MANTOOTH Investigation

Ferris State University

DFOR 310

Zachary C. Schulte

Table of Contents

Introduction

This week is my practical mid-term, and I am investigating the suspect Wes Mantooth's laptop. Investigators have been on Wes Mantooth's trail and have been searching for him on accounts of distributing drugs and fraudulent credit cards.

Imaging the Hard Drive

FTK Imager

I am using a software known as FTK Imager® to capture an image of the hard drive. After the laptop has been removed from the suspects home legally, I take it in the lab testing environment, I then pull the hard drive from the laptop and capture the BIOS system date and time. This will be used to create timestamps of files on the system.

After the BIOS system date and time has been documented properly, the hard drive gets installed back into the device. I then connect a write blocker on the laptop. This write blocker will allow me to capture an image of the hard drive without altering any of the files. It will then provide a bit-by-bit copy of all information within the drive. Figure 1.0 shows the case information that is provided before the image is created.

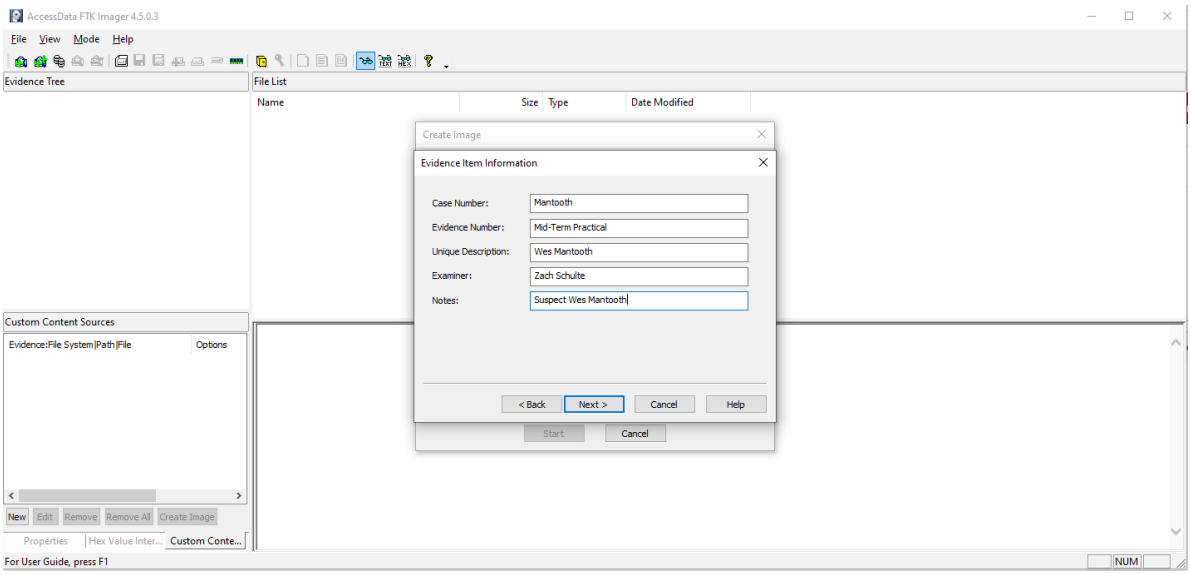

Figure 1.0

Figure 1.0 shows that my toolkit has a clean hard drive that has been tested clean.

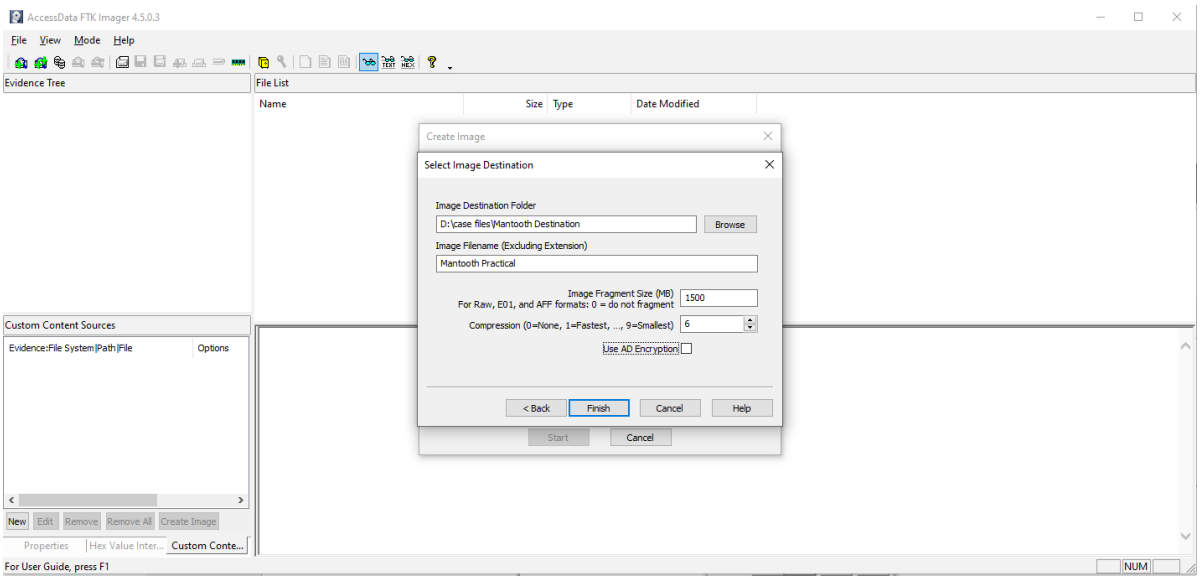

Figure 1.1

Figure 1.1 shows where the destination folder is and where the image will be stored.

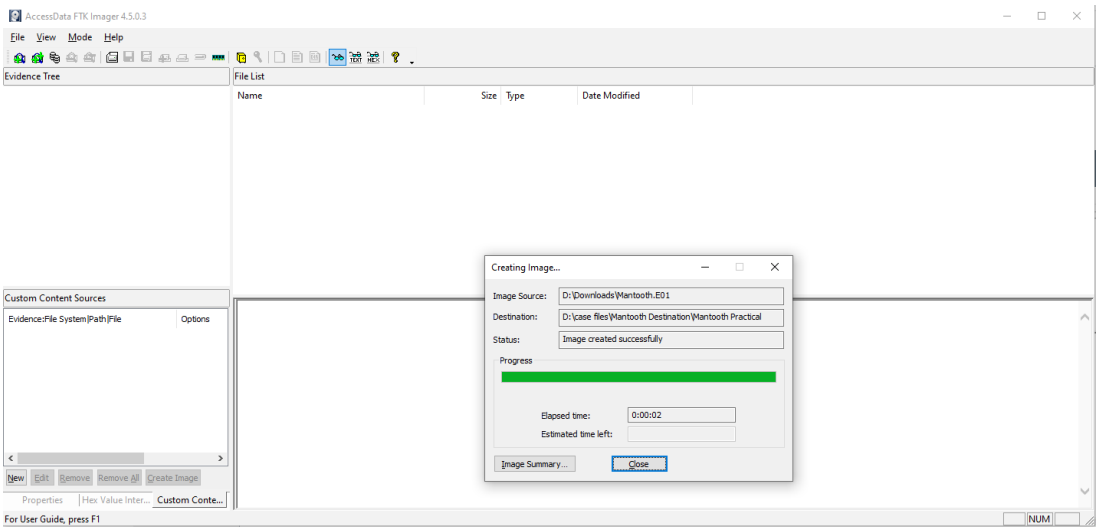

Figure 1.2

Figure 1.2 shows the physical creation of the image, where it is stored, and that the process of creating an image is complete.

After the image is finished creating, it will create a .txt document within that same folder that provides an image summary. This gives information related to the case number, evidence number, who the investigator is, and any notes related to the case. This information was copied from the summary.

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: Mantooth
Evidence Number: Mid-Term Practical
Unique description: Wes Mantooth
Examiner: Zach Schulte
Notes: Mid-Term Practical

Information for D:\case files\Mantooth Destination\Mantooth:

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: Mon Feb 20 13:30:06 2023

Acquisition finished: Mon Feb 20 13:30:07 2023
Segment list:
D:\case files\Mantooth Destination\Mantooth.E01

Image Verification Results:
Verification started: Mon Feb 20 13:30:07 2023
Verification finished: Mon Feb 20 13:30:08 2023
MD5 checksum: 31217210a1a69f272079a3bde3d9d8fc : verified
SHA1 checksum: 12e4ac047e328ca2bd63a4d65df25b3ecba55769 : verified

When you either download a file or take an image of a file you want to look at the hash values as they are a digital fingerprint of the file. “In simple terms, a hash value is a specific number string that’s created through an algorithm, and that is associated with a particular file. If the file is altered in any way, and you recalculate the value, the resulting hash will be different.” (Callaghan, 2020)

Figure 1.4 shows that both SHA-1 and MD5 hashes are matching. This means that we can continue the investigation on Wes Mantooth’s laptop.

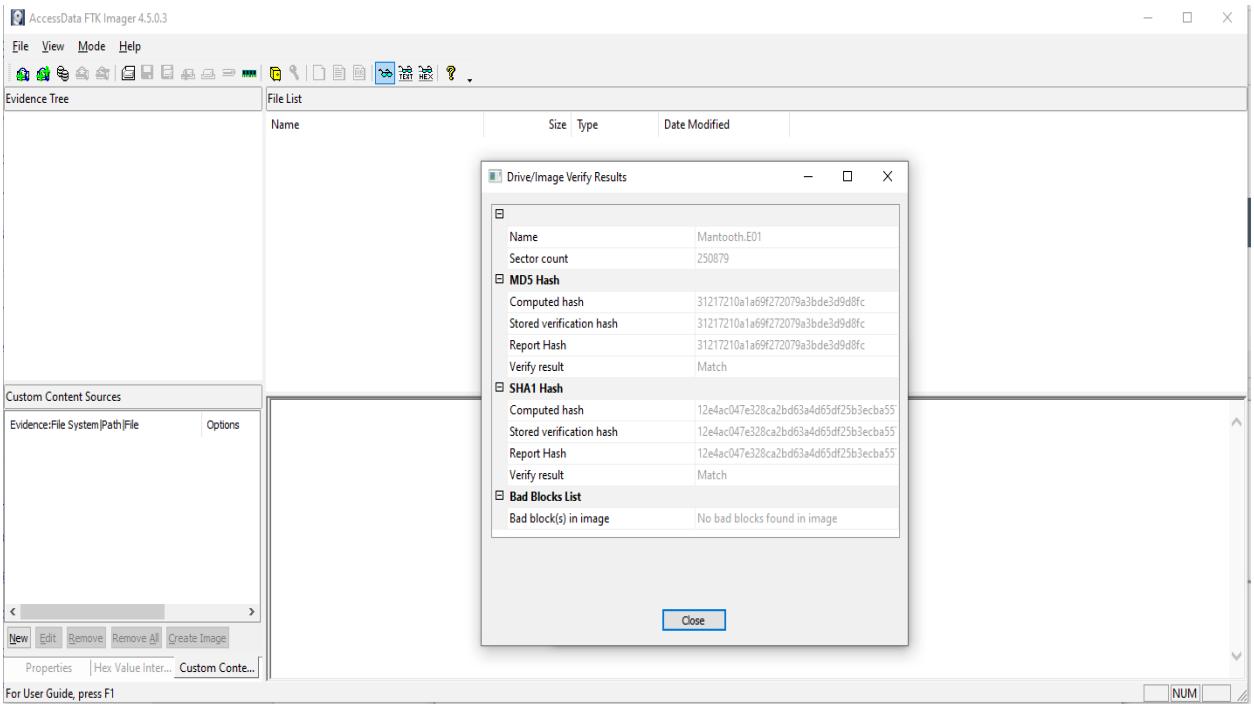

Figure 1.4

Figure 1.4 shows that the SHA-1 and MD5 hashes are matching on the image summary.

Presentation of Evidence

Forensic Explorer

The software I am currently using is called Forensic Explorer® V5.6.8. This software allows me to look at the image of the drive that I took. It also allows me to access the Windows Registry of the image. Figures 1.5-1.8 show the initial process of setting Forensic Explorer up

and providing the investigator information and time zone.

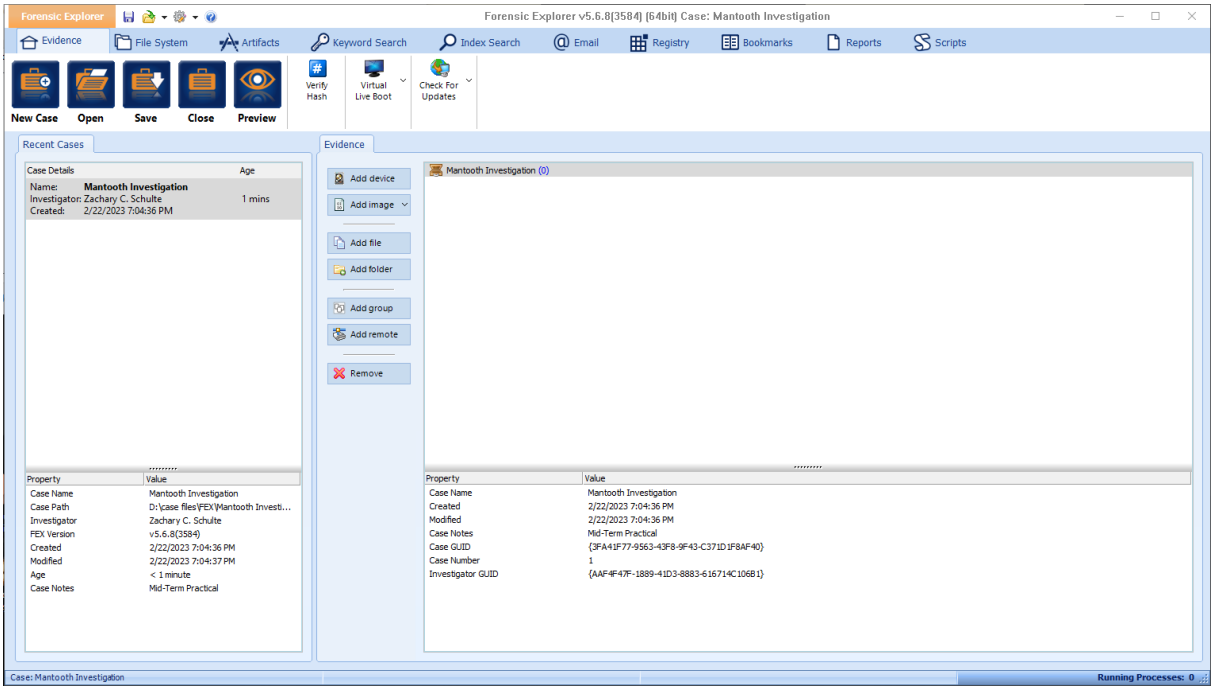

Figure 1.5

Figure 1.5 shows the opening of Forensic Explorer.

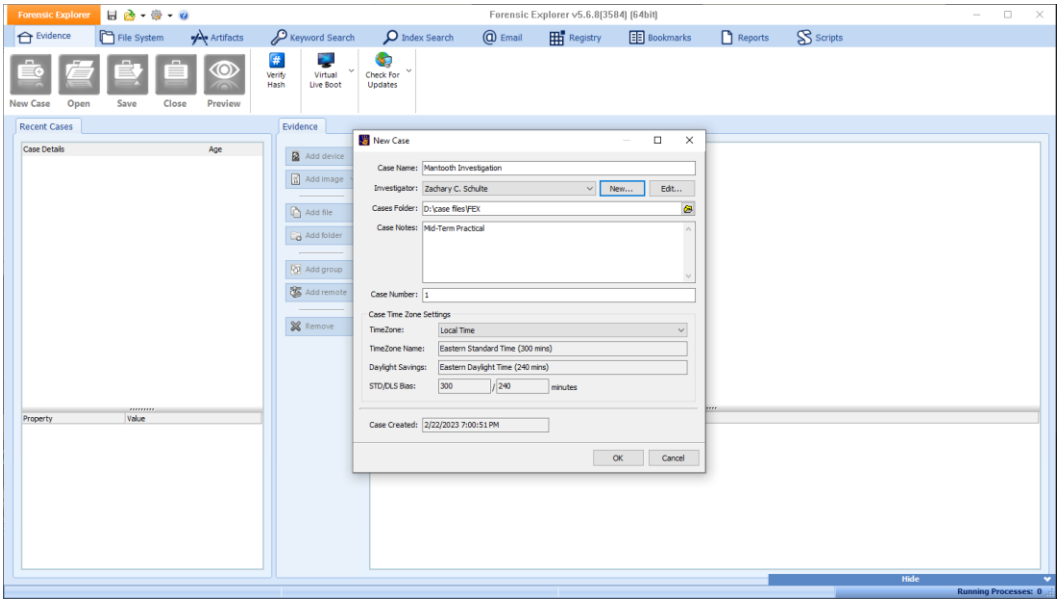

Figure 1.6

Figure 1.6 shows the creation of the new case including Case Name and Investigator information.

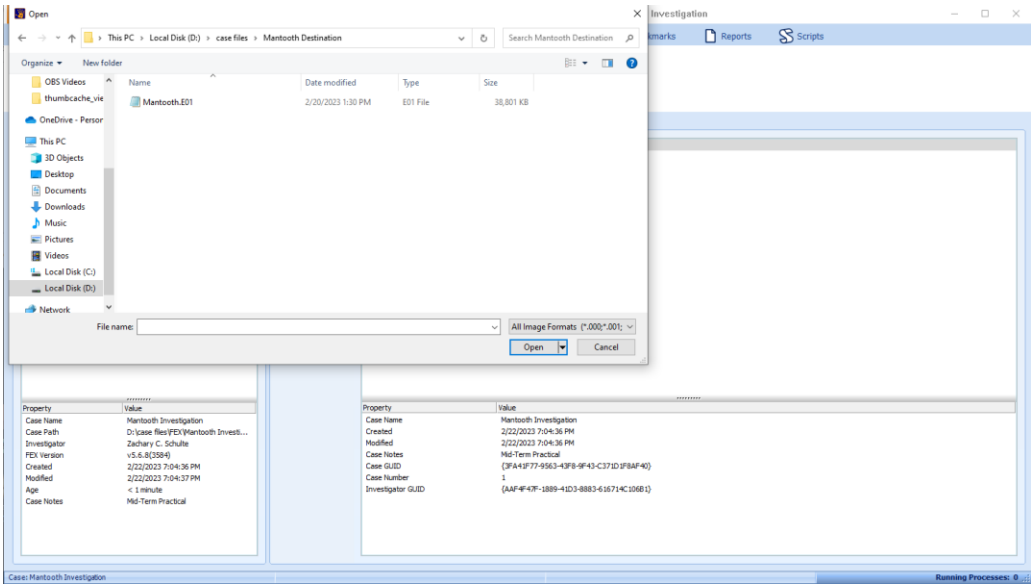

Figure 1.7

Figure 1.7 shows the process of loading the image file into Forensic Explorer.

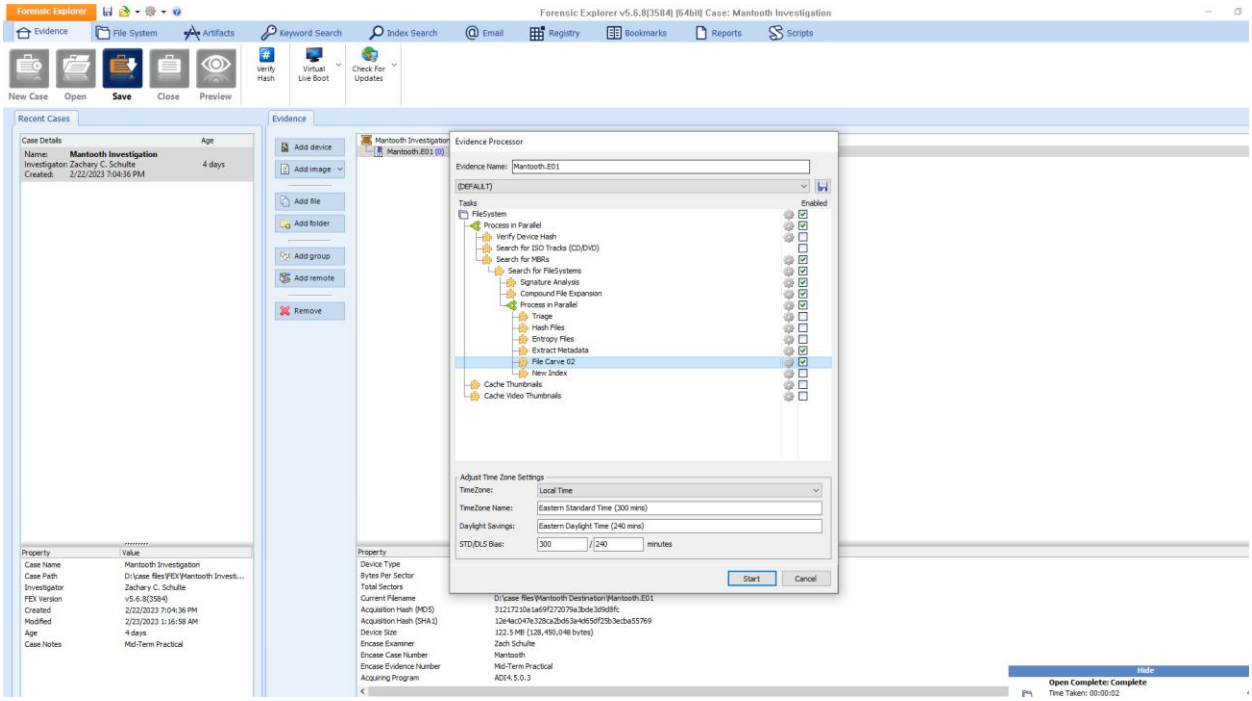

Figure 1.8

Figure 1.8 shows what data Forensic Explorer will be searching for. These are all the options I chose based on this case.

Registry

The registry is found on the Windows Operating systems, and I will be using Forensic Explorer to obtain the registry information. The Hives I am going to look at throughout this process are: NTUser.Dat, Software, System, Security Account Manager(SAM). To look at the registry information of the computer, I need to import it from the File System to the registry in Forensic Explorer. There is only one image file that has been imported into Forensic Explorer. Figures 1.9 – 2.0 show the image as well as where the registry information is found.

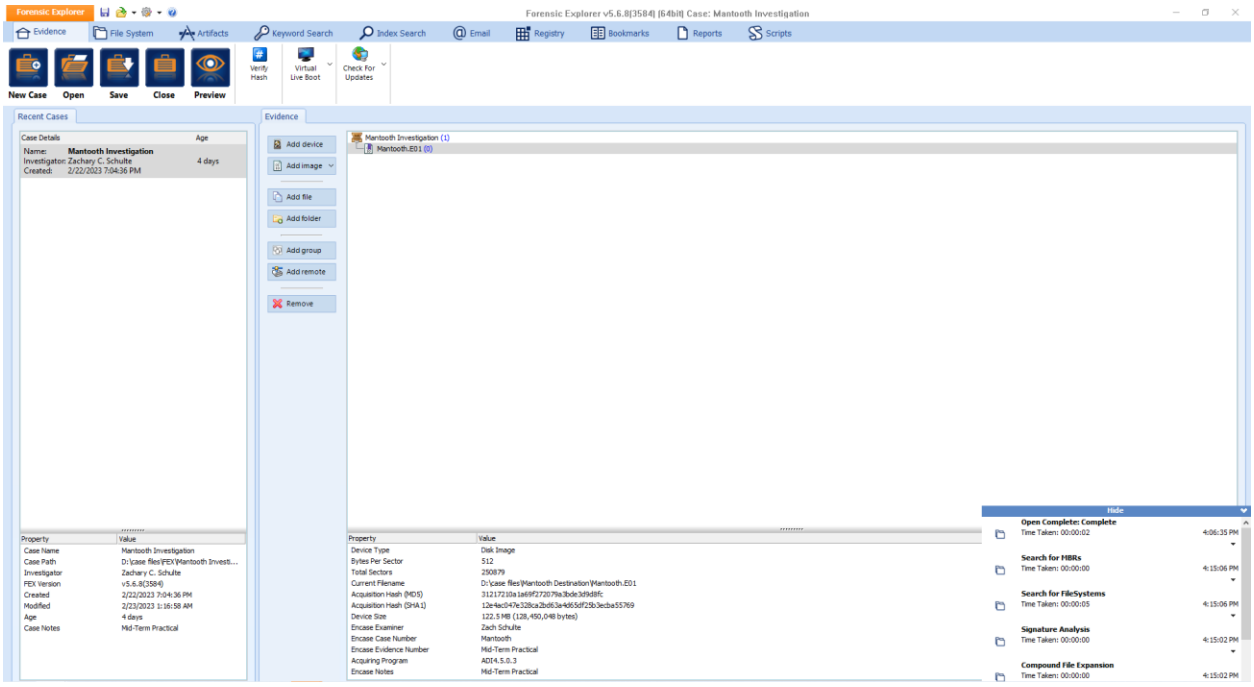

Figure 1.9

Figure 1.9 shows the initial loading of the case after the image has been properly loaded.

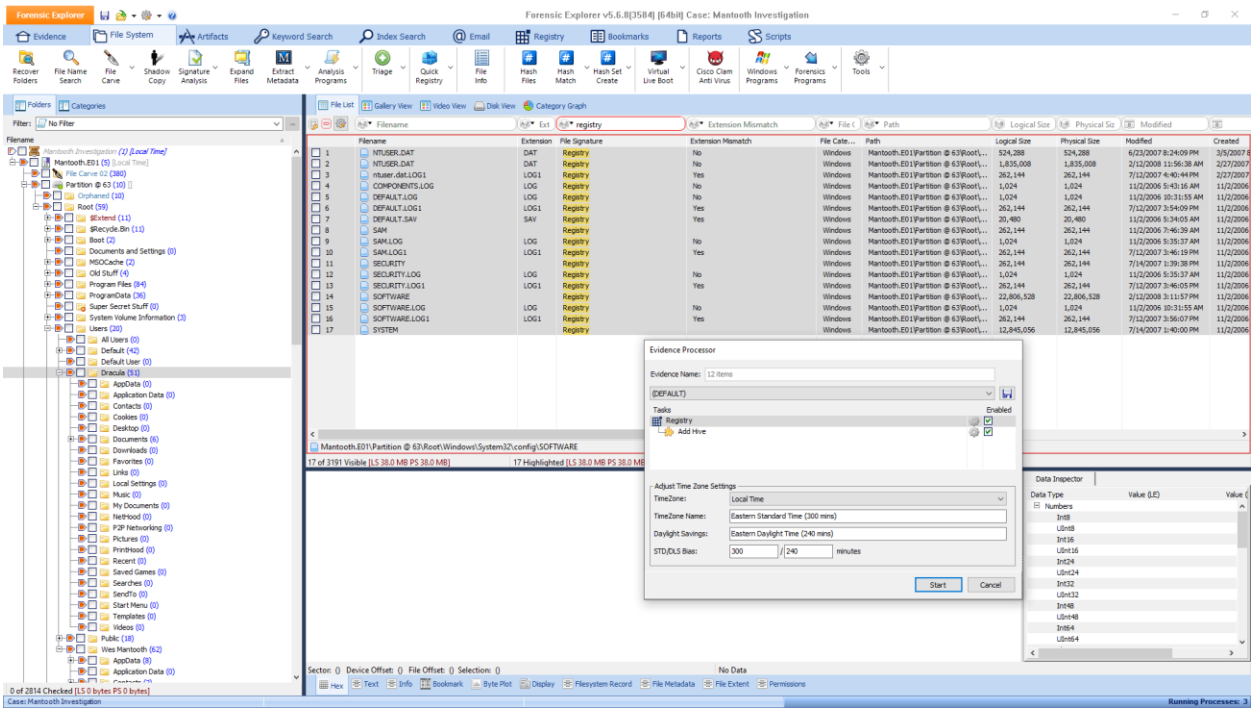

Figure 2.0

Figure 2.0 shows the registry data being sent to the registry module for it to be analyzed.

Security Accounts Manager

The Security Accounts Manager or (SAM) is the first hive of the registry I will be analyzing. This hive contains usernames as well as passwords for all accounts. There are five user accounts within this SAM hive registry. Pasted below directly from the SAM hive is the information related to all users set up.

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.

System.

The next hive in the registry is called system. This hive gives all the information located within the system or computer. Described and pasted below is the information related to the computer name that was entered at installation.

Computer name.

The computer name given was Wes Mantooth's first and last name hyphen PC.

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.

There appears to be no information on the last shutdown time recorded on this laptop.

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.

The time zone recorded states it is Mountain Standard Time.

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 Devices.

The next set of information I want to gather is related to external Universal Serial Bus (USB) storage devices that have been on this laptop previously. According to Forensic Explorer there have been fourteen USB devices.

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): 12-Feb-2008 17:21:52 [UTC]

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

Device GUID: {3e4bf6f7-e955-11db-bfe7-00038a000015}

Driver Letter: G

Last User: Wes Mantooth

~~~~~~~~~~~~~~~~

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): 06-Mar-2007 15:38:15 [UTC]

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

Device GUID: {43f97a97-cbf8-11db-a6d8-806e6f6e6963}

Last User: Wes Mantooth

~~~~~~~~~~~~~~~~

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): 09-Mar-2007 00:43:02 [UTC]

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

Device GUID: {43f97b9a-cbf8-11db-a6d8-00038a000015}

Last User: Wes Mantooth

~~~~~~~~~~~~~~~~

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM > SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Flash&Prod_Drive_SM_USB20&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): 12-Feb-2008 20:50:15 [UTC]

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

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

Last User: Wes Mantooth

~~~~~~~~~~~~~~~~

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 Class ID: Disk&Ven_Flash&Prod_Drive_UT_USB20&Rev_0.00

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): 12-Feb-2008 19:19:30 [UTC]

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

Device GUID: {6e45a80c-dd60-11db-bd31-00038a000015}

Driver Letter: F

Last User: Wes Mantooth

~~~~~~~~~~~~~~~~

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&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): 09-Mar-2007 01:22:15 [UTC]

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

Device GUID: {ddba5774-cdb5-11db-8899-00038a000015}

Last User: Wes Mantooth

~~~~~~~~~~~~~~~~

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): 11-Oct-2007 21:33:18 [UTC]

Last Connected (VID_&PID_): 14-Jul-2007 17:58:45 [UTC]

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

Driver Letter: E

Last User: Wes Mantooth

~~~~~~~~~~~~~~~~

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): 14-Jul-2007 17:58:25 [UTC]

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

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

Last User: Wes Mantooth
~~~~~~~~~~~~~~~~

~~~~~~~~~~~~~~~~

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): 13-Apr-2007 00:52:17 [UTC]

Last Connected (VID_&PID_): {Never}

Device GUID: {3e4bf70f-e955-11db-bfe7-00038a000015}

Driver Letter: H

Last User: Wes Mantooth

~~~~~~~~~~~~~~~~

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): 18-Jun-2007 22:18:48 [UTC]

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

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

Last User: Wes Mantooth

~~~~~~~~~~~~~~~~

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): 12-Feb-2008 16:48:34 [UTC]

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

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

Last User: Wes Mantooth

~~~~~~~~~~~~~~~~

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): 18-Apr-2007 01:54:09 [UTC]

Last Connected (VID_&PID_): {Never}

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

Last User: Wes Mantooth

~~~~~~~~~~~~~~~~

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.

Software.

The hive I want to gather information from next is called software. This hive registry contains information related to what is installed on the device, the original OS install date, network cards, and the default user name.

Default username.

There is no recorded default username located on this device.

Search for: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultUserName

Description: Stores the last user name entered in the Log On to Windows dialog box.

Reference: http://technet.microsoft.com/en-us/library/cc939710.aspx

==========
~~~~~~~~~~~~~~~~

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

Registry Key Processor finished.

Email Clients.

Search for: SOFTWARE\Clients\Mail

Description: Email clients.

Reference: http://msdn.microsoft.com/en-us/library/dd203067%28VS.85%29.aspx

==========

Mantooth.E01\SOFTWARE\Clients\Mail\AOL\

Mantooth.E01\SOFTWARE\Clients\Mail\AOL\Protocols\mailto\

Mantooth.E01\SOFTWARE\Clients\Mail\AOL\Protocols\mailto\

Mantooth.E01\SOFTWARE\Clients\Mail\AOL\Protocols\mailto\DefaultIcon\

Mantooth.E01\SOFTWARE\Clients\Mail\AOL\Protocols\mailto\shell\open\command\

Mantooth.E01\SOFTWARE\Clients\Mail\AOL\shell\open\command\

Mantooth.E01\SOFTWARE\Clients\Mail\Hotmail\

Mantooth.E01\SOFTWARE\Clients\Mail\Hotmail\Protocols\mailto\

Mantooth.E01\SOFTWARE\Clients\Mail\Hotmail\Protocols\mailto\

Mantooth.E01\SOFTWARE\Clients\Mail\Hotmail\Protocols\mailto\DefaultIcon\

Mantooth.E01\SOFTWARE\Clients\Mail\Hotmail\Protocols\mailto\shell\open\command\

Mantooth.E01\SOFTWARE\Clients\Mail\Hotmail\shell\open\command\

Mantooth.E01\SOFTWARE\Clients\Mail\Microsoft Outlook\

Mantooth.E01\SOFTWARE\Clients\Mail\Microsoft Outlook\Envelope\CLSID\

Mantooth.E01\SOFTWARE\Clients\Mail\Microsoft Outlook\Envelope\CurVer\

Mantooth.E01\SOFTWARE\Clients\Mail\Microsoft Outlook\Protocols\

Mantooth.E01\SOFTWARE\Clients\Mail\Microsoft Outlook\Protocols\mailto\

Mantooth.E01\SOFTWARE\Clients\Mail\Microsoft Outlook\Protocols\mailto\

Mantooth.E01\SOFTWARE\Clients\Mail\Microsoft Outlook\Protocols\mailto\DefaultIcon\

Mantooth.E01\SOFTWARE\Clients\Mail\Microsoft
Outlook\Protocols\mailto\shell\open\command\

Mantooth.E01\SOFTWARE\Clients\Mail\Microsoft Outlook\shell\open\command\

Mantooth.E01\SOFTWARE\Clients\Mail\Microsoft Outlook\shell\Properties\command\

Mantooth.E01\SOFTWARE\Clients\Mail\Windows Mail\

Mantooth.E01\SOFTWARE\Clients\Mail\Windows Mail\Envelope\CLSID\

Mantooth.E01\SOFTWARE\Clients\Mail\Windows Mail\Envelope\CurVer\

Mantooth.E01\SOFTWARE\Clients\Mail\Windows Mail\Protocols\mailto\

Mantooth.E01\SOFTWARE\Clients\Mail\Windows Mail\Protocols\mailto\

Mantooth.E01\SOFTWARE\Clients\Mail\Windows Mail\Protocols\mailto\DefaultIcon\

Mantooth.E01\SOFTWARE\Clients\Mail\Windows Mail\Protocols\mailto\shell\open\command\

Mantooth.E01\SOFTWARE\Clients\Mail\Windows Mail\shell\open\command\

Mantooth.E01\SOFTWARE\Clients\Mail\Yahoo! Mail\

Mantooth.E01\SOFTWARE\Clients\Mail\Yahoo! Mail\Protocols\mailto\

Mantooth.E01\SOFTWARE\Clients\Mail\Yahoo! Mail\Protocols\mailto\

Mantooth.E01\SOFTWARE\Clients\Mail\Yahoo! Mail\Protocols\mailto\DefaultIcon\

Mantooth.E01\SOFTWARE\Clients\Mail\Yahoo! Mail\Protocols\mailto\shell\open\command\

Mantooth.E01\SOFTWARE\Clients\Mail\Yahoo! Mail\shell\open\command\

Registry Key Processor finished.

OS Install Date.

The next piece of information I am going to look at is the Operating System install date (OS Install Date) which is on February 27th, 2007, at 7:22:03 PM.

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.

Registered User.

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.

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.

NTUser.Dat

The final registry hive I will gather information from is NTuser.dat. This hive registry has information on recent documents, and websites on Internet Explorer visited.

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.

==========

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.ad1\

Value	Data
~~	~~~~
0	recbin.ad1,File
1	RECBIN Dustin.ad1,File
2	recbinDustin.ad1,File
MRUListEx	2 1 0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.bek\

Value	Data
~~	~~~~
0	key.bek,File
MRUListEx	0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.bmp\

Value	Data
~~	~~~~
0	nationaltall.bmp,File
1	untitled.bmp,File
2	Guts.bmp,File
3	Camera.bmp,File
MRUListEx	0 3 2 1

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.doc\

Value	Data
~~	~~~~
0	C money plates.doc,File
1	Wes.doc,File
2	russ_2_Абажурный.doc,Unknown
3	russ_4_ящеркой.doc,Unknown
4	ar_test_نقيصته.doc,Unknown
5	Dear Sweetie.doc,File
6	Dear Sweetie2.doc,File
7	John.doc,File
MRUListEx	7 1 0 6 5 4 3 2

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.evtx\

Value	Data
~~	~~~~
0	Internet Explorer.evtx,File
1	Microsoft-Windows-ReadyBoost%4Operational.evtx,File
2	testevt.evtx,File
3	securityevt.evtx,File
MRUListEx	3 2 0 1

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.fang\

Value	Data
~~	~~~~
0	WM.fang,File
1	Wes.fang,File
MRUListEx	1 0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.gif\

Value	Data
~~	~~~~
0	Bill_Gates.gif,File
1	burgerkingandronald.gif,File
2	Ape_20shoot.gif,File
3	penguin_waiter_with_tray_sm_wht.gif,File
4	nationaltall.gif,File
5	91064B.gif,File
6	C01VNCCHK_e.gif,File
7	Z169PCHK_e.gif,File
8	Prescription2.gif,File
9	prescription.gif,File
MRUListEx	4 8 9 3 2 1 0 7 6 5

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.htm\

Value	Data
0	Enrollment approved for Web seminar Ken and Mitch's FTK 2 Test.htm,File
MRUListEx	0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.html\

Value	Data
0	165183.html,File
MRUListEx	0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.ini\

Value	Data
0	aim.ini,File

1	msn.ini,File
2	yahoo.ini,File
MRUListEx	0 2 1

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg\

Value	Data
~~	~~~~
0	Jaws Cat.jpg,File
1	useles_cat.jpg,File
2	fun81.jpg,File
3	Other Uncle Jon.jpg,File
4	cathelmet.jpg,File
5	Wes.jpg,File
6	doc-prescription.jpg,File
7	Dear ole Dad.jpg,File
8	clean-dazed-kitty.jpg,File
9	snaggle_kitty.jpg,File
MRUListEx	2 4 0 1 8 9 7 5 3 6

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.log\

Value	Data
~~	~~~~

0	edb00007.log,File
MRUListEx	0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.mht\

Value	Data
~~	~~~~
0	How to create and manipulate NTFS junction points.mht,File
1	Junction v1_04.mht,File
MRUListEx	1 0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf\

Value	Data
~~	~~~~
0	order851797-2007-04-12-13-17-02.pdf,File
1	order851797-2007-04-12-13-17-02 (1).pdf,File
MRUListEx	1 0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pf\

Value	Data
0	BESTCRYPT.EXE-7DE5BC83.pf,File
MRUListEx	0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.png\

Value	Data
0	funny.png,File
MRUListEx	0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.ppt\

Value	Data
0	ATM_THEFTS1.ppt,File
MRUListEx	0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.rtf\

Value	Data
~~	~~~~
MRUListEx	

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.tooth\

Value	Data
~~	~~~~
0	WM.tooth,File
MRUListEx	0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt\

Value	Data
~~	~~~~
0	Vista Mantooth Bitlocker Key 1.4.txt,File
1	You Got it!.txt,File
2	WorkerLog.txt,File
3	mykey.txt,File
4	New Text Document.txt,File
5	Wes Mantooth Image_Key_Dustin.txt,File
6	urls.txt.txt,File
7	key.txt,File
8	Mantooth Vista 1.4 Key.txt,File

9	Bitlocker Command.txt.txt,File
MRUListEx	0 5 4 1 9 8 7 6 3 2

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.xar\

Value	Data
~~	~~~~
0	~ar1730.xar,File
MRUListEx	0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.xls\

Value	Data
~~	~~~~
0	Those who owes.xls,File
1	CC Nums.xls,File
MRUListEx	1 0

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.zip\

Value	Data

~~	~~~~
0	Funny Vids.zip,File
1	Super Secret Stuff.zip,File
2	seanbefore.zip,File
MRUListEx	0 2 1

Key Found:
Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\

Value	Data
~~	~~~~
0	Dear Sweetie.doc,File
1	testevt.evtx,File
10	clean-dazed-kitty.jpg,File
100	Tooth Docs,File
101	Wes.fang,File
11	C money plates.doc,File
12	EFS DOCS,File
13	Wes.doc,File
14	Family Pix,File
15	fun81.jpg,File
16	nationaltall.gif,File
17	Car Titles,File
18	CC Nums.xls,File
19	Internet Explorer.evtx,File
2	Checks,File
20	WM.fang,File

21 91064B.gif,File
22 C01VNCCHK_e.gif,File
23 Dear ole Dad.jpg,File
24 Z169PCHK_e.gif,File
25 Prescription2.gif,File
26 prescription.gif,File
27 doc-prescription.jpg,File
28 order851797-2007-04-12-13-17-02 (1).pdf,File
29 restoredsalty,File
3 seanbefore,File
30 You Got it!.txt,File
31 Misc Docs,File
32 Funny Vids.zip,File
33 Local Disk (C:),File
34 Sounds and Video,File
35 Removable Disk (F:),File
36 How to create and manipulate NTFS junction points.mht,File
37 165183.html,File
38 Mr Smee,File
39 Pix,File
4 msn.ini,File
40 funny.png,File
41 order851797-2007-04-12-13-17-02.pdf,File
42 Bill_Gates.gif,File
43 101MSDCF,File
44 burgerkingandronald.gif,File
45 Johns Stuff (\\TRAINING-KEN),File
46 russ_2_Абажурный.doc,Unknown
47 russ_4_ящеркой.doc,Unknown

48 ar_test_نقيصته.doc,Unknown
49 Super Secret Stuff.zip,File
5 Scripts,File
50 WorkerLog.txt,File
51 Worker,File
52 mykey.txt,File
53 seanbefore.zip,File
54 useles_cat.jpg,File
55 Secret Stuff,File
56 edb00007.log,File
57 new,File
58 Those who owes.xls,File
59 ~ar1730.xar,File
6 My Internet Clearning Folder (\\mediacenter) (M:),File
60 Excel,File
61 untitled.bmp,File
62 Business Ideas,File
63 Guts.bmp,File
64 Camera.bmp,File
65 ATM_THEFTS1.ppt,File
66 Ape_20shoot.gif,File
67 Dear Sweetie2.doc,File
68 penguin_waiter_with_tray_sm_wht.gif,File
69 John.doc,File
7 nationaltall.bmp,File
70 recbin.ad1,File
71 Wes Mantooth Image_Key_Dustin.txt,File
72 RECBIN Dustin.ad1,File
73 recbinDustin.ad1,File

74 aim.ini,File

75 default,File

76 urls.txt.txt,File

77 Removable Disk (E:),File

78 key.txt,File

79 Mantooth Vista 1.4 Key.txt,File

8 Super Secret Stuff,File

80 Bitlocker Command.txt.txt,File

81 Vista Mantooth Bitlocker Key 1.4.txt,File

82 Logs,File

83 Microsoft-Windows-ReadyBoost%4Operational.evtx,File

84 BESTCRYPT.EXE-7DE5BC83.pf,File

85 Prefetch,File

86 Other Uncle Jon.jpg,File

87 Wes.jpg,File

88 Juncion.exe,File

89 Junction v1_04.mht,File

9 New Text Document.txt,File

90 Enrollment approved for Web seminar Ken and Mitch's FTK 2 Test.htm,File

91 MANTOOTH (F:),File

92 key.bek,File

93 snaggle_kitty.jpg,File

94 securityevt.evtx,File

95 WASHER (F:),File

96 Jaws Cat.jpg,File

97 cathelmet.jpg,File

98 yahoo.ini,File

99 WM.tooth,File

Key Found:
Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder\

Value	Data
0	Johns Stuff (\\TRAINING-KEN),File
1	Checks,File
10	Removable Disk (F:),File
11	Mr Smee,File
12	Car Titles,File
13	Misc Docs,File
14	Sounds and Video,File
15	Pix,File
16	101MSDCF,File
17	Super Secret Stuff,File
18	Worker,File
19	seanbefore,File
2	Scripts,File
20	new,File
21	Excel,File
22	Business Ideas,File
23	default,File
24	Removable Disk (E:),File
25	Logs,File
26	Prefetch,File
27	Family Pix,File
28	Juncion.exe,File

29 MANTOOTH (F:),File

3 WASHER (F:),File

4 EFS DOCS,File

5 My Internet Clearning Folder (\\mediacenter) (M:),File

6 Secret Stuff,File

7 Tooth Docs,File

8 restoredsalty,File

9 Local Disk (C:),File

MRUListEx 7 23 6 5 3 13 0 29 25 28 27 26 2 24 4 22 21 20 12 19 1 9 18 17 16 15 14 11 10 8

Key Found: Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\

Value Data

~~~~~ ~~~~

MRUListEx 100 101 20 99 81 71 75 74 98 4 55 15 32 97 96 54 10 6 95 9 31 30 94 1 45 93 92 91 90 82 19 88 89 36 14 23 87 86 85 84 83 5 7 16 25 27 26 80 79 78 77 76 73 72 70 12 69 13 18 11 68 67 0 66 62 65 64 63 61 59 58 60 57 56 17 3 2 53 33 52 51 50 49 8 48 47 46 44 43 39 42 34 28 40 24 22 21 41 38 37 35 29

Registry Key Processor finished.
~~~~~

Disk Structure

Partition Size

Within this device there is one image. On this image there are two partitions. On partition one (Partition @ 63) it contains 120~ megabytes of data. On partition 2 (Partition @ 224910) it contains 66~ megabytes of data.

Format.

Partition 1 (Partition @ 63) is formatted with NTFS. Partition 2 (Partition @ 224910) it is formatted with Ext2.

Active File Review

Axiom

This next software is called AXIOM Process and AXIOM Examine. Figures 2.1-2.3 show how the case is loaded in the software.

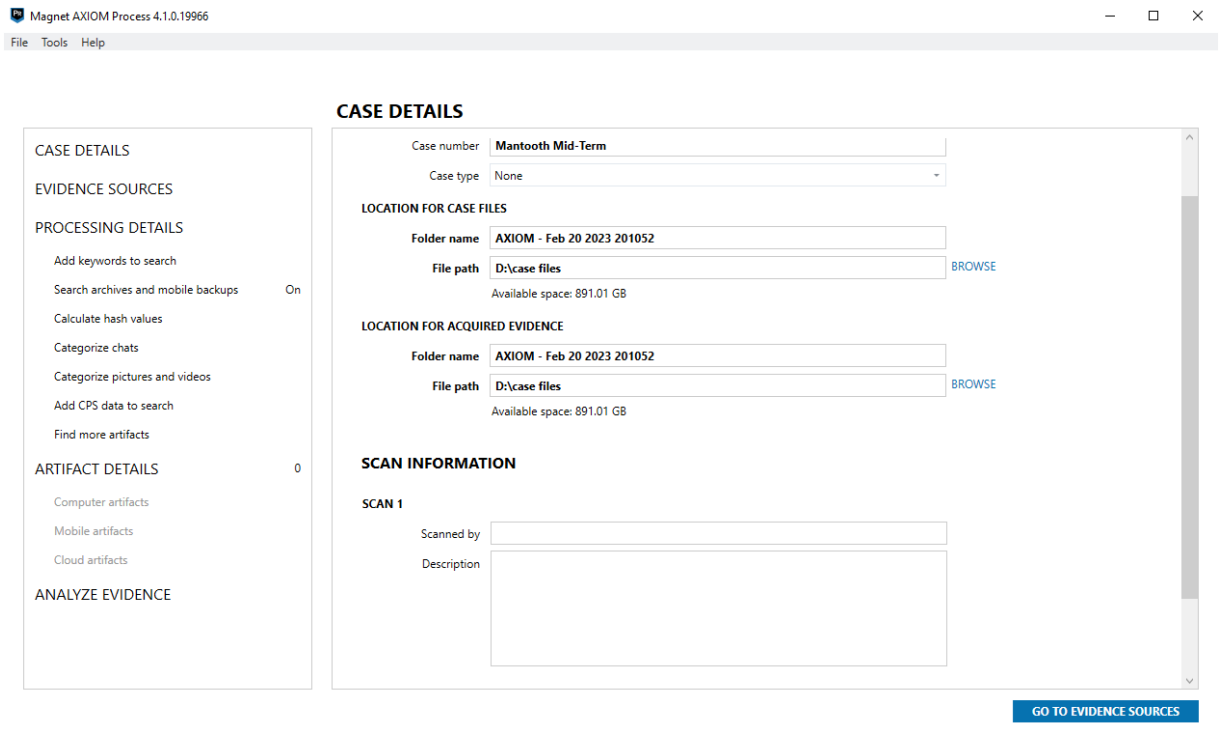

Figure 2.1

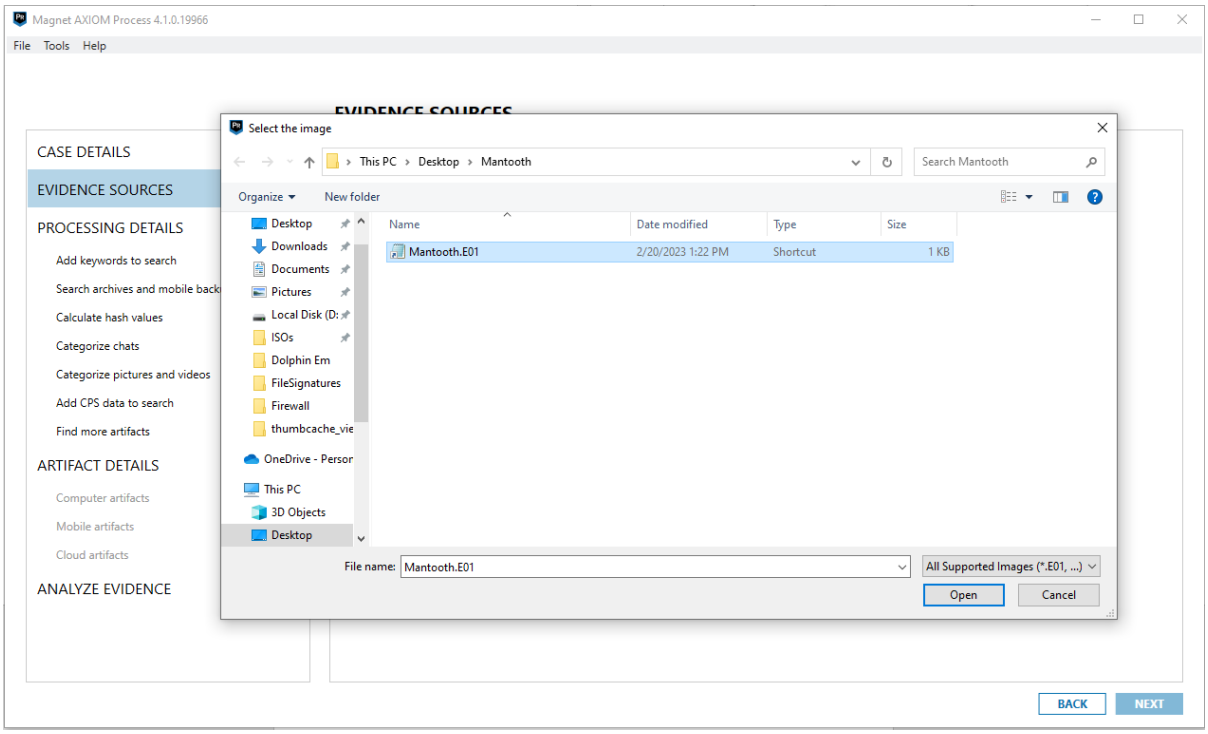

Figure 2.2

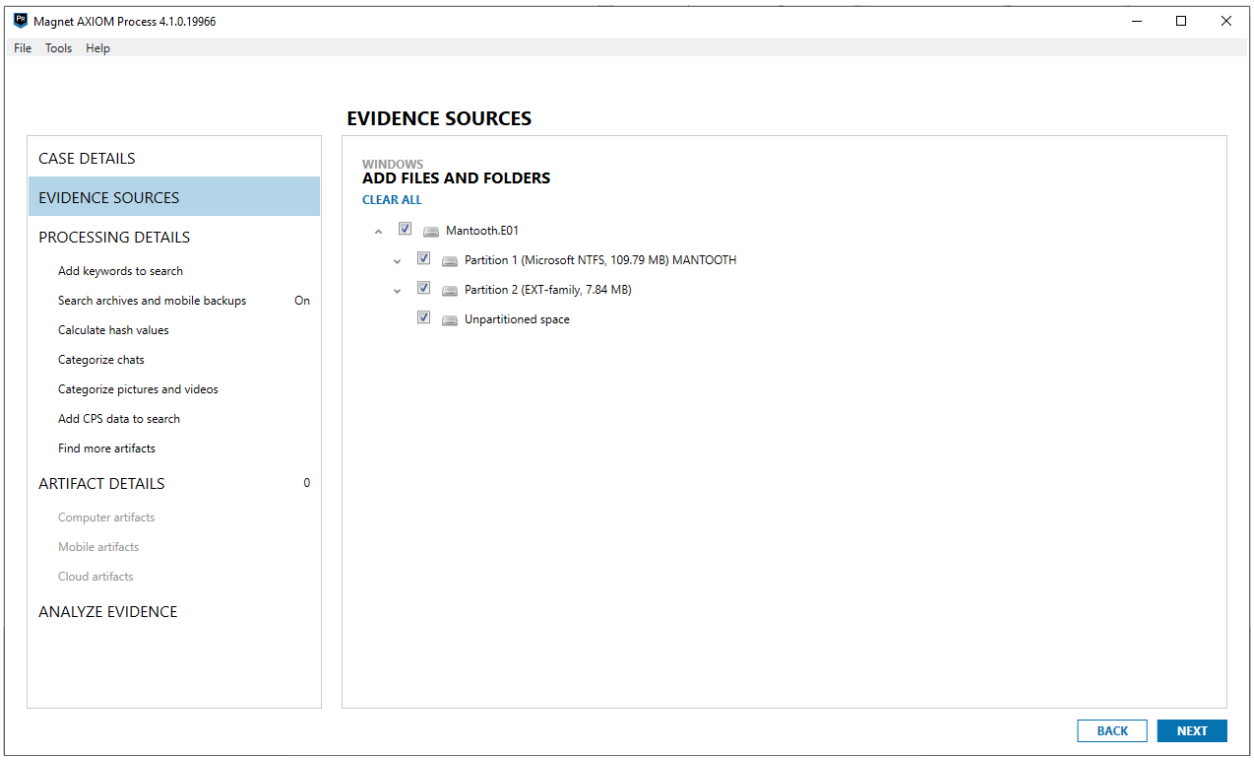

Figure 2.3

Web Related

Main History

This is the main history found on Internet Explorer and covers drug and atm stealing related searches. Figures 2.4 - 3.0 cover information related to Internet Explorer searches related to drug searches as well as atm stealing searches.

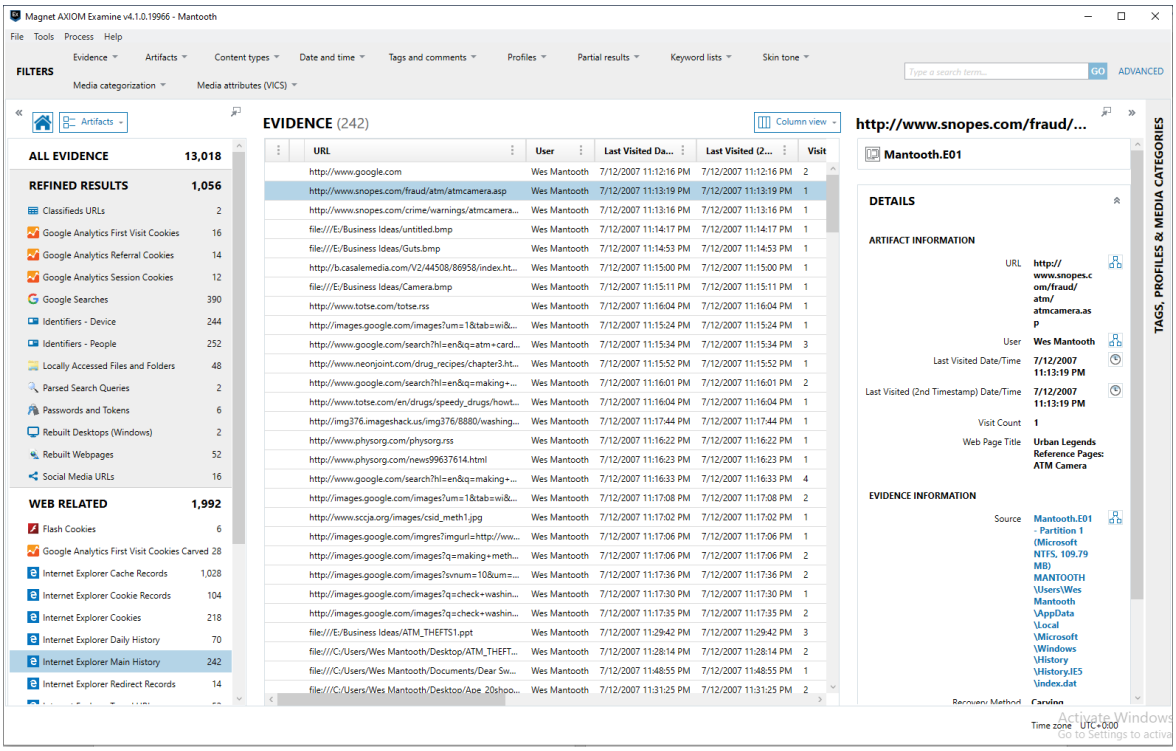
Magnet AXIOM Examine v4.1.0.19966 - Mantooth
File Tools Process Help
FILTERS
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone
Media categorization Media attributes (VICS)
ADVANCED
EVIDENCE (242)
ALL EVIDENCE 13,018
REFINED RESULTS 1,056
WEB RELATED 1,992
http://www.snopes.com/fraud/...
Mantooth.E01
DETAILS
ARTIFACT INFORMATION
EVIDENCE INFORMATION
TAGS, PROFILES & MEDIA CATEGORIES

Figure 2.4

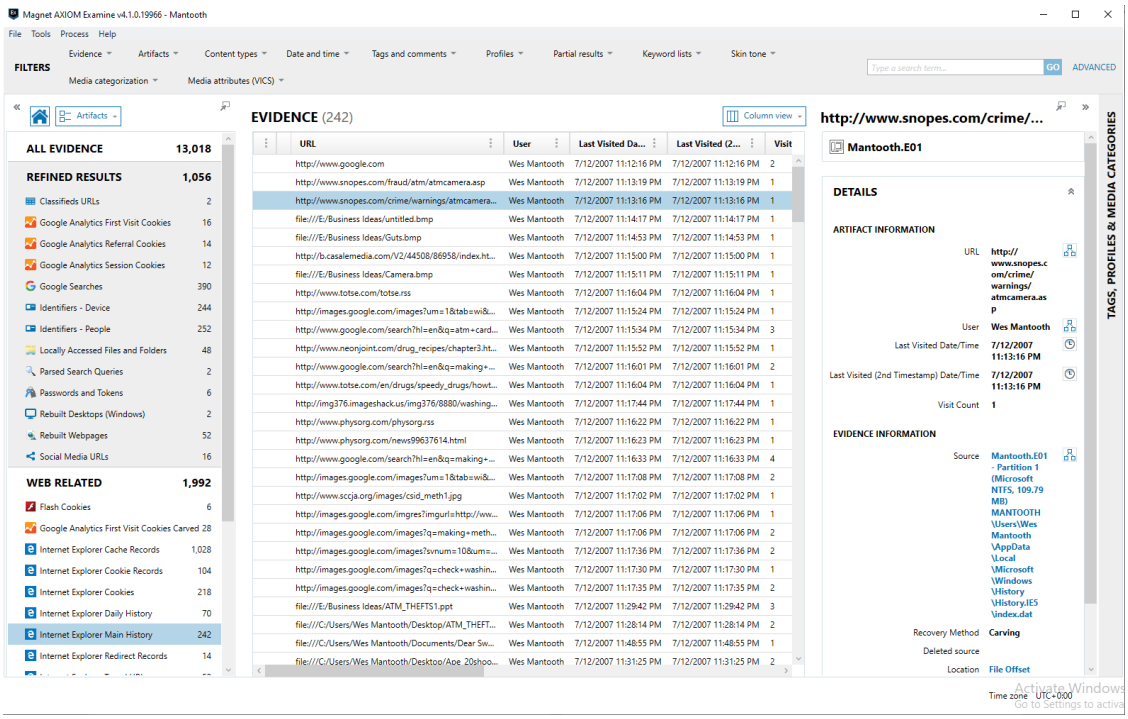
Magnet AXIOM Examine v4.1.0.19966 - Mantooth
File Tools Process Help
FILTERS
ADVANCED
EVIDENCE (242)
ALL EVIDENCE 13,018
REFINED RESULTS 1,056
WEB RELATED 1,992
http://www.snopes.com/crime/...
Mantooth.E01
DETAILS
ARTIFACT INFORMATION
EVIDENCE INFORMATION
TAGS, PROFILES & MEDIA CATEGORIES

Figure 2.5

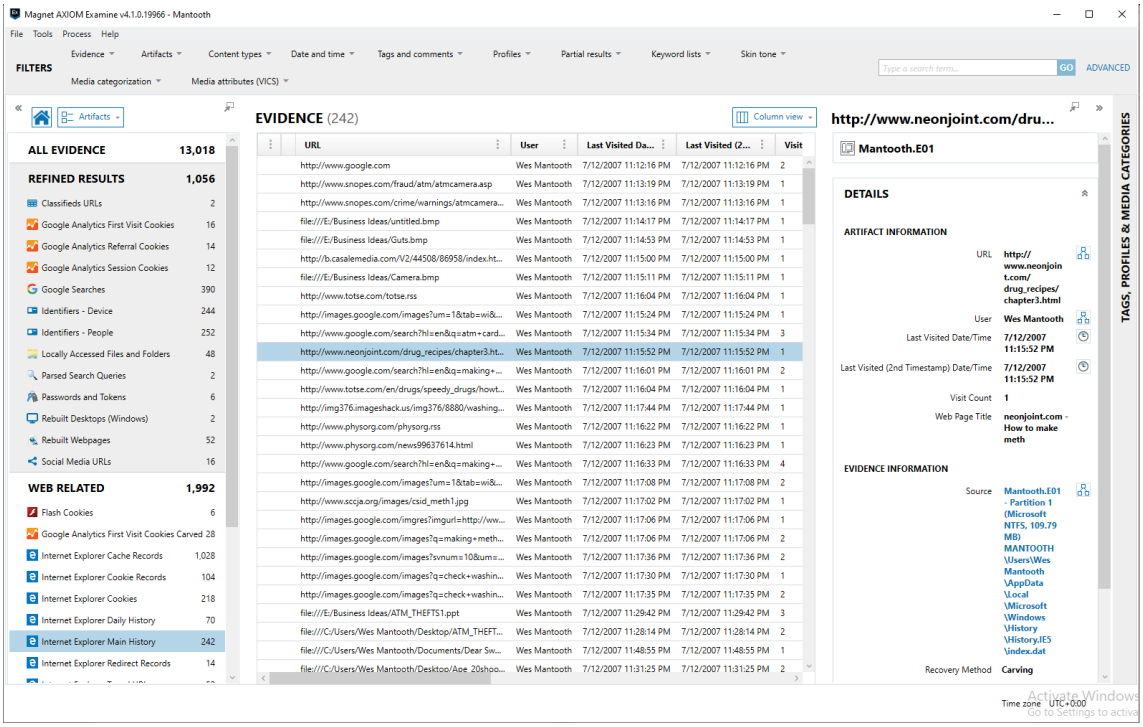

Figure 2.6

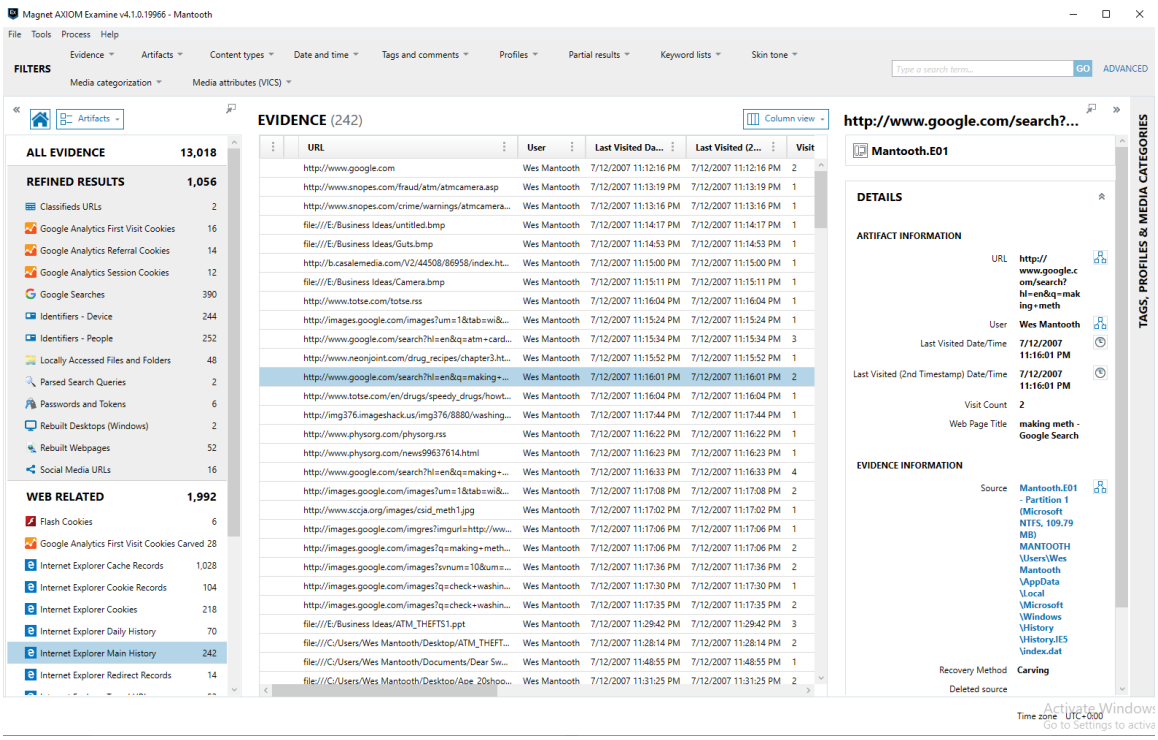

Figure 2.7

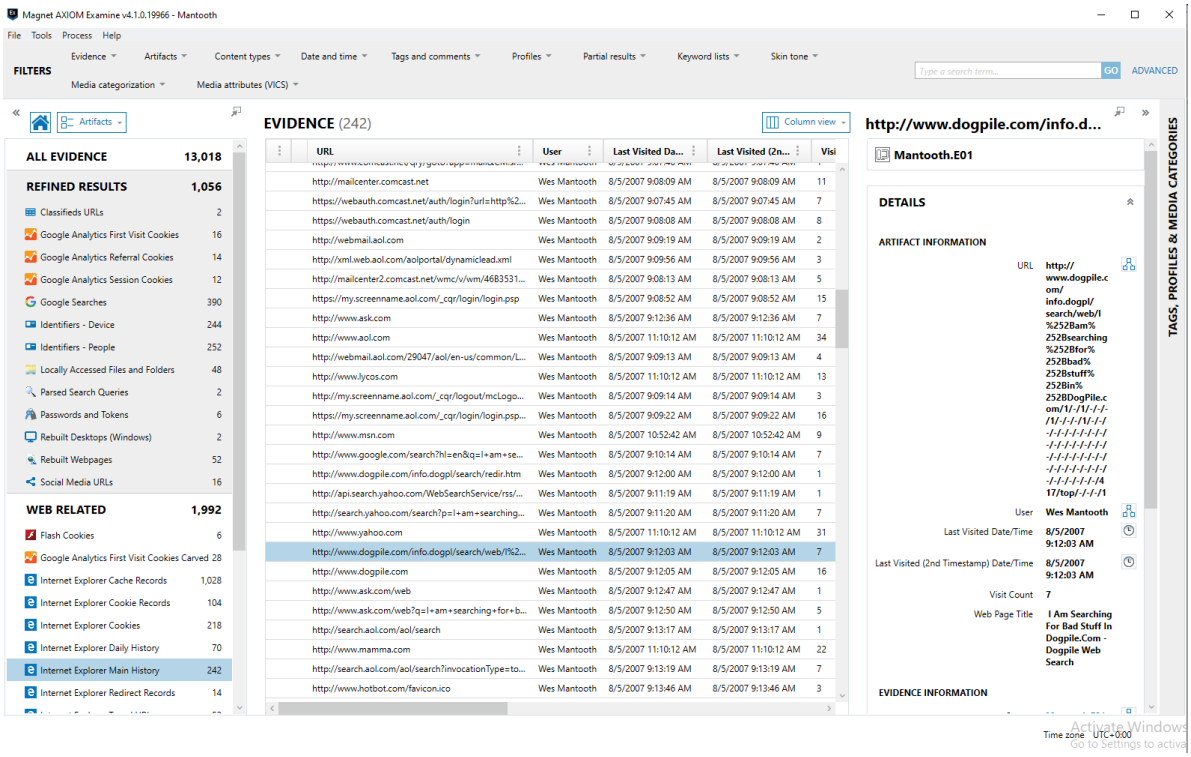

Figure 2.8

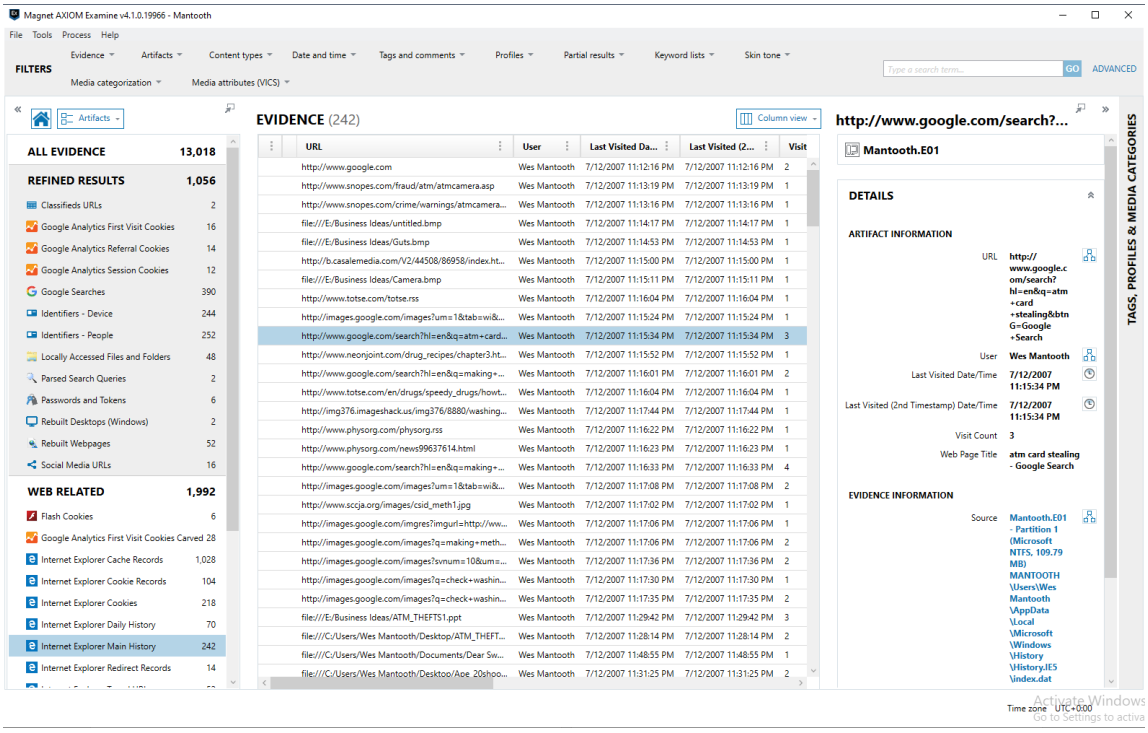

Figure 2.9

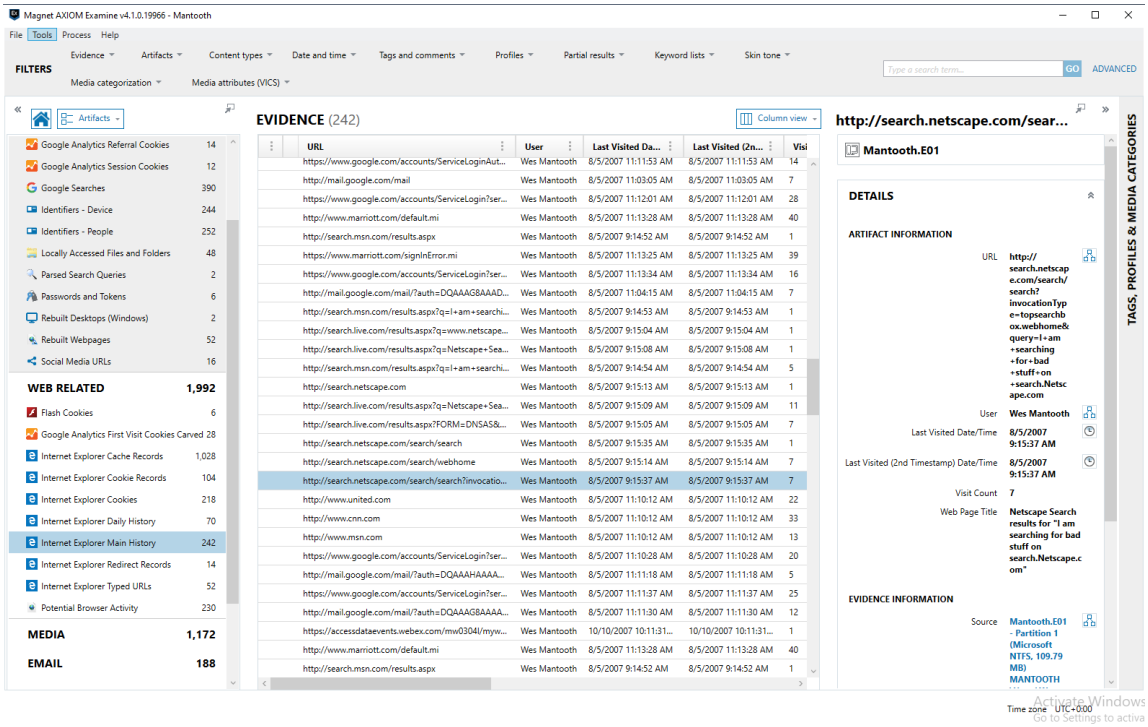

Figure 3.0

Daily History

This covers the daily history of the laptop on Internet Explorer before the device was legally obtained from the suspect, Wes Mantooth. Figure 3.1 - 3.5 contain searches related to atm stealing and drug searches.

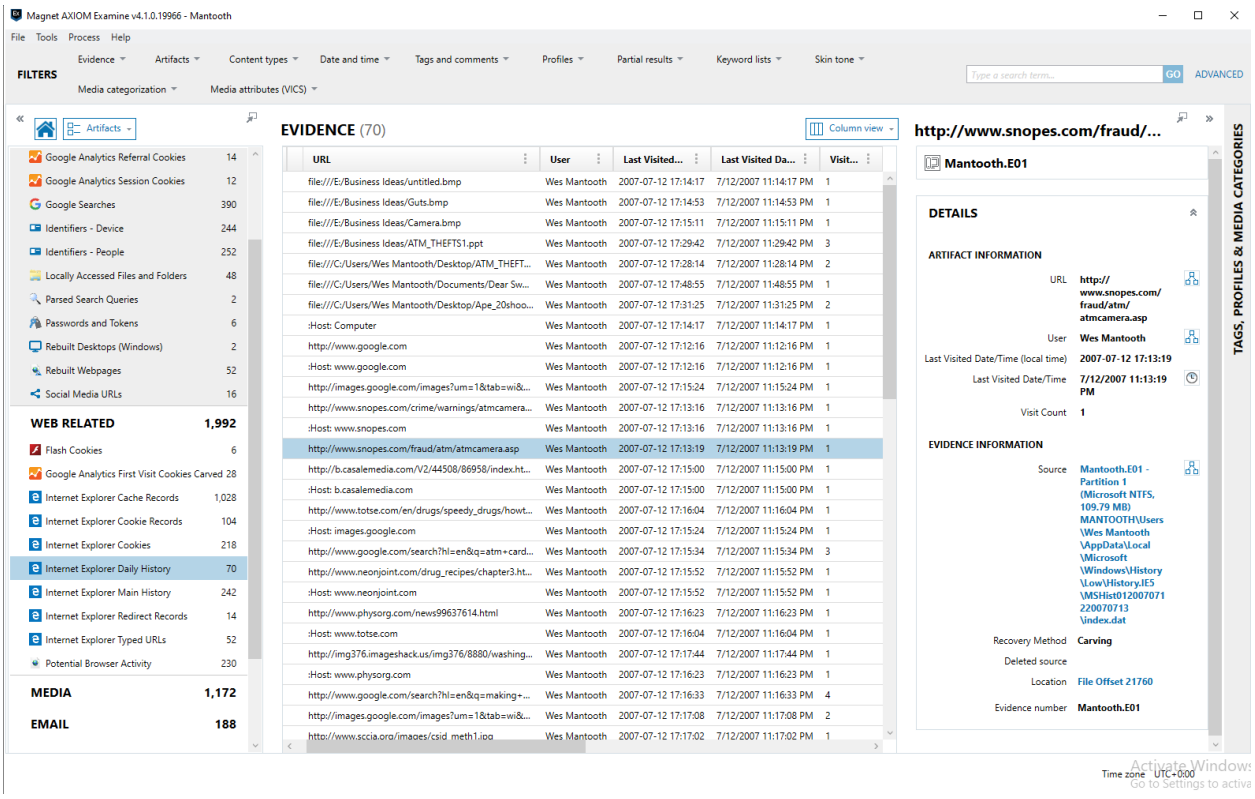
Magnet AXIOM Examine v4.1.0.19966 - Mantooth
File Tools Process Help
FILTERS
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone
Media categorization Media attributes (VICS)
ADVANCED
EVIDENCE (70)
Column view
http://www.snopes.com/fraud/...
Mantooth.E01
DETAILS
ARTIFACT INFORMATION
URL http://www.snopes.com/fraud/atm/atmcamera.asp
User Wes Mantooth
Last Visited Date/Time (local time) 2007-07-12 17:13:19
Last Visited Date/Time 7/12/2007 11:13:19 PM
Visit Count 1
EVIDENCE INFORMATION
Source Mantooth.E01 - Partition 1 (Microsoft NTFS, 109.79 MB) MANTOOTH\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012007071220070713\index.dat
Recovery Method Carving
Deleted source
Location File Offset 21760
Evidence number Mantooth.E01
TAGS, PROFILES & MEDIA CATEGORIES
WEB RELATED 1,992
MEDIA 1,172
EMAIL 188
Time zone UTC+0:00

Figure 3.1

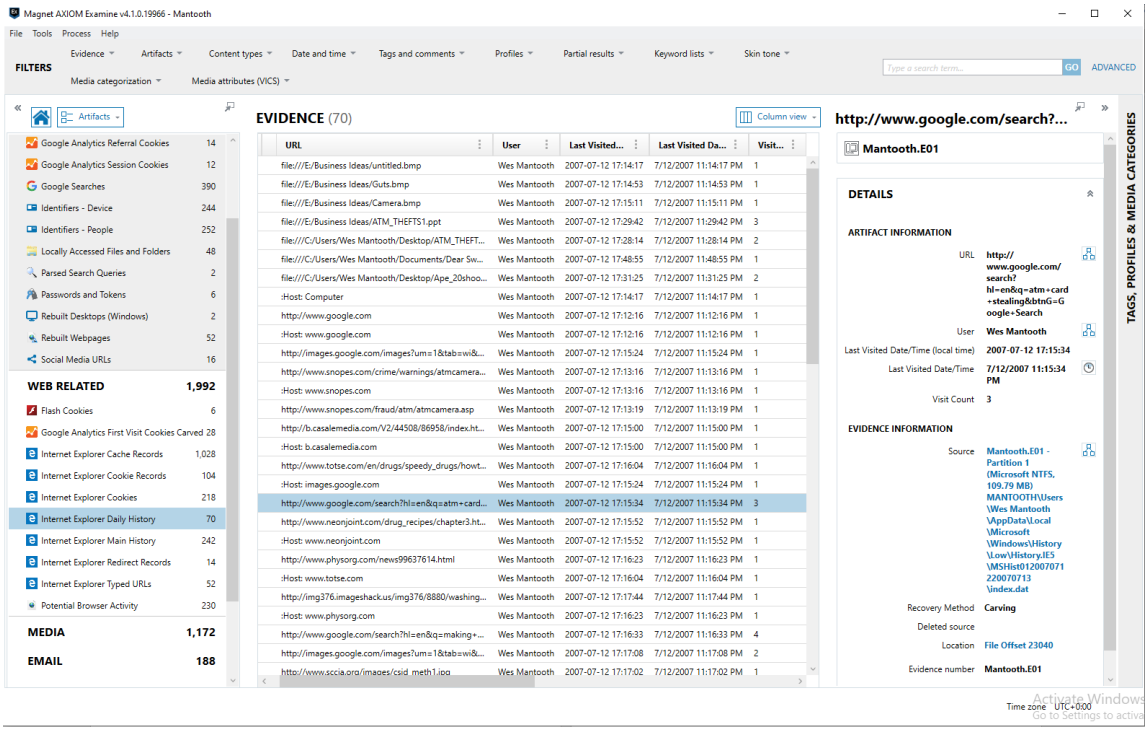
Magnet AXIOM Examine v4.1.0.19966 - Mantooth
EVIDENCE (70)
http://www.google.com/search?...
Mantooth.E01
DETAILS
ARTIFACT INFORMATION
URL http://www.google.com/search?hl=en&q=atm+card+stealing&btnG=Google+Search
User Wes Mantooth
Last Visited Date/Time (local time) 2007-07-12 17:15:34
Last Visited Date/Time 7/12/2007 11:15:34 PM
Visit Count 3
EVIDENCE INFORMATION
Source Mantooth.E01 - Partition 1 (Microsoft NTFS, 109.79 MB) MANTOOTH\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012007071220070713\index.dat
Recovery Method Carving
Deleted source
Location File Offset 23040
Evidence number Mantooth.E01
TAGS, PROFILES & MEDIA CATEGORIES
Time zone UTC+0:00

Figure 3.2

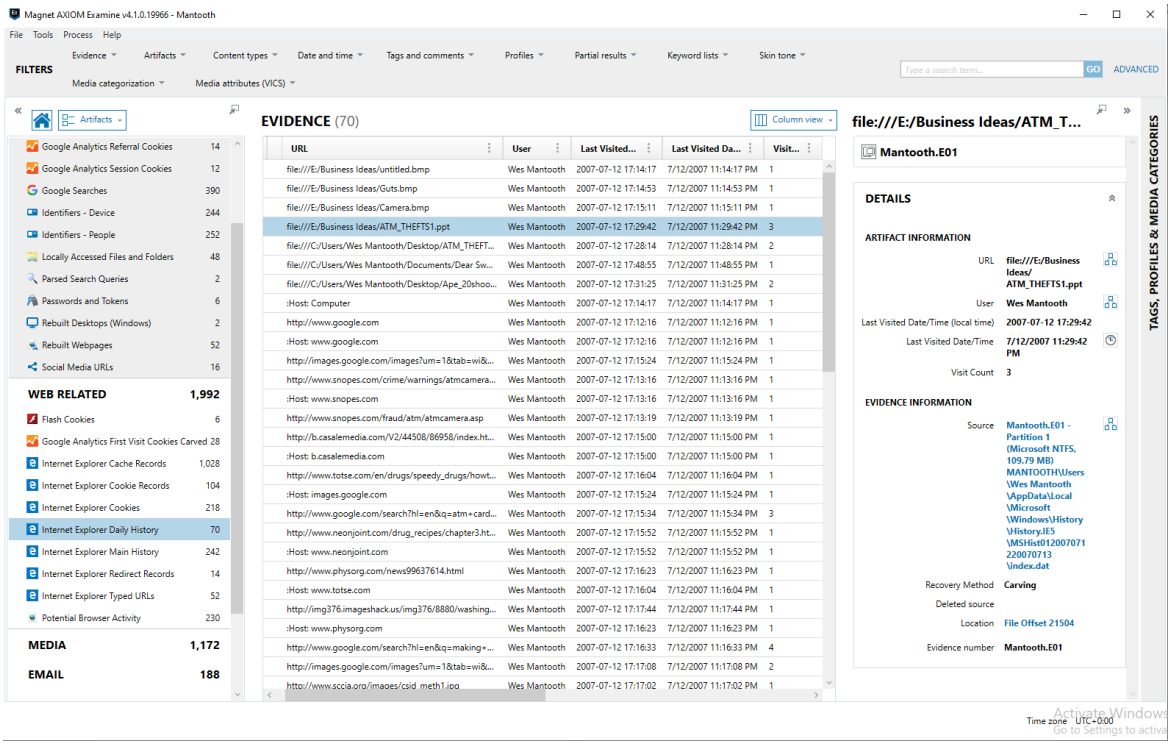

Figure 3.3

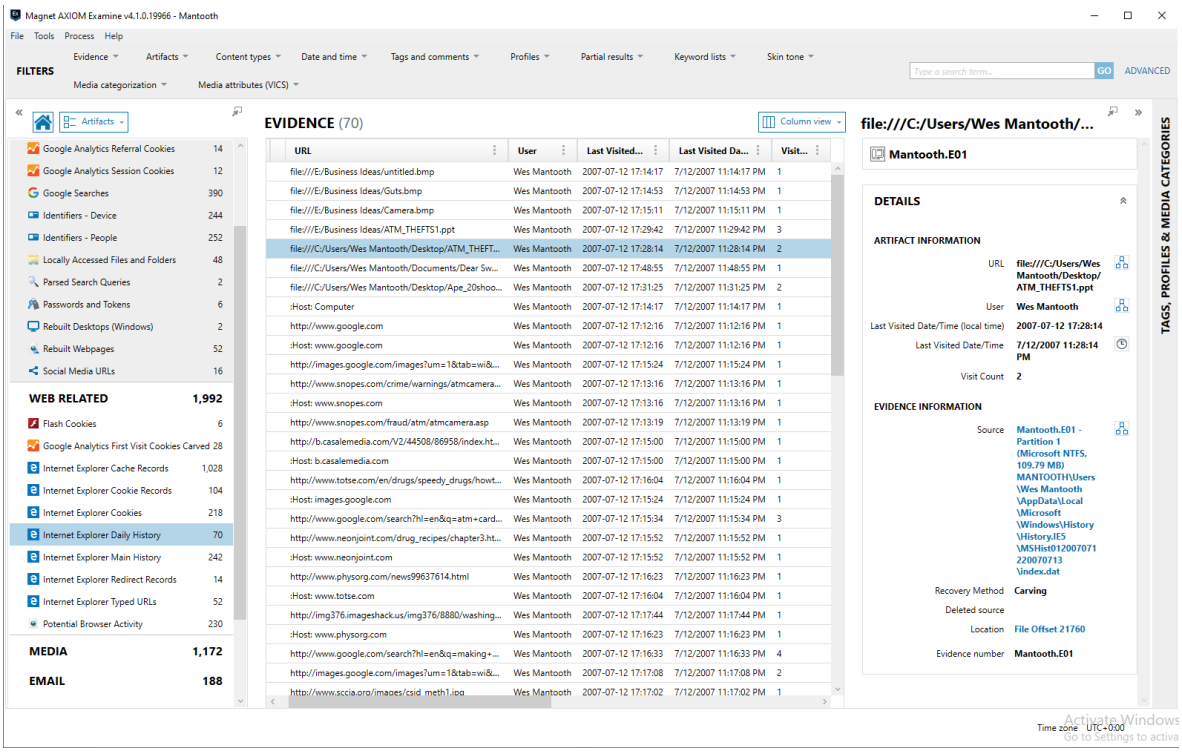

Figure 3.4

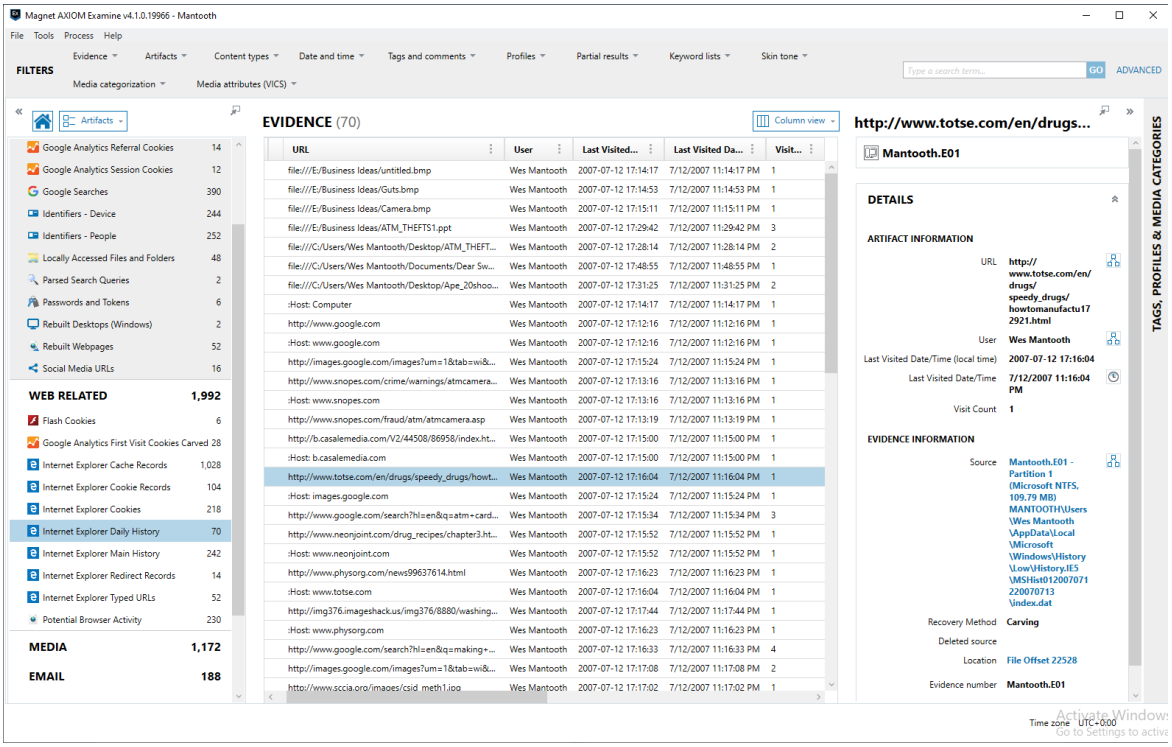

Figure 3.5

Media.

Photos.

All photos found on this device related to the web search history, along with any other possible illegal activities. This contains images of credit card information, atm stealing, drugs, meth labs, pills, various suspicious photos, and other illegal activities and substances. Figures 3.6 - 7.5 show these images.

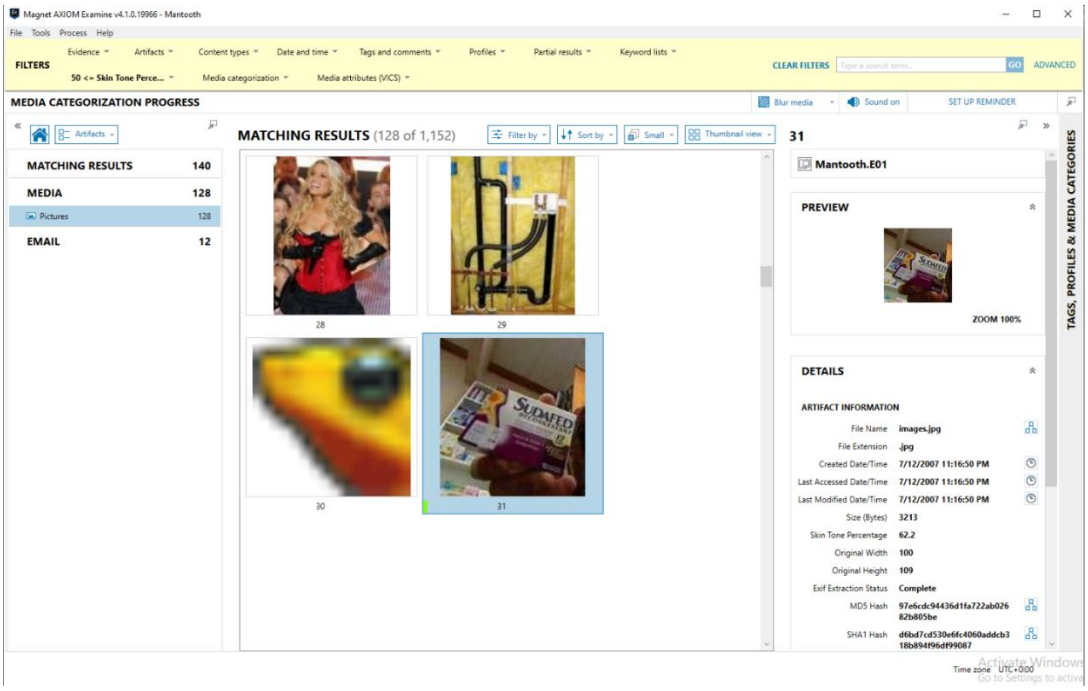

Figure 3.6

Figure 3.6 shows Sudafed a known agent of making drugs.

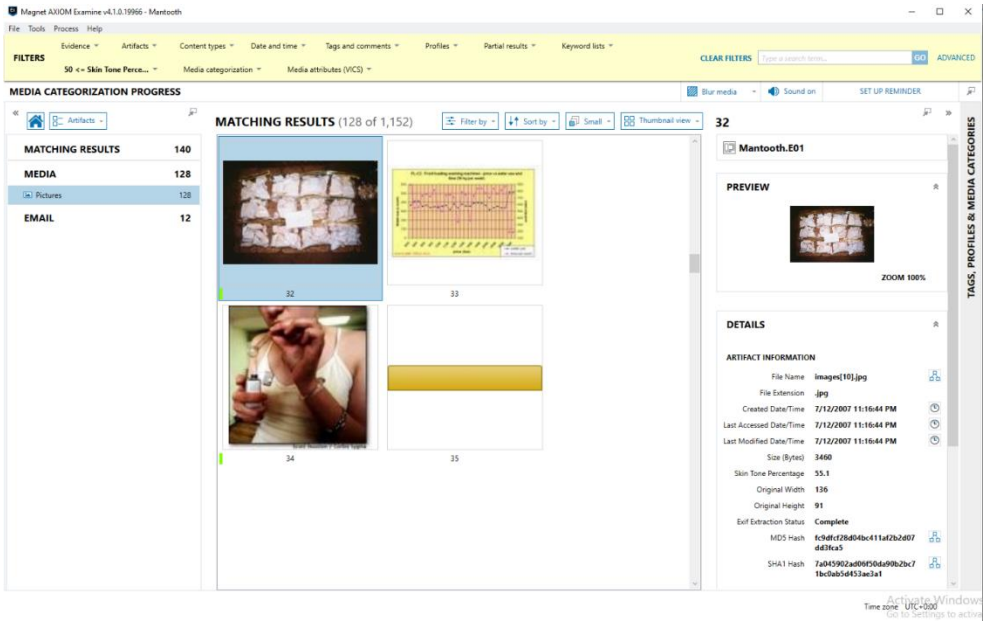

Figure 3.7

Figure 3.7 shows baggies of what appears to be meth.

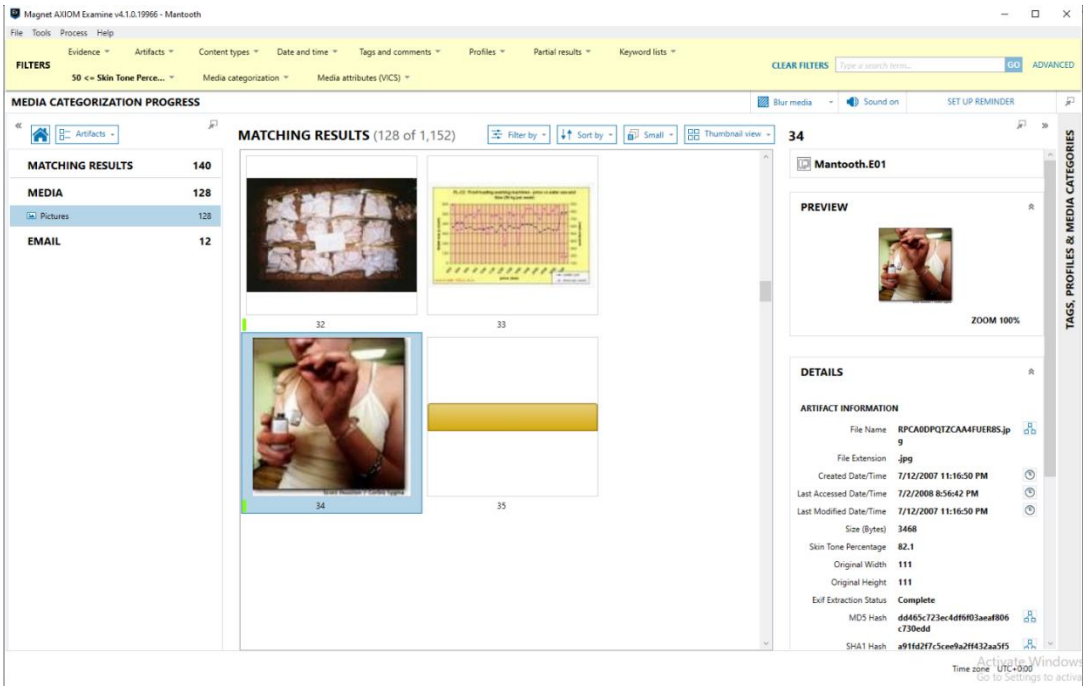

Figure 3.8

Figure 3.8 appears to be a man smoking an illegal substance out of a pipe.

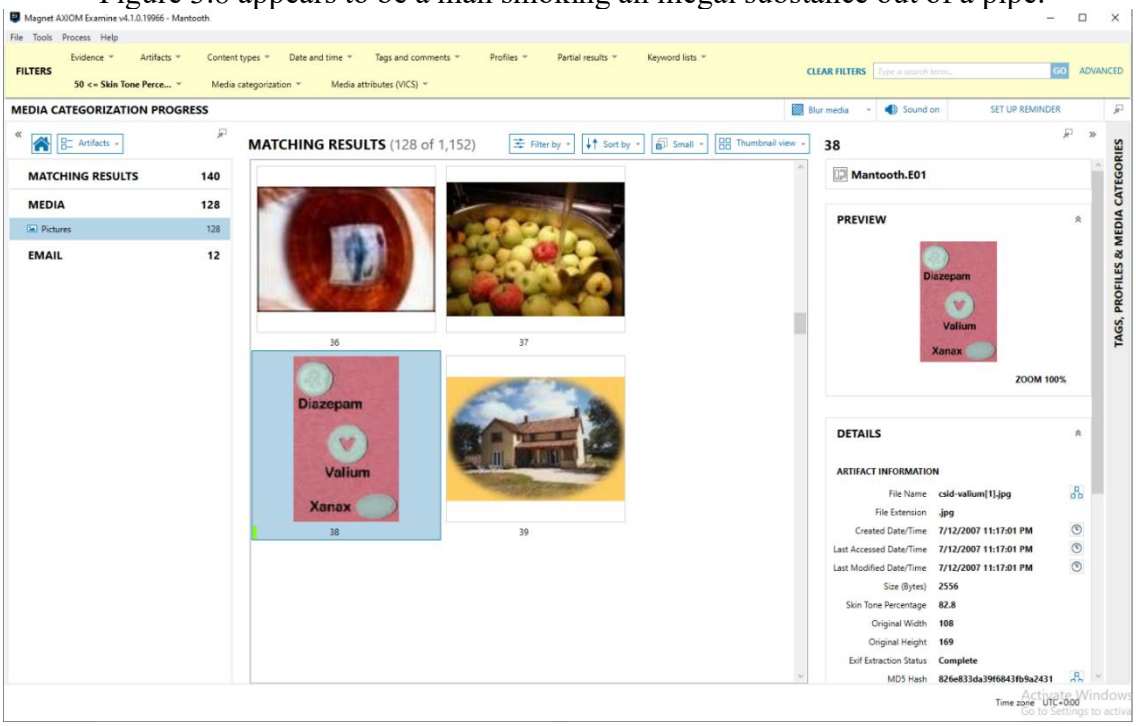

Figure 3.9

Figure 3.9 has various pills that are labeled.

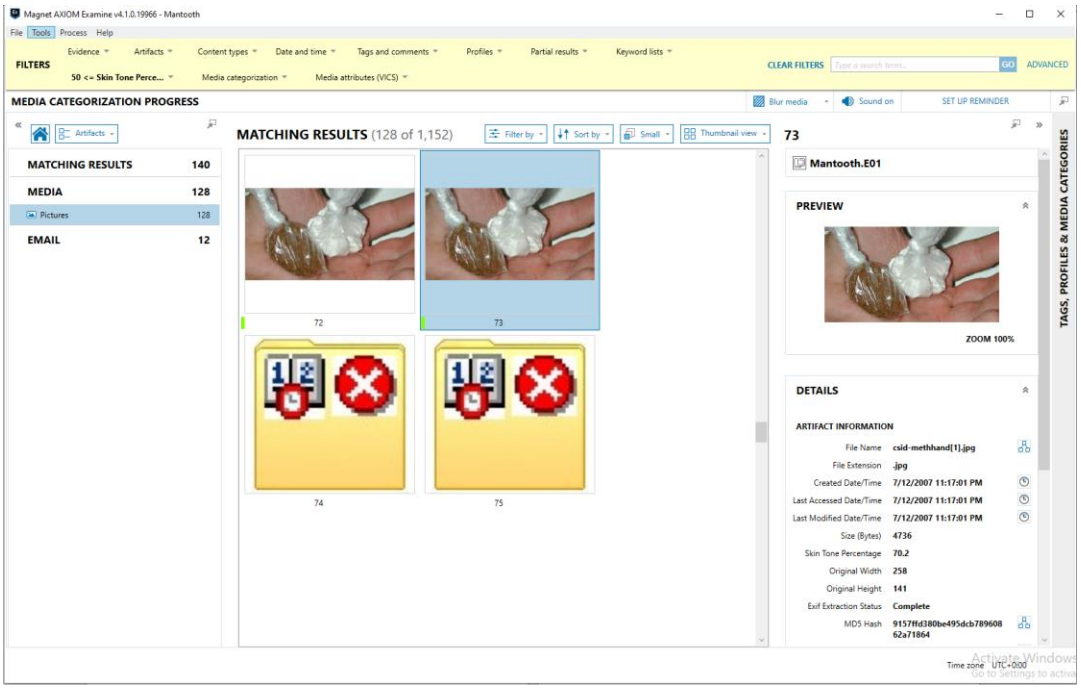

Figure 4.0

Figure 4.0 contains an image of small baggies of drugs.

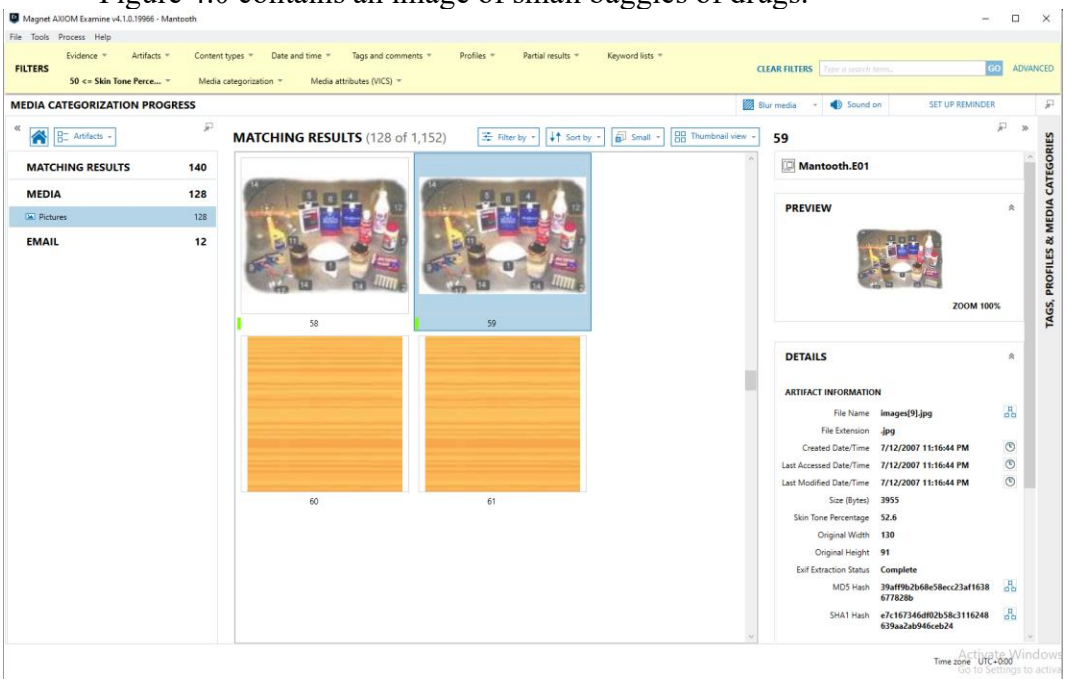

Figure 4.1

Figure 4.1 contains an image of ingredients and equipment for producing meth

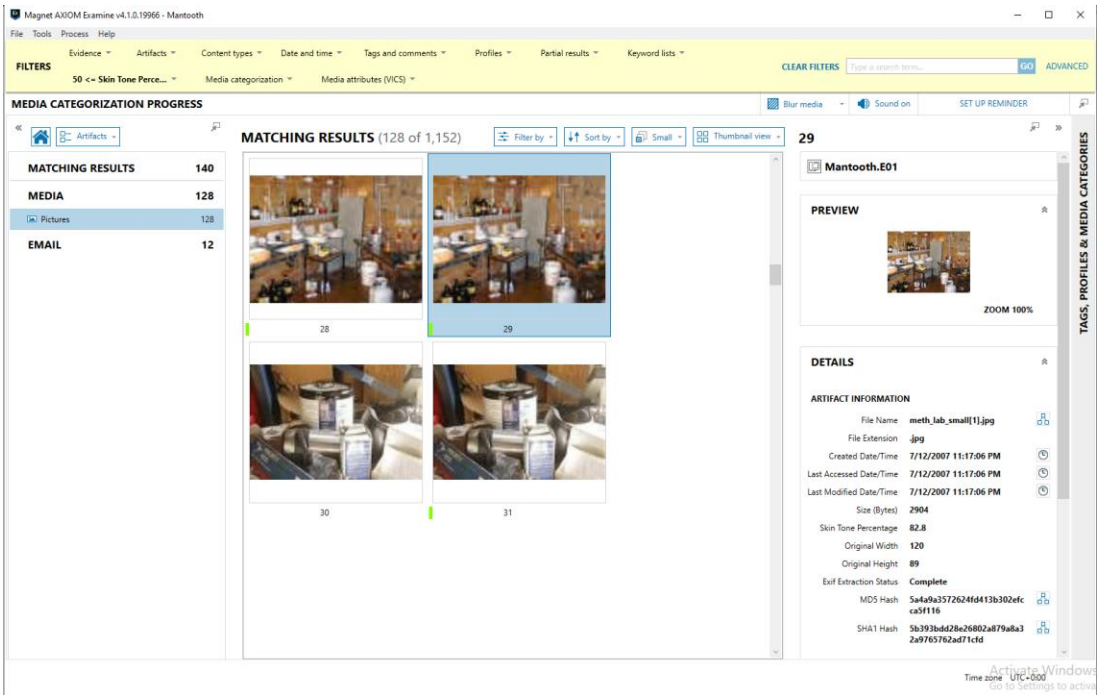

Figure 4.2

Figure 4.2 contains an image of a meth lab.

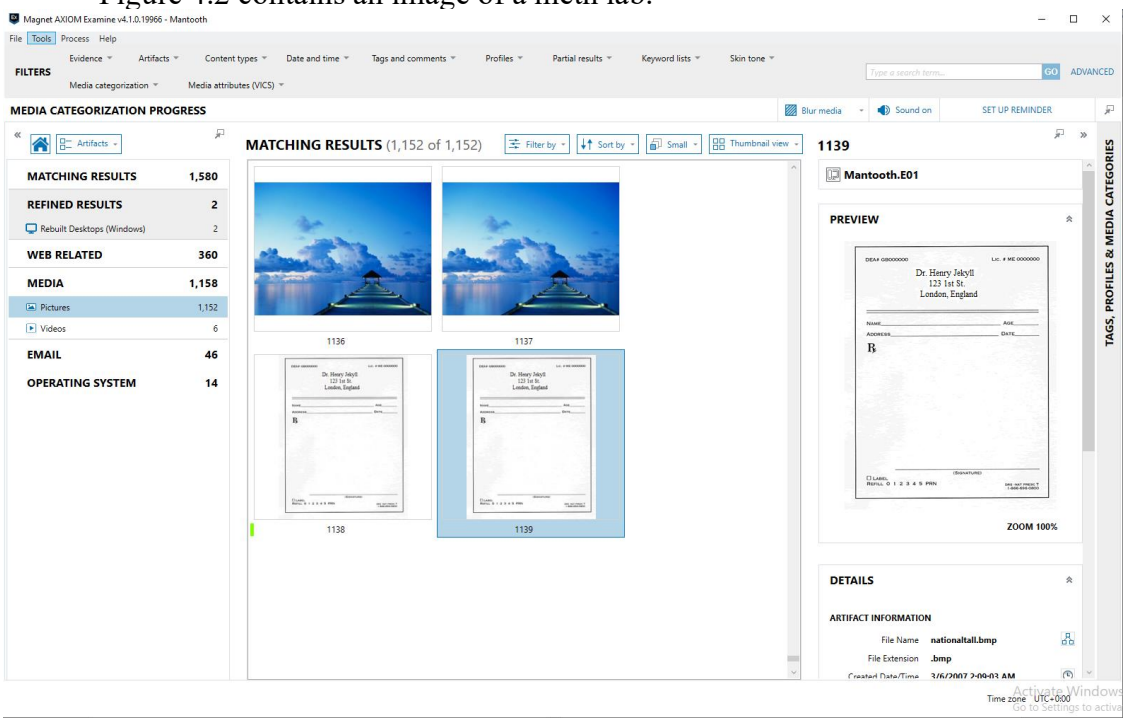

Figure 4.3

Figure 4.3 contains a forged templete for a doctor's pharmacuetical note.

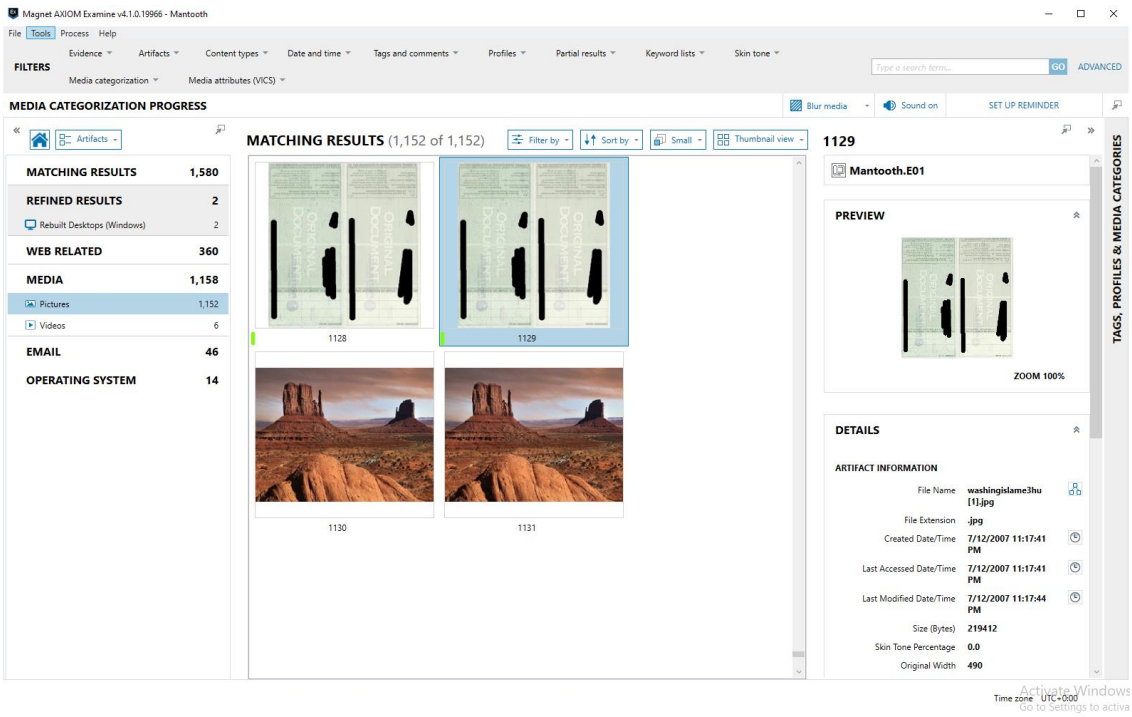

Figure 4.4

Figure 4.4 contains an image of check washing

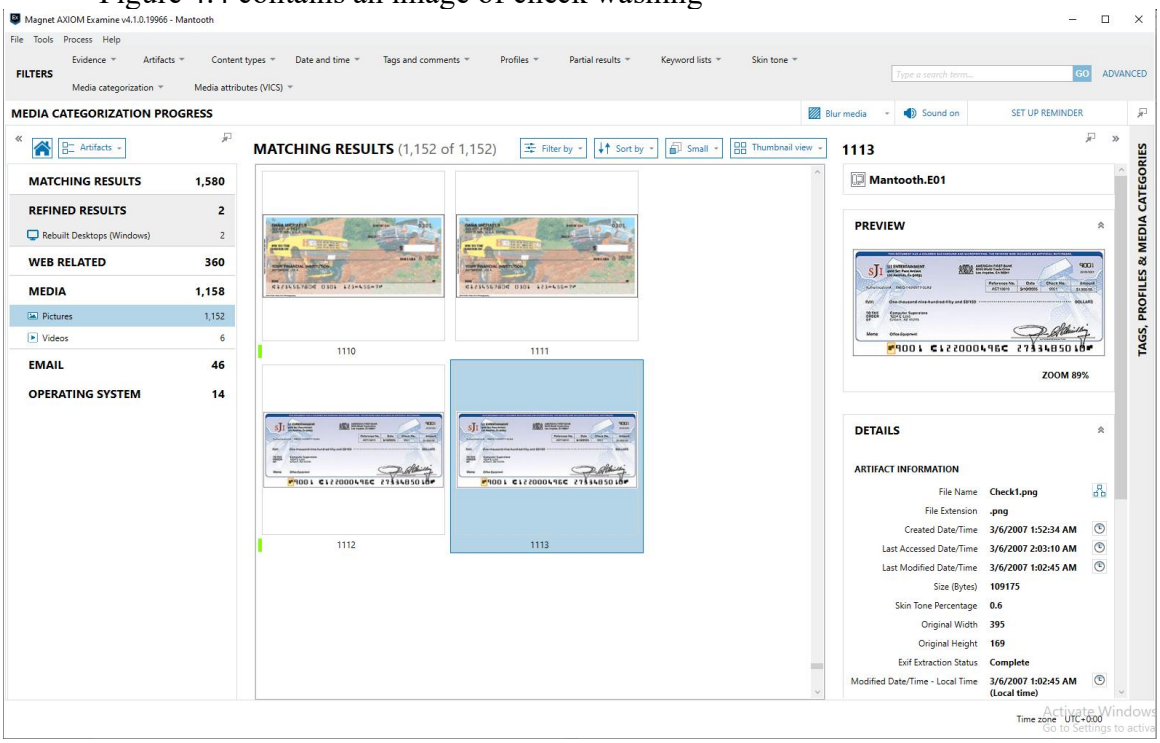

Figure 4.5

Figure 4.5 contains a cashier's check.

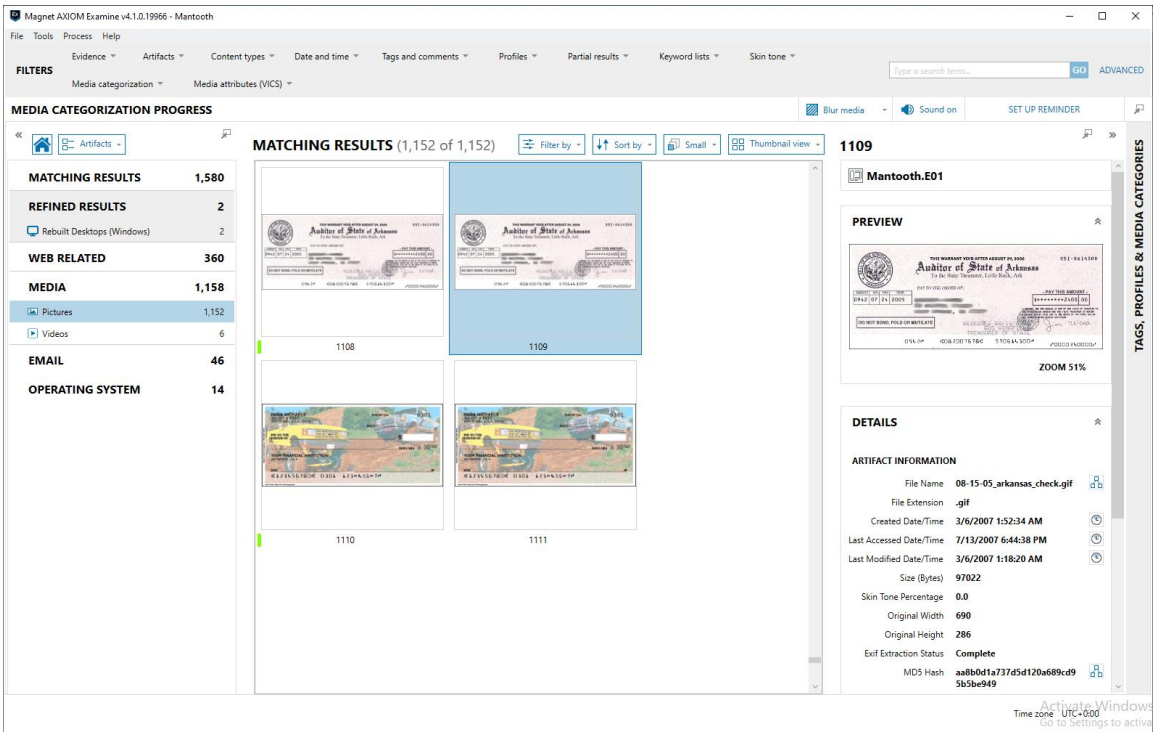

Figure 4.6

Figure 4.6 contains a cashier's check

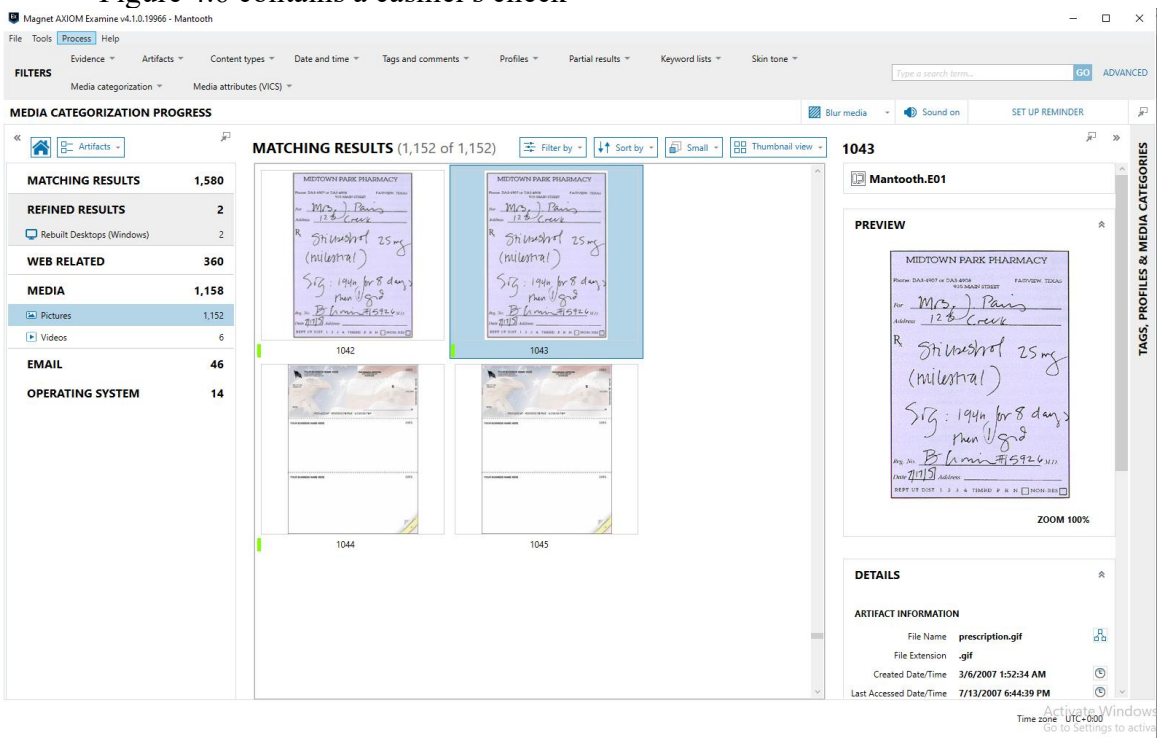

Figure 4.7

Figure 4.7 contains a forged doctors note with a prescription.

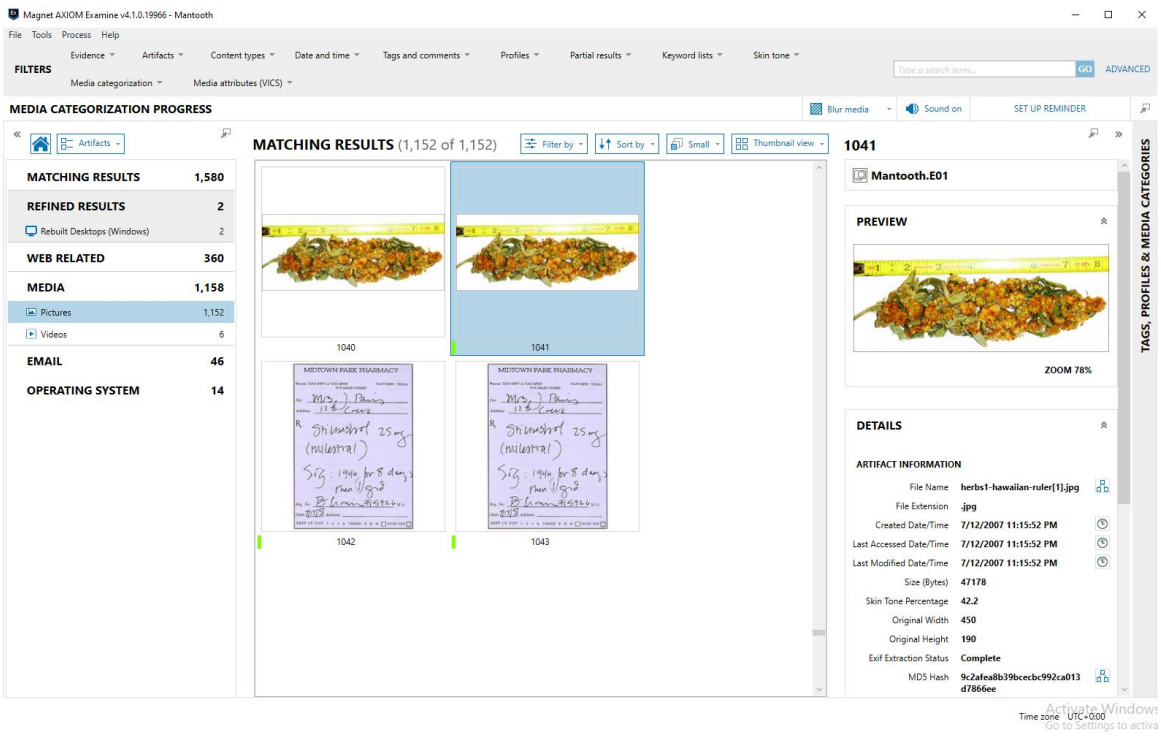

Figure 4.8

Figure 4.8 contains an image of a drug known as Hawaiian ruler.

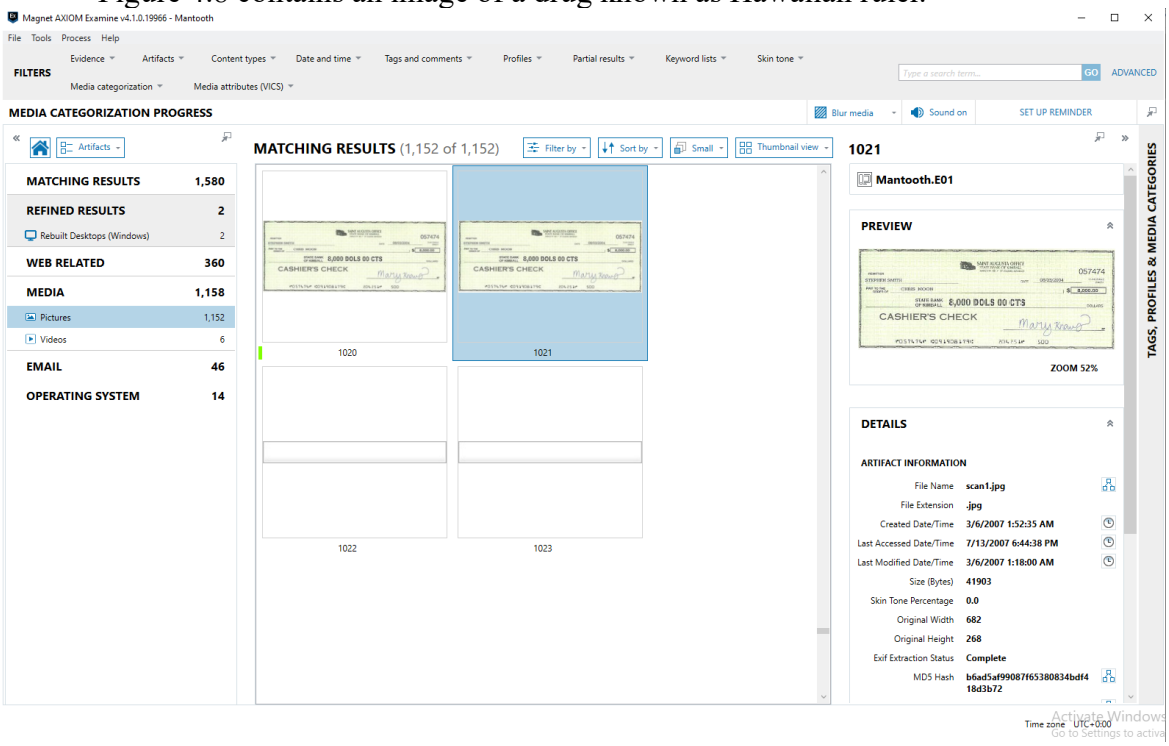

Figure 4.9

Figure 4.9 contains a cashier's check.

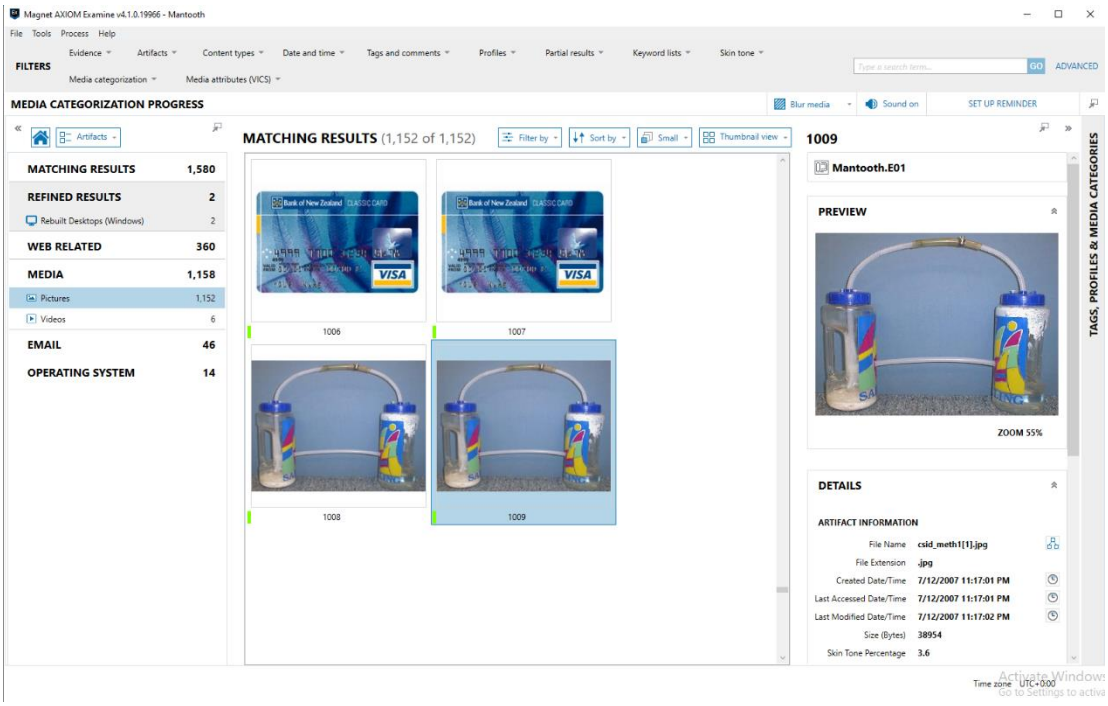

Figure 5.0

Figure 5.0 contains an image of equipment for meth production

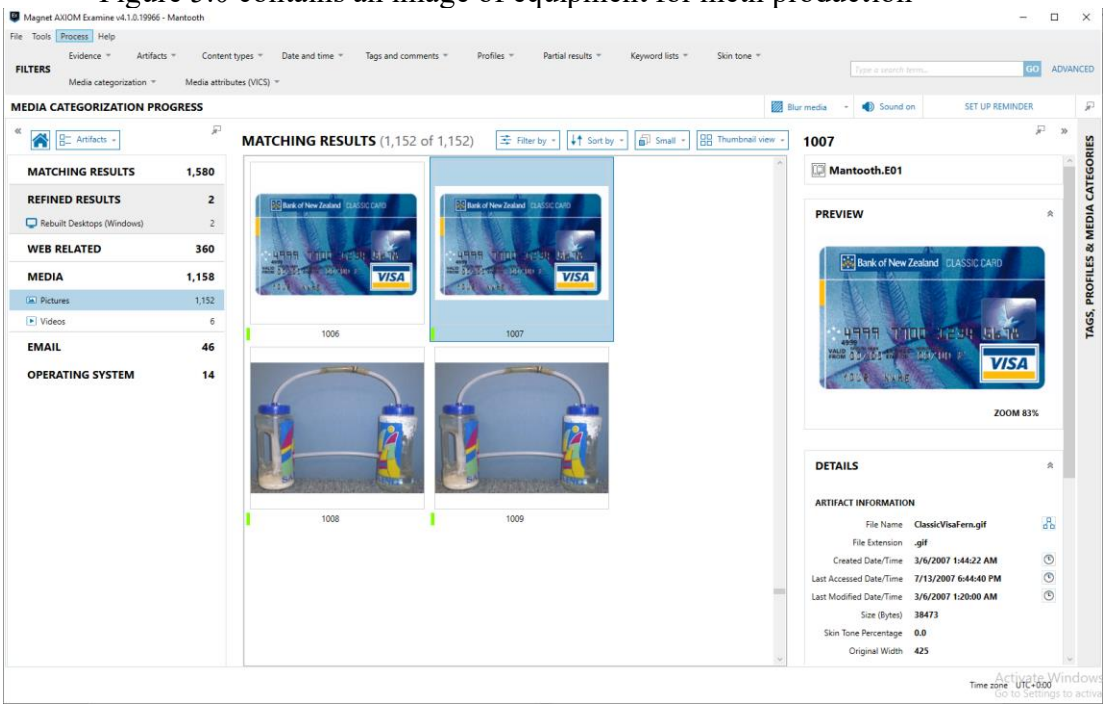

Figure 5.1

Figure 5.1 contains an image of a credit card, most likely stolen.

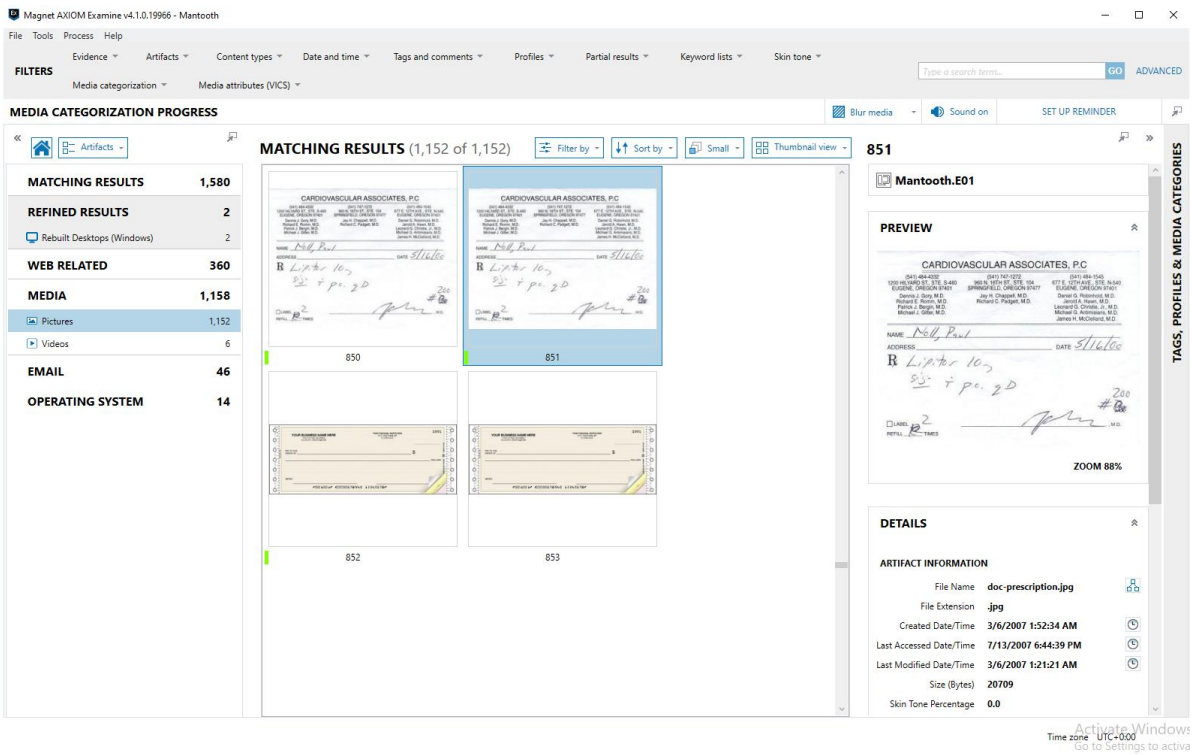

Figure 5.2

Figure 5.2 contains a forged doctor's note for a percription.

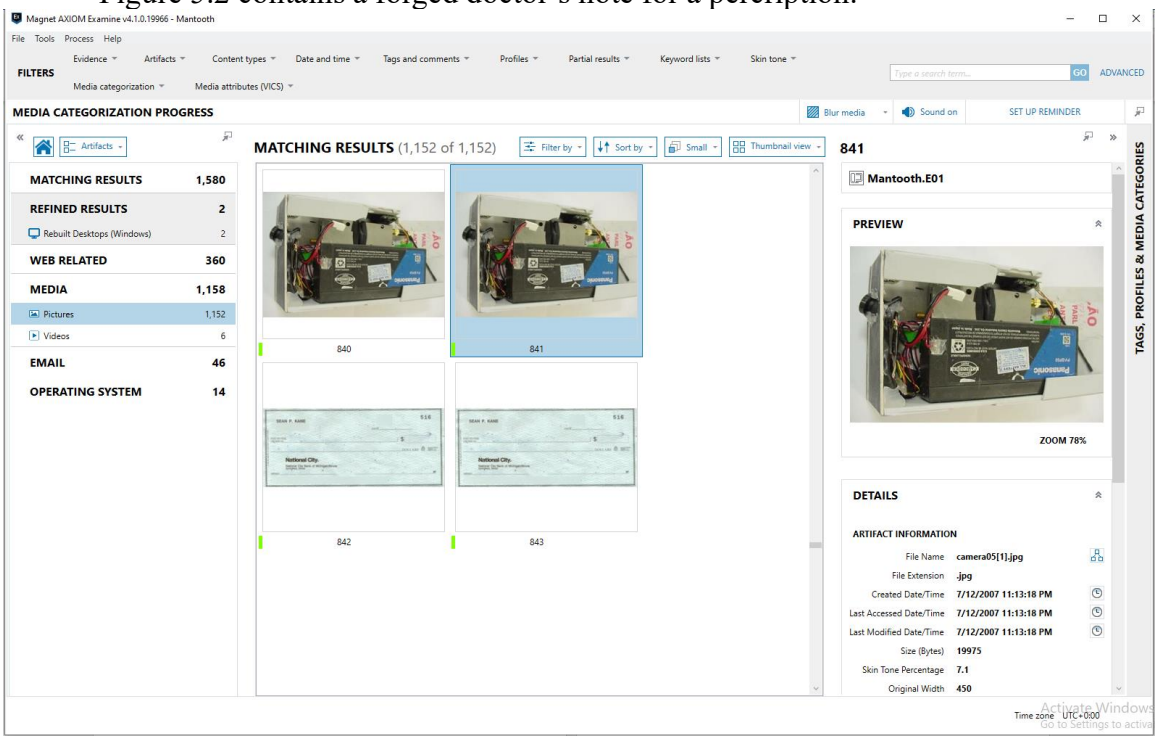

Figure 5.3

Figure 5.3 contains a photo of the inside of an atm machine.

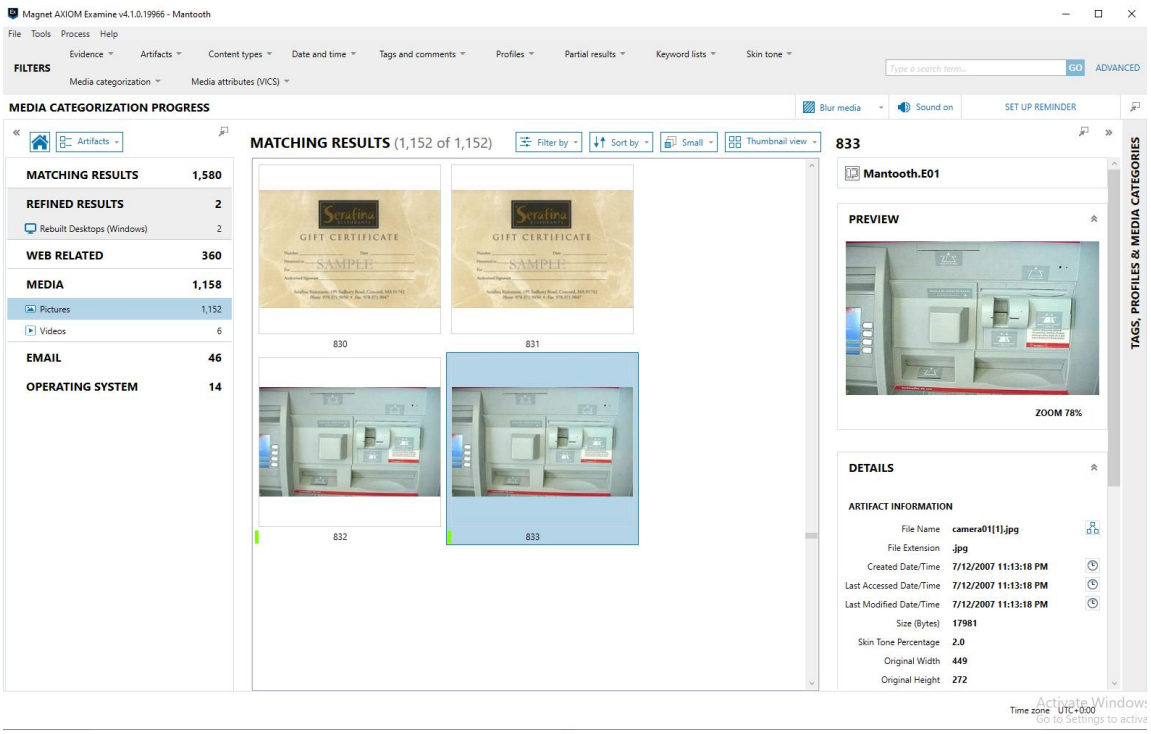

Figure 5.4

Figure 5.4 contains a picture of the outside of an atm machine.

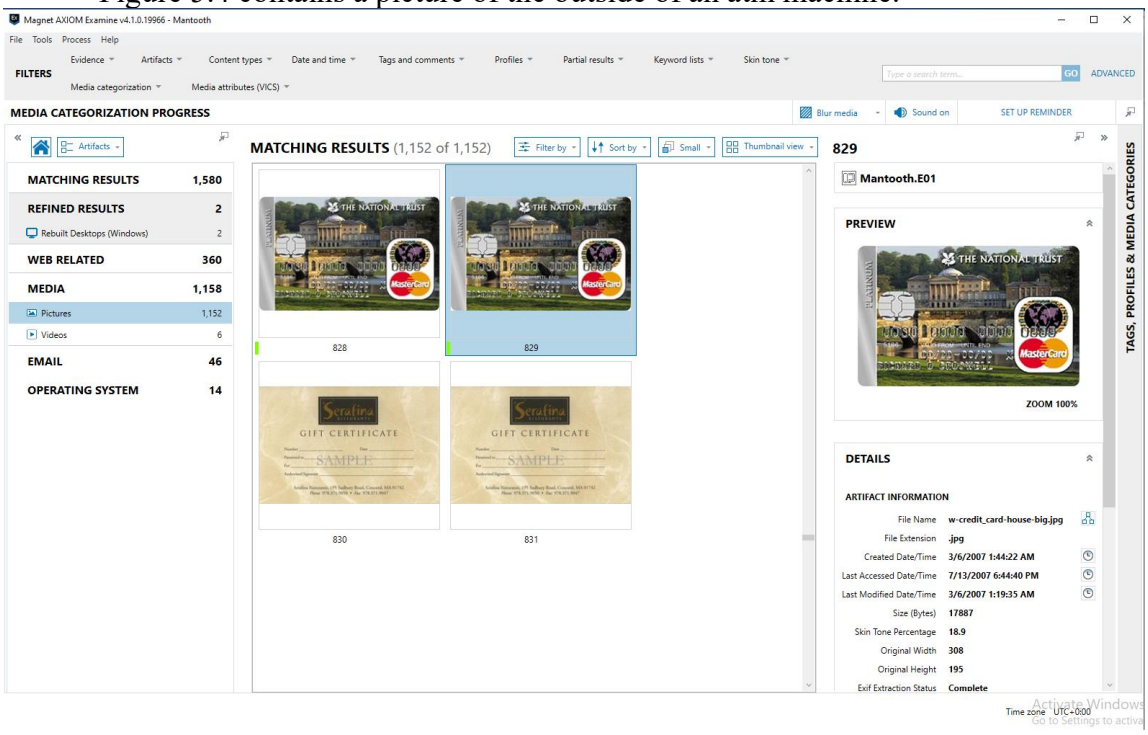

Figure 5.5

Figure 5.5 contains a picture of a fradulent credit card.

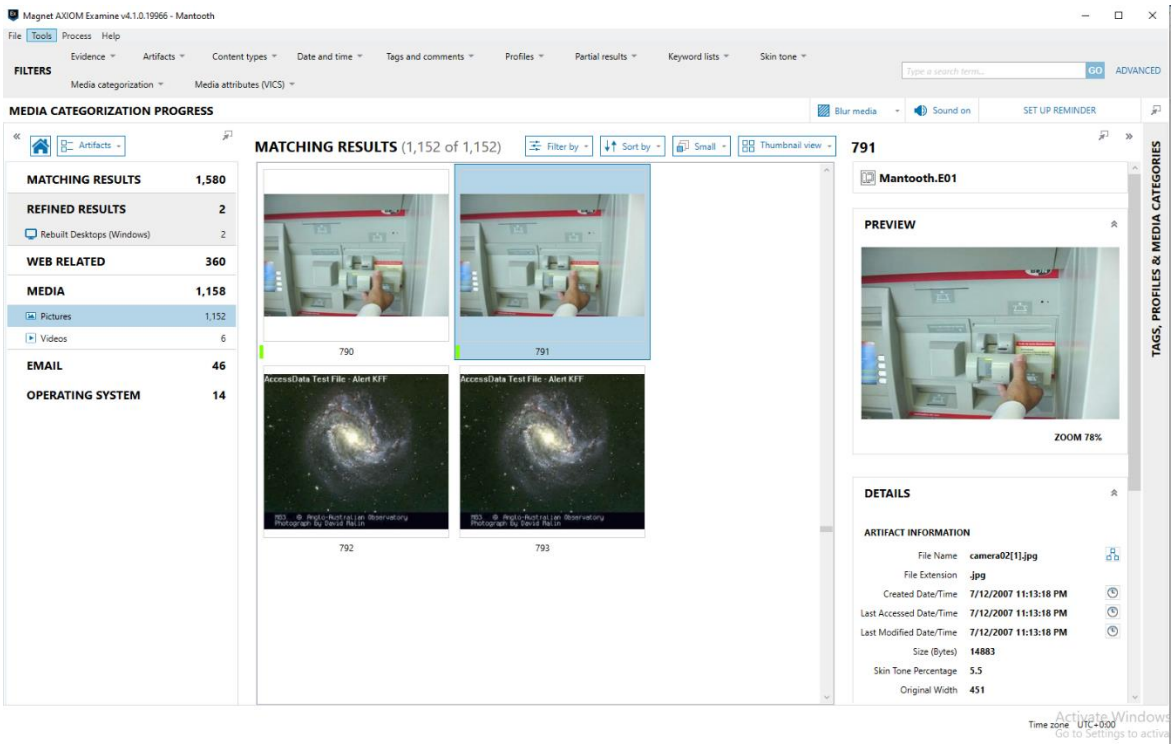

Figure 5.6

Figure 5.6 contains an image of an atm machine

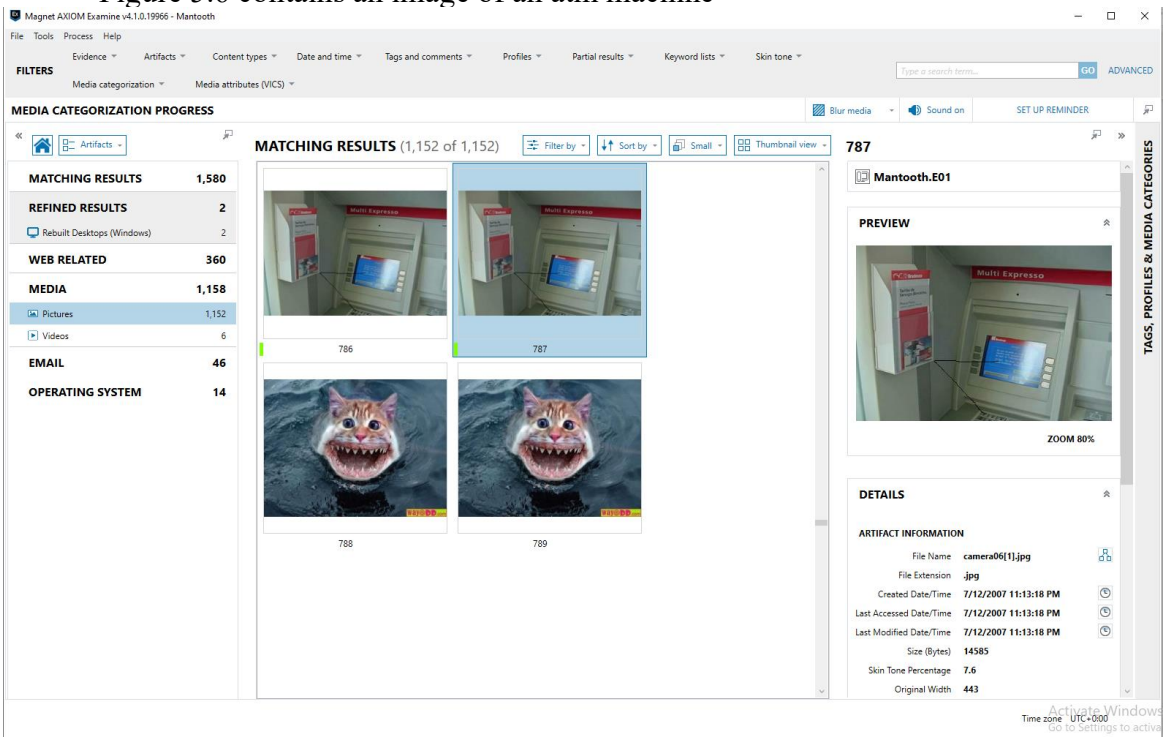

Figure 5.7

Figure 5.8 contains a picture of an atm machine.

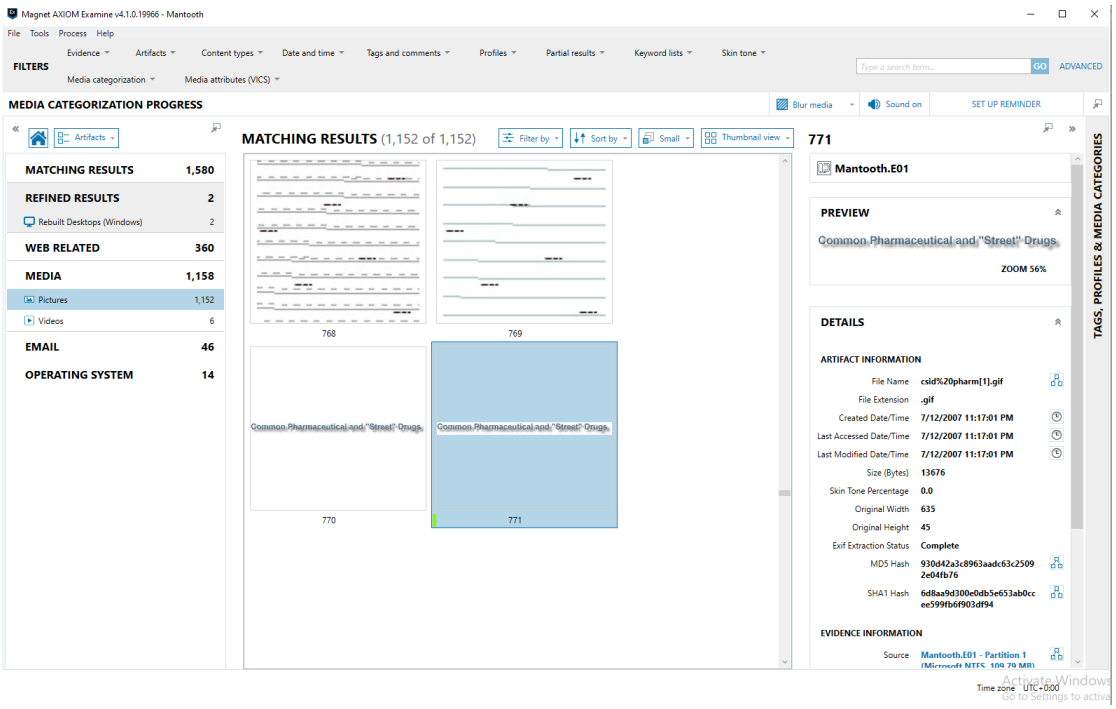

Figure 5.8

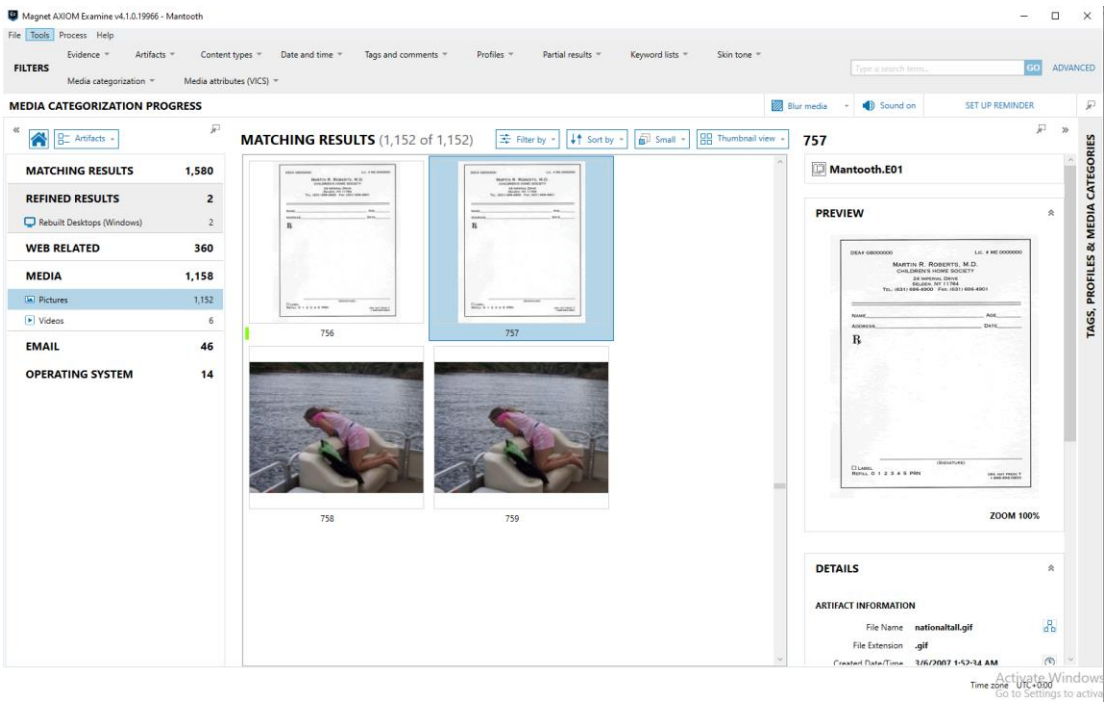

Figure 5.9

Figure 5.9 contains an image of a forged doctor's note template.

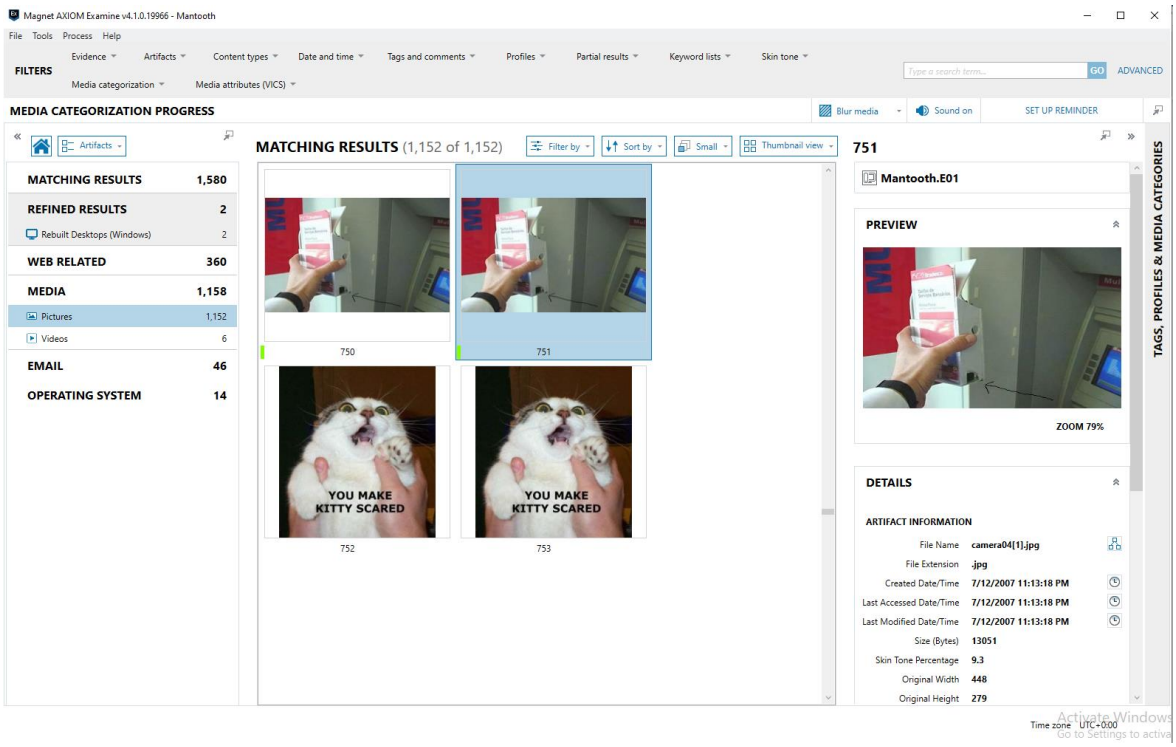

Figure 6.0

Figure 6.0 contains a picture of an atm machine being hacked.

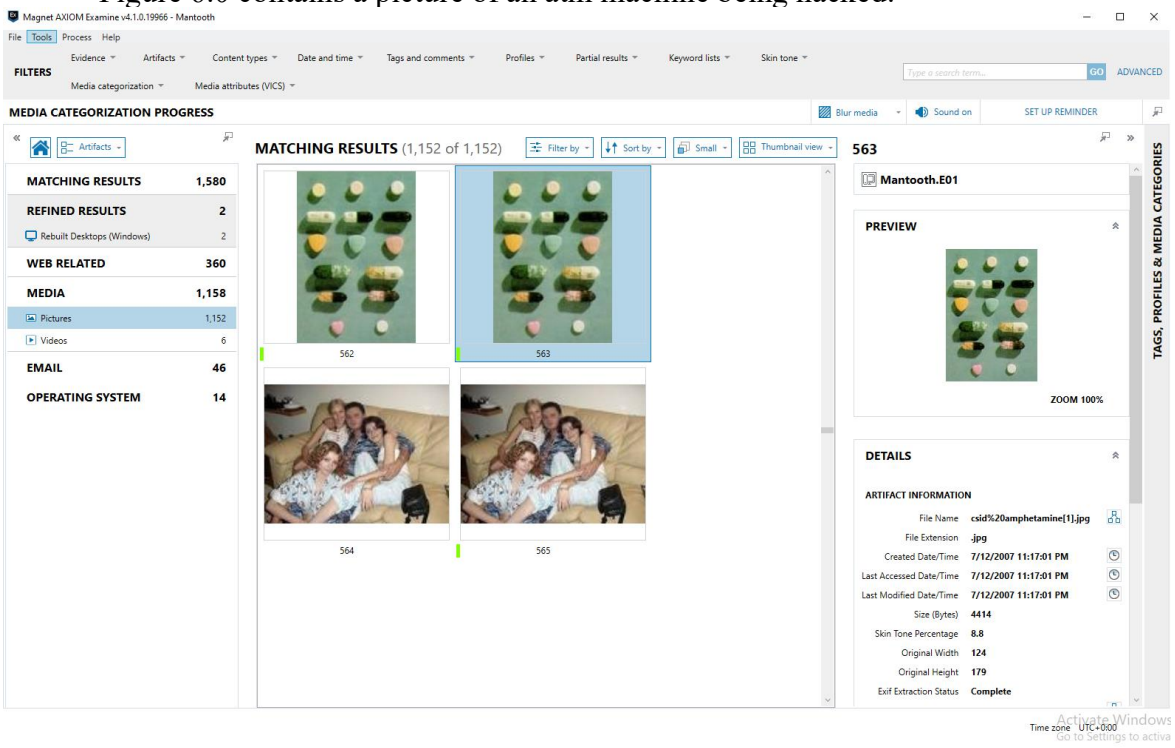

Figure 6.1

Figure 6.1 contains a picture of various pills.

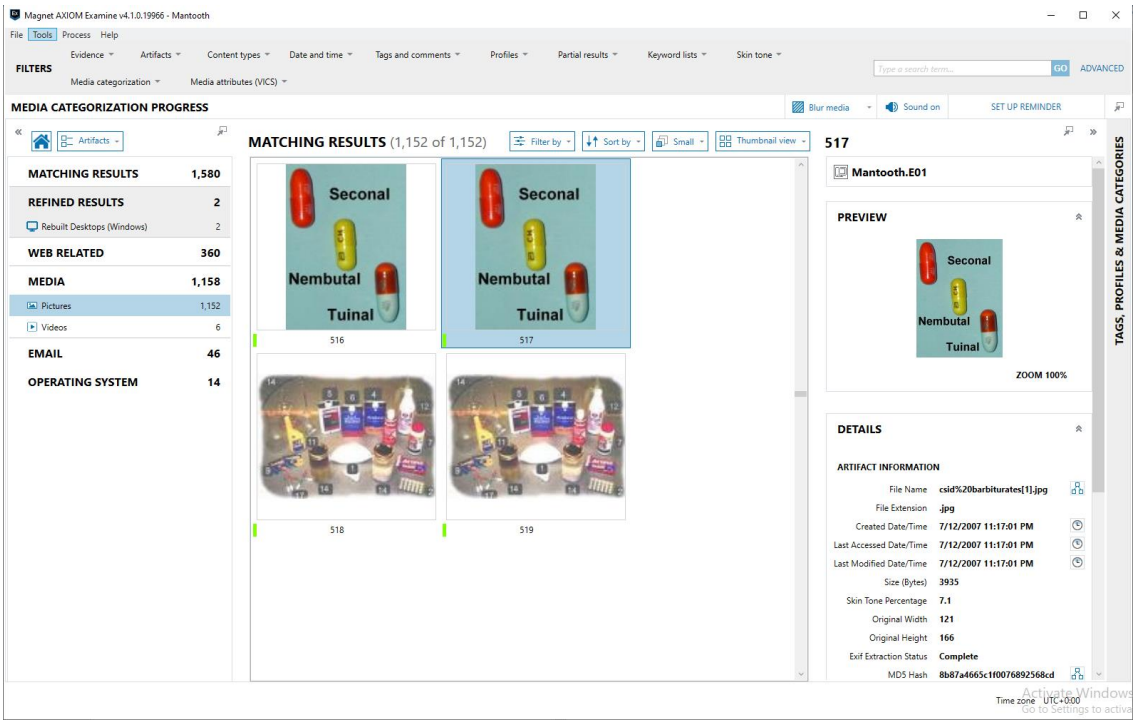

Figure 6.2

Figure 6.2 contains an image of labeled various pills such as Seconal.

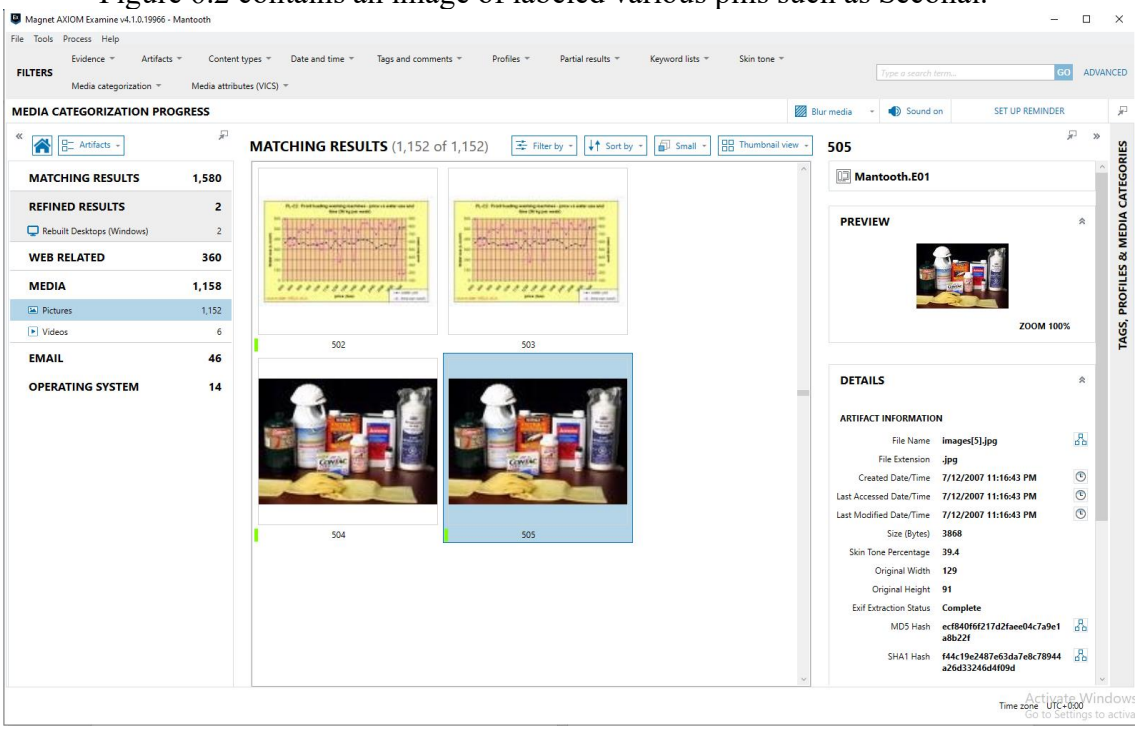

Figure 6.3

Figure 6.3 contains an image of various items needed to make meth.

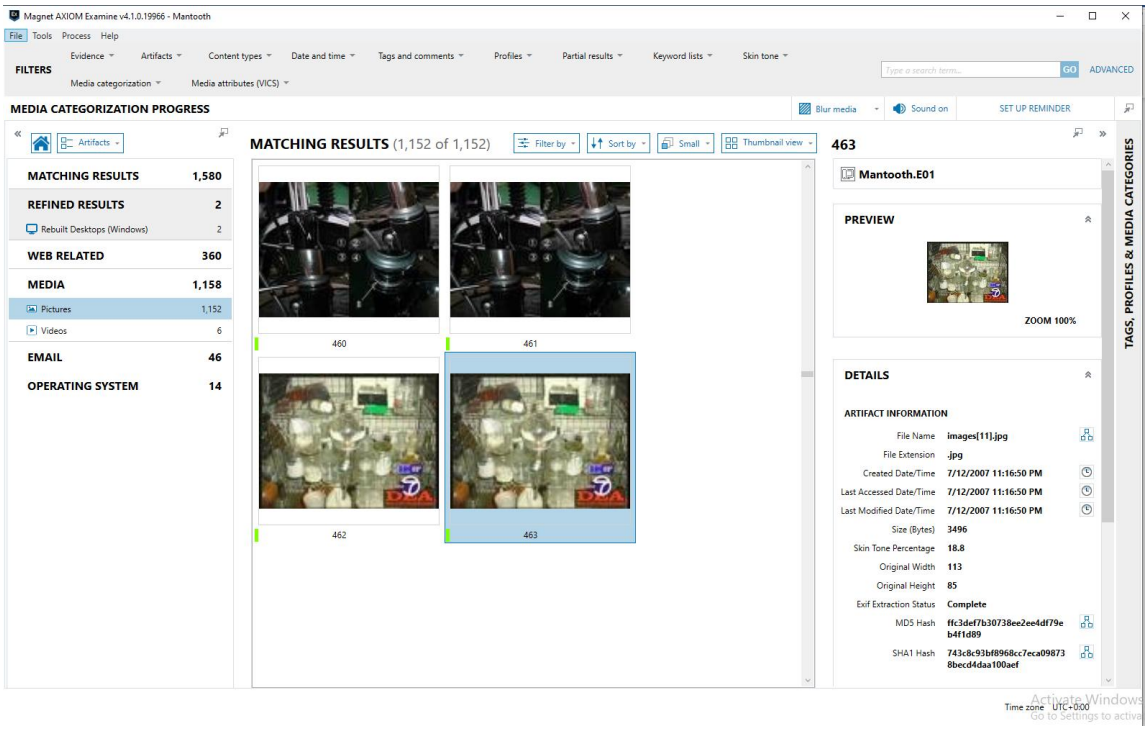

Figure 6.4

Figure 6.4 contains an image of various meth related processes.

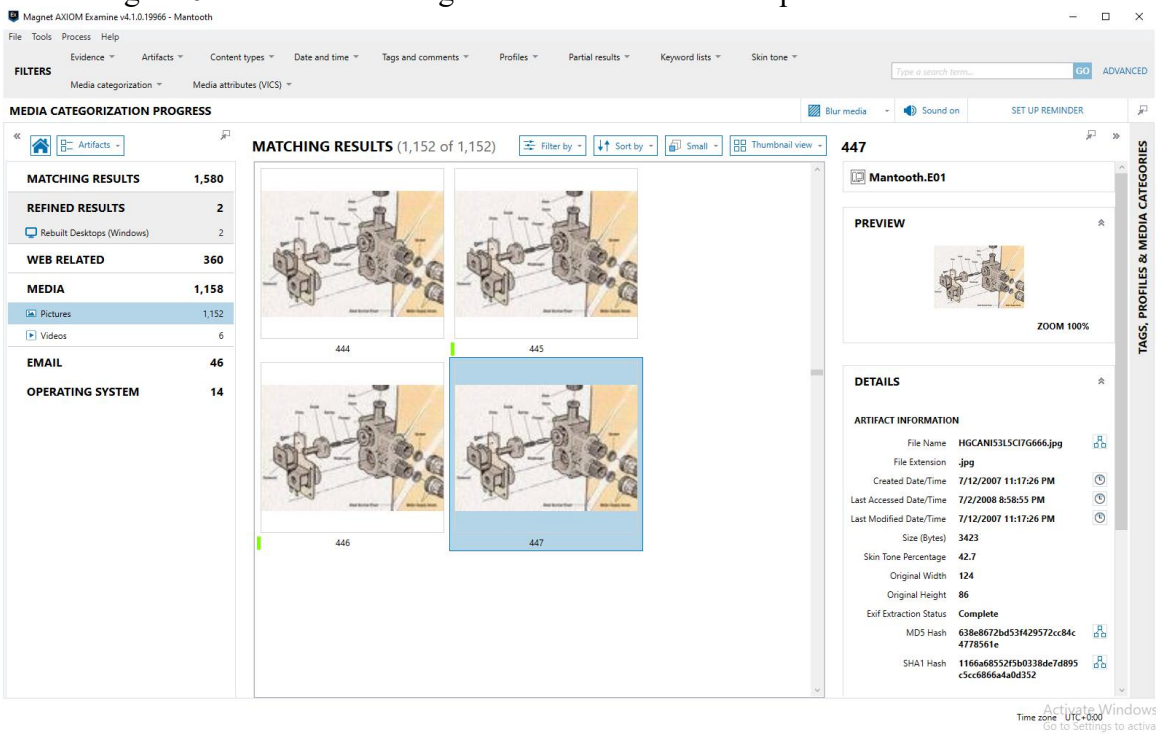

Figure 6.5

Figure 6.5 contains an image of the locking mechanism within an atm machine.

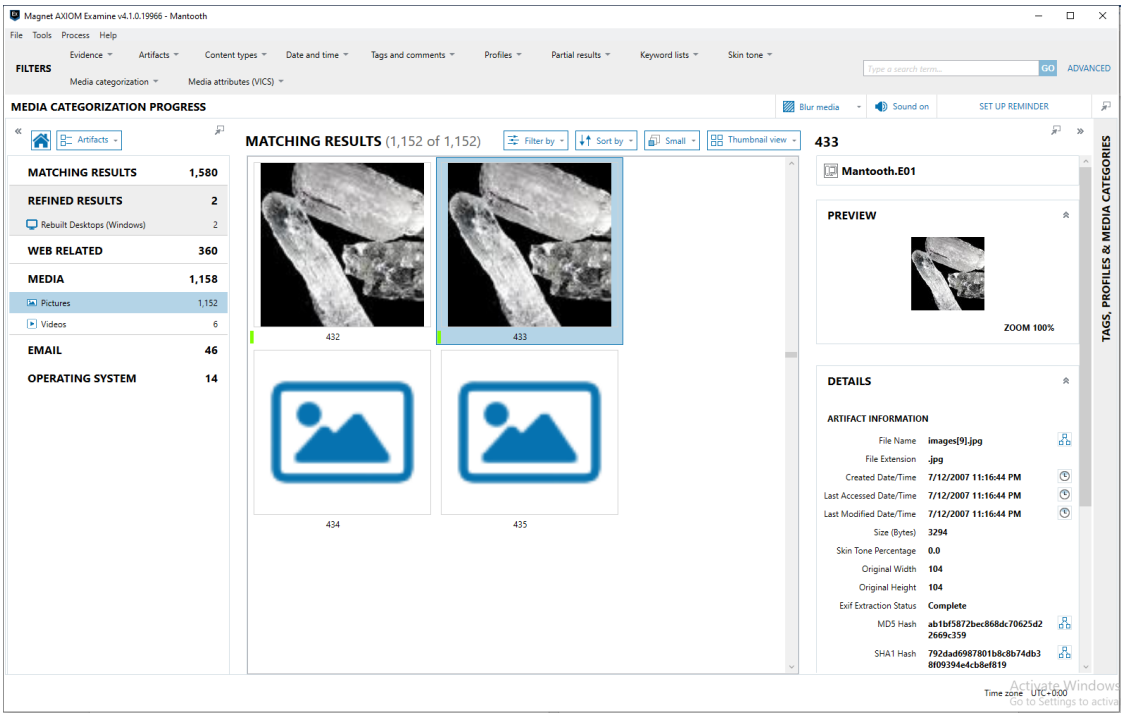

Figure 6.6

Figure 6.6 contains an image of a close-up photograph of meth crystals.

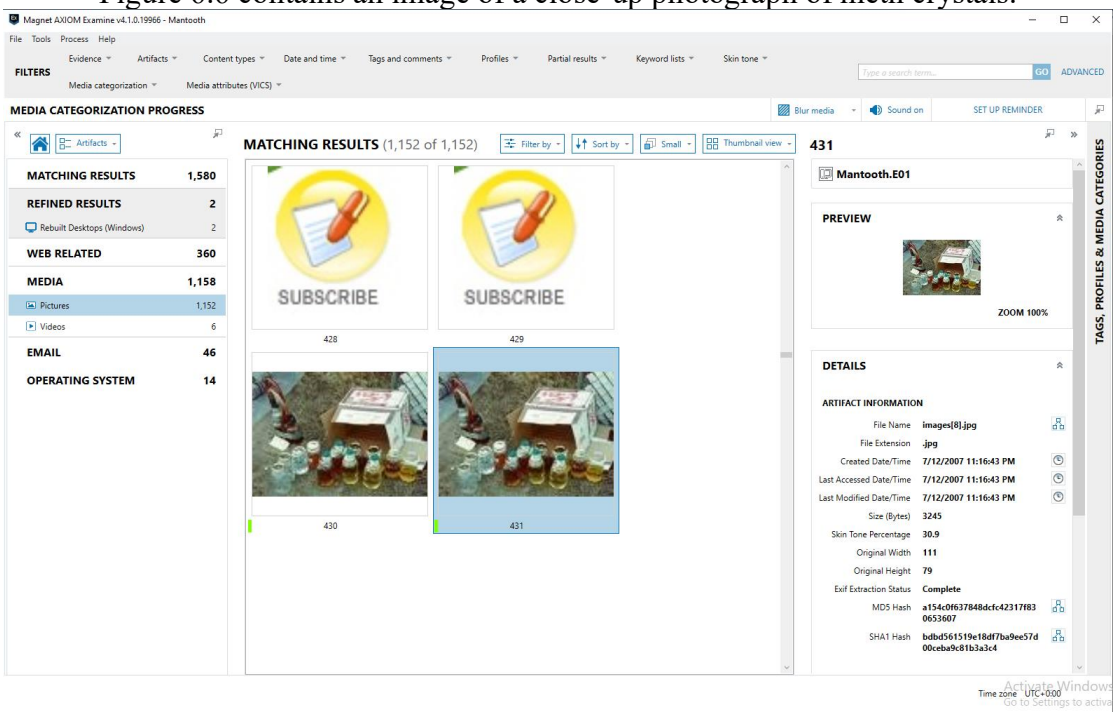

Figure 6.7

Figure 6.7 contains an image of meth production bottles.

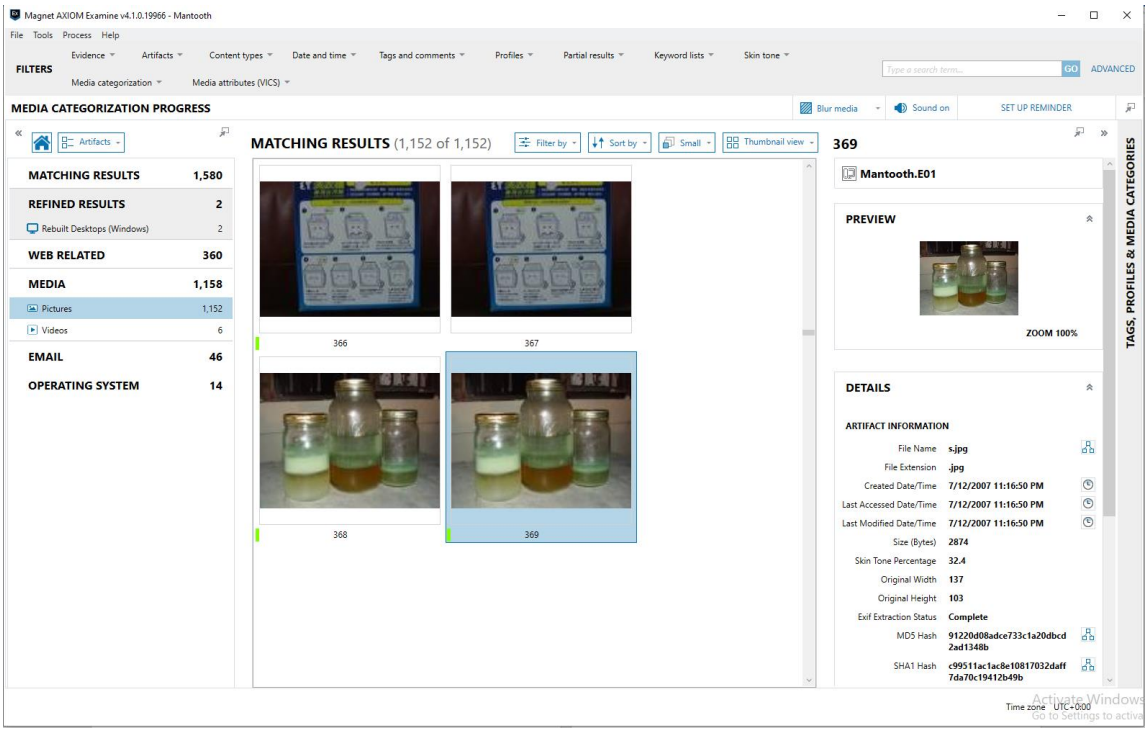

Figure 6.8

Figure 6.8 contains an image of meth bottles.

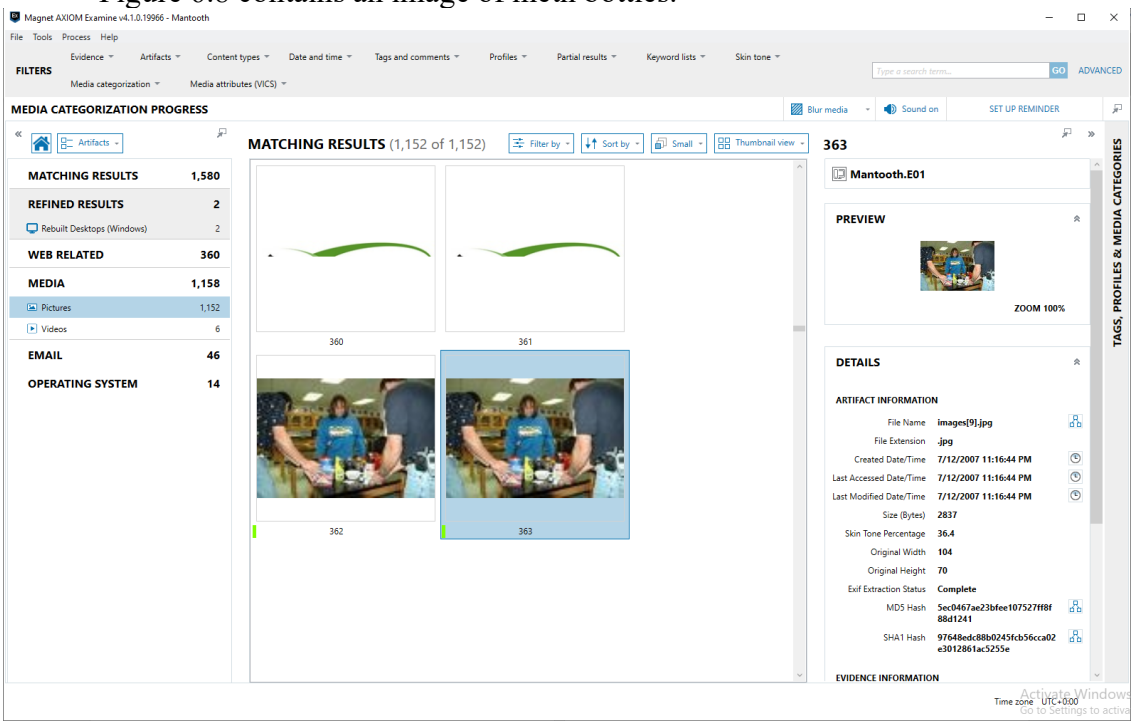

Figure 6.9

Figure 6.9 contains an image of teenagers or adults with drugs.

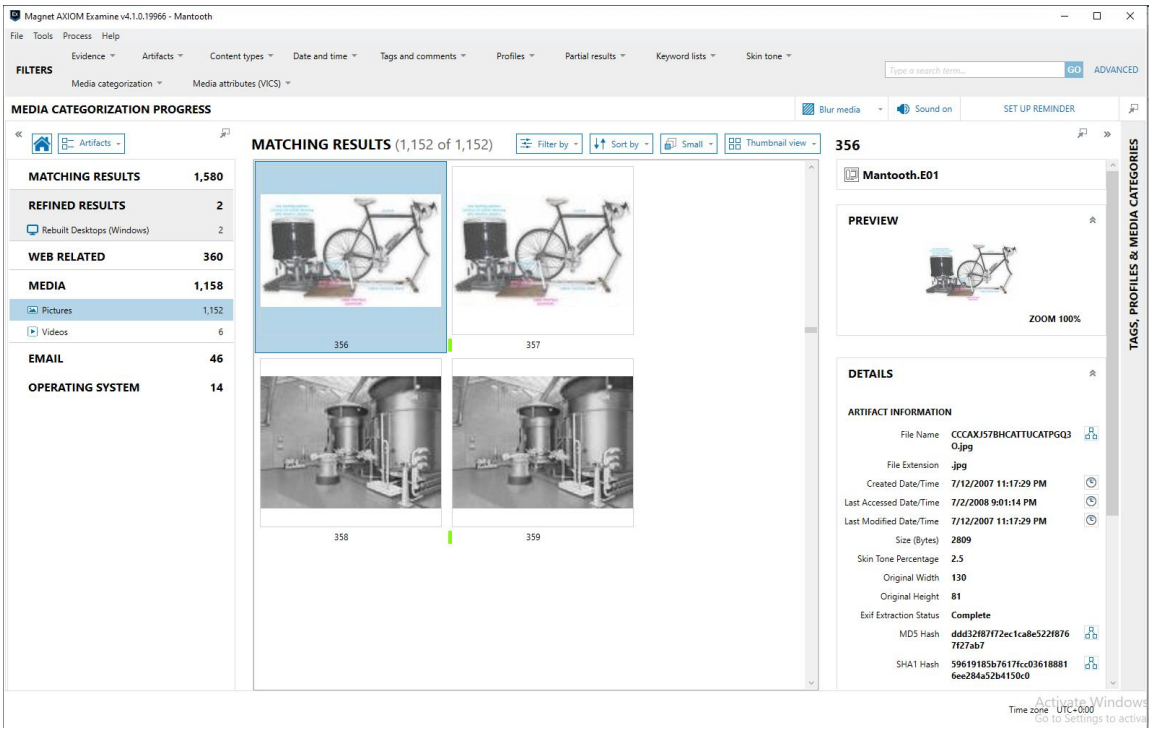

Figure 7.0

Figure 7.0 contains an image of a bike hooked up to a meth production station.

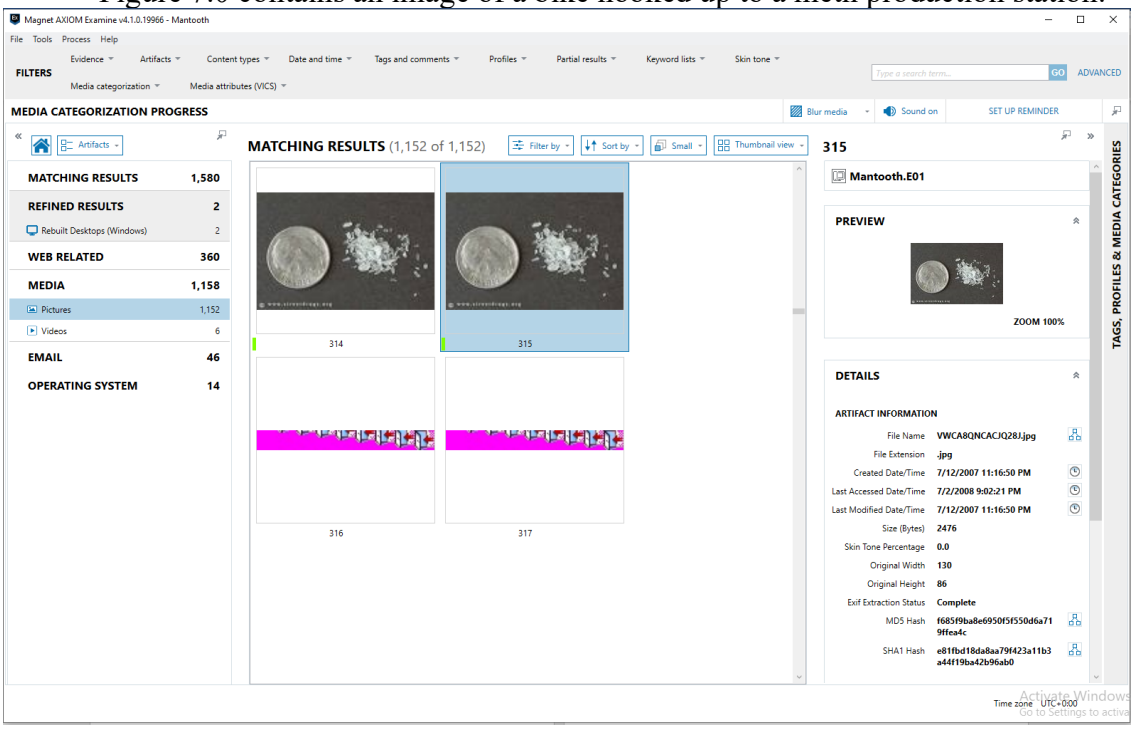

Figure 7.1

Figure 7.1 is an image of meth crystals nexted to a quarter for size comparison.

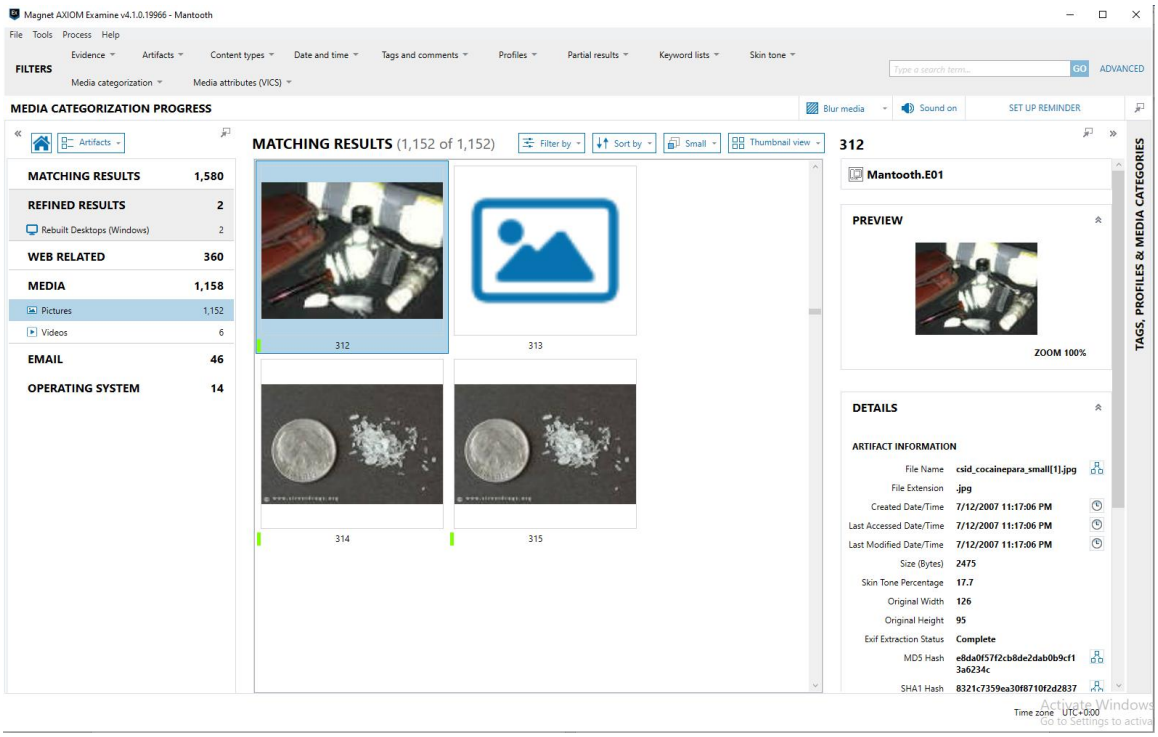

Figure 7.2

Figure 7.2 contains an image of meth ingredients.

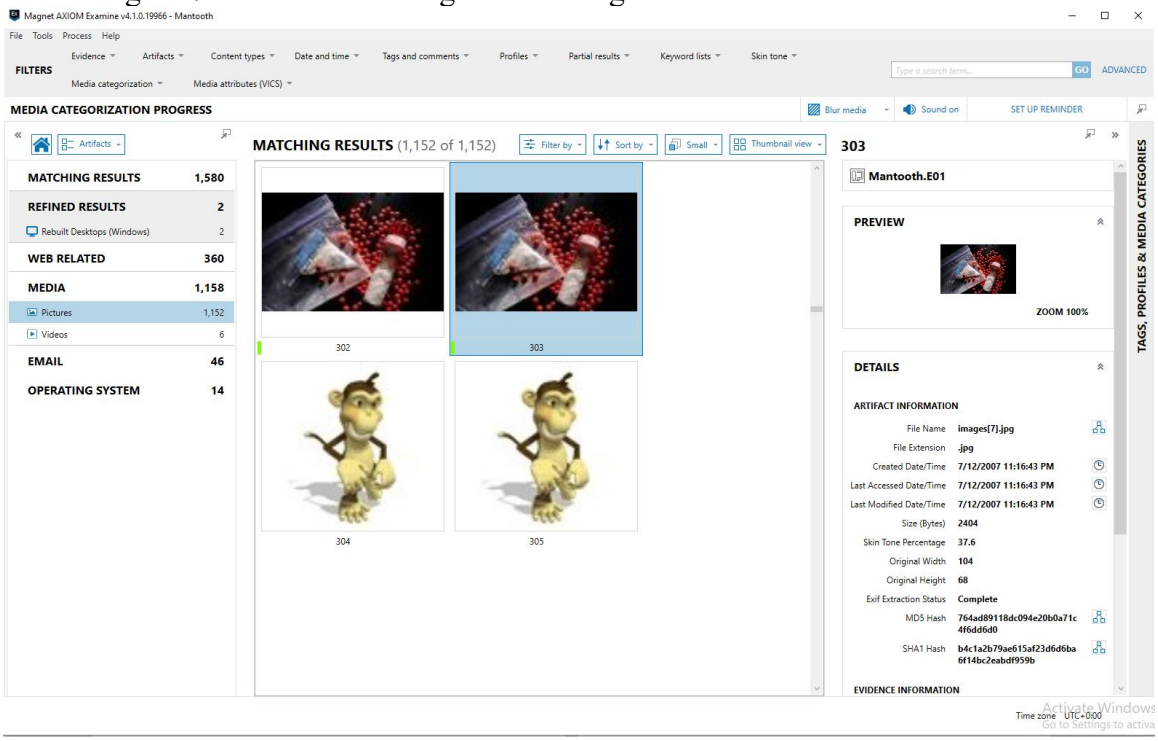

Figure 7.3

Figure 7.3 contains an image of pills.

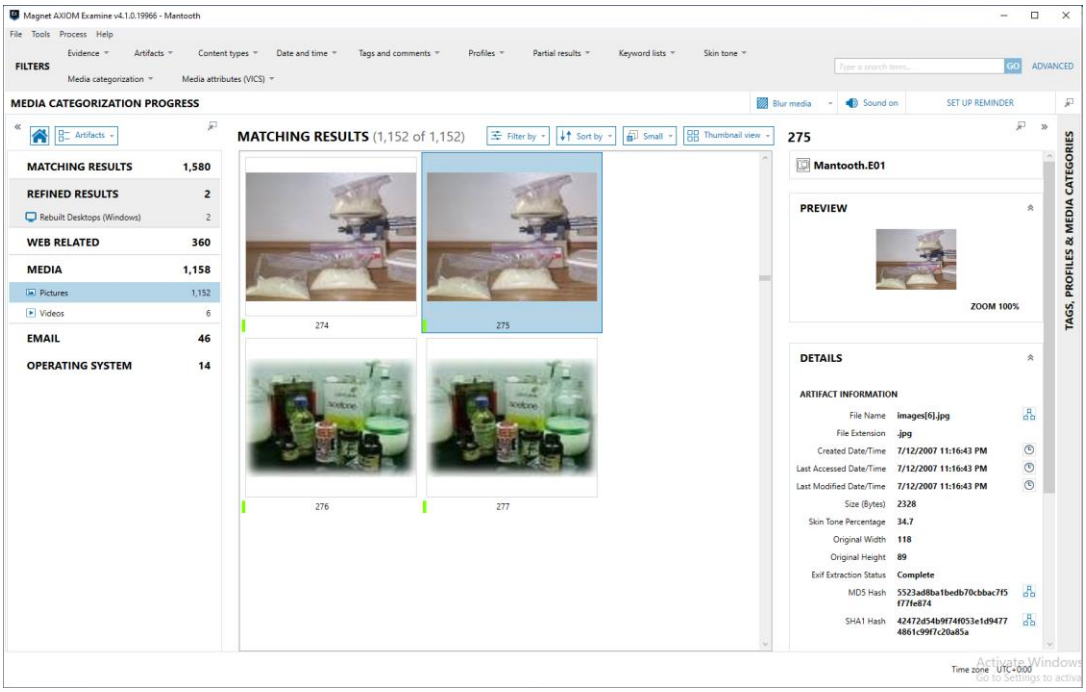

Figure 7.4

Figure 7.4 contains a weighing station for the meth.

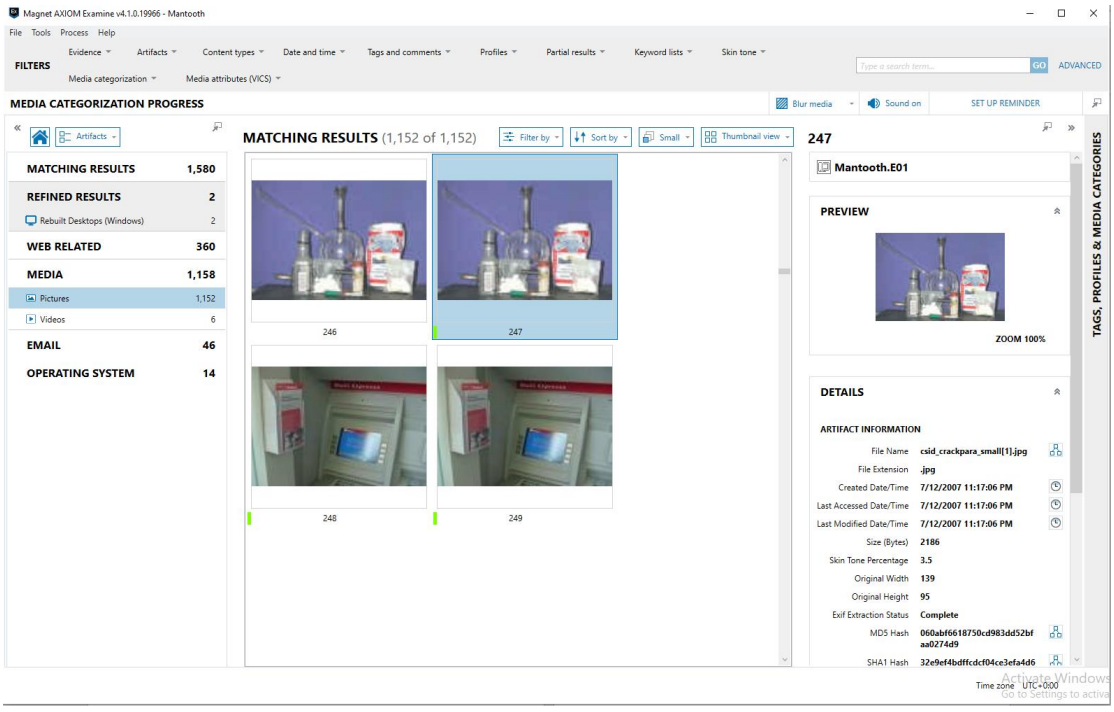

Figure 7.5

Figure 7.5 contains an image of a flask used for meth production.

Emails.

Email Attachments.

When reviewing the AXIOM email threads created under this disk image, there were several related to washing checks, making meth, and making money. Figures 7.6-8.4 contain these images.

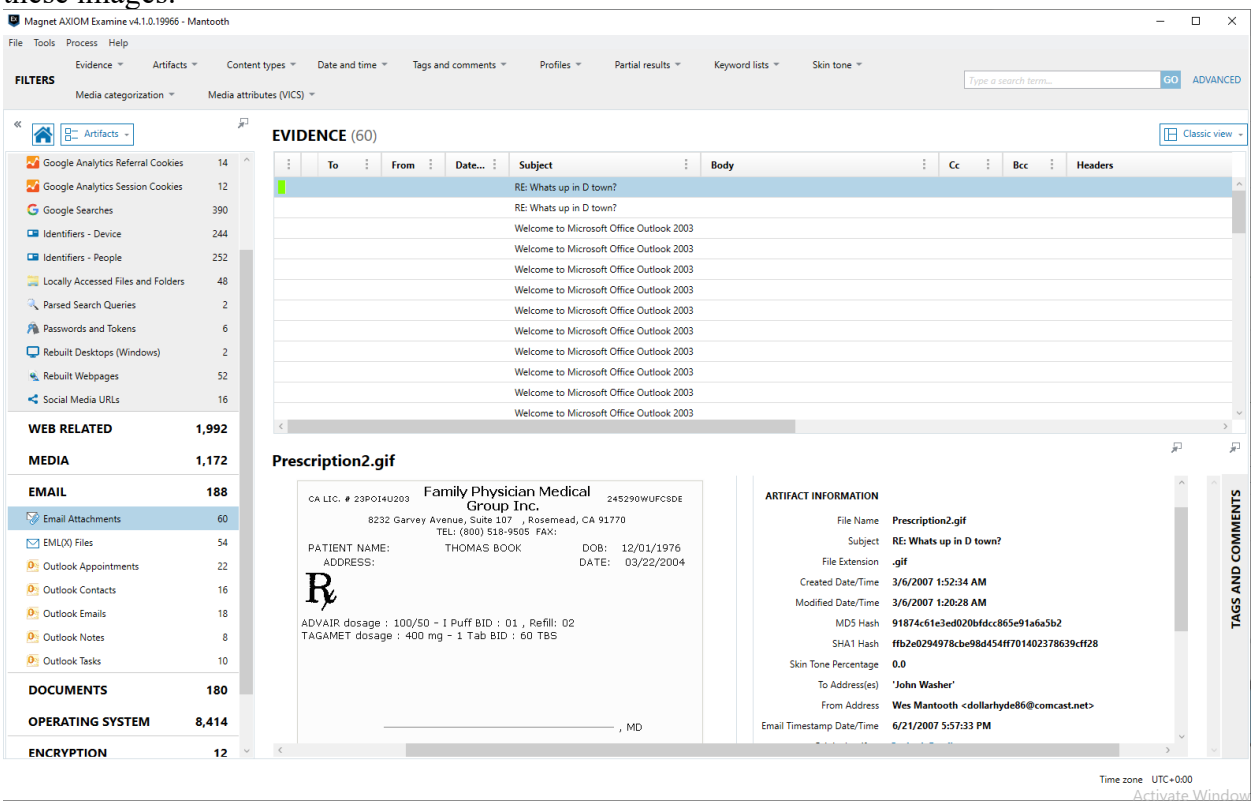

Figure 7.6

Figure 7.6 contains an email attachment of a fake prescription template.

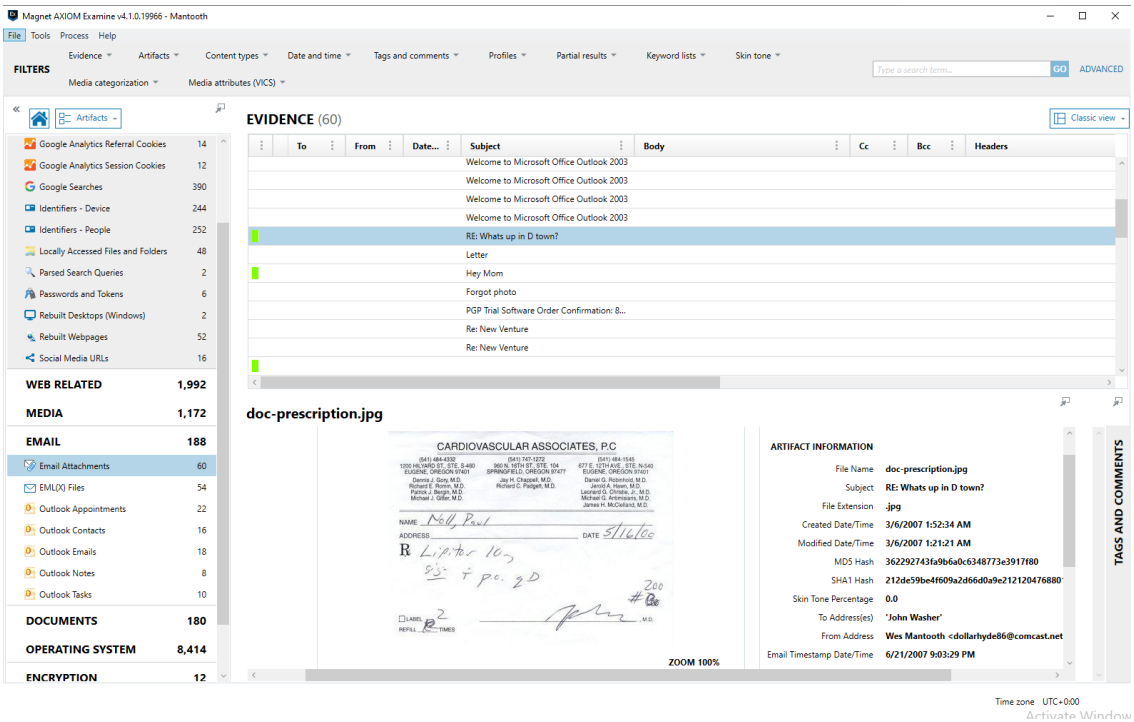

Figure 7.7

Figure 7.7 contains an email attachment of a fake prescription filled out.

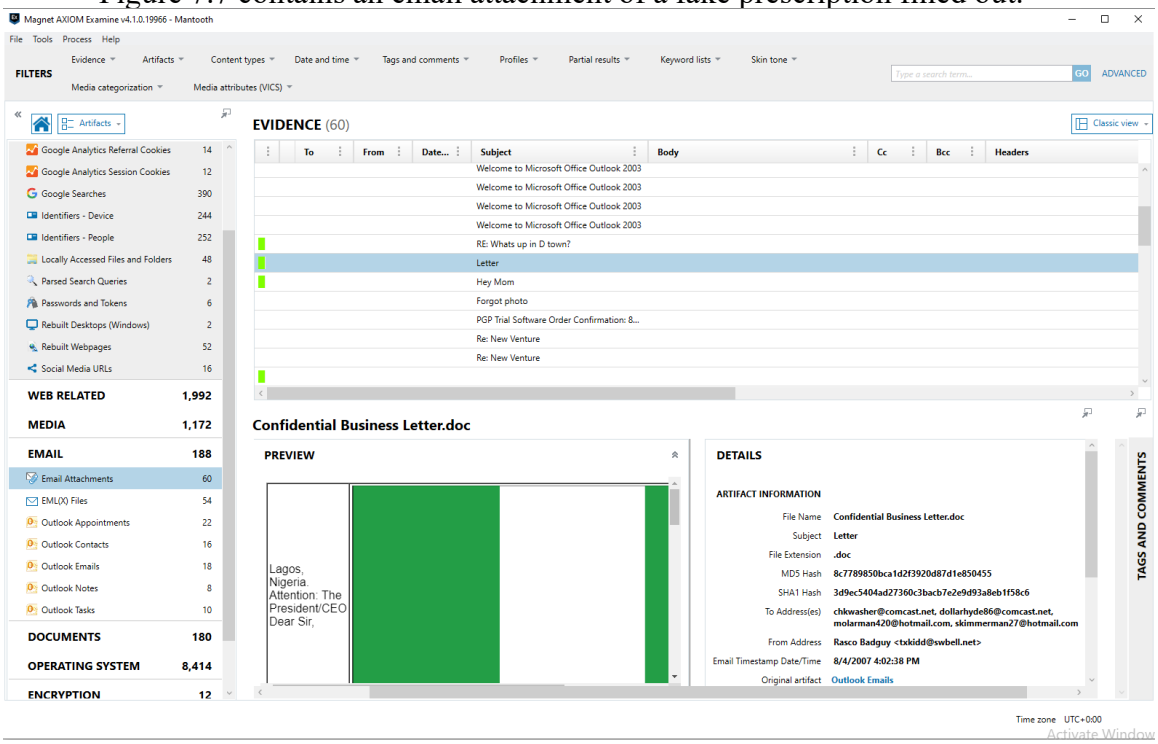

Figure 7.8

Figure 7.8 contains an email attachment of a confidential business letter.

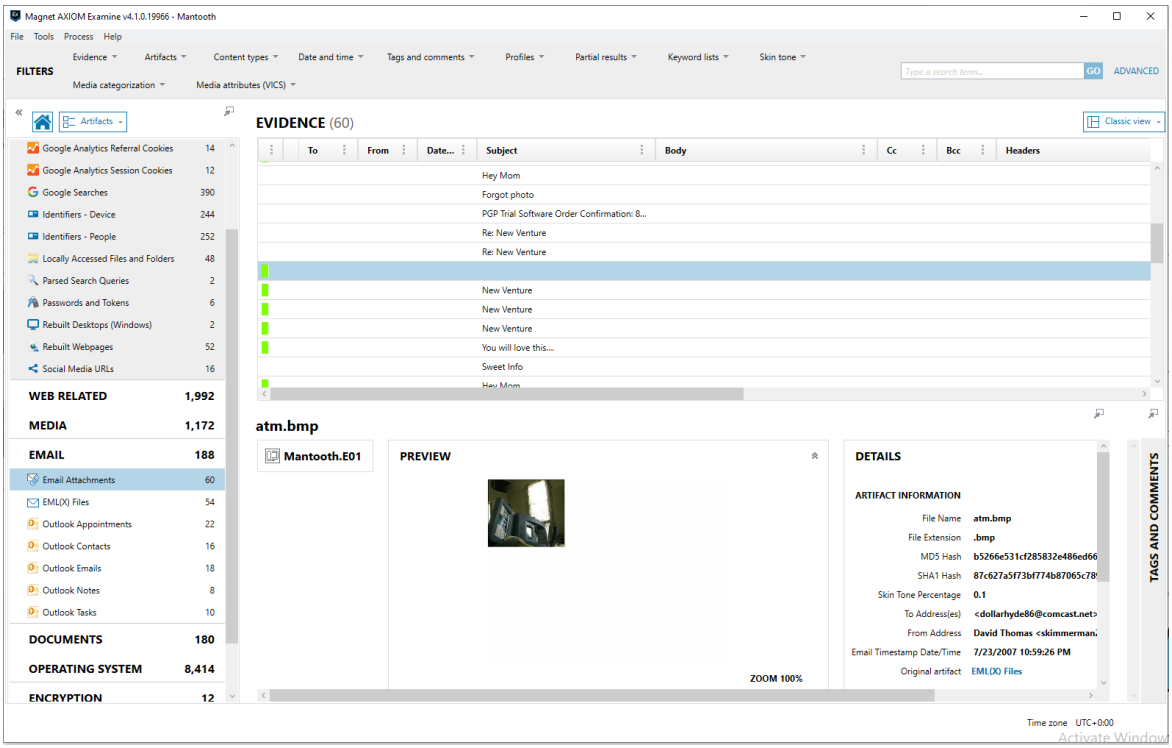

Figure 7.9

Figure 7.9 contains an email attachment of a hacked atm machine.

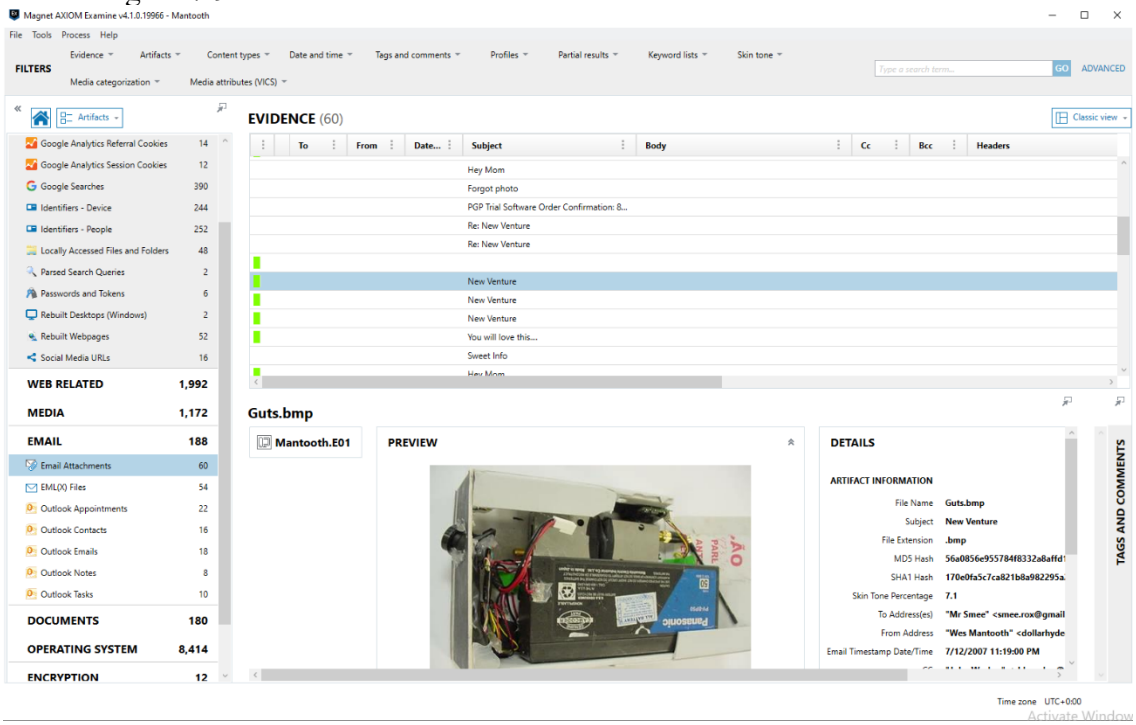

Figure 8.0 – Figure 8.2

Figure 8.0 – Figure 8.2 contain atm stealing procedures in attachment form.

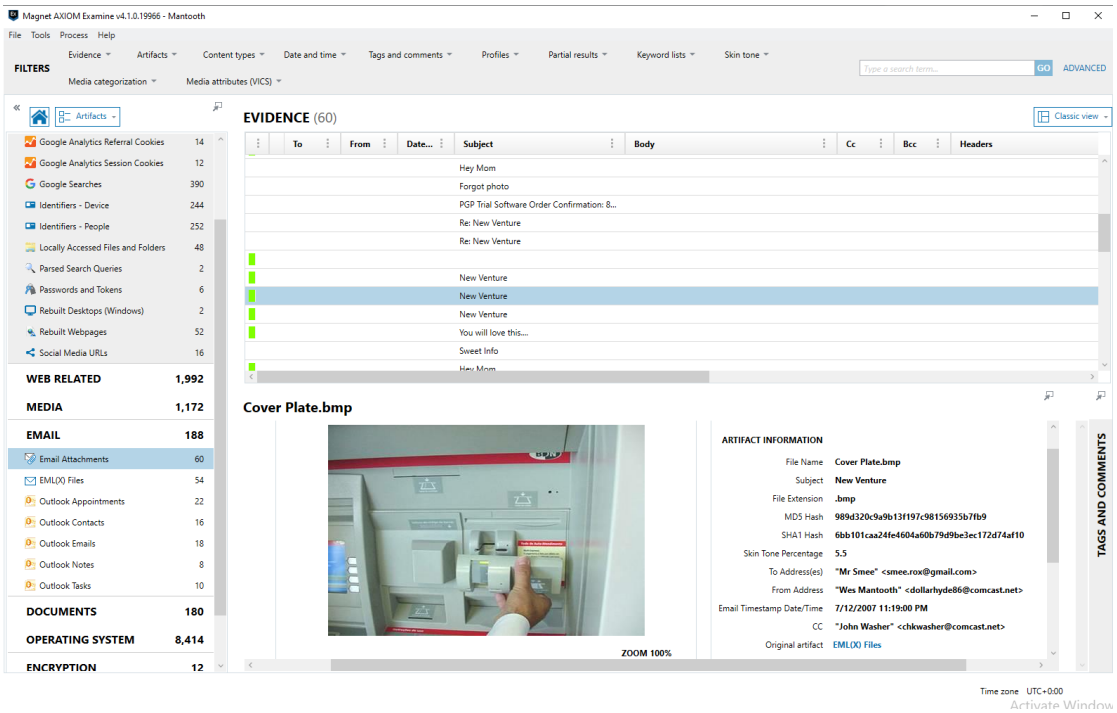

Figure 8.1

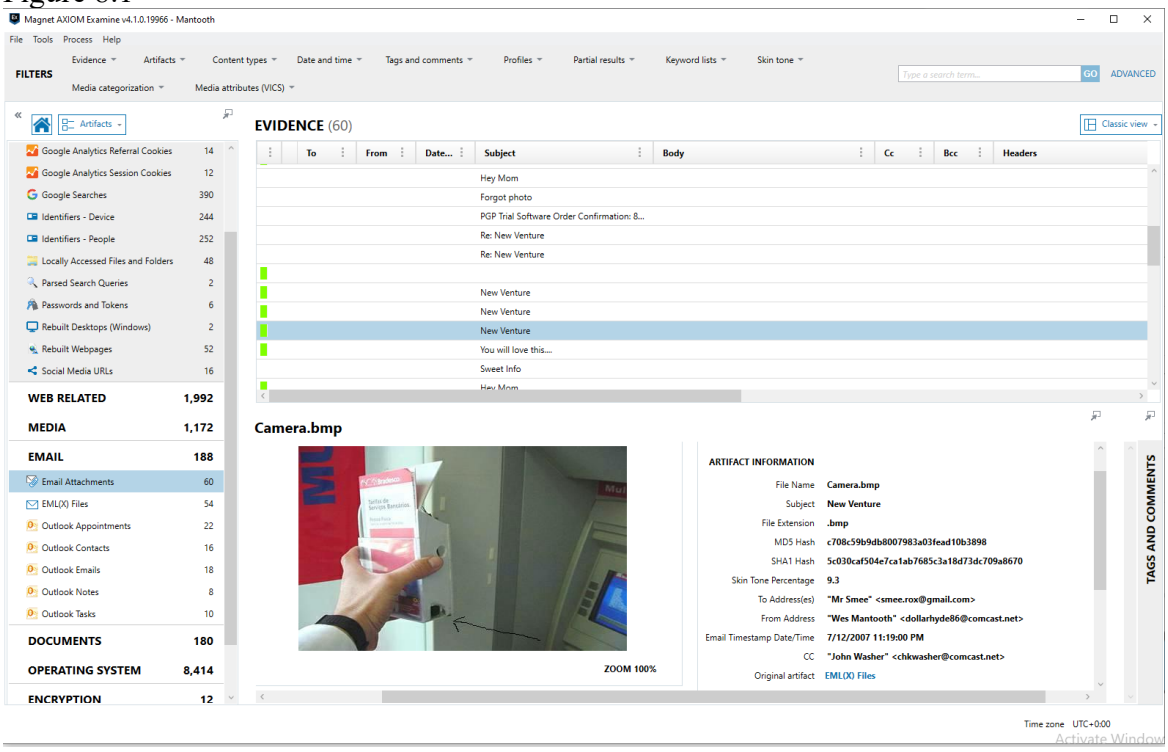

Figure 8.2

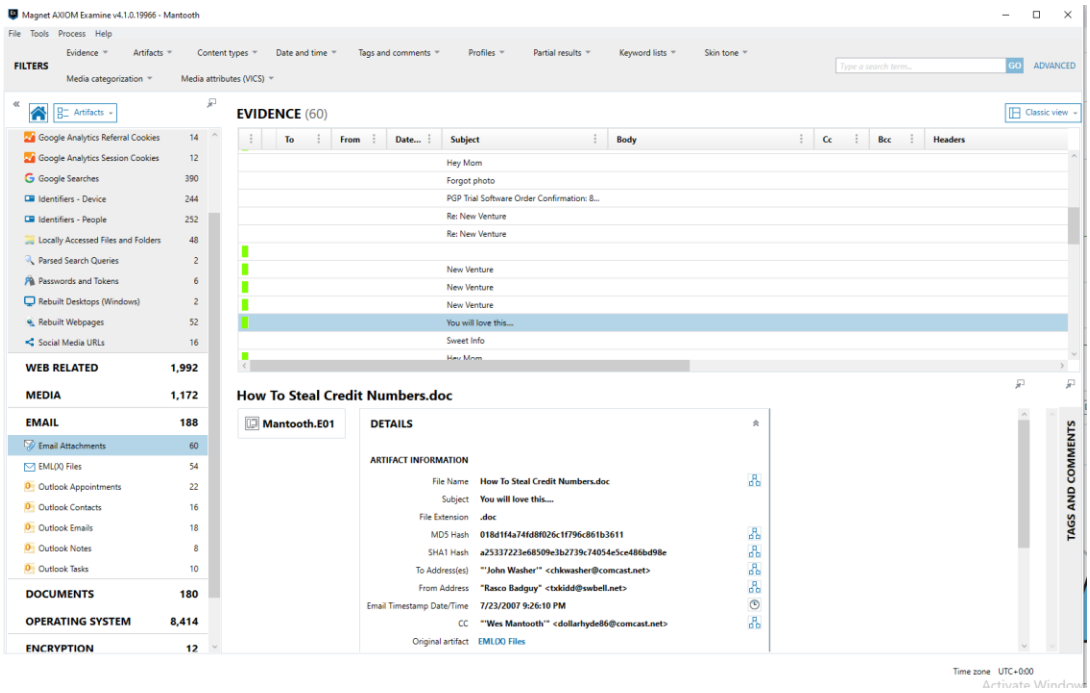

Figure 8.3

Figure 8.3 is an attachment of a .doc containing how to steal credit numbers.

EML(X) Files – These files contained conversations related to drugs along with the encryption program used for several files on this laptop. Figures 8.4 - 9.3

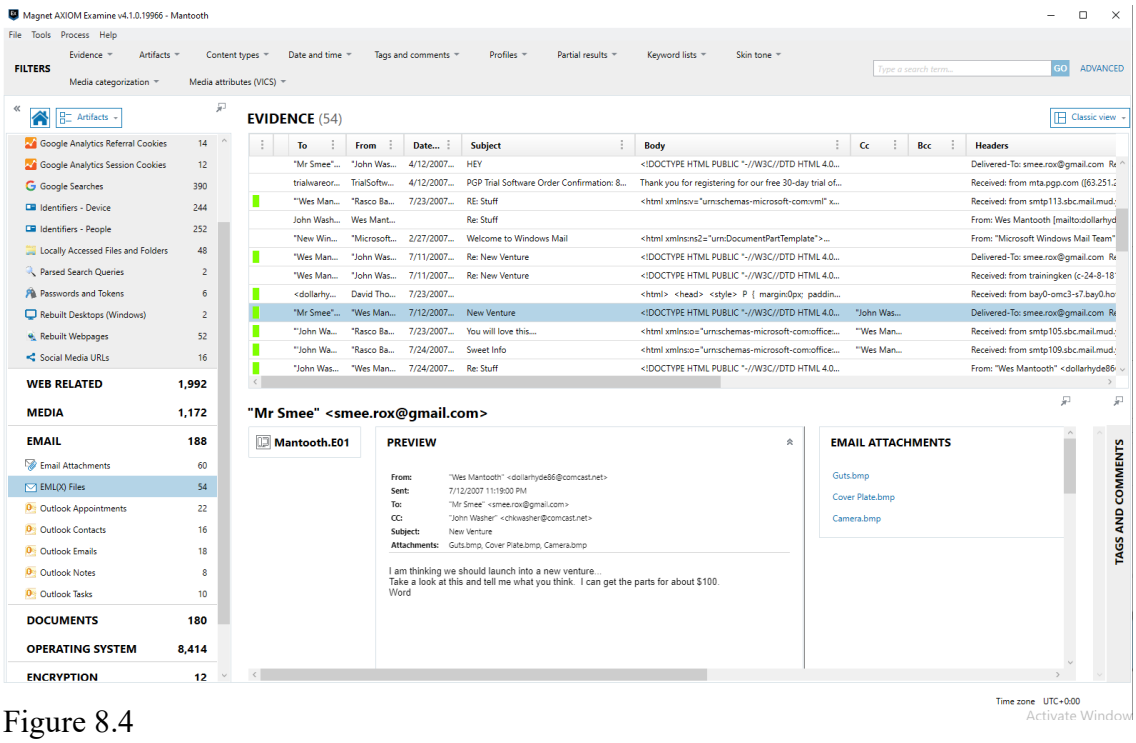

Figure 8.4

Figure 8.4 shows an email conversation between Mantooth and “Mr. Smee”.

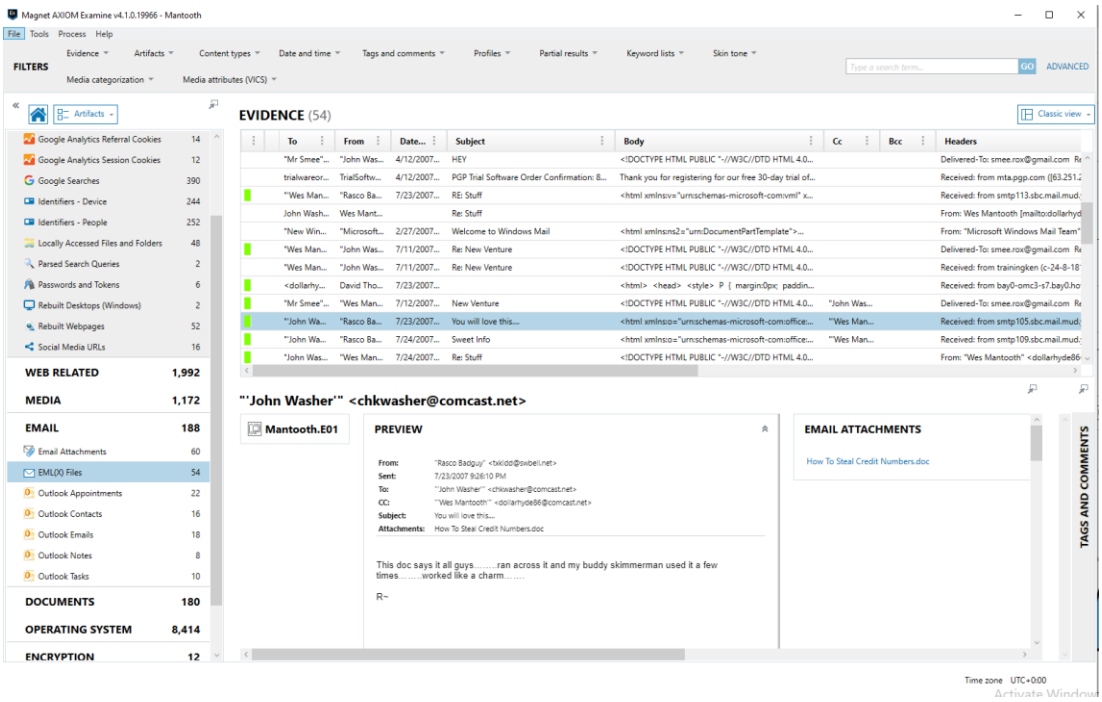

Figure 8.5

Figure 8.5 shows a conversation between John Washer and Wes Mantooth.

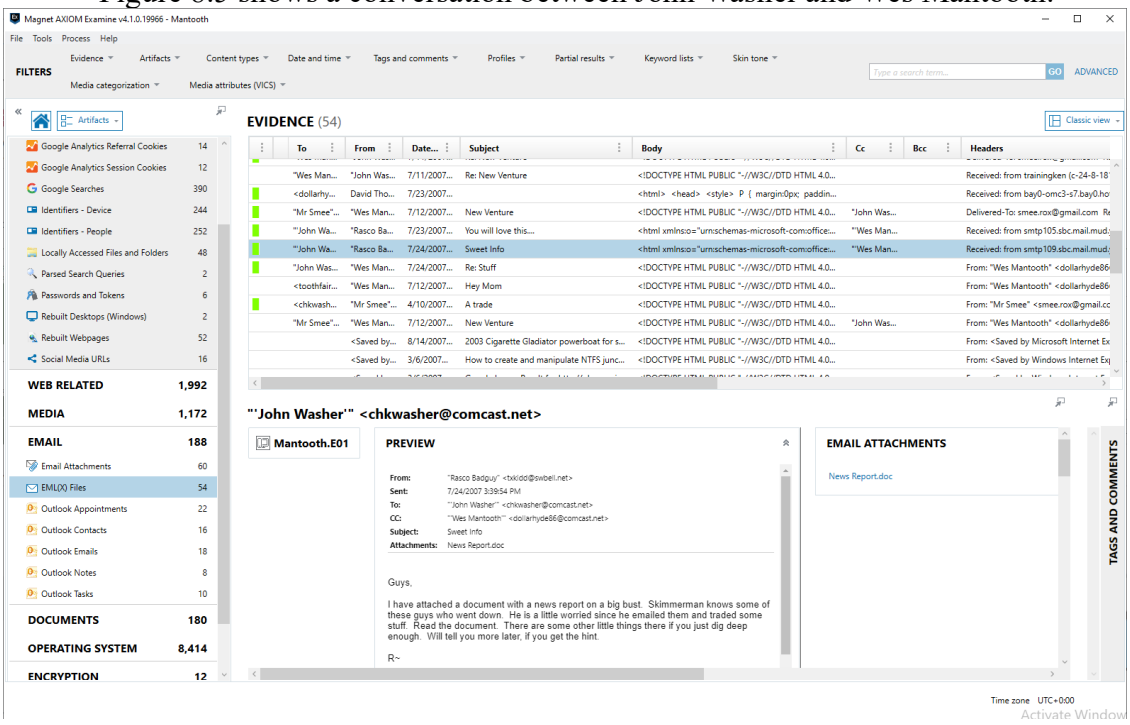

Figure 8.6

Figure 8.6 shows a drug conversation between John Washer and Wes Mantooth.

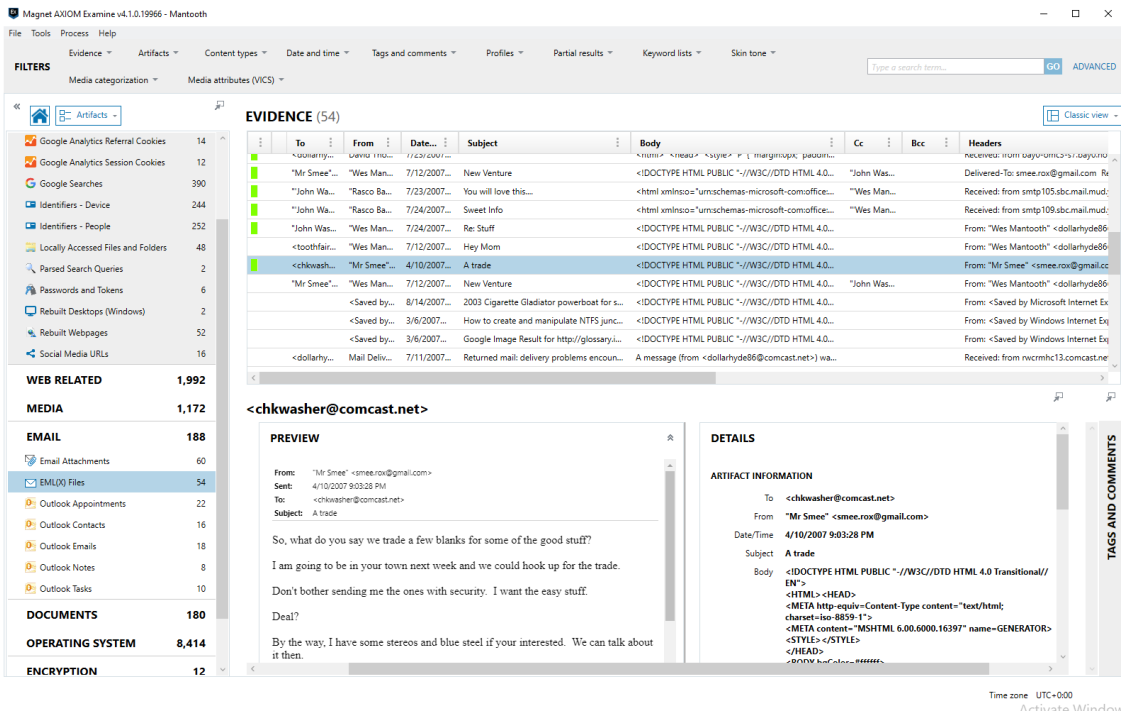

Figure 8.7

Figure 8.7 contains a conversation between Washer and Mantooth about drugs.

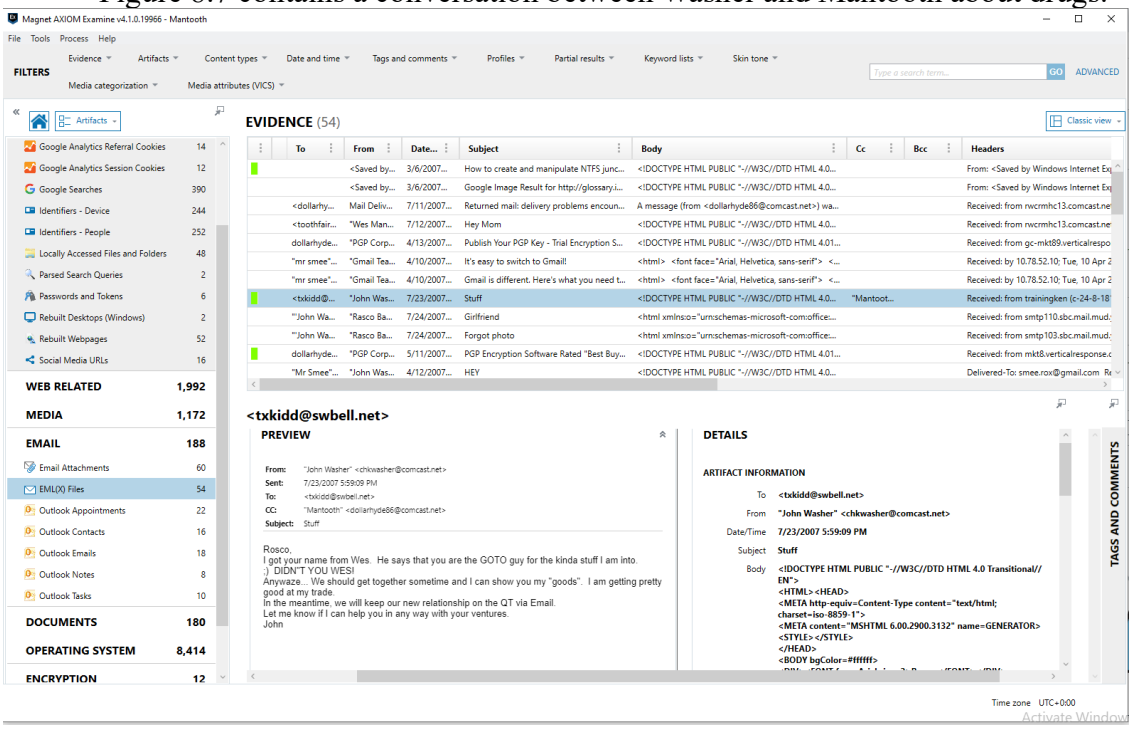

Figure 8.8

Figure 8.8 contains a new conversation about getting drugs from Wes Mantooth.

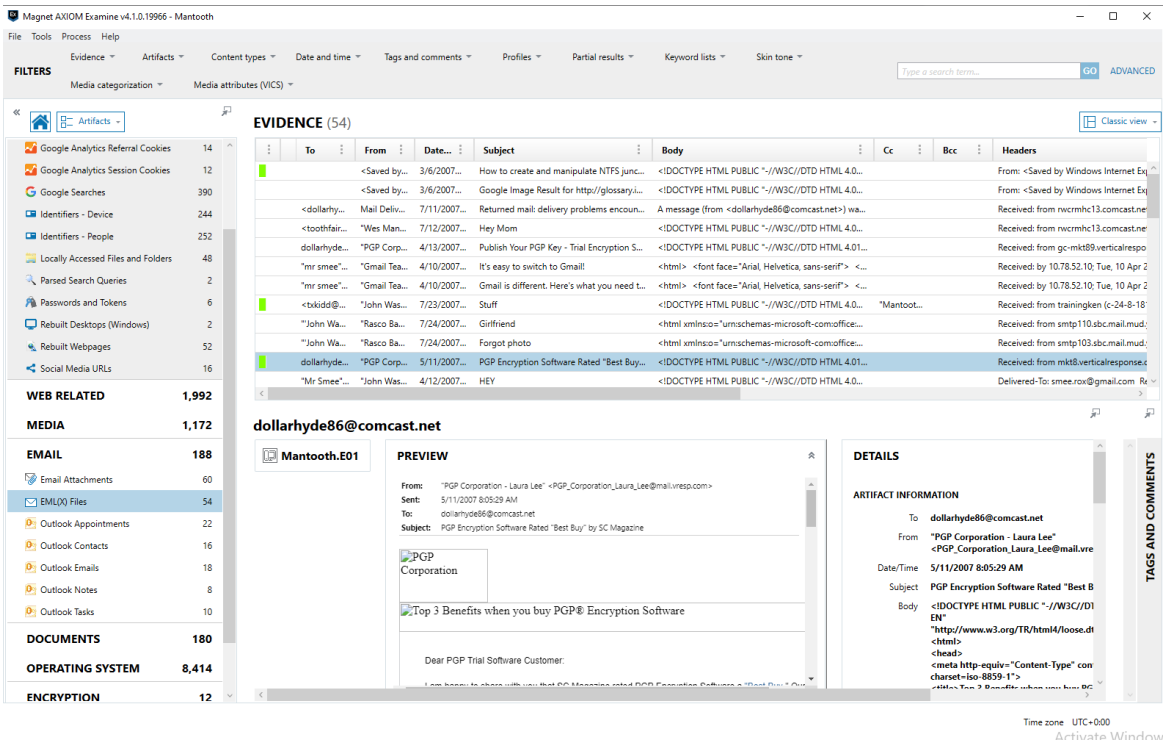

Figure 8.9

Figure 8.9 is an attachment for encryption software by comcast.net

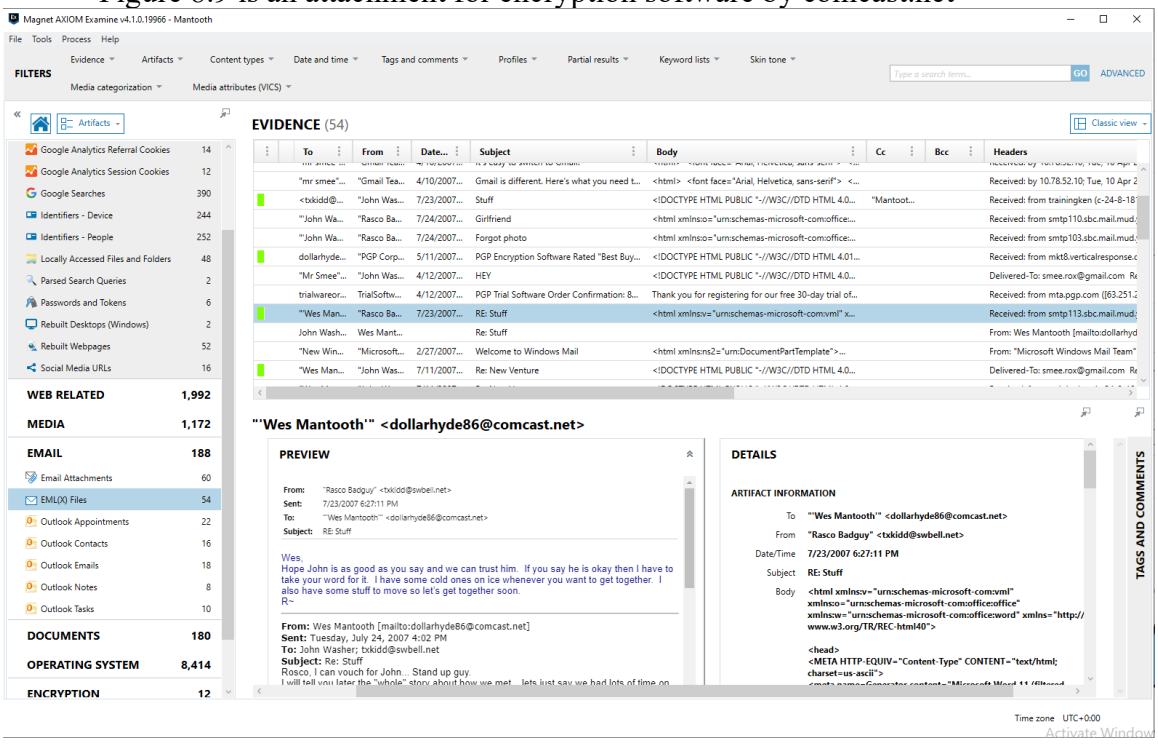

Figure 9.0

Figure 9.0 is a drug conversation between Wes Mantooth and “dollarhyde86”.

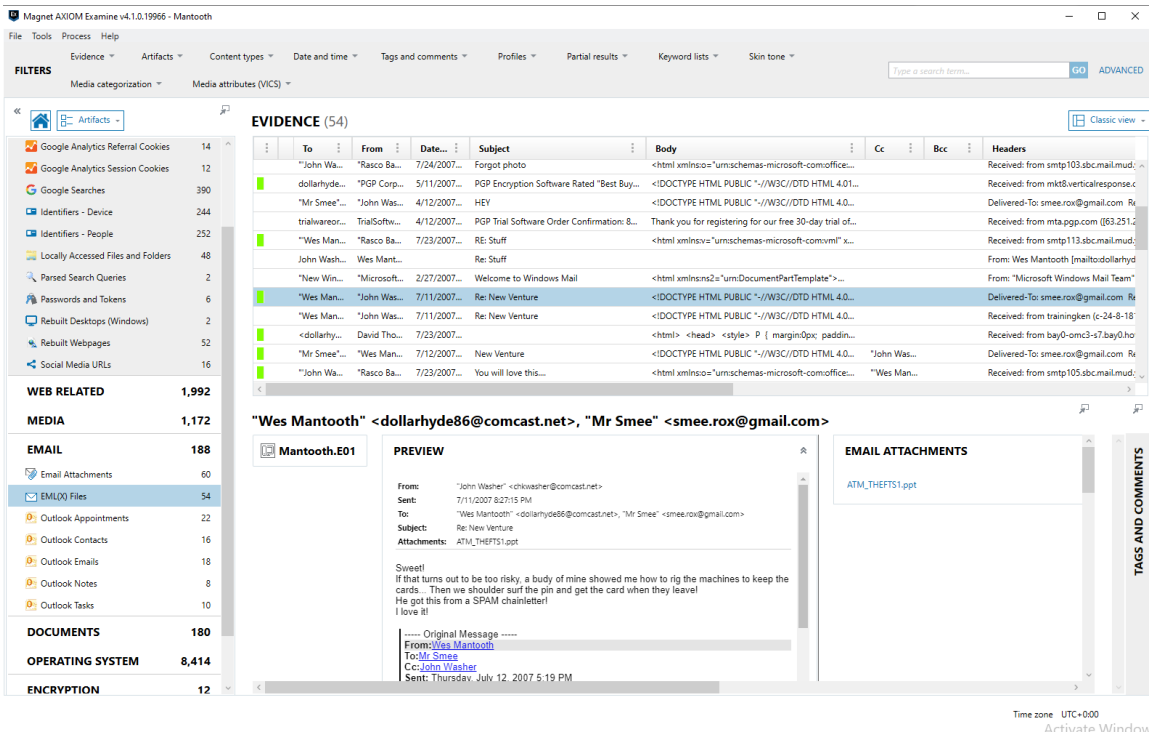

Figure 9.1

Figure 9.1 is a conversation between Mr.Smee, Dollarhyde86, and Wes Mantooth.

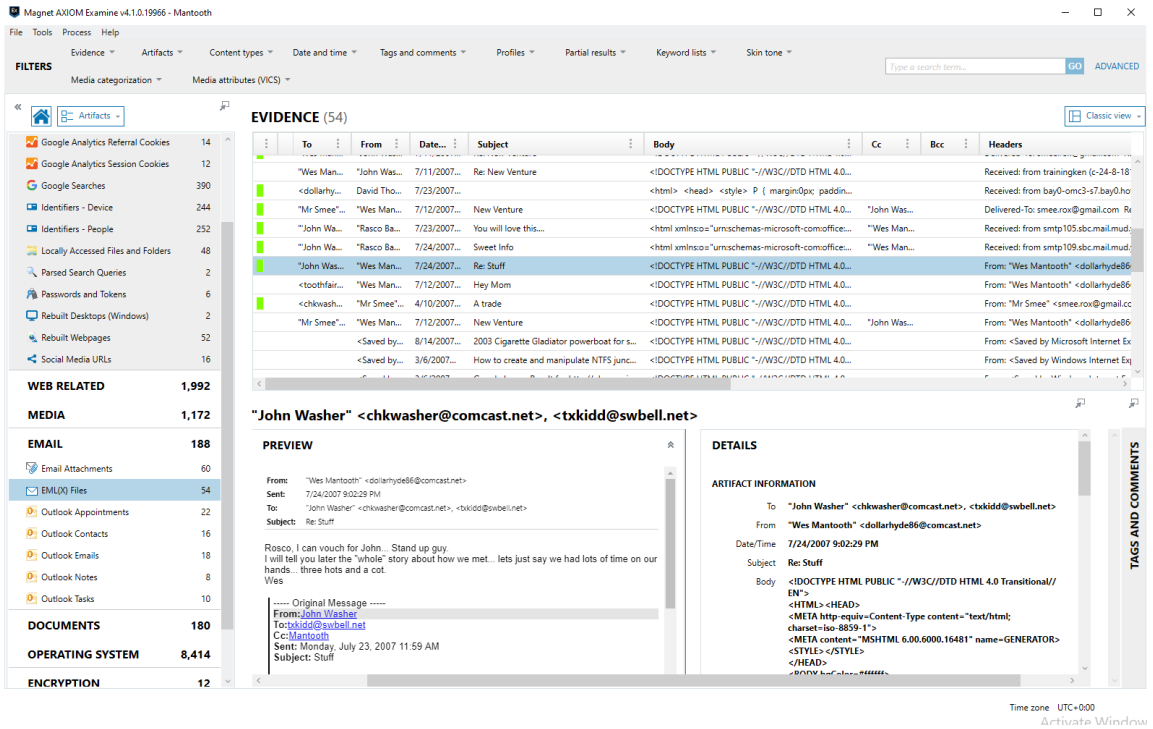

Figure 9.2

Figure 9.2 is a conversation between John Washer, chkwasher, and txkidd.

Outlook Appointments

This was appointments made within the Outlook email program and contained information related to check stealing and pharmaceutical drugs. Figures 9.3-9.6

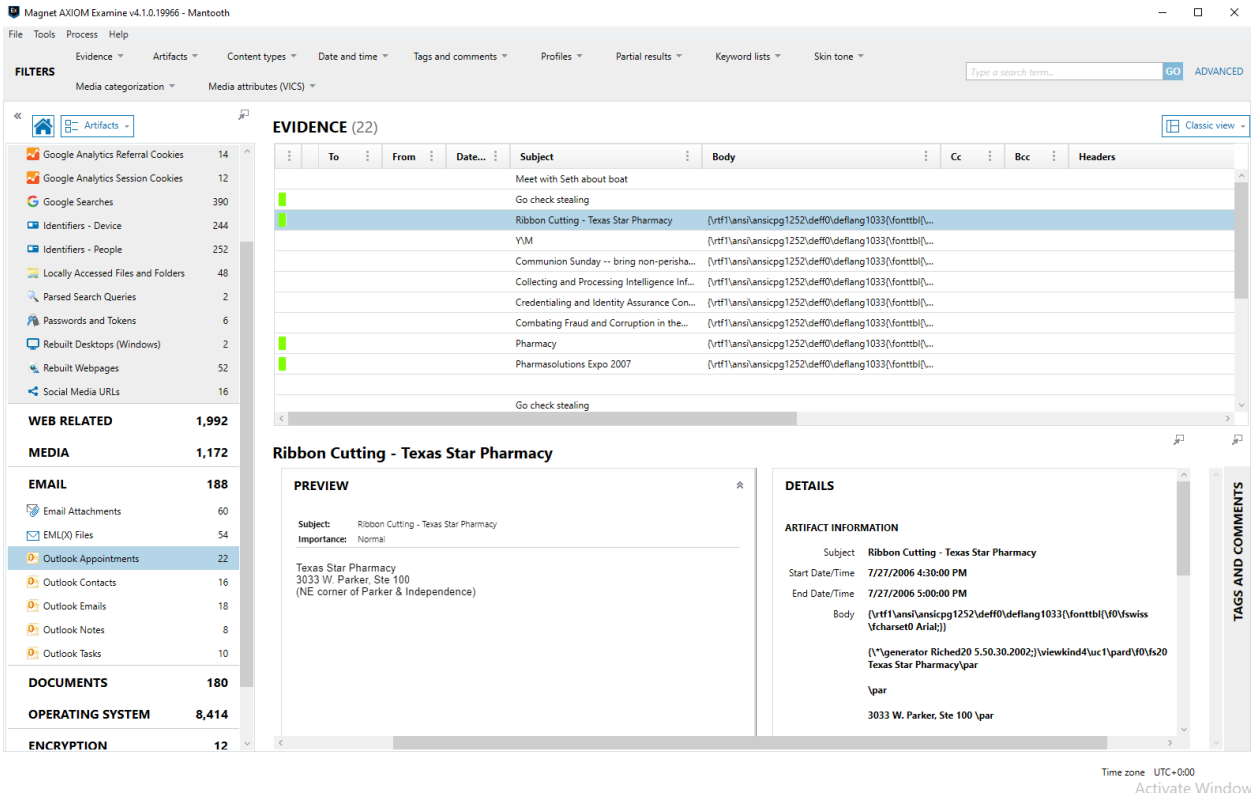

Figure 9.3

Figure 9.3 contains a pharmacy email for where Wes Mantooth got his Sudafed from.

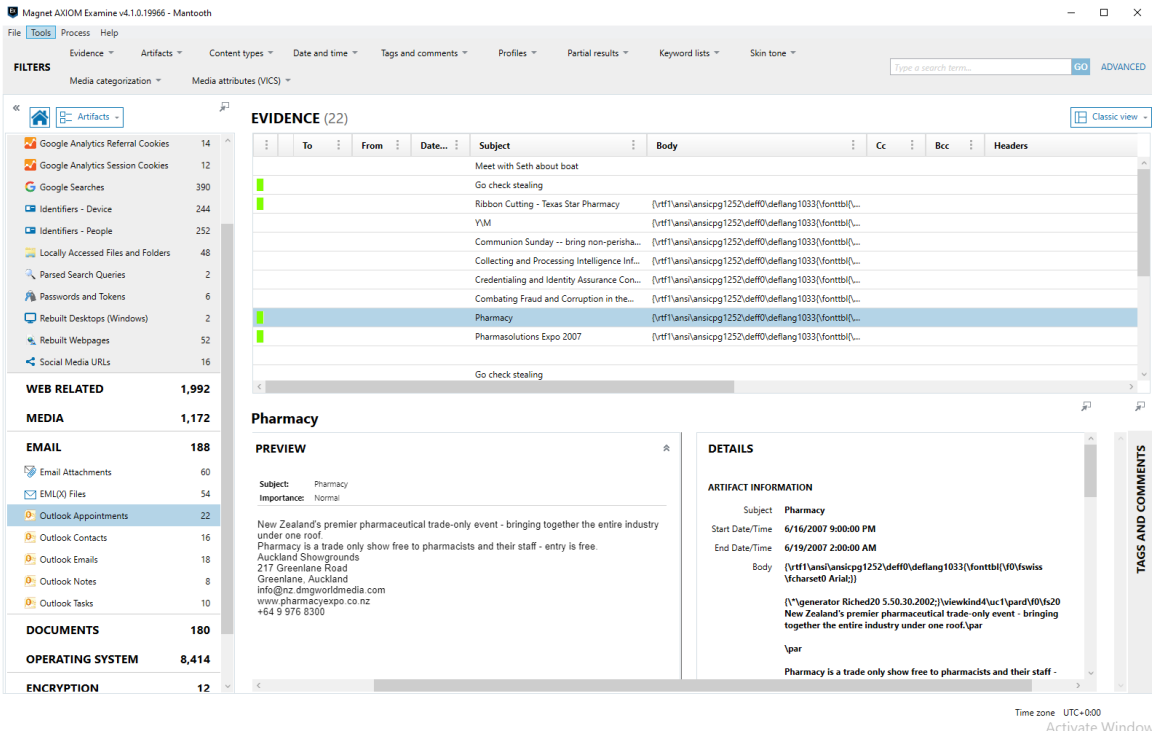

Figure 9.4

Figure 9.4 contains information about a pharmacy selling drugs illegally.

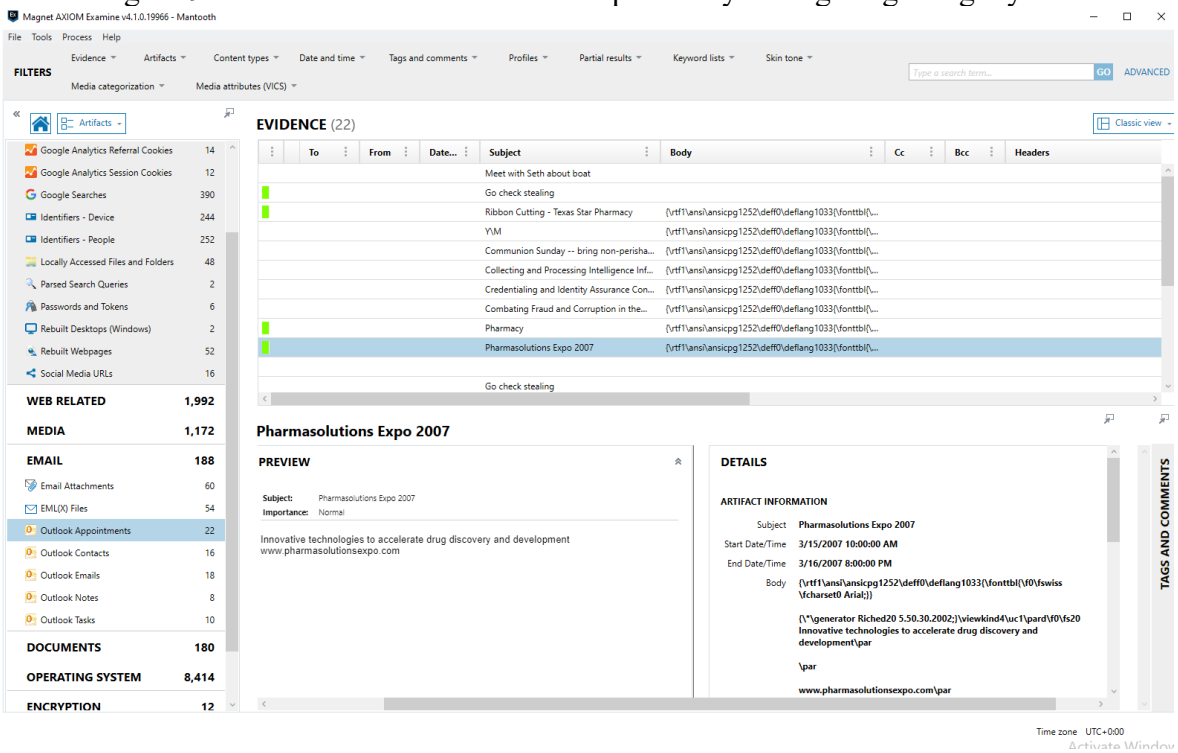

Figure 9.5

Figure 9.5 contains further information on a illegal pharmacy expo in 2007.

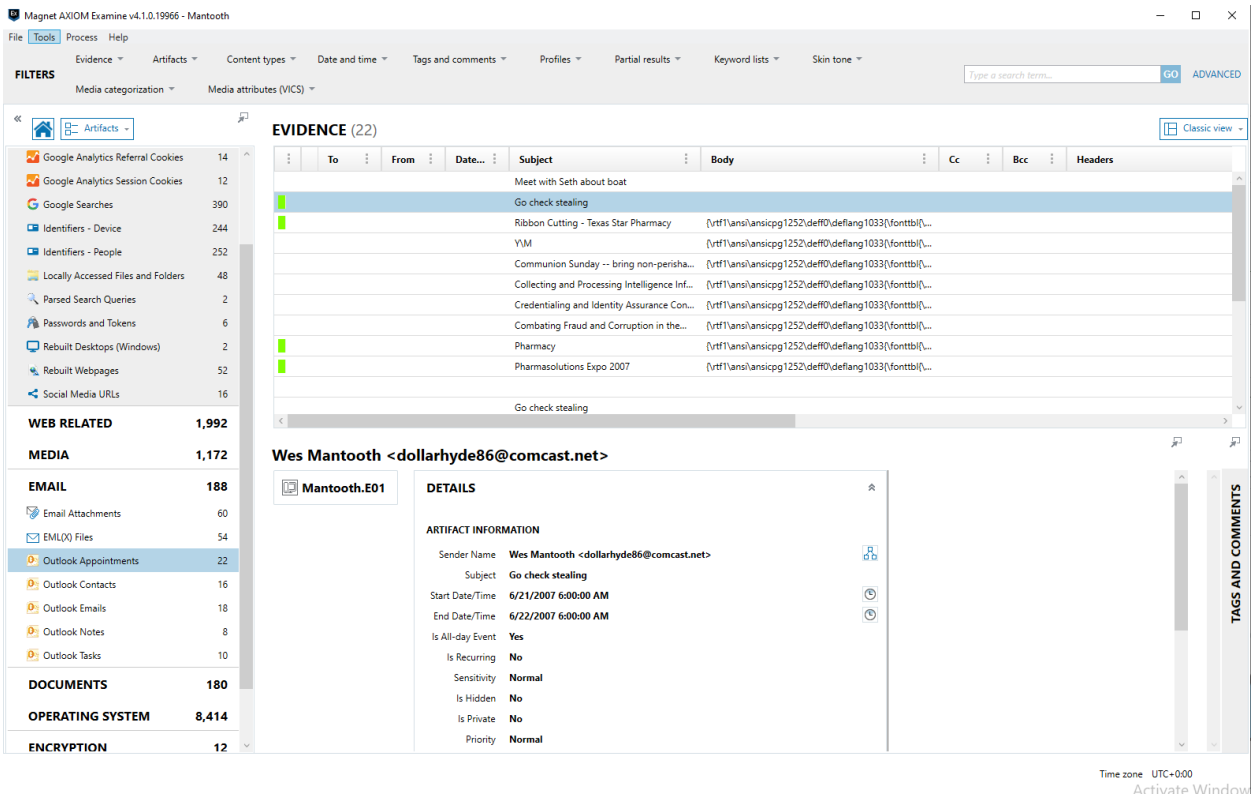

Figure 9.6

Figure 9.6 contains information about check stealing.

Outlook Contacts

These were the contacts used in the email threads and contained keywords such as ‘meth’. Figures 9.7 – 10.0

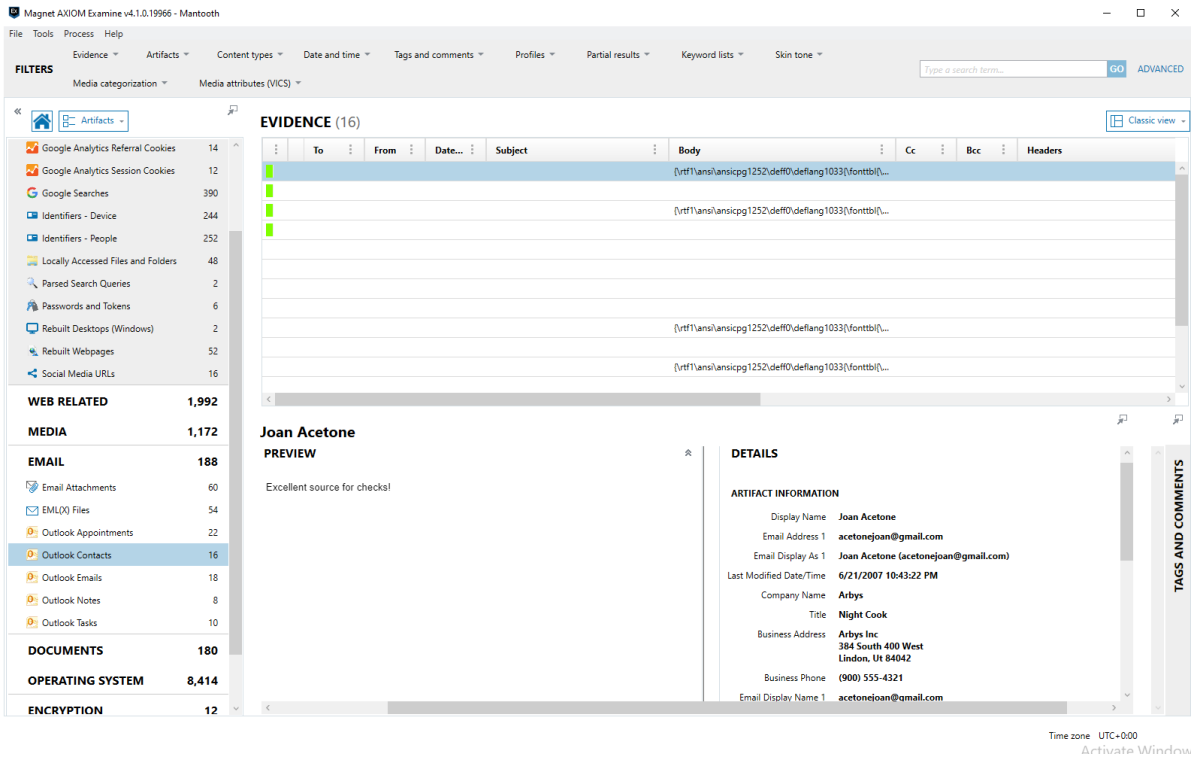

Figure 9.7

Figure 9.7 talks about a source for fraudulent cashier checks.

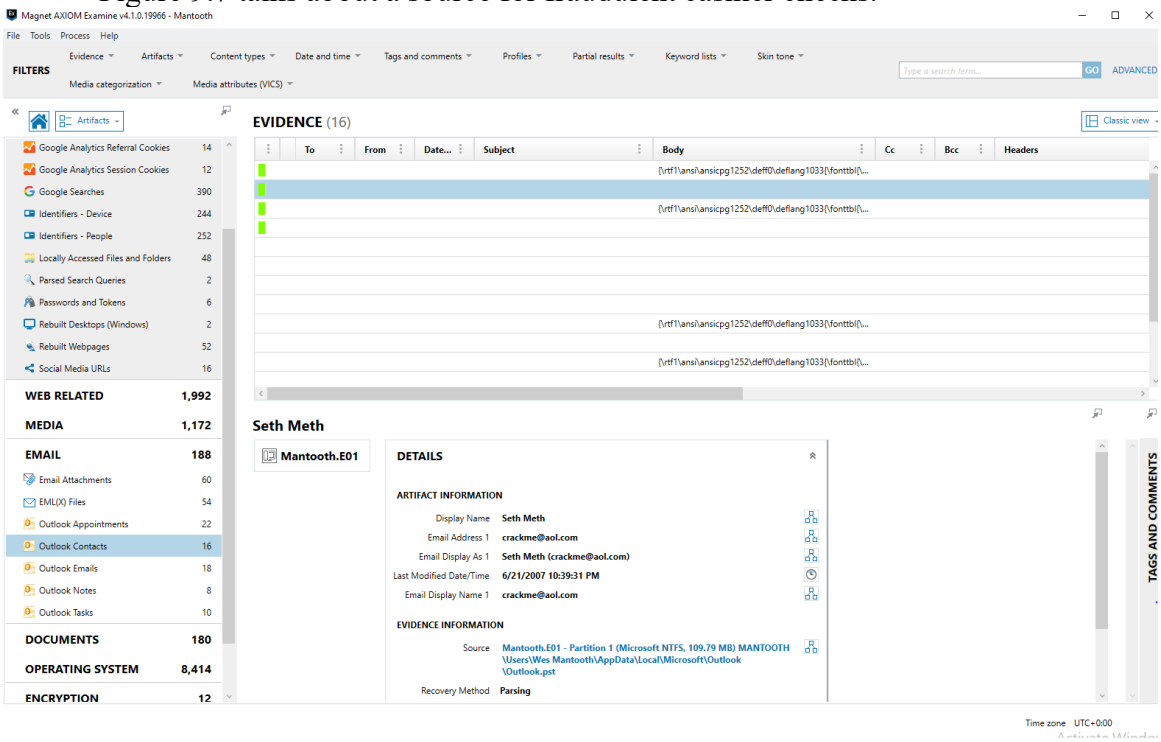

Figure 9.8

Figure 9.8 contains an email labeled “Seth Meth”.

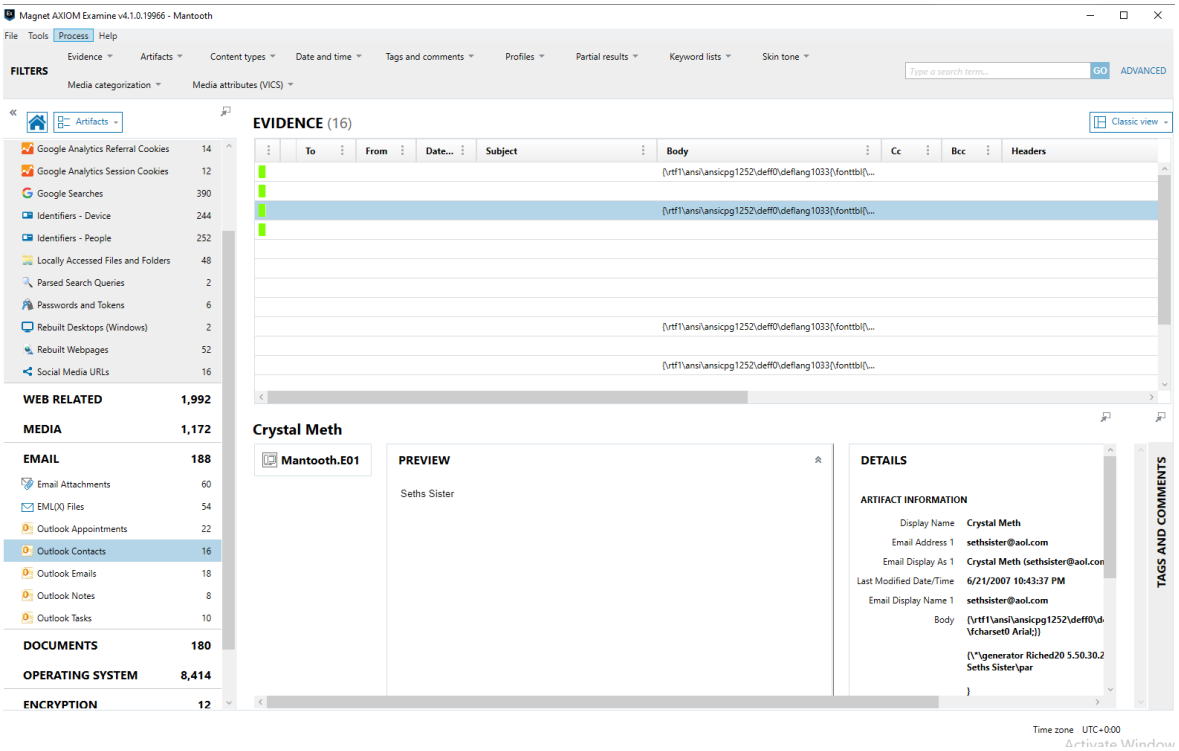

Figure 9.9

Figure 9.9 contains another email labeled "Crystal Meth".

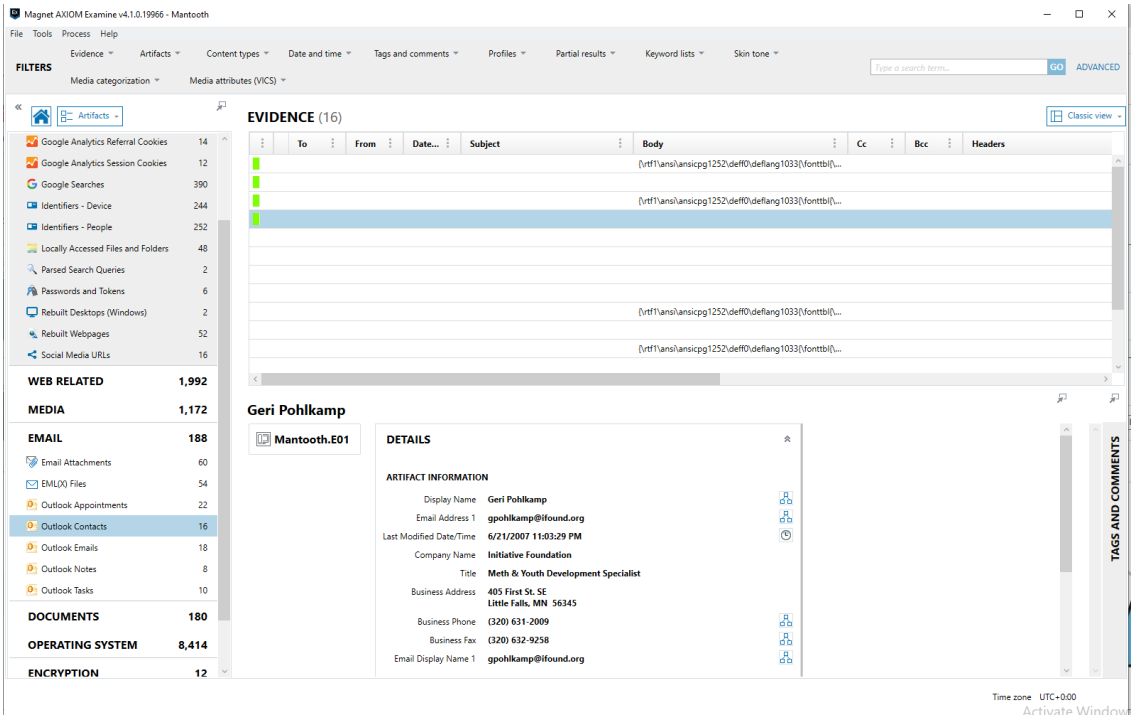

Figure 10.0

Figure 10.0 contains an email from Geri Pohlkamp about meth.

Outlook Emails

These emails contain messages from Outlook about drugs such as ‘Special K’ and ‘Meth’. Figures 10.1 – 10.7

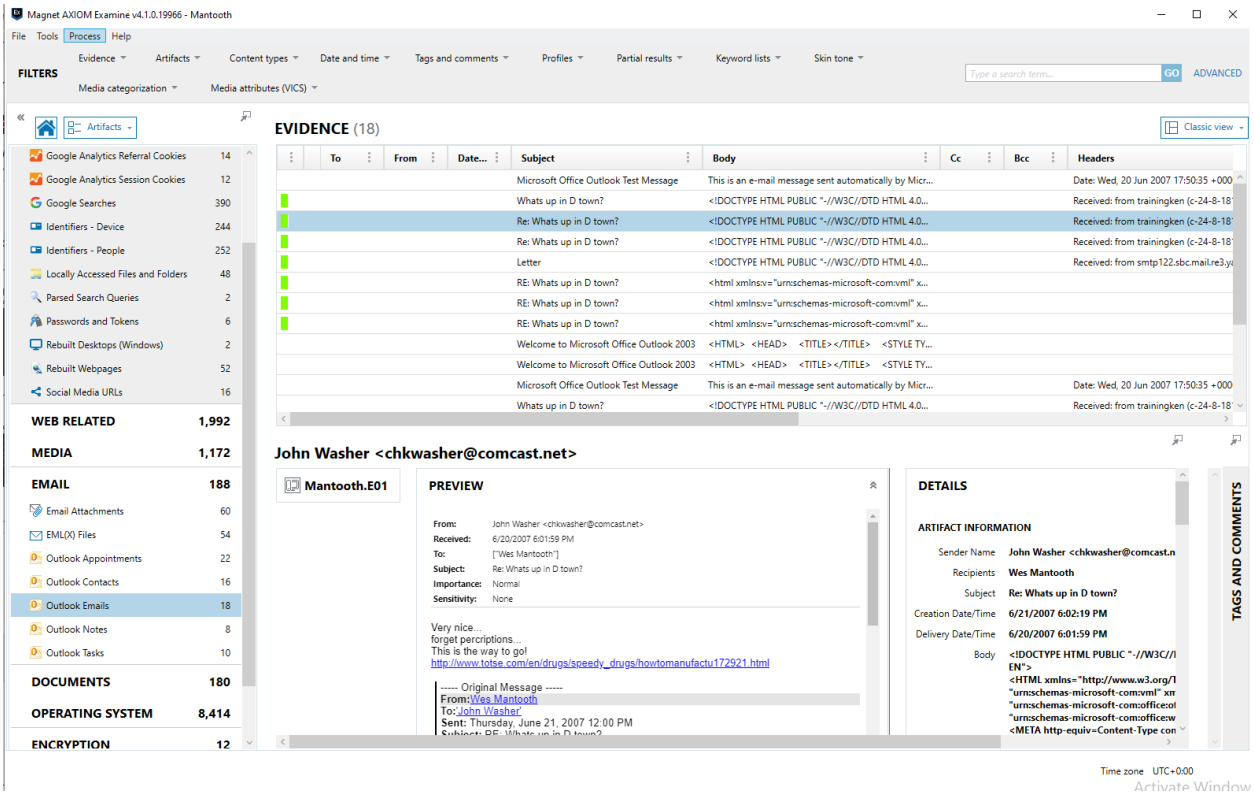

Figure 10.1

Figure 10.1 contains an Outlook email about meth from John Washer.

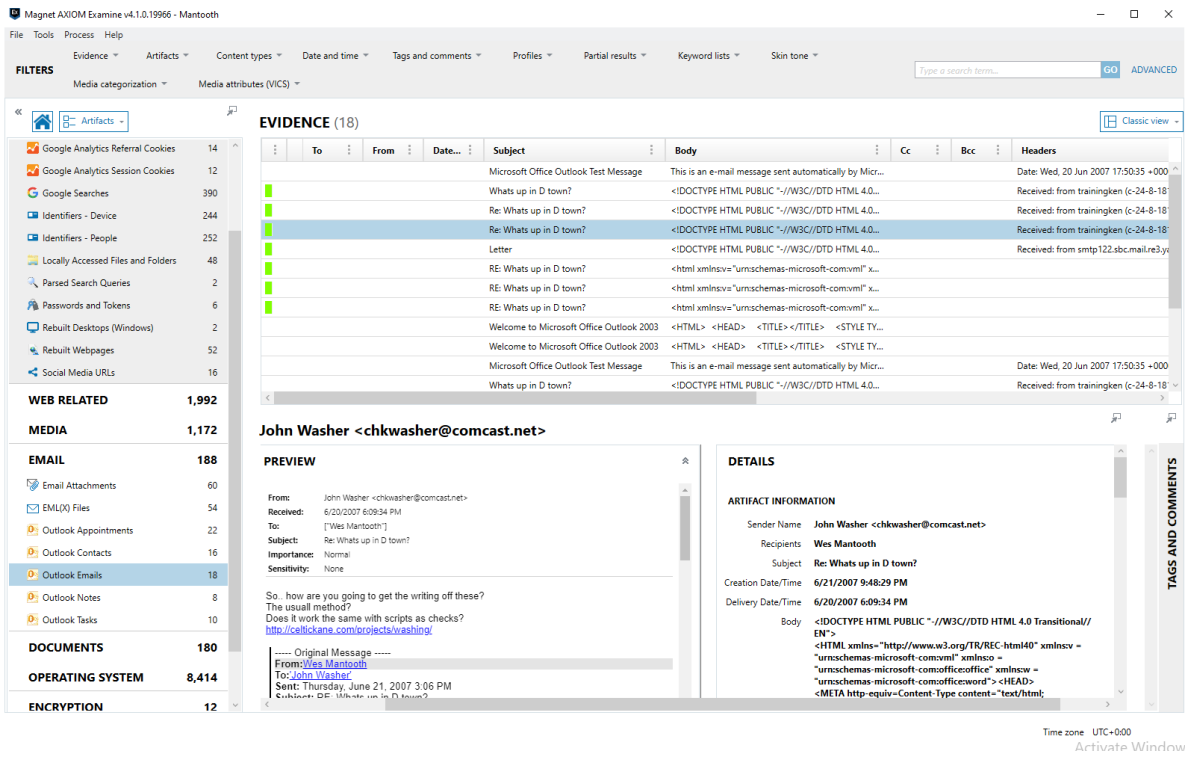

Figure 10.2

Figure 10.2 contains another email from John Washer about meth.

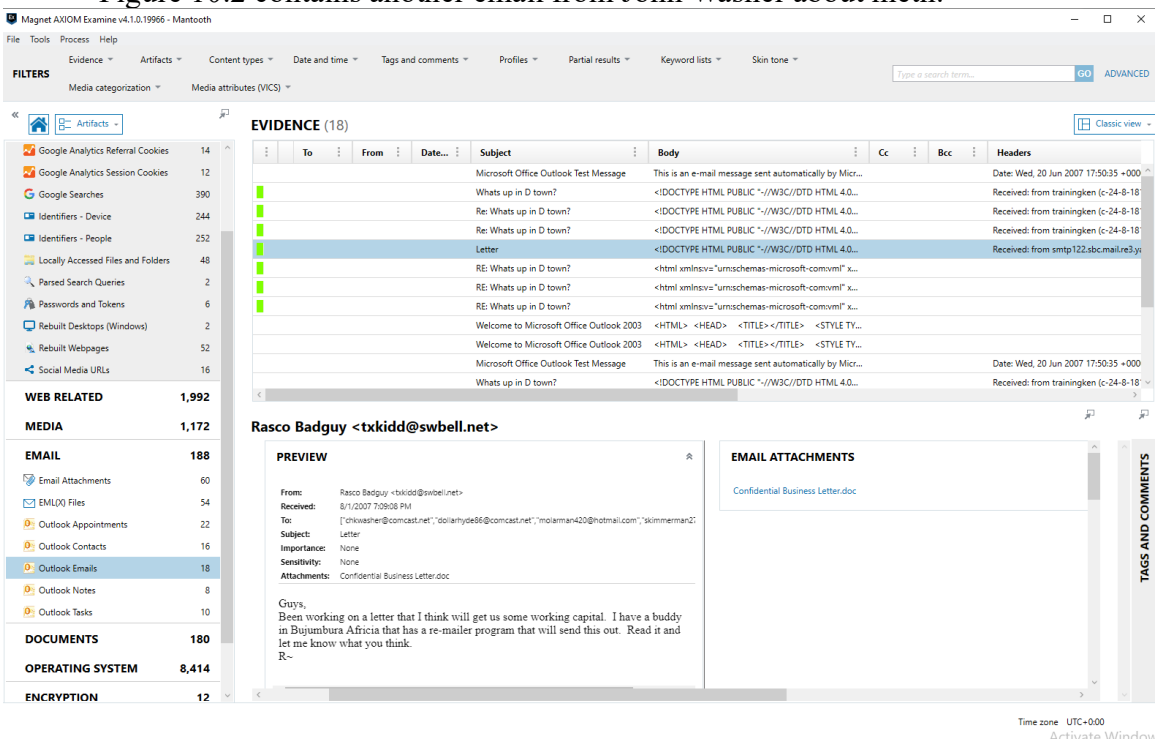

Figure 10.3

Figure 10.3 contains an email from Rasco Badguy about meth.

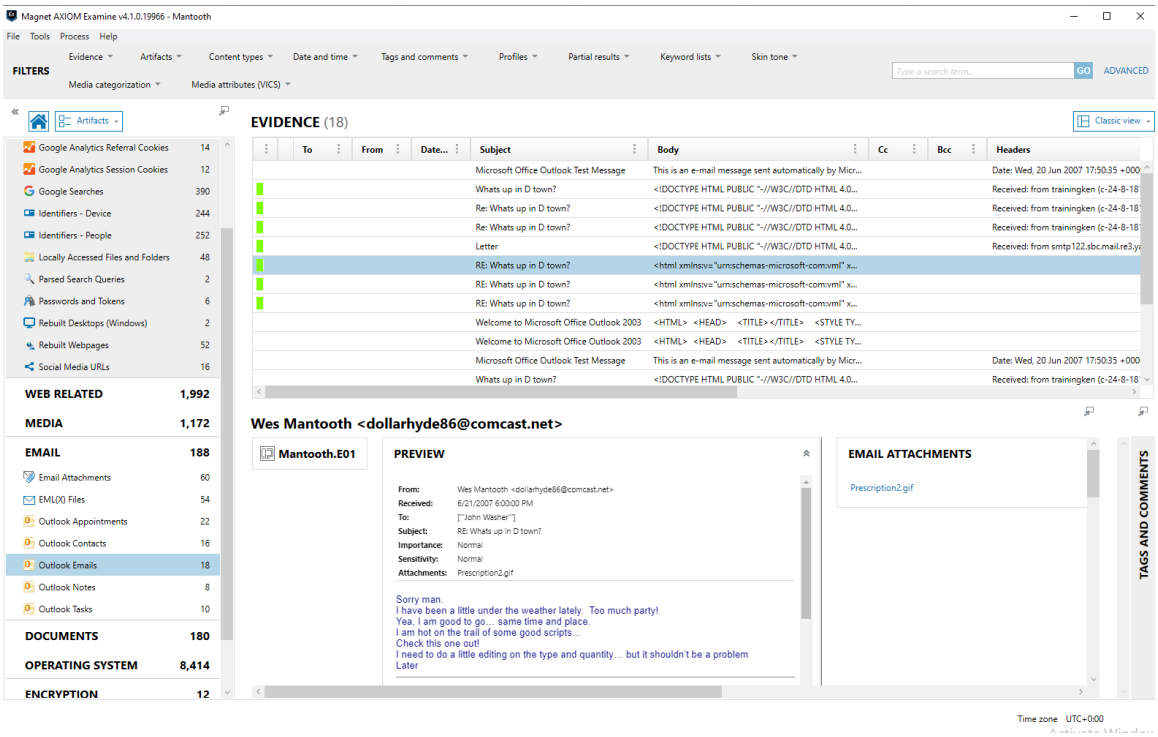

Figure 10.4 – 10.6 contain messages from dollarhyde.

Figure 10.4 contains a message from dollarhyde about meth.

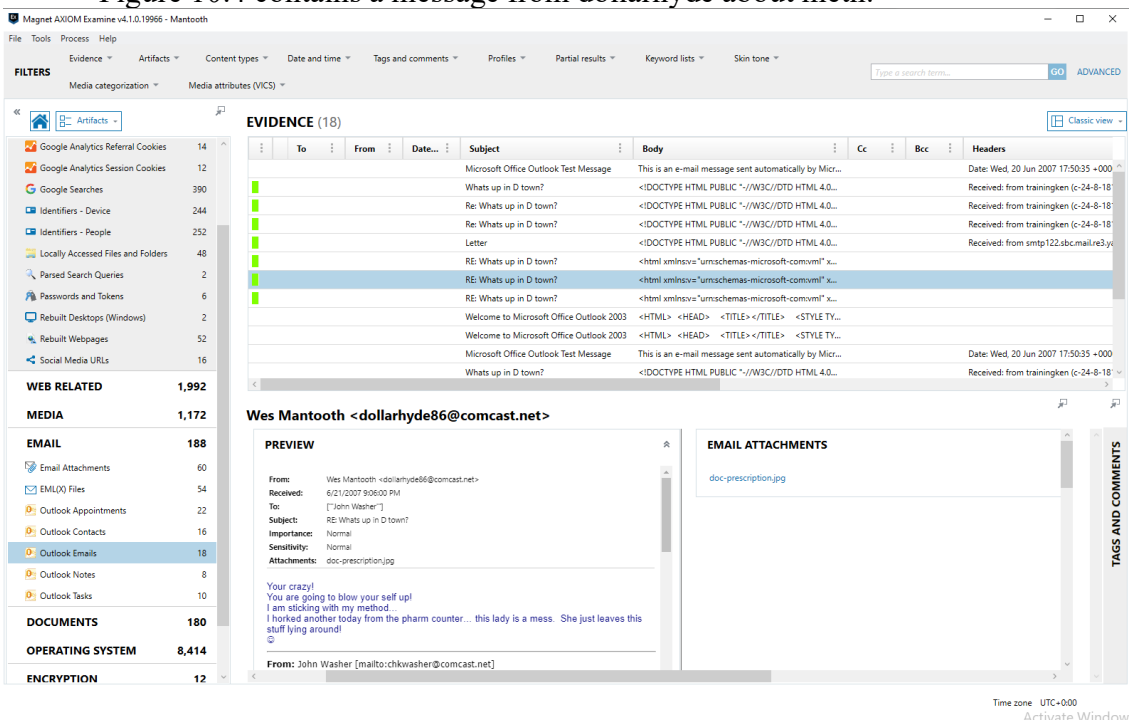

Figure 10.5

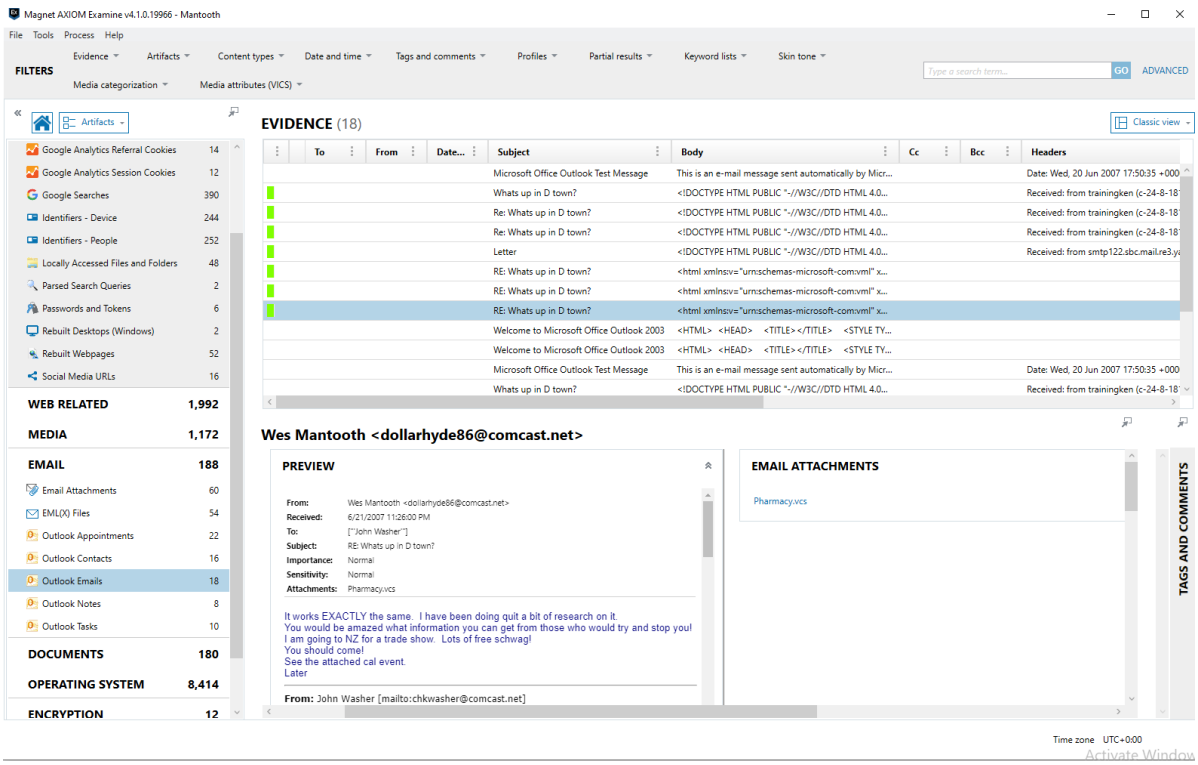

Figure 10.6

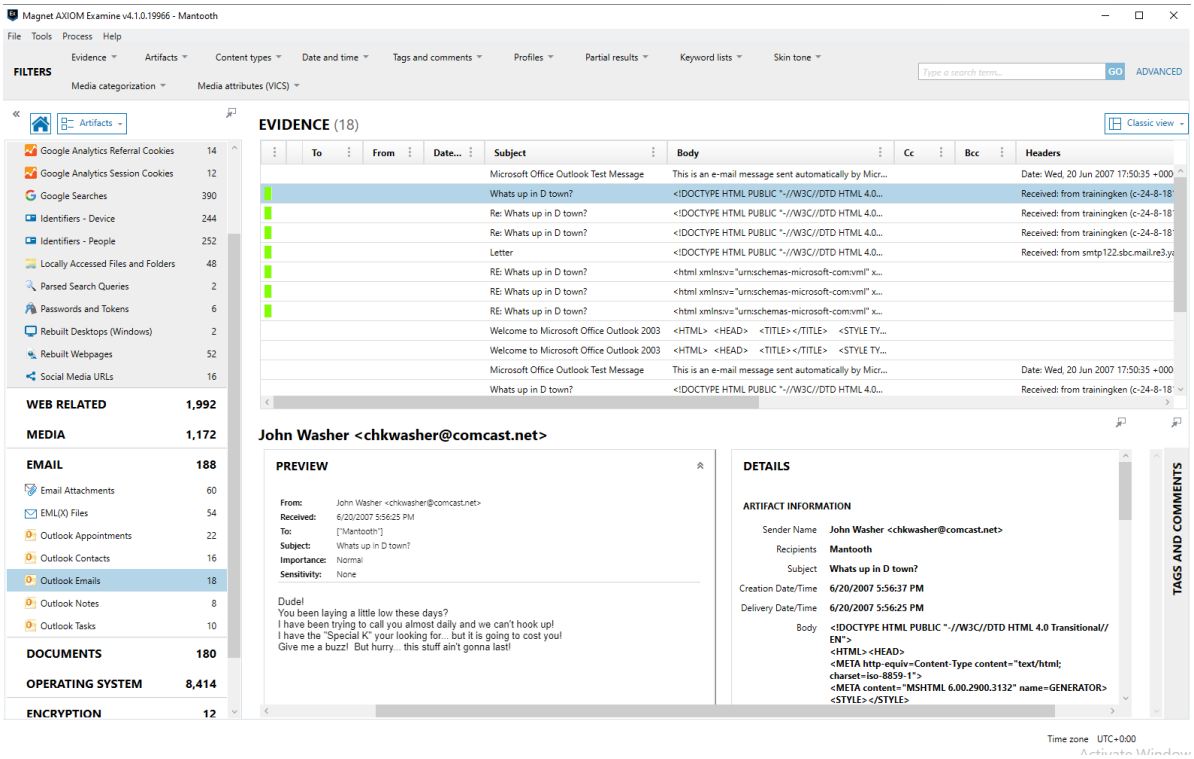

Figure 10.7

Figure 10.7 contains a message from chkwasher or checkwasher.

Outlook Notes

These notes contained in Outlook contained information about buying Acetone and check ripping. Figures 10.8-10.9

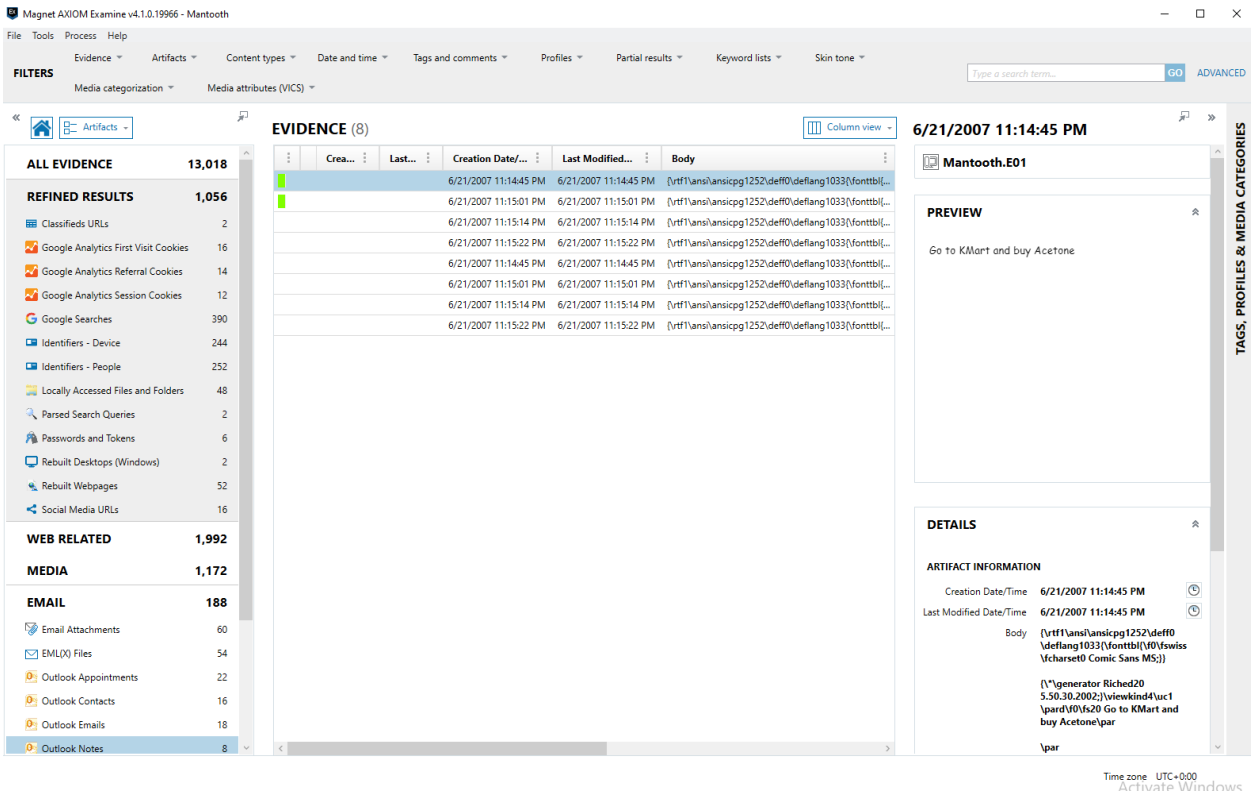

Figure 10.8

Figure 10.8 contains information about buying Acetone at Kmart.

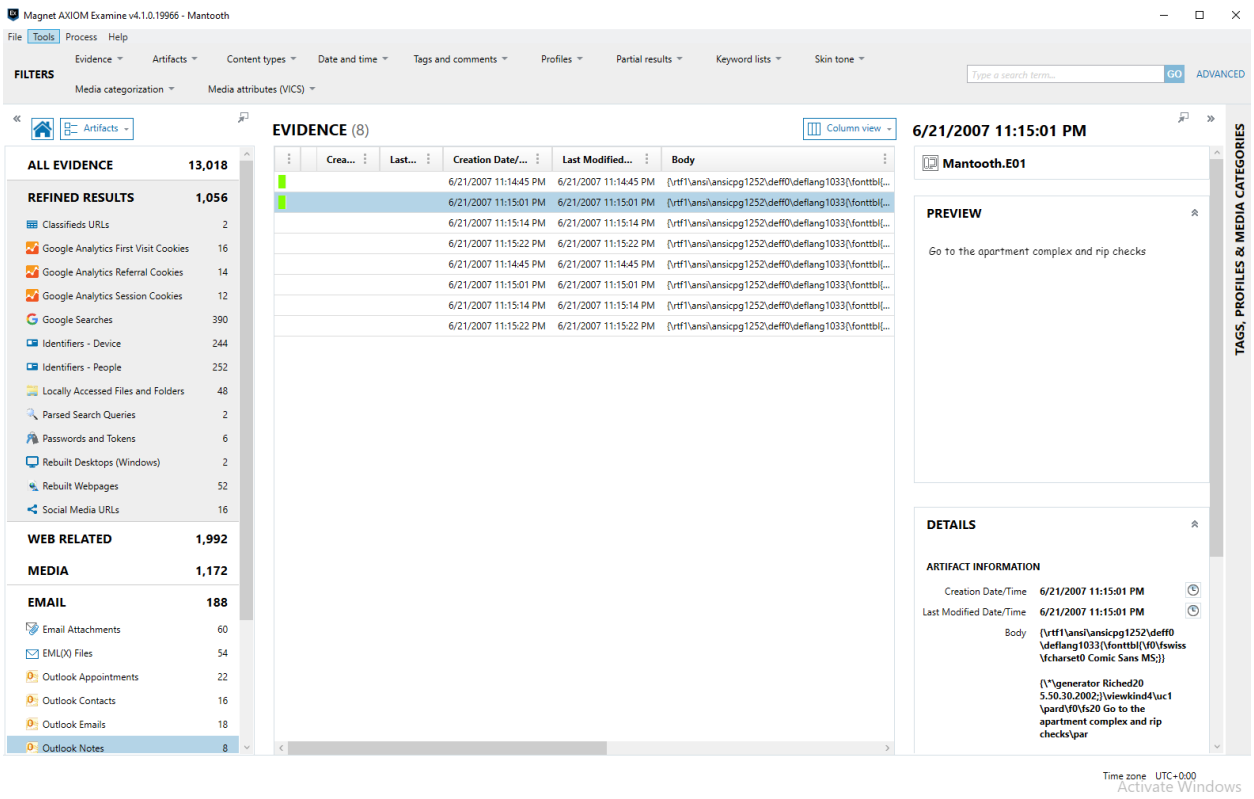

Figure 10.9

Figure 10.9 contains information about check ripping at an apartment complex.

Outlook Tasks

These note(s) contain information related to making meth, stealing checks, washing checks, pass checks, and making money. Figures 11.0 – 11.0

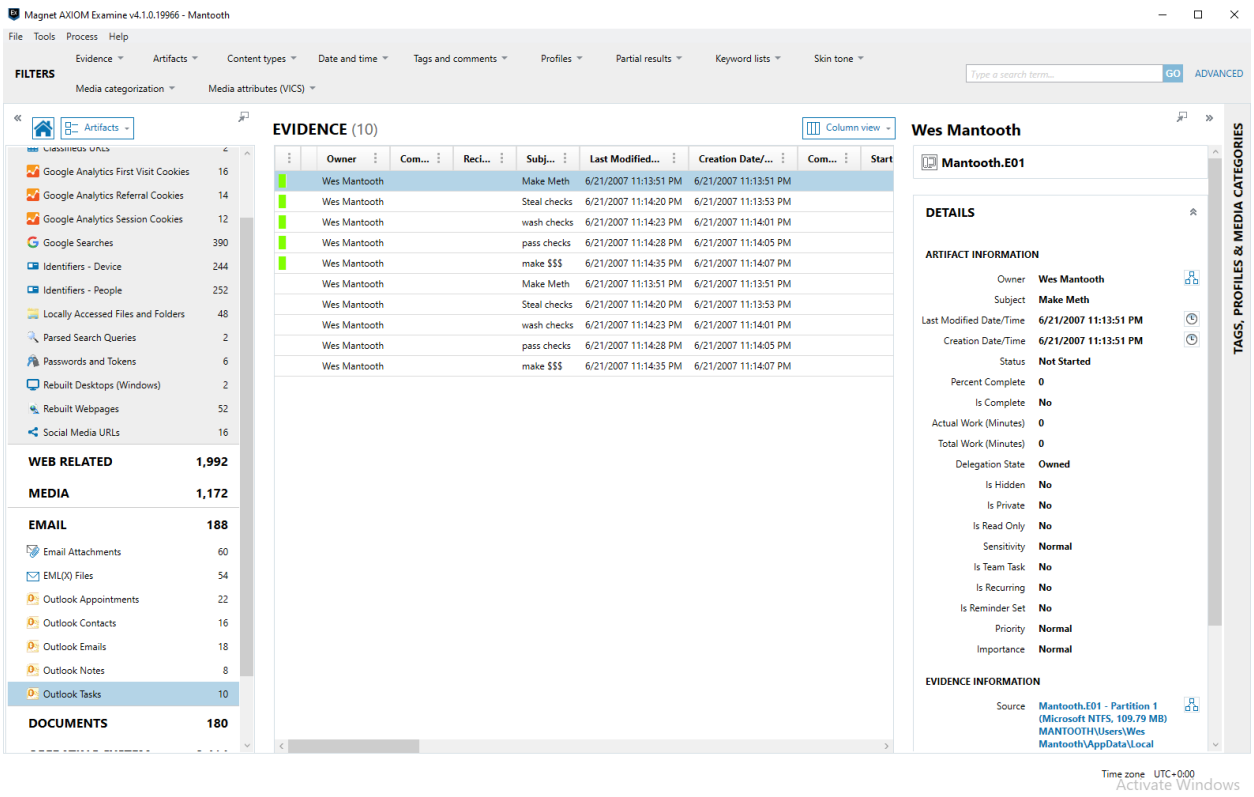

Figure 11.0

Documents

Excel Documents

These document(s) contain information about drugs sold to specific individuals, including what the drug was, who they are, and how much money it was. Figures 11.1 – 11.1

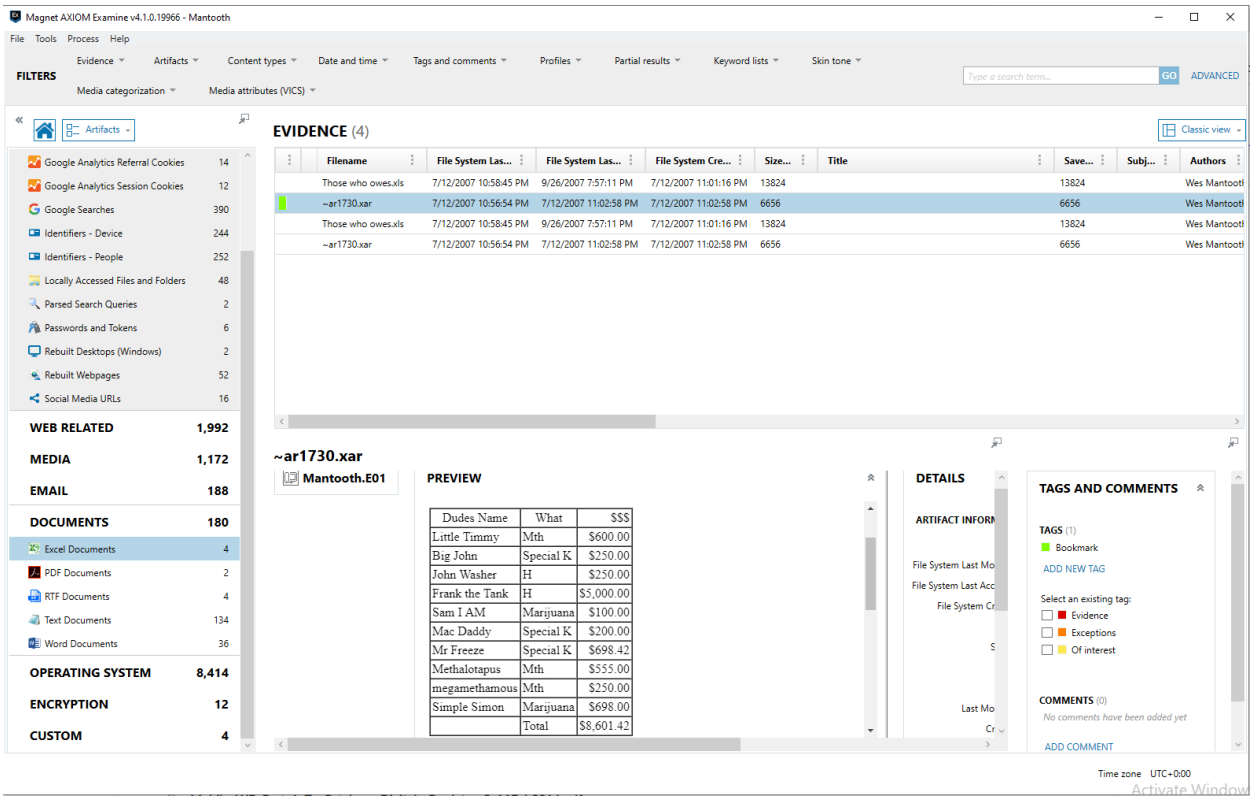

Figure 11.1

Text Documents

These text documents found on the image contain information related to drugs, drug advertising, passwords, and checks. Figures 11.2 – 12.0

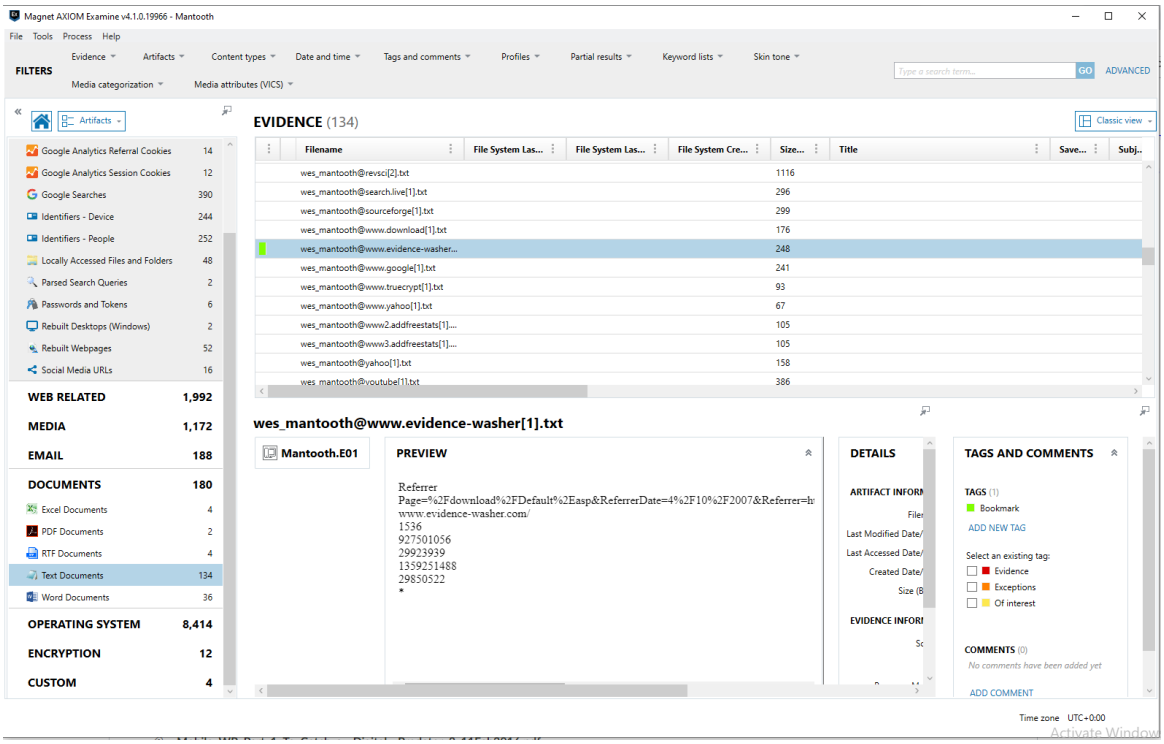

Figure 11.2

Figure 11.2 is a .txt file about evidence and references.

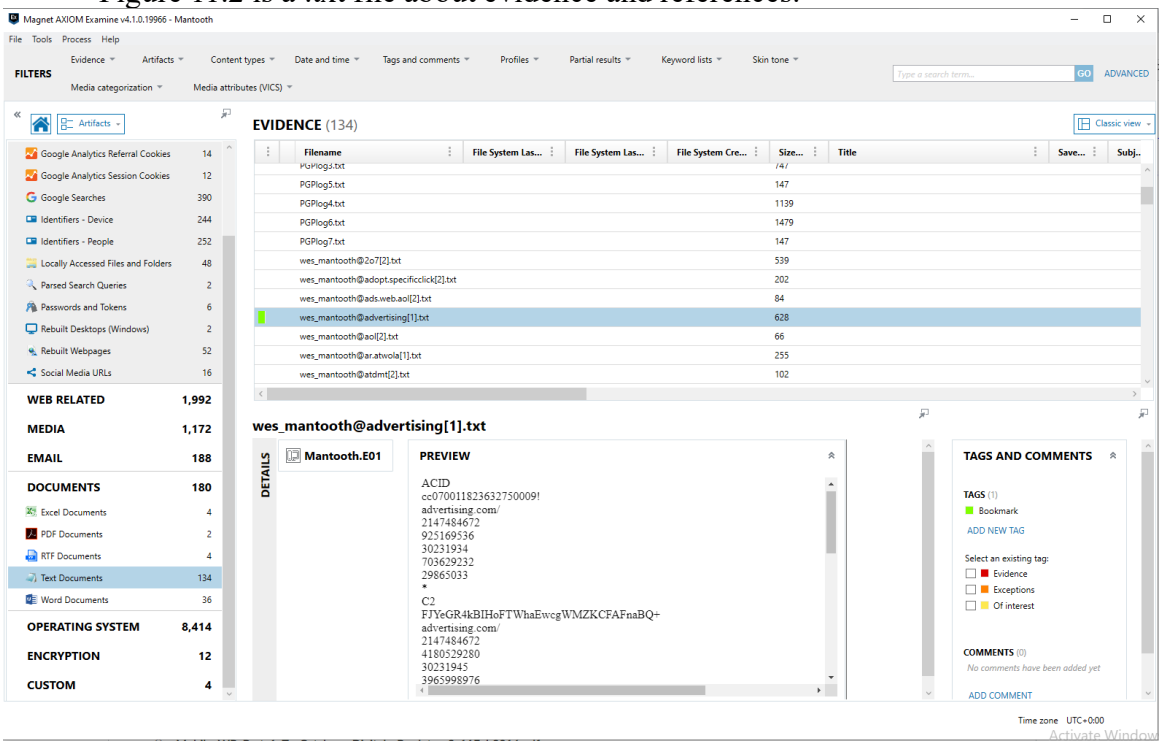

Figure 11.3

Figure 11.3 is an adverising board for his drugs.

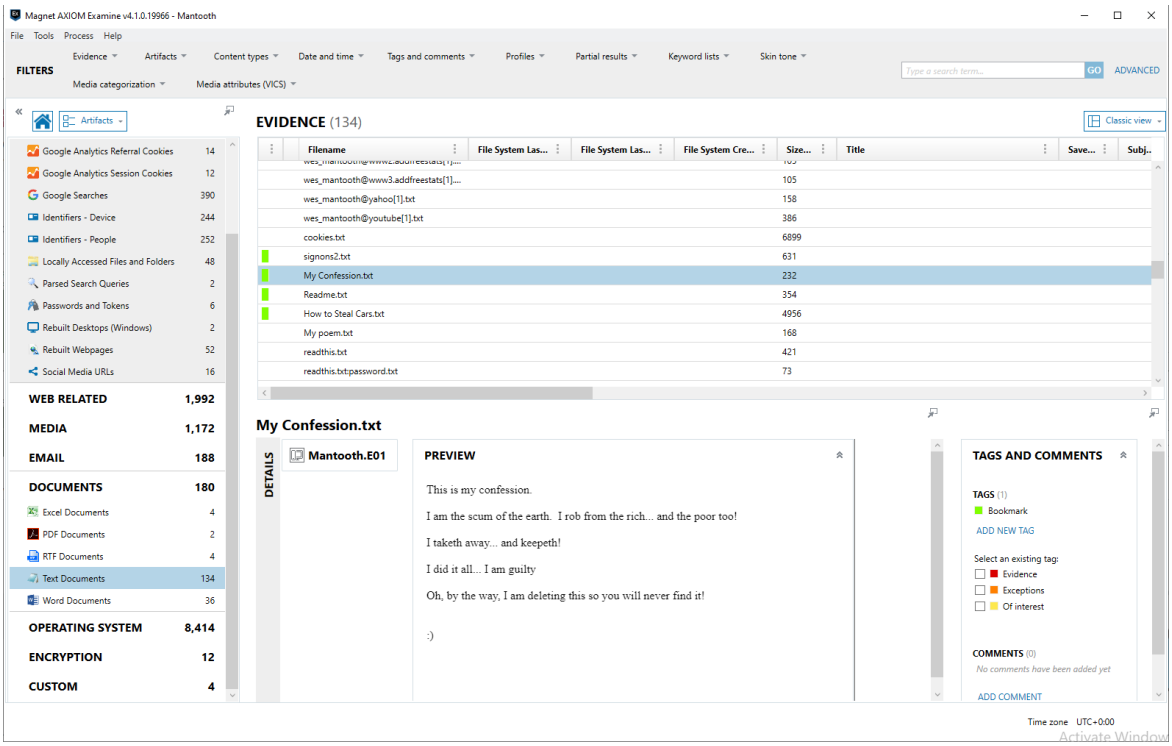

Figure 11.4

Figure 11.4 contains a confession .txt file about his crimes and how he is a bad person.

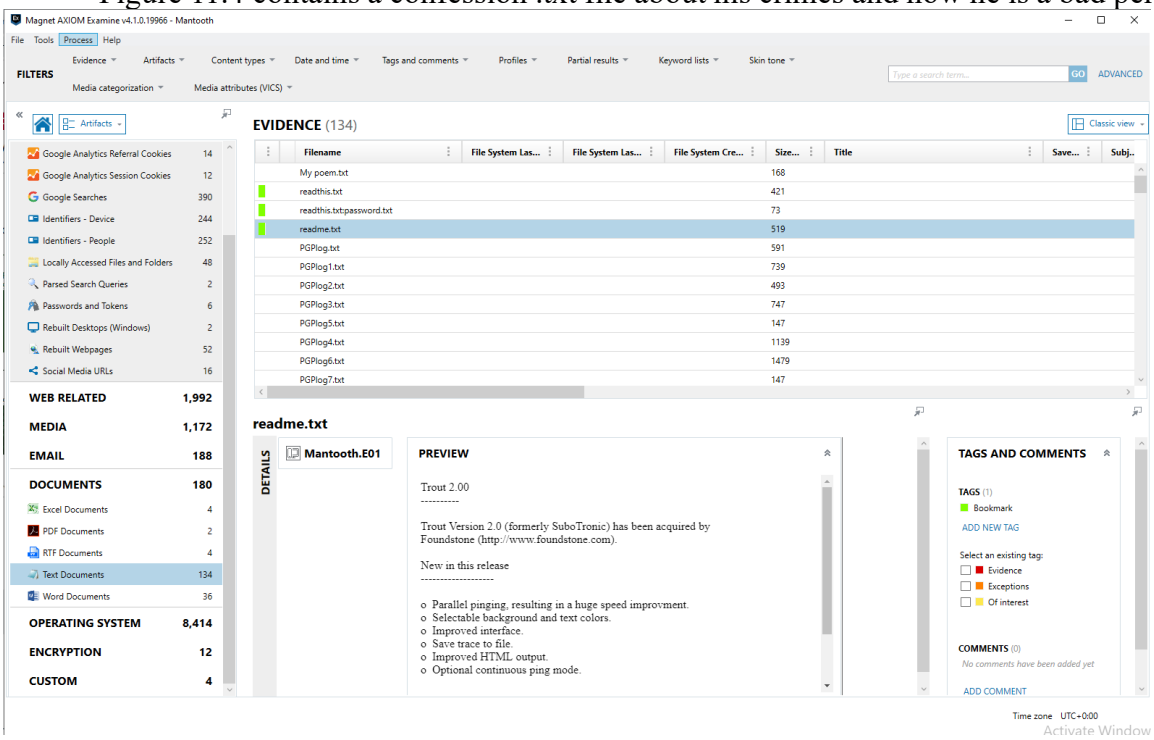

Figure 11.5

Figure 11.5 is a .txt file about the encryption software he is using.

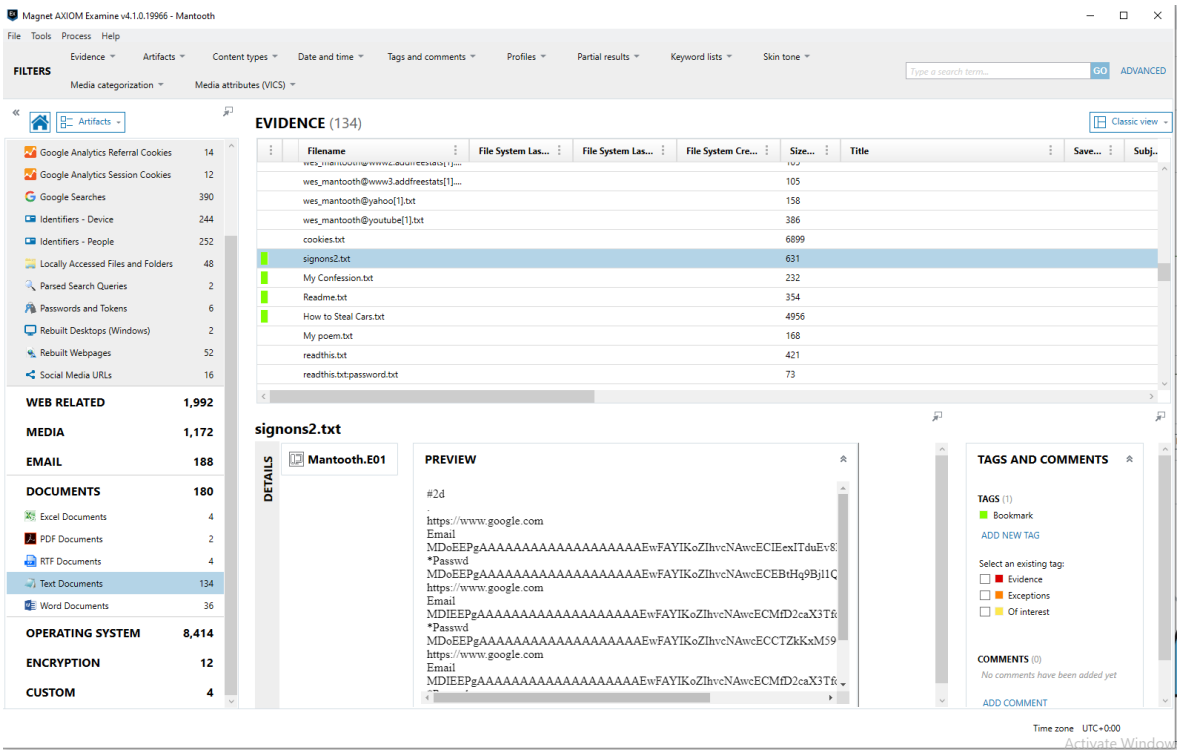

Figure 11.6

Figure 11.6 is a list of sign ons and passwords.

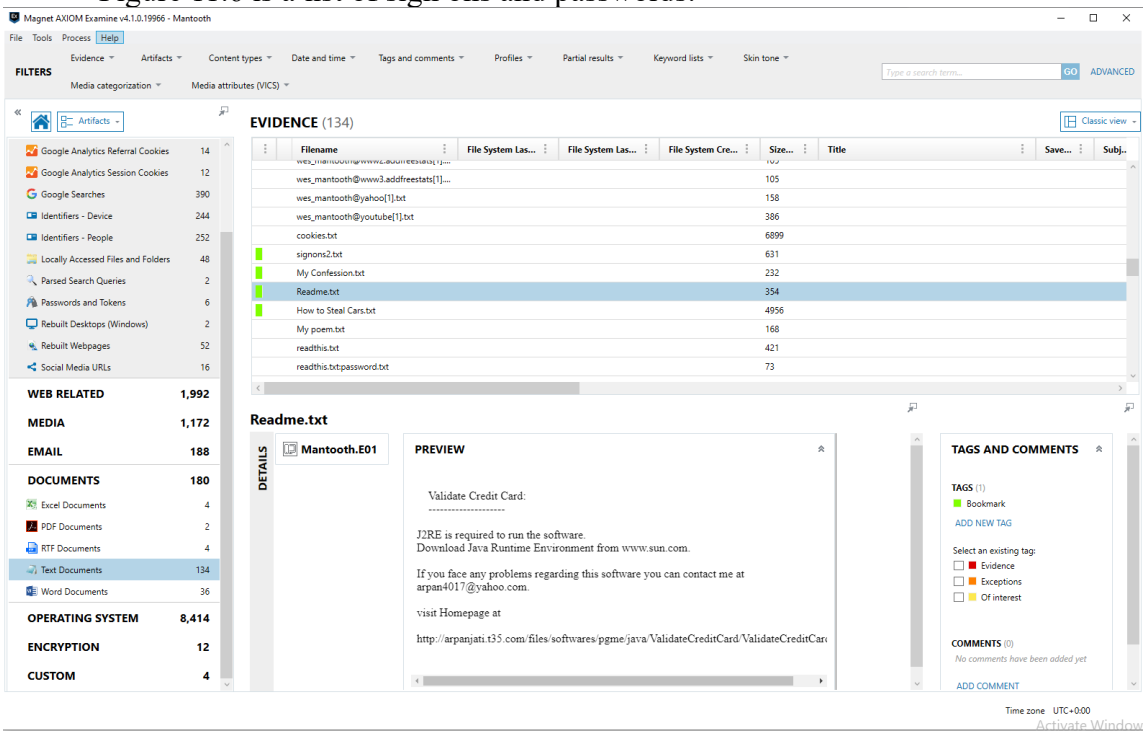

Figure 11.7

Figure 11.7 is a .txt file about validating fraudulent credit cards.

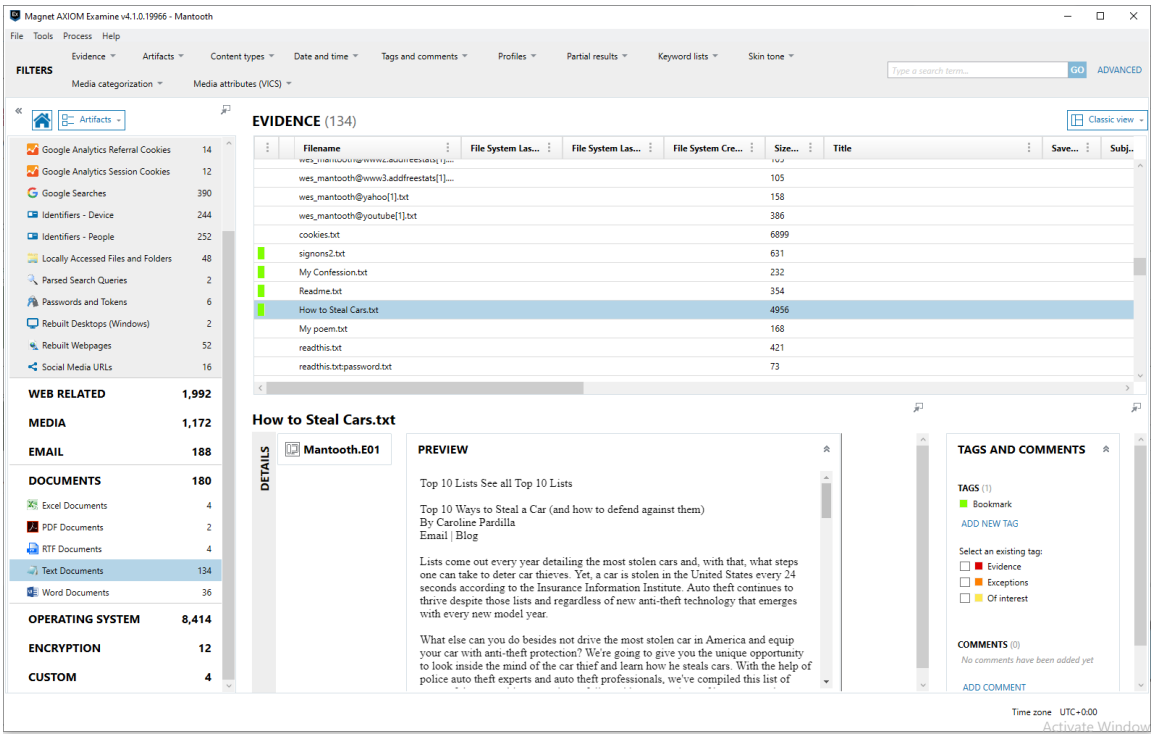

Figure 11.8

Figure 11.8 is a .txt file about stealing cars.

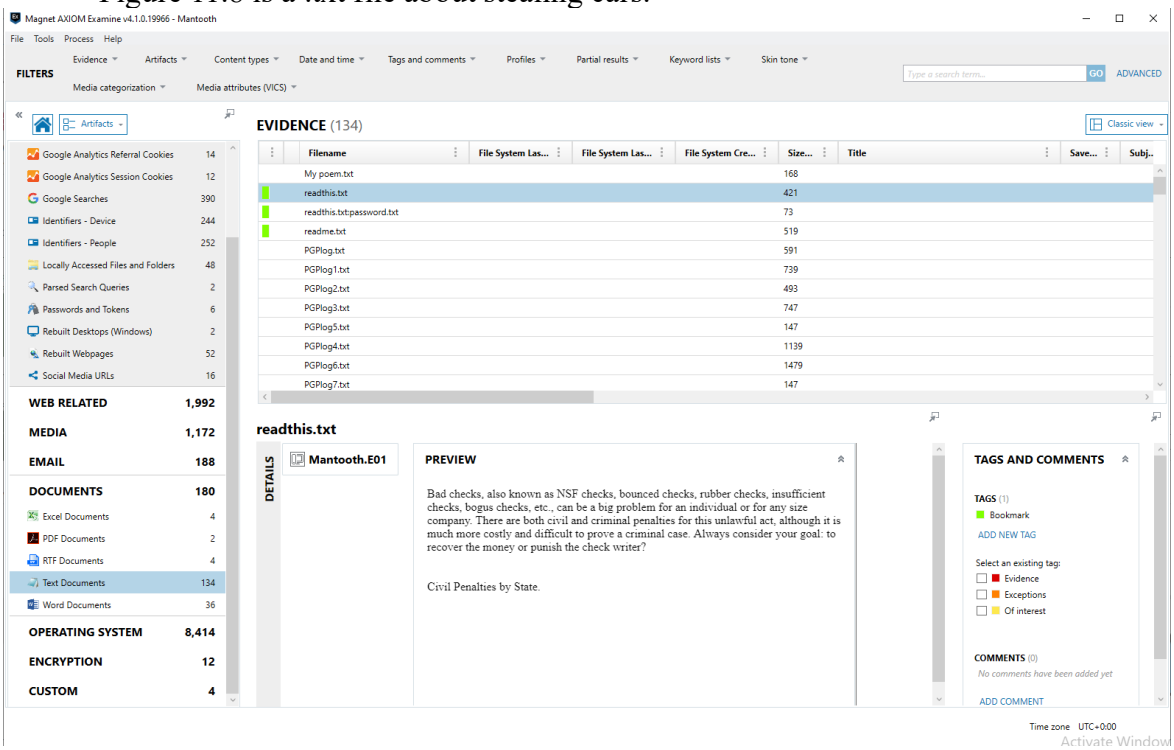

Figure 11.9

Figure 11.9 is a .txt file about bad checks.

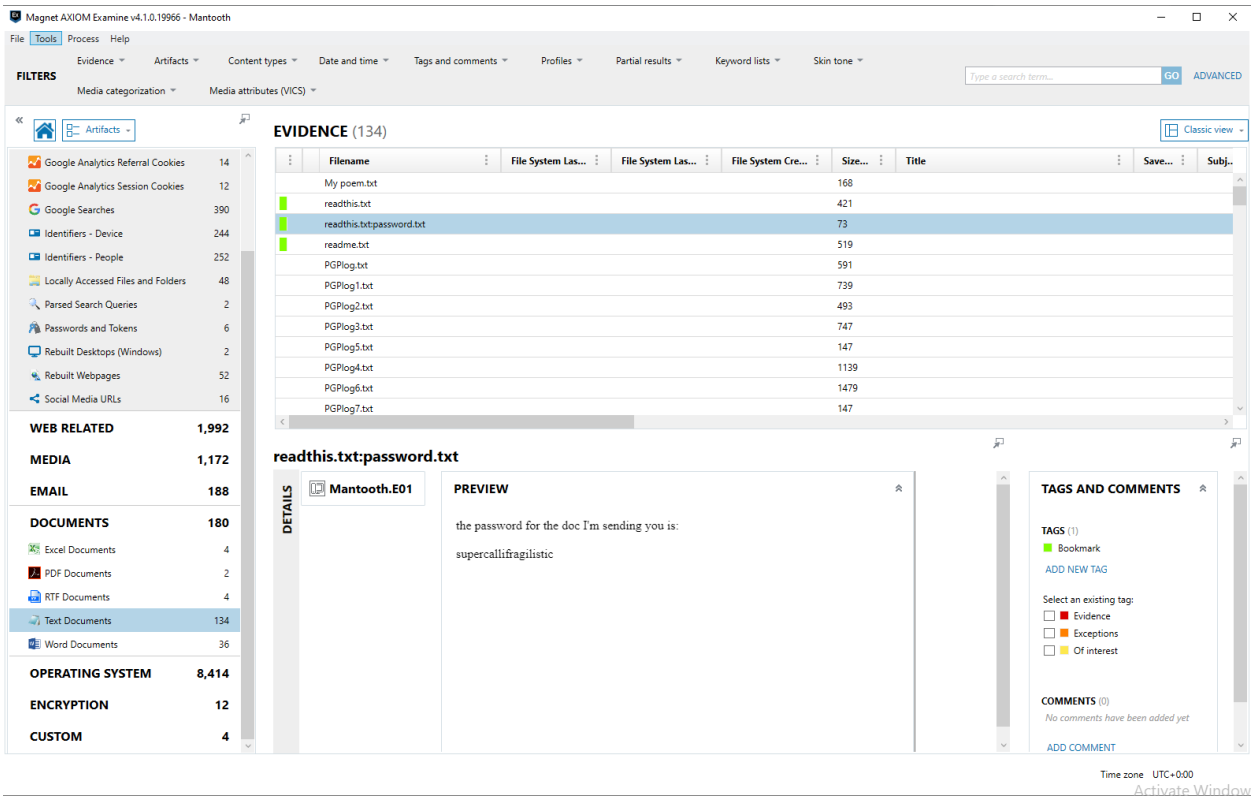

Figure 12.0

Figure 12.0 is a .txt file about his password which is supercalifragilistic.

Encryption.

This device does contain encryption tools. I was not able to access these files. There were fourteen encrypted files within this machine.

Conclusion

The image of the hard drive that I took was around thirty megabytes of information to process within both Forensic Explorer and Axiom Process.

The suspect in question is Wes Mantooth. On the laptop that we legally seized from Wes Mantooth there were multiple evidence files held on the device. The computer name is WESMANTOOTH-PC which is an indicator that he changed it himself to be his own name during the installation process.

When looking in the registry data there were multiple indicators that this laptop belonged to him. The time zone was set in Mountain Time Zone. Furthermore, located within the registry data there were multiple users such as Dracula, Wes Mantooth, Administrator, Guest, and Laurent.

When looking through Axiom I found evidence in the Web Search history for information related to drug searches, where to find drugs, how to steal ATMs, how to steal credit cards, selling meth, making meth, and other various illegal activity related searches.

From looking at Axiom I also found evidence within the photos located on this device. There were numerous photos of meth labs, people smoking meth, the process of creating meth, other various drugs such as Hawaiian ruler, pills, etc. There were also pictures of fraudulent credit cards, cashier's checks, and ATM hacking. Furthermore, located on this device were images of what can be assumed to be Wes Mantooth's family, photographs of him, and email attachments between him and his family, identifying that this laptop belonged to him.

There were also various emails that indicated he was selling drugs such as meth to these email contacts. There is multiple evidence files located within the email of his that identify him as the one selling these drugs and when these individuals could get more of these drugs.

There were also a few text files such as one particular one that showed who he was selling these drugs to, what type of drugs they were, and how much money he made from selling drugs to these individuals. There was also one .txt file named My Confession.txt in which he confessed to his crimes in figure 11.4.

This case was very in-depth and interesting. There was numerous evidence files located on this image. It appears Wes Mantooth was not actively trying to hide the evidence of him making and distributing drugs. The numerous email files, the photographs pertaining to him, as well as the registry data all points to him being guilty of these charges.

Appendix of Terms

Hard Drive – A piece of physical hardware that stores information in a combination of 1's and 0's.

Hash File – a digital fingerprint of each and every file.

HIVE – It is found only within the Windows operating system and has groups of information that only could be found on your computer.

Imaging a drive – A bit-by-bit copy of the original contents of a hard drive.

Internet Explorer – A web browser designed by Microsoft.

IP Address – Internet Protocol that each device is assigned and has a unique value to allow access onto the internet.

Mail Client – a program used by your computer to connect to your email. Ex: Outlook.

Operating System – The software on your computer that handles processes and memory. The three main ones are Windows, MacOS, and Linux.

Registry – Where all configuration settings are held.

Sterile Hard Drive – A hard drive that is wiped to all 0's and confirmed clean.

URL – Uniform Resource Locator, it is a web address that can be accessed.

USB – Universal Serial BUS, a serial connection that different devices can use, generally external.

Write Blocker – Software or physical piece of equipment that only allows information to be read-only.

References

Callaghan, P. (2020, August 6). *Why Hash Values Are Crucial in Evidence Collection & Digital Forensics*. Blog.pagefreezer.com. https://blog.pagefreezer.com/importance-hash-values-evidence-collection-digital-forensics#:~:text=In%20simple%20terms%2C%20a%20hash