

Mantooth Investigation

Ferris State University

DFOR310

Dr. Hawkins

Alexis Cherpes

March 9, 2025

Table of Contents

Overview	4
Imaging the Hard Drive.....	4
FTK Imager	4
Presentation of Evidence	7
Forensic Explorer.....	7
Registry.....	9
SAM	13
Local User Parse	13
Software Hive	17
OS Install Date.....	17
Product Name and ID.....	18
Registered Owner/Organization	18
Uninstalled Programs (metadata)	19
System Hive.....	26
Computer Name	26
Shutdown Time	27
Time zone	27
USB Storage device (parsed).....	29
NTUser Hive.....	39
Explorer Recent Docs	39
Explorer Type Paths	39
Internet Explorer Typed URL's	40
MS Office MRU.....	40
Windows MRU	41
Active File Review	41
Axiom.....	41
Media	46
Web Searches.....	51

Passwords	54
User Accounts.....	55
Documents	58
Encryption and Credentials	62
Recycle Bin.....	63
Conclusion	64
Appendix of Terms	65

Overview

This investigation pertains to an ongoing criminal case involving John Washer, now with new evidence linked to Wes Mantooth. The case encompasses a range of illegal activities with significant implications for financial fraud, prescription drug abuse, and public health. Wes Mantooth's laptop was recently seized and submitted for forensic examination. This case remains active and sensitive due to its criminal nature.

Imaging the Hard Drive

FTK Imager

After lawfully seizing the suspect Wes Mantooth's laptop in connection with the John Washer case, the device was transported to a secured forensic lab. To ensure the integrity of the digital evidence, I utilized software called FTK Imager to create a forensic image of the laptop's hard drive. A verified clean and sterile hard drive was prepared in advance to store the disk image. The imaging process took around 10-15 minutes due to the size of the file and the low connection to my internet. Once it was done FTK Imager generated a drive verification report and an image summary. I documented the SHA1 and MD5 hash values. The hash values serve as a digital fingerprint for the image. We are creating a bit-by-bit copy of the original drive which ensures the preservation of the evidence on the drive. Figure 1.1 shows the hashes provided and below it is the image summary.

Drive/Image Verify Results	
<input type="checkbox"/>	
Name	Mantooth Evidence.E01
Sector count	250879
<input type="checkbox"/> MD5 Hash	
Computed hash	31217210a1a69f272079a3bde3d9d8fc
Stored verification hash	31217210a1a69f272079a3bde3d9d8fc
Report Hash	31217210a1a69f272079a3bde3d9d8fc
Verify result	Match
<input type="checkbox"/> SHA1 Hash	
Computed hash	12e4ac047e328ca2bd63a4d65df25b3ecba55769
Stored verification hash	12e4ac047e328ca2bd63a4d65df25b3ecba55769
Report Hash	12e4ac047e328ca2bd63a4d65df25b3ecba55769
Verify result	Match
<input type="checkbox"/> Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 1.1

Image Summary

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: Mantooth Investigation

Evidence Number: Mantooth #001

Unique Description:

Examiner: Alexis Cherpes

Notes:

Information for C:\Users\acher\OneDrive\Desktop\Cases\MantoothEvidence#001\Mantooth Evidence:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Verification Hashes]

MD5 verification hash: 31217210a1a69f272079a3bde3d9d8fc

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 250,879

[Image]

Image Type: E01

Case number:

Evidence number:

Examiner:

Notes:

Acquired on OS: Windows XP

Acquired using: FTKI2.5.3.14

Acquire date: 7/2/2008 9:09:34 PM

System date: 7/2/2008 9:09:34 PM

Unique description: untitled

Source data size: 122 MB

Sector count: 250879

[Computed Hashes]

MD5 checksum: 31217210a1a69f272079a3bde3d9d8fc

SHA1 checksum: 12e4ac047e328ca2bd63a4d65df25b3ecba55769

Image Information:

Acquisition started: Wed Mar 5 21:05:22 2025

Acquisition finished: Wed Mar 5 21:05:22 2025

Segment list:

C:\Users\acher\OneDrive\Desktop\Cases\MantoothEvidence#001\Mantooth Evidence.E01

COMPUTED HASH : 31217210a1a69f272079a3bde3d9d8fc

COMPUTED HASH : 12e4ac047e328ca2bd63a4d65df25b3ecba55769

Image Verification Results:

Verification started: Wed Mar 5 21:05:22 2025

Verification finished: Wed Mar 5 21:05:23 2025

MD5 checksum: 31217210a1a69f272079a3bde3d9d8fc : verified

SHA1 checksum: 12e4ac047e328ca2bd63a4d65df25b3ecba55769 : verified

Presentation of Evidence

Forensic Explorer

To begin the analysis of the forensic image captured from Wes Mantooth's laptop, I used Forensic Explorer. This is a tool that enables detailed examinations of digital artifacts all while keeping the original data. This guarantees that investigative measures are conducted in accordance with established forensic protocols. After starting the Forensic Explorer application, I created a new case file titled "MantoothInvestigation", shown in Figure 1.2. Once the case was initialized, I imported the disk image using the "Add Image" function and proceeded to mount the image by navigating the appropriate storage directory, as shown in Figure 1.3 and 1.4.

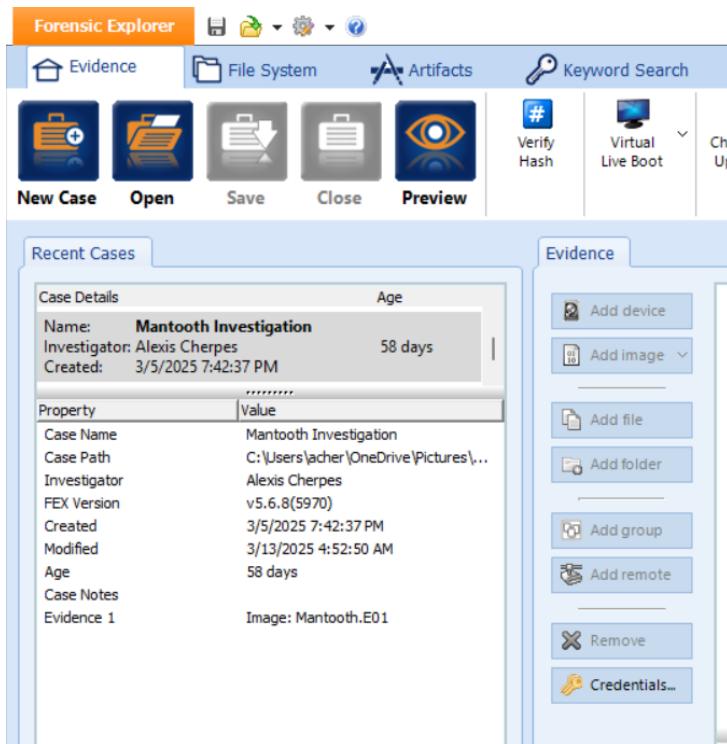


Figure 1.2

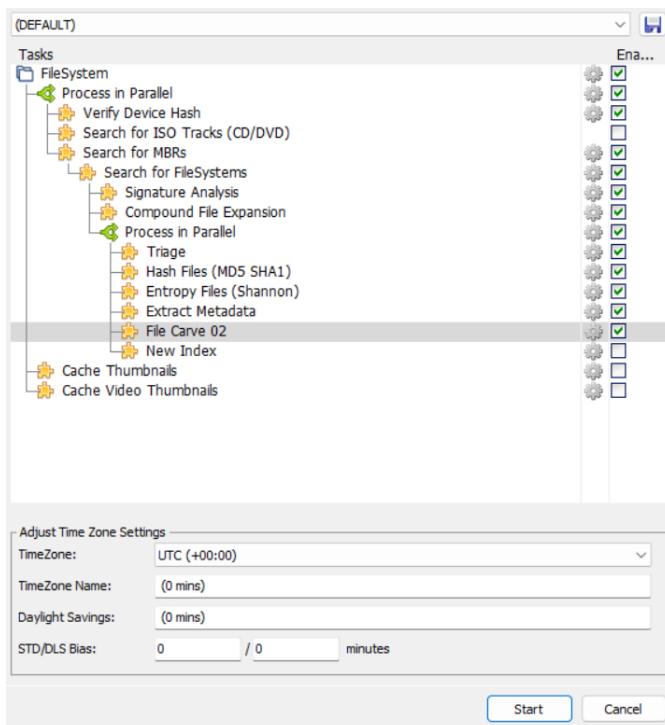


Figure 1.3

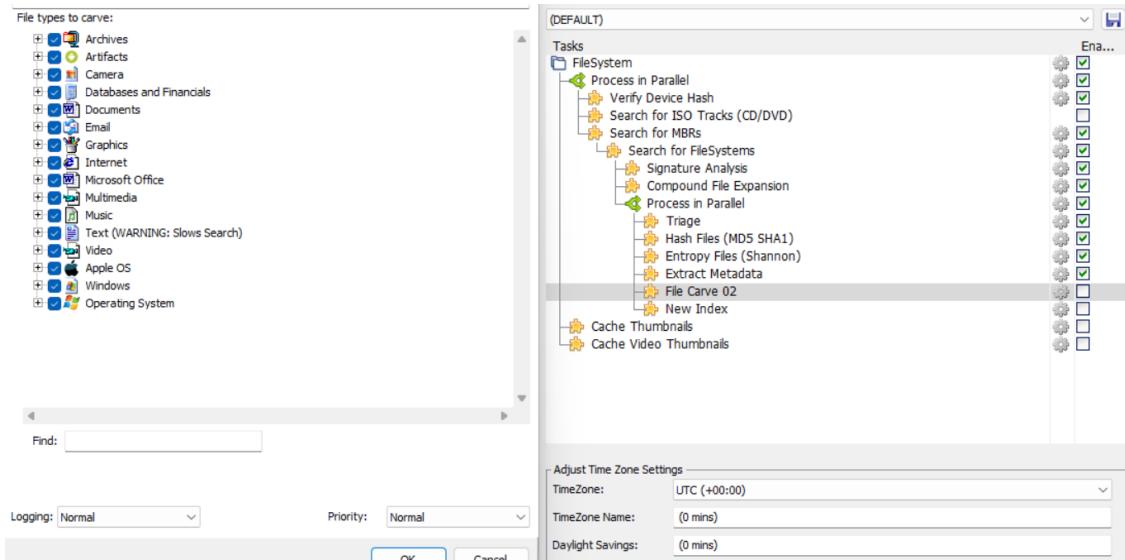


Figure 1.4

Registry

The Windows registry is a vital component in digital forensic investigations, especially when analyzing systems that happen to be running a Windows operating system. The registry contains a plethora of information including security settings, application data, system configurations, and user activity. The focus was placed on locating and analyzing four key registry hives. SAM, System, Software, and NTUser.dat. These hives are essential for reconstructing user behavior . As shown in Figures 1.5 and 1.6, I navigated from the Root directory then to the windows folder, then to the systems 32 folder, and finally reaching the config folder which should hold all those hive registries. SAM stands for Security Accounts Manager and it stores local user account names and encrypted password hashes. System contains operating system configuration data, this includes the computer name, startup settings, as well as hardware information. Software reveals details about the installed applications and the operating system installation date. Lastly, NTUser.dat provides user-specific information like

recent file access, software use and typed URLs. Figures 1.7 – 2.1 show the process of loading each hive into Forensic Explorer.

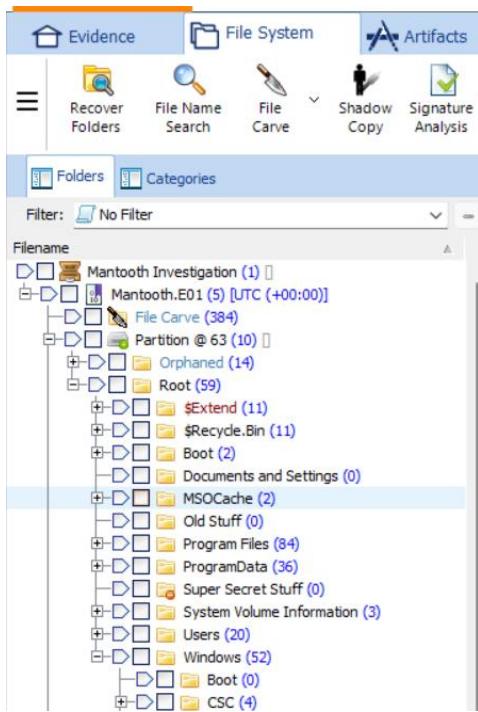


Figure 1.5

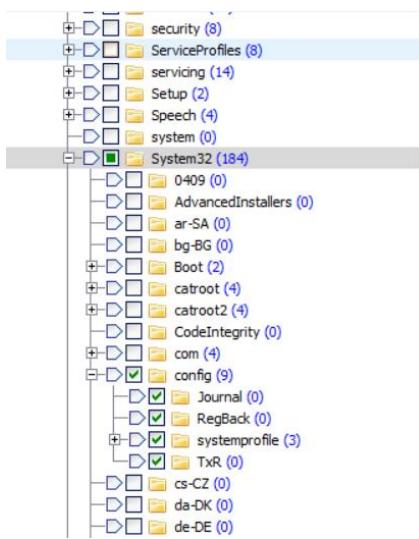


Figure 1.6

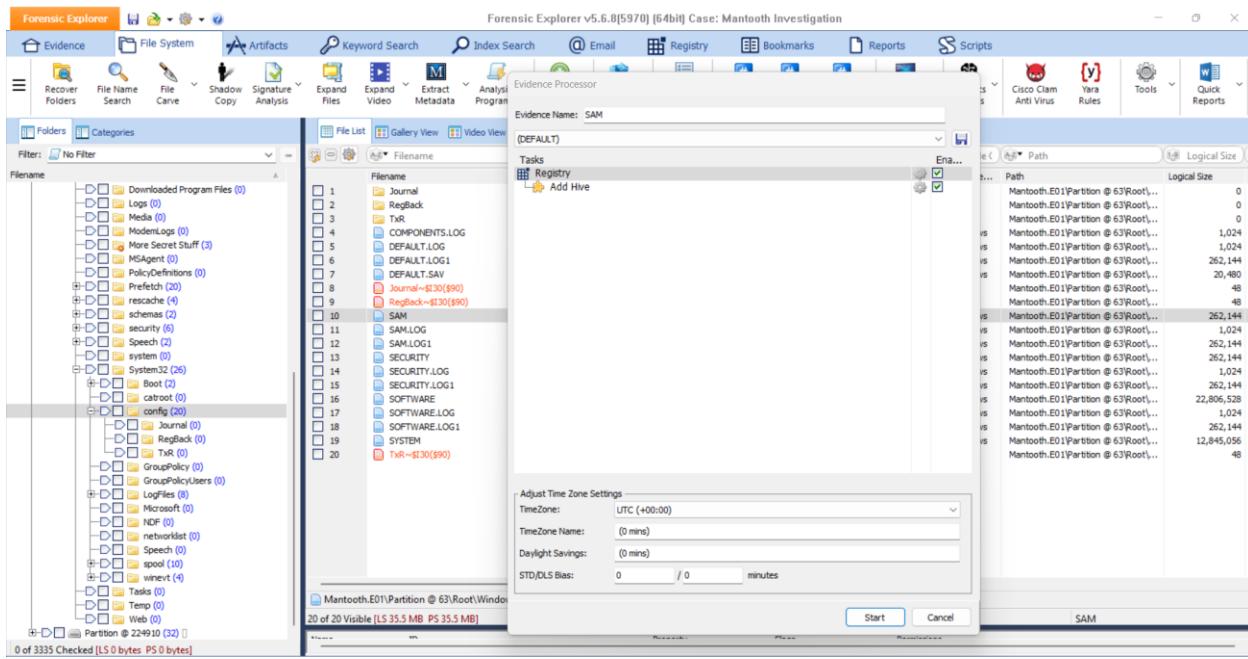


Figure 1.7 – SAM registry being added

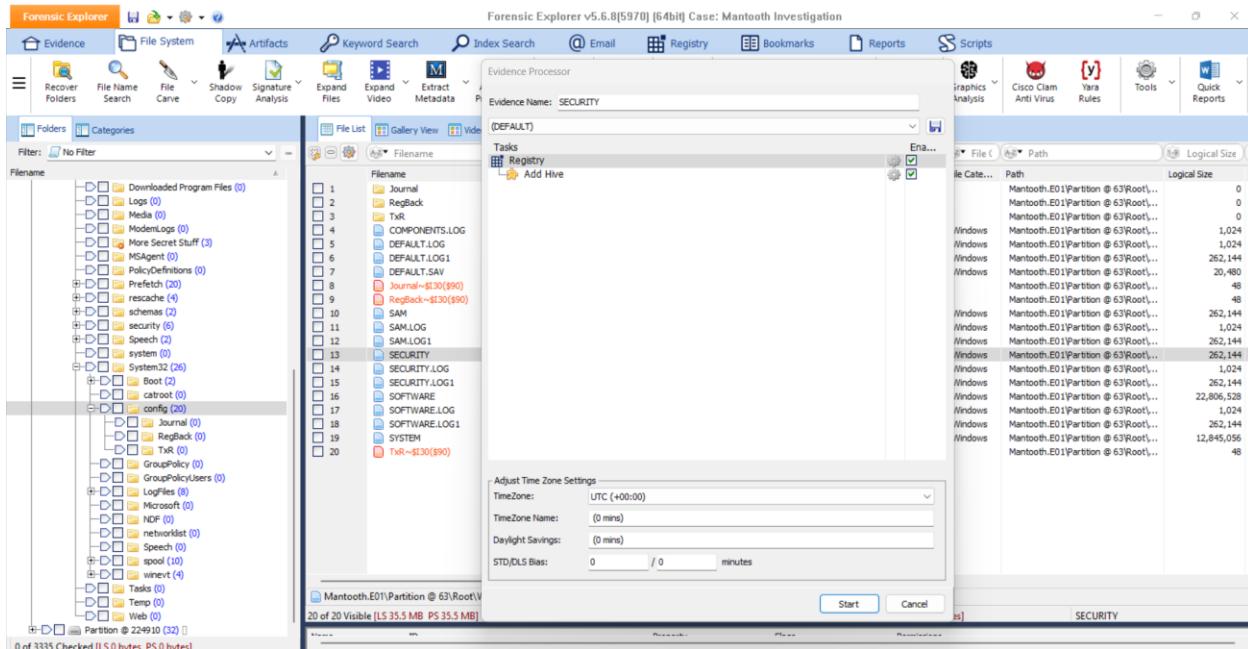


Figure 1.8 – Security registry being added

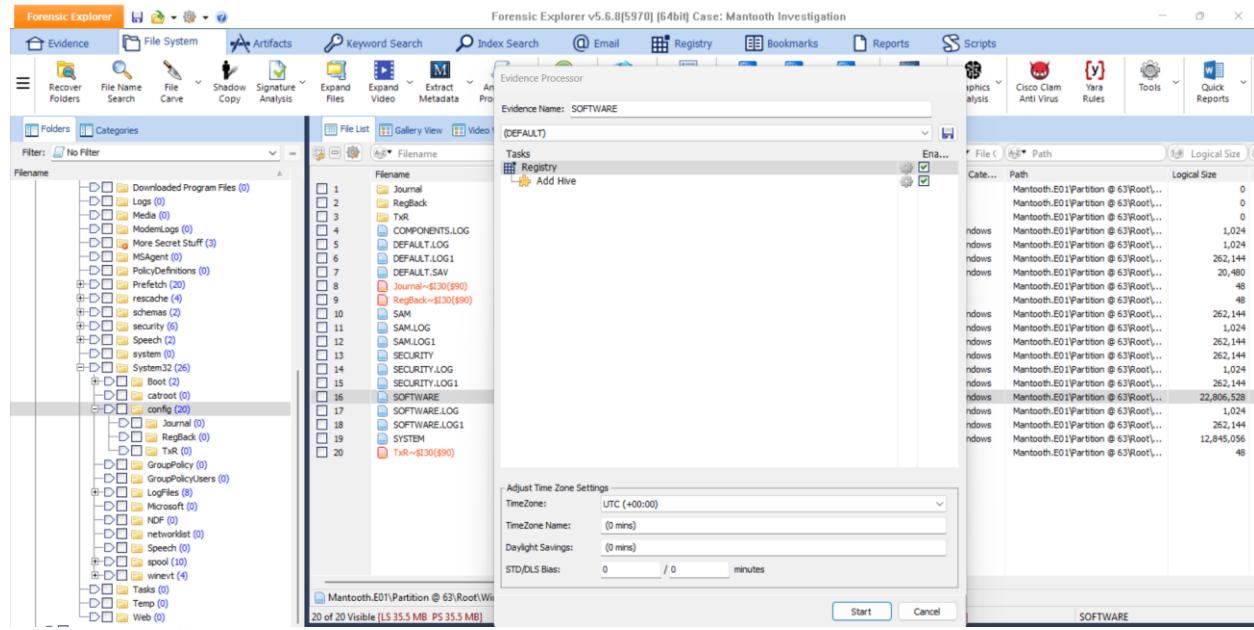


Figure 1.9 – Software registry being added

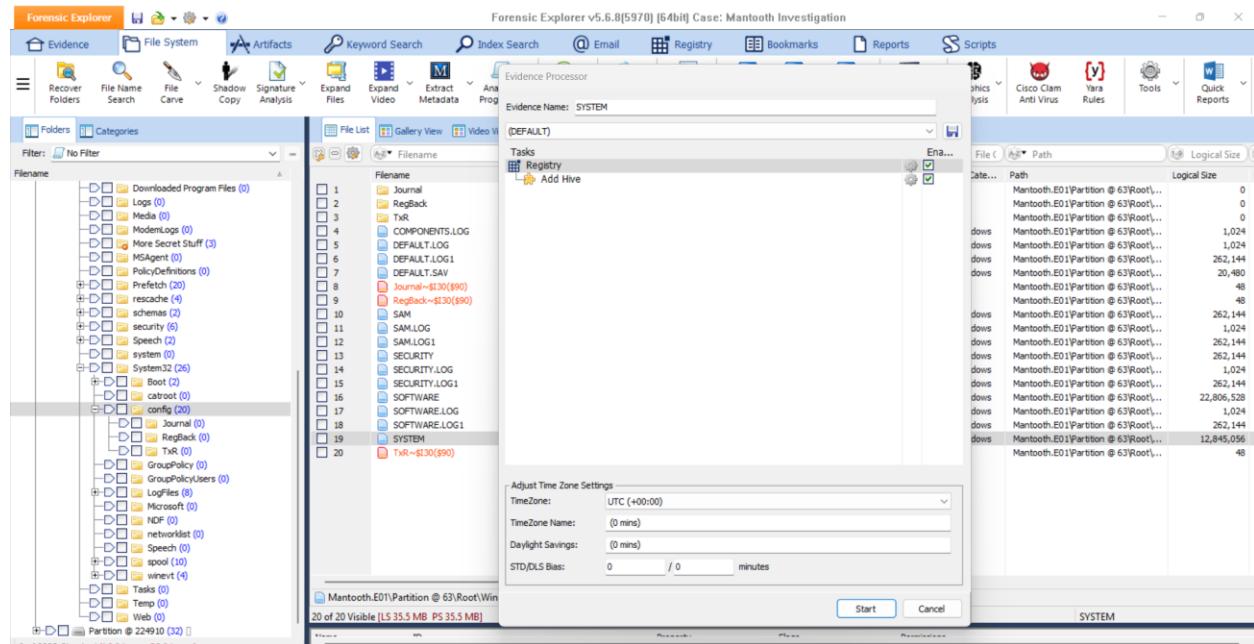


Figure 2.0 – System registry being added

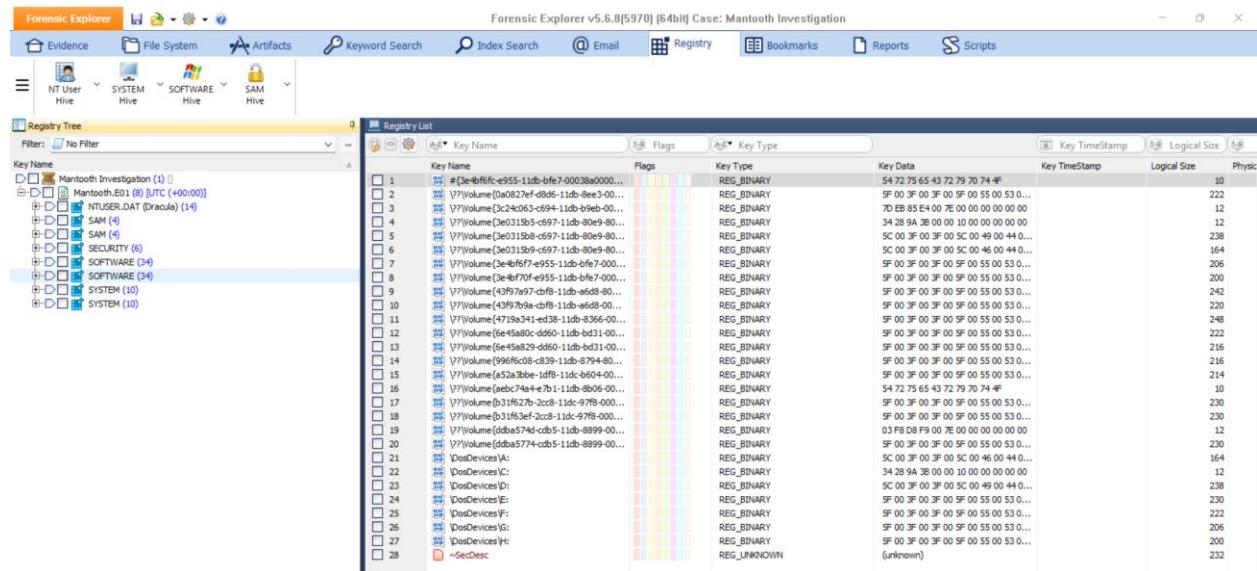


Figure 2.1 – The registry for the Mantooth Device

SAM

Local User Parse

The first hive of the registry is called

Parse: \SAM\Domains\Account\Users

User Name: Administrator

Full Name:

User ID: 500(\$01F4)

Account Created: 27-Feb-2007 18:29:26 [UTC]

Account Last Modified: 27-Feb-2007 19:21:54 [UTC]

Account Expires: {Never}

Account Type: (\$0000)

Account Status: Account disabled

Normal user account

Password does not expire

Comment: Built-in account for administering the computer/domain
Number Logins: 1
Last Login: 02-Nov-2006 13:02:01 [UTC]
Password Required: True
Password Last Set: 02-Nov-2006 13:08:15 [UTC]
Last Password Fail: {Never}
Invalid Password Count: 0
Country Code: 0 (Default)

~~~~~

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SAM >  
SAM\SAM\SAM\Domains\Account\Users\000001F4

---

User Name: Guest  
Full Name:  
User ID: 501(\$01F5)  
Account Created: 27-Feb-2007 18:29:26 [UTC]  
Account Last Modified: 27-Feb-2007 19:21:54 [UTC]  
Account Expires: {Never}  
Account Type: (\$0000)  
Account Status: Account disabled  
    Password not required (for Domain accounts)  
    Normal user account  
    Password does not expire  
Comment: Built-in account for guest access to the computer/domain  
Number Logins: 0  
Last Login: {Never}  
Password Required: False

Password Last Set: {Never}

Last Password Fail: {Never}

Invalid Password Count: 0

Country Code: 0 (Default)

~~~~~

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SAM >
SAM\SAM\SAM\Domains\Account\Users\000001F5

User Name: Wes Mantooth

User ID: 1000(\$03E8)

Account Created: 27-Feb-2007 18:29:10 [UTC]

Account Last Modified: 12-Feb-2008 20:13:16 [UTC]

Account Expires: {Never}

Account Type: (\$0000)

Account Status: Password not required (for Domain accounts)

Normal user account

Password does not expire

Number Logins: 96

Last Login: 12-Feb-2008 19:12:08 [UTC]

Password Required: True

Password Last Set: 27-Feb-2007 18:29:13 [UTC]

Password Hint: in your face

Last Password Fail: 12-Feb-2008 20:13:16 [UTC]

Invalid Password Count: 3

Country Code: 0 (Default)

~~~~~

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SAM >  
SAM\SAM\SAM\Domains\Account\Users\000003E8

User Name: Dracula  
Full Name: Count Dracula  
User ID: 1002(\$03EA)  
Account Created: 06-Mar-2007 01:25:43 [UTC]  
Account Last Modified: 12-Feb-2008 20:13:17 [UTC]  
Account Expires: {Never}  
Account Type: (\$0000)  
Account Status: Normal user account  
                  Password does not expire  
Comment: The Tooth Account  
Number Logins: 3  
Last Login: 02-Apr-2007 00:30:58 [UTC]  
Password Required: True  
Password Last Set: 02-Apr-2007 00:30:39 [UTC]  
Last Password Fail: 12-Feb-2008 20:13:17 [UTC]  
Invalid Password Count: 2  
Country Code: 0 (Default)

---

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SAM >  
SAM\SAM\SAM\Domains\Account\Users\000003EA

---

User Name: Laurent  
User ID: 1003(\$03EB)  
Account Created: 12-Feb-2008 00:13:36 [UTC]  
Account Last Modified: 12-Feb-2008 00:13:36 [UTC]  
Account Expires: {Never}

Account Type: (\$0000)  
Account Status: Normal user account  
Password does not expire  
Number Logins: 0  
Last Login: {Never}  
Password Required: False  
Password Last Set: {Never}  
Last Password Fail: {Never}  
Invalid Password Count: 0  
Country Code: 0 (Default)

~~~~~  
Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SAM >
SAM\SAM\SAM\Domains\Account\Users\000003EB

End of results.

Software Hive

OS Install Date

Search for: SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate
Description: Installation date of the Operating System.
Reference: None.

=====

Key Found: Mantooth.E01\SOFTWARE\Microsoft\Windows NT\CurrentVersion\

Value	Data
~~~~~	~~~~~
InstallDate	2/27/2007 7:22:03 PM

---

Registry Key Processor finished.

### Product Name and ID

Search for: SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName

Description: The name of the Operating System.

Reference: None.

---

---

Key Found: Mantooth.E01\SOFTWARE\Microsoft\Windows NT\CurrentVersion\

Value	Data
~~~~~	~~~~~
ProductId	89580-378-0753292-71704
ProductName	Windows Vista (TM) Ultimate
BuildLabEx	6000.16575.x86fre.vista_gdr.071009-1548

Registry Key Processor finished.

Registered Owner/Organization

Search for: SOFTWARE\Microsoft\Windows NT\CurrentVersion\ RegisteredOwner and RegisteredOrganization

Description: Owner and organization details entered at installation. Can be modified.

Reference: None.

Key Found: Mantooth.E01\SOFTWARE\Microsoft\Windows NT\CurrentVersion\

Value	Data
~~~~~	~~~~~

RegisteredOwner                   Wes Mantooth  
RegisteredOrganization            Volturi Enterprises

---

Registry Key Processor finished.

### Uninstalled Programs (metadata)

Search for: SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\

Description: Uninstall programs list.

Reference: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa372105%28v=vs.85%29.aspx>

---

---

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ActiveTouchMeeting Client\

Value	Data
~~~~~	~~~~~
DisplayName	WebEx
Publisher	WebEx Communications, Inc
URLInfoAbout	http://www.webex.com

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AIM_6\

Value	Data
~~~~~	~~~~~
DisplayName	AIM 6

---

Key Found: Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AOL Uninstaller\

Value	Data
~~~~~	~~~~~
DisplayName	AOL Uninstaller (Choose which Products to Remove)

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\BestCrypt\

Value	Data
~~~~~	~~~~~
DisplayName	BestCrypt 8.0

---

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileZilla\

Value	Data
~~~~~	~~~~~
DisplayName	FileZilla (remove only)

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox (2.0.0.3)\

Value	Data
~~~~~	~~~~~
DisplayName	Mozilla Firefox (2.0.0.3)
DisplayVersion	2.0.0.3 (en-US)
Publisher	Mozilla
URLInfoAbout	<a href="http://en-US.www.mozilla.com/en-US/">http://en-US.www.mozilla.com/en-US/</a>

---

Key Found: Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\P2P Networking\

Value	Data
-------	------

---

~~~~~

~~~~~

DisplayName

P2P Networking

---

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\QuickTime\

Value

Data

~~~~~

~~~~~

DisplayName

QuickTime

---

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\RealVNC_is1\

Value

Data

~~~~~

~~~~~

DisplayName

VNC Free Edition 4.1.2

DisplayVersion

4.1.2

Publisher

RealVNC Ltd.

URLInfoAbout

<http://www.realvnc.com>

---

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ShockwaveFlash\

Value

Data

~~~~~

~~~~~

DisplayName

Adobe Flash Player 9 ActiveX

DisplayVersion

9

Publisher

Adobe Systems

---

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Trillian\

Value	Data
~~~~~	~~~~~
DisplayName	Trillian

Key Found:
Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TrueCrypt\

Value	Data
~~~~~	~~~~~
DisplayName	TrueCrypt
Publisher	TrueCrypt Foundation
URLInfoAbout	<a href="http://www.truecrypt.org/">http://www.truecrypt.org/</a>

---

Key Found:  
Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ViewpointMediaPlayer\

Value	Data
~~~~~	~~~~~
DisplayName	Viewpoint Media Player

Key Found:
Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinRAR archiver\

Value	Data
~~~~~	~~~~~
DisplayName	WinRAR archiver

---

Key Found:  
Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Yahoo! Companion\

Value	Data
~~~~~	~~~~~

DisplayName	Yahoo! Toolbar
-------------	----------------

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Yahoo!
Customizations\

Value	Data
~~~~~	~~~~~
DisplayName	Yahoo! Browser Services

---

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Yahoo! Internet Mail\

Value	Data
~~~~~	~~~~~
DisplayName	Yahoo! Internet Mail

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Yahoo! Messenger\

Value	Data
~~~~~	~~~~~
DisplayName	Yahoo! Messenger

---

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Yahoo! Toolbar\

Value	Data
~~~~~	~~~~~
DisplayName	Yahoo! Toolbar

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\YInstHelper\

Value	Data
~~~~~	~~~~~
DisplayName	Yahoo! Install Manager

---

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1A17C9B5-2A6C-4E9B-A279-B4AD49D2FE51}\

Value	Data
~~~~~	~~~~~
DisplayName	AccessData DNA 3 Worker
DisplayVersion	3.3
Publisher	AccessData
URLInfoAbout	http://www.accessdata.com

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{44CDBD1B-89FB-4E02-8319-2A4C550F664A}\

Value	Data
~~~~~	~~~~~
DisplayName	RTC Client API v1.2
DisplayVersion	1.2.0000
Publisher	Microsoft
URLInfoAbout	<a href="http://www.microsoft.com">http://www.microsoft.com</a>

---

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{571700F0-DB9D-4B3A-B03D-35A14BB5939F}\

Value	Data
~~~~~	~~~~~

DisplayName	Windows Live Messenger
DisplayVersion	8.1.0178.00
Publisher	Microsoft Corporation
URLInfoAbout	

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{91120409-6000-11D3-8CFE-0150048383C9}\

Value	Data
~~~~~	~~~~~
DisplayName	Microsoft Office Standard Edition 2003
DisplayVersion	11.0.5614.0
Publisher	Microsoft Corporation
URLInfoAbout	<a href="http://www.microsoft.com/support">http://www.microsoft.com/support</a>

---

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{AC76BA86-7AD7-1033-7B44-A80000000002}\

Value	Data
~~~~~	~~~~~
DisplayName	Adobe Reader 8
DisplayVersion	8.0.0
Publisher	Adobe Systems Incorporated
URLInfoAbout	http://www.adobe.com

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{E1D8B687-F098-4C43-B388-CFE3C621EE38}\

Value	Data
-------	------

~~~~~

~~~~~

DisplayName	AccessData FTK Imager
DisplayVersion	2.5.1
Publisher	AccessData

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{FD951CD4-4600-4F32-83D4-AEA3E504D900}\

Value	Data
~~~~~	~~~~~
DisplayName	AccessData Registry Viewer
DisplayVersion	1.5
Publisher	AccessData

---

Registry Key Processor finished.

## System Hive

### Computer Name

Search for: SYSTEM\ControlSet###\Control\ComputerName\ComputerName\

Description: Owner details entered at installation. Can be modified.

Reference: None.

---

---

Key Found:

Mantooth.E01\SYSTEM\ControlSet001\Control\ComputerName\ComputerName\

Value	Data
~~~~~	~~~~~
ComputerName	WESMANTOOTH-PC

Key Found:

Mantooth.E01\SYSTEM\ControlSet003\Control\ComputerName\ComputerName\

Value	Data
~~~~~	~~~~~
ComputerName	WESMANTOOOTH-PC

---

Registry Key Processor finished.

### Shutdown Time

Search for: SYSTEM\ControlSet###\Control\Windows\ShutdownTime\

Description: Last computer shutdown time.

Reference: None.

---

---

No keys were found. Check this Result in the Registry Module.

---

Registry Key Processor finished.

### Time zone

Search for: SYSTEM\ControlSet###\Control\TimeZoneInformation\

Description: The time zone setting.

Reference: None.

---

---

Key Found: Mantooth.E01\SYSTEM\ControlSet001\Control\TimeZoneInformation\

Value	Data
~~~~~	~~~~~

ActiveTimeBias	0x0168
Bias	0x01A4
DaylightBias	0xFFFFFC4
DaylightName	@tzres.dll,-191
DaylightStart
DynamicDaylightTimeDisabled	0x0000
StandardBias	0x0000
StandardName	@tzres.dll,-192
StandardStart
TimeZoneKeyName	Mountain Standard Time

Key Found: Mantooth.E01\SYSTEM\ControlSet003\Control\TimeZoneInformation\

Value	Data
~~~~~	~~~~~
ActiveTimeBias	0x0168
Bias	0x01A4
DaylightBias	0xFFFFFC4
DaylightName	@tzres.dll,-191
DaylightStart	.....
DynamicDaylightTimeDisabled	0x0000
StandardBias	0x0000
StandardName	@tzres.dll,-192
StandardStart	.....
TimeZoneKeyName	Mountain Standard Time

---

Registry Key Processor finished.

## USB Storage device (parsed)

---

USB Device 1:

Friendly Name: Apple iPod USB Device  
Serial Number: 000A270014B302AB&0  
Device Class ID: Disk&Ven_Apple&Prod_iPod&Rev_1.62  
Device Type: Disk  
Vendor Name: Apple  
Vendor ID: 05AC  
Product Name: iPod  
Product ID: 1209  
Revision: 1.62  
First Connected (setupapi): {Never}  
Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]  
Last Connected (MountPoints2): {Never}  
Last Connected (VID_&PID_): 14-Jul-2007 17:56:41 [UTC]  
Device GUID: {3e4bf6f7-e955-11db-bfe7-00038a000015}  
Driver Letter: G

---

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >  
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Apple&Prod_iPod&Rev_1.62  
\000A270014B302AB&0

---

USB Device 2:

Friendly Name: Flash Drive SM_USB20 USB Device  
Serial Number: 6&6b8c30&0&AA14012714842&0  
Device Type: Disk  
Vendor Name: Flash

Vendor ID: 090C  
Product Name: Drive_SM_USB20  
Product ID: 1000  
Revision: 1000  
First Connected (setupapi): {Never}  
Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]  
Last Connected (MountPoints2): {Never}  
Last Connected (VID_&PID_): 14-Jul-2007 17:56:41 [UTC]  
Device GUID: {43f97a97-cbf8-11db-a6d8-806e6f6e6963}

---

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >  
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Flash&Prod_Drive_SM_USB  
20&Rev_1000\6&6b8c30&0&AA14012714842&0

---

#### USB Device 3:

Friendly Name: Flash Drive SM_USB20 USB Device  
Serial Number: AA14012714842&0  
Device Type: Disk  
Vendor Name: Flash  
Vendor ID: 090C  
Product Name: Drive_SM_USB20  
Product ID: 1000  
Revision: 1000  
First Connected (setupapi): {Never}  
Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]  
Last Connected (MountPoints2): {Never}  
Last Connected (VID_&PID_): 14-Jul-2007 17:56:41 [UTC]  
Device GUID: {43f97b9a-cbf8-11db-a6d8-00038a000015}

~~~~~  
Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven\_Flash&Prod\_Drive\_SM\_USB
20&Rev\_1000\AA14012714842&0

USB Device 4:

Friendly Name: Flash Drive UT\_USB20 USB Device

Serial Number: 0000000000C80F&0

Device Type: Disk

Vendor Name: Flash

Vendor ID: 0457

Product Name: Drive\_UT\_USB20

Product ID: 0151

Revision: 0.00

First Connected (setupapi): {Never}

Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]

Last Connected (MountPoints2): {Never}

Last Connected (VID\_&PID\_): 14-Jul-2007 17:56:41 [UTC]

Device GUID: {0a0827ef-d8d6-11db-8ee3-00038a000015}

~~~~~

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >  
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Flash&Prod_Drive_UT_USB  
20&Rev_0.00\0000000000C80F&0

---

USB Device 5:

Friendly Name: Flash Drive UT_USB20 USB Device

Serial Number: 0000000000C9BA&0

Device Type: Disk

Vendor Name: Flash  
Vendor ID: 0457  
Product Name: Drive_UT_USB20  
Product ID: 0151  
Revision: 0.00  
First Connected (setupapi): {Never}  
Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]  
Last Connected (MountPoints2): {Never}  
Last Connected (VID_&PID_): 14-Jul-2007 17:56:41 [UTC]  
Device GUID: {6e45a80c-dd60-11db-bd31-00038a000015}

~~~~~

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven\_Flash&Prod\_Drive\_UT\_USB
20&Rev \_0.00\0000000000C9BA&0

USB Device 6:

Friendly Name: Maxtor 6 B300R0 USB Device
Serial Number: 8396
Device Type: Disk
Vendor Name: Maxtor\_6
Vendor ID: 067B
Product Name: B300R0
Product ID: 3507
Revision: BAH4
First Connected (setupapi): {Never}
Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]
Last Connected (MountPoints2): {Never}
Last Connected (VID\_&PID\_): 14-Jul-2007 17:56:41 [UTC]

~~~~~  
Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >  
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Maxtor_6&Prod_B300R0&R  
ev_BAH4\8396

---

USB Device 7:

Friendly Name: Maxtor 6 B300R0 USB Device  
Serial Number: 8B76  
Device Type: Disk  
Vendor Name: Maxtor_6  
Vendor ID: 067B  
Product Name: B300R0  
Product ID: 3507  
Revision: BAH4  
First Connected (setupapi): {Never}  
Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]  
Last Connected (MountPoints2): {Never}  
Last Connected (VID_&PID_): 14-Jul-2007 17:56:41 [UTC]

~~~~~

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven\_Maxtor\_6&Prod\_B300R0&R
ev\_BAH4\8B76

USB Device 8:

Friendly Name: SanDisk Cruzer Mini USB Device
Serial Number: SNDK3066A40516400406&0
Device Type: Disk
Vendor Name: SanDisk

Vendor ID: 0781
Product Name: Cruzer\_Mini
Product ID: 5150
Revision: 0.1
First Connected (setupapi): {Never}
Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]
Last Connected (MountPoints2): {Never}
Last Connected (VID\_&PID\_): 14-Jul-2007 17:56:41 [UTC]
Device GUID: {ddba5774-cdb5-11db-8899-00038a000015}

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven\_SanDisk&Prod\_Cruzer\_Mini
&Rev\_0.1\SNDK3066A40516400406&0

USB Device 9:

Friendly Name: SanDisk Cruzer Mini USB Device
Serial Number: SNDK4DB2A41B47901706&0
Device Class ID: Disk&Ven\_SanDisk&Prod\_Cruzer\_Mini&Rev\_0.1
Device Type: Disk
Vendor Name: SanDisk
Vendor ID: 0781
Product Name: Cruzer\_Mini
Product ID: 5150
Revision: 0.1
First Connected (setupapi): {Never}
Connected After Reboot (USBSTOR): 14-Jul-2007 17:58:46 [UTC]
Last Connected (MountPoints2): {Never}
Last Connected (VID\_&PID\_): 14-Jul-2007 17:58:45 [UTC]

Device GUID: {b31f627b-2cc8-11dc-97f8-00038a000015}

Driver Letter: E

~~~~~  
Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >  
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Cruzer_Mini  
&Rev_0.1\SNDK4DB2A41B47901706&0

---

USB Device 10:

Friendly Name: SanDisk Cruzer Mini USB Device

Serial Number: 20043513310C7A22D0C8&0

Device Type: Disk

Vendor Name: SanDisk

Vendor ID: 0781

Product Name: Cruzer_Mini

Product ID: 5150

Revision: 0.2

First Connected (setupapi): {Never}

Connected After Reboot (USBSTOR): 14-Jul-2007 17:58:25 [UTC]

Last Connected (MountPoints2): {Never}

Last Connected (VID_&PID_): 14-Jul-2007 17:58:25 [UTC]

Device GUID: {b31f63ef-2cc8-11dc-97f8-00038a000015}

~~~~~  
Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven\_SanDisk&Prod\_Cruzer\_Mini
&Rev\_0.2\20043513310C7A22D0C8&0

USB Device 11:

Friendly Name: Sony Sony DSC USB Device

Serial Number: 6&382957cd&0
Device Class ID: Disk&Ven\_Sony&Prod\_Sony\_DSC&Rev\_5.00
Device Type: Disk
Vendor Name: Sony
Product Name: Sony\_DSC
Revision: 5.00
First Connected (setupapi): {Never}
Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]
Last Connected (MountPoints2): {Never}
Last Connected (VID\_&PID\_): {Never}
Device GUID: {3e4bf70f-e955-11db-bfe7-00038a000015}
Driver Letter: H

~~~~~

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >  
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Sony&Prod_Sony_DSC&Rev  
_5.00\6&382957cd&0

---

#### USB Device 12:

Friendly Name: TREK TD2SMART G3 USB Device  
Serial Number: 23090525338296&0  
Device Type: Disk  
Vendor Name: TREK  
Vendor ID: 0A16  
Product Name: TD2SMART_G3  
Product ID: 9005  
Revision: 2.20  
First Connected (setupapi): {Never}  
Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]

Last Connected (MountPoints2): {Never}

Last Connected (VID_&PID_): 14-Jul-2007 17:56:41 [UTC]

Device GUID: {a52a3bbe-1df8-11dc-b604-00038a000015}

~~~~~

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven\_TREK&Prod\_TD2SMART\_G
3&Rev\_2.20\23090525338296&0

USB Device 13:

Friendly Name: TREK TD2SMART G3M USB Device

Serial Number: 10120515511949&0

Device Type: Disk

Vendor Name: TREK

Vendor ID: 0A16

Product Name: TD2SMART\_G3M

Product ID: 9005

Revision: 2.40

First Connected (setupapi): {Never}

Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]

Last Connected (MountPoints2): {Never}

Last Connected (VID\_&PID\_): 14-Jul-2007 17:56:41 [UTC]

Device GUID: {6e45a829-dd60-11db-bd31-00038a000015}

~~~~~

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >  
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_TREK&Prod_TD2SMART_G  
3M&Rev_2.40\10120515511949&0

---

USB Device 14:

Friendly Name:

Serial Number: 10120516721518&0

Device Type: Disk

Vendor Name: TREK

Vendor ID: 0A16

Product Name: TD2SMART_G3M

Product ID: 9005

Revision: 2.40

First Connected (setupapi): {Never}

Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]

Last Connected (MountPoints2): {Never}

Last Connected (VID_&PID_): 14-Jul-2007 17:56:41 [UTC]

Device GUID: {996f6c08-c839-11db-8794-806e6f6e6963}

---

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >  
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_TREK&Prod_TD2SMART_G  
3M&Rev_2.40\10120516721518&0

---

USB Device 15:

Friendly Name: USB 2.0 Flash Disk USB Device

Serial Number: 6&2507d51a&0&AA10000000000623&0

Device Type: Disk

Vendor Name: USB_2.0

Product Name: Flash_Disk

Revision: 1100

First Connected (setupapi): {Never}

Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]

Last Connected (MountPoints2): {Never}

Last Connected (VID_ &PID_): {Never}

Device GUID: {4719a341-ed38-11db-8366-00038a000015}

~~~~~

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven\_USB\_2.0&Prod\_Flash\_Disk&
Rev\_1100\6&2507d51a&0&AA10000000000623&0

End of results.

NTUser Hive

Explorer Recent Docs

Search for: NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Description: Recent documents as listed in the Windows "My Recent Documents" menu.

Further information about the relative order of the listed files can be extracted from the
"MRUListEx" value.

Reference: None.

=====

====

No keys were found. Check this Result in the Registry Module.

Registry Key Processor finished.

Explorer Type Paths

Search for: NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths\

Description: Paths typed into the Windows Explorer address bar.

Reference: None.

=====

====

No keys were found. Check this Result in the Registry Module.

Registry Key Processor finished.

Internet Explorer Typed URL's

Search for: NTUSER\Software\Microsoft\Internet Explorer\TypedURLs

Description: URLs typed into the Internet Explorer address bar.

Reference: None.

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs\

| Value | Data |
|-------|---|
| ~~~~~ | ~~~~~ |
| url1 | http://go.microsoft.com/fwlink/?LinkId=69157 |

Registry Key Processor finished.

MS Office MRU

Search for: NTUSER\Software\Microsoft\Office\xx.x\XXX\XXX MRU

Description: Recent Office files: Word, Excel, PowerPoint, OneNote, Publisher, etc.
(Includes "File" and "Place" MRUs).

Reference: None.

No keys were found. Check this Result in the Registry Module.

Registry Key Processor finished.

Windows MRU

Search for: NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Description: Items recently run from the Windows Start "Run" bar.

Reference: None.

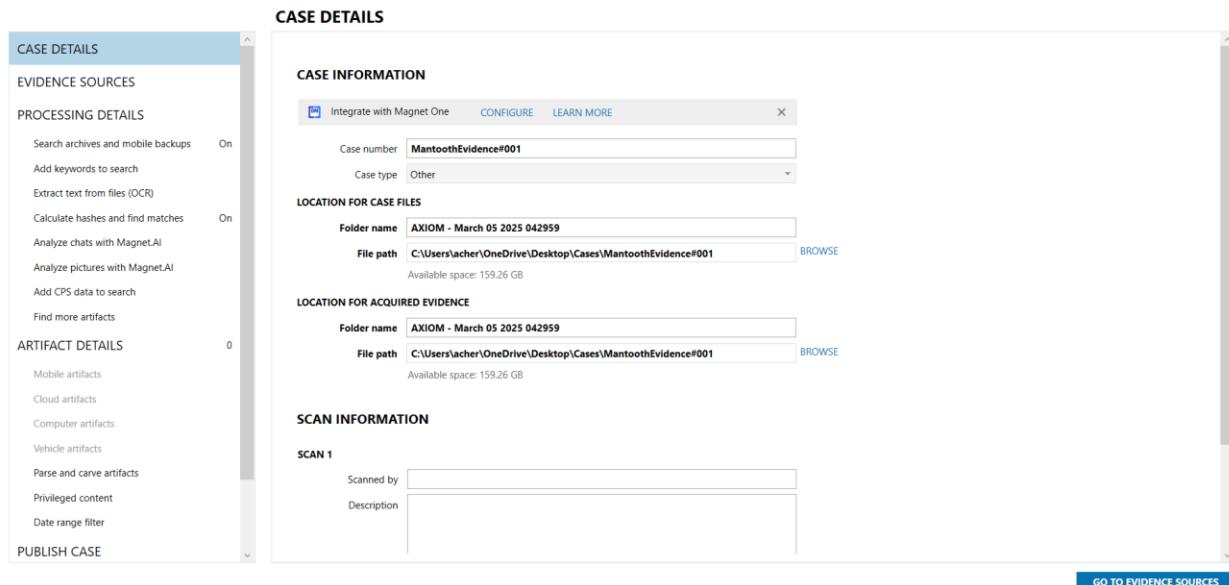
No keys were found. Check this Result in the Registry Module.

Registry Key Processor finished.

Active File Review

Axiom

The next part of the investigation involved using Magnet Axiom, both process and examine. Figures 2.2-3.3 show the process involved defining the case name, specifying the image source, and selecting relevant evidence.



The screenshot shows the 'CASE DETAILS' interface in Magnet Axiom. On the left, there's a sidebar with sections like 'CASE DETAILS', 'EVIDENCE SOURCES', 'PROCESSING DETAILS', 'ARTIFACT DETAILS', and 'PUBLISH CASE'. The main area is titled 'CASE INFORMATION' and contains fields for 'Case number' (set to 'MantoothEvidence#001') and 'Case type' (set to 'Other'). Below this is the 'LOCATION FOR CASE FILES' section, which includes a 'Folder name' field ('AXIOM - March 05 2025 042959') and a 'File path' field ('C:\Users\acher\OneDrive\Desktop\Cases\MantoothEvidence#001'). It also shows 'Available space: 159.26 GB'. The 'LOCATION FOR ACQUIRED EVIDENCE' section has similar fields. At the bottom, there's a 'SCAN INFORMATION' section with a 'SCAN 1' entry. A 'GO TO EVIDENCE SOURCES' button is at the bottom right.

Figure 2.2 – Label the case and create a folder for this case to go into

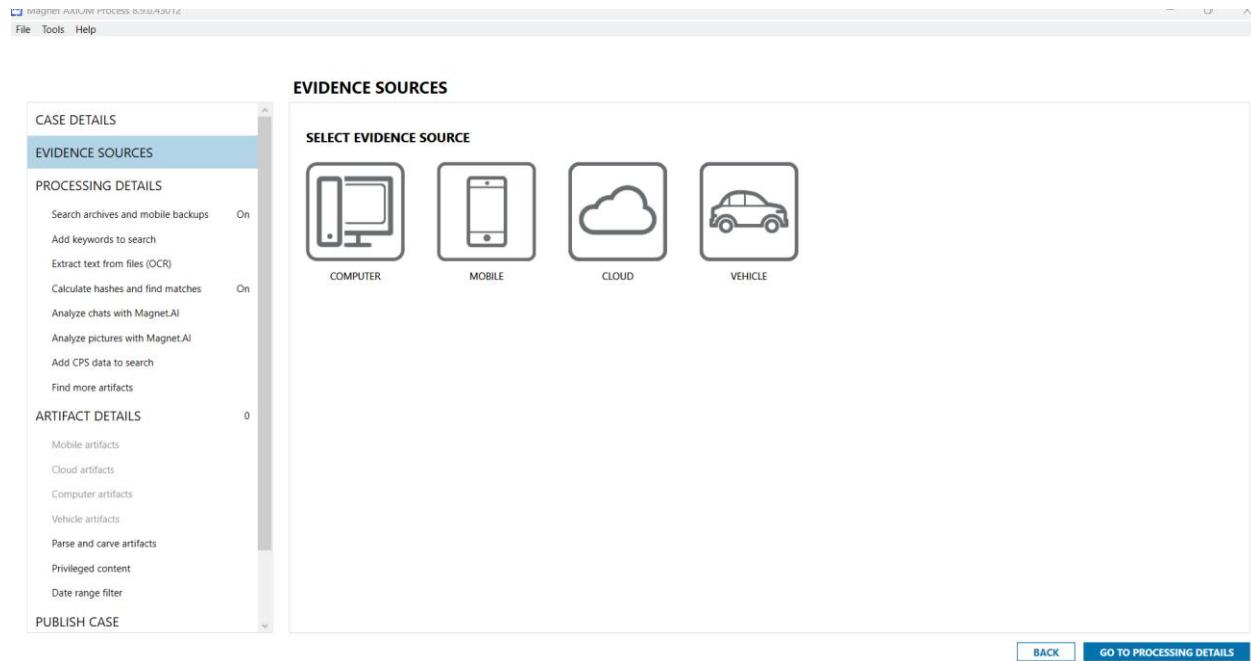


Figure 2.5 – Select “Computer”

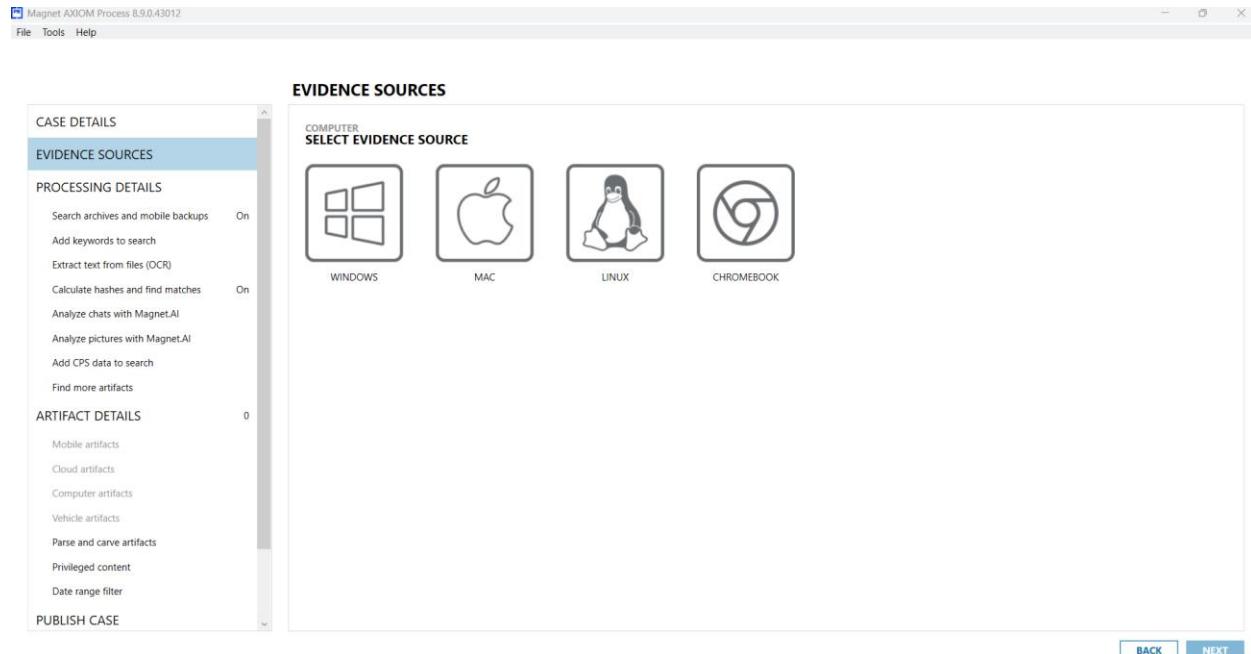


Figure 2.6 – Select “Windows”

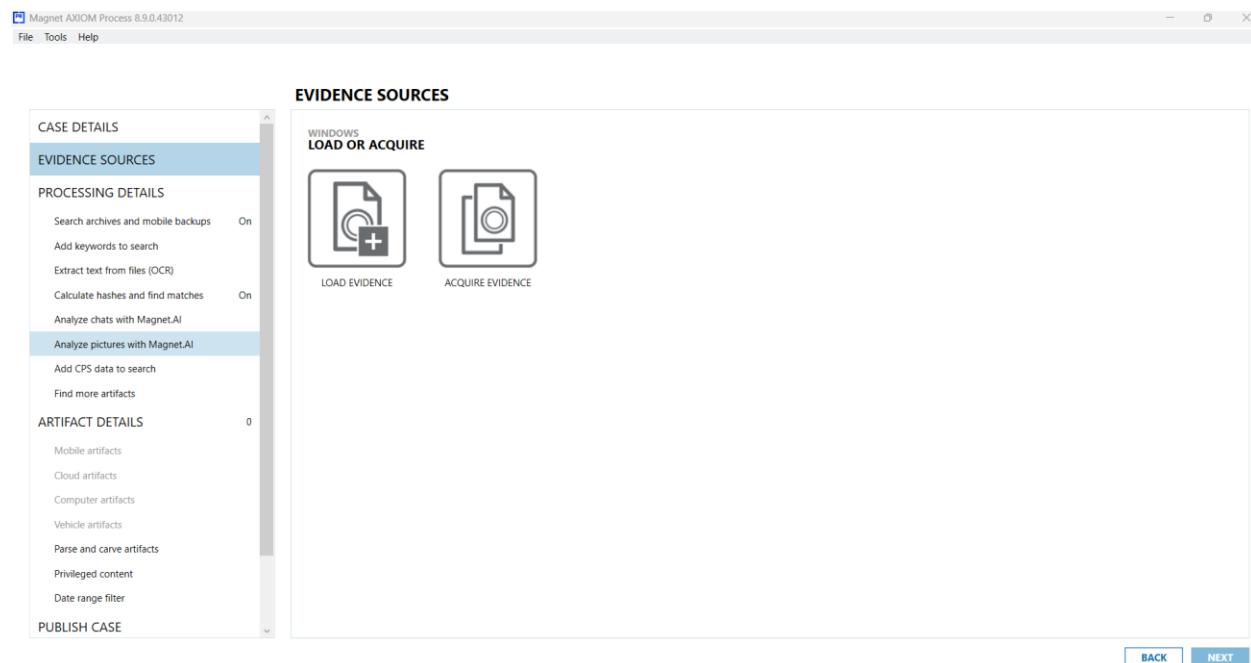


Figure 2.7 – Select “Load Evidence”

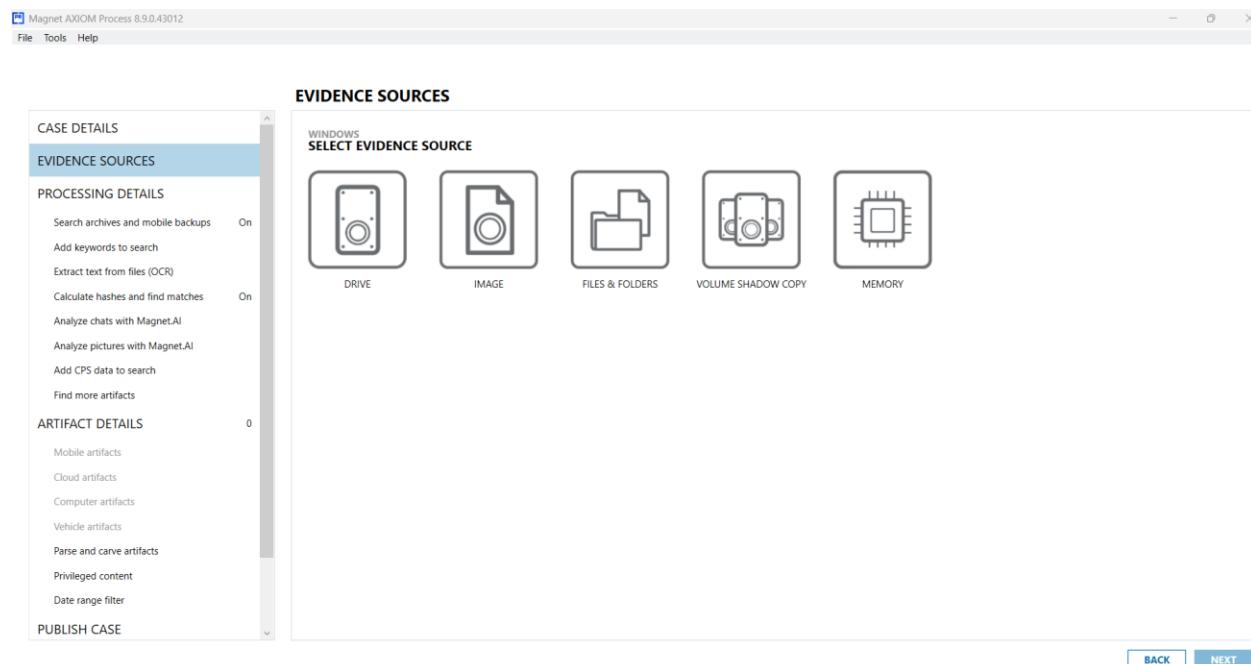


Figure 2.8 – Select “Image”

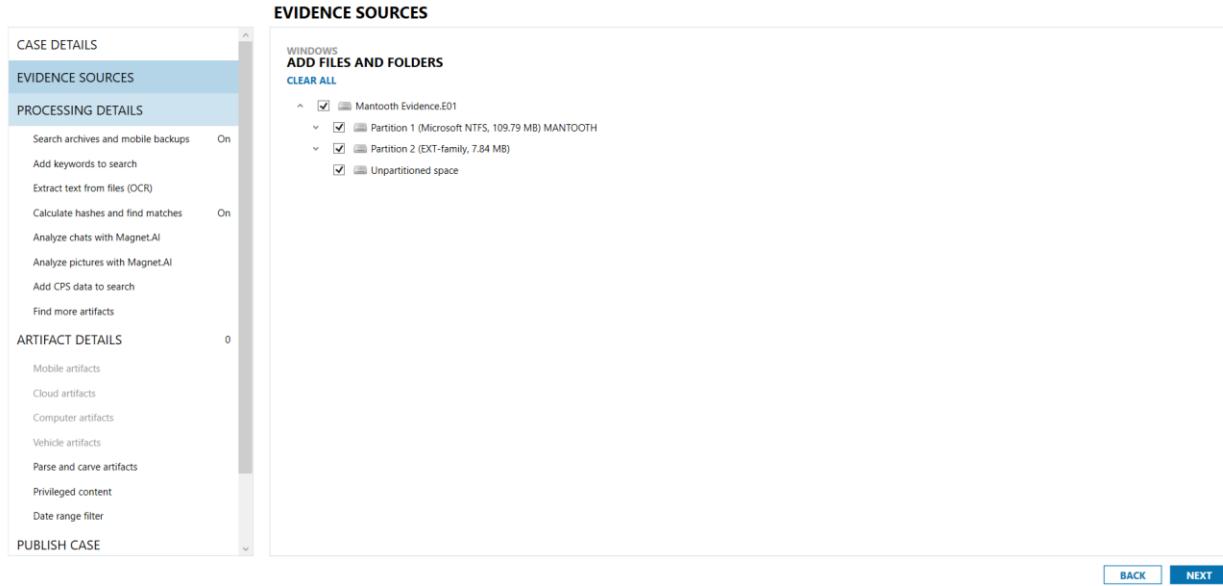


Figure 2.9 – Select the file

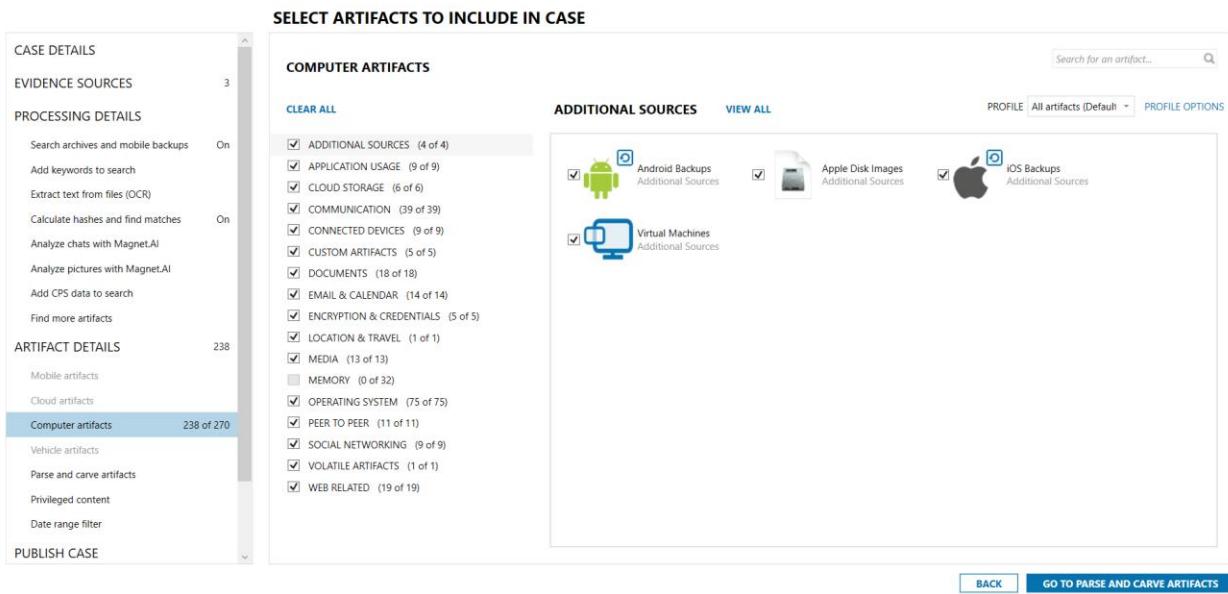


Figure 3.0 – Select the defaults up until “Computer Artifacts”, then select all the options

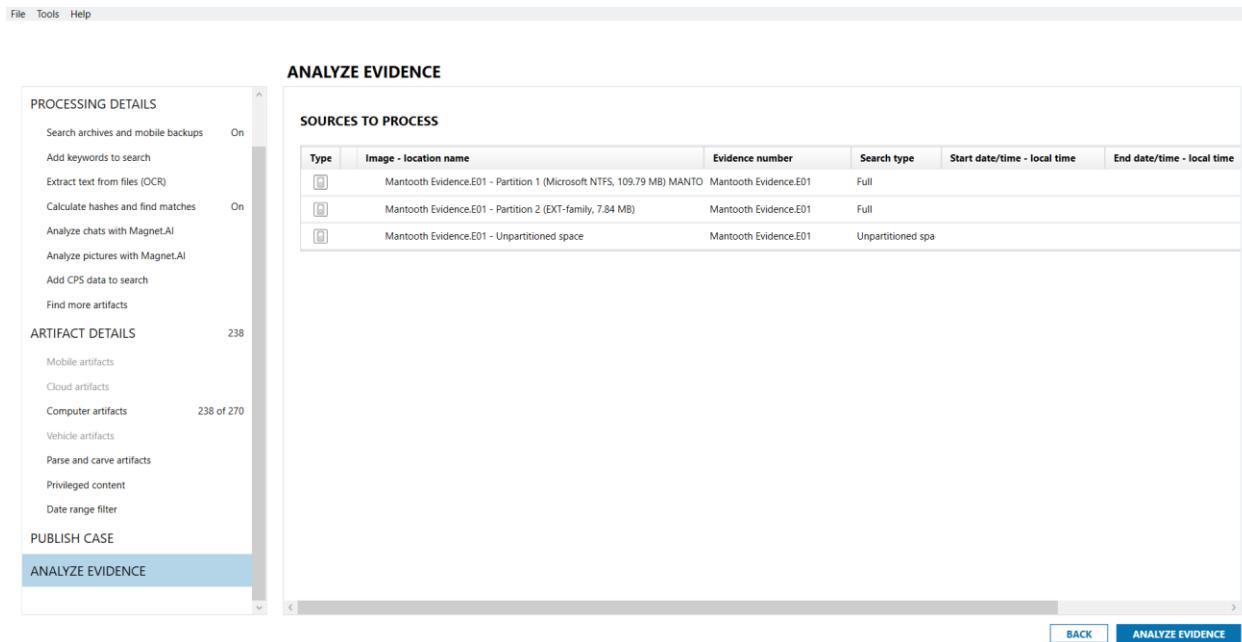


Figure 3.1 – Select all the defaults until “Analyze Evidence”, then analyze the evidence

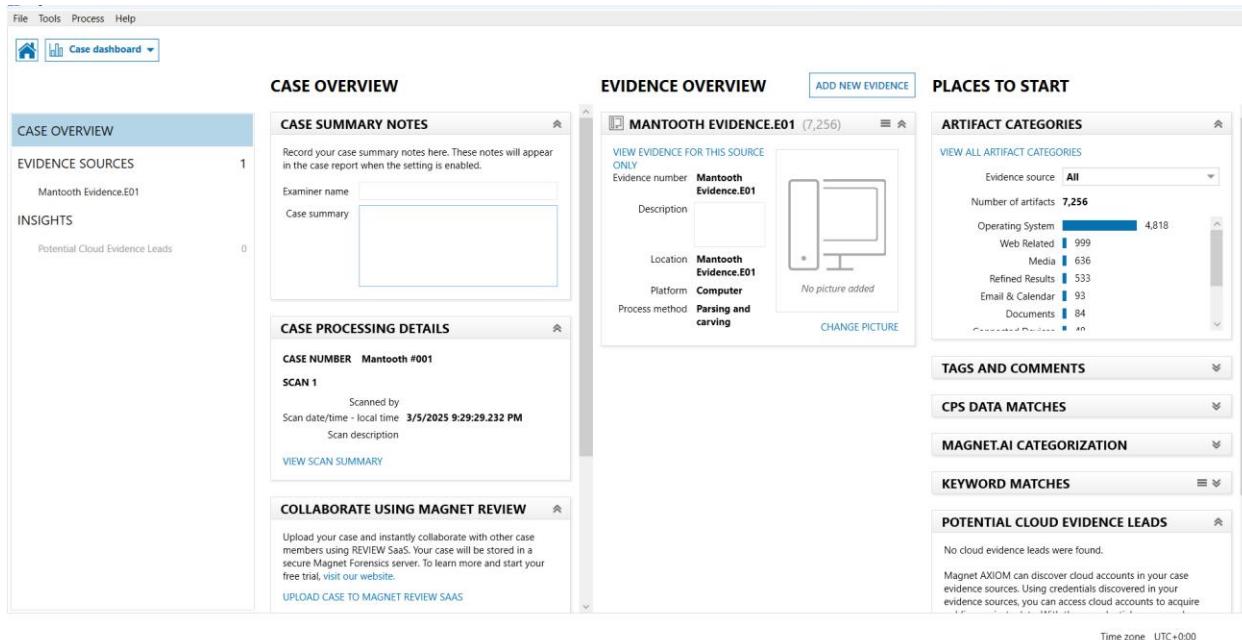


Figure 3.2 – Case Overview

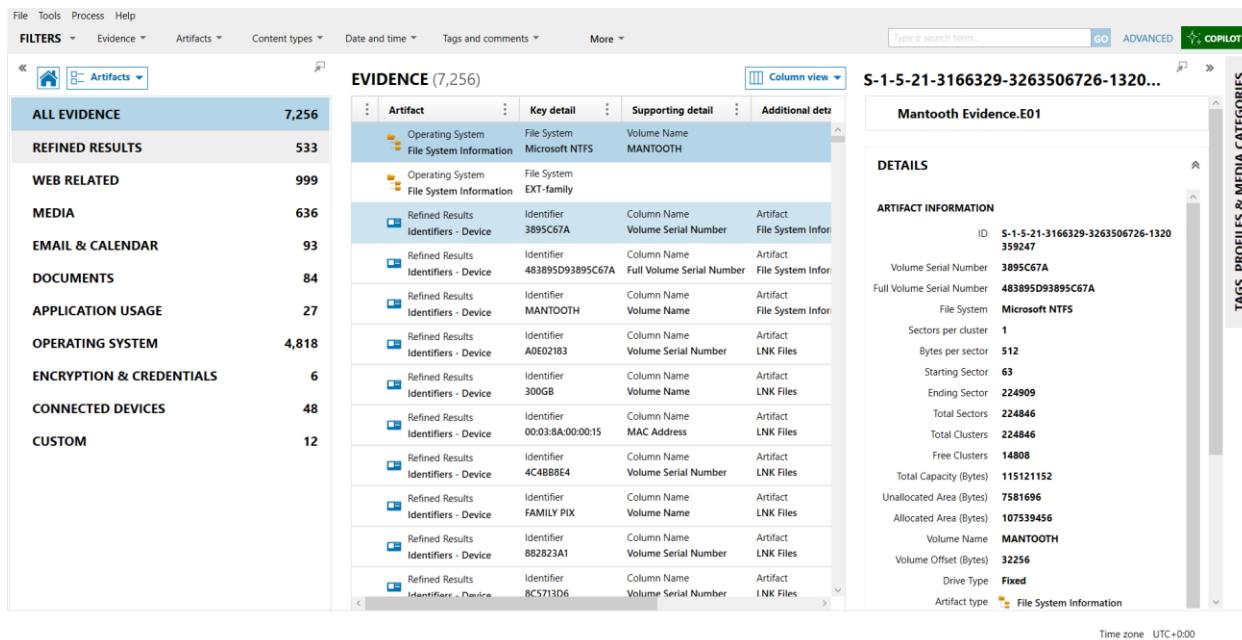


Figure 3.3 – Analyzed Evidence

Media

During the examination of Wes Mantooth’s drive while using Axiom Examine, several media files were discovered in a folder labeled “Media” Shown in Figure 3.3 – 4.5, the images recovered appear to be connected to the criminals activities. These photos of forged prescription templates, scanned images of fake checks, images of credit cards, and pictures of materials consistent with drug making. There were also pictures of credit card skimmers being placed on ATM’s, this suggests involvement with financial fraud.

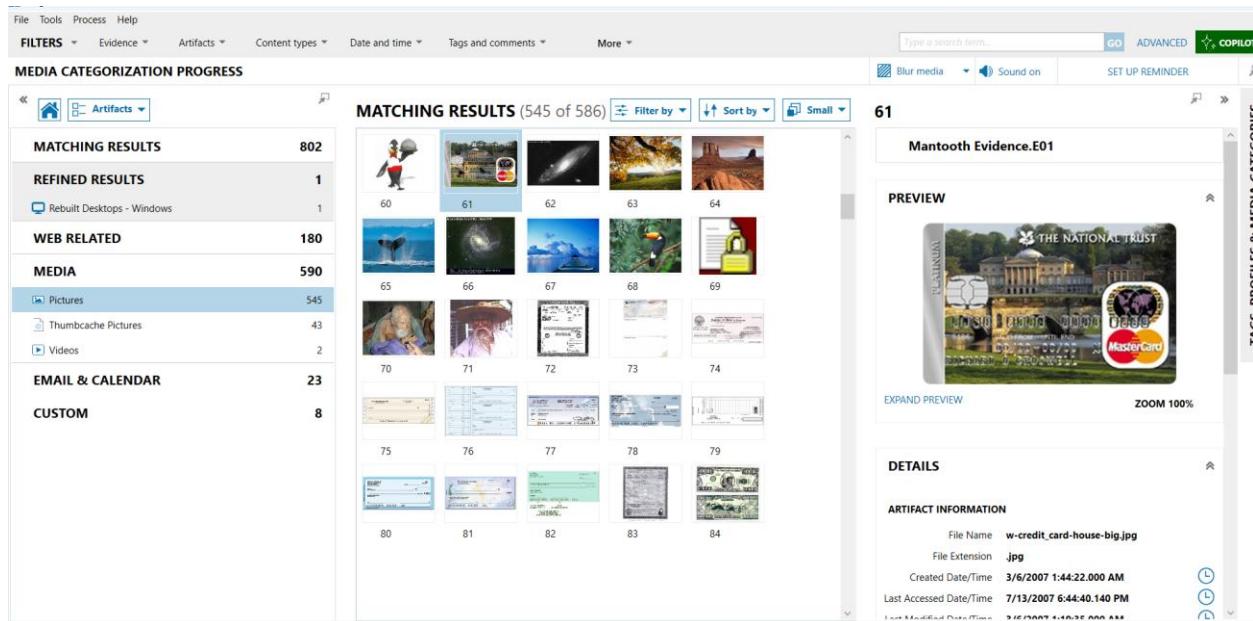


Figure 3.4 – Picture of credit card as well as multiple checks

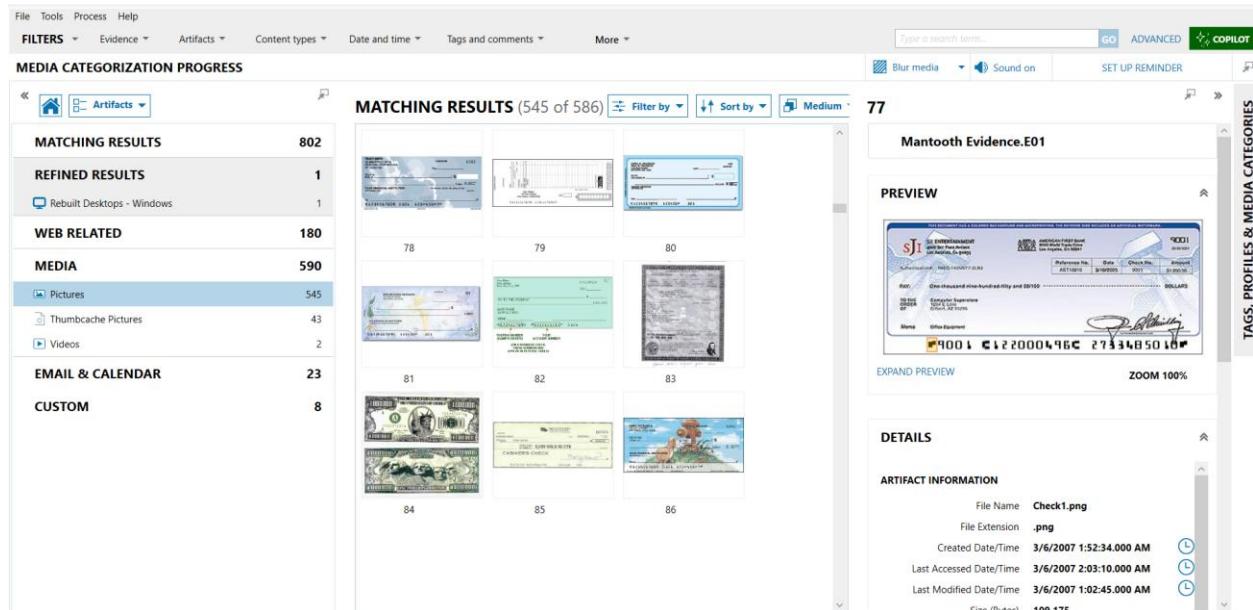


Figure 3.5 – Picture of a check with more checks in view

MEDIA CATEGORIZATION PROGRESS

| MATCHING RESULTS | |
|-----------------------------|------------|
| REFINED RESULTS | 1 |
| Rebuilt Desktops - Windows | 1 |
| WEB RELATED | 180 |
| MEDIA | 590 |
| Pictures | 545 |
| Thumbcache Pictures | 43 |
| Videos | 2 |
| EMAIL & CALENDAR | 23 |
| CUSTOM | 8 |

MATCHING RESULTS (545 of 586)

PREVIEW

93

Family Physician Medical Group Inc.
8232 Garvey Avenue, Suite 107 , Rosemead, CA 91770
TEL: (800) 518-9505 FAX:
PATIENT NAME: THOMAS BOOK DOB: 12/01/1976
ADDRESS:

ADVAIR dosage : 100/50 - 1 Puff BID : 01 , Refill: 02
TAGAMET dosage : 400 mg - 1 Tab BID : 60 TBS

Rx

John Doe MD

LABEL DO NOT SUBSTITUTE

RELATED MEDIA ARTIFACTS (2)

DETAILS

Time zone UTC+000

Figure 3.6 – Fake pharmacy doctors note

MEDIA CATEGORIZATION PROGRESS

| MATCHING RESULTS | |
|-----------------------------|------------|
| REFINED RESULTS | 1 |
| Rebuilt Desktops - Windows | 1 |
| WEB RELATED | 180 |
| MEDIA | 590 |
| Pictures | 545 |
| Thumbcache Pictures | 43 |
| Videos | 2 |
| EMAIL & CALENDAR | 23 |
| CUSTOM | 8 |

MATCHING RESULTS (545 of 586)

PREVIEW

127

Mantooth Evidence.E01

DETAILS

ARTIFACT INFORMATION

Size (Bytes) 20,625
Skin Tone Percentage 0.0

Figure 3.7 – Legal documents with more scans of checks

The screenshot shows a digital forensic tool's user interface. The top navigation bar includes 'File', 'Tools', 'Process', 'Help', 'FILTERS' (Evidence, Artifacts, Content types, Date and time, Tags and comments, More), 'ADVANCED', 'COPILOT', and search fields. The left sidebar displays 'MEDIA CATEGORIZATION PROGRESS' with categories like MATCHING RESULTS (802), REFINED RESULTS (1), WEB RELATED (180), MEDIA (590) (selected), EMAIL & CALENDAR (23), and CUSTOM (8). The main pane shows 'MATCHING RESULTS (545 of 586)' with various thumbnails labeled 144 through 152. The right pane details evidence item 147, titled 'Mantooth Evidence.E01', showing a preview of a Bank of New Zealand CLASSIC CARD and its details: Size (Bytes) 15,914, Skin Tone Percentage 0.4, Original Width 256, Original Height 169, and Exif Extraction Status Complete. A note indicates 'Time zone UTC+0:00'.

Figure 3.8 – Credit card with more fraudulent certificates and checks

The screenshot shows a digital forensic tool's user interface. The top navigation bar includes 'File', 'Tools', 'Process', 'Help', 'FILTERS' (Evidence, Artifacts, Content types, Date and time, Tags and comments, More), 'ADVANCED', 'COPILOT', and search fields. The left sidebar displays 'MEDIA CATEGORIZATION PROGRESS' with categories like MATCHING RESULTS (802), REFINED RESULTS (1), WEB RELATED (180), MEDIA (590) (selected), EMAIL & CALENDAR (23), and CUSTOM (8). The main pane shows 'MATCHING RESULTS (545 of 586)' with various thumbnails labeled 276 through 284. The right pane details evidence item 283, titled 'Mantooth Evidence.E01', showing a preview of a photograph and its details: File Name Images[8].jpg, File Extension jpg, Created Date/Time 7/13/2007 11:00:16.000 PM, Last Accessed Date/Time 7/13/2007 11:00:16.000 PM, Last Modified Date/Time 7/13/2007 11:00:16.000 PM, and Size (Bytes) 2,238. A note indicates 'Time zone UTC+0:00'.

Figure 3.9 – Credit card skimmer on an ATM

Screenshot of a digital forensic tool interface showing matching results for artifacts. The left sidebar shows a tree view of evidence items, with 'Pictures' selected under 'MEDIA'. The main pane displays 'MATCHING RESULTS (545 of 586)' with various thumbnail images numbered 339 through 347. The right pane details a specific artifact: 'Mantooth Evidence.E01', showing a preview of a photo of ingredients, related media artifacts (2), and detailed information including file name, extension, and creation date.

Figure 4.0 – Picture of ingredients for paraphernalia

Screenshot of a digital forensic tool interface showing matching results for artifacts. The left sidebar shows a tree view of evidence items, with 'Pictures' selected under 'MEDIA'. The main pane displays 'MATCHING RESULTS (545 of 586)' with various thumbnail images numbered 375 through 383. The right pane details a specific artifact: 'Mantooth Evidence.E01', showing a preview of a photo of ingredients, related media artifacts (2), and detailed information including file name, extension, and creation date.

Figure 4.1 – More pictures of ingredients to make some paraphernalia

Web Searches

A review of the browser artifacts revealed highly incriminating web activity. Figures 4.2 – 4.6 show the suspect conducting multiple Google searches about check washing, meth production, as well as just looking up that they know the things they are looking up is illegal. One image shows 13 searches on check washing, while another one shows over 50 searches containing the word “meth.”

The screenshot displays a digital forensic interface for evidence analysis. At the top, there are filters for Evidence, Artifacts, Content types, Date and time, Tags and comments, and a search bar for 'check washing'. Below the filters, the 'Artifacts' tab is selected. The main pane shows 'MATCHING RESULTS (13 of 195)' for the query 'check washing'. The results list various URLs from Google Images related to check washing. To the left, a sidebar shows 'MATCHING RESULTS' (29), 'REFINED RESULTS' (16) including 'Google Searches' (13) and 'Rebuilt Webpages' (3), and 'WEB RELATED' (13) including 'Internet Explorer Cache Records' (7), 'Internet Explorer Daily History' (3), and 'Internet Explorer Main History' (3). On the right, there is a 'TAGS AND COMMENTS' section which is currently empty, showing a note that 'No tags have been added yet'.

Figure 4.2 – 13 google searches for check washing

The screenshot shows a digital forensic interface with a yellow header bar containing 'File', 'Tools', 'Process', 'Help', 'Evidence', 'Artifacts', 'Content types', 'Date and time', 'Tags and comments', 'More', 'SAVE FILTERS', 'CLEAR FILTERS', and a search bar. A 'FILTERS' dropdown is open, showing a single filter 'meth'. The main area displays 'MATCHING RESULTS (58 of 195)'.

MATCHING RESULTS:

- REFINED RESULTS:** 70
 - Google Searches: 58
 - Identifiers - People: 4
 - Rebuilt Webpages: 8
- WEB RELATED:** 99
- MEDIA:** 5
- EMAIL & CALENDAR:** 10
- DOCUMENTS:** 4

Details for the first result:

ARTIFACT INFORMATION:

- Search Term: **tbn:JzvLs5x\_X1MspM:http://www.fims.uwo.ca/newmedia2006/images/public/9...**
- URL: **http://tbn0.google.com/images?q=tbn:JzvLs5x\_X1MspM:http://www.fims.uwo.ca/newmedia2006/images/public/9%2520Assets/MethArticleImages/DeglovedHand.jpg**

TAGS AND COMMENTS:

- No tags have been added yet.
- Add New Tag
- Select an existing tag:
 - Bookmark
 - Evidence

Figure 4.3 – 58 google searches containing the word meth

The screenshot shows a digital forensic interface with a yellow header bar containing 'File', 'Tools', 'Process', 'Help', 'Evidence', 'Artifacts', 'Content types', 'Date and time', 'Tags and comments', 'More', 'SAVE FILTERS', 'CLEAR FILTERS', and a search bar. A 'FILTERS' dropdown is open, showing a single filter 'making meth'. The main area displays 'MATCHING RESULTS (14 of 195)'.

MATCHING RESULTS:

- REFINED RESULTS:** 17
 - Google Searches: 14
 - Rebuilt Webpages: 3
- WEB RELATED:** 14

Details for the first result:

ARTIFACT INFORMATION:

- Search Term: **making meth**
- URL: **http://www.google.com/search?hl=en&q=making+meth**
- Date/Time: **7/12/2007 11:16:33.000 PM**
- Web Page Title: **making meth - Google Search**

TAGS AND COMMENTS:

- No tags have been added yet.
- Add New Tag
- Select an existing tag:
 - Bookmark
 - Evidence

Figure 4.4 – 14 google searches for Making meth

The screenshot shows the MANTOOOTH investigation interface. The left sidebar displays a tree view of evidence categories: ALL EVIDENCE (7,256), Refined Results (533), and WEB RELATED (999). The Refined Results section includes items like Classified URLs, Google Analytics First Visit Cookies, Google Analytics Referral Cookies, Google Analytics Session Cookies, and Google Searches (195). The main pane shows a list of URLs under the heading 'EVIDENCE (195)'. One URL is highlighted in blue: <http://www.google.com/search?q=+making+meth&num=10&um=1&hl=en&q=making%20meth>. The right pane provides details for this artifact, including the search term 'I am searching for bad stuff on Google', the URL, and the date/time (8/5/2007 9:10:40 AM). A 'TAGS AND COMMENTS' section indicates no tags have been added yet.

Figure 4.5 - Knows they are looking for bad things on google

The screenshot shows the MANTOOOTH investigation interface. The left sidebar displays a tree view of evidence categories: ALL EVIDENCE (7,256), Refined Results (533), and WEB RELATED (999). The Refined Results section includes items like Classified URLs, Google Analytics First Visit Cookies, Google Analytics Referral Cookies, Google Analytics Session Cookies, and Google Searches (195). The main pane shows a list of URLs under the heading 'EVIDENCE (195)'. One URL is highlighted in blue: [http://tbn0.google.com/images?q=tbn:nZOxJlpUp4XSZM:http://www.utexas.edu/police/alerts/atm\\_scam/atm1.jpg](http://tbn0.google.com/images?q=tbn:nZOxJlpUp4XSZM:http://www.utexas.edu/police/alerts/atm_scam/atm1.jpg). The right pane provides details for this artifact, including the search term 'tbn:nZOxJlpUp4XSZM:http://www.utexas.edu/police/alerts/atm\_scam/atm1.jpg', the URL, and the date/time (7/12/2007 11:15:23.788 PM). A 'TAGS AND COMMENTS' section indicates no tags have been added yet.

Figure 4.6 – Texas police alert

Passwords

The password recovery tool within AXIOM identified several saved credentials from the system. Figures 4.7 – 4.9 show passwords linked to multiple user accounts. These accounts are labeled “Dracula”, “Administrator”, and “Wes Mantooth.”

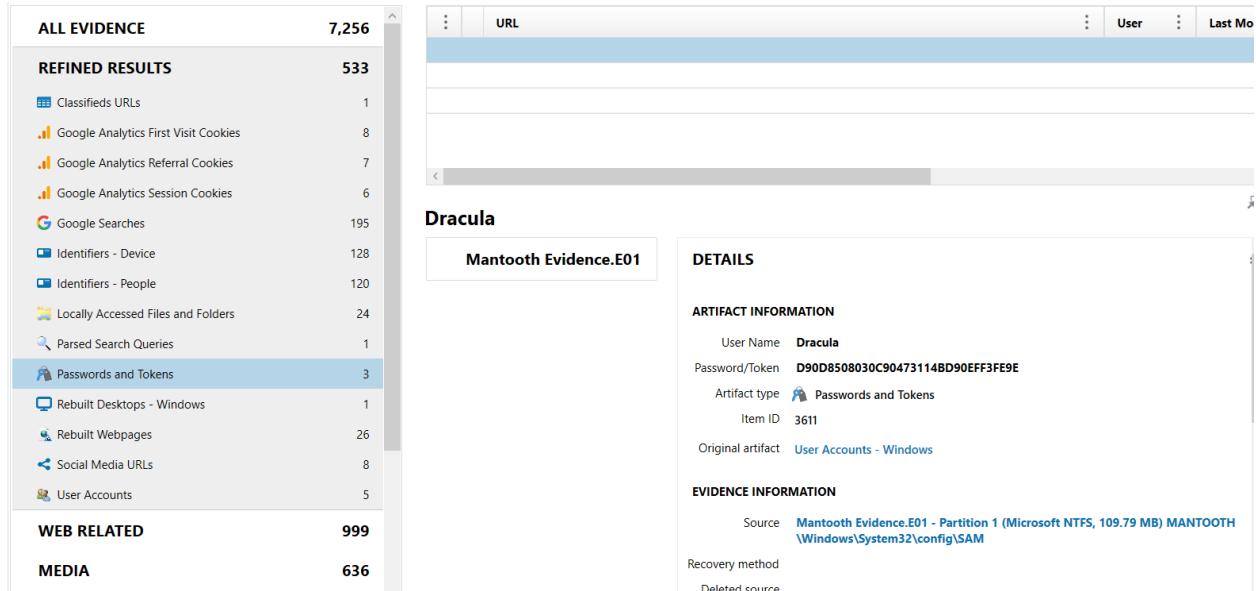


Figure 4.7 – Password for Dracula

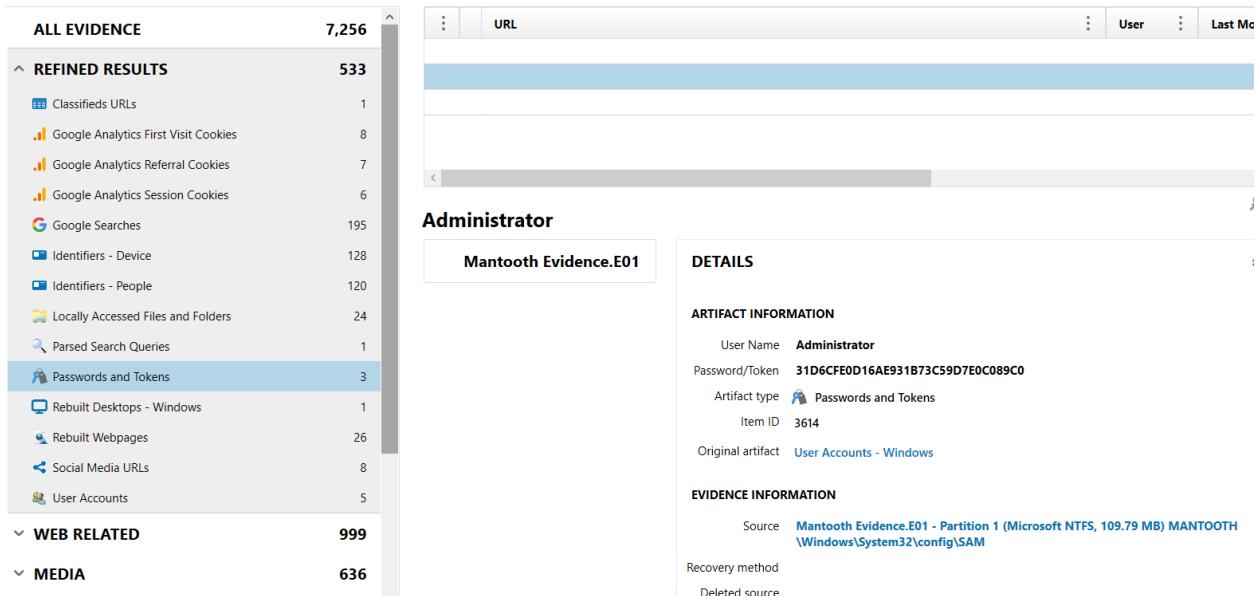
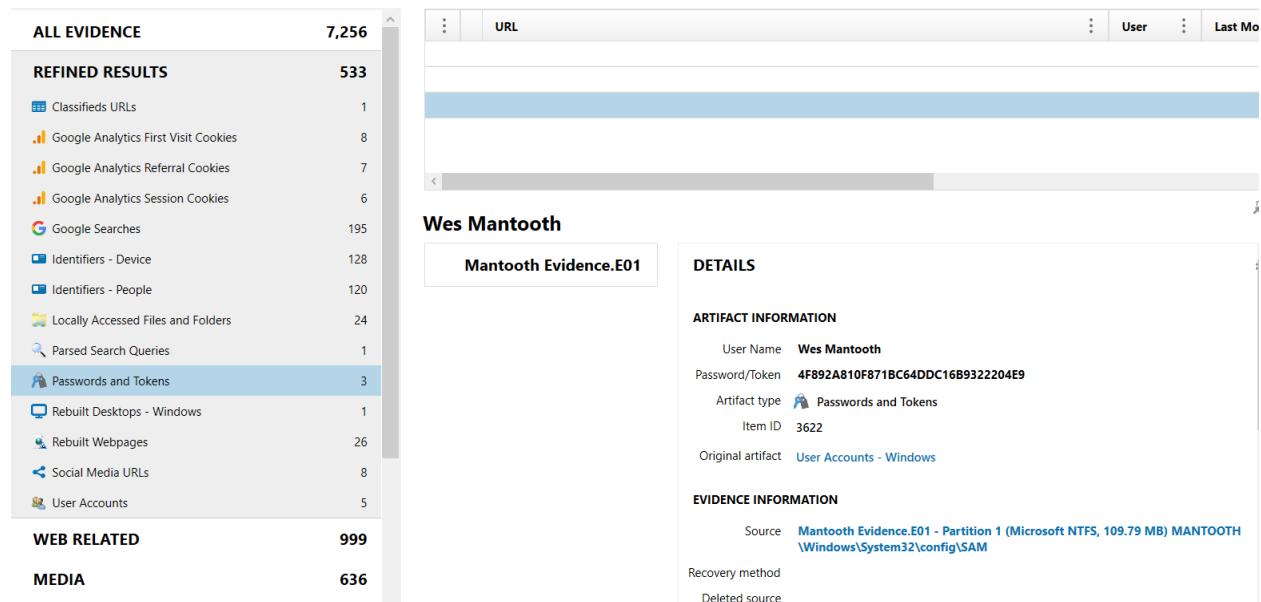


Figure 4.8 – Password for Administrator*Figure 4.9 – Password for Wes Mantooth*

User Accounts

Analysis of the user account registry revealed that there are five distinct profiles configured on this system. Figures 5.0 – 5.4 show the accounts listed, Dracula, Administrator, Laurent, Guest, and Wes Mantooth. The multiple users raises concern about possibly sharing access to this device. Dracula could be an alias that is used by Wes Mantooth, but the documents found on the device were suspicious.

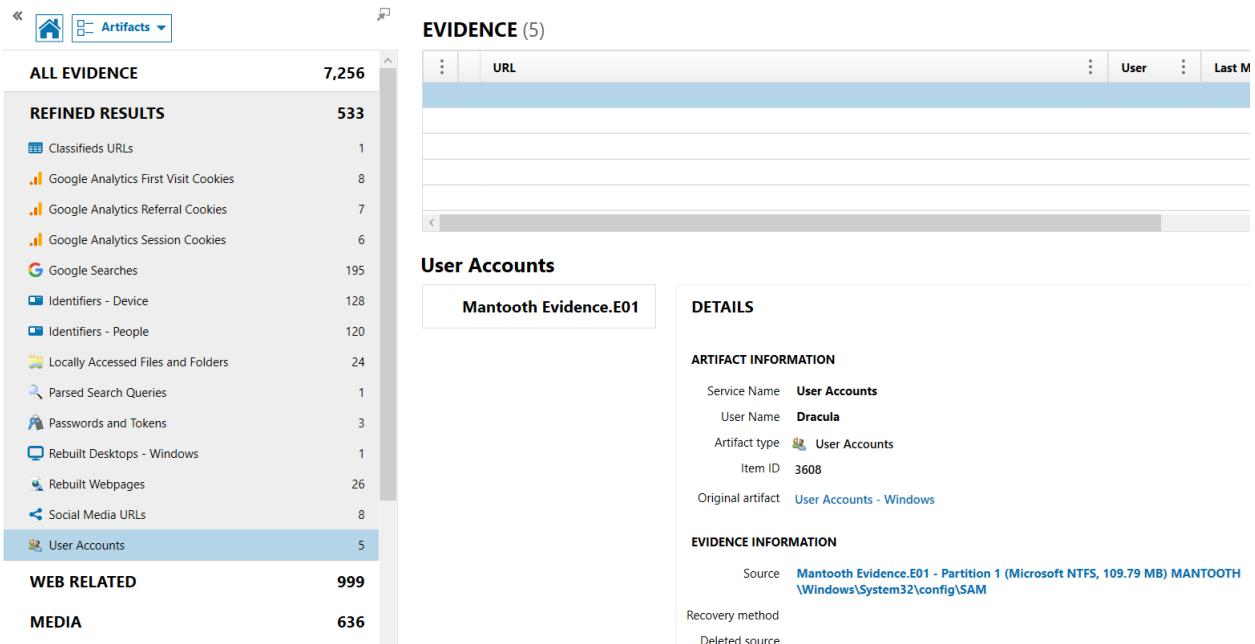


Figure 5.0 – Dracula user account

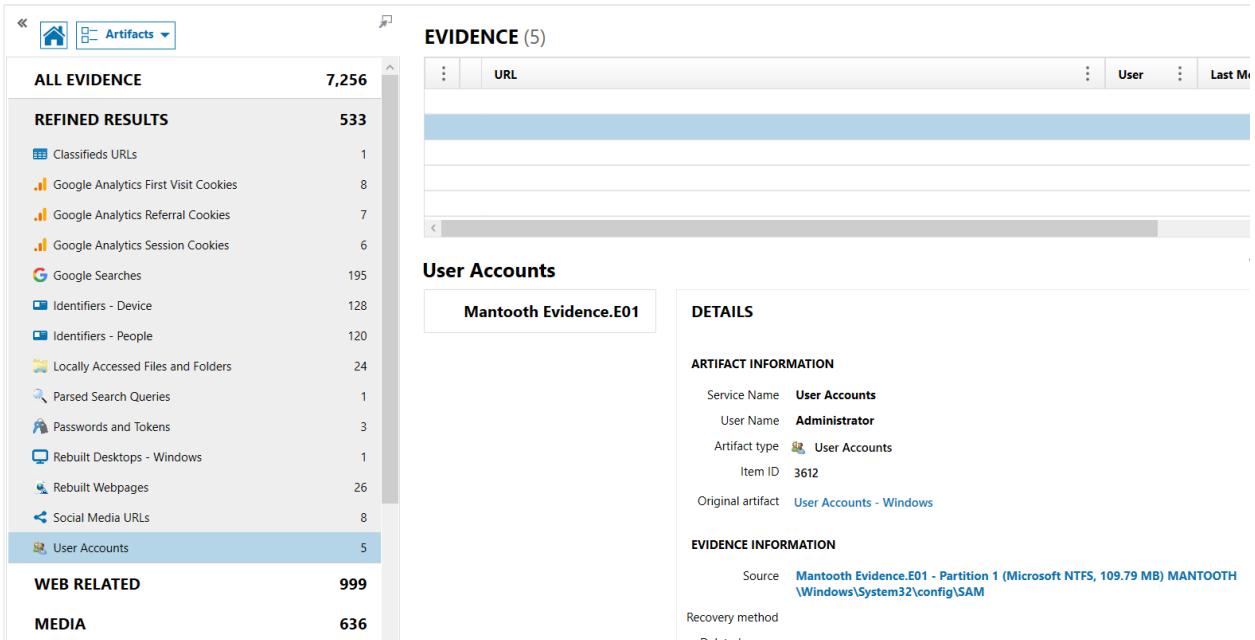


Figure 5.1 – Administrator user account

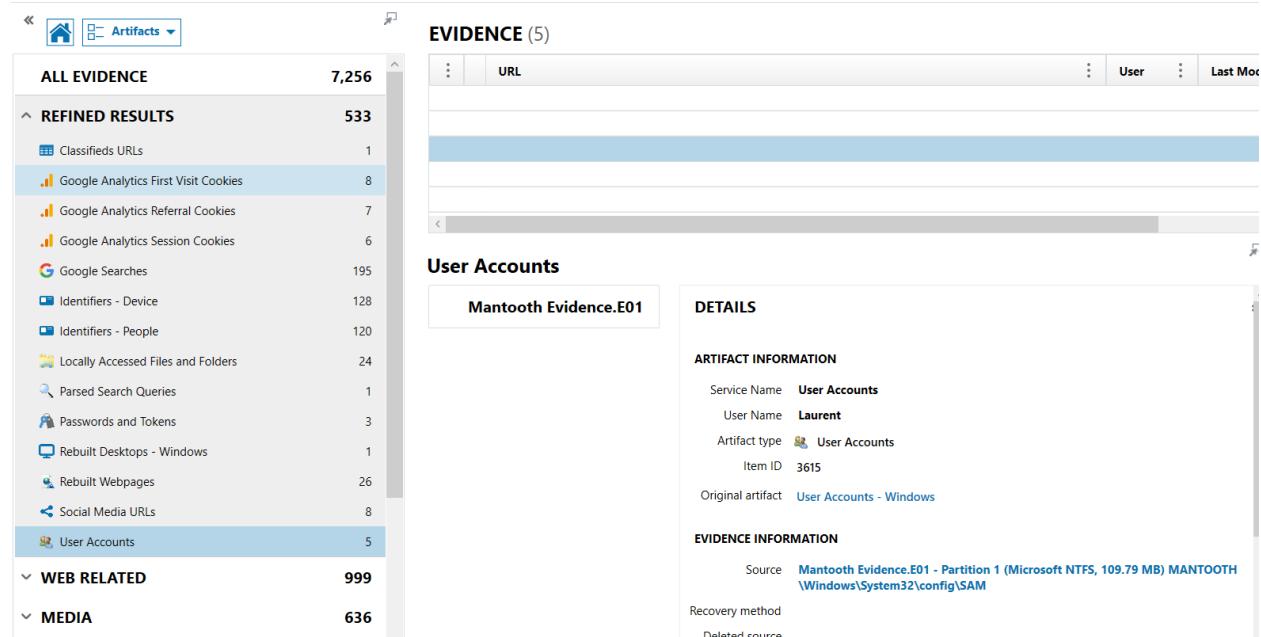


Figure 5.2 – Laurent user account

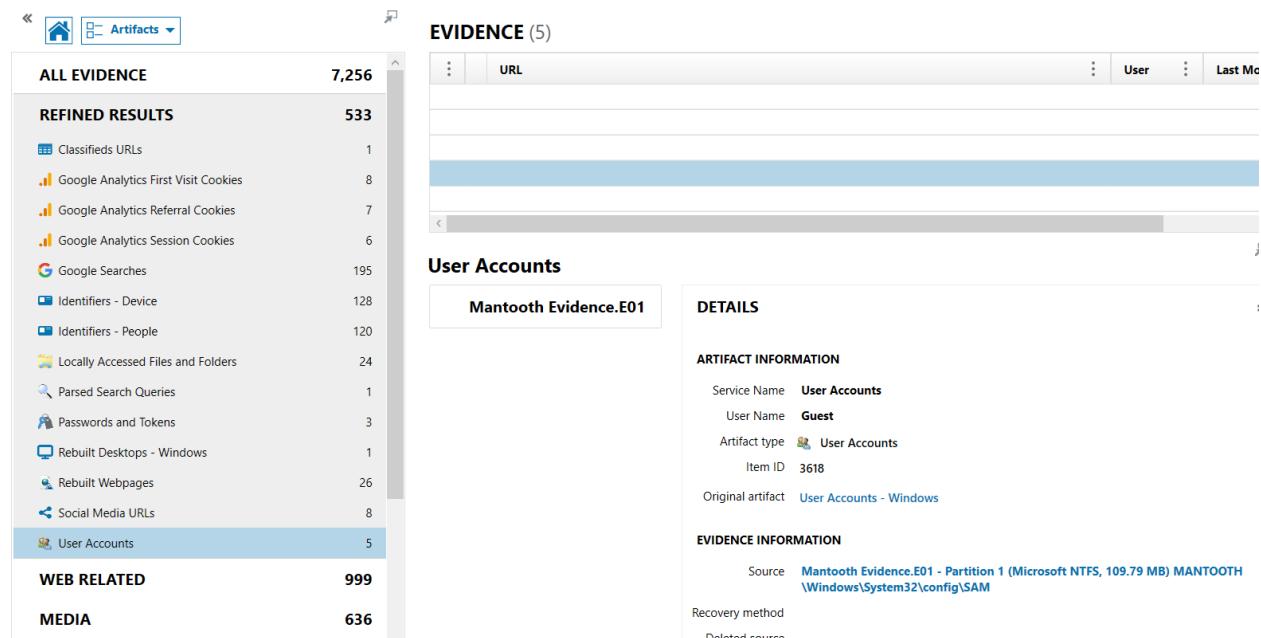


Figure 5.3 – Guest user account

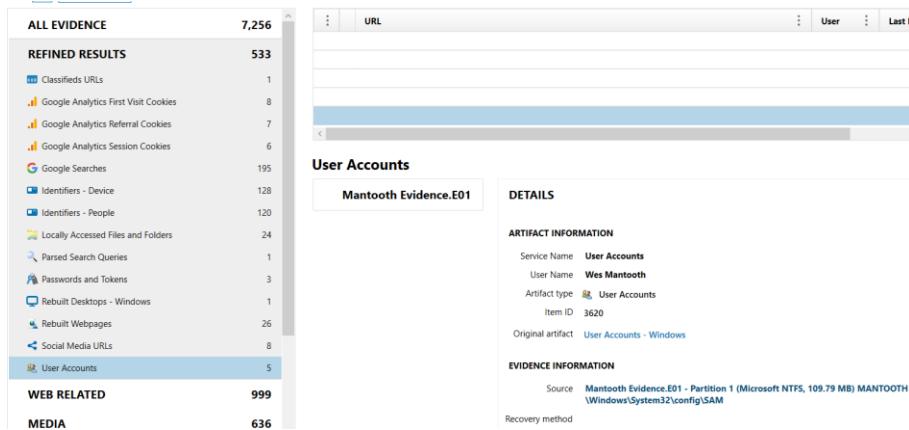


Figure 5.4 – Wes Mantooth user account

Documents

The forensic review of the suspects documents revealed files directly related to the criminal allegations. Figures 5.5 – 6.2 consist of a love letter, multiple vampire themed documents, and a confession document saying he committed all his crimes. There was also a file labeled “How to Steal Cars.txt” and a password-protected node that is labeled “read this.txt.” These documents could serve as evidence of intent.

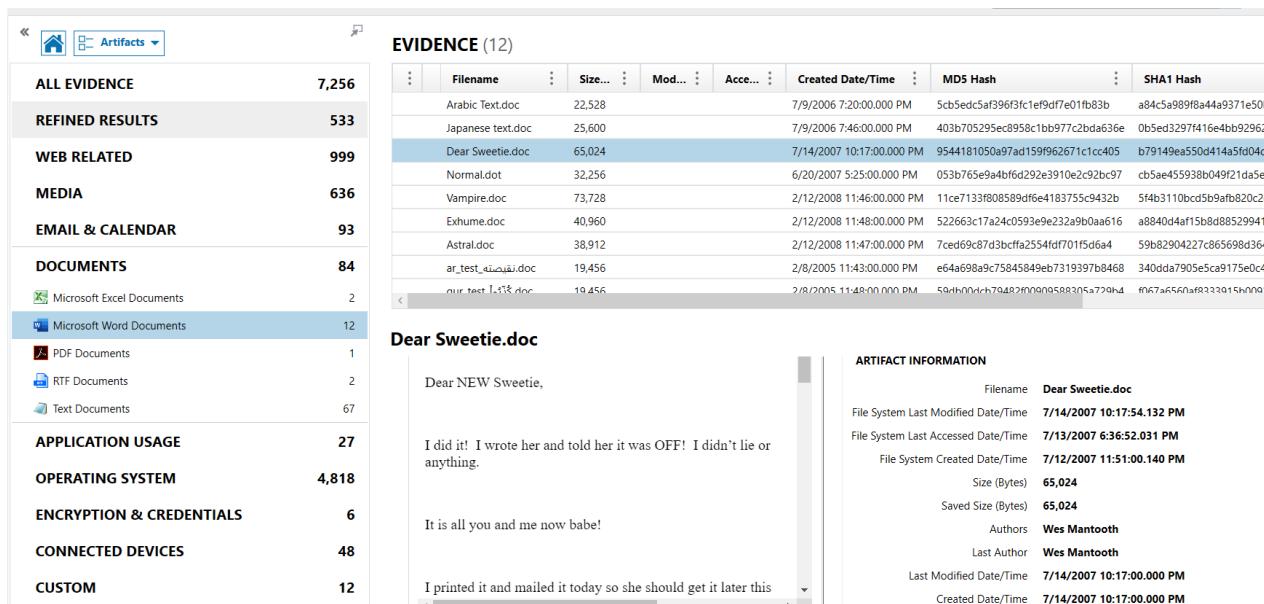


Figure 5.5 – Document from Wes Mantooth to his NEW sweetie

The screenshot shows the MANTOOTH investigation interface. On the left, a sidebar displays a tree view of evidence categories and sub-categories. The 'DOCUMENTS' category is expanded, showing Microsoft Word Documents, PDF Documents, RTF Documents, and Text Documents. The 'Microsoft Word Documents' section contains one item named 'Vampire.doc'. The main pane is titled 'EVIDENCE (12)' and lists 12 items. One item, 'Vampire.doc', is highlighted. The details for 'Vampire.doc' are shown on the right, including its file information: Filename: Vampire.doc, File System Last Modified Date/Time: 2/13/2008 12:06:54.000, File System Last Accessed Date/Time: 2/13/2008 12:53:11.609, File System Created Date/Time: 2/13/2008 12:53:11.609, Size (Bytes): 73,728, Title: Vampire, Saved Size (Bytes): 73,728, Last Author: XXX XXXXXX, Last Modified Date/Time: 2/13/2008 12:06:00.000, and Created Date/Time: 2/12/2008 11:46:00.000.

Figure 5.6 – Wikipedia page about vampires, makes sense for a Dracula user

The screenshot shows the MANTOOTH investigation interface. The sidebar is identical to Figure 5.6, with the 'Microsoft Word Documents' section expanded to show 'Exhum.e.doc'. The main pane is titled 'EVIDENCE (12)' and lists 12 items. One item, 'Exhum.e.doc', is highlighted. The details for 'Exhum.e.doc' are shown on the right, including its file information: Filename: Exhum.e.doc, File System Last Modified Date/Time: 2/13/2008 12:08:20.000 /, File System Last Accessed Date/Time: 2/13/2008 12:53:11.687 /, File System Created Date/Time: 2/13/2008 12:53:11.687 /, Size (Bytes): 40,960, Title: Exhuming the Vampire, Saved Size (Bytes): 40,960, Last Author: XXX XXXXXX, Last Modified Date/Time: 2/13/2008 12:07:00.000 /, and Created Date/Time: 2/12/2008 11:48:00.000 /.

Figure 5.7 – Story about vampires

EVIDENCE (12)

| | Filename | Size... | Mod... | Acce... | Created Date/Time | MDS Hash | SHA1 Hash |
|---------------------|----------|---------|--------|---------|--------------------------|---|---|
| Arabic.Text.doc | 22,528 | | | | 7/9/2006 7:20:00:00 PM | 5cb5edc5af396f3fc1ef9df7e01fb83b | a84c5e989f8a44a9371e50bdef262a5ce1570988 |
| Japanese.text.doc | 25,600 | | | | 7/9/2006 7:46:00:00 PM | 403b705295ec8958c1bb977c2bda636e | 0b5ed32974164bb92962a2e75c62e1a13638b2 |
| Dear.Sweetie.doc | 65,024 | | | | 7/14/2007 10:17:00:00 PM | 9544181050a97ad159962671c1cc405 | b79149ea550d414a5fd04c0f384fbcd95fa97e |
| Normal.dot | 32,256 | | | | 6/20/2007 5:25:00:00 PM | 053b765e9abf6cd292e3910e2c2bdc97 | cbsae4559380b049f21d5e4d4f2e813bd732 |
| Vampire.doc | 73,728 | | | | 2/12/2008 11:46:00:00 PM | 11c71133808589dfe6e18375c5432b | 5f4b3110bcd5b9af8b820c2e3ff444e6827a282 |
| Exhume.doc | 40,960 | | | | 2/12/2008 11:48:00:00 PM | 522663c17a24c0593e9e232a9b0aa616 | a8840d4af15b8d088529941252dc095258e604830 |
| Astral.doc | 38,912 | | | | 2/12/2008 11:47:00:00 PM | 7ced69c87d3bcfa2554fd701f5d6a4 | 59b82904227c65698d364fa50c51a5cc663e001 |
| ar_test_العنوان.doc | 19,456 | | | | 2/8/2005 11:43:00:00 PM | e64a698a9c7504849eb7319397b8468 | 340dda7905e5ca9175e04d7e7c5412d3e3267e |
| our_test_1.xls.doc | 19,456 | | | | 2/8/2005 11:48:00:00 PM | 59b82904227c65698d364fa50c51a5cc663e001 | 9a74a560a8333915h0j0j7r7n7r5c9baaa8a |

Astral.doc

FIND

Astral\_Vampire

A psychic vampire that exists on the astral plane. It can also be a skilled magician who's physical body has died, but chooses to resist the second death or astral death, by way of becoming a psychic vampire... It is also a psychic vampire that has died in the physical plane but for some reason may not be able to incarnate.

Emotional Vampire

It is important to note that there are three forms of emotional vampires: The First one is the psychological term of an emotionally needy person. This person may not technically be a vampire just an ordinary mundane who might have had something traumatize them, and they crave constant attention or emotional energy from a person...Unfortunately for the vampire community, psychologists coined the term "psychic vampire", to represent these emotional vampires...They are often

ARTIFACT INFORMATION

| | |
|-------------------------------------|---------------------------|
| Filename | Astral.doc |
| File System Last Modified Date/Time | 2/13/2008 12:09:04:000 AM |
| File System Last Accessed Date/Time | 2/13/2008 12:53:11.750 AM |
| File System Created Date/Time | 2/13/2008 12:53:11.734 AM |
| Size (Bytes) | 38,912 |
| Title | Astral Vampire |
| Saved Size (Bytes) | 38,912 |
| Last Author | XXX XXXXXX |
| Last Modified Date/Time | 2/13/2008 12:07:00:000 AM |
| Created Date/Time | 2/12/2008 11:47:00:000 PM |

TAG!

No t
ADD

Select
□ ■
□ □
□ □
□ □

Figure 5.8 – Different types of vampires

EVIDENCE (67)

| | Filename | Size... | Mod... | Acce... | Created Date/Time | MDS Hash | SHA1 Hash |
|---------------------------|----------|--------------|--------------|--------------------------|----------------------------------|---|-----------|
| My.poem.txt | 168 | 4/13/2007... | 7/13/2007... | 4/13/2007 1:01:38.000 AM | 100532339b2b7e466e8b99f687c2bb7a | f5e06ab83ba5830dfdcda238c7a20f49689101675 | |
| readthis.txt | 421 | 7/13/2007... | 7/13/2007... | 3/6/2007 2:16:55.000 AM | 94d1af666b1a813cd05d452cd33404cc | 62af329a7b0702b7d4159d938e6bf4f33bddd9f | |
| readthis.txt.password.... | 73 | 7/13/2007... | 7/13/2007... | 3/6/2007 2:16:55.000 AM | 18a2b15b7e0d0499186a2fe321a0 | b228298580076f0daa699c9b5041ed2d282... | |
| readme.txt | 519 | 11/13/200... | 7/14/2007... | 7/14/2007 6:02:20.346 PM | 4f13601b5dfe6b56672fed5fd206cf | 9212461ec880f0ab083f06ae1fcba1aae857846b | |
| PGPLog.txt | 591 | 7/7/2007... | 7/7/2007... | 7/7/2007 10:57:32.606 PM | a3f9393b71b2d1edcf5b75be6fcfd7a | 521890f47b6e03cb1be5a9821e2d4ee8b8024542 | |
| PGPLog1.txt | 739 | 6/24/2007... | 7/7/2007... | 7/7/2007 10:57:32.648 PM | a6d0075332hd9f8887b6d2705f59ab8 | 1ae2a5195d99aa48a2544f867e76e7d0d8d5413c | |
| PGPLog2.txt | 493 | 6/22/2007... | 7/7/2007... | 7/7/2007 10:57:32.728 PM | 608g2d24130e441be4b2d4565b585 | f5b5dd046894e1346fc6782bc1b73d471a29 | |
| PGPLog3.txt | 747 | 6/21/2007... | 7/7/2007... | 7/7/2007 10:57:32.774 PM | 6ffe02a6e8b7e1cd4d256d4ec69cd93 | f34925cf7e048e517d63910080d7af5a97043094 | |
| PGPLog4.txt | 1,130 | 6/20/2007... | 7/7/2007... | 7/7/2007 10:57:32.823 PM | 6h12795a745e610952763e414de1a45 | 4d717da10hahk7rrawr111h7f3a3d1h8r01 | |

My.poem.txt

FIND

In the yard of a farmer named Skutter, there lived a brown cow who gave butter.

She said, I should spurn being used as a churn, cause it really is hard on the utter!

ARTIFACT INFORMATION

| | |
|--------------------|---|
| Filename | My.poem.txt |
| Size (Bytes) | 168 |
| Modified Date/Time | 4/13/2007 1:06:14.110 AM |
| Accessed Date/Time | 7/13/2007 6:37:44.421 PM |
| Created Date/Time | 4/13/2007 1:01:38.000 AM |
| MDS Hash | 100532339b2b7e466e8b99f687c2bb7a |
| SHA1 Hash | f5e06ab83ba5830dfdcda238c7a20f49689101675 |
| Artifact type | Text Documents |
| Item ID | 227 |

TAG!

No t
ADD

Select
□ ■
□ □
□ □
□ □

Figure 5.9 – Short poem

| EVIDENCE (67) | |
|---------------------------|-------|
| ALL EVIDENCE | 7,256 |
| REFINED RESULTS | 533 |
| WEB RELATED | 999 |
| MEDIA | 636 |
| EMAIL & CALENDAR | 93 |
| DOCUMENTS | 84 |
| Microsoft Excel Documents | 2 |
| Microsoft Word Documents | 12 |
| PDF Documents | 1 |
| RTF Documents | 2 |
| Text Documents | 67 |
| APPLICATION USAGE | 27 |
| OPERATING SYSTEM | 4,818 |
| ENCRYPTION & CREDENTIALS | 6 |
| CONNECTED DEVICES | 48 |
| CUSTOM | 12 |

readthis.txt:password.txt

| PREVIEW | |
|---------|---|
| FIND | the password for the doc I'm sending you is:
supercallifragilistic |

| DETAILS | |
|----------------------|------------------------------------|
| ARTIFACT INFORMATION | |
| Filename | readthis.txt:password.txt |
| Size (Bytes) | 73 |
| Modified Date/Time | 7/13/2007 6:59:08.000 PM |
| Accessed Date/Time | 7/13/2007 7:05:02.140 PM |
| Created Date/Time | 3/6/2007 2:16:55.000 AM |
| MD5 Hash | 18a2b15fb7ee8d49c9186a2fec3211a0 |
| SHA1 Hash | b228298580076f0ddaa6959cb56041edd2 |
| Artifact type | Text Documents |

Figure 6.0 – Password for read this.txt

| EVIDENCE (67) | |
|---------------------------|-------|
| ALL EVIDENCE | 7,256 |
| REFINED RESULTS | 533 |
| WEB RELATED | 999 |
| MEDIA | 636 |
| EMAIL & CALENDAR | 93 |
| DOCUMENTS | 84 |
| Microsoft Excel Documents | 2 |
| Microsoft Word Documents | 12 |
| PDF Documents | 1 |
| RTF Documents | 2 |
| Text Documents | 67 |
| APPLICATION USAGE | 27 |
| OPERATING SYSTEM | 4,818 |
| ENCRYPTION & CREDENTIALS | 6 |
| CONNECTED DEVICES | 48 |
| CUSTOM | 12 |

My Confession.txt

| PREVIEW | |
|---------|---|
| FIND | 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! |

| DETAILS | |
|----------------------|--|
| ARTIFACT INFORMATION | |
| Filename | My Confession.txt |
| Size (Bytes) | 232 |
| Modified Date/Time | 8/14/2007 9:26:41.770 PM |
| Accessed Date/Time | 2/13/2008 12:53:11.953 AM |
| Created Date/Time | 2/13/2008 12:53:11.953 AM |
| MD5 Hash | 08600d459d2af187c5943e354518d885 |
| SHA1 Hash | 620b85d6efbf2e01811cd0e8d10c563dfc11b5a0 |
| Artifact type | Text Documents |
| Item ID | 5962 |

Figure 6.1 – Confession text

The screenshot shows the 'Artifacts' tab selected in the top navigation bar. The main pane displays a table titled 'EVIDENCE (67)' with columns for Filename, Size..., Mod..., Acc..., Created Date/Time, MD5 Hash, and SHA1 Hash. One row is highlighted for 'How to Steal Cars.txt'. To the left is a sidebar with a tree view of evidence categories and their counts.

| EVIDENCE (67) | | | | | | | |
|-----------------------|----------|--------------|--------------|---------------------------|----------------------------------|--|-----------|
| | Filename | Size... | Mod... | Acc... | Created Date/Time | MD5 Hash | SHA1 Hash |
| wes_mantooth@yahoo... | 158 | 6/18/2007... | 7/7/2007... | 7/7/2007 10:57:26.906 PM | 030533bb89d3e7e8264077c52f5bd2 | 65c31ba9e7040a0cd914b8985b66ae | |
| wes_mantooth@out... | 386 | 4/10/2007... | 7/7/2007... | 7/7/2007 10:57:26.950 PM | 041ed9ef6f66eaaf96de8af4fe3e450f | 380fbf071ae4ca9e6997bc09142911394 | |
| cookies.txt | 6,899 | 4/12/2007... | 7/7/2007... | 7/7/2007 10:57:31.315 PM | f1e8d32b13ff63fc6ea4a1a687395eed | 30da8b966cb2fc098827f10bf02e6e40 | |
| signons2.txt | 631 | 4/10/2007... | 7/7/2007... | 7/7/2007 10:57:18.002 PM | 3e3701573f0f058b047c076353590667 | 8de91ee8a835b16cf248c69e43bb03d | |
| My Confession.txt | 232 | 8/14/2007... | 2/13/2008... | 2/13/2008 12:53:11.953 AM | 08600d459d2af187c5943e354518d885 | 620b85d6efbf2e01811cd0e8d10c563d | |
| Readme.txt | 354 | 1/30/2007... | | | 627edb48c5e4c22891ba05fb6f7e | 5ebf9d9362b0fe9723510cc4c1513e961c | |
| How to Steal Cars.txt | 4,956 | 8/15/2007... | 8/15/2007... | 8/15/2007 6:10:46.000 PM | 9866e5371005b1e536b7a16d8fb9d85b | 6a8c743c61f3997bb0e7503cb68088b5abc04b10 | |

How to Steal Cars.txt

PREVIEW

FIND Top 10 Lists See all Top 10 Lists

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

DETAILS

ARTIFACT INFORMATION

- Filename: How to Steal Cars.txt
- Size (Bytes): 4,956
- Modified Date/Time: 8/15/2007 6:10:46.000 PM
- Accessed Date/Time: 8/15/2007 6:11:02.000 PM
- Created Date/Time: 8/15/2007 6:10:46.000 PM
- MD5 Hash: 9866e5371005b1e536b7a16d8fb9d85b
- SHA1 Hash: 6a8c743c61f3997bb0e7503cb68088b5abc04b10
- Artifact type: Text Documents
- Item ID: 7250

Figure 6.2 – How to Steal Cars.txt

Encryption and Credentials

Six encrypted files were identified during this investigation, as seen in Figure 6.3.

Decryption was unsuccessful. These files could contain crucial information that is intentionally hidden. No password plaintext credentials were found directly linked to these encrypted files.

The screenshot shows the 'Artifacts' tab selected in the top navigation bar. The main pane displays a table titled 'EVIDENCE (6)' with columns for File Name, File..., Detected File..., File Created Date/T..., File Modified Date..., File Accessed Date/..., and MD5 Hash. One row is highlighted for 'CRACK\_ME'. To the left is a sidebar with a tree view of evidence categories and their counts.

| EVIDENCE (6) | | | | | | | |
|----------------------|-----------|---------------------|---------------------------|---------------------------|---------------------------|--------------------------------|----------|
| | File Name | File... | Detected File... | File Created Date/T... | File Modified Date... | File Accessed Date/... | MD5 Hash |
| CRACK_ME | 1,048,576 | Encrypted Container | 4/11/2007 1:27:59.000 AM | 4/10/2007 10:06:34.000 PM | 6/20/2008 3:50:52.658 PM | 5a4f05e108dfd3b466166b428144d9 | |
| Those who owes.xls | 13,824 | Excel | 7/12/2007 11:01:16.447 PM | 7/12/2007 10:58:45.735 PM | 9/26/2007 7:57:11.859 PM | 655c3528129b43a3267c27f23507a3 | |
| secring.skr | 2,944 | Pgp | 4/13/2007 12:26:33.000 AM | 7/7/2007 8:30:23.000 PM | 4/13/2007 12:26:33.000 AM | 66f6ba488735fea0720306fe65b42c | |
| ar_test_٤صٰنٰع.doc | 19,456 | Word | 2/13/2008 12:53:11.984 AM | 5/26/2006 11:09:02.000 PM | 2/13/2008 12:53:12.015 AM | e64a989ac758459467e319397b64 | |
| qur_test_۱۹۴۳.doc | 19,456 | Word | 2/13/2008 12:53:12.046 AM | 5/26/2006 11:09:08.000 PM | 2/13/2008 12:53:12.046 AM | 59db00dc794820090988305a725 | |
| russ_2_Абакурный.doc | 19,456 | Word | 2/13/2008 12:53:12.062 AM | 5/26/2006 11:09:08.000 PM | 2/13/2008 12:53:12.062 AM | 1d6908ad43811c7945ed83ea564 | |

CRACK\_ME

DETAILS

ARTIFACT INFORMATION

- File Name: CRACK\_ME
- File Size (Bytes): 1,048,576
- Detected File Type: Encrypted Container
- File Created Date/Time: 4/11/2007 1:27:59.000 AM
- File Modified Date/Time: 4/10/2007 10:06:34.000 PM
- File Accessed Date/Time: 6/20/2008 3:50:52.658 PM
- MD5 Hash: 5a4f05e108dfd3b466166b428144d9e5
- SHA1 Hash: c5ee46da850d0f719ddaa79ec83f49a9b06772
- Artifact type: Encrypted Files

Figure 6.3 – 6 Encrypted files

Recycle Bin

A single deleted file was identified as “Validate Credit Card.zip”, Figure 6.4. The filename suggests the contents may involve tools related to credit card fraud. Since this file was placed in the recycle bin it shows the suspect is trying to dispose of evidence.

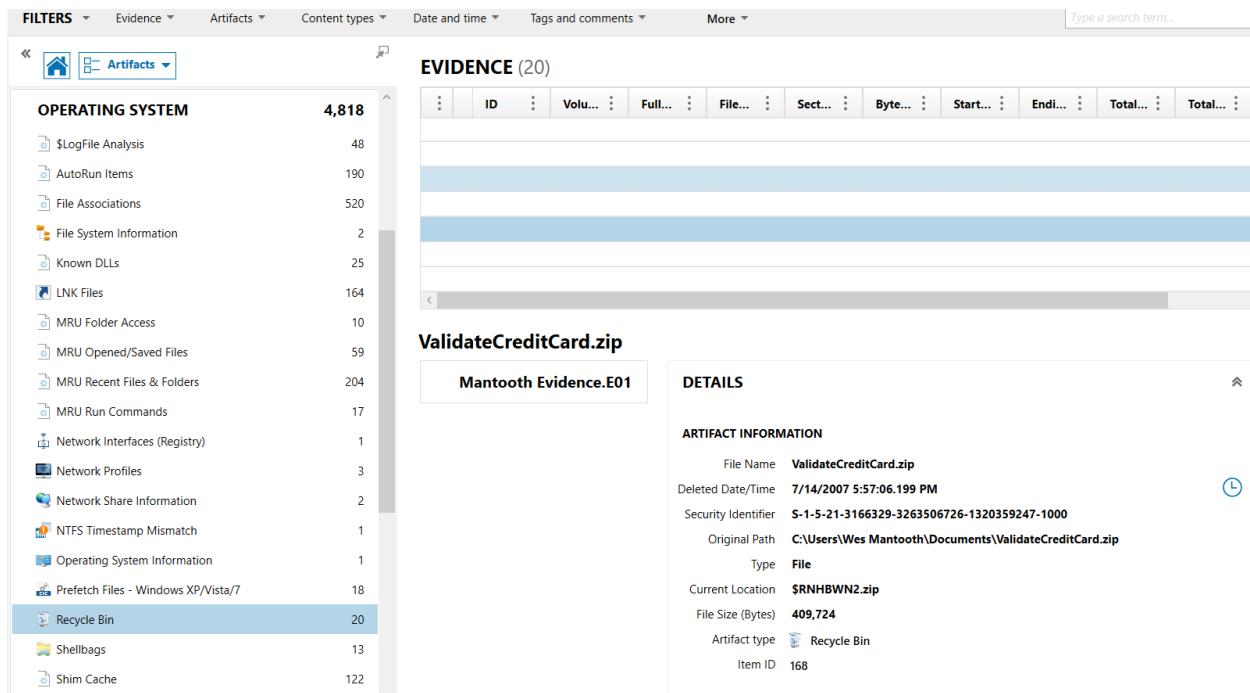


Figure 6.4 – Validate Credit Card

Conclusion

The forensic examination of Wes Mantooth's laptop was conducted with careful attention to preserving the integrity of the evidence. I utilized FTK Imager to create an exact disk image and ensured all the files and data were analyzed according to proper digital forensics procedures. After the imaging process, the forensic analysis was performed using Forensic Explorer and AXIOM. These are two digital forensic tools that allow for detailed examination all while keeping the original data. Due to these two systems, a thorough review of the suspect's laptop was created. The analysis revealed substantial evidence linking the suspect to multiple forms of criminal activity. Media files were recovered from the drive that included images of fake prescriptions, counterfeit checks and ingredients commonly associated with making meth. The suspect's search history included numerous searches relating to check washing and how to make meth. In the Recycle bin, a zip file was discovered by the name of "validate credit card.zip." This shows that the suspect very well could have something they wanted to hide. The digital forensic evidence that was collected from Wes Mantooth's laptop helps the ongoing investigation relating to drug and fraud schemes.

Appendix of Terms

AXIOM – A digital investigation tool designed collect, examine, and interpret data.

Check Washing – A form of fraud that involves the alteration of checks.

Digital Forensics – The practice of collecting, preserving, analyzing, and digital evidence in a legally manner.

Disk Image – An exact digital replica of a device.

Encrypted File – A file that has been encoded to restrict access, passwords are required.

Forensic Explorer – A forensic analysis tool used to examine and interpret data from disk images.

FTK Imager – A tool that used to make exact copies of data from digital storage devices forensic images of digital storage devices.

Hash Value – Special code made from data to help check if the data has been changed.