	3	0	0	0	3

Case No. Evidence No.

Page No. 0 2

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER State Police	**RECEIVER** Bloomsburg University
Name: Nick Drehel Signature: ND Evidence Modified: Yes / [✓ No] Date & Time: 08/20/22	Name: Scott Inch Signature: SI Date & Time: 08/20/22
SUBMITTER Bloomsburg University	**RECEIVER** Czyryca Corporation
Name: Scott Inch Signature: SI Evidence Modified: Yes / [✓ No] Date & Time: 09/16/22	Name: Aidan Czyryca Signature: AC Date & Time: 09/16/22
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Yes / No Date & Time:	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Yes / No Date & Time:	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Yes / No Date & Time:	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Yes / No Date & Time:	Name: Signature: Date & Time:
SUBMITTER	**RECEIVER**
Name: Signature: Evidence Modified: Yes / No Date & Time:	Name: Signature: Date & Time:

If this form is full please continue on another page

Figure 67: Chain of Custody Form for Washer Hard Drive.

Conclusion

In this examination, I believe that the forensic images provided for analysis contain sufficient information to support that Wes Mantooth was involved in criminal activity, John Washer was involved in criminal activity, and that the two men were accomplices in some shared illegal actions. In the case of Wes Mantooth, there are many records found inside of devices and accounts in his possession that strongly supports the claim that he has possession of illegal substances and is actively commiting financial fraud. In the case of John Washer, there are enough records found inside of the device and accounts that are in his possession that support the claim that he has or recently had possession of illegal substances and was planning to commit financial fraud. Lastly, the two men were certainly knowledgable of and supported each other's illegal activities due to the large amount of recorded interation between the two and suspected interation that could not be explicitly recorded by the computers examined.