Mantooth Investigation

Ferris State University

DFOR310

Dr. Hawkins

Alexis Cherpes

March 9, 2025

Table of Contents

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.

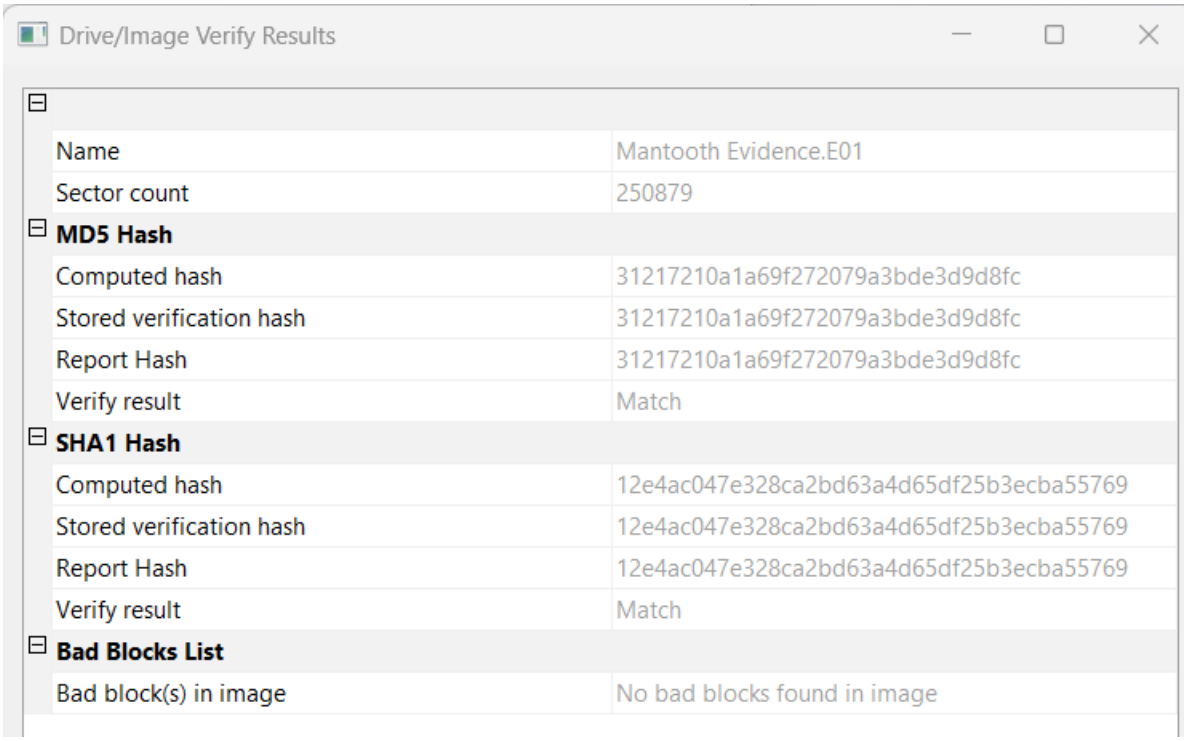

Figure 1.1

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.

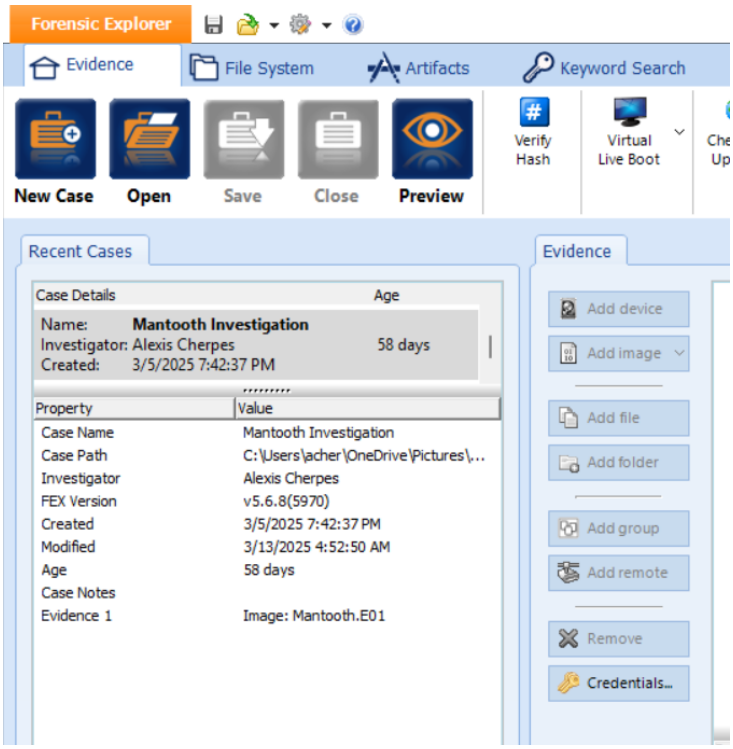

Figure 1.2

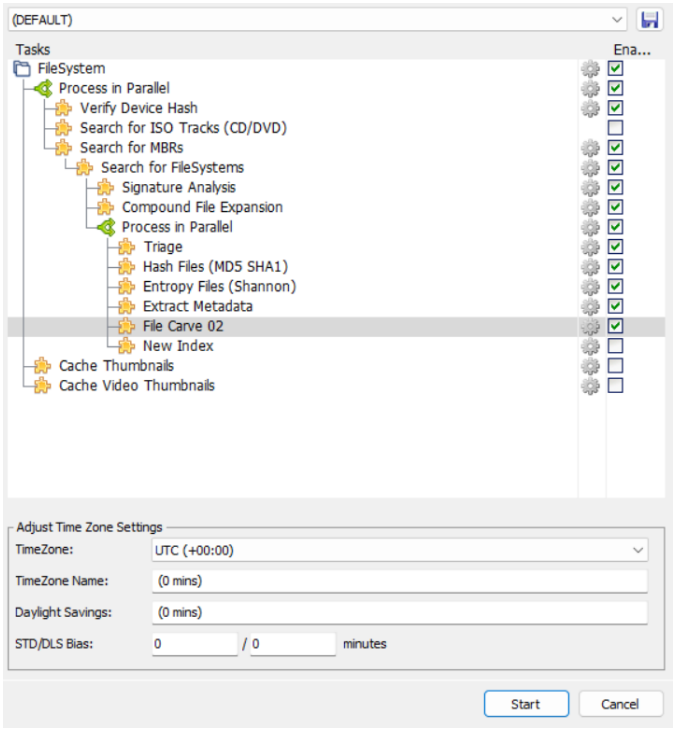

Figure 1.3

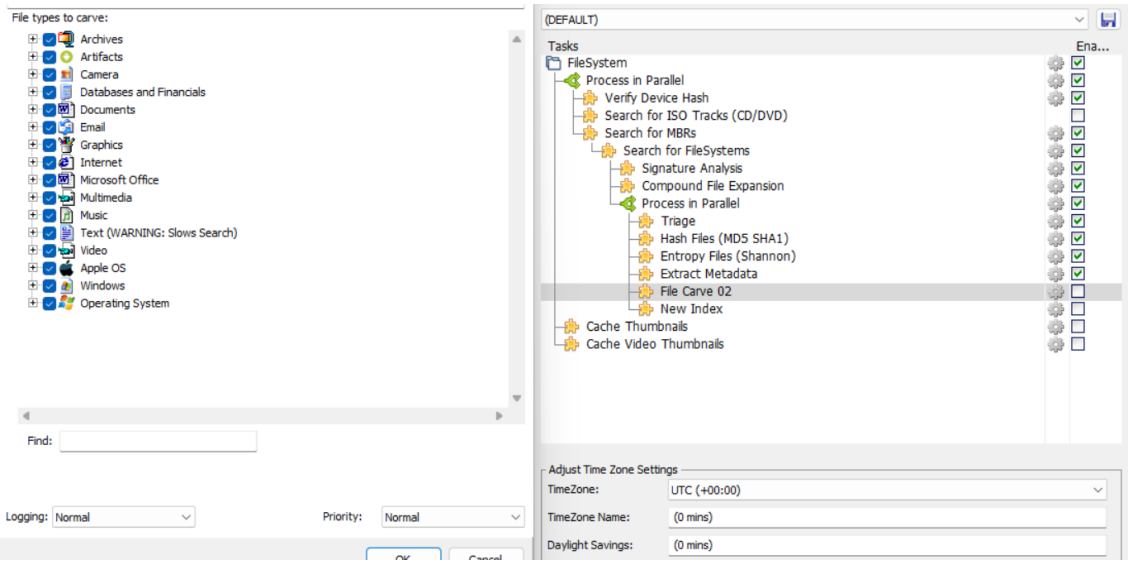

Figure 1.4

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 week 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.

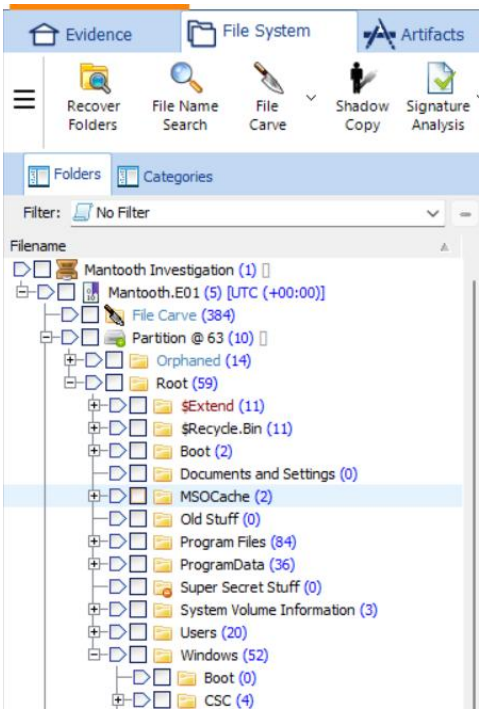

Figure 1.5

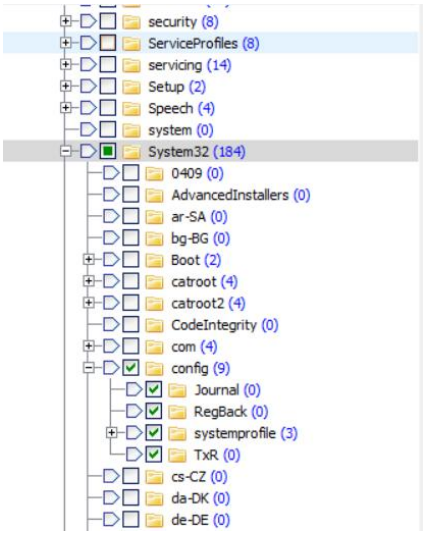

Figure 1.6

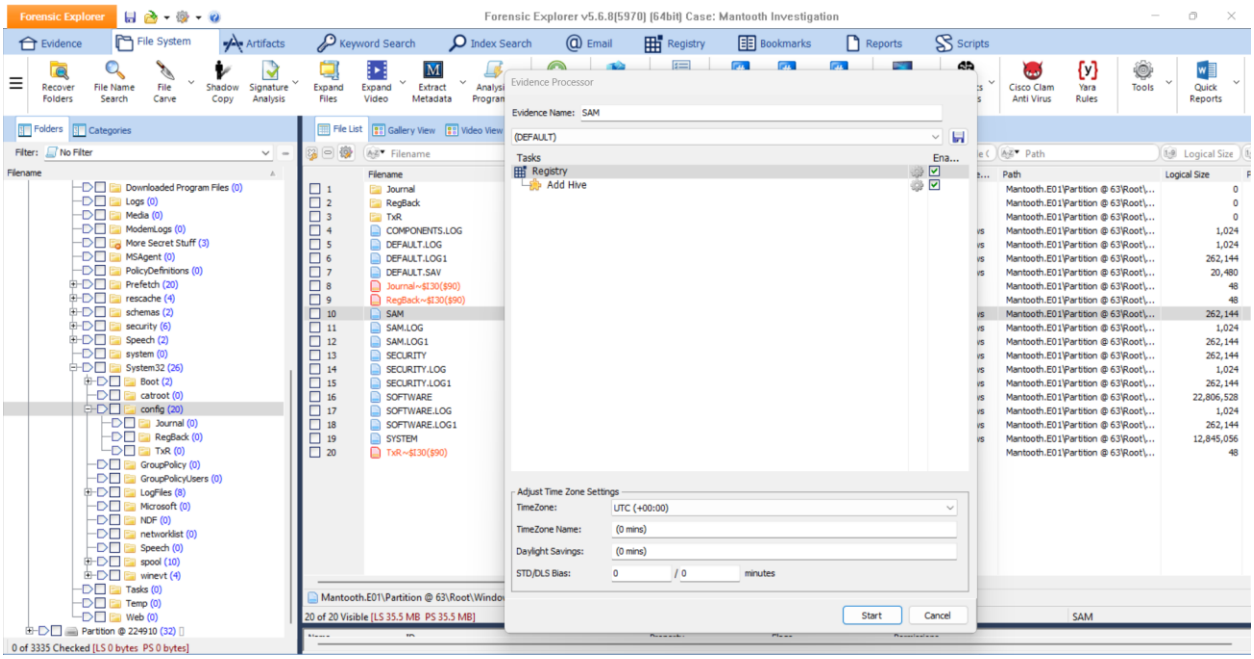

Figure 1.7 – SAM registry being added

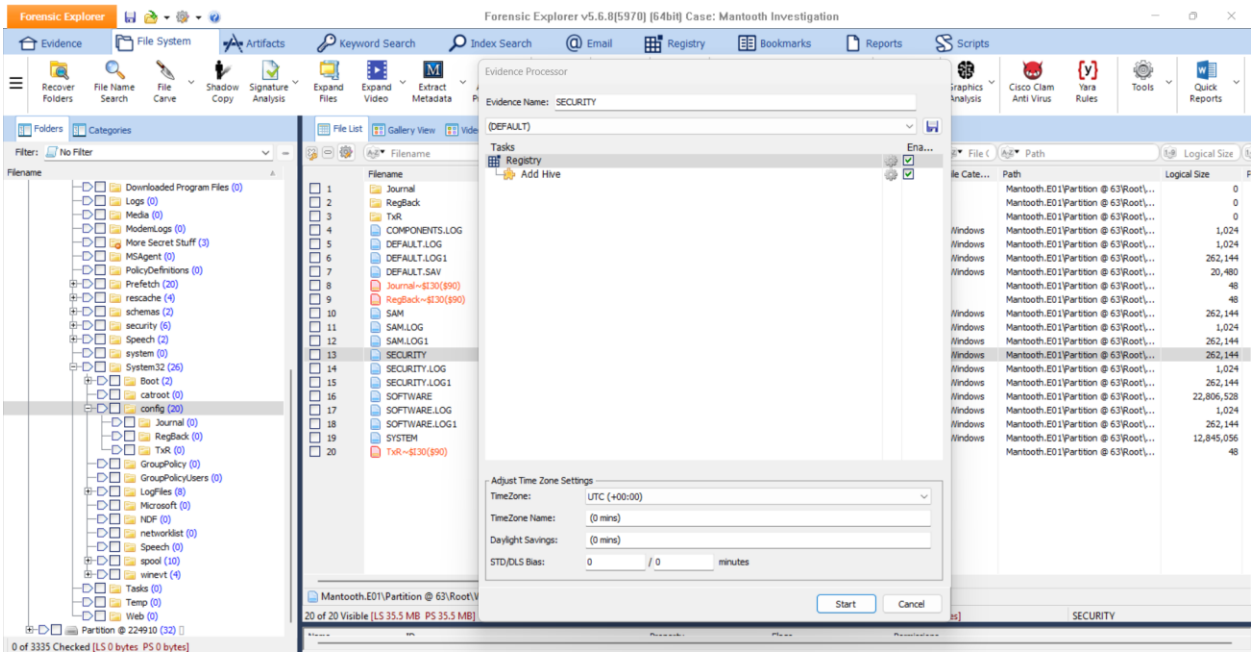

Figure 1.8 – Security registry being added

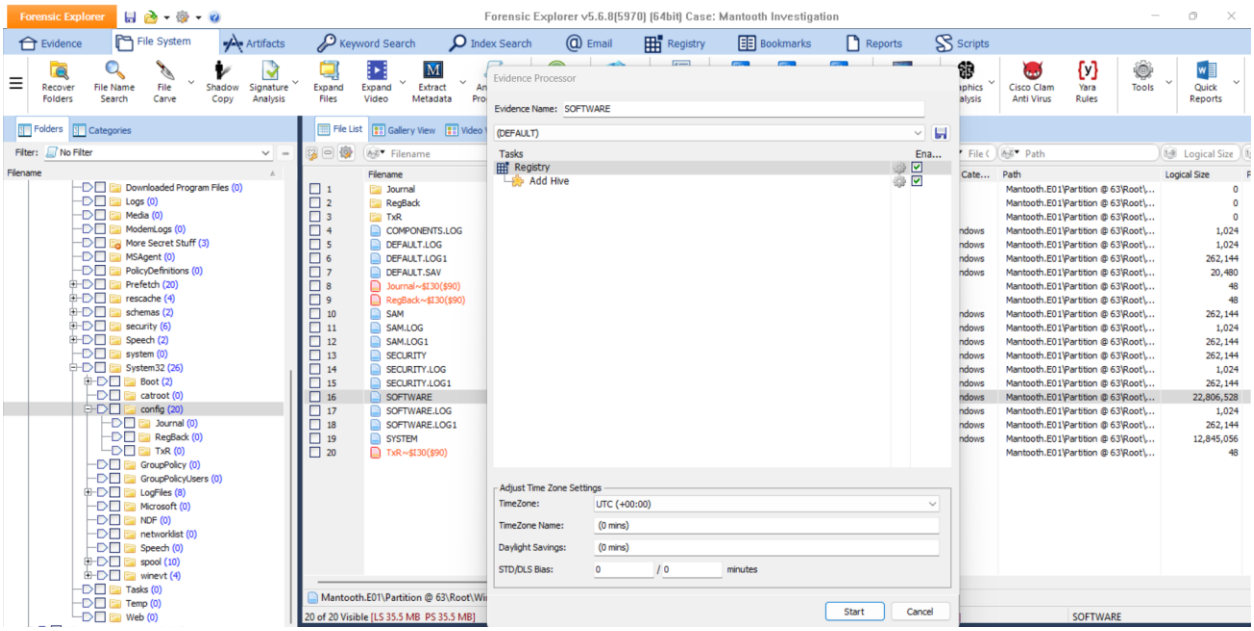

Figure 1.9 – Software registry being added

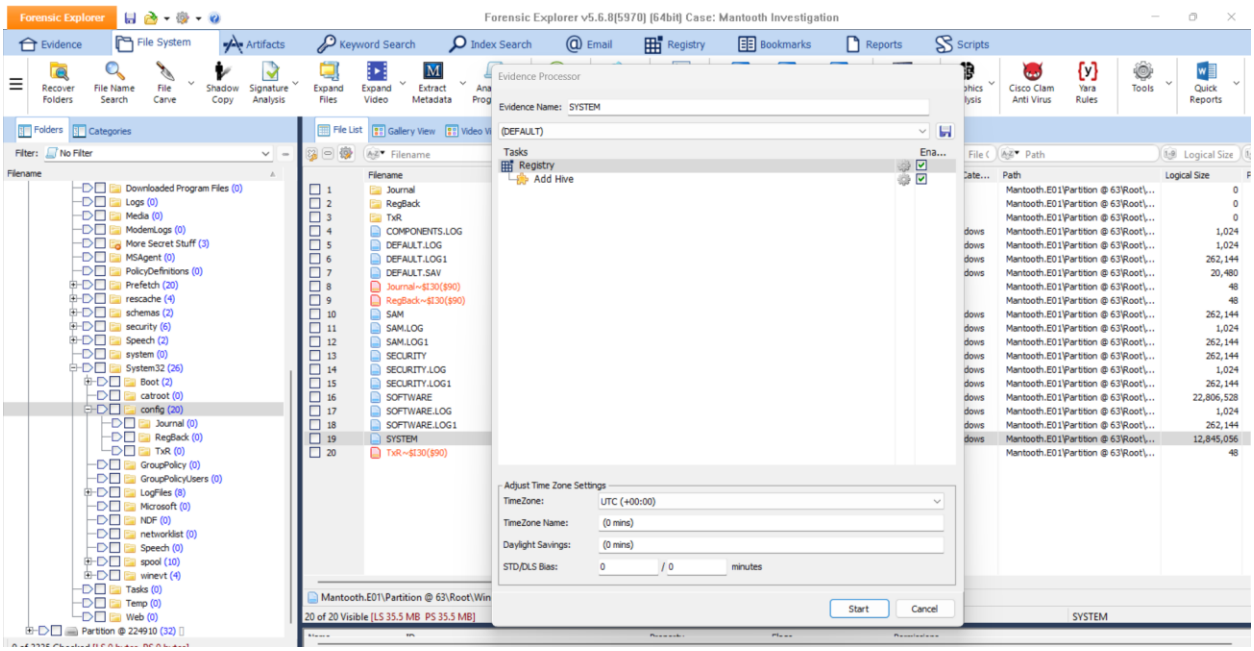

Figure 2.0 – System registry being added

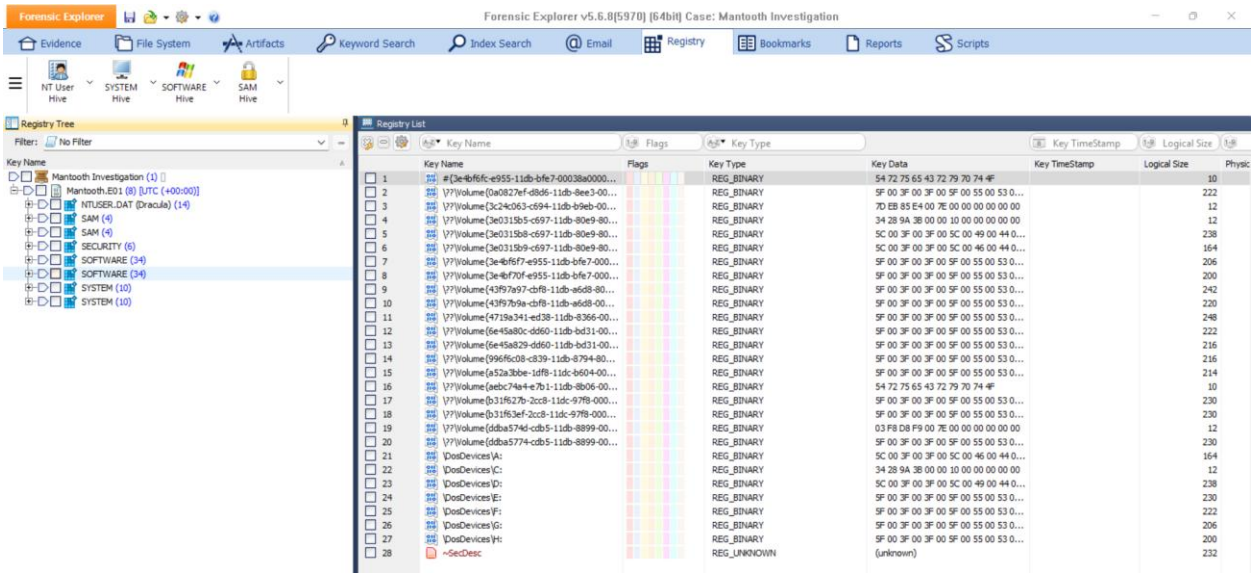

Figure 2.1 – The registry for the Mantooth Device

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\ActiveTouchMeetingClient\

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 http://en-US.www.mozilla.com/en-US/

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 http://www.truecrypt.org/

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	http://www.microsoft.com

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	http://www.microsoft.com/support

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	WESMANTOOTH-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 0xFFFFFFC4

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 0xFFFFFFC4

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_USB20&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_USB20&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&Rev_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&Rev_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_G3&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_G3M&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_G3M&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.

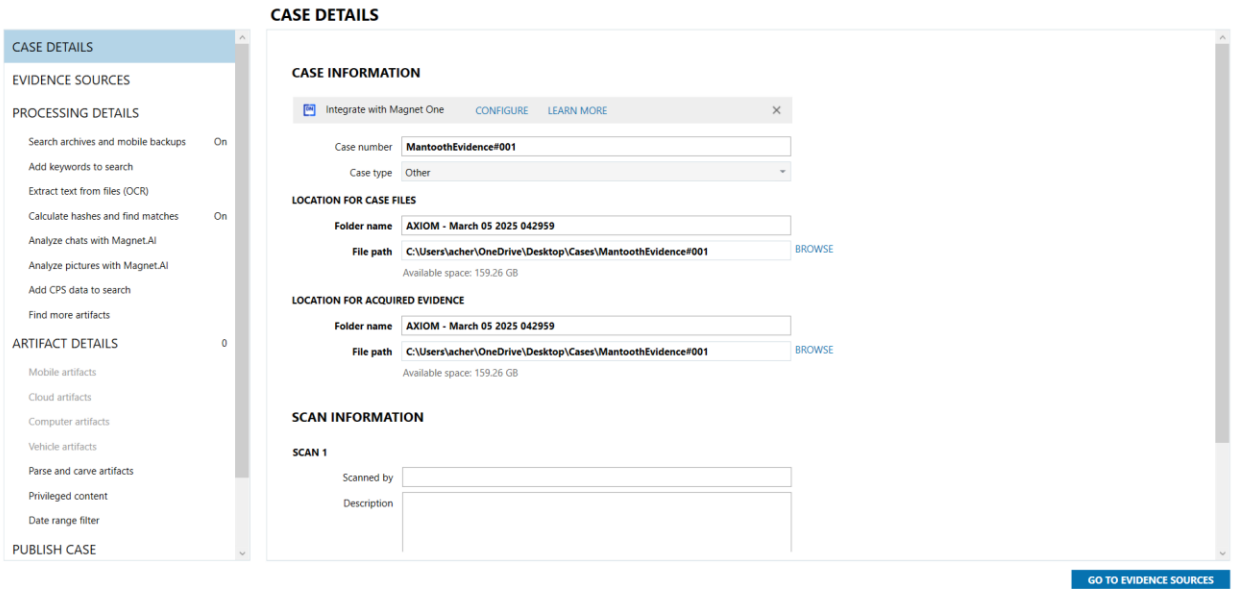

Figure 2.2 – Label the case and create a folder for this case to go into

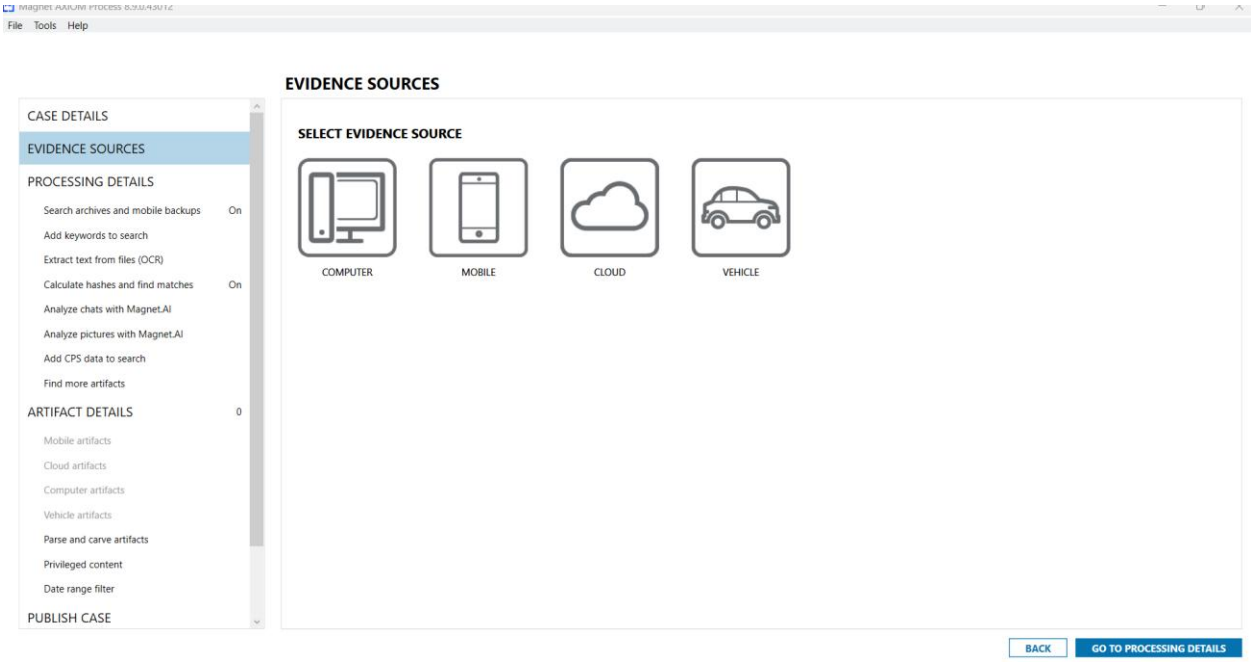

Figure 2.5 – Select "Computer"

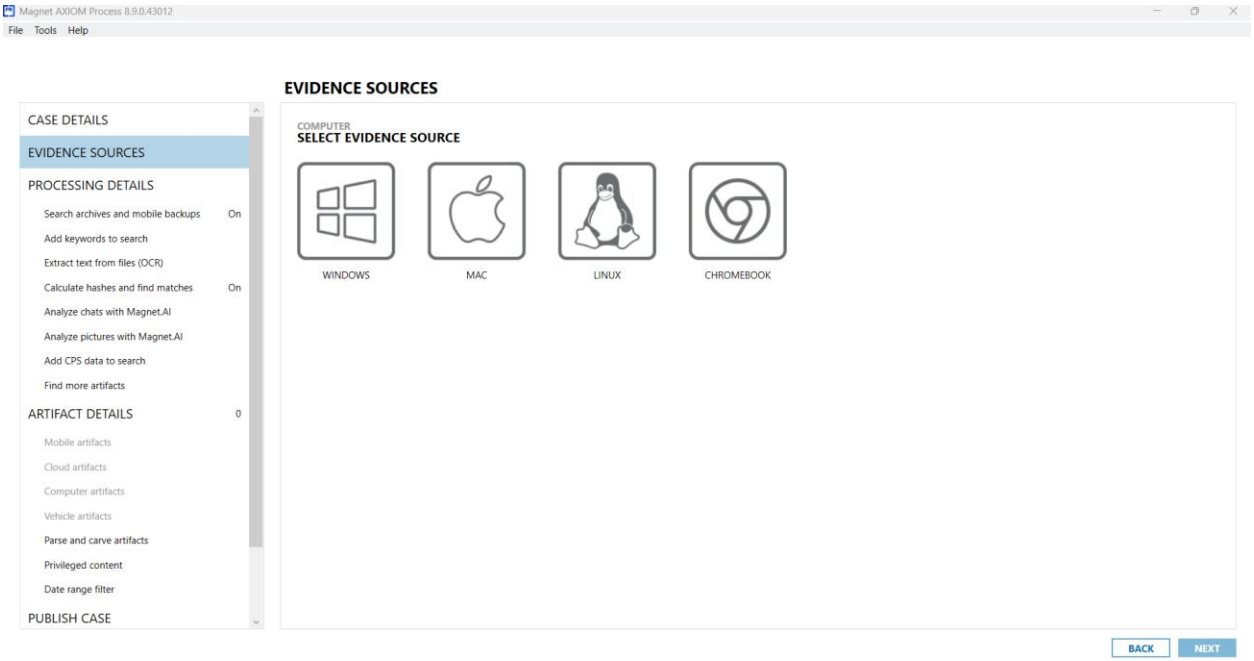

Figure 2.6 – Select "Windows"

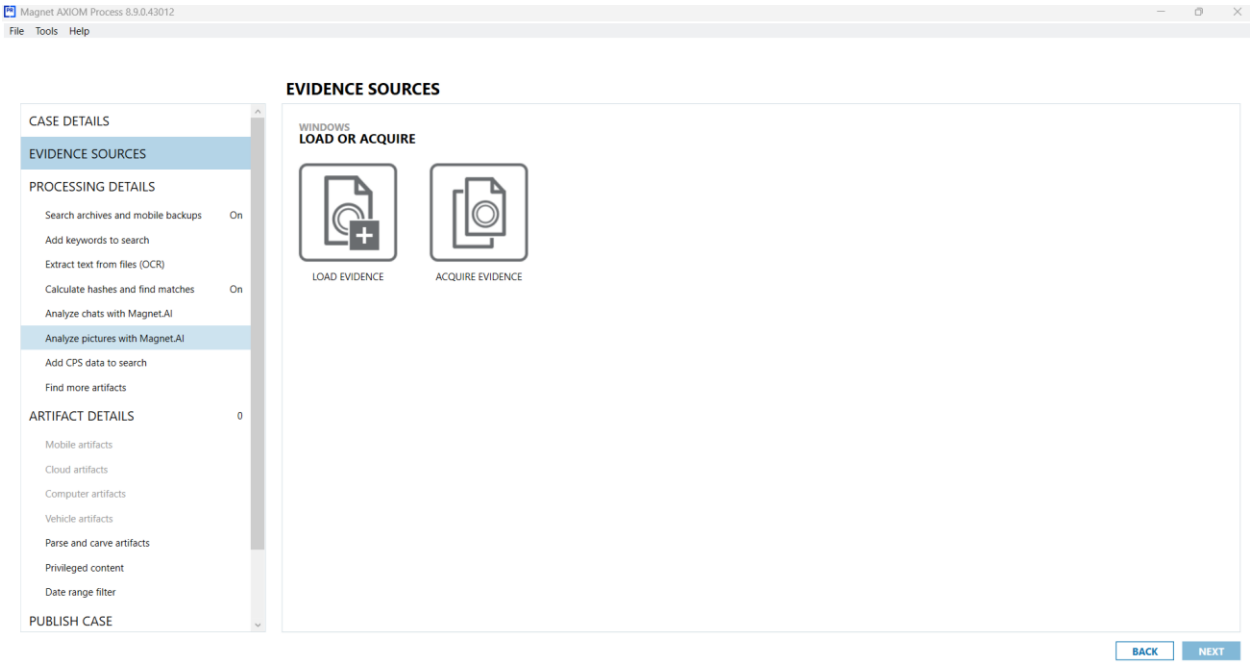

Figure 2.7 – Select "Load Evidence"

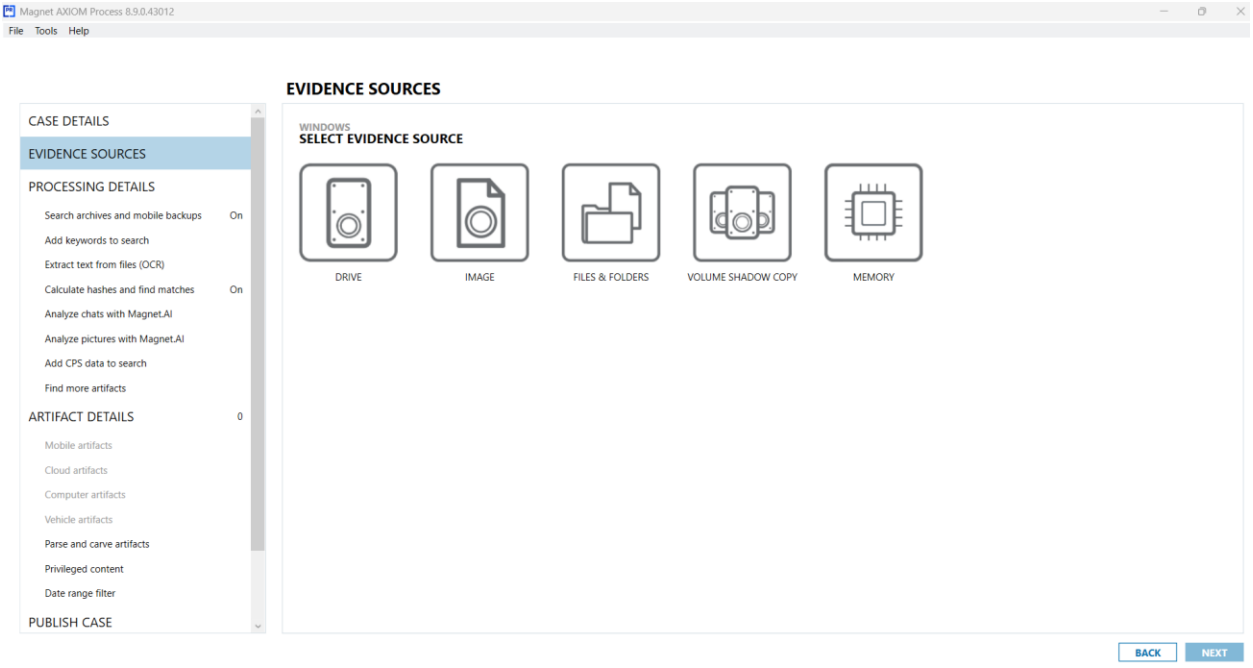

Figure 2.8 – Select "Image"

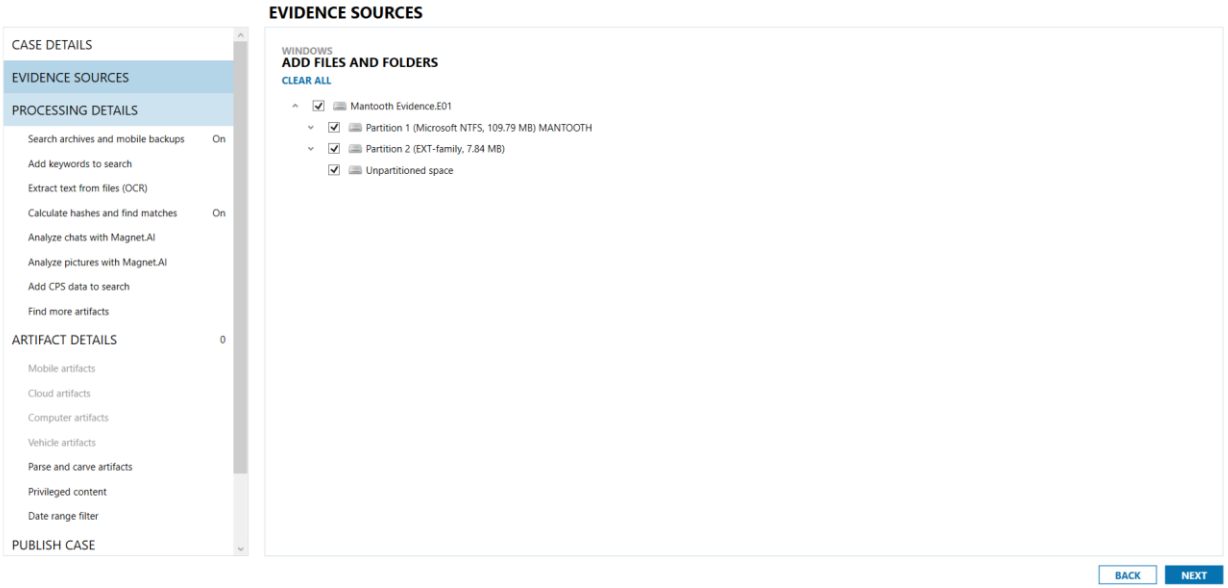

Figure 2.9 – Select the file

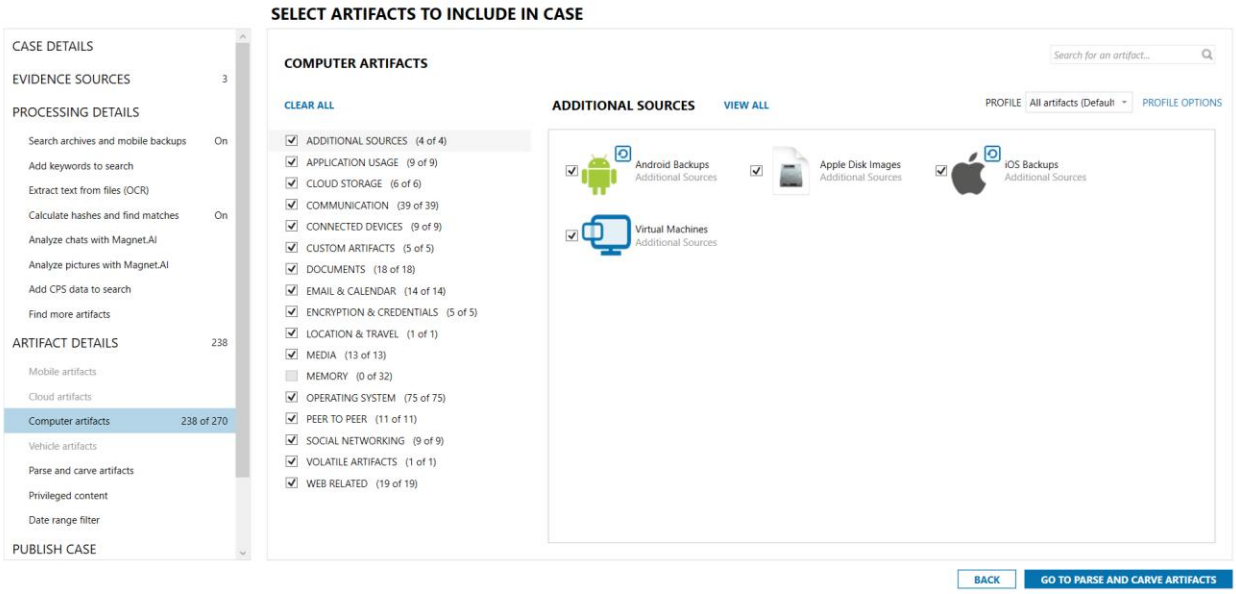

Figure 3.0 – Select the defaults up until "Computer Artifacts", then select all the options

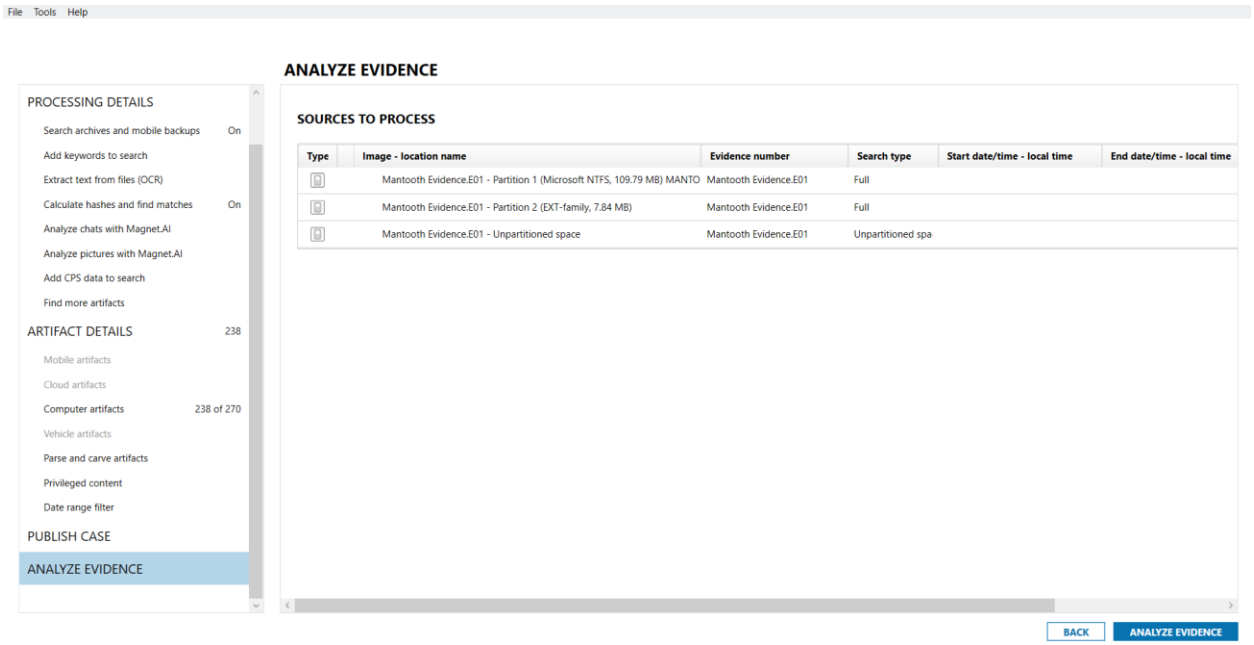

Figure 3.1 – Select all the defaults until "Analyze Evidence", then analyze the evidence

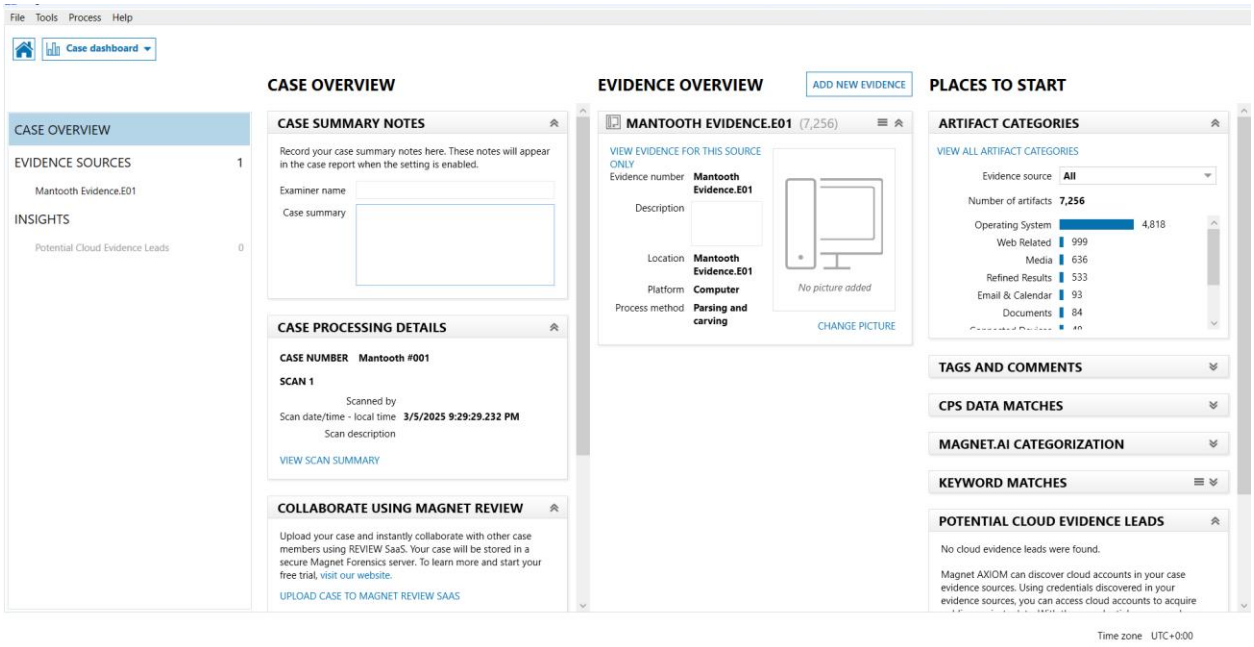

Figure 3.2 – Case Overview

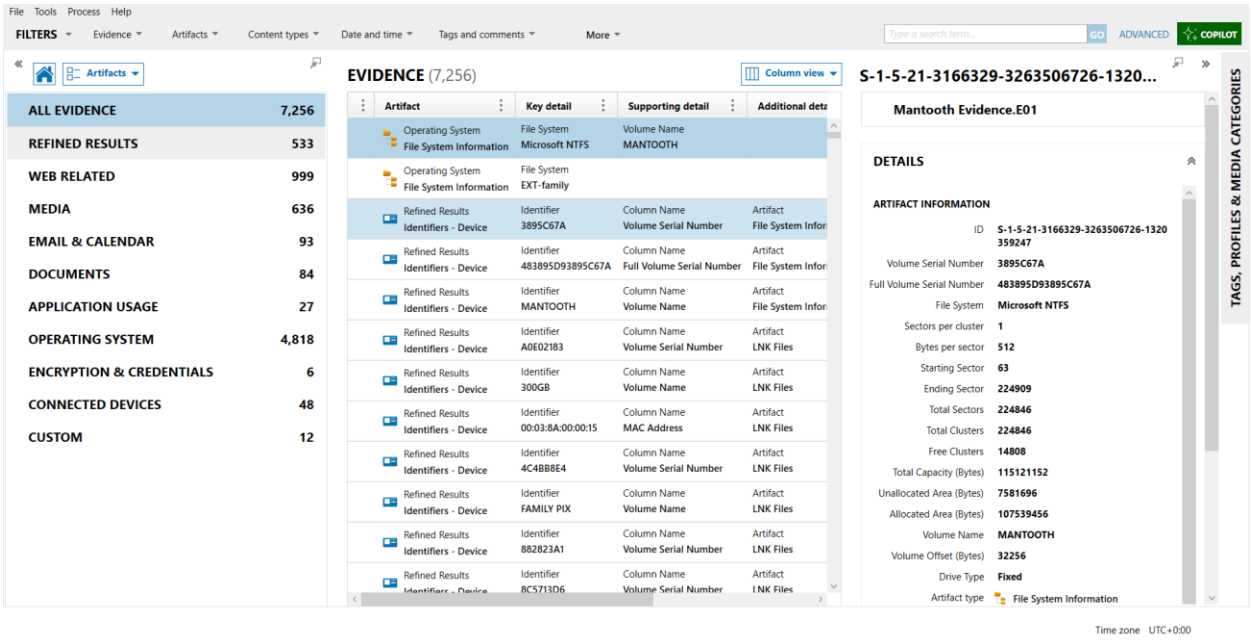

Figure 3.3 – Analyzed Evidence

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.

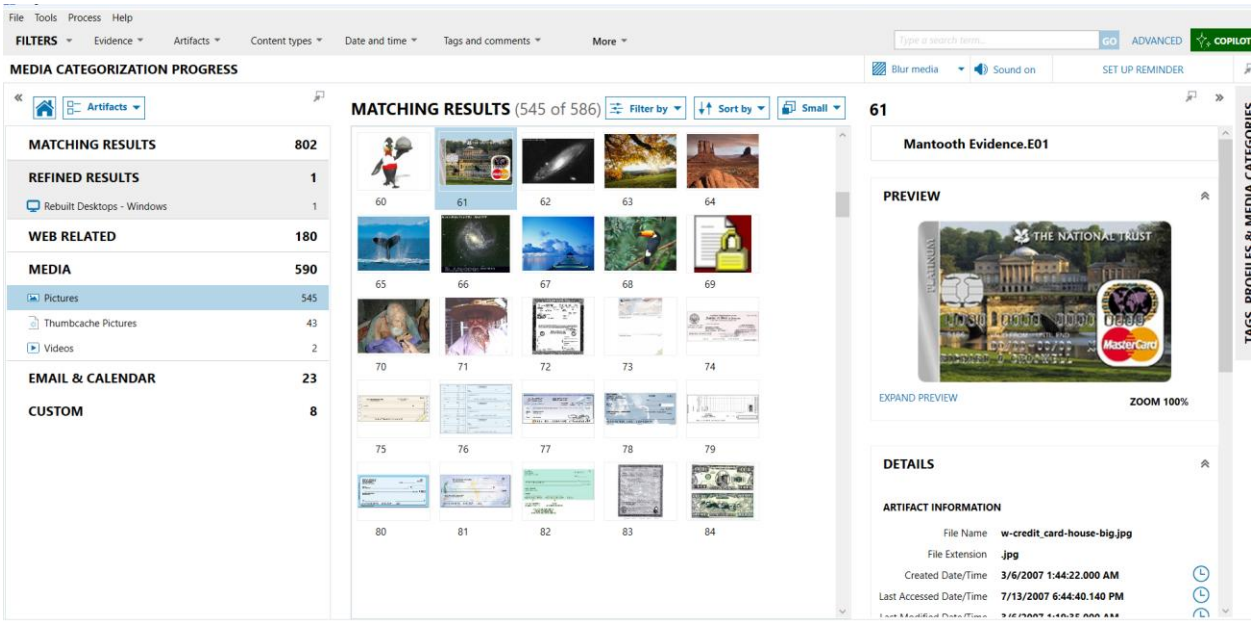

Figure 3.4 – Picture of credit card as well as multiple checks

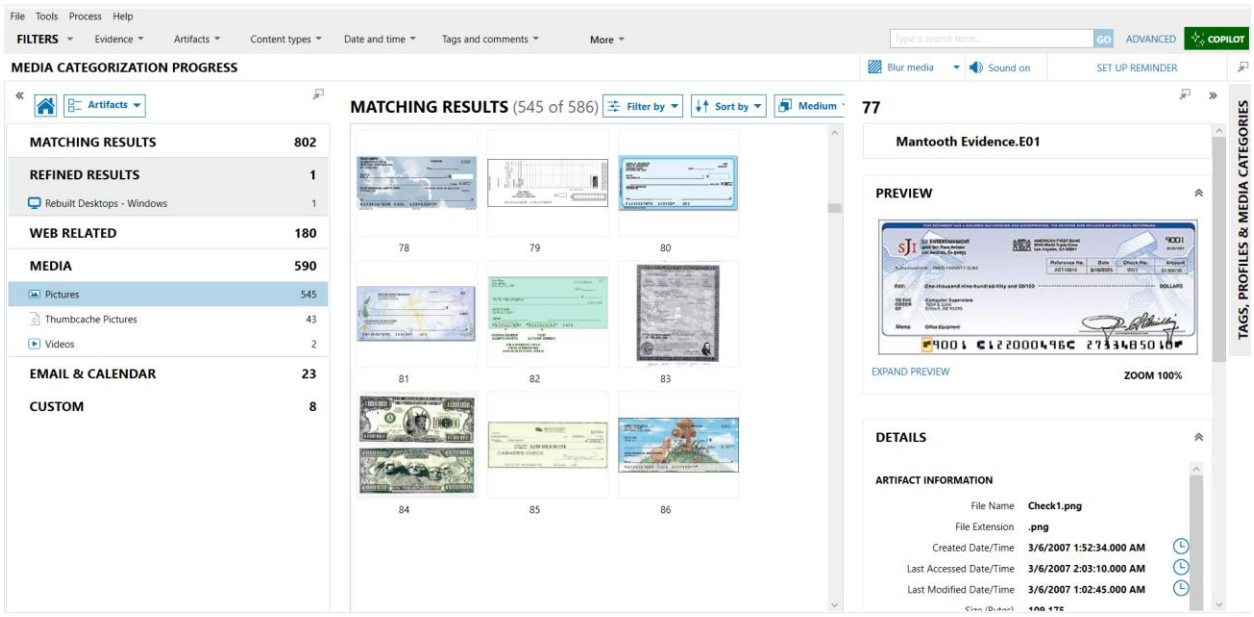

Figure 3.5 – Picture of a check with more checks in view

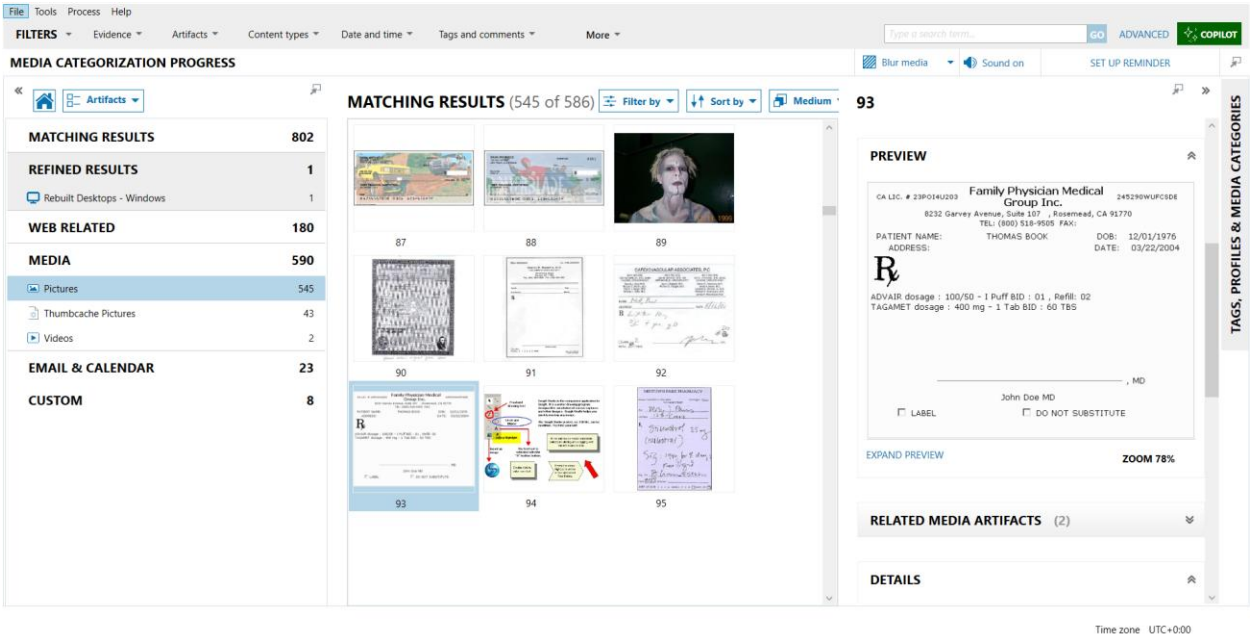

Figure 3.6 – Fake pharmacy doctors note

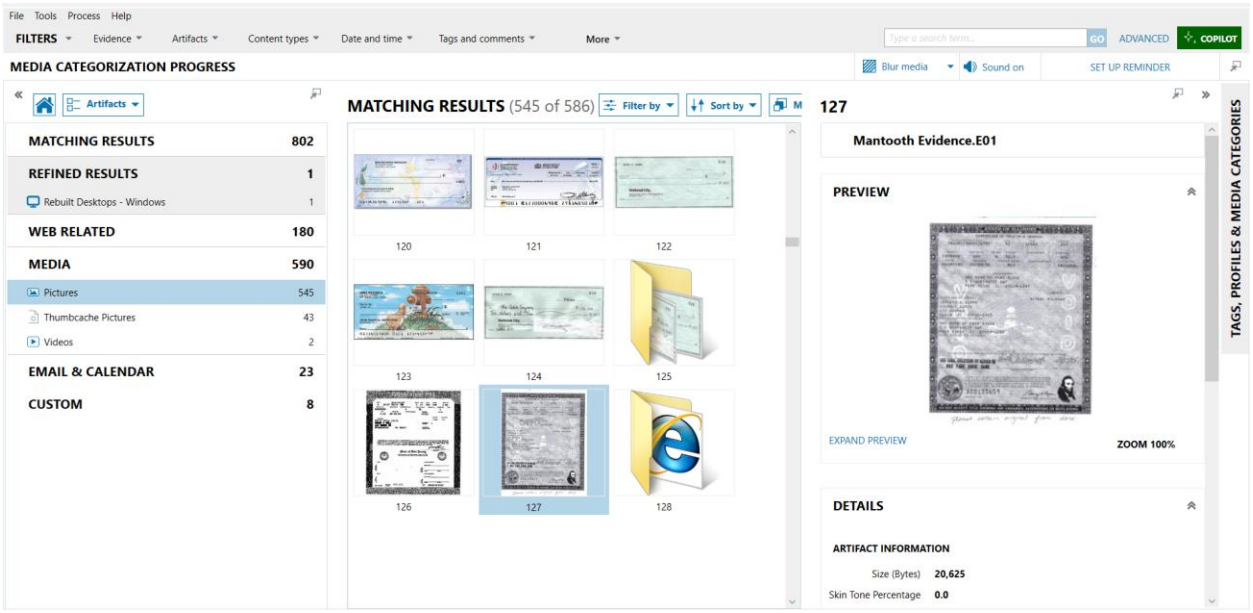

Figure 3.7 – Legal documents with more scans of checks

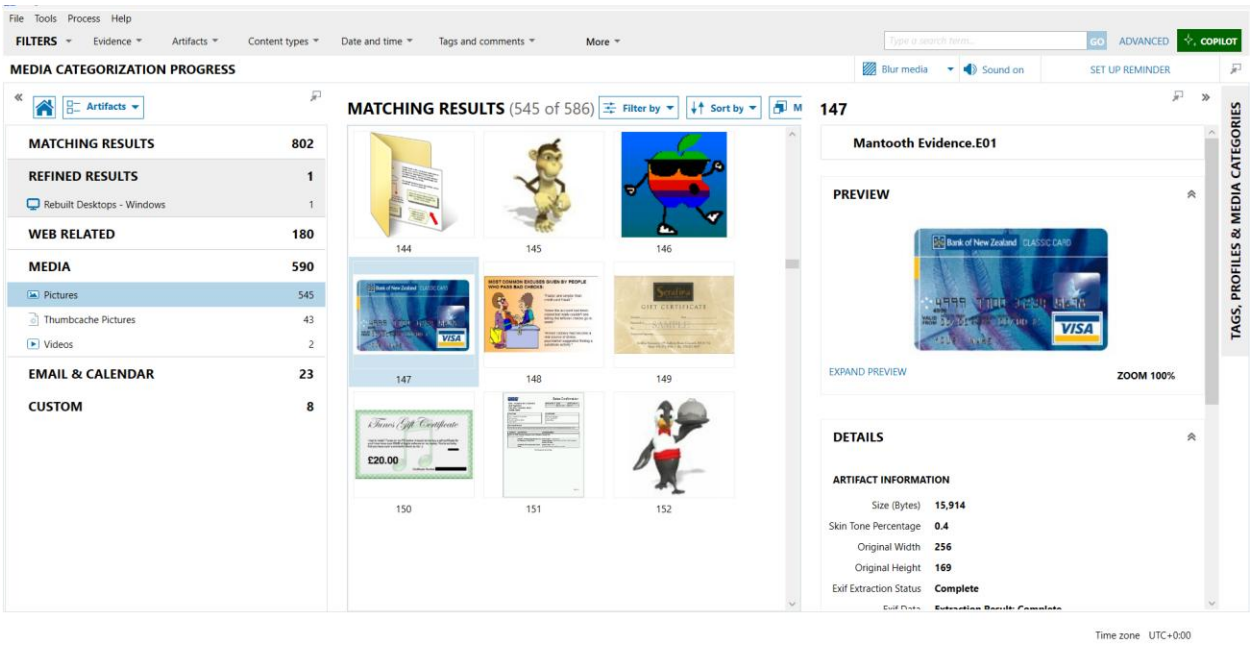

Figure 3.8 – Credit card with more fraudulent certificates and checks

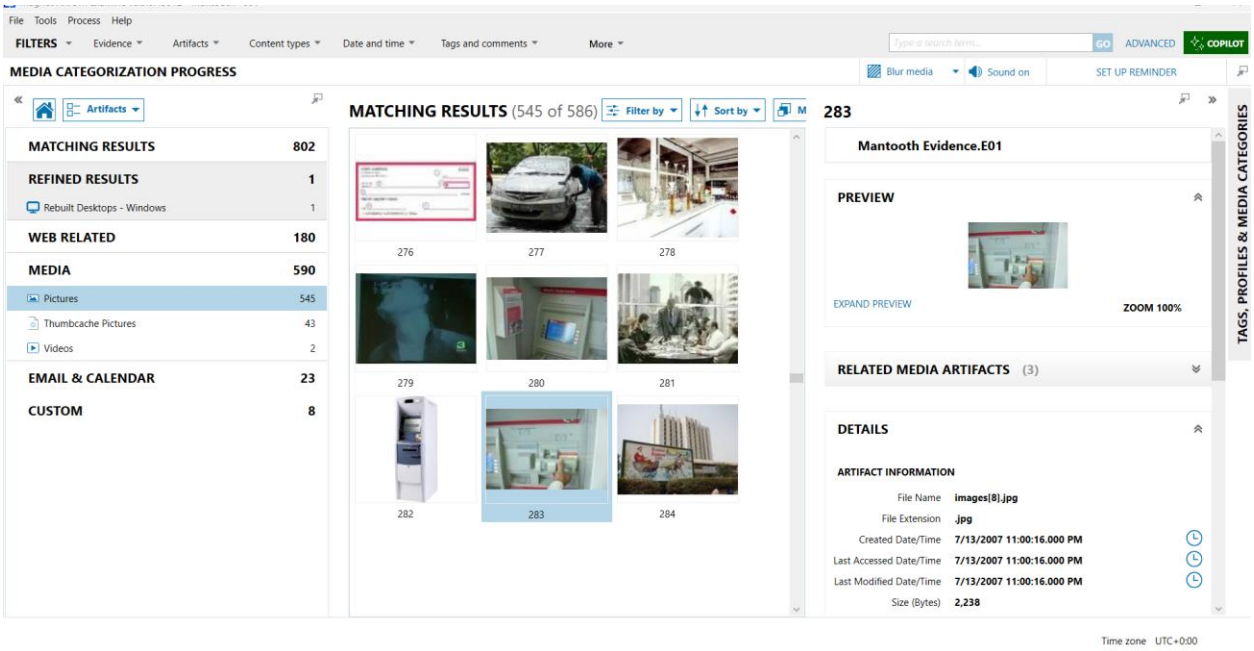

Figure 3.9 – Credit card skimmer on an ATM

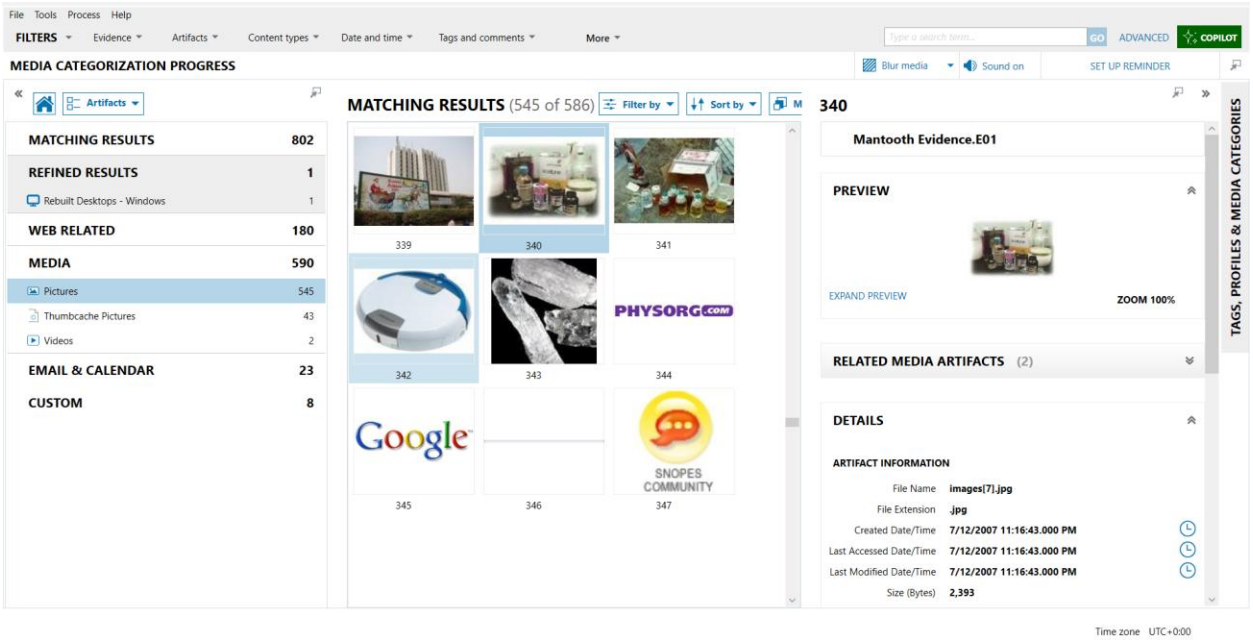

Figure 4.0 – Picture of ingredients for paraphernalia

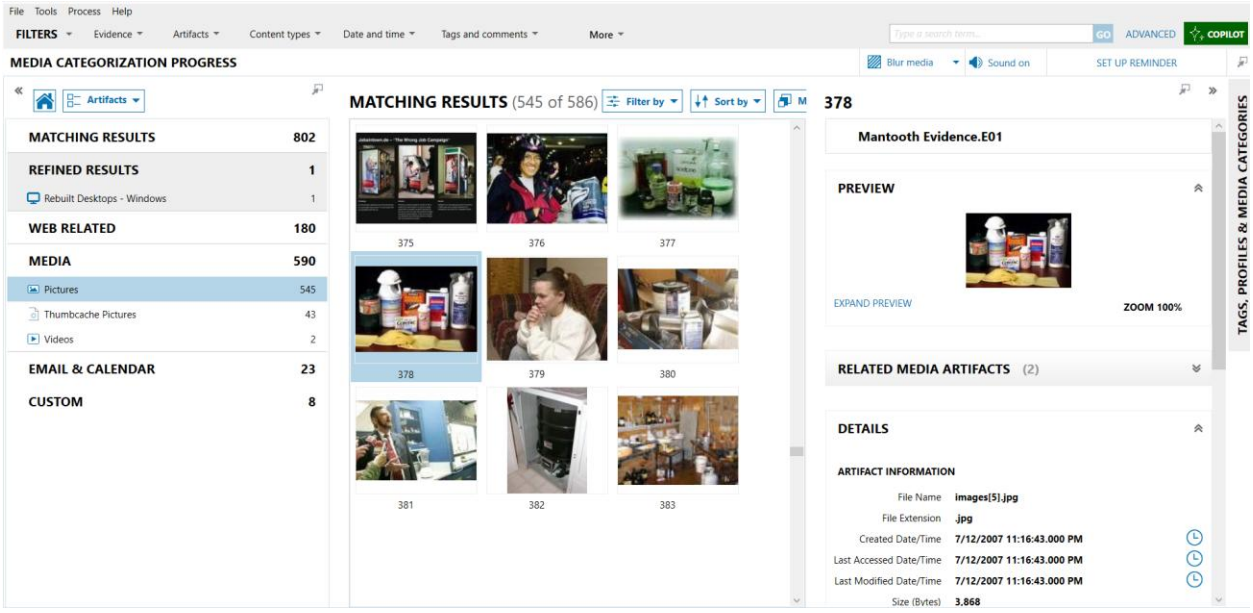

Figure 4.1 – More pictures of ingredients to make some paraphernalia

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.”

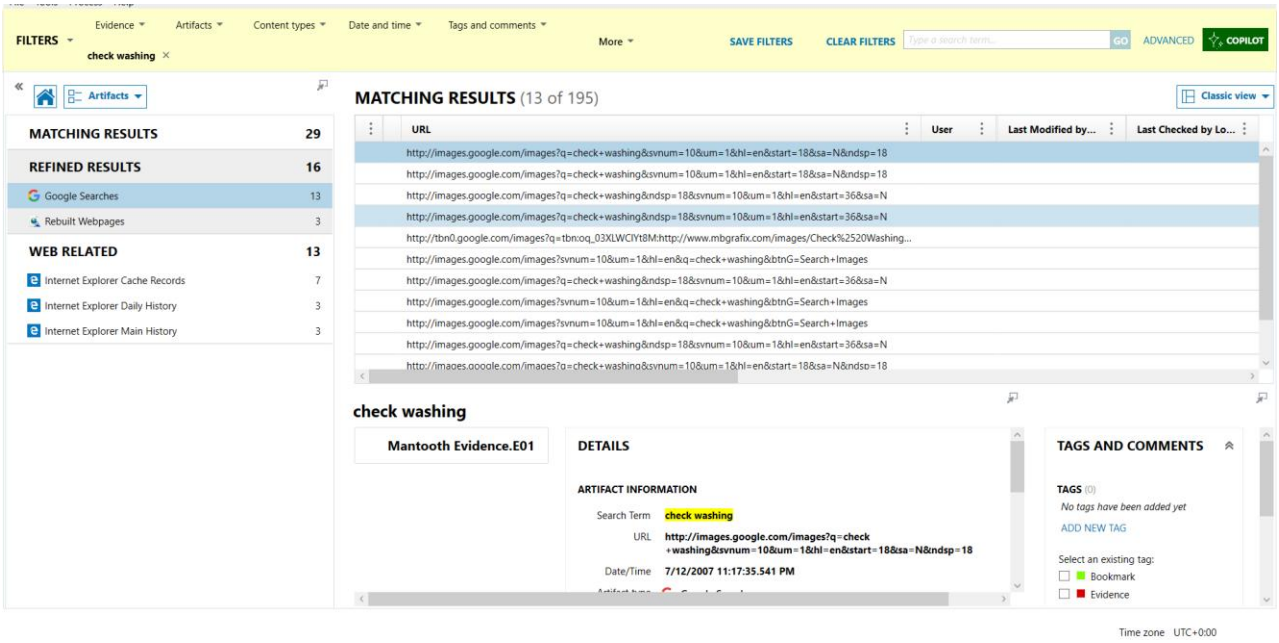

Figure 4.2 – 13 google searches for check washing

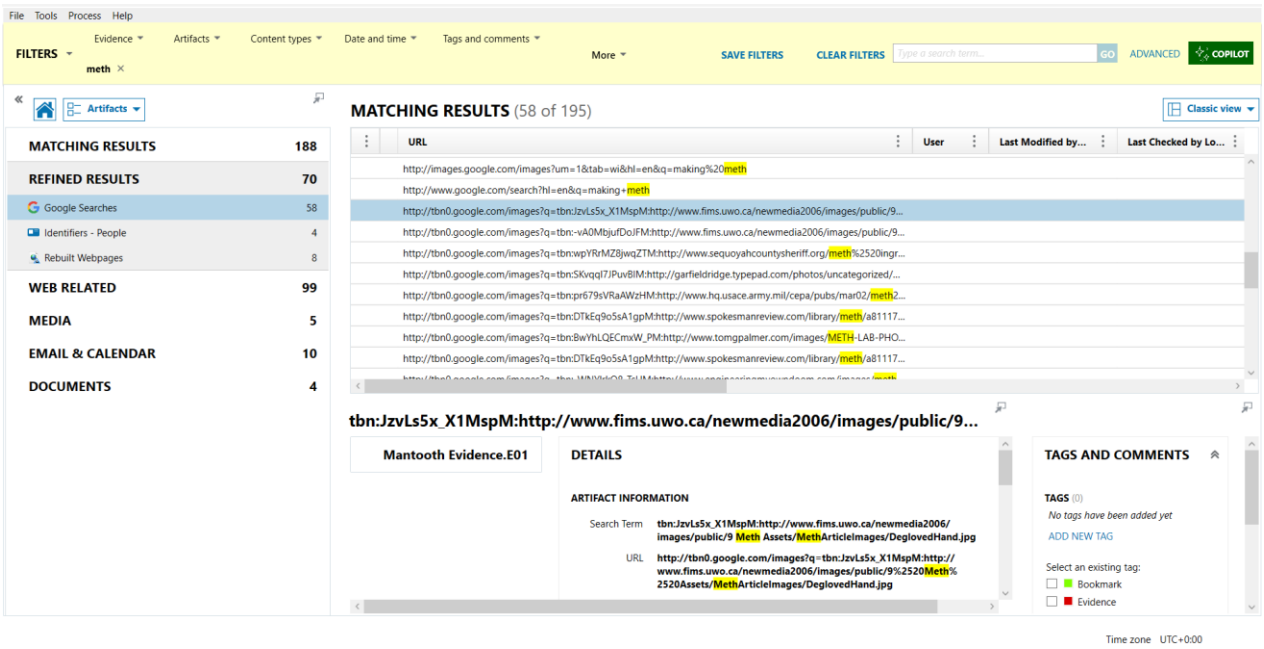

Figure 4.3 – 58 google searches containing the word meth

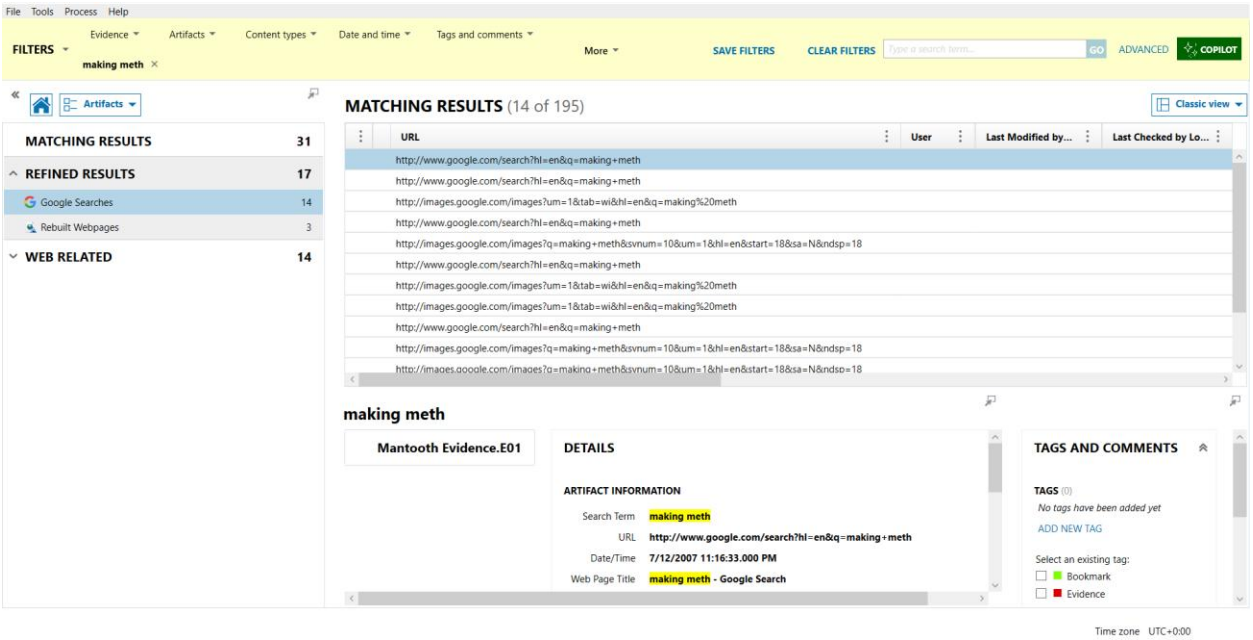

Figure 4.4 – 14 google searches for Making meth

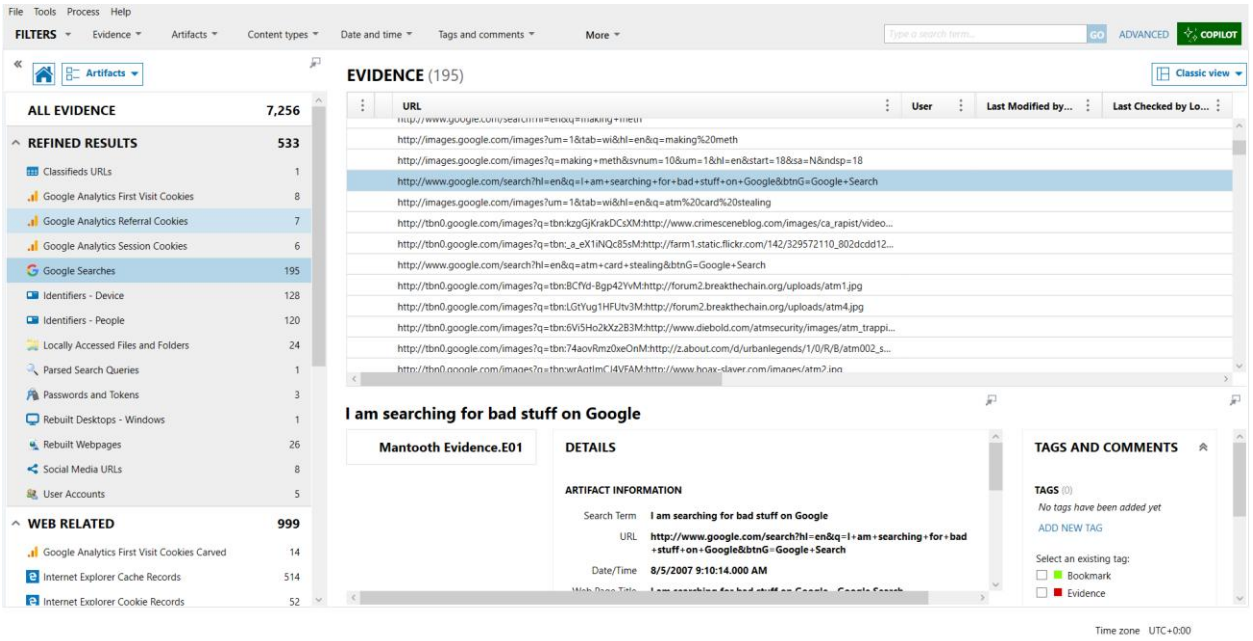

Figure 4.5 - Knows they are looking for bad things on google

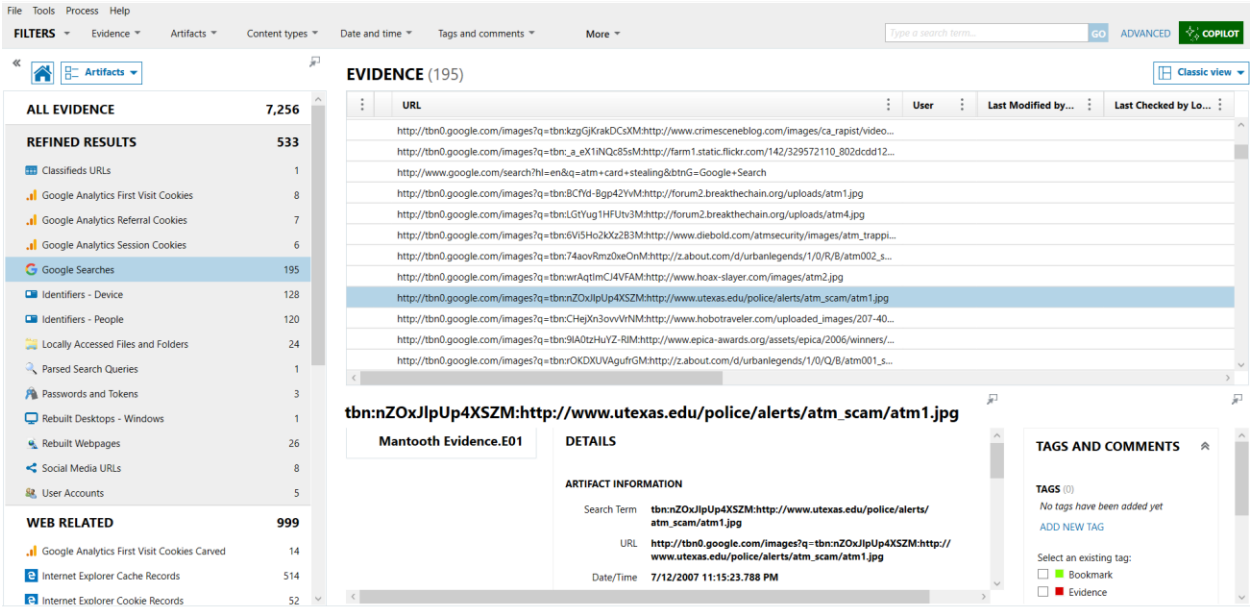

Figure 4.6 – Texas police alert

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.”

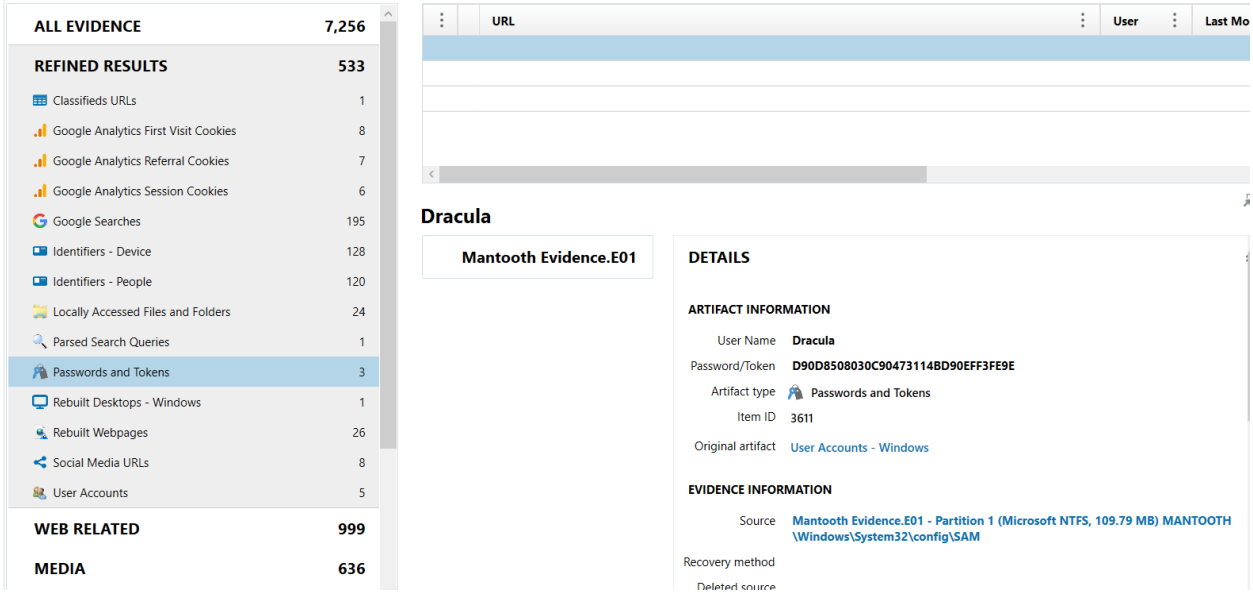

Figure 4.7 – Password for Dracula

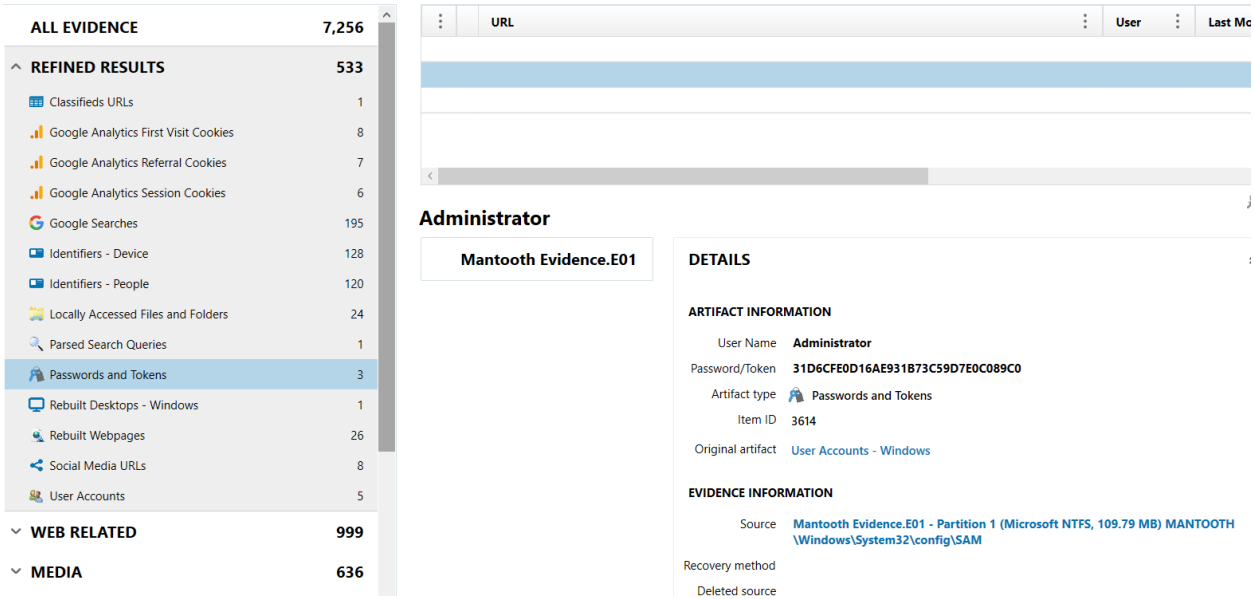

Figure 4.8 – Password for Administrator

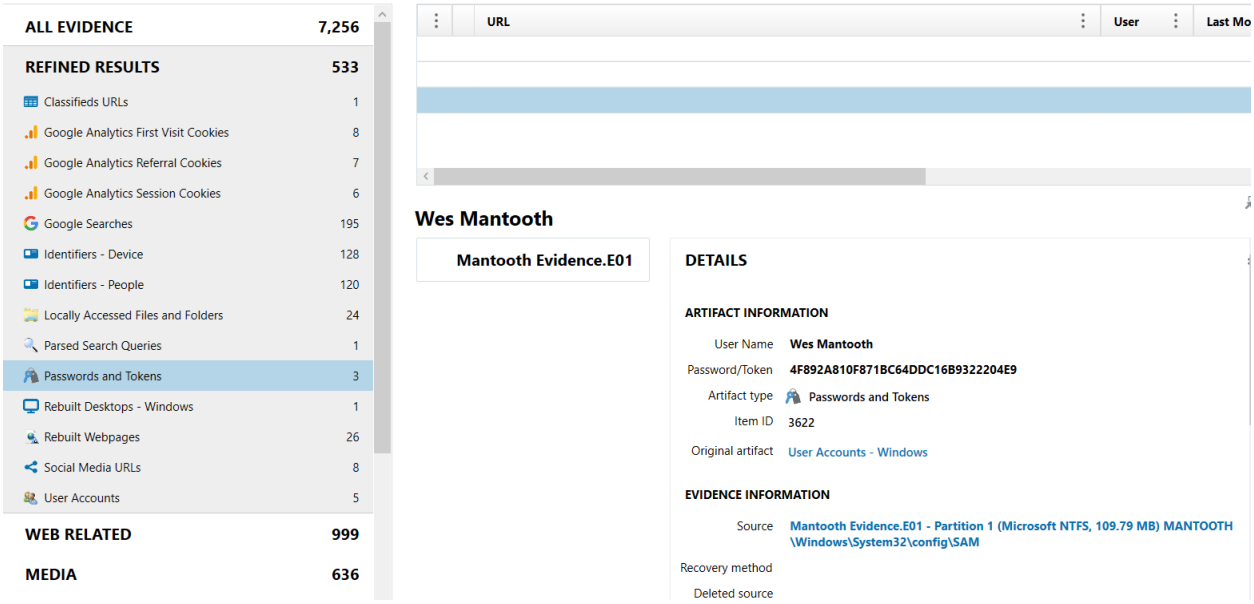

Figure 4.9 – Password for Wes Mantooth

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.

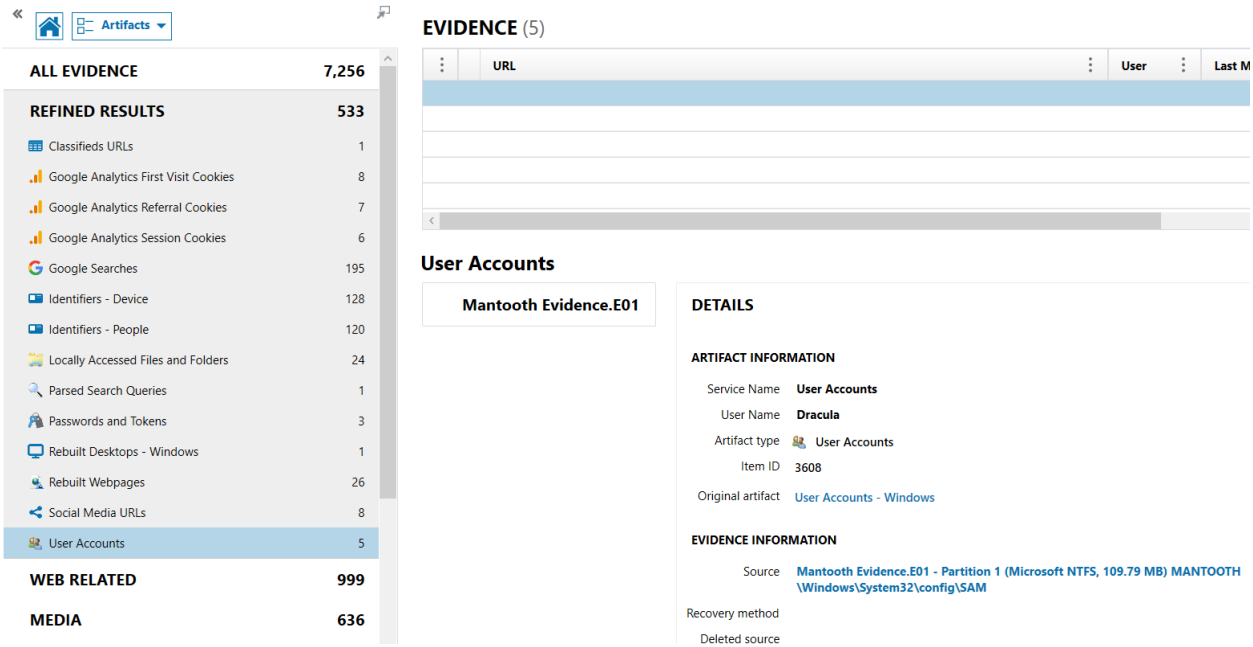

Figure 5.0 – Dracula user account

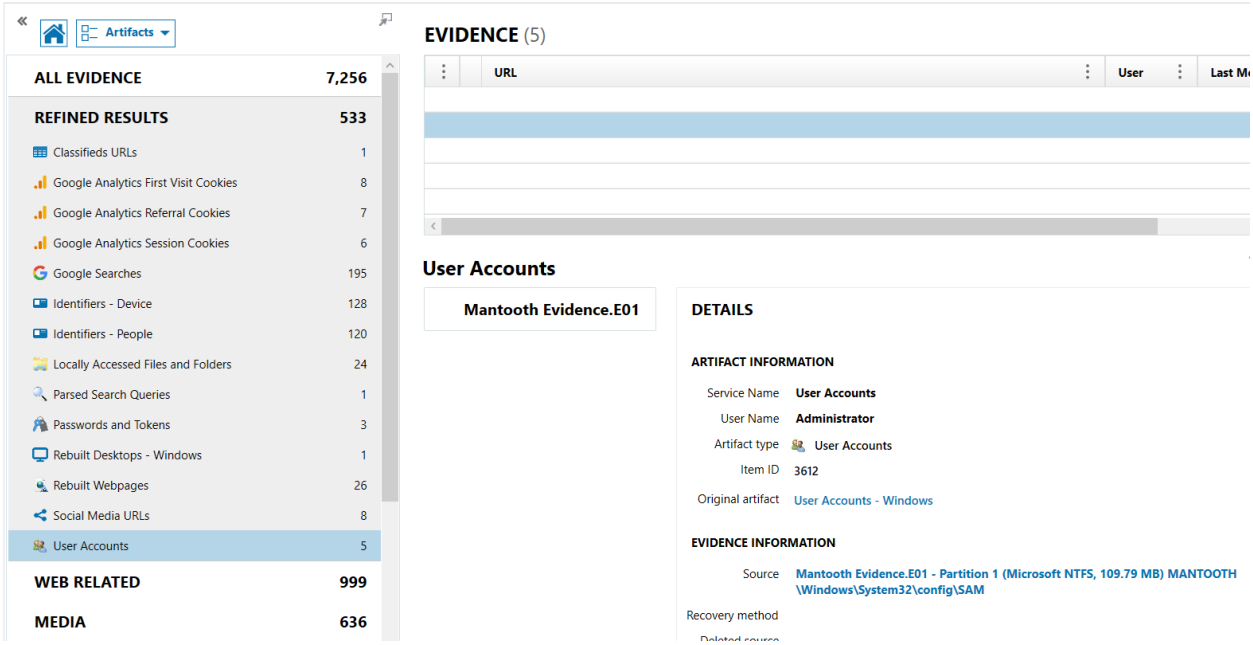

Figure 5.1 – Administrator user account

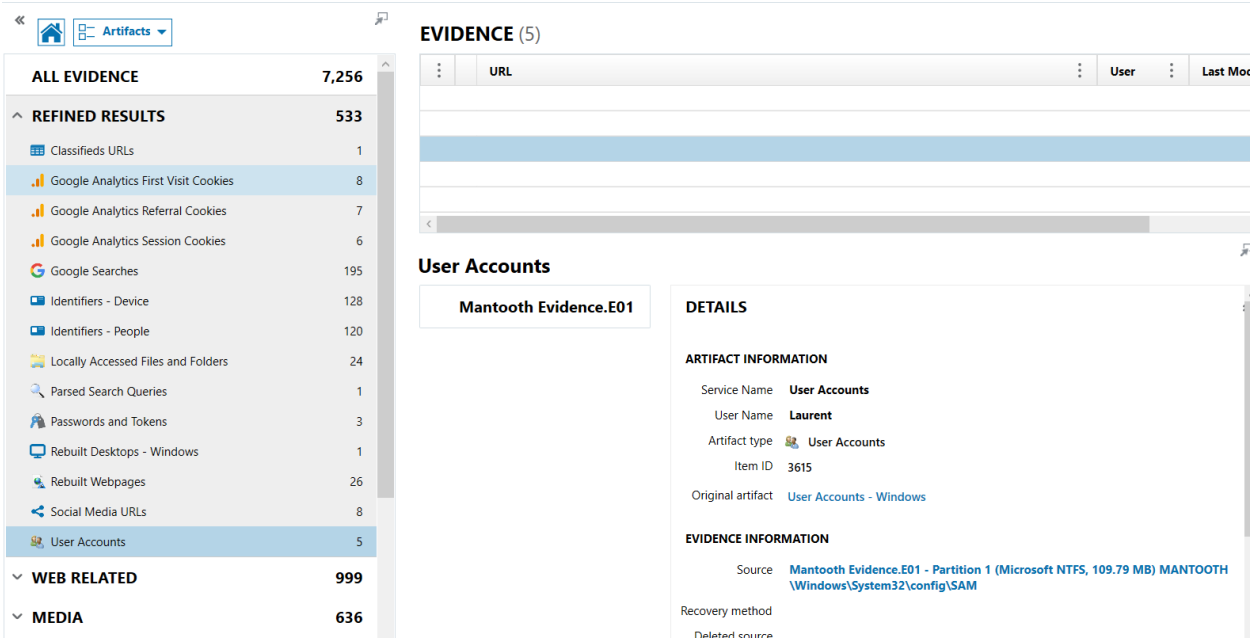

Figure 5.2 – Laurent user account

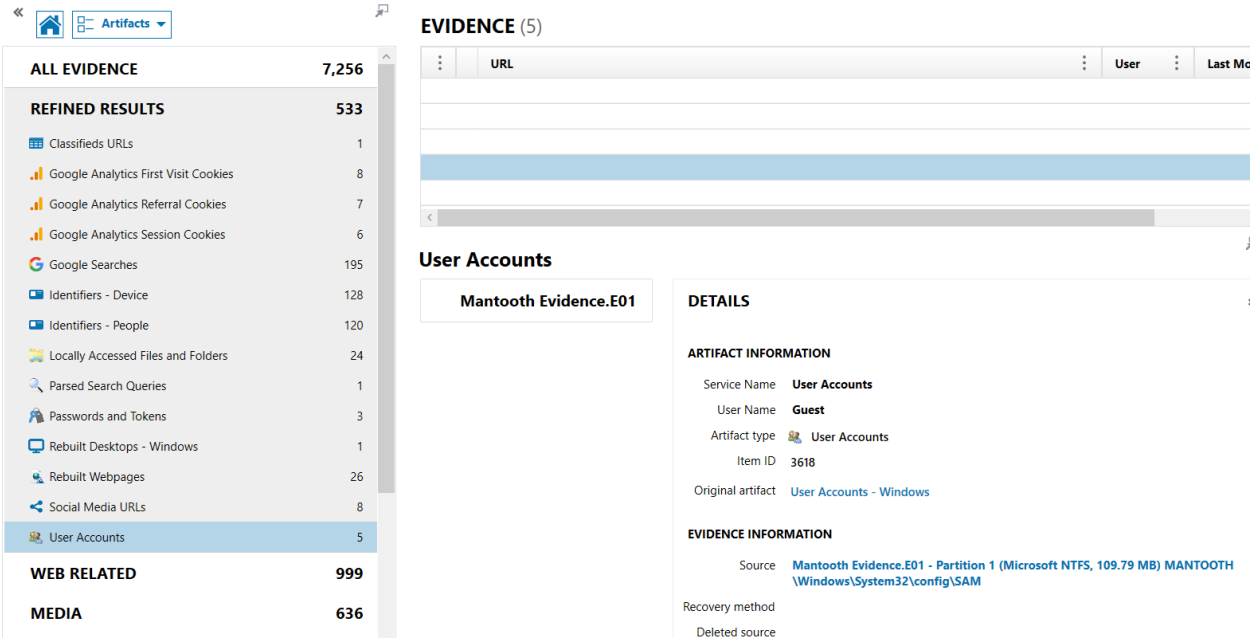

Figure 5.3 – Guest user account

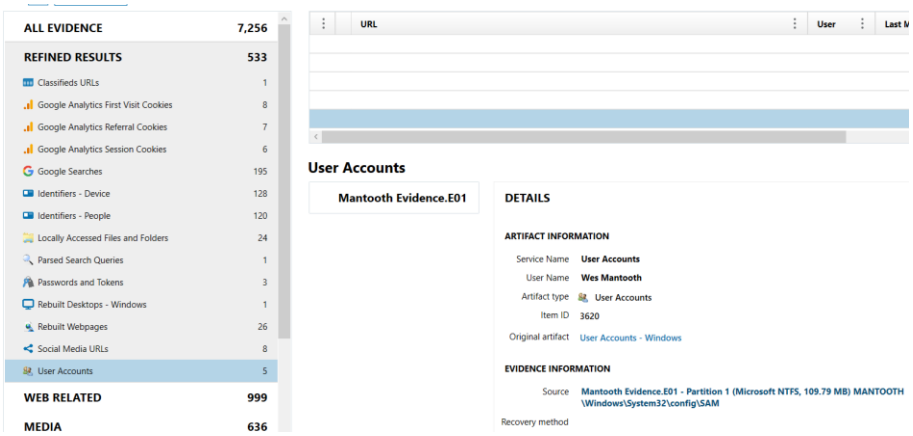

Figure 5.4 – Wes Mantooth user account

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.

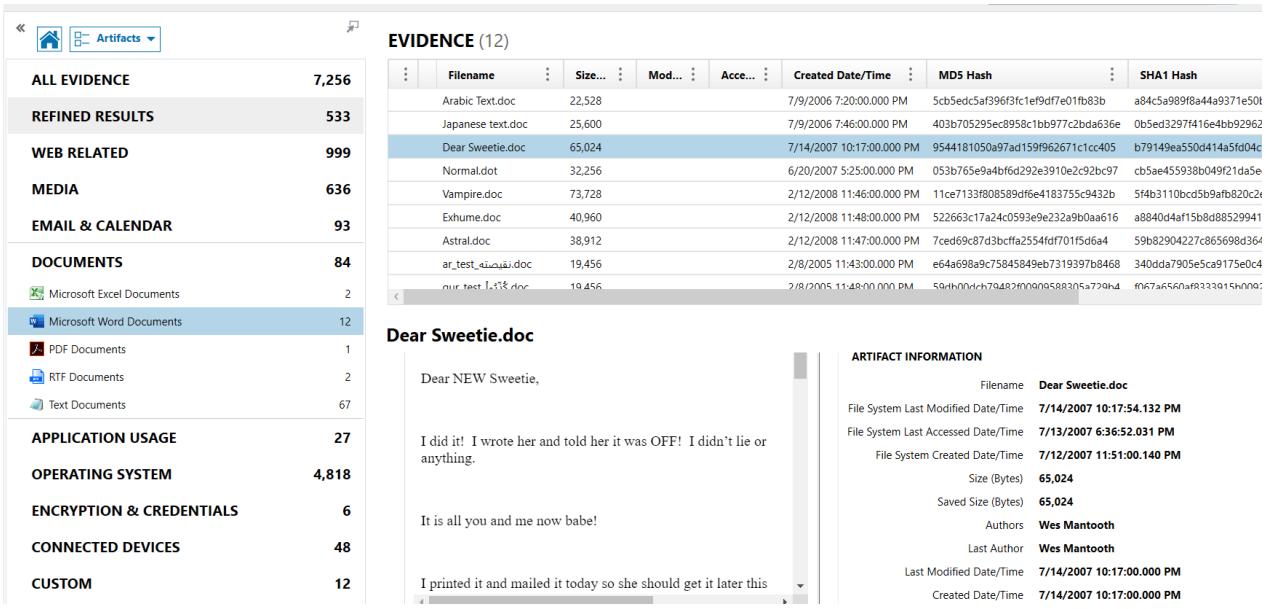

Figure 5.5 – Document from Wes Mantooth to his NEW sweetie

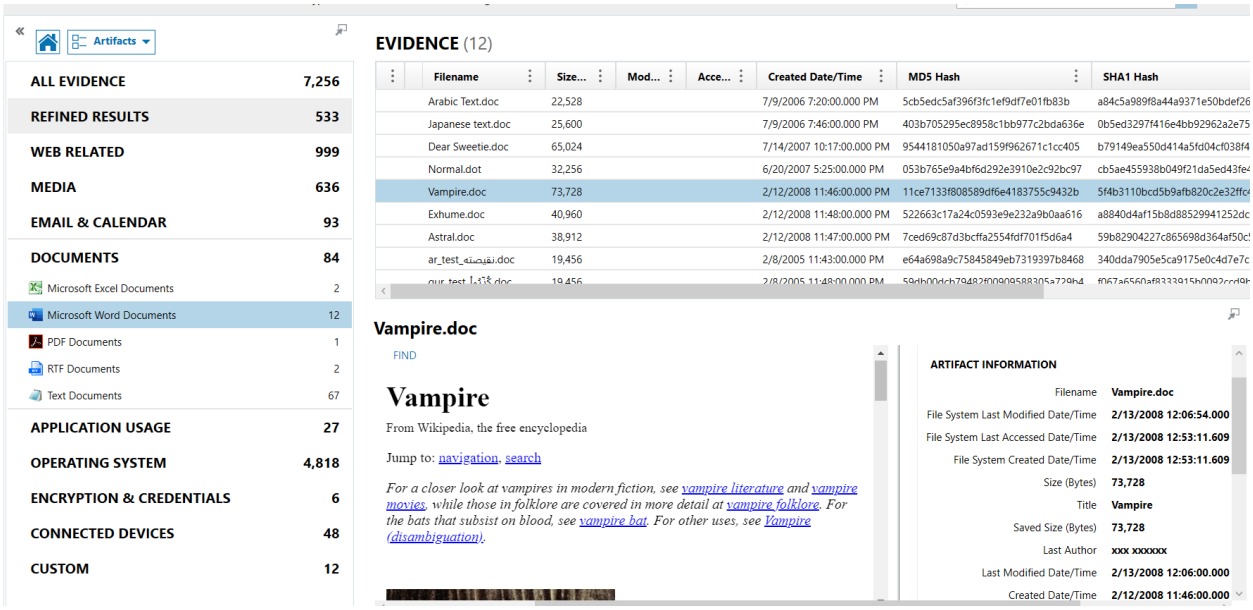

Figure 5.6 – Wikipedia page about vampires, makes sense for a Dracula user

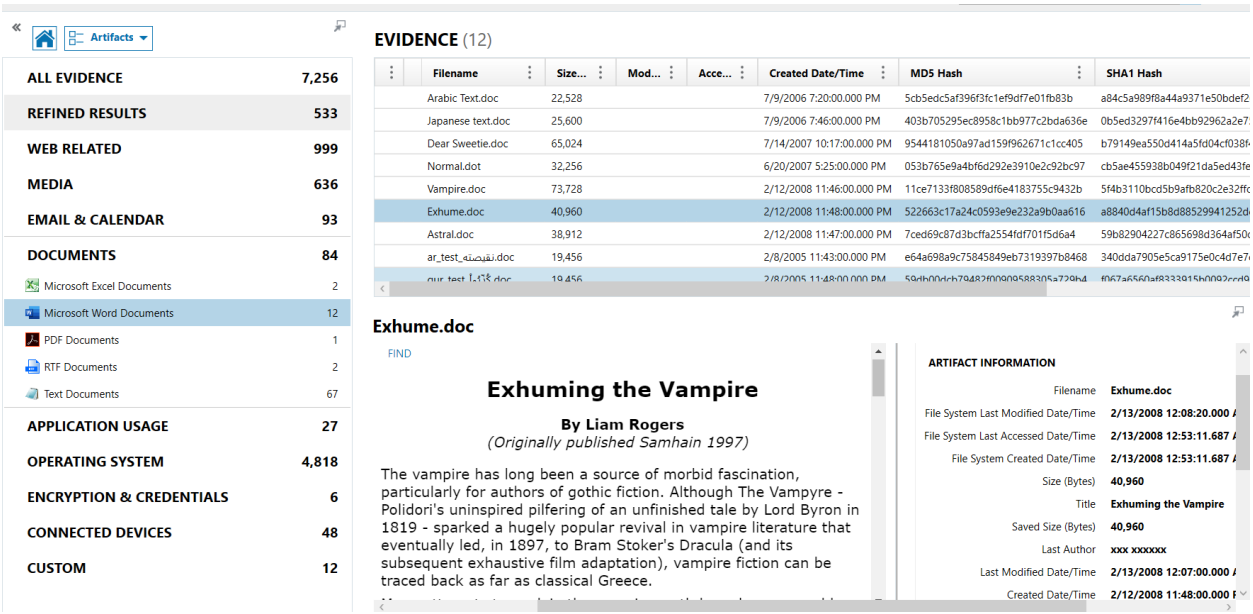

Figure 5.7 – Story about vampires

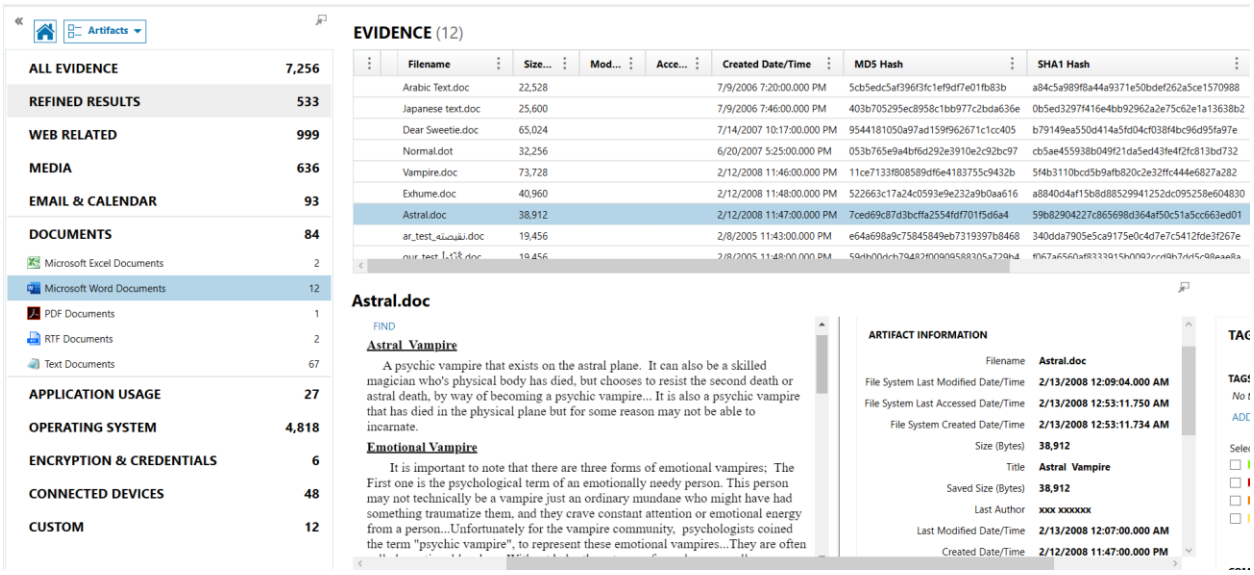

Figure 5.8 – Different types of vampires

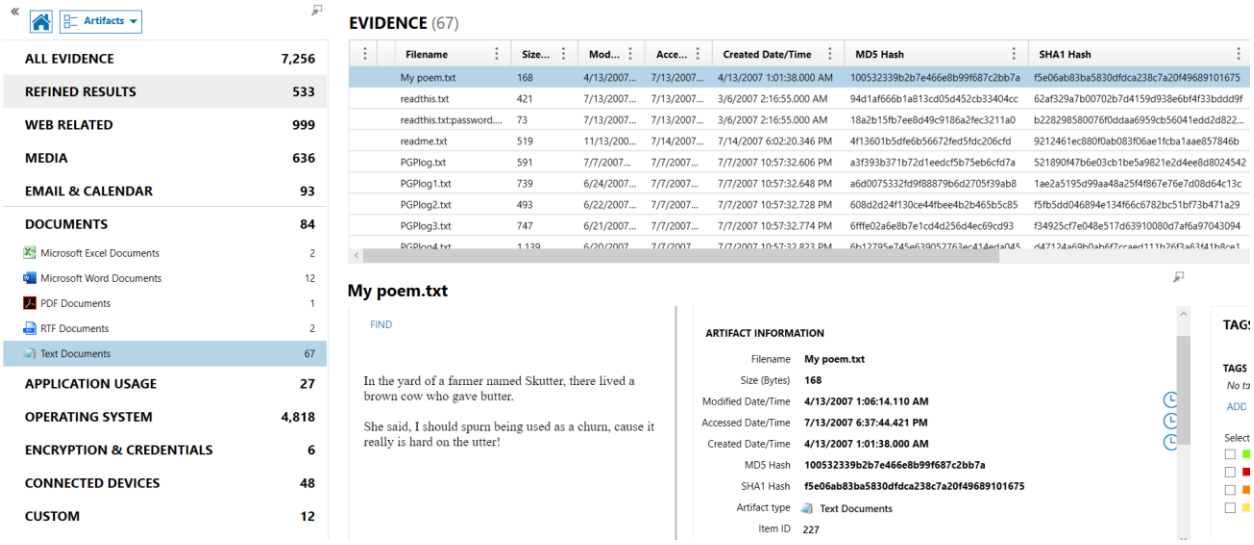

Figure 5.9 – Short poem

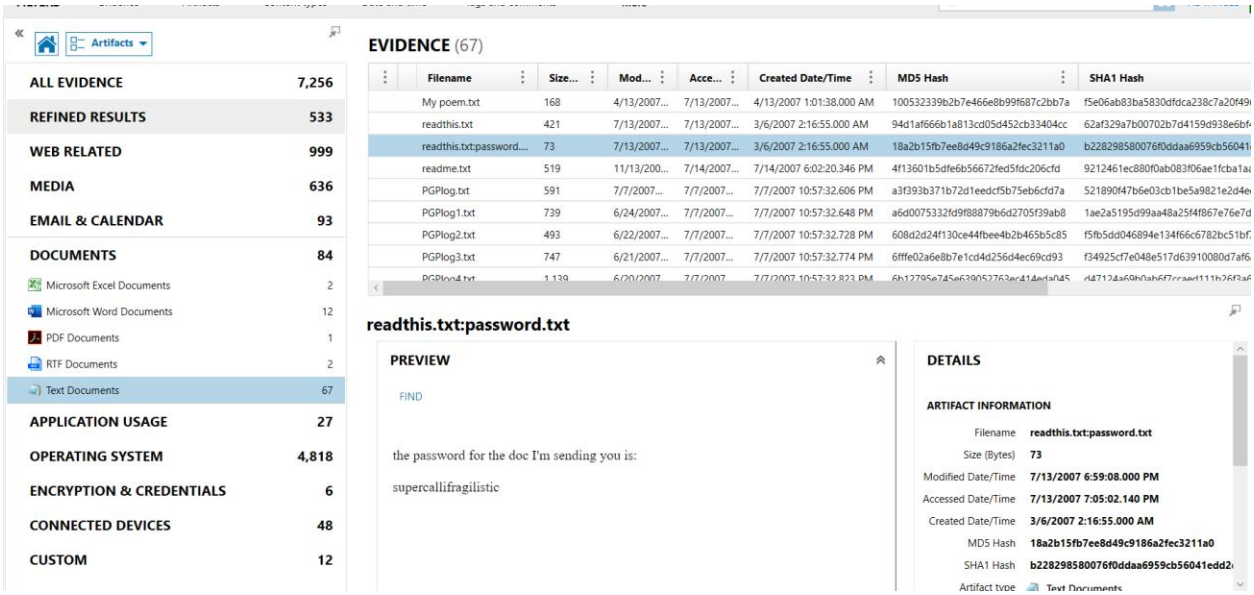

Figure 6.0 – Password for read this.txt

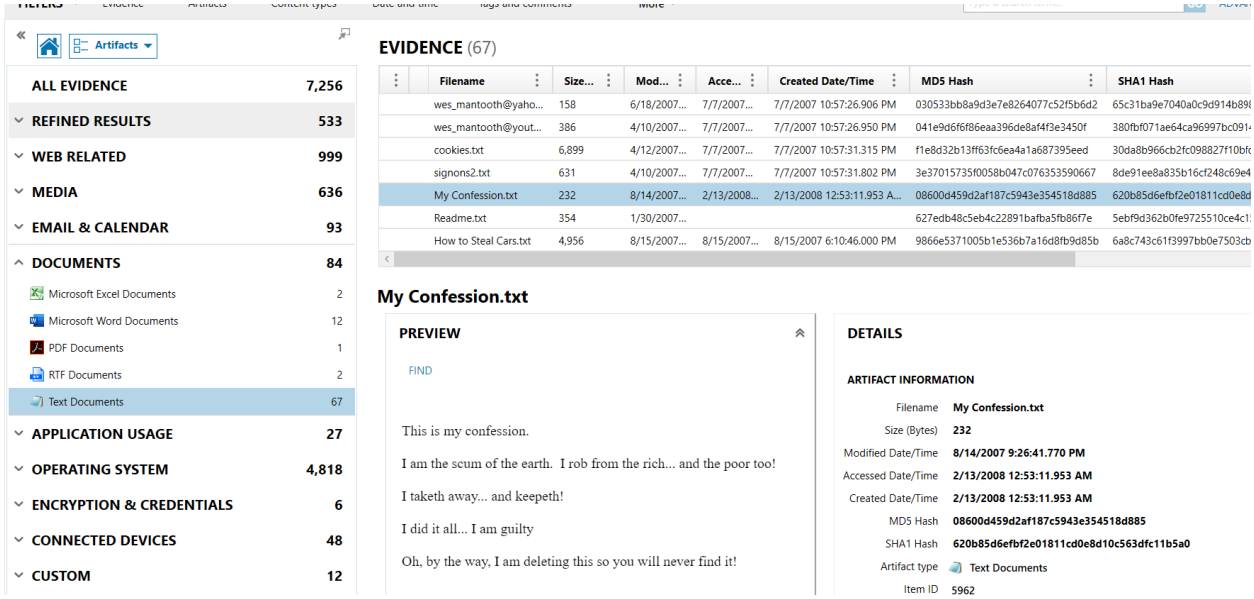

Figure 6.1 – Confession text

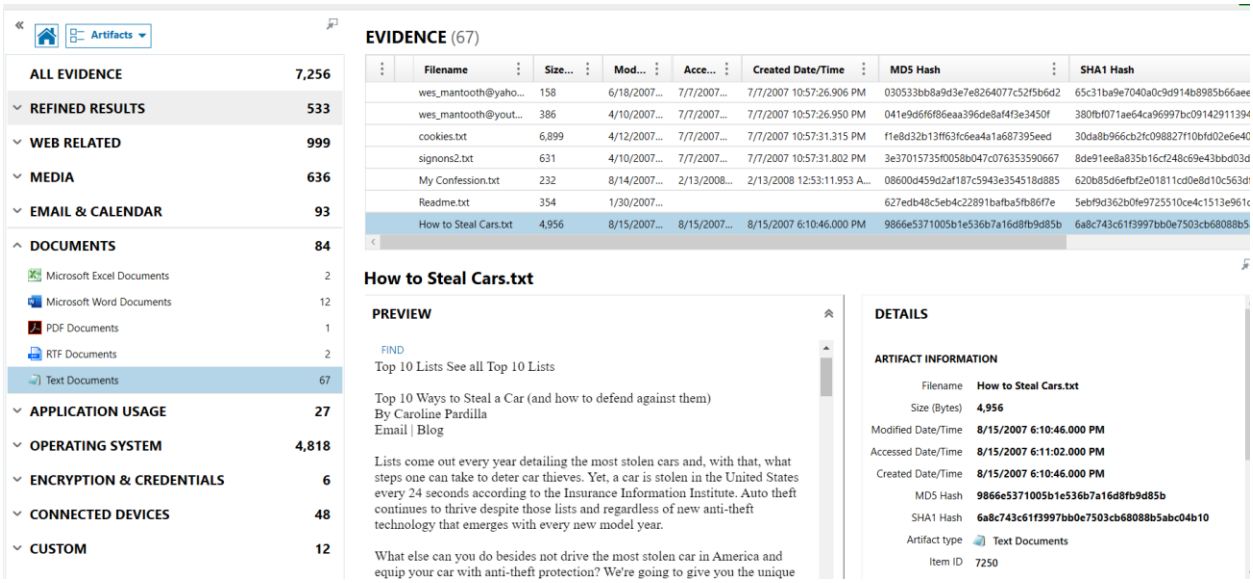

Figure 6.2 – How to Steal Cars.txt

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.

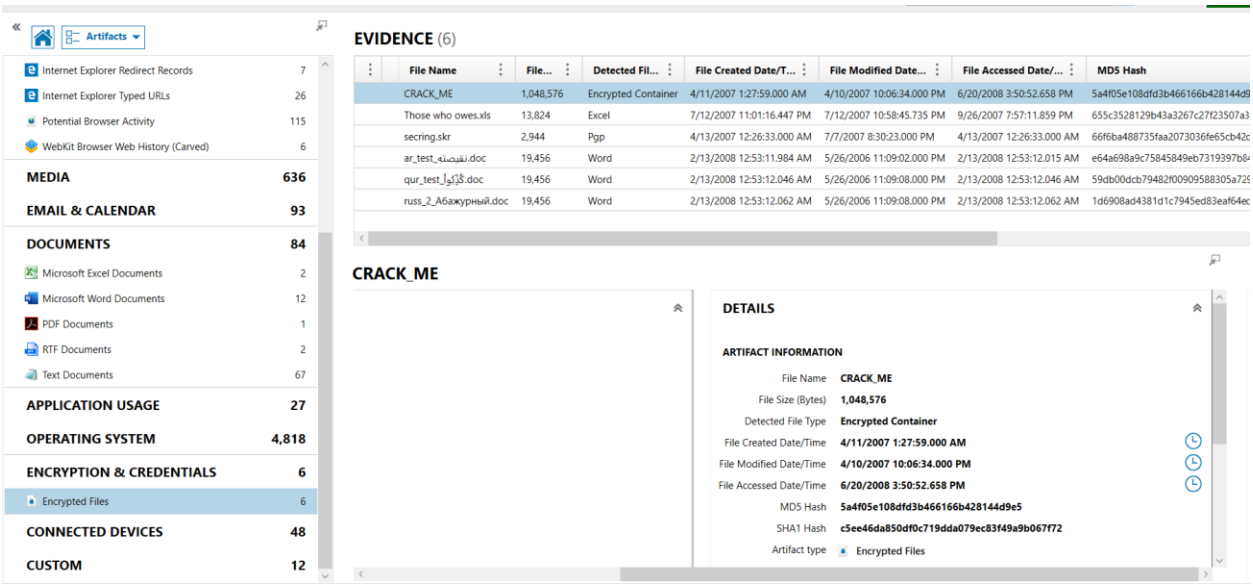

Figure 6.3 – 6 Encrypted files

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.

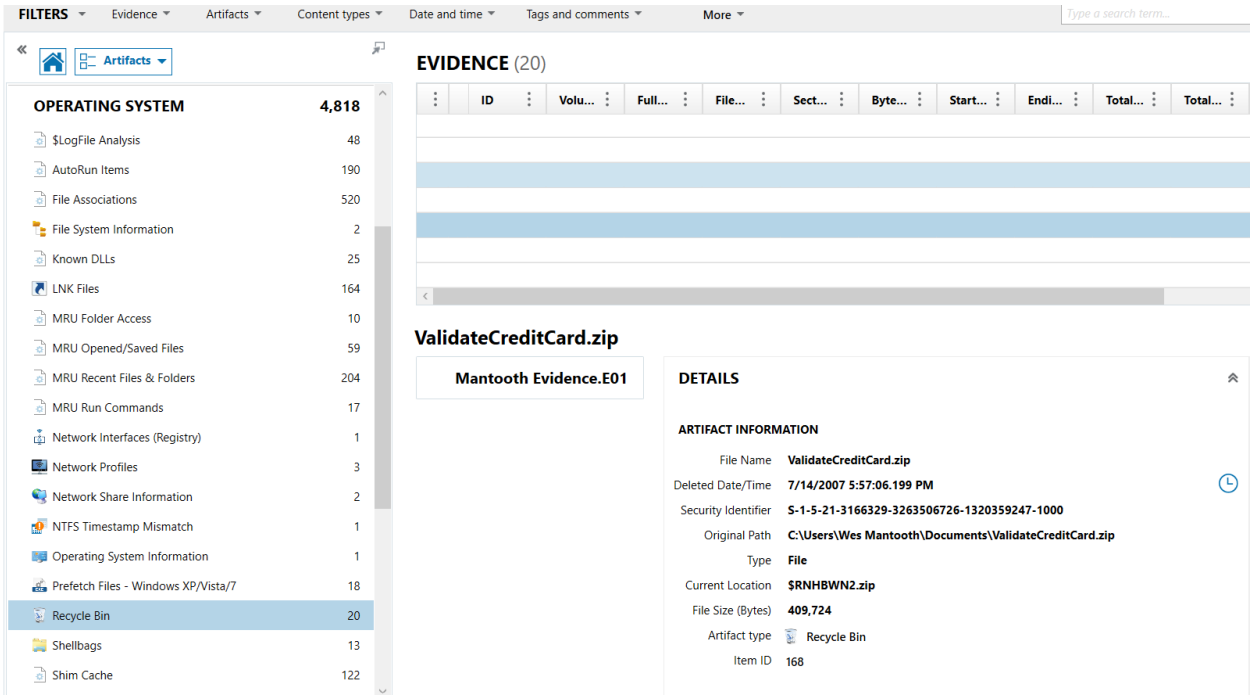

Figure 6.4 – Validate Credit Card

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 suspects 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.