

MANTOOTH Investigation

Ferris State University

DFOR 310

Zachary C. Schulte

## Table of Contents

<b>Introduction .....</b>	<b>3</b>
<b>Imaging the Hard Drive.....</b>	<b>3</b>
<b>FTK Imager .....</b>	<b>3</b>
<b>Presentation of Evidence .....</b>	<b>8</b>
<b>Forensic Explorer .....</b>	<b>8</b>
<b>Registry.....</b>	<b>11</b>
<b>Security Accounts Manger.....</b>	<b>12</b>
<b>System.....</b>	<b>16</b>
<b>Software.....</b>	<b>29</b>
<b>NTUser.Dat.....</b>	<b>43</b>
<b>Disk Structure .....</b>	<b>59</b>
<b>Partition Size .....</b>	<b>59</b>
<b>Format.....</b>	<b>59</b>
<b>Active File Review .....</b>	<b>59</b>
<b>Axiom.....</b>	<b>59</b>
<b>Web Related.....</b>	<b>61</b>
<b>Media.....</b>	<b>68</b>
<b>Documents.....</b>	<b>109</b>
<b>Encryption.....</b>	<b>115</b>
<b>Conclusion .....</b>	<b>116</b>
<b>Appendix of Terms .....</b>	<b>118</b>
<b>References .....</b>	<b>119</b>

## **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.

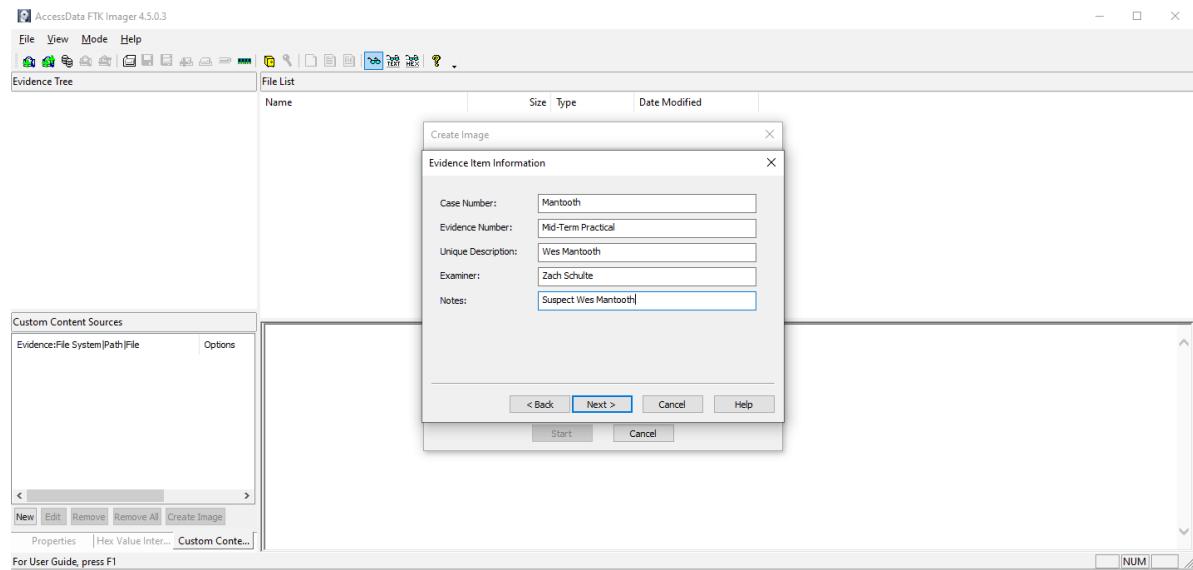


Figure 1.0

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

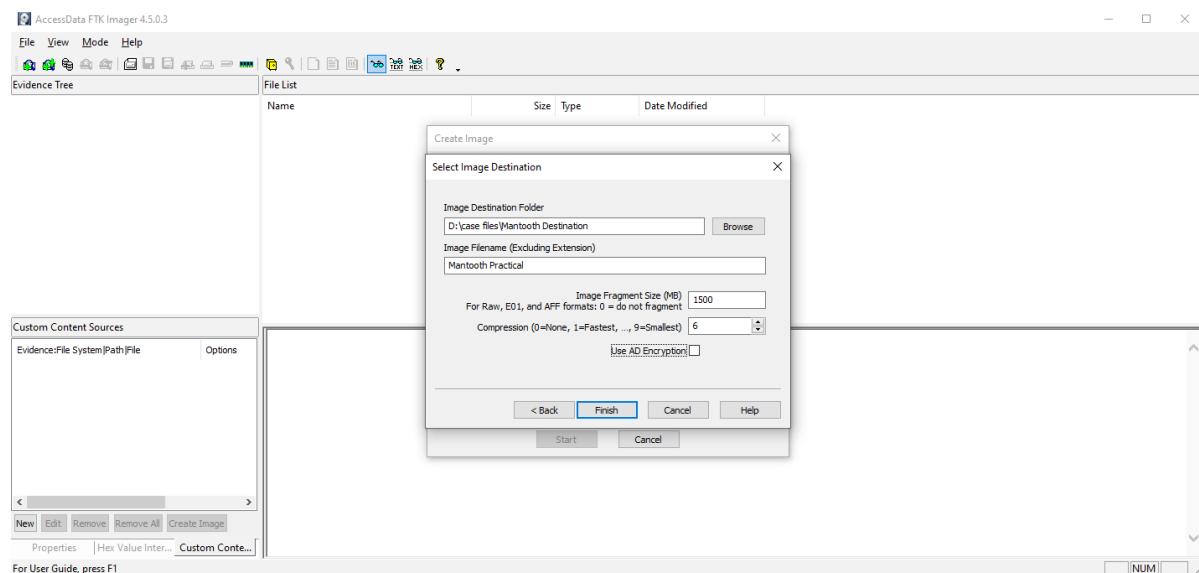


Figure 1.1

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

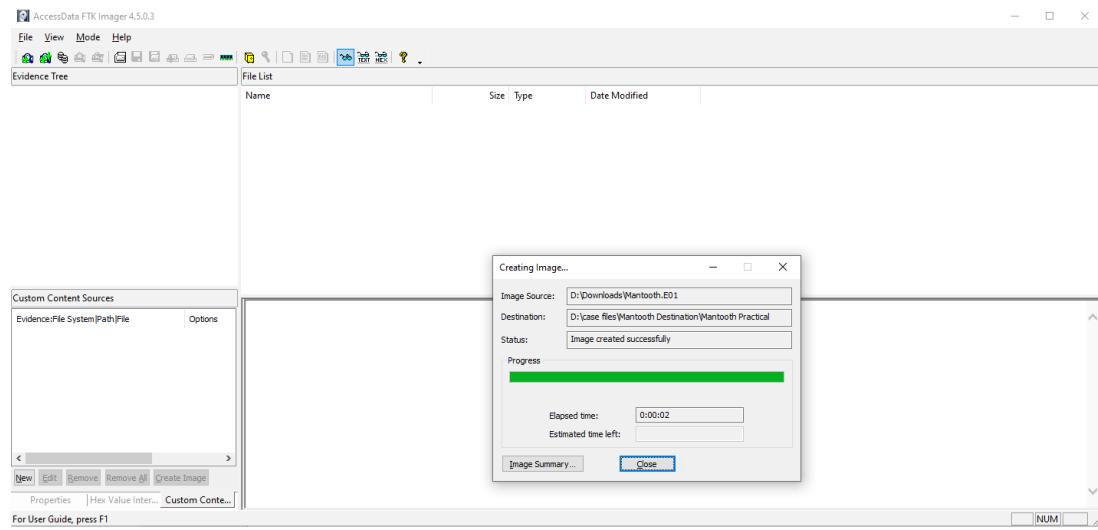


Figure 1.2

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.

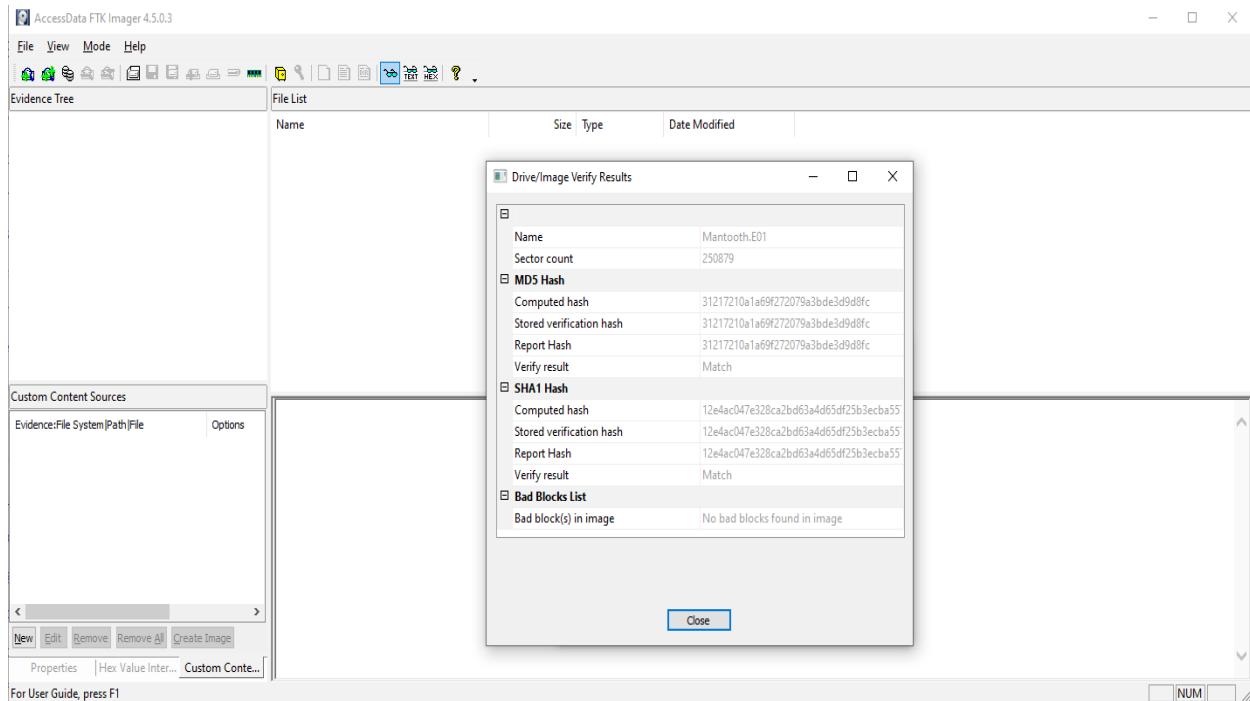


Figure 1.4

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.

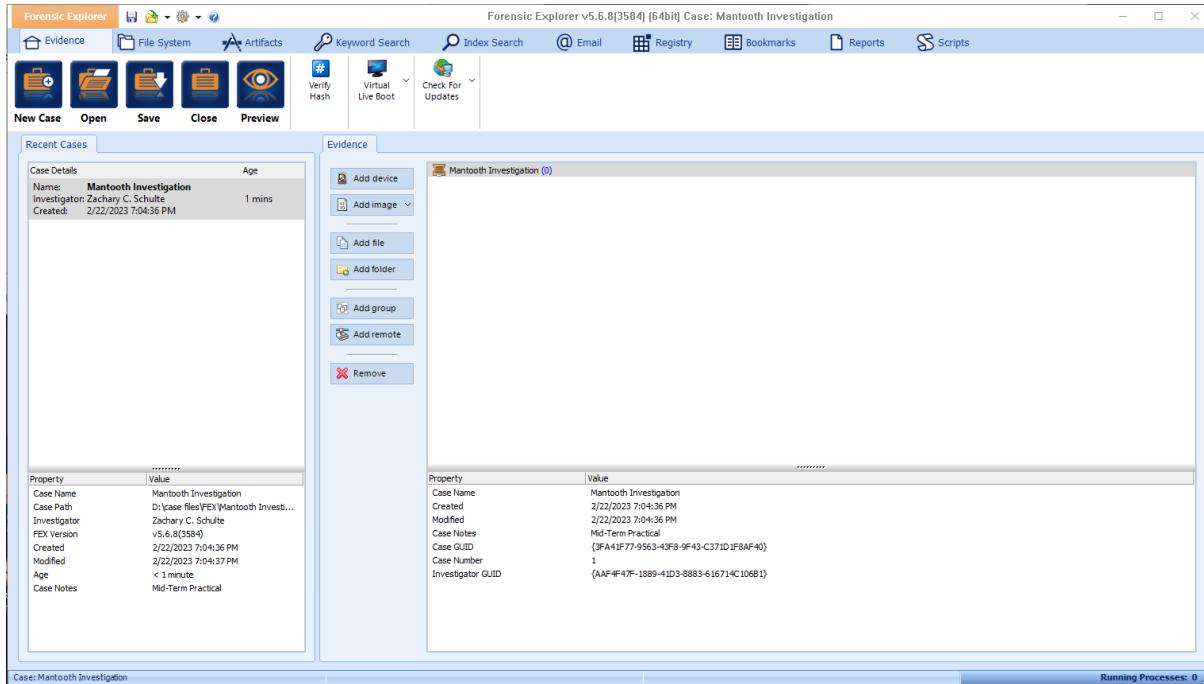


Figure 1.5

Figure 1.5 shows the opening of Forensic Explorer.

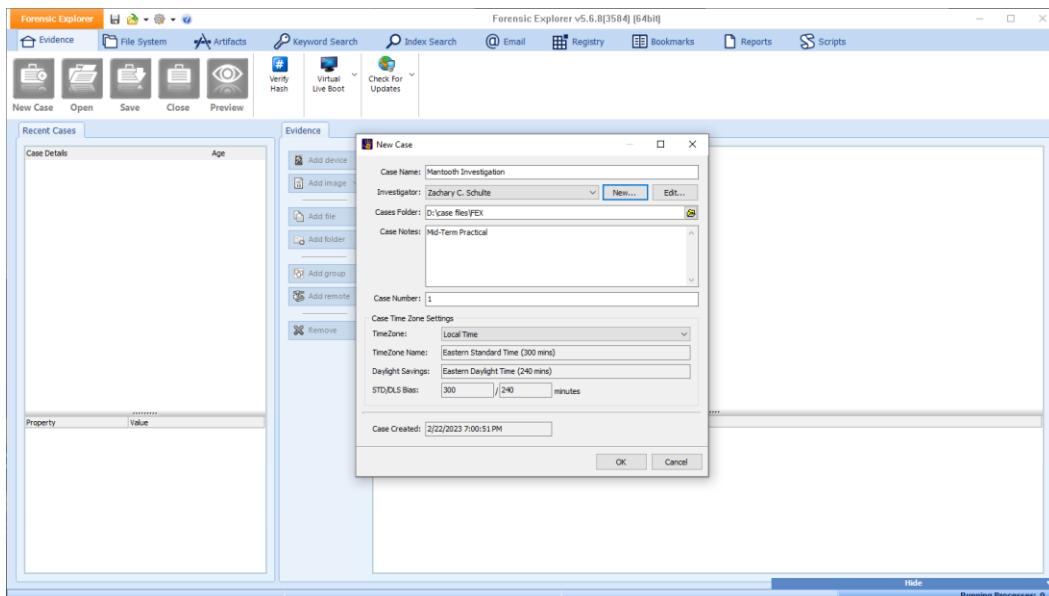


Figure 1.6

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

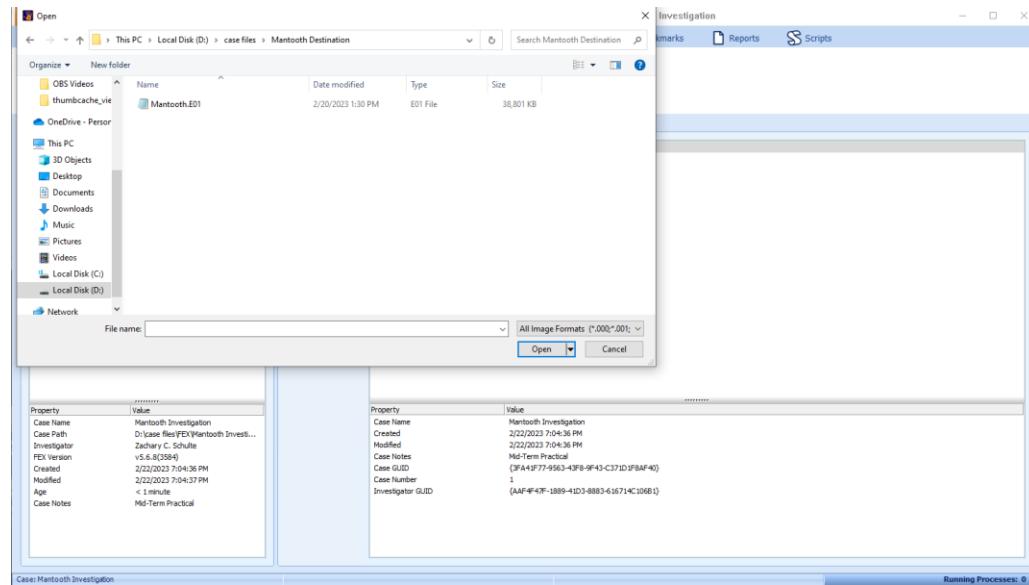


Figure 1.7

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

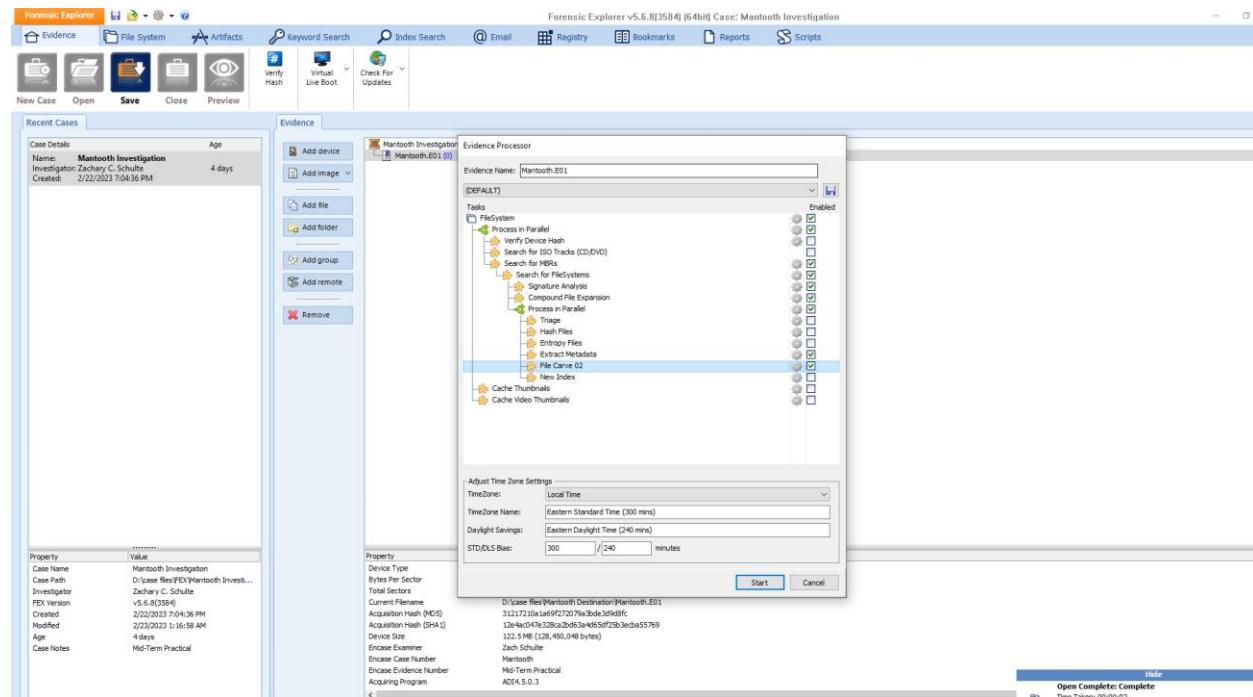


Figure 1.8

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.

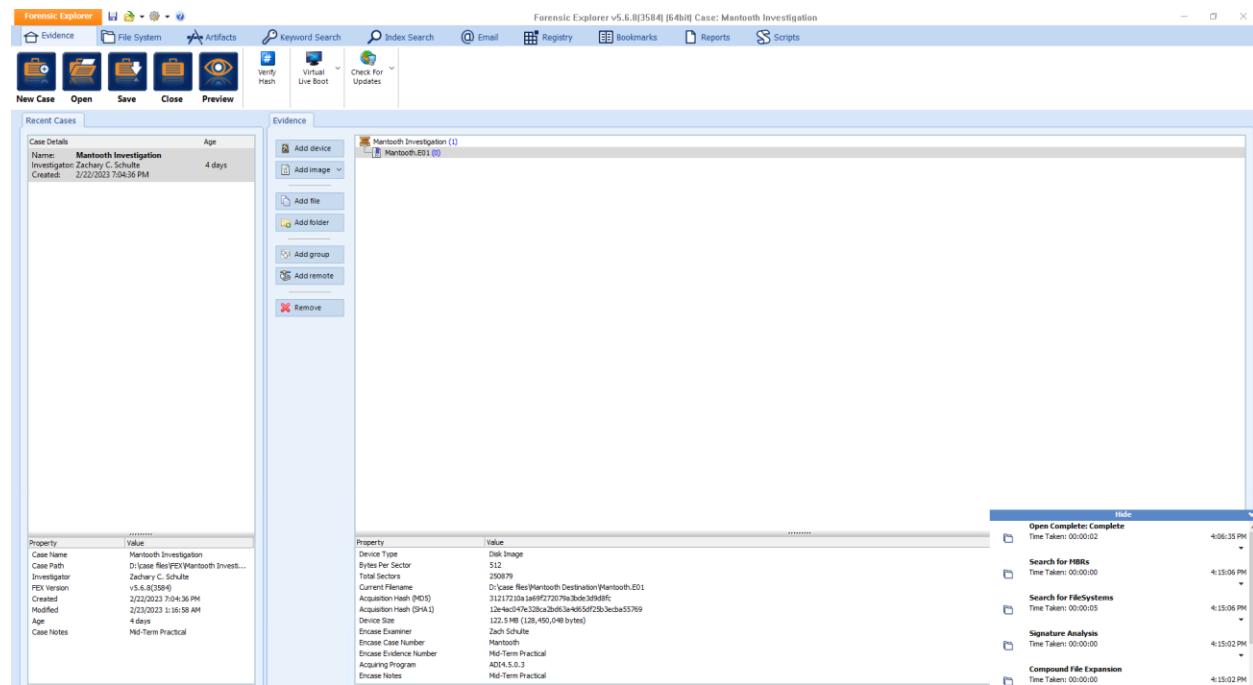


Figure 1.9

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

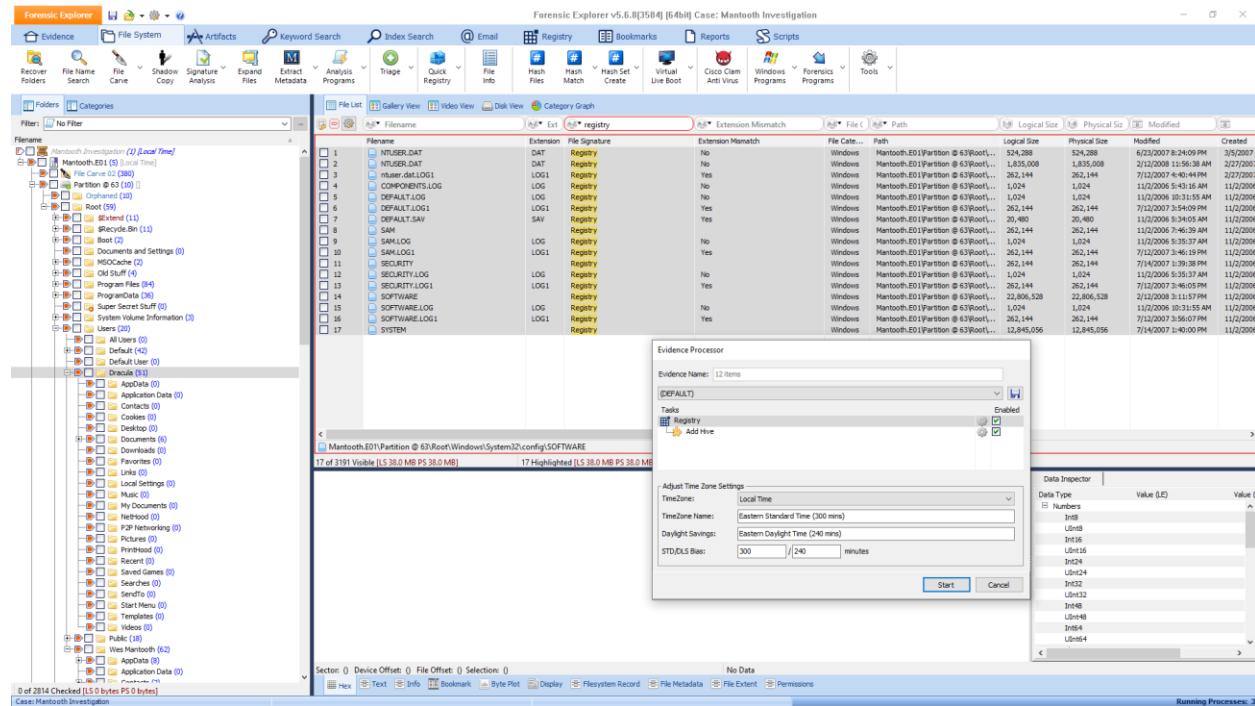


Figure 2.0

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	WESMANTOOOTH-PC

---

---

Key Found:

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

Value	Data
~~~~~	~~~~~
ComputerName	WESMANTOOOTH-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	0xFFFFFFF4
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	0xFFFFFFF4
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\_USB  
20&Rev\_1000\6&6b8c30&0&AA14012714842&0

---

USB Device 3:

Friendly Name: Flash Drive SM\_USB20 USB Device  
Serial Number: AA14012714842&0  
Device Type: Disk

Vendor Name: Flash  
Vendor ID: 090C  
Product Name: Drive\_SM\_USB20  
Product ID: 1000  
Revision: 1000  
First Connected (setupapi): {Never}  
Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]  
Last Connected (MountPoints2): 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\_USB  
20&Rev\_1000\AA14012714842&0

---

#### USB Device 4:

Friendly Name: Flash Drive UT\_USB20 USB Device  
Serial Number: 000000000C80F&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\000000000C80F&0

---

USB Device 5:

Friendly Name: Flash Drive UT\_USB20 USB Device  
Serial Number: 000000000C9BA&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\000000000C9BA&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\_G  
3&Rev\_2.20\23090525338296&0

---

#### USB Device 13:

Friendly Name: TREK TD2SMART G3M USB Device  
Serial Number: 10120515511949&0  
Device Type: Disk  
Vendor Name: TREK  
Vendor ID: 0A16  
Product Name: TD2SMART\_G3M  
Product ID: 9005  
Revision: 2.40  
First Connected (setupapi): {Never}  
Connected After Reboot (USBSTOR): 14-Jul-2007 17:56:41 [UTC]  
Last Connected (MountPoints2): 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\_G  
3M&Rev\_2.40\10120515511949&0

---

USB Device 14:

Friendly Name:

Serial Number: 10120516721518&0

Device Type: Disk

Vendor Name: TREK

Vendor ID: 0A16

Product Name: TD2SMART\_G3M

Product ID: 9005

Revision: 2.40

First Connected (setupapi): {Never}

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

Last Connected (MountPoints2): {Never}

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

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

~~~~~

Source: Mantooth.E01\Partition @ 63\Root\Windows\System32\config\SYSTEM >  
SYSTEM\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven\_TREK&Prod\_TD2SMART\_G  
3M&Rev\_2.40\10120516721518&0

---

USB Device 15:

Friendly Name: USB 2.0 Flash Disk USB Device

Serial Number: 6&2507d51a&0&AA1000000000623&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&AA1000000000623&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 27<sup>th</sup>, 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\ActiveTouchMeeting Client\

Value	Data
~~~~~	~~~~~
DisplayName	WebEx
Publisher	WebEx Communications, Inc
URLInfoAbout	<a href="http://www.webex.com">http://www.webex.com</a>

---

---

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	<a href="http://www.realvnc.com">http://www.realvnc.com</a>

---

-----

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

Value	Data
~~~~~	~~~~~
DisplayName	Adobe Flash Player 9 ActiveX
DisplayVersion	9
Publisher	Adobe Systems

---

Key Found:

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

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

---

Key Found:

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

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

---

Key Found:

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

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

---

-----

Key Found:

Mantooth.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinRAR archiver\

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

---

-----

Key Found:

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

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

---

-----

Key Found:

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

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

---

-----

Key Found:

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

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

DisplayName	Yahoo! Internet Mail
-------------	----------------------

---

---

Key Found:

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

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

---

---

Key Found:

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

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

---

---

Key Found:

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

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

---

---

Key Found:

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

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

---

~~~~~

|                |                                                                   |
|----------------|-------------------------------------------------------------------|
| DisplayName    | AccessData DNA 3 Worker                                           |
| DisplayVersion | 3.3                                                               |
| Publisher      | AccessData                                                        |
| URLInfoAbout   | <a href="http://www.accessdata.com">http://www.accessdata.com</a> |

---

~~~~~

Key Found:

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

Value

Data

---

~~~~~

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

---

~~~~~

Key Found:

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

Value

Data

---

~~~~~

|                |                        |
|----------------|------------------------|
| DisplayName    | Windows Live Messenger |
| DisplayVersion | 8.1.0178.00            |
| Publisher      | Microsoft Corporation  |
| URLInfoAbout   |                        |

---

~~~~~

Key Found:

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

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

---

Key Found:

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

Value	Data
~~~~~	~~~~~
DisplayName	Adobe Reader 8
DisplayVersion	8.0.0
Publisher	Adobe Systems Incorporated
URLInfoAbout	<a href="http://www.adobe.com">http://www.adobe.com</a>

---

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\RecentDo  
cs\.bek\

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

---

---

Key Found:

Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDo  
cs\.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_.نفیصته.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\RecentDo  
cs\.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\RecentDo  
cs\.html\

Value	Data
~~~~~	~~~~~
0	165183.html,File
MRUListEx	0

---

-----  
-----

Key Found:

Mantooth.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDo  
cs\.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\_نیصتہ.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\RecentDo  
cs\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                  | MANTOOOTH (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\RecentDo  
cs\

| Value     | Data                                                                                                                                                                                                                                                                                                               |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ~~~~~     | ~~~~~                                                                                                                                                                                                                                                                                                              |
| MRUListEx | 100 101 20 99 81 71 75 74 98 4 55 15 32 97 96 54 10 6 95 9<br>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<br>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<br>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.

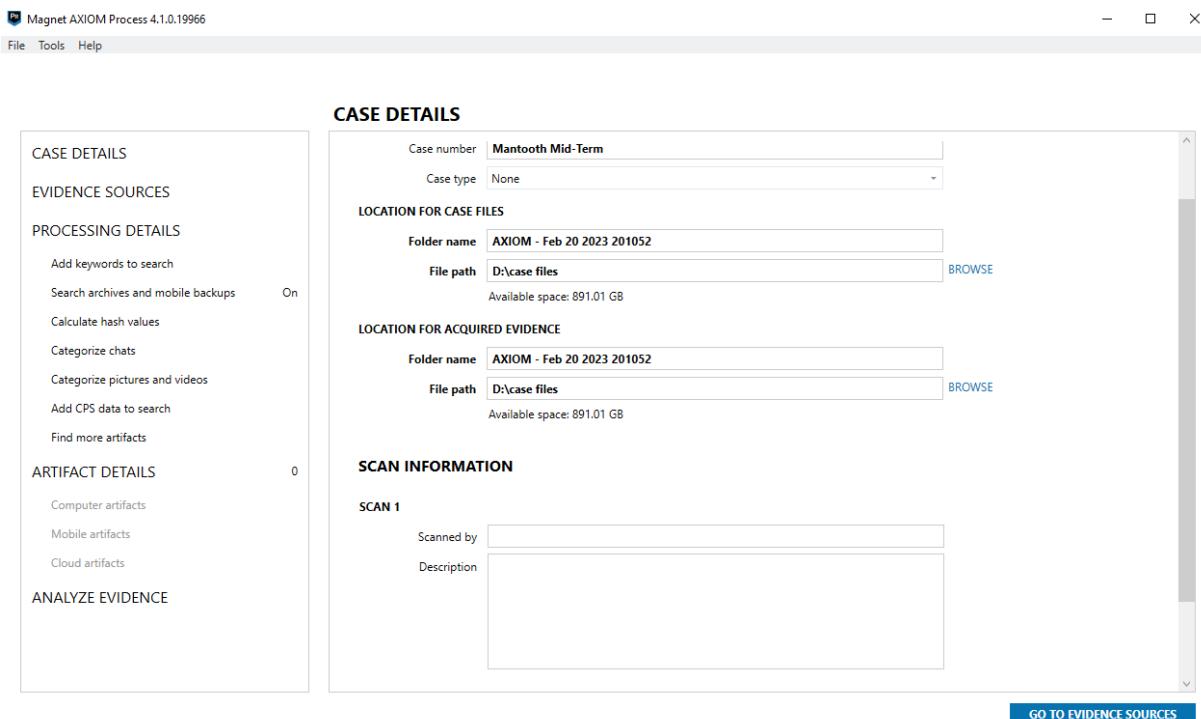


Figure 2.1

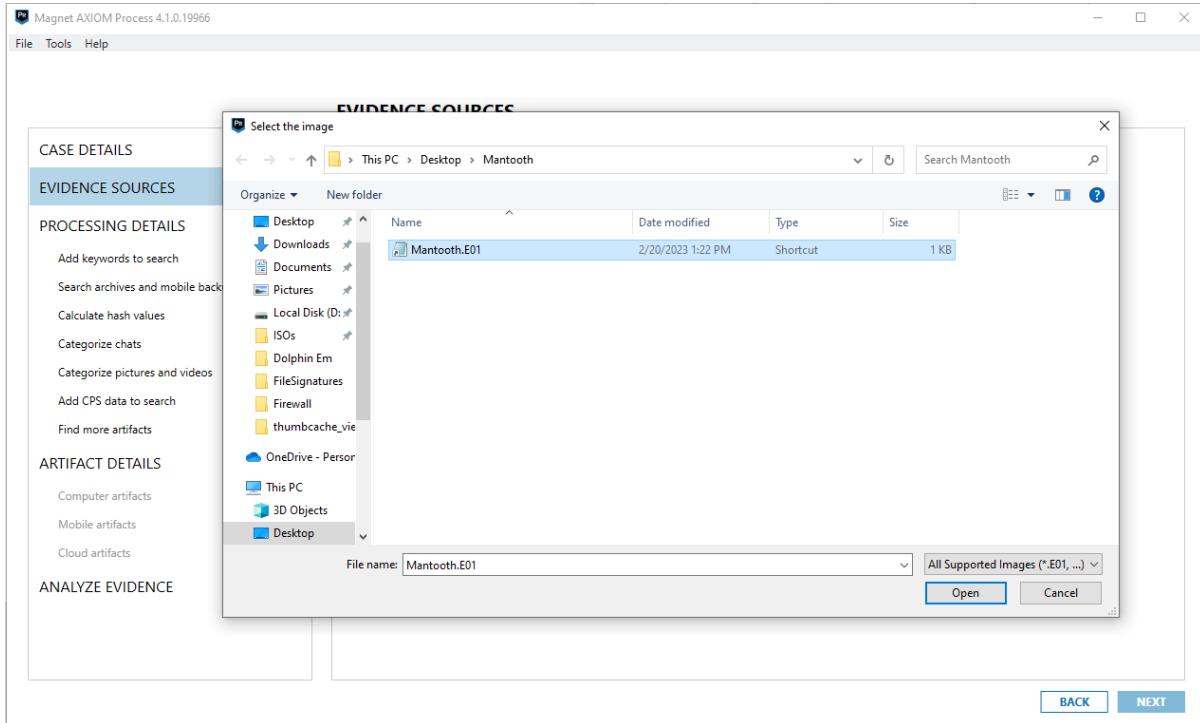


Figure 2.2

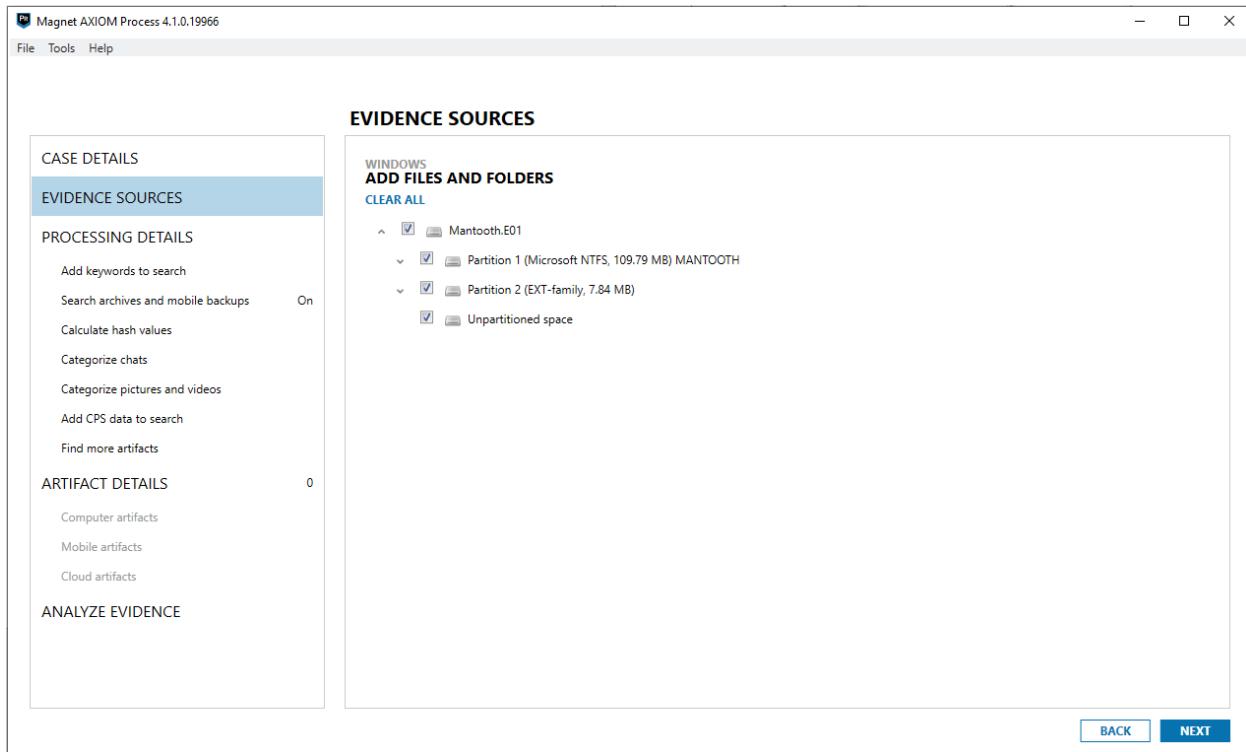


Figure 2.3

## 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.

**EVIDENCE (242)**

| URL                                                  | User         | Last Visited Date     | Last Visited (2...)   | Visit |
|------------------------------------------------------|--------------|-----------------------|-----------------------|-------|
| http://www.google.com                                | Wes Mantooth | 7/12/2007 11:12:16 PM | 7/12/2007 11:12:16 PM | 2     |
| http://www.snopes.com/fraud/atm/atmcamera.asp        | Wes Mantooth | 7/12/2007 11:13:19 PM | 7/12/2007 11:13:19 PM | 1     |
| http://www.snopes.com/crime/warnings/atmcamera...    | Wes Mantooth | 7/12/2007 11:13:16 PM | 7/12/2007 11:13:16 PM | 1     |
| file:///E/Business Ideas/unitled.bmp                 | Wes Mantooth | 7/12/2007 11:14:17 PM | 7/12/2007 11:14:17 PM | 1     |
| file:///E/Business Ideas/Guts.bmp                    | Wes Mantooth | 7/12/2007 11:14:53 PM | 7/12/2007 11:14:53 PM | 1     |
| http://basalemedia.com/V2/44508/86958/index.htm...   | Wes Mantooth | 7/12/2007 11:15:00 PM | 7/12/2007 11:15:00 PM | 1     |
| file:///E/Business Ideas/Camera.bmp                  | Wes Mantooth | 7/12/2007 11:15:11 PM | 7/12/2007 11:15:11 PM | 1     |
| http://www.tots.e.com/tots.e...                      | Wes Mantooth | 7/12/2007 11:16:04 PM | 7/12/2007 11:16:04 PM | 1     |
| http://images.google.com/images?um=1&tab=wi&...      | Wes Mantooth | 7/12/2007 11:15:24 PM | 7/12/2007 11:15:24 PM | 1     |
| http://www.google.com/search?hl=en&q=atm+card...     | Wes Mantooth | 7/12/2007 11:15:34 PM | 7/12/2007 11:15:34 PM | 3     |
| http://www.neonjoin.com/drug_recipes/chapter3.h...   | Wes Mantooth | 7/12/2007 11:15:52 PM | 7/12/2007 11:15:52 PM | 1     |
| http://www.google.com/search?hl=en&q=making+...      | Wes Mantooth | 7/12/2007 11:16:01 PM | 7/12/2007 11:16:01 PM | 2     |
| http://www.tots.e.com/en/drugs/speedy_drugs/how...   | Wes Mantooth | 7/12/2007 11:16:04 PM | 7/12/2007 11:16:04 PM | 1     |
| http://img376.imageshack.us/img376/8880/washing...   | Wes Mantooth | 7/12/2007 11:17:44 PM | 7/12/2007 11:17:44 PM | 1     |
| http://www.physorg.com/physorg...                    | Wes Mantooth | 7/12/2007 11:16:22 PM | 7/12/2007 11:16:22 PM | 1     |
| http://www.physorg.com/news99637614.html             | Wes Mantooth | 7/12/2007 11:16:23 PM | 7/12/2007 11:16:23 PM | 1     |
| http://www.google.com/search?hl=en&q=making+...      | Wes Mantooth | 7/12/2007 11:16:33 PM | 7/12/2007 11:16:33 PM | 4     |
| http://images.google.com/images?um=1&tab=wi&...      | Wes Mantooth | 7/12/2007 11:17:08 PM | 7/12/2007 11:17:08 PM | 2     |
| http://www.sccja.org/images/csid_meth1.jpg           | Wes Mantooth | 7/12/2007 11:17:02 PM | 7/12/2007 11:17:02 PM | 1     |
| http://images.google.com/imgres?imgurl=http://ww...  | Wes Mantooth | 7/12/2007 11:17:06 PM | 7/12/2007 11:17:06 PM | 1     |
| http://images.google.com/images?q=making+meth...     | Wes Mantooth | 7/12/2007 11:17:06 PM | 7/12/2007 11:17:06 PM | 2     |
| http://images.google.com/images?svnum=10&um=...      | Wes Mantooth | 7/12/2007 11:17:36 PM | 7/12/2007 11:17:36 PM | 2     |
| http://www.google.com/search?hl=en&q=check+washin... | Wes Mantooth | 7/12/2007 11:17:30 PM | 7/12/2007 11:17:30 PM | 1     |
| http://images.google.com/images?q=check+washin...    | Wes Mantooth | 7/12/2007 11:17:35 PM | 7/12/2007 11:17:35 PM | 2     |
| file:///E/Business Ideas/ATM_THEFTS1.ppt             | Wes Mantooth | 7/12/2007 11:29:42 PM | 7/12/2007 11:29:42 PM | 3     |
| file:///C/Users/Wes Mantooth/Desktop/ATM_THEFT...    | Wes Mantooth | 7/12/2007 11:28:14 PM | 7/12/2007 11:28:14 PM | 2     |
| file:///C/Users/Wes Mantooth/Documents/Dear Sw...    | Wes Mantooth | 7/12/2007 11:48:55 PM | 7/12/2007 11:48:55 PM | 1     |
| file:///C/Users/Wes Mantooth/Desktop/Aoe_20shoo...   | Wes Mantooth | 7/12/2007 11:31:25 PM | 7/12/2007 11:31:25 PM | 2     |

Figure 2.4

**EVIDENCE (242)**

| URL                                                  | User         | Last Visited Date     | Last Visited (2...)   | Visit |
|------------------------------------------------------|--------------|-----------------------|-----------------------|-------|
| http://www.google.com                                | Wes Mantooth | 7/12/2007 11:12:16 PM | 7/12/2007 11:12:16 PM | 2     |
| http://www.snopes.com/fraud/atm/atmcamera.asp        | Wes Mantooth | 7/12/2007 11:13:19 PM | 7/12/2007 11:13:19 PM | 1     |
| http://www.snopes.com/crime/warnings/atmcamera...    | Wes Mantooth | 7/12/2007 11:13:16 PM | 7/12/2007 11:13:16 PM | 1     |
| file:///E/Business Ideas/unitled.bmp                 | Wes Mantooth | 7/12/2007 11:14:17 PM | 7/12/2007 11:14:17 PM | 1     |
| file:///E/Business Ideas/Guts.bmp                    | Wes Mantooth | 7/12/2007 11:14:53 PM | 7/12/2007 11:14:53 PM | 1     |
| http://basalemedia.com/V2/44508/86958/index.htm...   | Wes Mantooth | 7/12/2007 11:15:00 PM | 7/12/2007 11:15:00 PM | 1     |
| file:///E/Business Ideas/Camera.bmp                  | Wes Mantooth | 7/12/2007 11:15:11 PM | 7/12/2007 11:15:11 PM | 1     |
| http://www.tots.e.com/tots.e...                      | Wes Mantooth | 7/12/2007 11:16:04 PM | 7/12/2007 11:16:04 PM | 1     |
| http://images.google.com/images?um=1&tab=wi&...      | Wes Mantooth | 7/12/2007 11:15:24 PM | 7/12/2007 11:15:24 PM | 1     |
| http://www.google.com/search?hl=en&q=atm+card...     | Wes Mantooth | 7/12/2007 11:15:34 PM | 7/12/2007 11:15:34 PM | 3     |
| http://www.neonjoin.com/drug_recipes/chapter3.h...   | Wes Mantooth | 7/12/2007 11:15:52 PM | 7/12/2007 11:15:52 PM | 1     |
| http://www.google.com/search?hl=en&q=making+...      | Wes Mantooth | 7/12/2007 11:16:01 PM | 7/12/2007 11:16:01 PM | 2     |
| http://www.tots.e.com/en/drugs/speedy_drugs/how...   | Wes Mantooth | 7/12/2007 11:16:04 PM | 7/12/2007 11:16:04 PM | 1     |
| http://img376.imageshack.us/img376/8880/washing...   | Wes Mantooth | 7/12/2007 11:17:44 PM | 7/12/2007 11:17:44 PM | 1     |
| http://www.physorg.com/physorg...                    | Wes Mantooth | 7/12/2007 11:16:22 PM | 7/12/2007 11:16:22 PM | 1     |
| http://www.physorg.com/news99637614.html             | Wes Mantooth | 7/12/2007 11:16:23 PM | 7/12/2007 11:16:23 PM | 1     |
| http://www.google.com/search?hl=en&q=making+...      | Wes Mantooth | 7/12/2007 11:16:33 PM | 7/12/2007 11:16:33 PM | 4     |
| http://images.google.com/images?um=1&tab=wi&...      | Wes Mantooth | 7/12/2007 11:17:08 PM | 7/12/2007 11:17:08 PM | 2     |
| http://www.sccja.org/images/csid_meth1.jpg           | Wes Mantooth | 7/12/2007 11:17:02 PM | 7/12/2007 11:17:02 PM | 1     |
| http://images.google.com/imgres?imgurl=http://ww...  | Wes Mantooth | 7/12/2007 11:17:06 PM | 7/12/2007 11:17:06 PM | 1     |
| http://images.google.com/images?q=making+meth...     | Wes Mantooth | 7/12/2007 11:17:06 PM | 7/12/2007 11:17:06 PM | 2     |
| http://images.google.com/images?svnum=10&um=...      | Wes Mantooth | 7/12/2007 11:17:36 PM | 7/12/2007 11:17:36 PM | 2     |
| http://www.google.com/search?hl=en&q=check+washin... | Wes Mantooth | 7/12/2007 11:17:30 PM | 7/12/2007 11:17:30 PM | 1     |
| http://images.google.com/images?q=check+washin...    | Wes Mantooth | 7/12/2007 11:17:35 PM | 7/12/2007 11:17:35 PM | 2     |
| file:///E/Business Ideas/ATM_THEFTS1.ppt             | Wes Mantooth | 7/12/2007 11:29:42 PM | 7/12/2007 11:29:42 PM | 3     |
| file:///C/Users/Wes Mantooth/Desktop/ATM_THEFT...    | Wes Mantooth | 7/12/2007 11:28:14 PM | 7/12/2007 11:28:14 PM | 2     |
| file:///C/Users/Wes Mantooth/Documents/Dear Sw...    | Wes Mantooth | 7/12/2007 11:48:55 PM | 7/12/2007 11:48:55 PM | 1     |
| file:///C/Users/Wes Mantooth/Desktop/Aoe_20shoo...   | Wes Mantooth | 7/12/2007 11:31:25 PM | 7/12/2007 11:31:25 PM | 2     |

Figure 2.5

The screenshot shows the Magnet AXIOM interface. The left pane displays a tree view of evidence categories like 'ALL EVIDENCE' (13,018), 'REFINED RESULTS' (1,056), and 'WEB RELATED' (1,992). The right pane shows a detailed view of an artifact from 'Mantooth.E01'. The artifact information includes:

- URL:** http://www.neonjoint.com/drug\_recipes/chapter3.html
- User:** Wes Mantooth
- Last Visited Date/Time:** 7/12/2007 11:55:2 PM
- Last Visited (2nd Timestamp) Date/Time:** 7/12/2007 11:55:2 PM
- Visit Count:** 1
- Web Page Title:** neonjoint.com - How to make meth

The evidence information section lists various file paths and their details, such as source (Partition 1), file type (Microsoft NTFS, 109.79 MB), and recovery method (Carving).

Figure 2.6

This screenshot is identical to Figure 2.5, showing the same evidence results and artifact details for the URL http://www.neonjoint.com/drug\_recipes/chapter3.html. The artifact information and evidence information sections are identical to those in Figure 2.5.

Figure 2.7

**EVIDENCE (242)**

| URL                                                   | User         | Last Visited Date    | Visit |
|-------------------------------------------------------|--------------|----------------------|-------|
| http://mailcenter.comcast.net                         | Wes Mantooth | 8/5/2007 9:08:09 AM  | 11    |
| https://webauth.comcast.net/auth/login?url=http%2..._ | Wes Mantooth | 8/5/2007 9:07:45 AM  | 7     |
| https://webauth.comcast.net/auth/login                | Wes Mantooth | 8/5/2007 9:08:08 AM  | 8     |
| http://webmail.aol.com                                | Wes Mantooth | 8/5/2007 9:09:19 AM  | 2     |
| http://xml.web.aol.net/acportal/dynamiclead.kml       | Wes Mantooth | 8/5/2007 9:09:56 AM  | 3     |
| http://mailcenter2.comcast.net/wmc/vim/4683531..._    | Wes Mantooth | 8/5/2007 9:08:13 AM  | 5     |
| https://my.screenname.aol.com/_cqr/login/login.psp    | Wes Mantooth | 8/5/2007 9:08:52 AM  | 15    |
| http://www.ask.com                                    | Wes Mantooth | 8/5/2007 9:12:36 AM  | 7     |
| http://www.aol.com                                    | Wes Mantooth | 8/5/2007 11:10:12 AM | 34    |
| http://webmail.aol.com/29047/aol/en-us/common/L...    | Wes Mantooth | 8/5/2007 9:09:13 AM  | 4     |
| http://www.lycos.com                                  | Wes Mantooth | 8/5/2007 11:10:12 AM | 13    |
| http://my.screenname.aol.com/_cqr/logout/mLogou...    | Wes Mantooth | 8/5/2007 9:09:14 AM  | 3     |
| https://my.screenname.aol.com/_cqr/login/login.psp    | Wes Mantooth | 8/5/2007 9:09:22 AM  | 16    |
| http://www.msn.com                                    | Wes Mantooth | 8/5/2007 10:52:42 AM | 9     |
| http://www.google.com/search?hl=en&q=+am+*...+        | Wes Mantooth | 8/5/2007 9:10:14 AM  | 7     |
| http://www.dogpile.com/info.dogp/search/edit.htm      | Wes Mantooth | 8/5/2007 9:12:00 AM  | 1     |
| http://api.search.yahoo.com/WebSearchService/rss/...  | Wes Mantooth | 8/5/2007 9:11:19 AM  | 1     |
| http://search.yahoo.com/search?p=+am+searching+...    | Wes Mantooth | 8/5/2007 9:11:20 AM  | 7     |
| http://www.yahoo.com                                  | Wes Mantooth | 8/5/2007 11:10:12 AM | 31    |
| http://www.dogpile.com/info.dogp/search/web/!%2...    | Wes Mantooth | 8/5/2007 9:12:03 AM  | 7     |
| http://www.dogpile.com                                | Wes Mantooth | 8/5/2007 9:12:05 AM  | 16    |
| http://www.ask.com/web                                | Wes Mantooth | 8/5/2007 9:12:47 AM  | 1     |
| http://www.ask.com/web?q=+am+searching+for+b...       | Wes Mantooth | 8/5/2007 9:12:50 AM  | 5     |
| http://search.aol.com/aol/search                      | Wes Mantooth | 8/5/2007 9:13:17 AM  | 1     |
| http://www.mamma.com                                  | Wes Mantooth | 8/5/2007 11:10:12 AM | 22    |
| http://search.aol.com/aol/search?invocationType=to... | Wes Mantooth | 8/5/2007 9:13:19 AM  | 7     |
| http://www.hotbot.com/favicon.ico                     | Wes Mantooth | 8/5/2007 9:13:46 AM  | 3     |

**DETAILS**

**ARTIFACT INFORMATION**

- URL: http://www.dogpile.com/info.dogp/search/web/!%2...
- User: Wes Mantooth
- Last Visited Date/Time: 8/5/2007 9:12:03 AM
- Last Visited (2nd Timestamp) Date/Time: 8/5/2007 9:12:03 AM
- Visit Count: 7
- Web Page Title: I Am Searching For Bad Stuff In Dogpile.Com - Dogpile Web Search

**EVIDENCE INFORMATION**

Activate Windows  
Time zone UTC-000  
Go to Settings to activate

Figure 2.8

**EVIDENCE (242)**

| URL                                                 | User         | Last Visited Date     | Visit |
|-----------------------------------------------------|--------------|-----------------------|-------|
| http://www.google.com                               | Wes Mantooth | 7/12/2007 11:12:16 PM | 2     |
| http://www.snapes.com/fraud/atk/atmcamera.asp       | Wes Mantooth | 7/12/2007 11:13:19 PM | 1     |
| http://www.snapes.com/crime/warnings/atmcamera..._  | Wes Mantooth | 7/12/2007 11:13:16 PM | 1     |
| file:///E:/Business Ideas/united.bmp                | Wes Mantooth | 7/12/2007 11:14:17 PM | 1     |
| file:///E:/Business Ideas/Guts.bmp                  | Wes Mantooth | 7/12/2007 11:14:53 PM | 1     |
| http://b.casalemedia.com/V/4450/86958/index.htm     | Wes Mantooth | 7/12/2007 11:15:00 PM | 1     |
| file:///E:/Business Ideas/Camera.bmp                | Wes Mantooth | 7/12/2007 11:15:11 PM | 1     |
| http://www.totse.com/totse.css                      | Wes Mantooth | 7/12/2007 11:16:04 PM | 1     |
| http://images.google.com/images?um=1&tbo=wi&...     | Wes Mantooth | 7/12/2007 11:16:24 PM | 1     |
| http://www.google.com/search?hl=en&q=atm+card...    | Wes Mantooth | 7/12/2007 11:15:34 PM | 3     |
| http://www.neonjnt.com/drug_recipes/chapter3.htm    | Wes Mantooth | 7/12/2007 11:15:52 PM | 1     |
| http://www.google.com/search?hl=en&q=making+...     | Wes Mantooth | 7/12/2007 11:16:01 PM | 2     |
| http://www.totse.com/en/drugs/speedy_drugs/how...   | Wes Mantooth | 7/12/2007 11:16:04 PM | 1     |
| http://img376.imageshack.us/img376/8880/washing...  | Wes Mantooth | 7/12/2007 11:17:44 PM | 1     |
| http://www.physorg.com/physorg.rss                  | Wes Mantooth | 7/12/2007 11:16:22 PM | 1     |
| http://www.physorg.com/news99637614.html            | Wes Mantooth | 7/12/2007 11:16:23 PM | 1     |
| http://www.google.com/search?hl=en&q=making+...     | Wes Mantooth | 7/12/2007 11:16:33 PM | 4     |
| http://images.google.com/images?um=1&tbo=wi&...     | Wes Mantooth | 7/12/2007 11:17:08 PM | 2     |
| http://www.scpa.org/images/cid_meth1.jpg            | Wes Mantooth | 7/12/2007 11:17:02 PM | 1     |
| http://images.google.com/imgres?imgurl=http://w...  | Wes Mantooth | 7/12/2007 11:17:06 PM | 1     |
| http://images.google.com/images?q=making+meth...    | Wes Mantooth | 7/12/2007 11:17:06 PM | 2     |
| http://images.google.com/images?sznum=10&um=1...    | Wes Mantooth | 7/12/2007 11:17:36 PM | 2     |
| http://images.google.com/images?q=check+washin...   | Wes Mantooth | 7/12/2007 11:17:30 PM | 1     |
| http://images.google.com/images?q=check+washin...   | Wes Mantooth | 7/12/2007 11:17:35 PM | 2     |
| file:///E:/Business Ideas/ATM_THEFT1.ppt            | Wes Mantooth | 7/12/2007 11:29:42 PM | 3     |
| file:///C:/Users/Wes Mantooth/Desktop/ATM_THEFT...  | Wes Mantooth | 7/12/2007 11:28:14 PM | 2     |
| file:///C:/Users/Wes Mantooth/Documents/Dear Sw...  | Wes Mantooth | 7/12/2007 11:48:55 PM | 1     |
| file:///C:/Users/Wes Mantooth/Desktop/Aoe_20shoo... | Wes Mantooth | 7/12/2007 11:31:25 PM | 2     |

**DETAILS**

**ARTIFACT INFORMATION**

- URL: http://www.google.com/search?hl=en&q=atm+card...
- User: Wes Mantooth
- Last Visited Date/Time: 7/12/2007 11:16:22 PM
- Last Visited (2nd Timestamp) Date/Time: 7/12/2007 11:15:34 PM
- Visit Count: 3
- Web Page Title: atm card stealing - Google Search

**EVIDENCE INFORMATION**

Activate Windows  
Time zone UTC-000  
Go to Settings to activate

Figure 2.9

The screenshot shows the Magnet AXIOM Examine interface. The left sidebar displays a tree view of artifacts categorized into Google Analytics, WEB RELATED, MEDIA, and EMAIL. The 'WEB RELATED' section is expanded, showing 1,992 items. The 'EMAIL' section shows 188 items. The main pane, titled 'EVIDENCE (242)', lists 242 entries with columns for URL, User, Last Visited Date, Last Visited (2nd), and Visits. A specific entry for 'http://search.netscape.com/search...' is selected. The right pane provides a detailed view of this artifact, including 'ARTIFACT INFORMATION' (User: Wes Mantooth, URL: http://search.netscape.com/search/...), 'EVIDENCE INFORMATION' (Source: Mantooth.E01, Partition 1, Microsoft NTFS, 109.79 MB), and a 'TAGS, PROFILES & MEDIA CATEGORIES' section.

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

**EVIDENCE (70)**

| URL                                                   | User         | Last Visited...     | Last Visited Da...    | Visit... |
|-------------------------------------------------------|--------------|---------------------|-----------------------|----------|
| file:///E/Business Ideas/Untitled.bmp                 | Wes Mantooth | 2007-07-12 17:14:17 | 7/12/2007 11:14:17 PM | 1        |
| file:///E/Business Ideas/Guts.bmp                     | Wes Mantooth | 2007-07-12 17:14:53 | 7/12/2007 11:14:53 PM | 1        |
| file:///E/Business Ideas/Camera.bmp                   | Wes Mantooth | 2007-07-12 17:15:11 | 7/12/2007 11:15:11 PM | 1        |
| file:///E/Business Ideas/ATM_THEFTS1.ppt              | Wes Mantooth | 2007-07-12 17:29:42 | 7/12/2007 11:29:42 PM | 3        |
| file:///C/Users/Wes Mantooth/Desktop/ATM_THEFT...     | Wes Mantooth | 2007-07-12 17:28:14 | 7/12/2007 11:28:14 PM | 2        |
| file:///C/Users/Wes Mantooth/Documents/Dear Sw...     | Wes Mantooth | 2007-07-12 17:48:55 | 7/12/2007 11:48:55 PM | 1        |
| file:///C/Users/Wes Mantooth/Desktop/Ape_20hoo...     | Wes Mantooth | 2007-07-12 17:31:25 | 7/12/2007 11:31:25 PM | 2        |
| :Host: Computer                                       | Wes Mantooth | 2007-07-12 17:14:17 | 7/12/2007 11:14:17 PM | 1        |
| http://www.google.com                                 | Wes Mantooth | 2007-07-12 17:12:16 | 7/12/2007 11:12:16 PM | 1        |
| :Host: www.google.com                                 | Wes Mantooth | 2007-07-12 17:12:16 | 7/12/2007 11:12:16 PM | 1        |
| http://images.google.com/images?um=1&tab=wi&...       | Wes Mantooth | 2007-07-12 17:15:24 | 7/12/2007 11:15:24 PM | 1        |
| http://www.snopes.com/crime/warnings/atmcamera...     | Wes Mantooth | 2007-07-12 17:13:16 | 7/12/2007 11:13:16 PM | 1        |
| :Host: snopes.com                                     | Wes Mantooth | 2007-07-12 17:13:16 | 7/12/2007 11:13:16 PM | 1        |
| http://www.snopes.com/fraud/atmcamera.asp             | Wes Mantooth | 2007-07-12 17:13:19 | 7/12/2007 11:13:19 PM | 1        |
| http://b.casalemedia.com/V2/44508/86958/index.htm...  | Wes Mantooth | 2007-07-12 17:15:00 | 7/12/2007 11:15:00 PM | 1        |
| :Host: b.casalemedia.com                              | Wes Mantooth | 2007-07-12 17:15:00 | 7/12/2007 11:15:00 PM | 1        |
| http://www.tots.com/en/drugs/speedy_drugs/howto...    | Wes Mantooth | 2007-07-12 17:16:04 | 7/12/2007 11:16:04 PM | 1        |
| :Host: images.google.com                              | Wes Mantooth | 2007-07-12 17:15:24 | 7/12/2007 11:15:24 PM | 1        |
| http://www.google.com/search?q=atm+card+steal...      | Wes Mantooth | 2007-07-12 17:15:34 | 7/12/2007 11:15:34 PM | 3        |
| http://www.neonjoint.com/drug_recipes/chapter3.htm... | Wes Mantooth | 2007-07-12 17:15:52 | 7/12/2007 11:15:52 PM | 1        |
| :Host: www.neonjoint.com                              | Wes Mantooth | 2007-07-12 17:15:52 | 7/12/2007 11:15:52 PM | 1        |
| http://www.physorg.com/news99637614.html              | Wes Mantooth | 2007-07-12 17:16:23 | 7/12/2007 11:16:23 PM | 1        |
| :Host: www.tots.com                                   | Wes Mantooth | 2007-07-12 17:16:04 | 7/12/2007 11:16:04 PM | 1        |
| http://img376.imageshack.us/img376/8880/washing...    | Wes Mantooth | 2007-07-12 17:17:44 | 7/12/2007 11:17:44 PM | 1        |
| :Host: www.physorg.com                                | Wes Mantooth | 2007-07-12 17:16:23 | 7/12/2007 11:16:23 PM | 1        |
| http://www.google.com/search?q=making+an+...          | Wes Mantooth | 2007-07-12 17:16:33 | 7/12/2007 11:16:33 PM | 4        |
| http://images.google.com/images?um=1&tab=wi&...       | Wes Mantooth | 2007-07-12 17:17:08 | 7/12/2007 11:17:08 PM | 2        |
| http://www.sccia.org/images/csid_meth1.ico            | Wes Mantooth | 2007-07-12 17:17:02 | 7/12/2007 11:17:02 PM | 1        |

**ARTIFACT INFORMATION**

**EVIDENCE INFORMATION**

Source: Mantooth.E01 - Partition 1 (Microsoft NTFS, 109.79 MB) MANTOOOTH\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\History\LowHistoryIE5\MSHist012007071220070713\index.dat

Recovery Method: Carving

Deleted source: File Offset 21760

Location: File Offset 21760

Evidence number: Mantooth.E01

Activate Windows Time zone: UTC-0000 Go to Settings to activate

Figure 3.1

Magnet AXIOM Examine v4.1.0.19966 - Mantooth

**EVIDENCE (70)**

| URL                                                   | User         | Last Visited...     | Last Visited Da...    | Visit... |
|-------------------------------------------------------|--------------|---------------------|-----------------------|----------|
| file:///E/Business Ideas/Untitled.bmp                 | Wes Mantooth | 2007-07-12 17:14:17 | 7/12/2007 11:14:17 PM | 1        |
| file:///E/Business Ideas/Guts.bmp                     | Wes Mantooth | 2007-07-12 17:14:53 | 7/12/2007 11:14:53 PM | 1        |
| file:///E/Business Ideas/Camera.bmp                   | Wes Mantooth | 2007-07-12 17:15:11 | 7/12/2007 11:15:11 PM | 1        |
| file:///E/Business Ideas/ATM_THEFTS1.ppt              | Wes Mantooth | 2007-07-12 17:29:42 | 7/12/2007 11:29:42 PM | 3        |
| file:///C/Users/Wes Mantooth/Desktop/ATM_THEFT...     | Wes Mantooth | 2007-07-12 17:28:14 | 7/12/2007 11:28:14 PM | 2        |
| file:///C/Users/Wes Mantooth/Documents/Dear Sw...     | Wes Mantooth | 2007-07-12 17:48:55 | 7/12/2007 11:48:55 PM | 1        |
| file:///C/Users/Wes Mantooth/Desktop/Ape_20hoo...     | Wes Mantooth | 2007-07-12 17:31:25 | 7/12/2007 11:31:25 PM | 2        |
| :Host: Computer                                       | Wes Mantooth | 2007-07-12 17:14:17 | 7/12/2007 11:14:17 PM | 1        |
| http://www.google.com                                 | Wes Mantooth | 2007-07-12 17:12:16 | 7/12/2007 11:12:16 PM | 1        |
| :Host: www.google.com                                 | Wes Mantooth | 2007-07-12 17:12:16 | 7/12/2007 11:12:16 PM | 1        |
| http://images.google.com/images?um=1&tab=wi&...       | Wes Mantooth | 2007-07-12 17:15:24 | 7/12/2007 11:15:24 PM | 1        |
| http://www.snopes.com/crime/warnings/atmcamera...     | Wes Mantooth | 2007-07-12 17:13:16 | 7/12/2007 11:13:16 PM | 1        |
| :Host: snopes.com                                     | Wes Mantooth | 2007-07-12 17:13:16 | 7/12/2007 11:13:16 PM | 1        |
| http://www.snopes.com/fraud/atmcamera.asp             | Wes Mantooth | 2007-07-12 17:13:19 | 7/12/2007 11:13:19 PM | 1        |
| http://b.casalemedia.com/V2/44508/86958/index.htm...  | Wes Mantooth | 2007-07-12 17:15:00 | 7/12/2007 11:15:00 PM | 1        |
| :Host: b.casalemedia.com                              | Wes Mantooth | 2007-07-12 17:15:00 | 7/12/2007 11:15:00 PM | 1        |
| http://www.tots.com/en/drugs/speedy_drugs/howto...    | Wes Mantooth | 2007-07-12 17:16:04 | 7/12/2007 11:16:04 PM | 1        |
| :Host: images.google.com                              | Wes Mantooth | 2007-07-12 17:15:24 | 7/12/2007 11:15:24 PM | 1        |
| http://www.google.com/search?q=atm+card+steal...      | Wes Mantooth | 2007-07-12 17:15:34 | 7/12/2007 11:15:34 PM | 3        |
| http://www.neonjoint.com/drug_recipes/chapter3.htm... | Wes Mantooth | 2007-07-12 17:15:52 | 7/12/2007 11:15:52 PM | 1        |
| :Host: www.neonjoint.com                              | Wes Mantooth | 2007-07-12 17:15:52 | 7/12/2007 11:15:52 PM | 1        |
| http://www.physorg.com/news99637614.html              | Wes Mantooth | 2007-07-12 17:16:23 | 7/12/2007 11:16:23 PM | 1        |
| :Host: www.tots.com                                   | Wes Mantooth | 2007-07-12 17:16:04 | 7/12/2007 11:16:04 PM | 1        |
| http://img376.imageshack.us/img376/8880/washing...    | Wes Mantooth | 2007-07-12 17:17:44 | 7/12/2007 11:17:44 PM | 1        |
| :Host: www.physorg.com                                | Wes Mantooth | 2007-07-12 17:16:23 | 7/12/2007 11:16:23 PM | 1        |
| http://www.google.com/search?q=making+an+...          | Wes Mantooth | 2007-07-12 17:16:33 | 7/12/2007 11:16:33 PM | 4        |
| http://images.google.com/images?um=1&tab=wi&...       | Wes Mantooth | 2007-07-12 17:17:08 | 7/12/2007 11:17:08 PM | 2        |
| http://www.sccia.org/images/csid_meth1.ico            | Wes Mantooth | 2007-07-12 17:17:02 | 7/12/2007 11:17:02 PM | 1        |

**ARTIFACT INFORMATION**

**EVIDENCE INFORMATION**

Source: Mantooth.E01 - Partition 1 (Microsoft NTFS, 109.79 MB) MANTOOOTH\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\History\LowHistoryIE5\MSHist012007071220070713\index.dat

Recovery Method: Carving

Deleted source: File Offset 23040

Location: File Offset 23040

Evidence number: Mantooth.E01

Activate Windows Time zone: UTC-0000 Go to Settings to activate

Figure 3.2

The screenshot shows the Magnet AXIOM interface with the following details:

**EVIDENCE (70)**

|                                                     | URL          | User                | Last Visited...       | Last Visited Da... | Visit... |
|-----------------------------------------------------|--------------|---------------------|-----------------------|--------------------|----------|
| file:///E:/Business Ideas/unitled.bmp               | Wes Mantooth | 2007-07-12 17:14:17 | 7/12/2007 11:14:17 PM | 1                  |          |
| file:///E:/Business Ideas/Guts.bmp                  | Wes Mantooth | 2007-07-12 17:14:53 | 7/12/2007 11:14:53 PM | 1                  |          |
| file:///E:/Business Ideas/Camera.bmp                | Wes Mantooth | 2007-07-12 17:15:11 | 7/12/2007 11:15:11 PM | 1                  |          |
| file:///E:/Business Ideas/ATM_THEFTS1.ppt           | Wes Mantooth | 2007-07-12 17:29:42 | 7/12/2007 11:29:42 PM | 3                  |          |
| file:///C:/Users/Wes Mantooth/Desktop/ATM_THEFT...  | Wes Mantooth | 2007-07-12 17:28:14 | 7/12/2007 11:28:14 PM | 2                  |          |
| file:///C:/Users/Wes Mantooth/Documents/Dear Sw...  | Wes Mantooth | 2007-07-12 17:48:55 | 7/12/2007 11:48:55 PM | 1                  |          |
| file:///C:/Users/Wes Mantooth/Desktop/Ape_20shoo... | Wes Mantooth | 2007-07-12 17:31:25 | 7/12/2007 11:31:25 PM | 2                  |          |
| :Host: Computer                                     | Wes Mantooth | 2007-07-12 17:14:17 | 7/12/2007 11:14:17 PM | 1                  |          |
| http://www.google.com                               | Wes Mantooth | 2007-07-12 17:12:16 | 7/12/2007 11:12:16 PM | 1                  |          |
| :Host: www.google.com                               | Wes Mantooth | 2007-07-12 17:12:16 | 7/12/2007 11:12:16 PM | 1                  |          |
| http://images.google.com/images?um=1&tab=wi&...     | Wes Mantooth | 2007-07-12 17:15:24 | 7/12/2007 11:15:24 PM | 1                  |          |
| http://www.snapes.com/crime/warnings/atmcamera...   | Wes Mantooth | 2007-07-12 17:13:16 | 7/12/2007 11:13:16 PM | 1                  |          |
| :Host: www.snapes.com                               | Wes Mantooth | 2007-07-12 17:13:16 | 7/12/2007 11:13:16 PM | 1                  |          |
| http://www.snapes.com/fraud/atm/atmcamera.asp       | Wes Mantooth | 2007-07-12 17:13:19 | 7/12/2007 11:13:19 PM | 1                  |          |
| http://b.casalemedia.com/V2/44508/86958/index.ht... | Wes Mantooth | 2007-07-12 17:15:00 | 7/12/2007 11:15:00 PM | 1                  |          |
| :Host: b.casalemedia.com                            | Wes Mantooth | 2007-07-12 17:15:00 | 7/12/2007 11:15:00 PM | 1                  |          |
| http://www.totse.com/en/drugs/speedy_drugs/how...   | Wes Mantooth | 2007-07-12 17:16:04 | 7/12/2007 11:16:04 PM | 1                  |          |
| :Host: images.google.com                            | Wes Mantooth | 2007-07-12 17:15:24 | 7/12/2007 11:15:24 PM | 1                  |          |
| http://www.google.com/search?q=atm+card+...         | Wes Mantooth | 2007-07-12 17:15:34 | 7/12/2007 11:15:34 PM | 3                  |          |
| http://www.neonpoint.com/drug_recipes/chapter3.h... | Wes Mantooth | 2007-07-12 17:15:52 | 7/12/2007 11:15:52 PM | 1                  |          |
| :Host: www.neonpoint.com                            | Wes Mantooth | 2007-07-12 17:15:52 | 7/12/2007 11:15:52 PM | 1                  |          |
| http://www.physorg.com/news99637614.html            | Wes Mantooth | 2007-07-12 17:16:23 | 7/12/2007 11:16:23 PM | 1                  |          |
| :Host: totse.com                                    | Wes Mantooth | 2007-07-12 17:16:04 | 7/12/2007 11:16:04 PM | 1                  |          |
| http://img376.imageshack.us/img376/8880/washing...  | Wes Mantooth | 2007-07-12 17:17:44 | 7/12/2007 11:17:44 PM | 1                  |          |
| :Host: www.physorg.com                              | Wes Mantooth | 2007-07-12 17:16:23 | 7/12/2007 11:16:23 PM | 1                  |          |
| http://www.google.com/search?q=making+...           | Wes Mantooth | 2007-07-12 17:16:33 | 7/12/2007 11:16:33 PM | 4                  |          |
| http://images.google.com/images?um=1&tab=wi&...     | Wes Mantooth | 2007-07-12 17:17:08 | 7/12/2007 11:17:08 PM | 2                  |          |
| http://www.sccia.ora/images/cid_meth1.ico           | Wes Mantooth | 2007-07-12 17:17:02 | 7/12/2007 11:17:02 PM | 1                  |          |

**ARTIFACT INFORMATION**

- URL: file:///E:/Business Ideas/ATM\_THEFTS1.ppt
- User: Wes Mantooth
- Last Visited Date/Time (local time): 2007-07-12 17:29:42 PM
- Last Visited Date/Time: 7/12/2007 11:29:42 PM
- Visit Count: 3

**EVIDENCE INFORMATION**

- Source: Mantooth.E01 - Partition 1 (Microsoft NTFS, 109.79 MB) MANTOOOTH\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\History\History.IE5 VMSHist012007071 220070713\Index.dat
- Recovery Method: Carving
- Deleted source: File Offset 21504
- Location: File Offset 21504
- Evidence number: Mantooth.E01

Figure 3.3

The screenshot shows the Magnet AXIOM interface with the following details:

**EVIDENCE (70)**

|                                                     | URL          | User                | Last Visited...       | Last Visited Da... | Visit... |
|-----------------------------------------------------|--------------|---------------------|-----------------------|--------------------|----------|
| file:///E:/Business Ideas/unitled.bmp               | Wes Mantooth | 2007-07-12 17:14:17 | 7/12/2007 11:14:17 PM | 1                  |          |
| file:///E:/Business Ideas/Guts.bmp                  | Wes Mantooth | 2007-07-12 17:14:53 | 7/12/2007 11:14:53 PM | 1                  |          |
| file:///E:/Business Ideas/Camera.bmp                | Wes Mantooth | 2007-07-12 17:15:11 | 7/12/2007 11:15:11 PM | 1                  |          |
| file:///E:/Business Ideas/ATM_THEFTS1.ppt           | Wes Mantooth | 2007-07-12 17:29:42 | 7/12/2007 11:29:42 PM | 3                  |          |
| file:///C:/Users/Wes Mantooth/Desktop/ATM_THEFT...  | Wes Mantooth | 2007-07-12 17:28:14 | 7/12/2007 11:28:14 PM | 2                  |          |
| file:///C:/Users/Wes Mantooth/Documents/Dear Sw...  | Wes Mantooth | 2007-07-12 17:48:55 | 7/12/2007 11:48:55 PM | 1                  |          |
| file:///C:/Users/Wes Mantooth/Desktop/Ape_20shoo... | Wes Mantooth | 2007-07-12 17:31:25 | 7/12/2007 11:31:25 PM | 2                  |          |
| :Host: Computer                                     | Wes Mantooth | 2007-07-12 17:14:17 | 7/12/2007 11:14:17 PM | 1                  |          |
| http://www.google.com                               | Wes Mantooth | 2007-07-12 17:12:16 | 7/12/2007 11:12:16 PM | 1                  |          |
| :Host: www.google.com                               | Wes Mantooth | 2007-07-12 17:12:16 | 7/12/2007 11:12:16 PM | 1                  |          |
| http://images.google.com/images?um=1&tab=wi&...     | Wes Mantooth | 2007-07-12 17:15:24 | 7/12/2007 11:15:24 PM | 1                  |          |
| http://www.snapes.com/crime/warnings/atmcamera...   | Wes Mantooth | 2007-07-12 17:13:16 | 7/12/2007 11:13:16 PM | 1                  |          |
| :Host: www.snapes.com                               | Wes Mantooth | 2007-07-12 17:13:16 | 7/12/2007 11:13:16 PM | 1                  |          |
| http://www.snapes.com/fraud/atm/atmcamera.asp       | Wes Mantooth | 2007-07-12 17:13:19 | 7/12/2007 11:13:19 PM | 1                  |          |
| http://b.casalemedia.com/V2/44508/86958/index.ht... | Wes Mantooth | 2007-07-12 17:15:00 | 7/12/2007 11:15:00 PM | 1                  |          |
| :Host: b.casalemedia.com                            | Wes Mantooth | 2007-07-12 17:15:00 | 7/12/2007 11:15:00 PM | 1                  |          |
| http://www.totse.com/en/drugs/speedy_drugs/how...   | Wes Mantooth | 2007-07-12 17:16:04 | 7/12/2007 11:16:04 PM | 1                  |          |
| :Host: images.google.com                            | Wes Mantooth | 2007-07-12 17:15:24 | 7/12/2007 11:15:24 PM | 1                  |          |
| http://www.google.com/search?q=atm+card+...         | Wes Mantooth | 2007-07-12 17:15:34 | 7/12/2007 11:15:34 PM | 3                  |          |
| http://www.neonpoint.com/drug_recipes/chapter3.h... | Wes Mantooth | 2007-07-12 17:15:52 | 7/12/2007 11:15:52 PM | 1                  |          |
| :Host: www.neonpoint.com                            | Wes Mantooth | 2007-07-12 17:15:52 | 7/12/2007 11:15:52 PM | 1                  |          |
| http://www.physorg.com/news99637614.html            | Wes Mantooth | 2007-07-12 17:16:23 | 7/12/2007 11:16:23 PM | 1                  |          |
| :Host: totse.com                                    | Wes Mantooth | 2007-07-12 17:16:04 | 7/12/2007 11:16:04 PM | 1                  |          |
| http://img376.imageshack.us/img376/8880/washing...  | Wes Mantooth | 2007-07-12 17:17:44 | 7/12/2007 11:17:44 PM | 1                  |          |
| :Host: www.physorg.com                              | Wes Mantooth | 2007-07-12 17:16:23 | 7/12/2007 11:16:23 PM | 1                  |          |
| http://www.google.com/search?q=making+...           | Wes Mantooth | 2007-07-12 17:16:33 | 7/12/2007 11:16:33 PM | 4                  |          |
| http://images.google.com/images?um=1&tab=wi&...     | Wes Mantooth | 2007-07-12 17:17:08 | 7/12/2007 11:17:08 PM | 2                  |          |
| http://www.sccia.ora/images/cid_meth1.ico           | Wes Mantooth | 2007-07-12 17:17:02 | 7/12/2007 11:17:02 PM | 1                  |          |

**ARTIFACT INFORMATION**

- URL: file:///C:/Users/Wes Mantooth/Desktop/ATM\_THEFTS1.ppt
- User: Wes Mantooth
- Last Visited Date/Time (local time): 2007-07-12 17:28:14
- Last Visited Date/Time: 7/12/2007 11:28:14 PM
- Visit Count: 2

**EVIDENCE INFORMATION**

- Source: Mantooth.E01 - Partition 1 (Microsoft NTFS, 109.79 MB) MANTOOOTH\Users\Wes Mantooth\AppData\Local\Microsoft\Windows\History\History.IE5 VMSHist012007071 220070713\Index.dat
- Recovery Method: Carving
- Deleted source: File Offset 21760
- Location: File Offset 21760
- Evidence number: Mantooth.E01

Figure 3.4

The screenshot shows the Magnet AXIOM Examine interface. The main window displays a list of evidence items under several categories: Google Analytics Referral Cookies (14), Google Analytics Session Cookies (12), Google Searches (390), Identifiers - Device (244), Identifiers - People (252), Locally Accessed Files and Folders (48), Parsed Search Queries (2), Passwords and Tokens (6), Rebuilt Desktops (Windows) (2), Rebuilt Webpages (52), and Social Media URLs (16). Below these are sections for WEB RELATED (1,992), MEDIA (1,172), and EMAIL (188) artifacts.

A detailed view of an artifact is shown on the right side of the interface. The artifact is titled "http://www.totse.com/en/drugs...". It includes sections for DETAILS, ARTIFACT INFORMATION, TAGS, PROFILES & MEDIA CATEGORIES, and EVIDENCE INFORMATION. The DETAILS section shows the URL, User (Wes Mantooth), Last Visited Date/Time (2007-07-12 17:16:04 PM), and Visit Count (1). The ARTIFACT INFORMATION section provides a breakdown of the source (Mantooth.E01 - Partition 1 (Microsoft NTFS, 109.79 MB)), user (Wes Mantooth), and various file paths. The EVIDENCE INFORMATION section details the recovery method (Carving), deleted source, location (File Offset 22528), and evidence number (Mantooth.E01).

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.

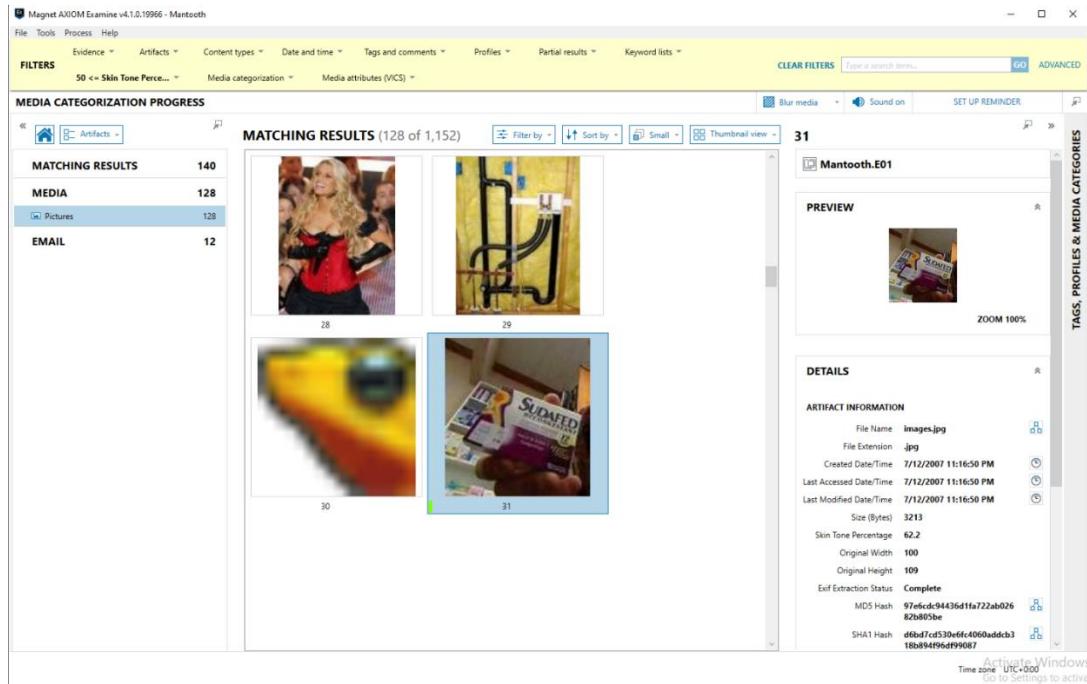


Figure 3.6

Figure 3.6 shows Sudafed a known agent of making drugs.

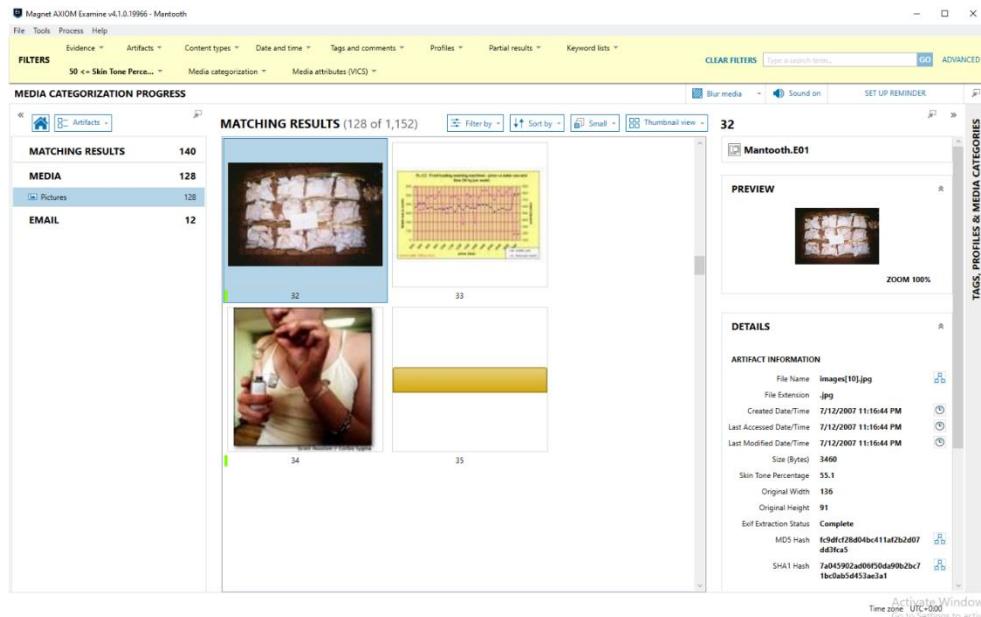


Figure 3.7

Figure 3.7 shows baggies of what appears to be meth.

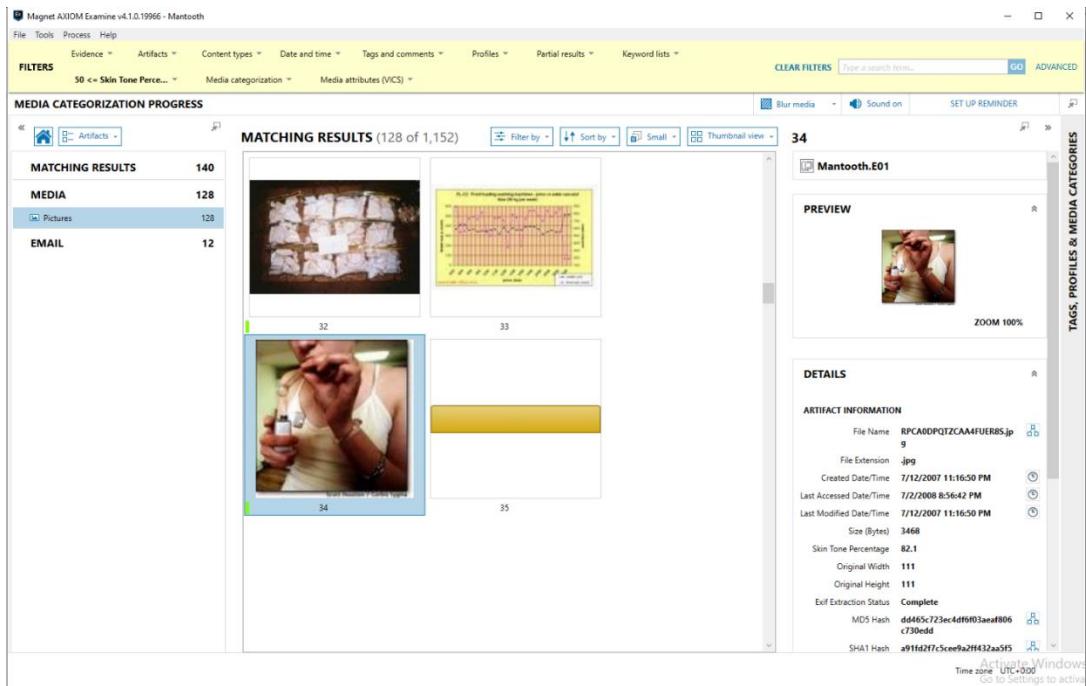


Figure 3.8

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

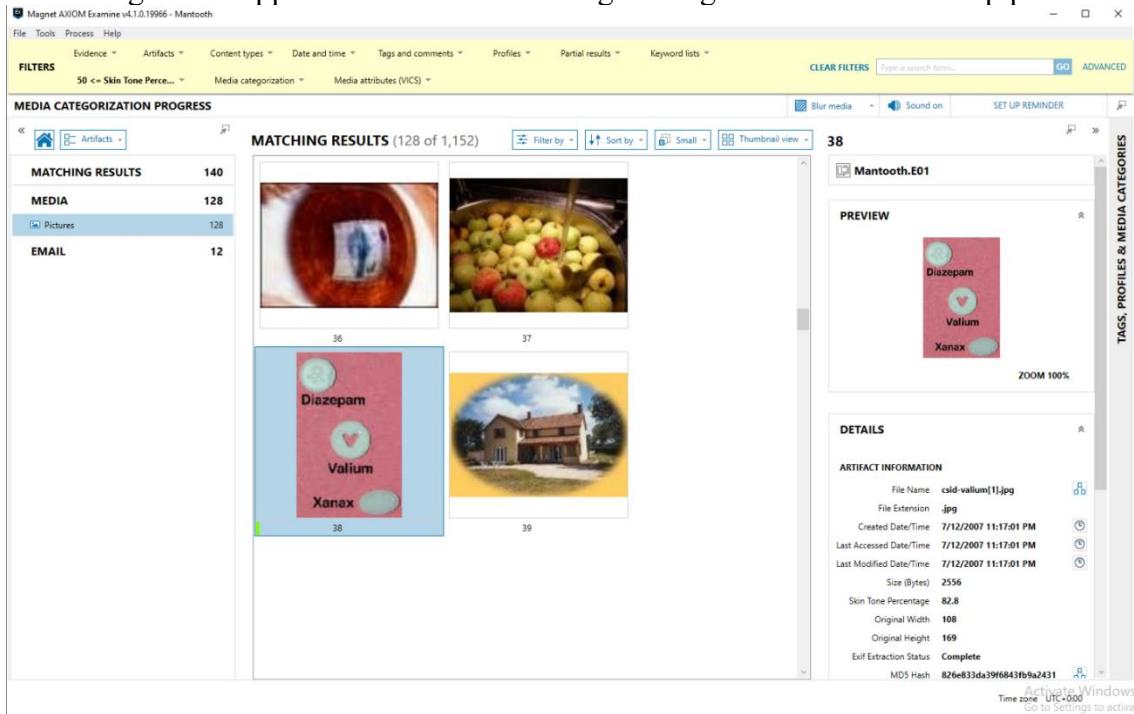


Figure 3.9

Figure 3.9 has various pills that are labeled.

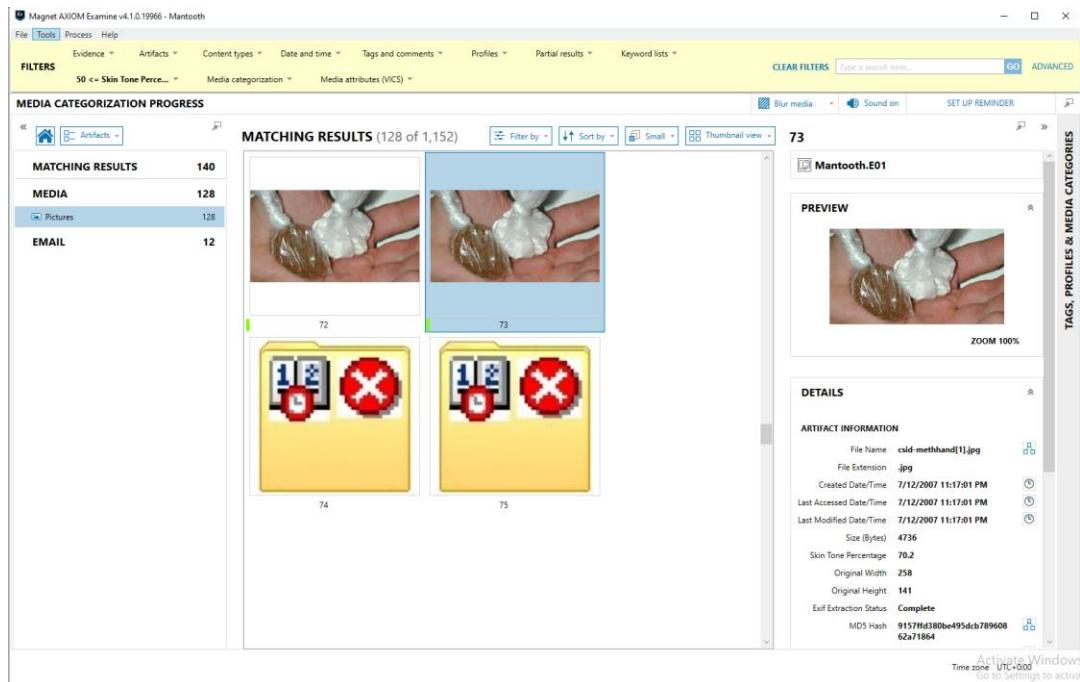


Figure 4.0

Figure 4.0 contains an image of small baggies of drugs.

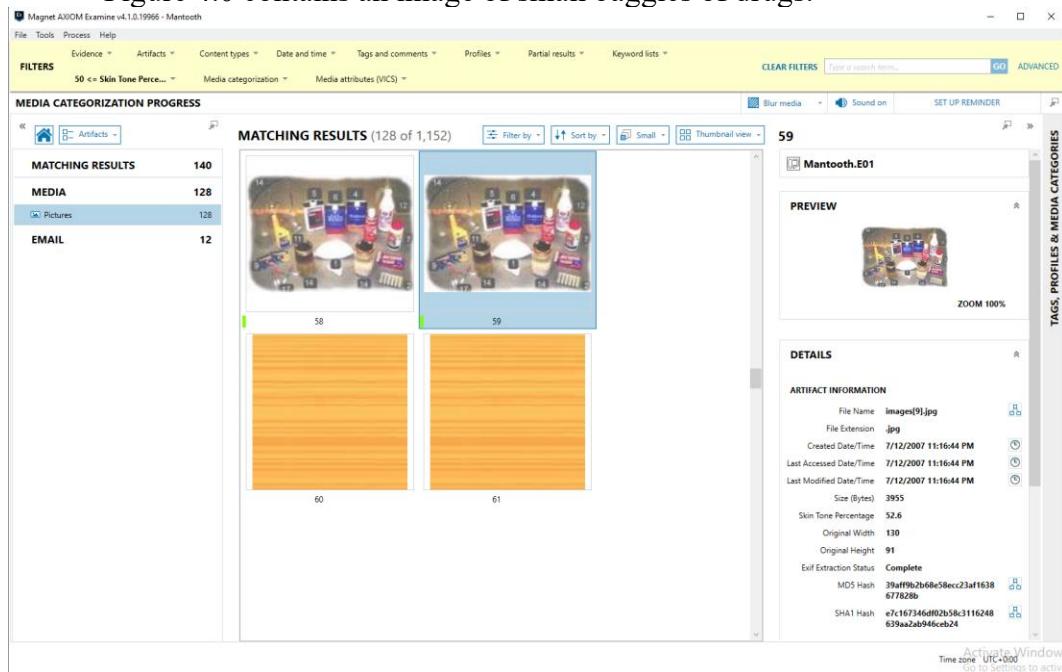


Figure 4.1

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

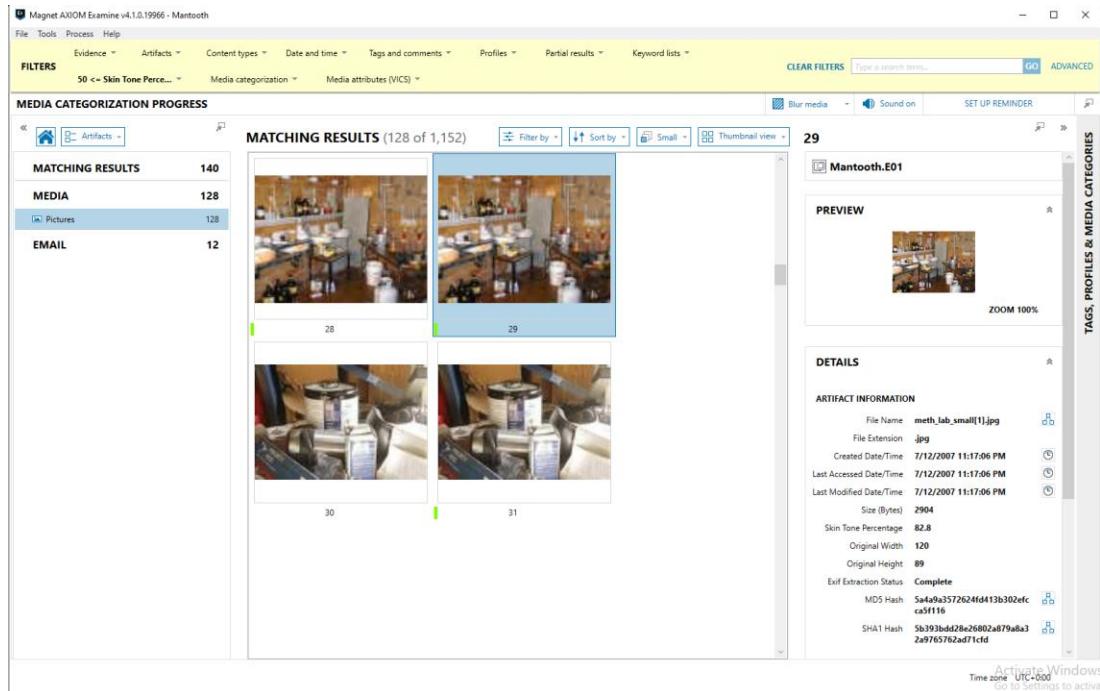


Figure 4.2

Figure 4.2 contains an image of a meth lab.

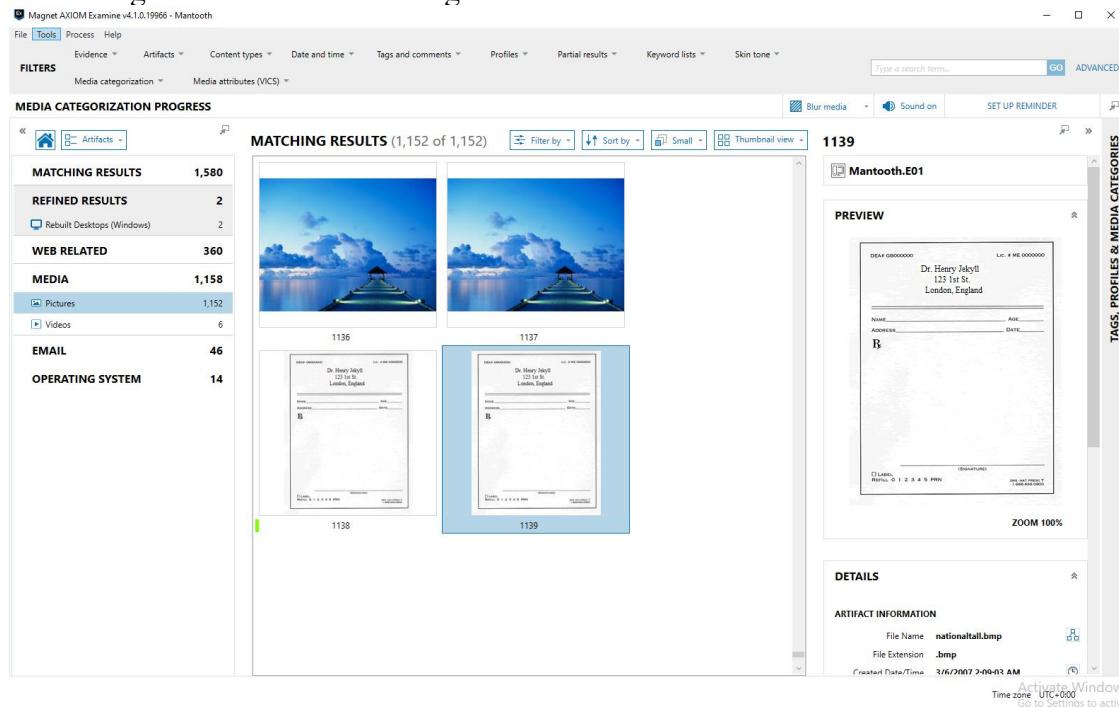


Figure 4.3

Figure 4.3 contains a forged template for a doctor's pharmaceutical note.

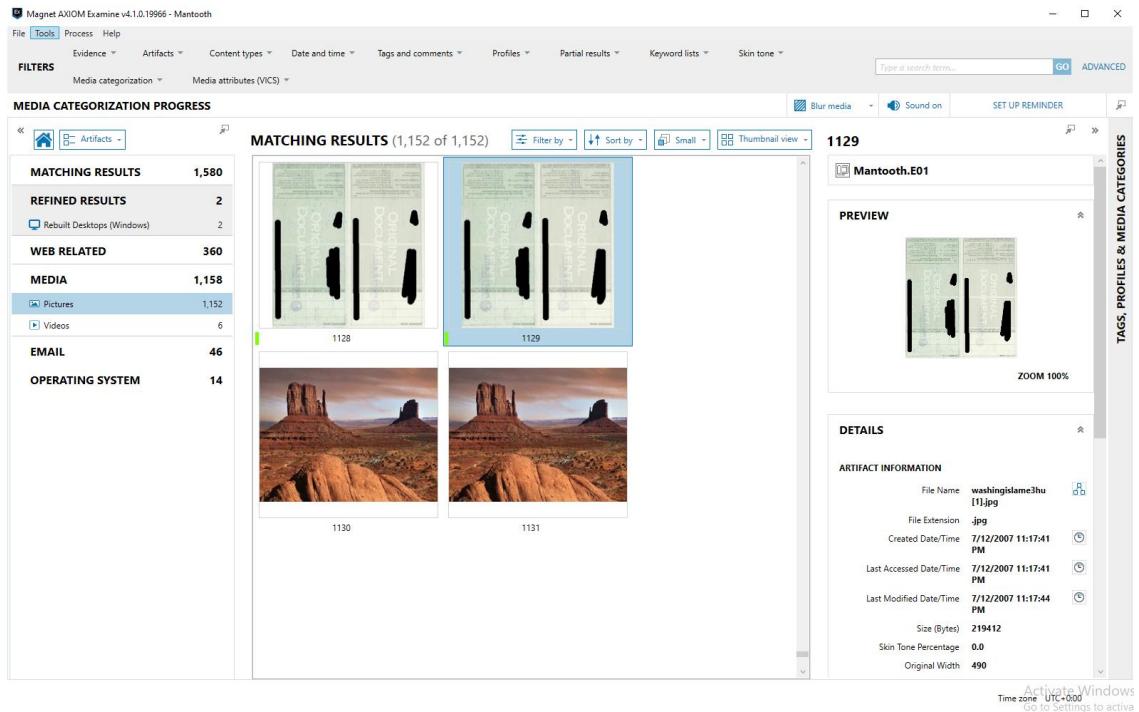


Figure 4.4

Figure 4.4 contains an image of check washing

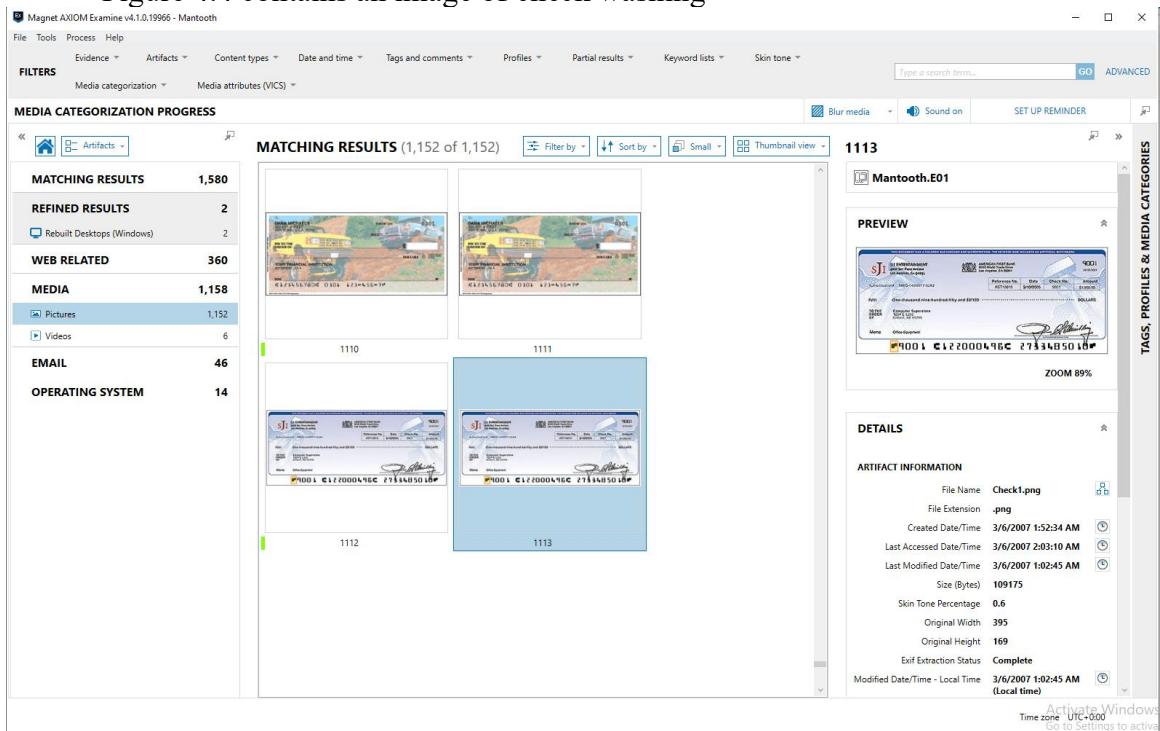


Figure 4.5

Figure 4.5 contains a cashier's check.

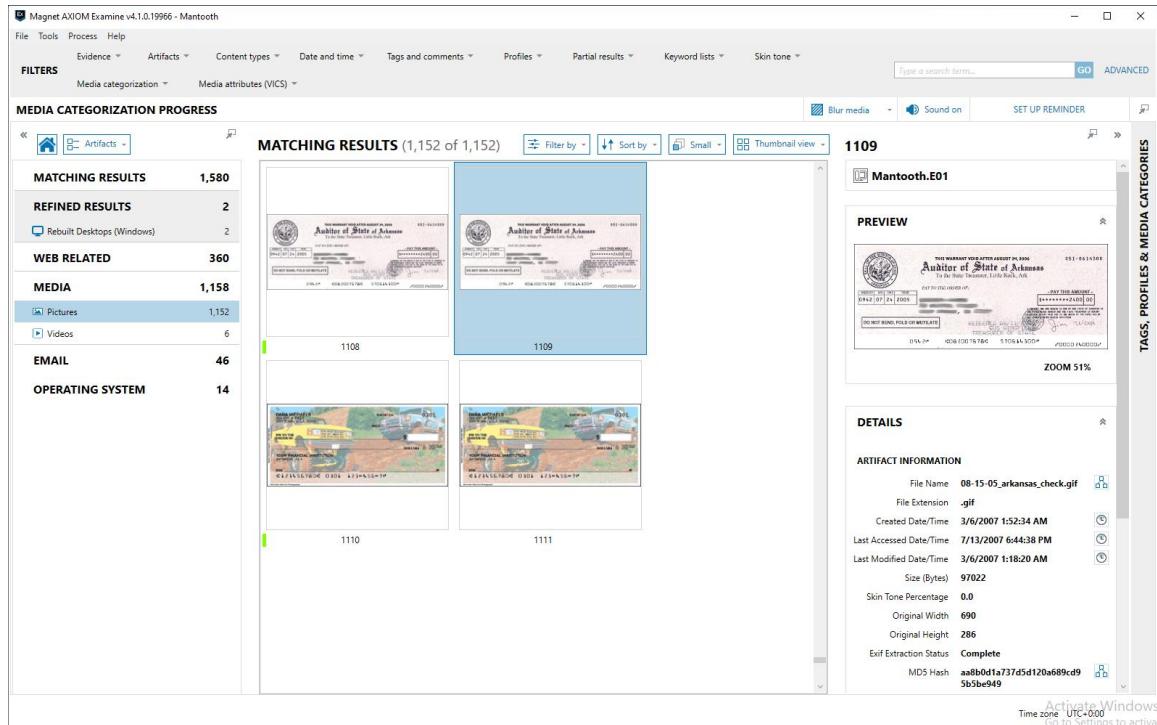


Figure 4.6

Figure 4.6 contains a cashier's check

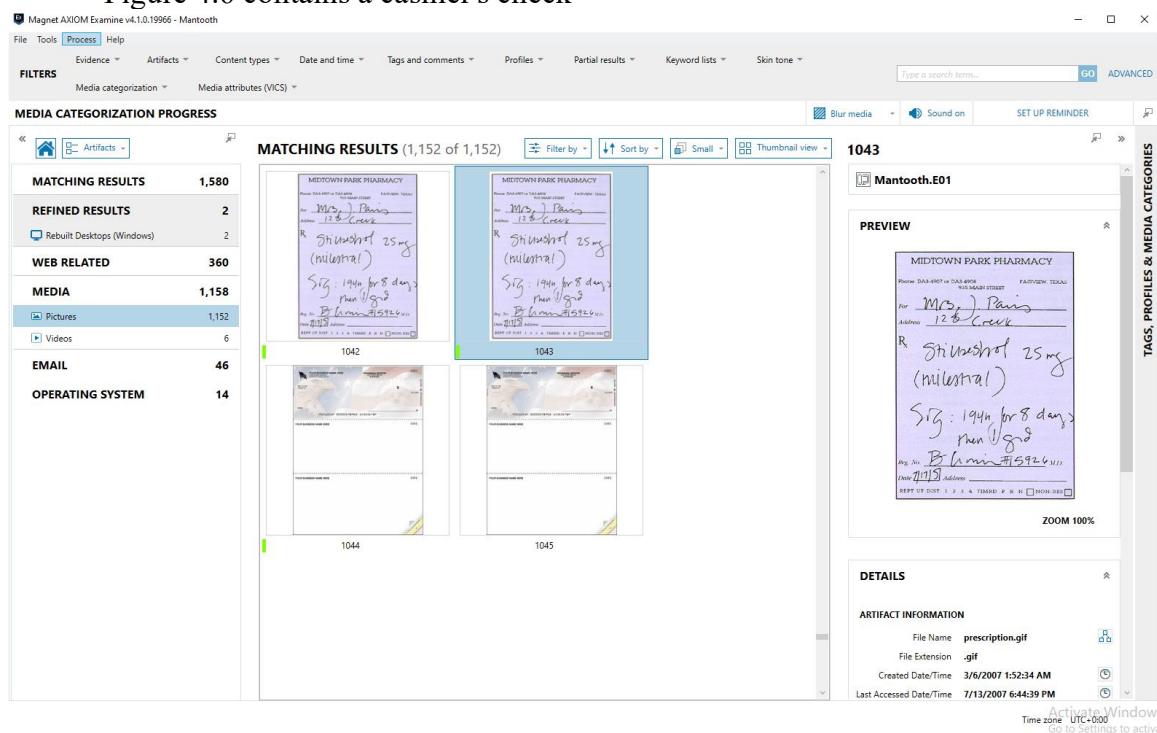


Figure 4.7

Figure 4.7 contains a forged doctors note with a prescription.

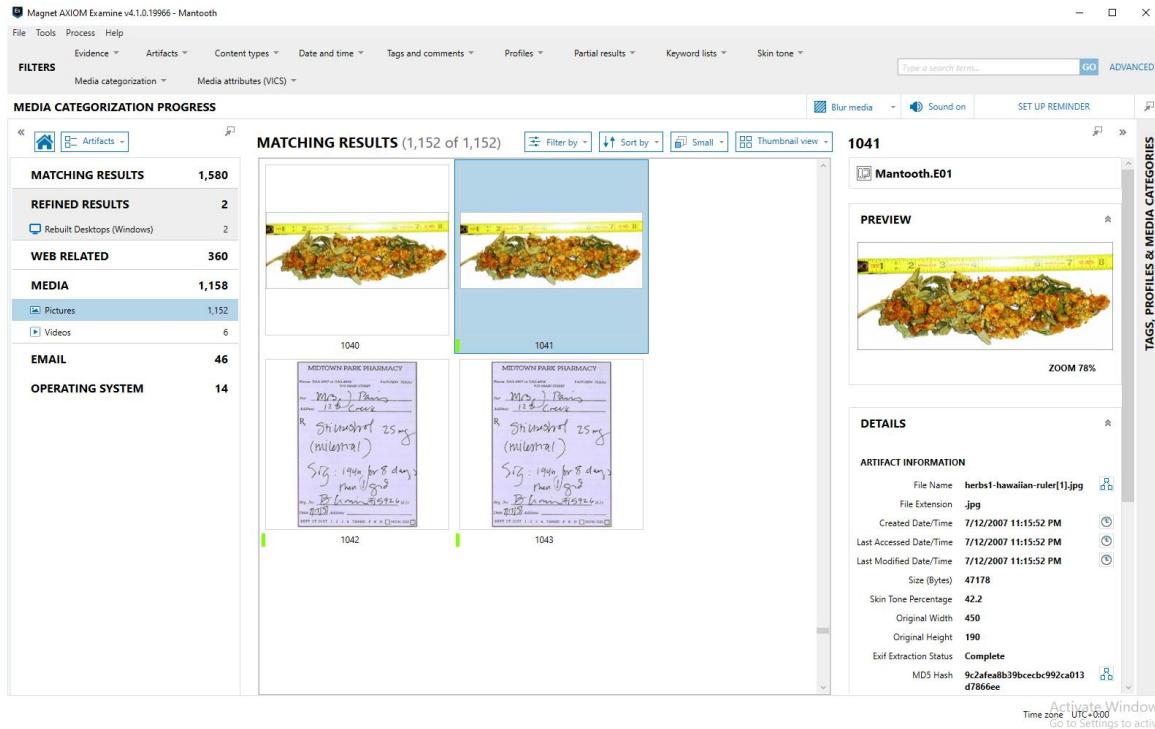


Figure 4.8

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

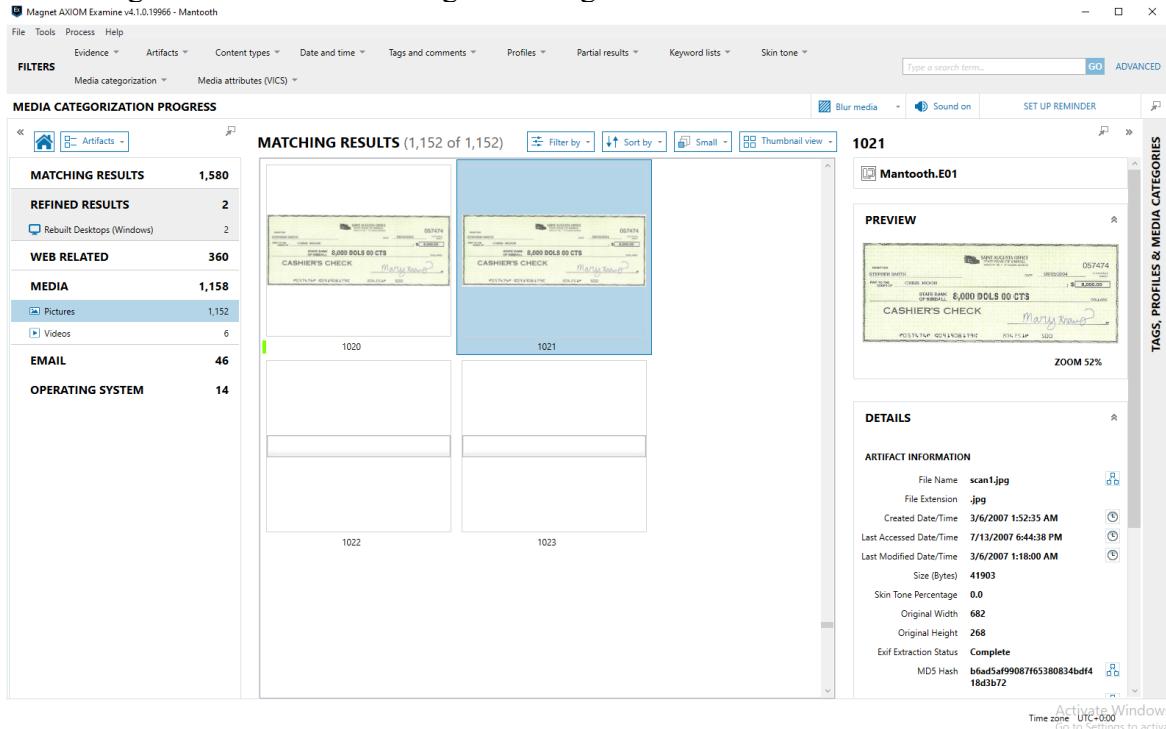


Figure 4.9

Figure 4.9 contains a cashier's check.

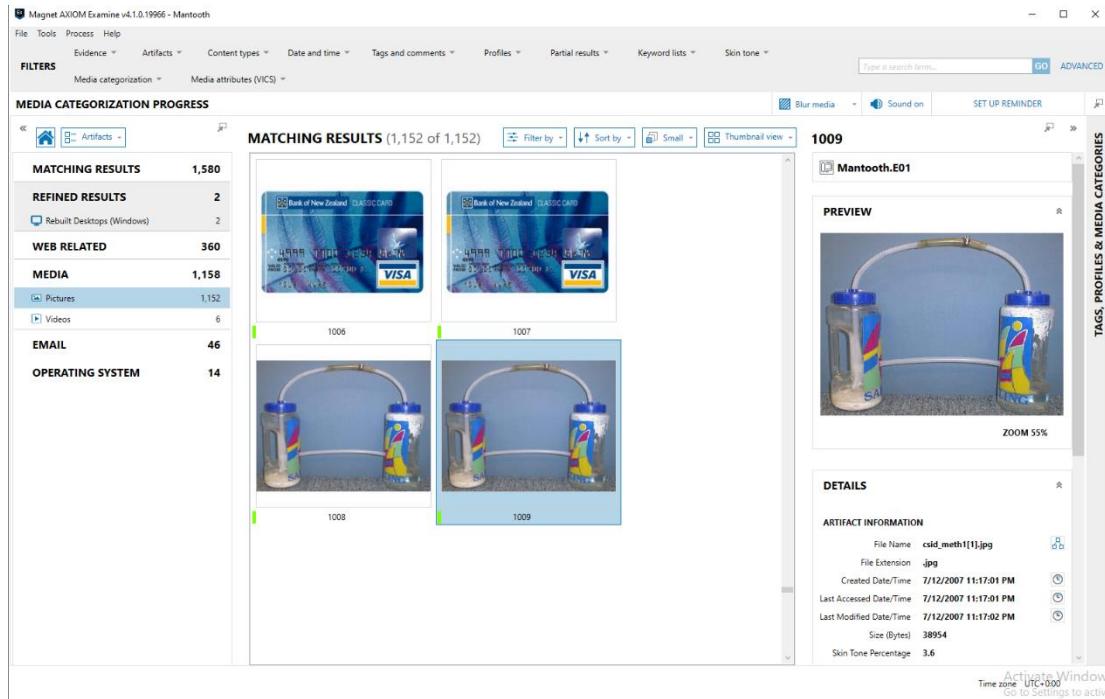


Figure 5.0

Figure 5.0 contains an image of equipment for meth production

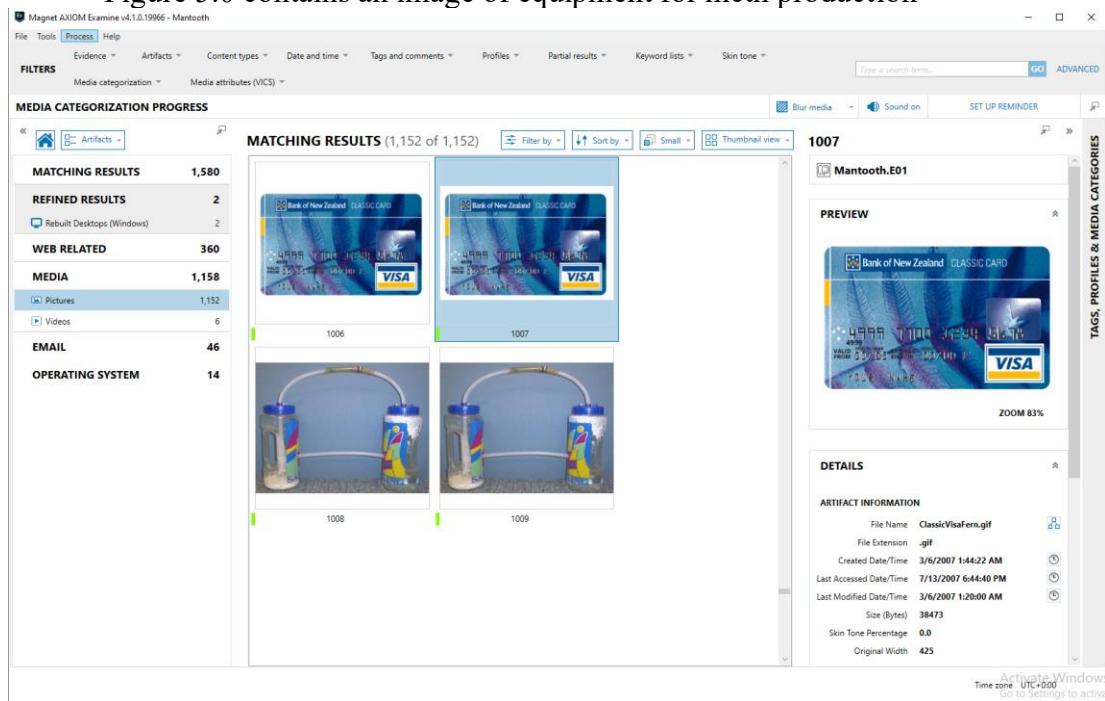


Figure 5.1

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

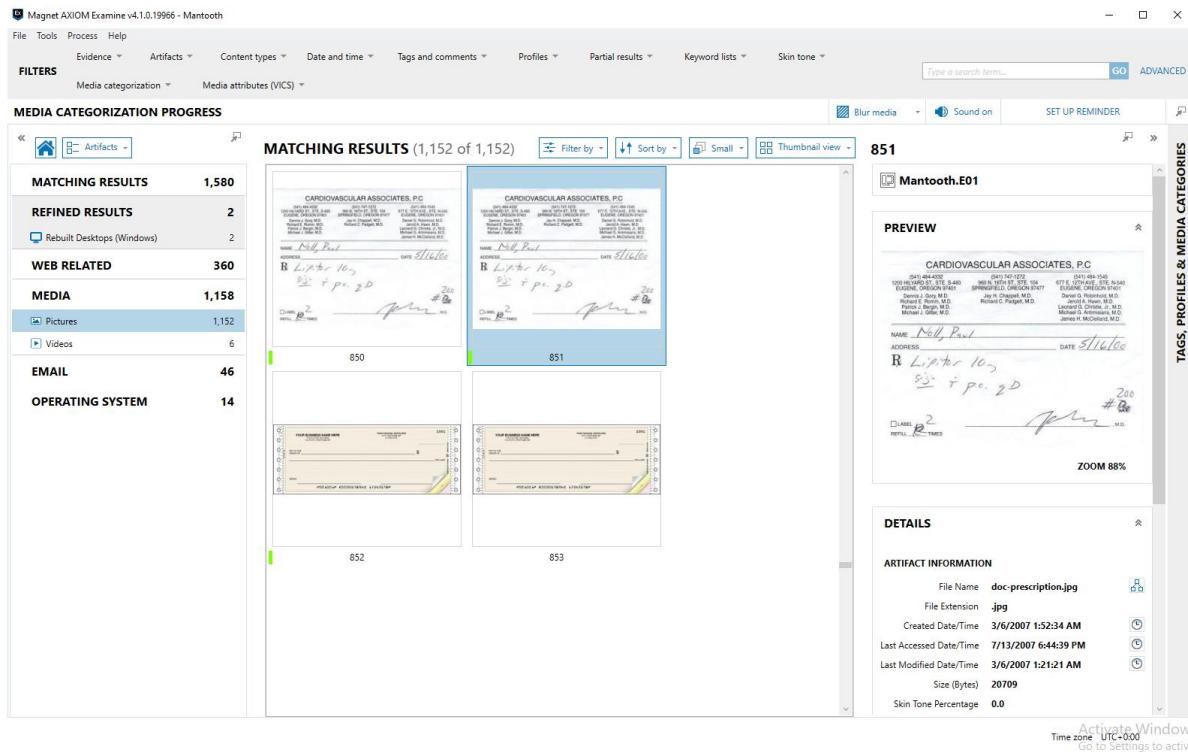


Figure 5.2

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

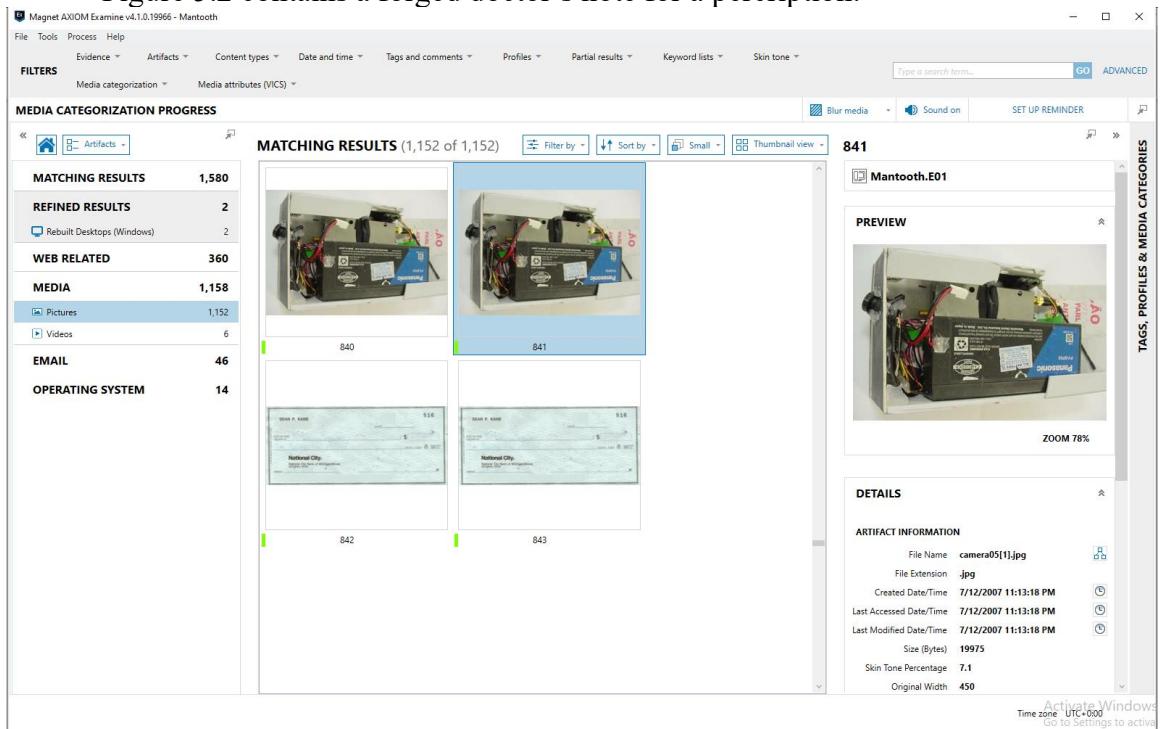


Figure 5.3

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

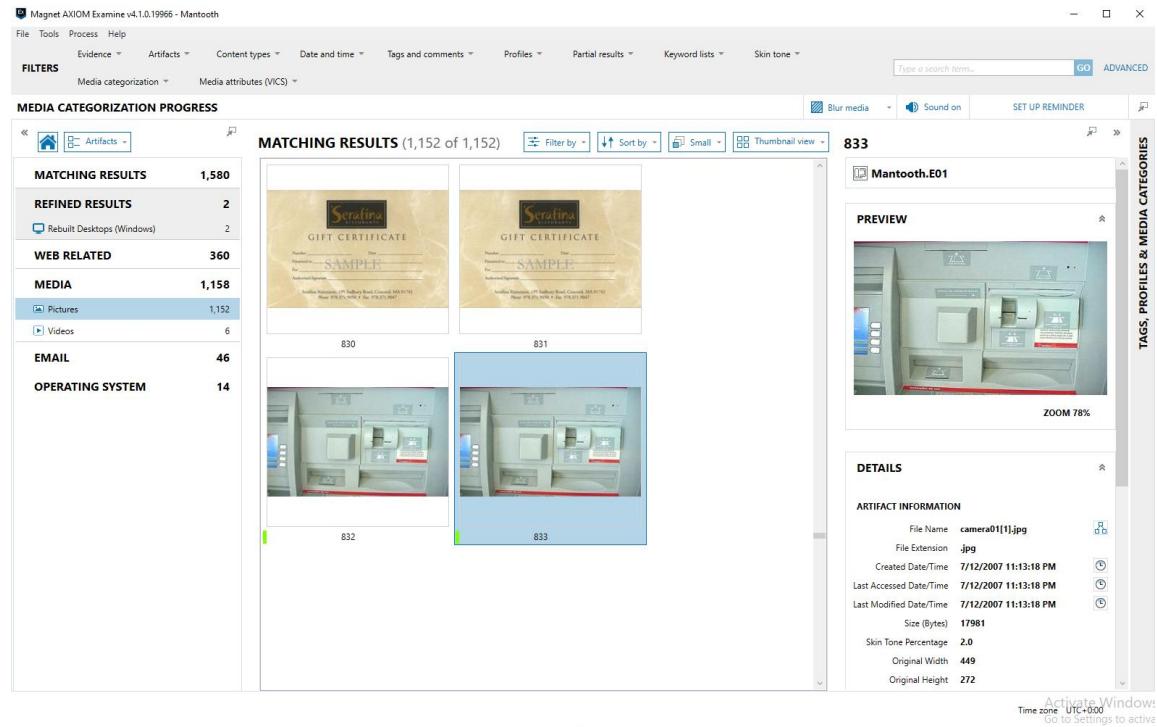


Figure 5.4

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

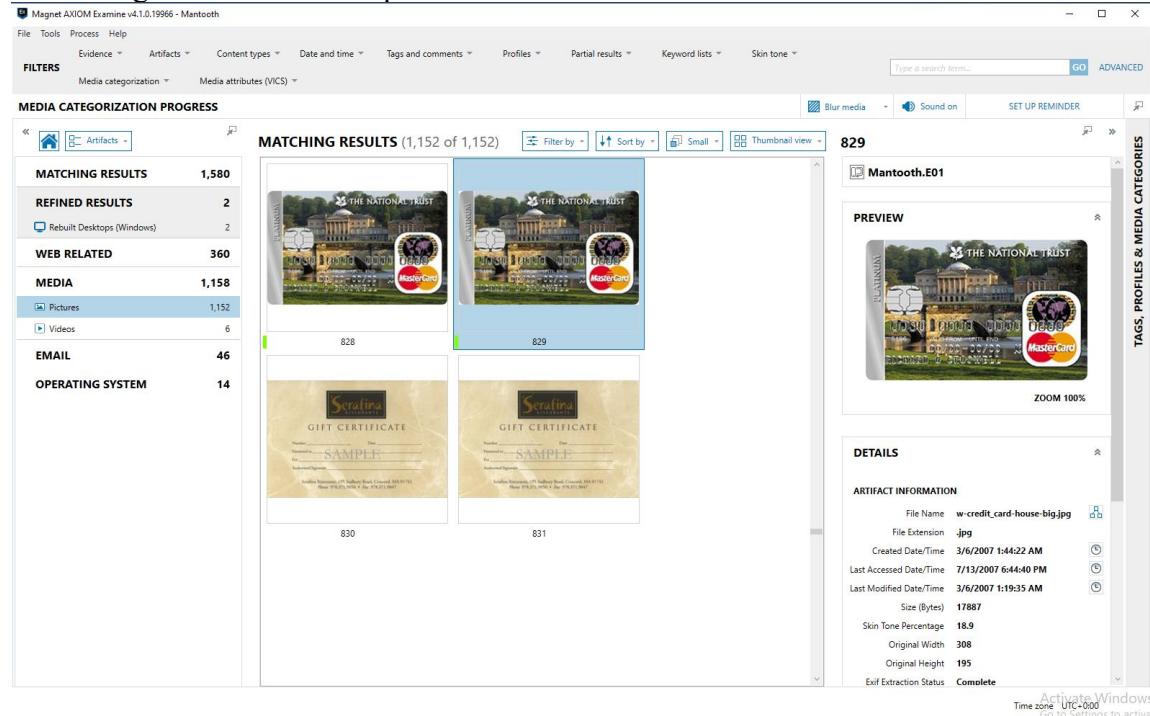


Figure 5.5

Figure 5.5 contains a picture of a fraudulent credit card.

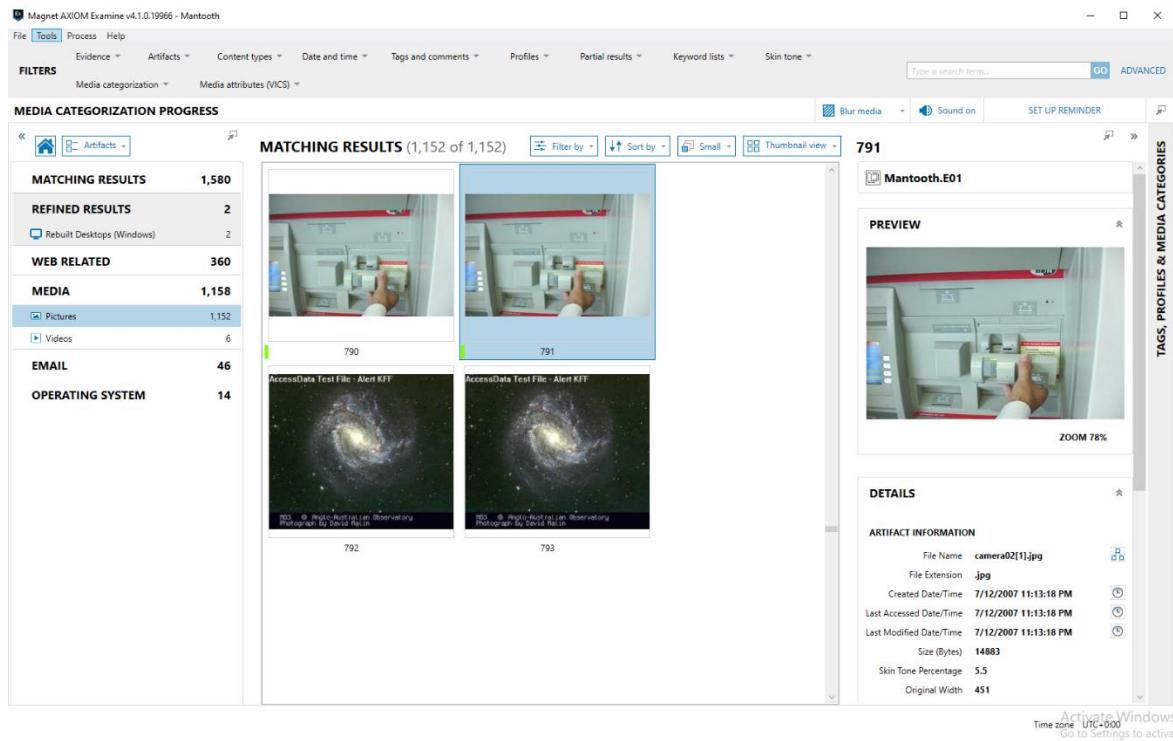


Figure 5.6

Figure 5.6 contains an image of an atm machine

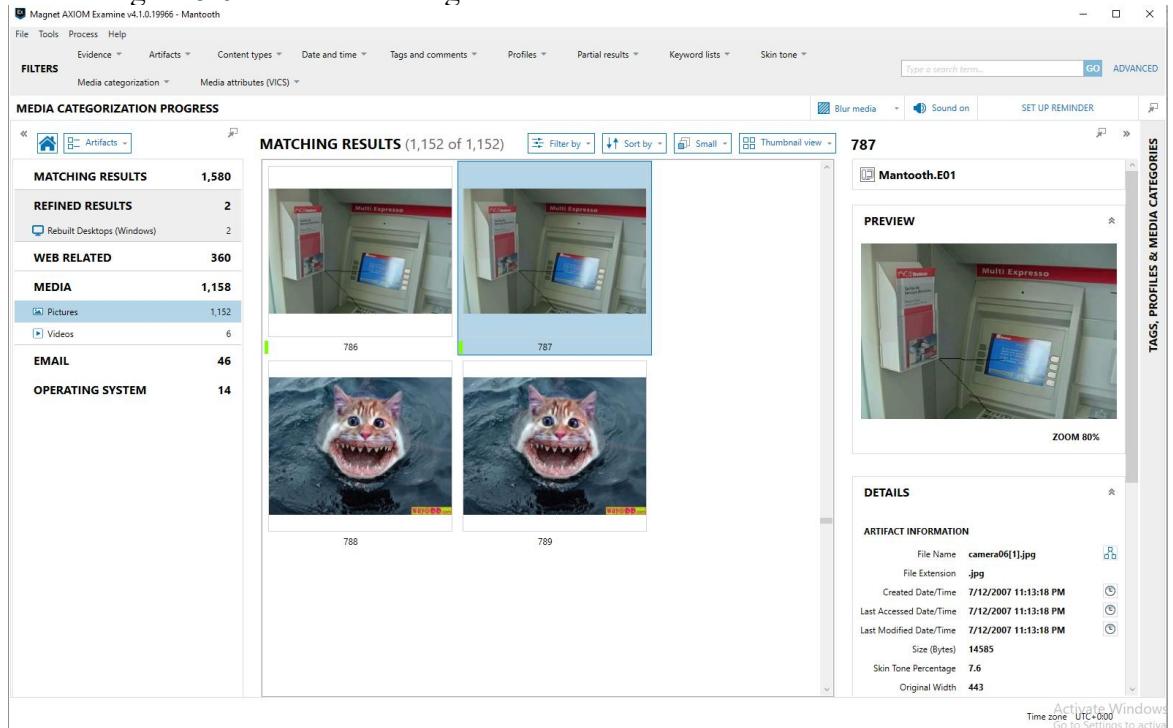


Figure 5.7

Figure 5.8 contains a picture of an atm machine.

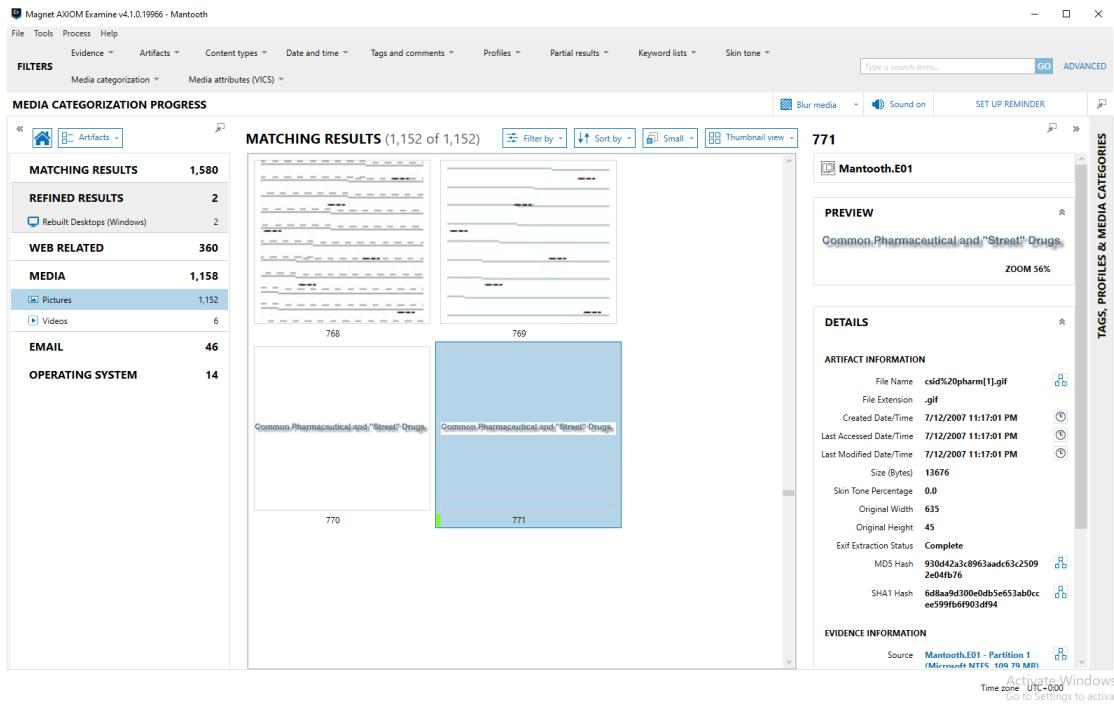


Figure 5.8

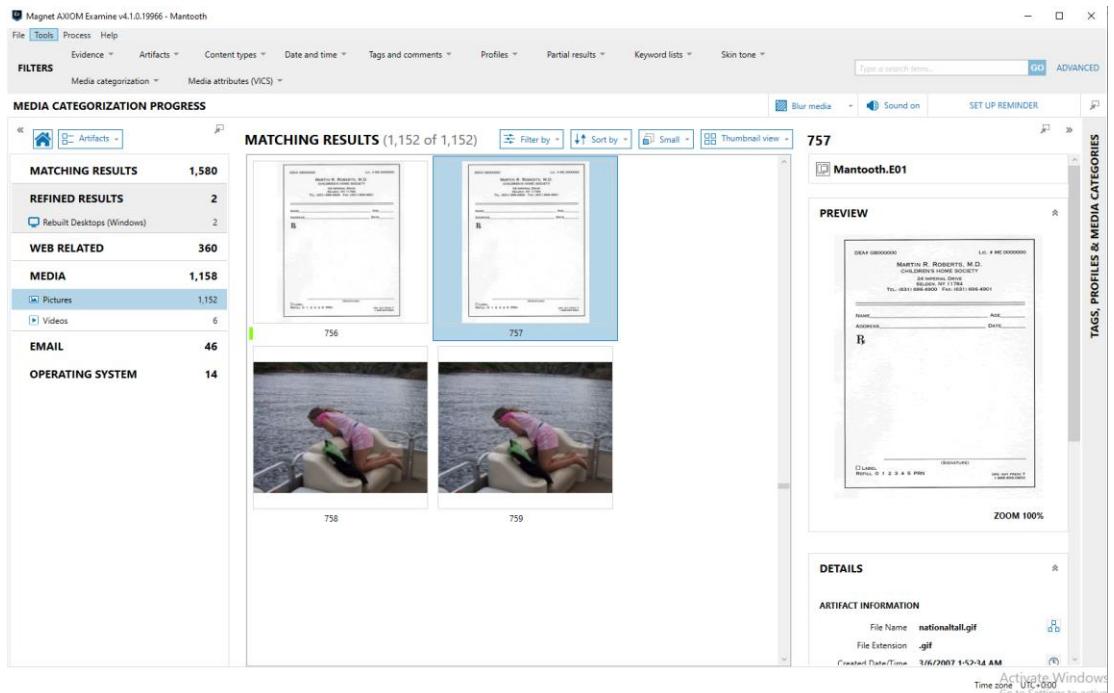


Figure 5.9

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

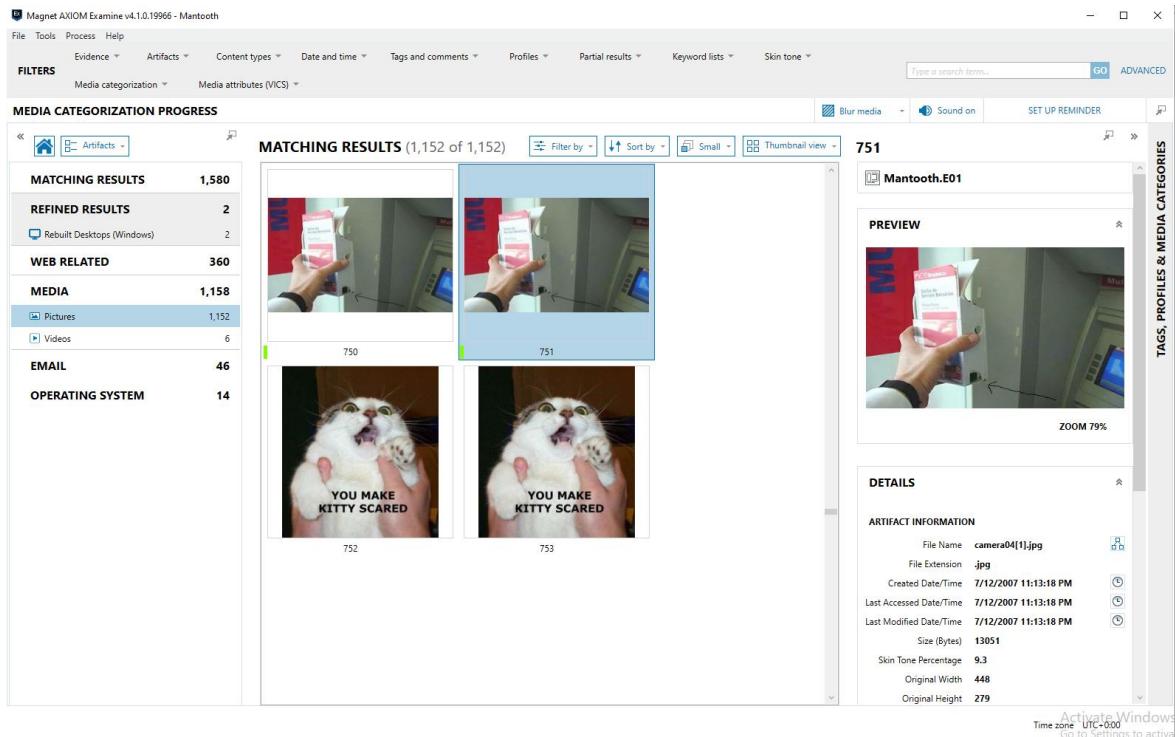


Figure 6.0

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

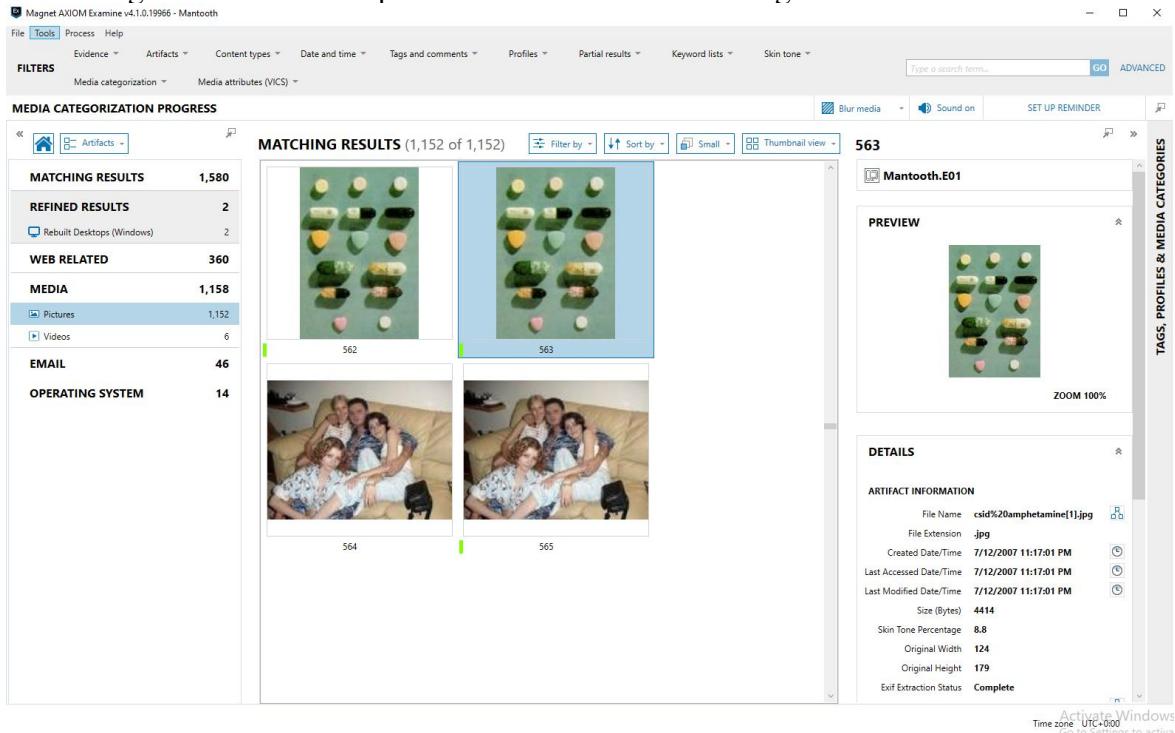


Figure 6.1

Figure 6.1 contains a picture of various pills.

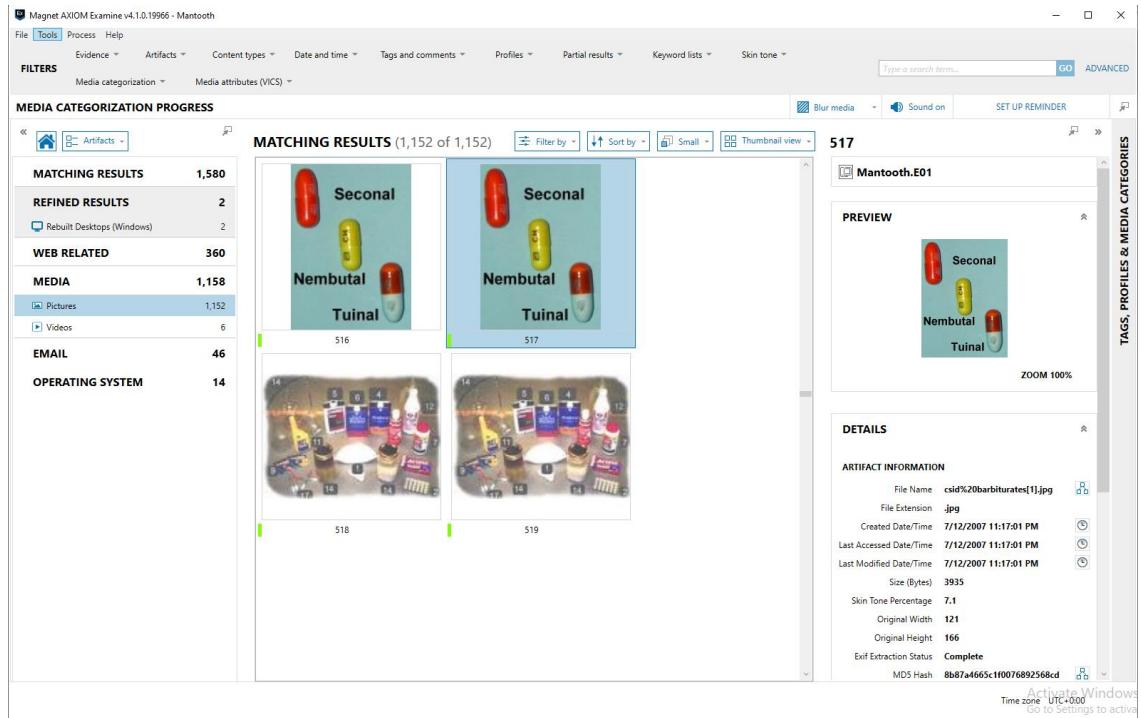


Figure 6.2

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

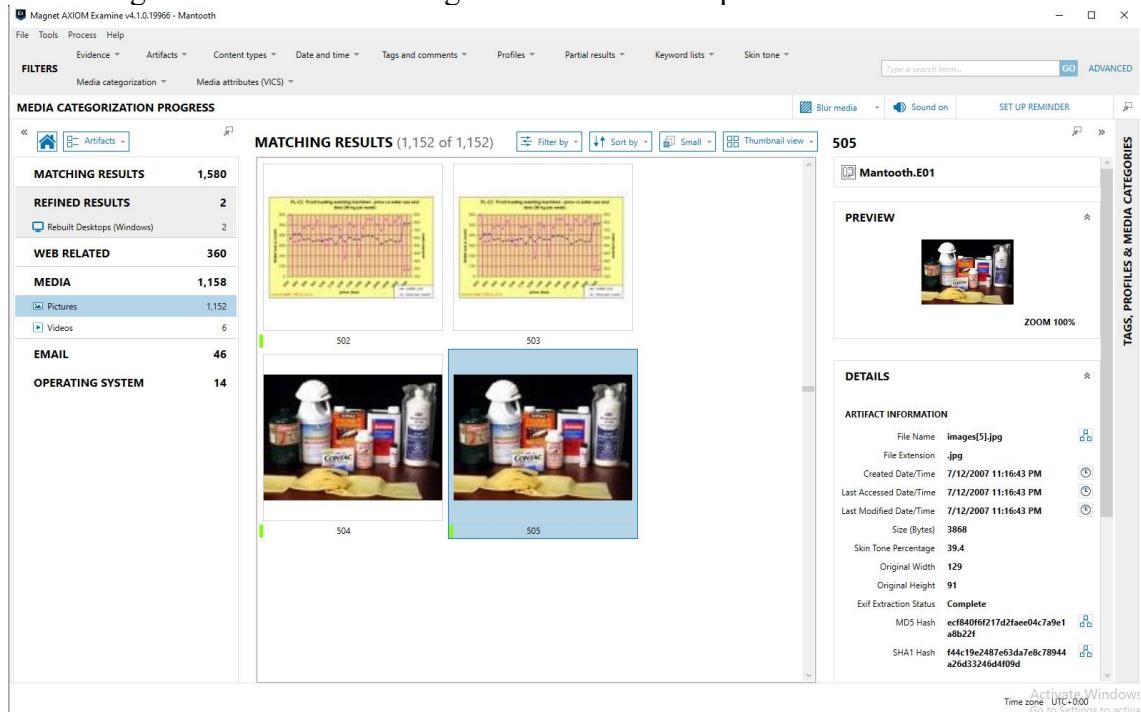


Figure 6.3

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

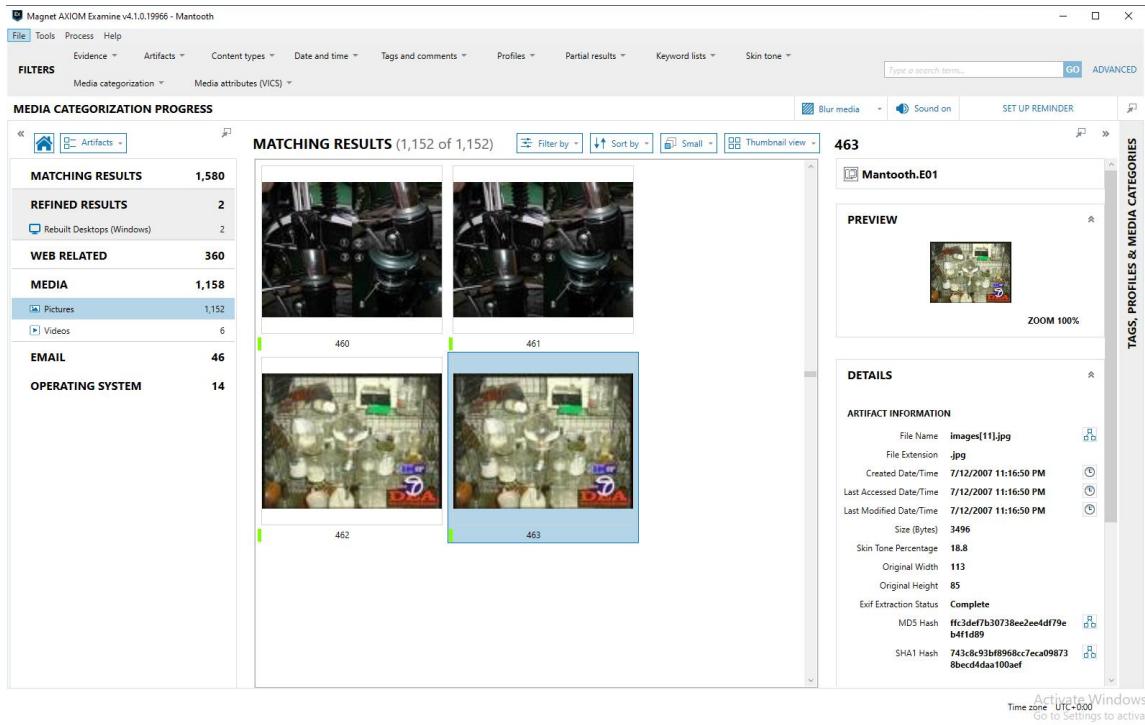


Figure 6.4

Figure 6.4 contains an image of various meth related processes.

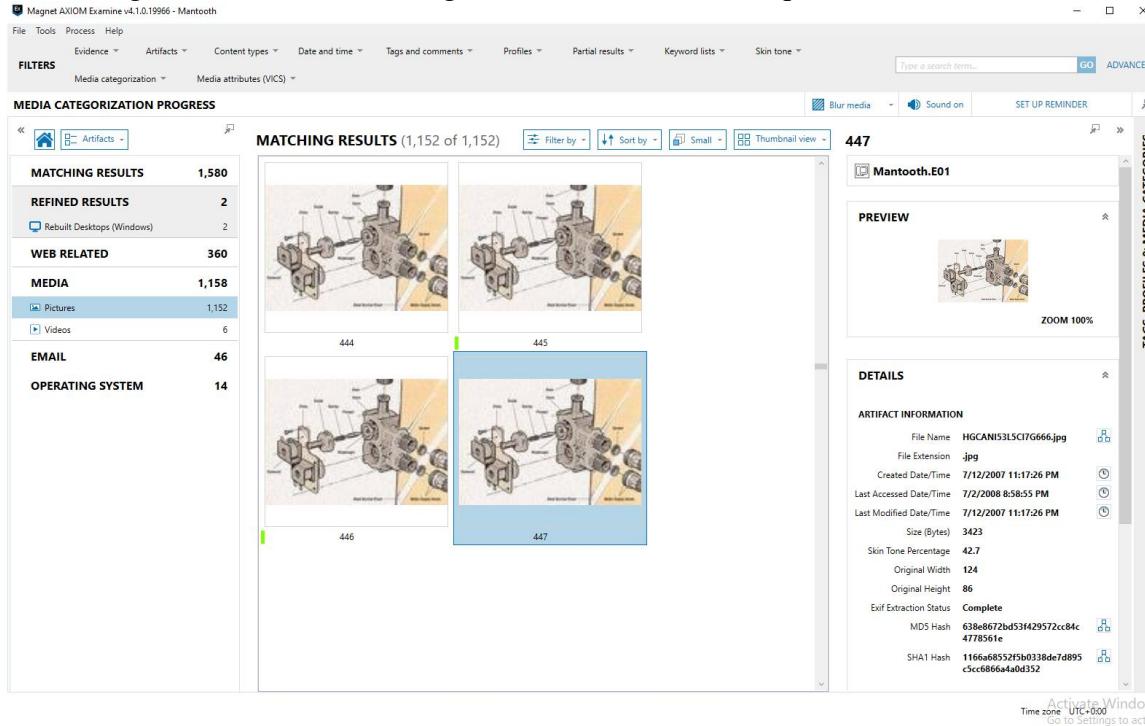


Figure 6.5

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

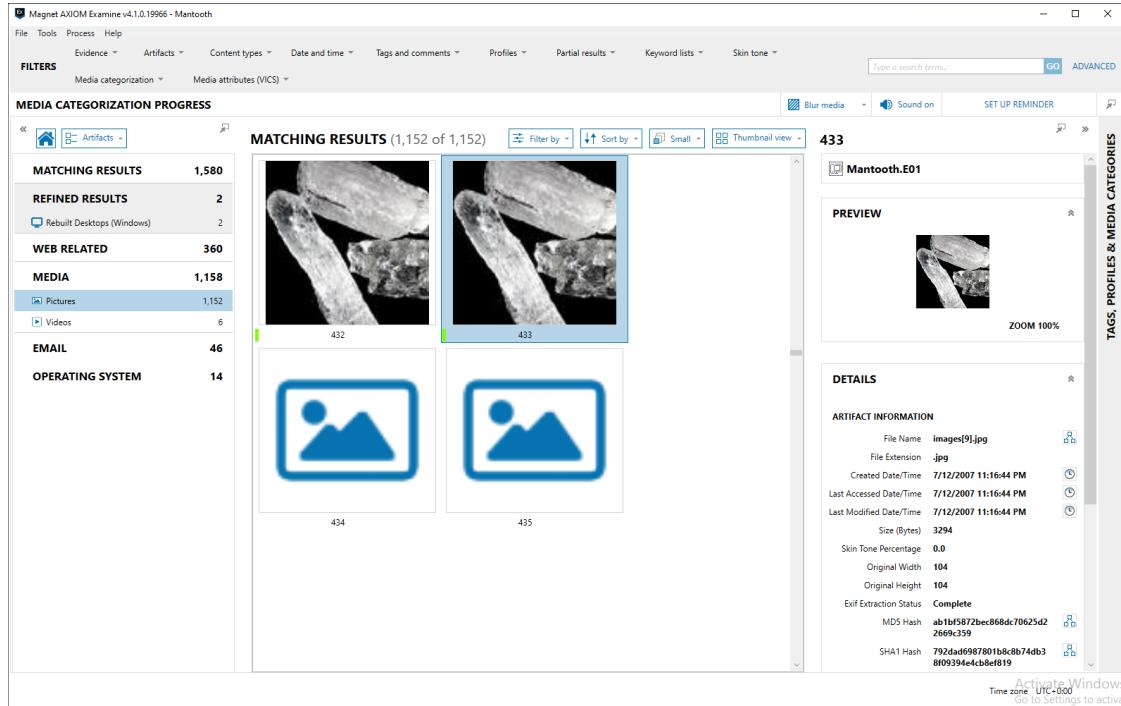


Figure 6.6

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

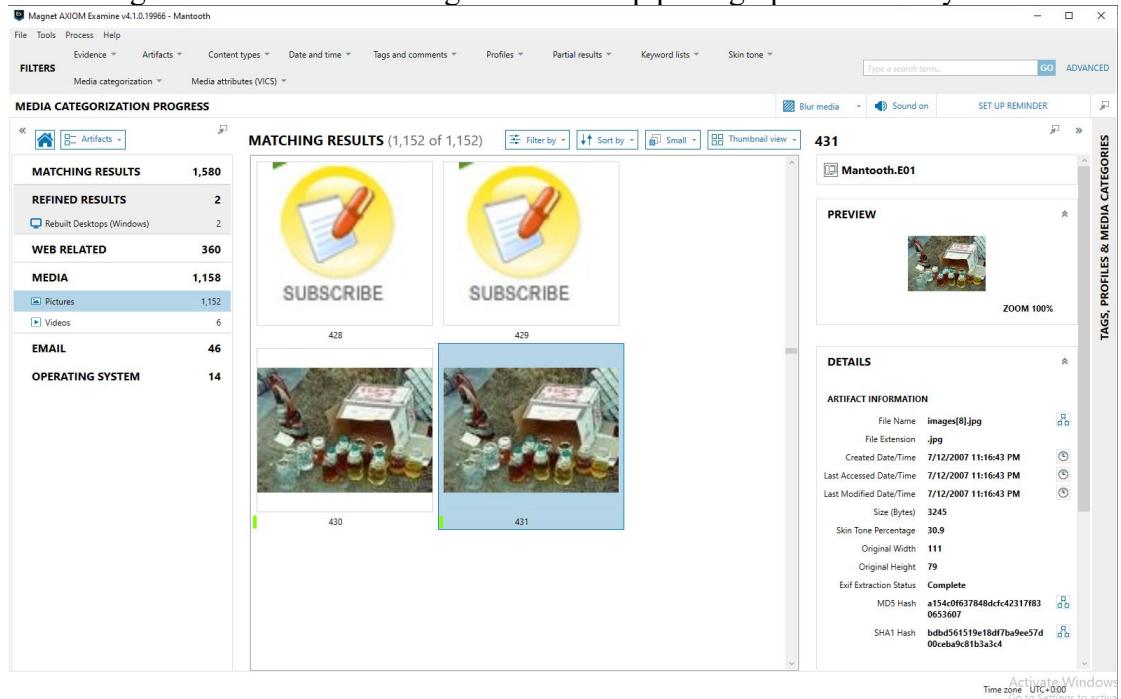


Figure 6.7

Figure 6.7 contains an image of meth production bottles.

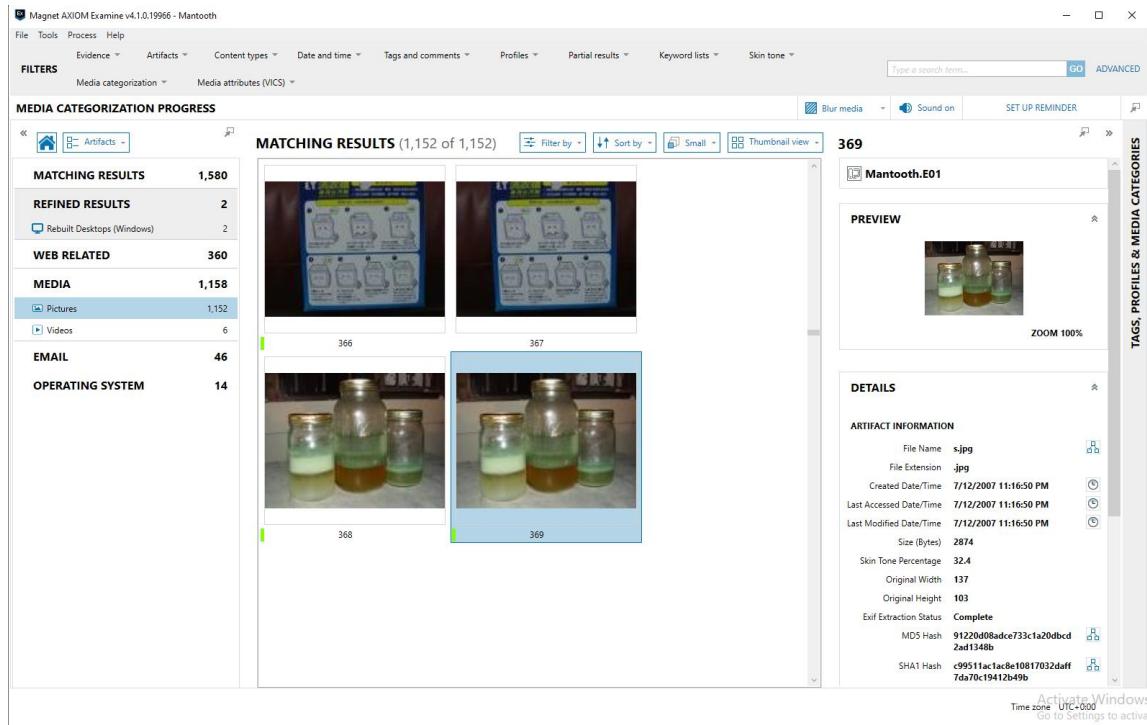


Figure 6.8

Figure 6.8 contains an image of meth bottles.

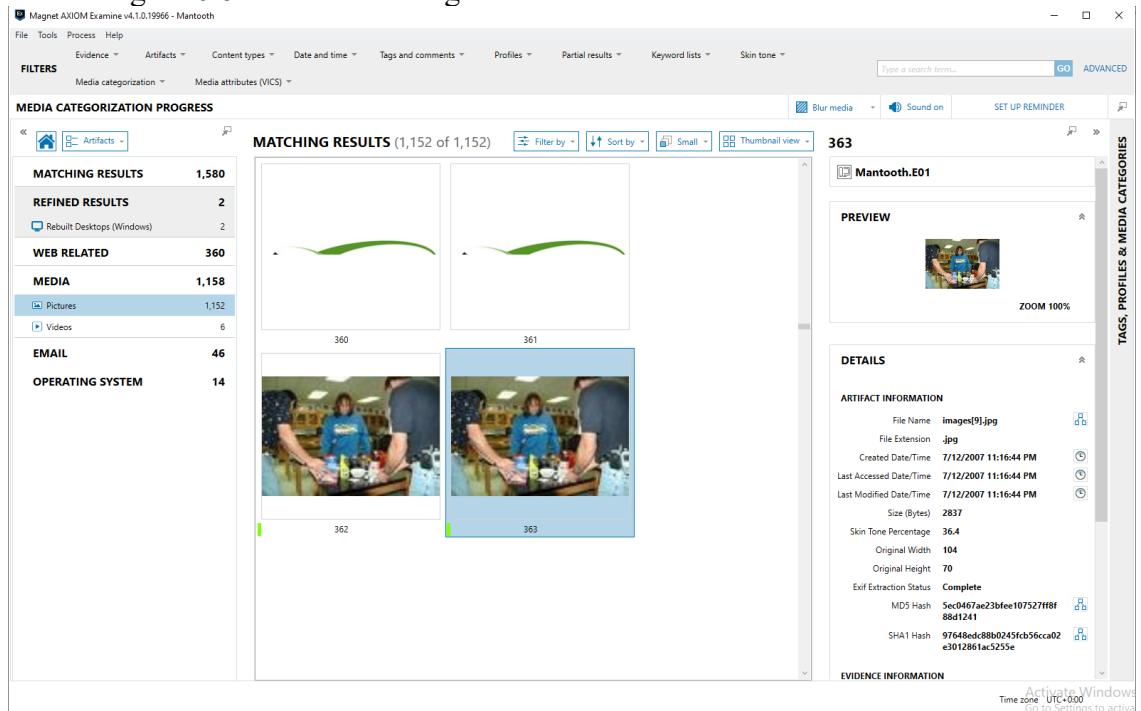


Figure 6.9

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

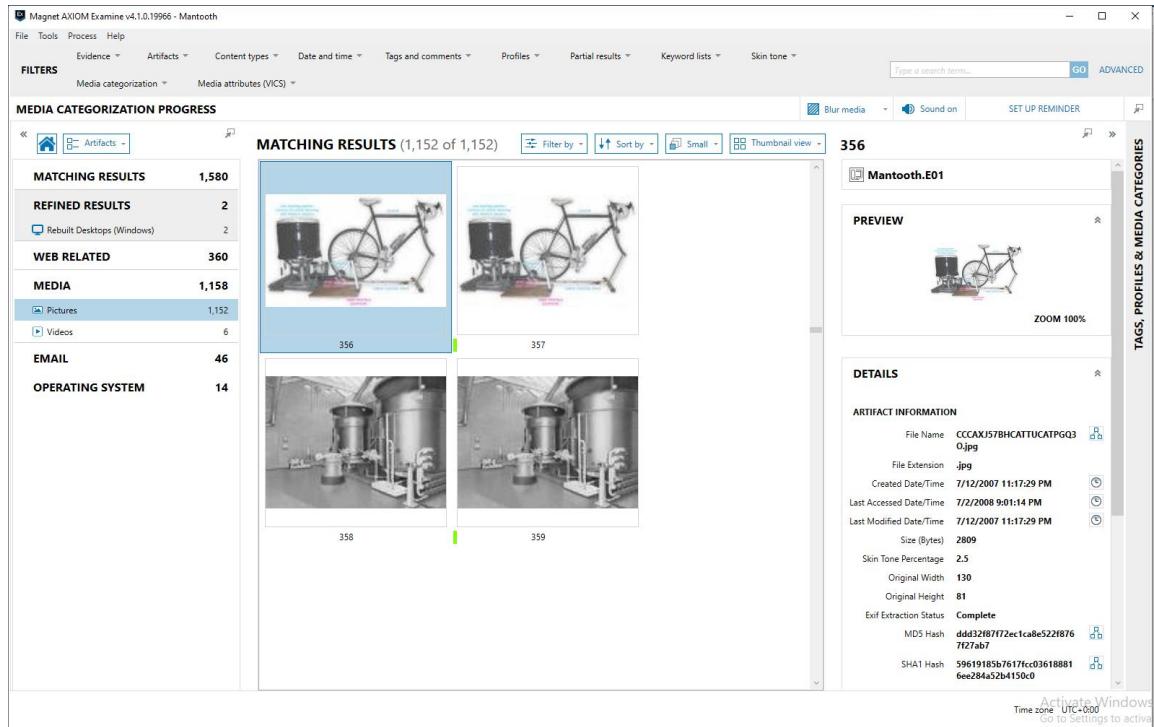


Figure 7.0

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

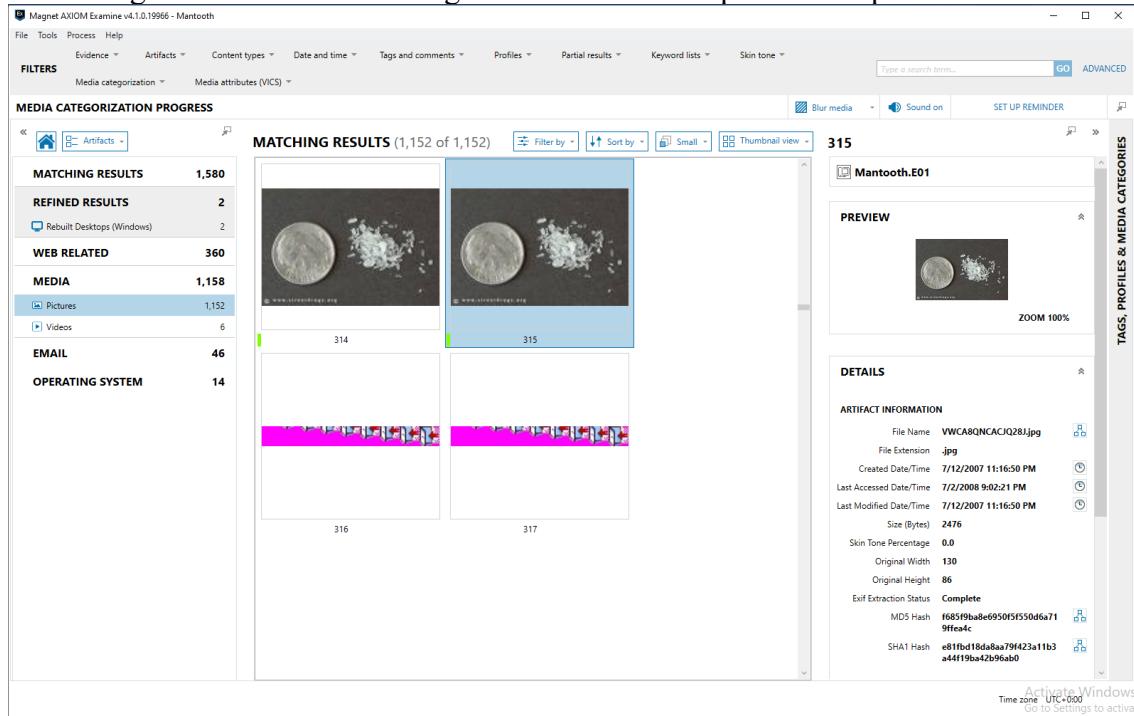


Figure 7.1

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

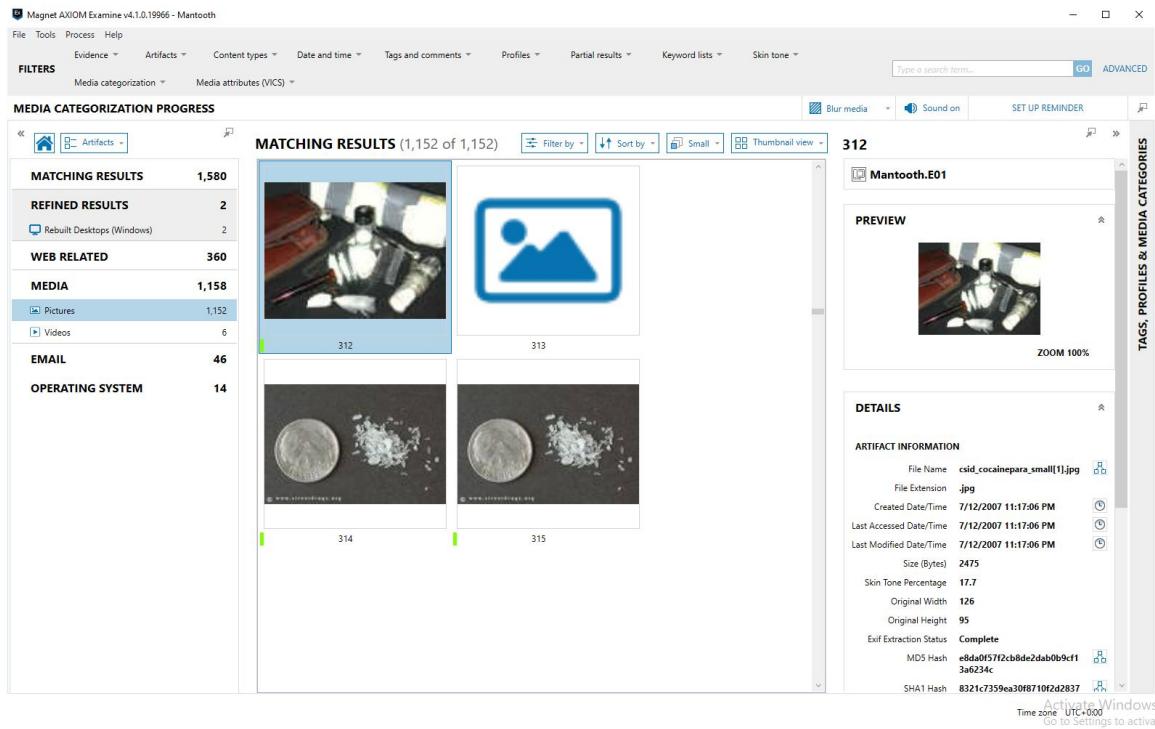


Figure 7.2

Figure 7.2 contains an image of meth ingredients.

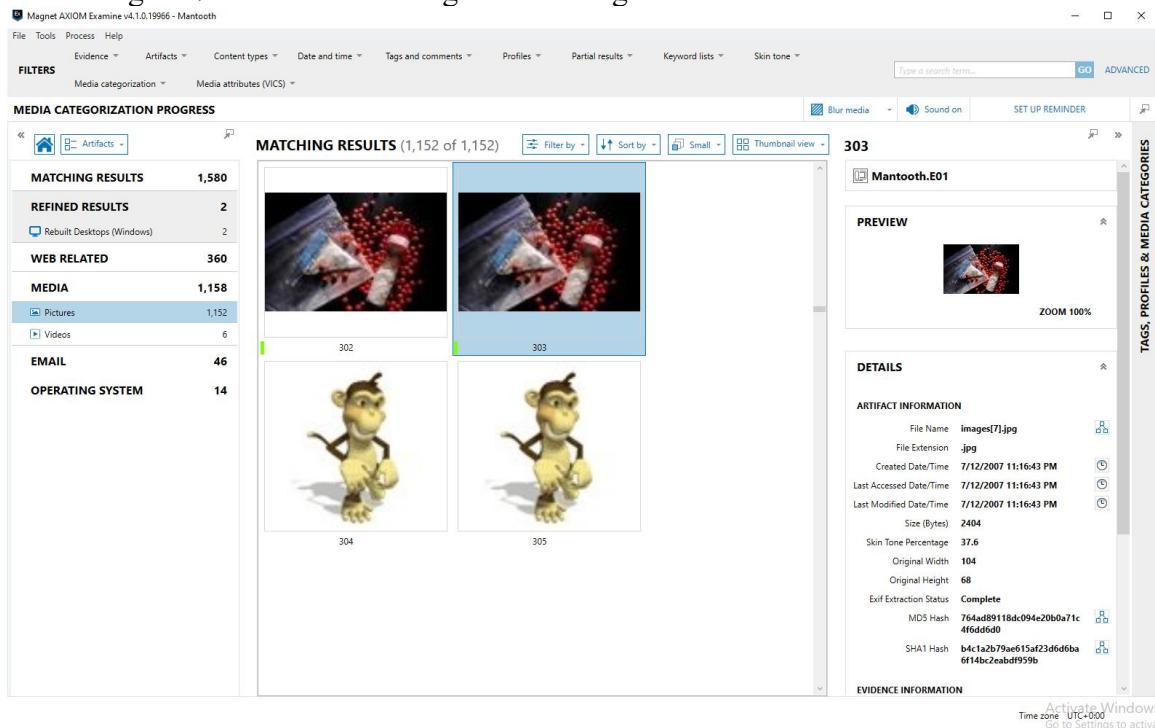


Figure 7.3

Figure 7.3 contains an image of pills.

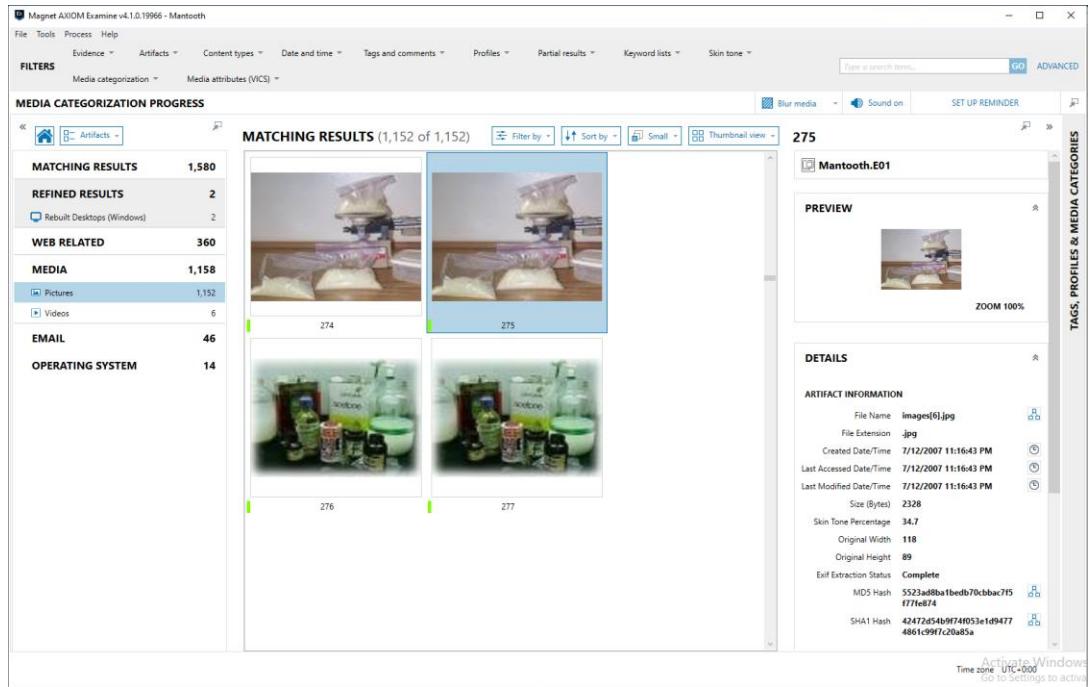


Figure 7.4

Figure 7.4 contains a weighing station for the meth.

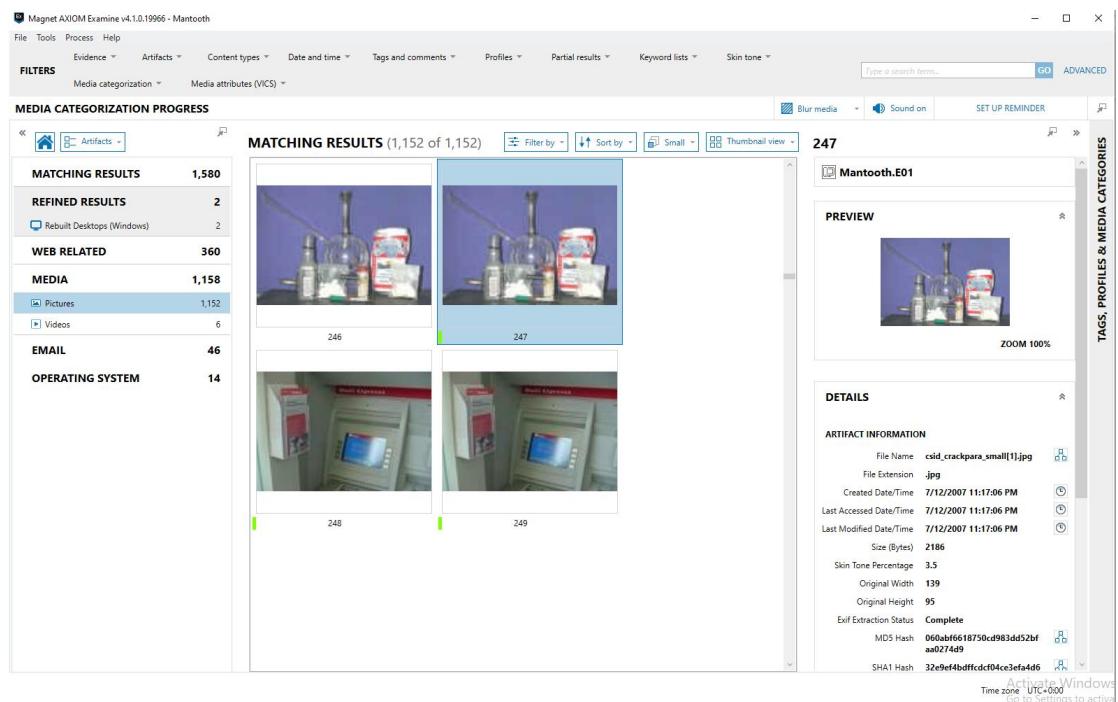


Figure 7.5

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.

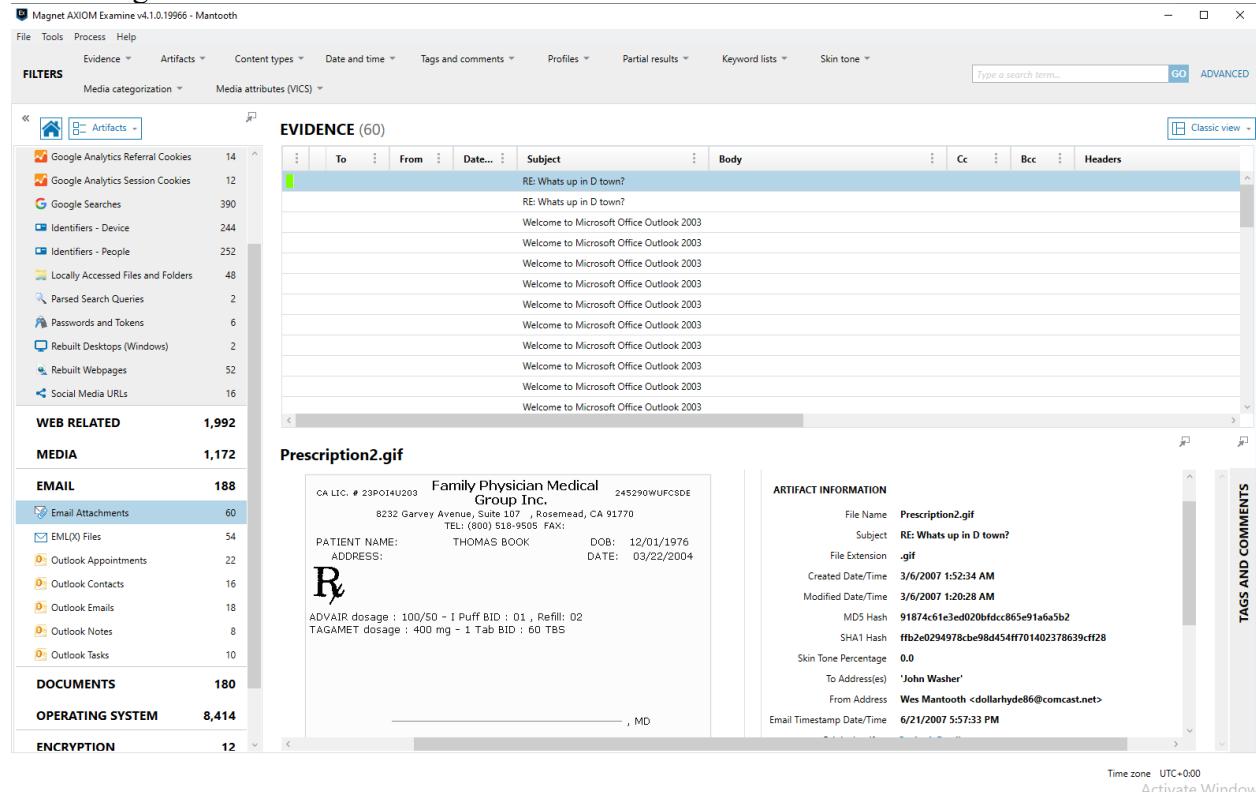


Figure 7.6

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

The screenshot shows the Magnet AXIOM interface with the following details:

- EVIDENCE (60):** A list of artifacts found, including Google Analytics Referral Cookies (14), Google Analytics Session Cookies (12), Google Searches (390), Identifiers - Device (244), Identifiers - People (252), Locally Accessed Files and Folders (48), Parsed Search Queries (2), Passwords and Tokens (6), Rebuilt Desktops (Windows) (2), Rebuilt Webpages (52), and Social Media URLs (16).
- WEB RELATED:** Total count is 1,992.
- MEDIA:** Total count is 1,172.
- EMAIL:** Total count is 188, with Email Attachments (60) highlighted.
- DOCUMENTS:** Total count is 180.
- OPERATING SYSTEM:** Total count is 8,414.
- ENCRYPTION:** Total count is 12.

**ARTIFACT INFORMATION (doc-prescription.jpg):**

- File Name: doc-prescription.jpg
- Subject: RE: Whats up in D town?
- File Extension: jpg
- Created Date/Time: 3/6/2007 1:52:34 AM
- Modified Date/Time: 3/6/2007 1:52:11 AM
- MDS Hash: 362292743f9b6a0c6348773e3917f6880
- SHA1 Hash: 212d598e4f69a2a666d09e212120476880
- Skin Tone Percentage: 0.0
- To Address(es): 'John Washer'
- From Address: Wes Mantooth <dollarhyde86@comcast.net>
- Email Timestamp Date/Time: 6/21/2007 9:03:29 PM

**TAGS AND COMMENTS:** Time zone UTC+000, Activate Windows.

Figure 7.7

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

The screenshot shows the Magnet AXIOM interface with the following details:

- EVIDENCE (60):** A list of artifacts found, including Google Analytics Referral Cookies (14), Google Analytics Session Cookies (12), Google Searches (390), Identifiers - Device (244), Identifiers - People (252), Locally Accessed Files and Folders (48), Parsed Search Queries (2), Passwords and Tokens (6), Rebuilt Desktops (Windows) (2), Rebuilt Webpages (52), and Social Media URLs (16).
- WEB RELATED:** Total count is 1,992.
- MEDIA:** Total count is 1,172.
- EMAIL:** Total count is 188, with Email Attachments (60) highlighted.
- DOCUMENTS:** Total count is 180.
- OPERATING SYSTEM:** Total count is 8,414.
- ENCRYPTION:** Total count is 12.

**ARTIFACT INFORMATION (Confidential Business Letter.doc):**

- File Name: Confidential Business Letter.doc
- Subject: Letter
- File Extension: .doc
- MDS Hash: 8c7789850ac1d2f3920d87d1e850455
- SHA1 Hash: 3d9ec5404ad27360c3bacb7e2e9d93a8eb1f58c6
- To Address(es): chkwasher@comcast.net, dollarhyde86@comcast.net, molerman20@hotmail.com, skimmerman27@hotmail.com
- From Address: Rasco Badguy <txkidd@swbell.net>
- Email Timestamp Date/Time: 8/4/2007 4:02:38 PM
- Original artifact: Outlook Emails

**TAGS AND COMMENTS:** Time zone UTC+000, Activate Windows.

Figure 7.8

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

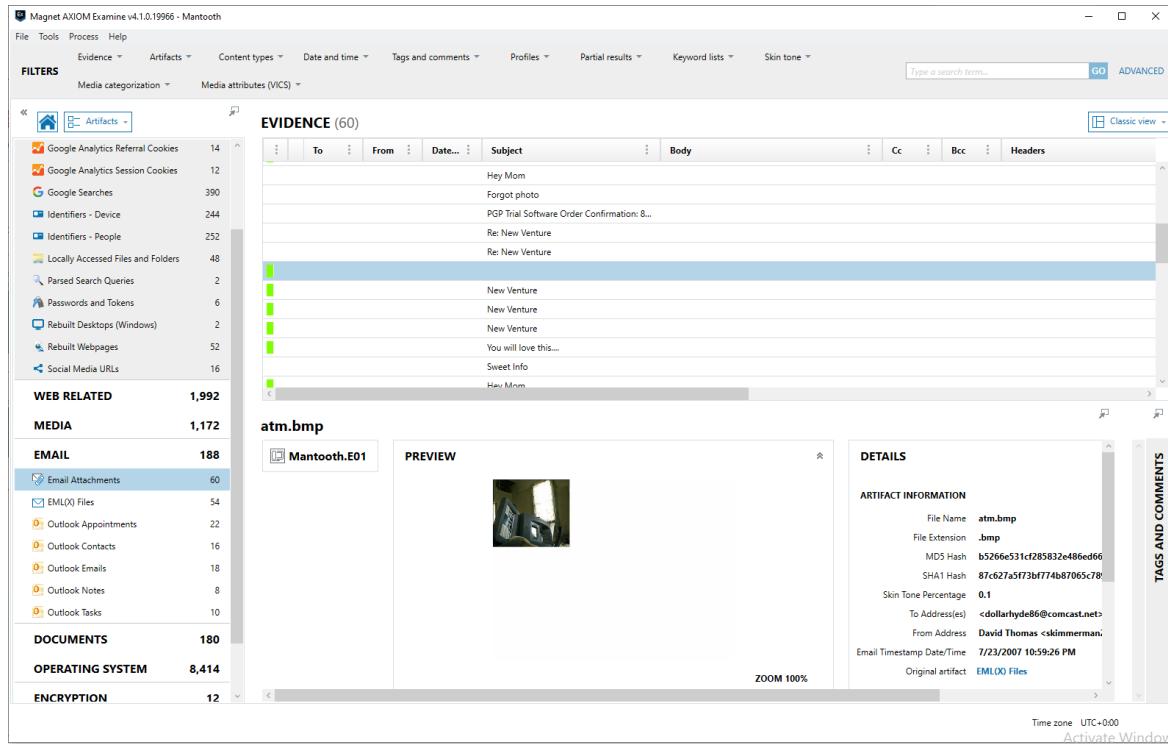


Figure 7.9

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

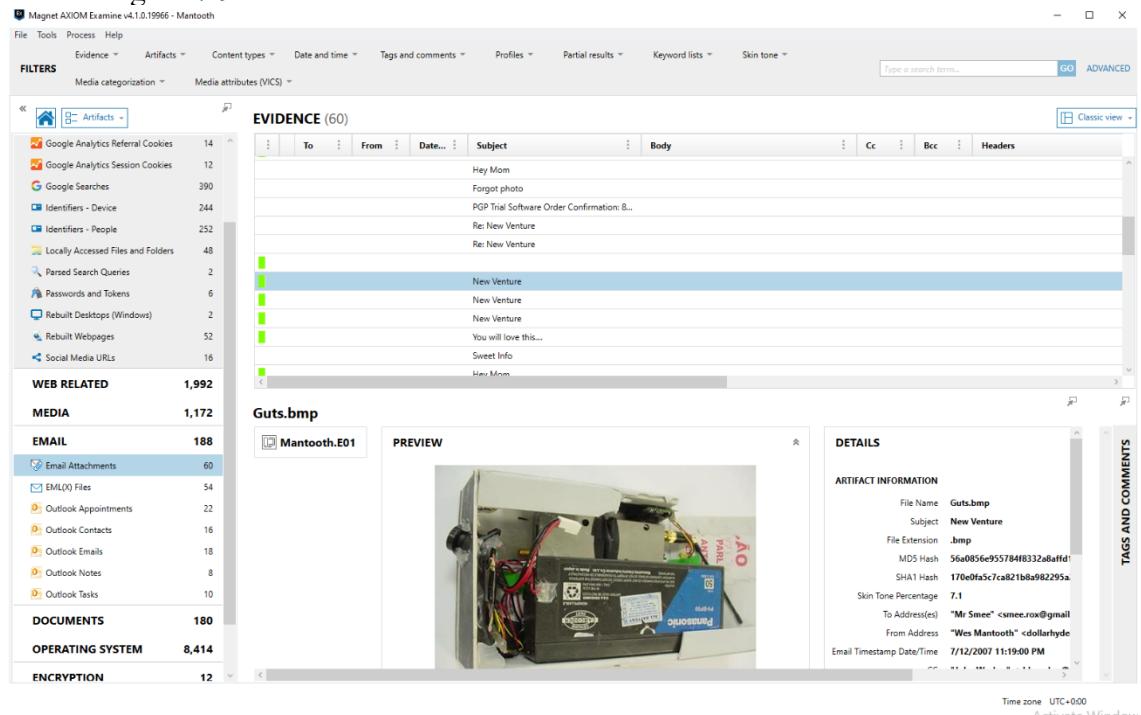


Figure 8.0 – Figure 8.2

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

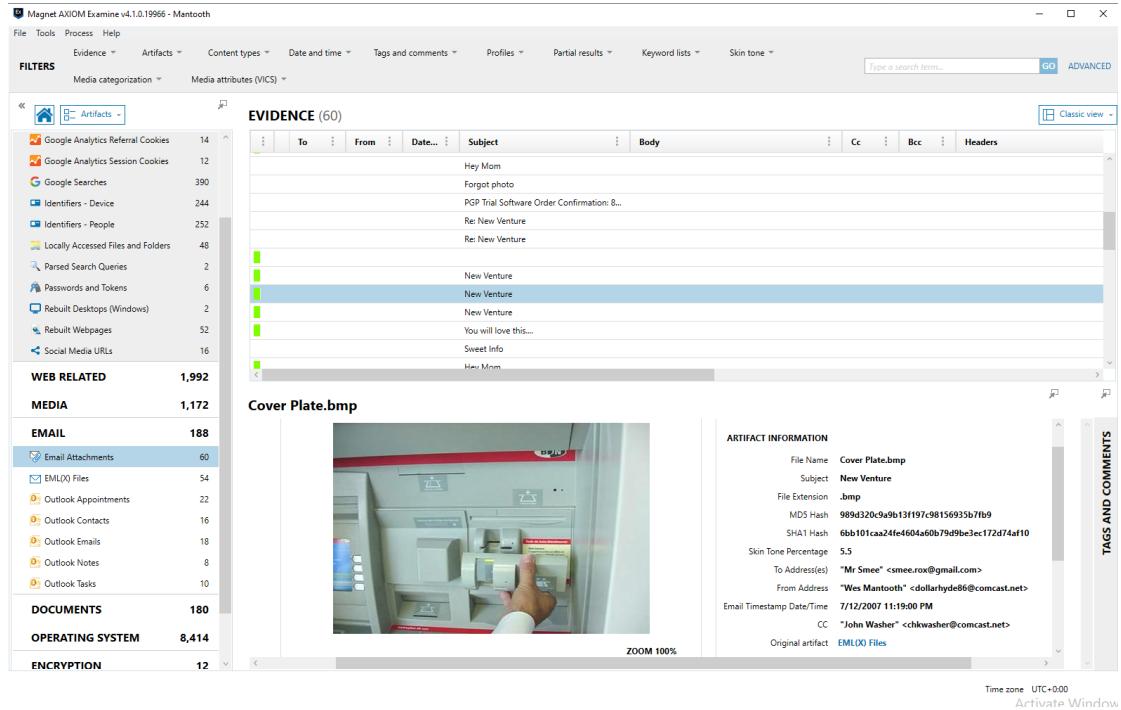


Figure 8.1

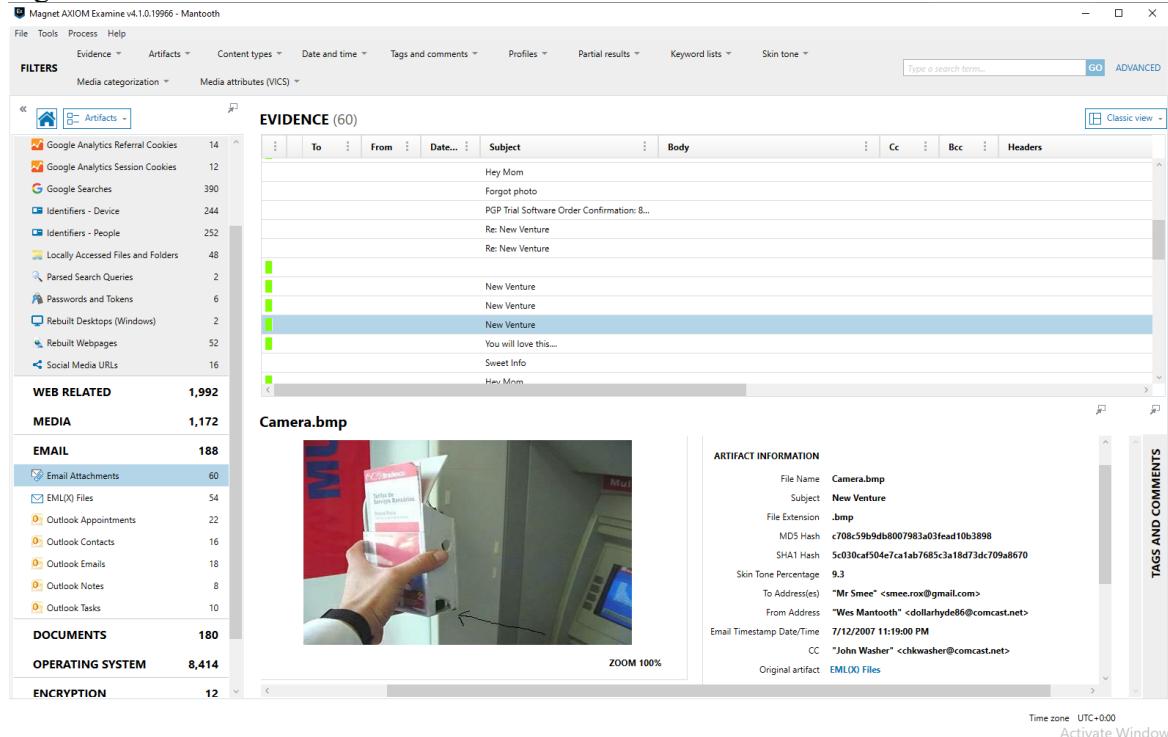


Figure 8.2

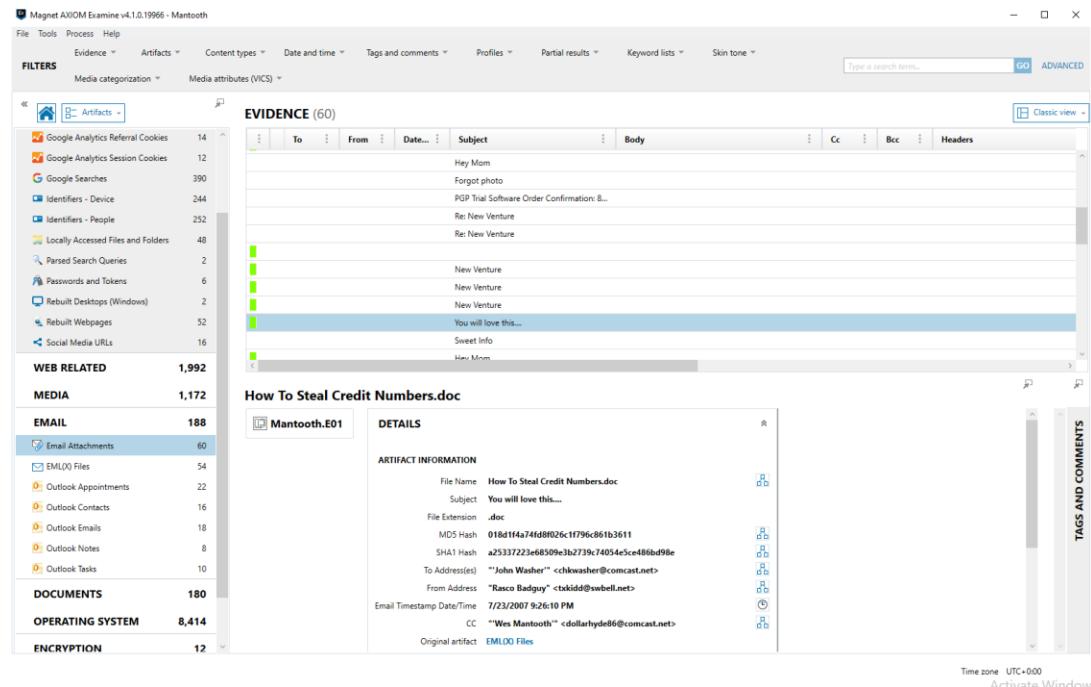


Figure 8.3

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

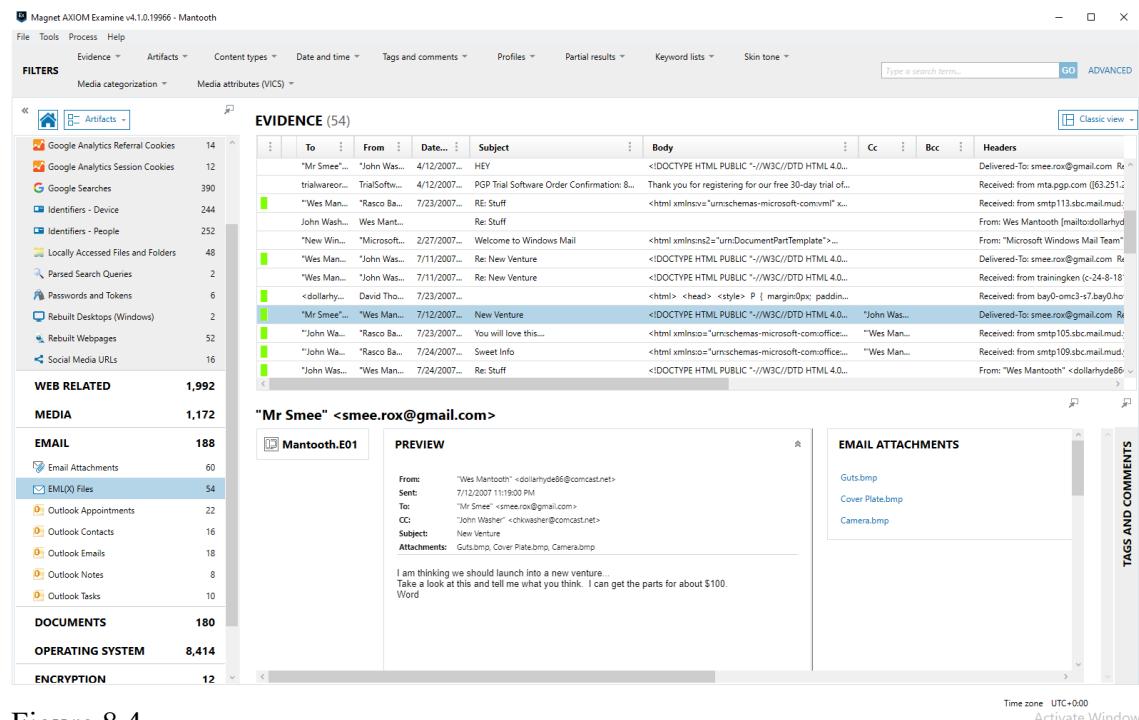


Figure 8.4

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

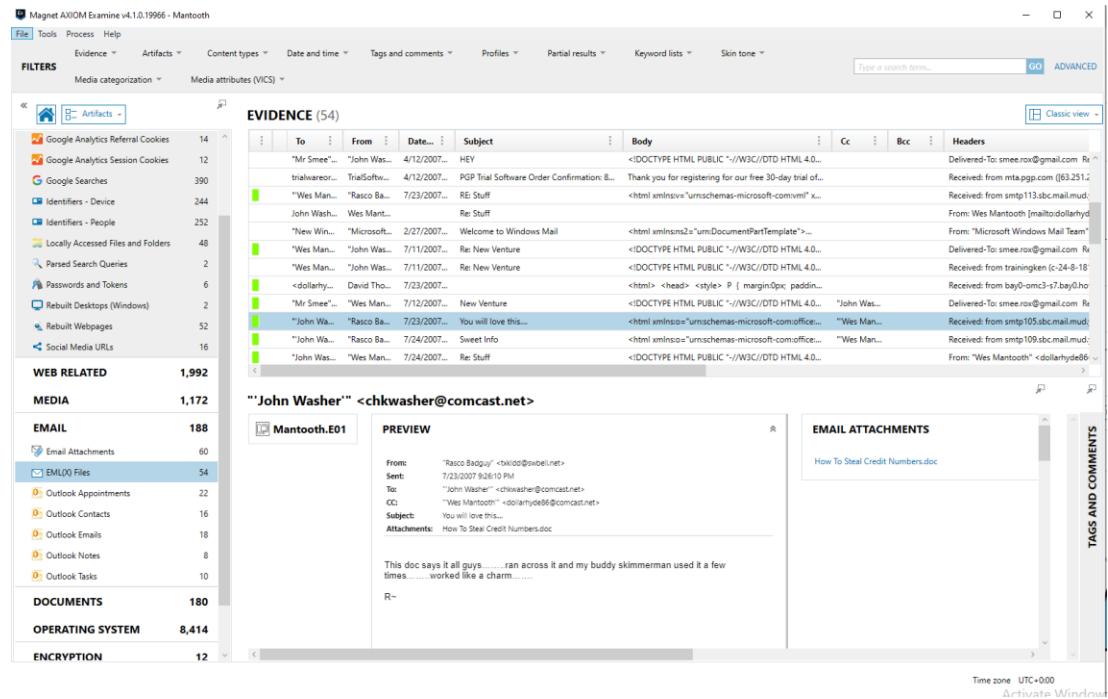


Figure 8.5

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

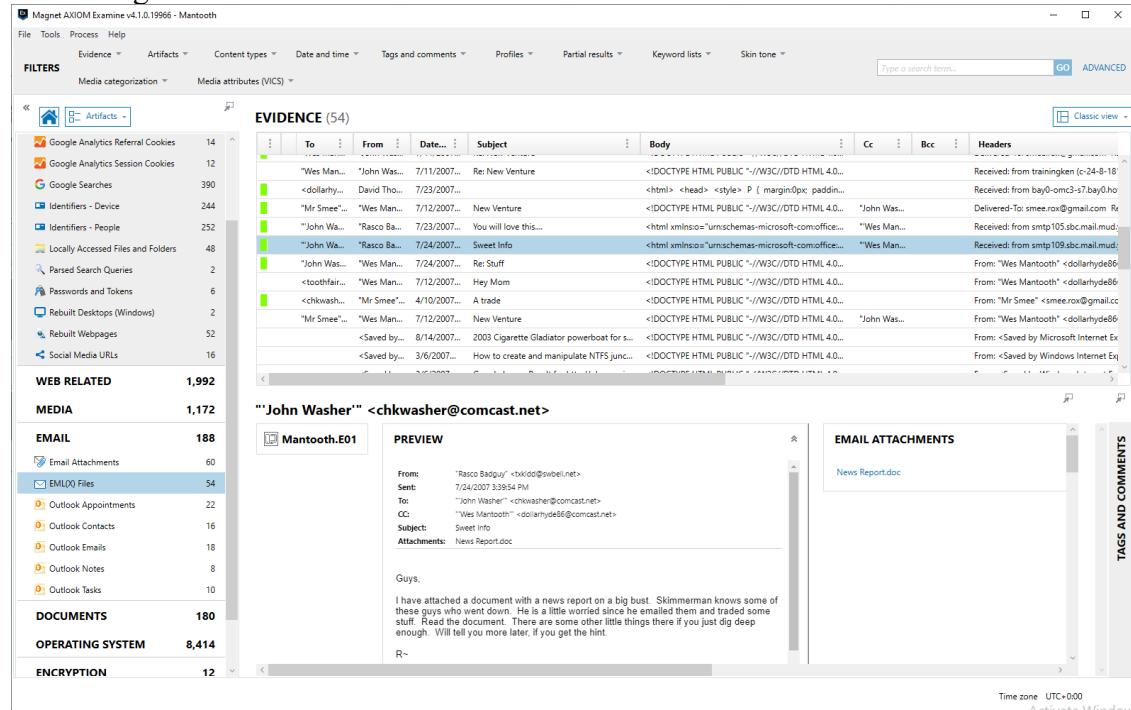


Figure 8.6

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

The screenshot shows the Magnet AXIOM interface with the following details:

- EVIDENCE (54)** table:
 

|    | To             | From          | Date         | Subject                                     | Body                                            | Cc | Bcc | Headers                                    |
|----|----------------|---------------|--------------|---------------------------------------------|-------------------------------------------------|----|-----|--------------------------------------------|
| 1  | <university... | David...@...  | 7/25/2007... | New Venture                                 | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...  |    |     | Received: from univ...unmc...s7.oxyuni...  |
| 2  | "Mr Smee"...   | "Wes Man..."  | 7/12/2007... | You will love this...                       | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...  |    |     | Delivered-To: smee.rox@gmail.com Rx        |
| 3  | "John Wa..."   | "Rasco Ba..." | 7/23/2007... | Sweet Info                                  | <html xmlns="urn:schemas-microsoft-com:offic... |    |     | Received: from smtp105.sbcmail.mud...      |
| 4  | "John Wa..."   | "Rasco Ba..." | 7/24/2007... | Re: Stuff                                   | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...  |    |     | Received: from smtp105.sbcmail.mud...      |
| 5  | "John Was..."  | "Wes Man..."  | 7/24/2007... | Hey Mom                                     | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...  |    |     | From: <Wes Mantooth> <dollarhyde66...      |
| 6  | <othofair...   | "Wes Man..."  | 7/12/2007... | A trade                                     | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...  |    |     | From: <Wes Mantooth> <dollarhyde66...      |
| 7  | <chkwash...    | "Mr Smee"...  | 4/10/2007... | New Venture                                 | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...  |    |     | From: "Mr Smee" <smee.rox@gmail.cc         |
| 8  | "Mr Smee"...   |               | 8/14/2007... | 2003 Cigarette Gladiator powerboat for s... | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...  |    |     | From: "Wes Mantooth" <dollarhyde66...      |
| 9  |                |               | 3/6/2007...  | How to create and manipulate NTFS junc...   | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...  |    |     | From: <Saved by Microsoft Internet Ex...   |
| 10 |                |               | 3/6/2007...  | Google Image Result for http://glossary.... | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...  |    |     | From: <Saved by Windows Internet Explor... |
| 11 |                |               | 7/11/2007... | Returned mail: delivery problems encoun...  | A message from <dollarhyde66@comcast.net> wa... |    |     | Received: from rwmcmc13.comcast.net...     |
- ARTIFACT INFORMATION** for the selected email:
 

|           |                                                                                                                                                                                                                                                              |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To        | <chkwasher@comcast.net>                                                                                                                                                                                                                                      |
| From      | "Mr Smee" <smee.rox@gmail.com>                                                                                                                                                                                                                               |
| Date/Time | 4/10/2007 9:03:28 PM                                                                                                                                                                                                                                         |
| Subject   | A trade                                                                                                                                                                                                                                                      |
| Body      | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"><HTML><HEAD><META http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><META content="MSHTML 6.00.6000.16397" name=GENERATOR><STYLE></STYLE></HEAD><BODY style="color: #000000;"> |
- TAGS AND COMMENTS**

Figure 8.7

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

The screenshot shows the Magnet AXIOM interface with the following details:

- EVIDENCE (54)** table:
 

|    | To                         | From           | Date         | Subject                                       | Body                                                  | Cc | Bcc | Headers                                    |
|----|----------------------------|----------------|--------------|-----------------------------------------------|-------------------------------------------------------|----|-----|--------------------------------------------|
| 1  | <university...             | <Saved by...   | 3/6/2007...  | How to create and manipulate NTFS junc...     | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...        |    |     | From: <Saved by Windows Internet Explor... |
| 2  | <Saved by...               | <Saved by...   | 3/6/2007...  | Google Image Result for http://glossary....   | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...        |    |     | From: <Saved by Windows Internet Explor... |
| 3  | <dollarhyde66@comcast.net> | Mail Deliv...  | 7/11/2007... | Returned mail: delivery problems encoun...    | A message from <dollarhyde66@comcast.net> wa...       |    |     | Received: from rwmcmc13.comcast.net...     |
| 4  | <othofair...               | "Wes Man..."   | 7/12/2007... | Hey Mom                                       | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...        |    |     | Received: from rwmcmc13.comcast.net...     |
| 5  | <othofair...               | "Rasco Ba..."  | 7/24/2007... | Stuff                                         | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...        |    |     | Received: from gc-mk89.verticalrespo...    |
| 6  | "John Wa..."               | "PGP Corp..."  | 4/13/2007... | Publish Your PGP Key - Trial Encryption S...  | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01..."      |    |     | Received: by 10.78.52.10; Tue, 10 Apr 2    |
| 7  | "Mr Smee"...               | "Gmail Tea..." | 4/10/2007... | It's easy to switch to Gmail!                 | <html><font face="Arial, Helvetica, sans-serif"> <... |    |     | Received: by 10.78.52.10; Tue, 10 Apr 2    |
| 8  | "Mr Smee"...               | "Gmail Tea..." | 4/10/2007... | Gmail is different. Here's what you need t... | <html><font face="Arial, Helvetica, sans-serif"> <... |    |     | Received: by 10.78.52.10; Tue, 10 Apr 2    |
| 9  | <txkidd@swbell.net>        | "John Was..."  | 7/23/2007... | Stuff                                         | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...        |    |     | Received: from trainingm (c-24-8-18)       |
| 10 | "John Wa..."               | "Rasco Ba..."  | 7/24/2007... | Girlfriend                                    | <html xmlns="urn:schemas-microsoft-com:office..."     |    |     | Received: from smtp110.sbcmail.mud...      |
| 11 | "John Wa..."               | "Rasco Ba..."  | 7/24/2007... | Forgot photo                                  | <html xmlns="urn:schemas-microsoft-com:office..."     |    |     | Received: from smtp103.sbcmail.mud...      |
| 12 | dollarhyde66@comcast.net   | "PGP Corp..."  | 5/11/2007... | PGP Encryption Software Rated "Best Buy"      | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01..."      |    |     | Received: from mx103.verticalresponse.c... |
| 13 | "Mr Smee"...               | "John Was..."  | 4/12/2007... | HEY                                           | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...        |    |     | Delivered-To: smee.rox@gmail.com Rx        |
- ARTIFACT INFORMATION** for the selected email:
 

|           |                                                                                                                                                                                                                                                             |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To        | <txkidd@swbell.net>                                                                                                                                                                                                                                         |
| From      | "John Washer" <chkwasher@comcast.net>                                                                                                                                                                                                                       |
| Date/Time | 7/23/2007 5:59:09 PM                                                                                                                                                                                                                                        |
| Subject   | Stuff                                                                                                                                                                                                                                                       |
| Body      | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"><HTML><HEAD><META http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><META content="MSHTML 6.00.2900.3132" name=GENERATOR><STYLE></STYLE></HEAD><BODY style="color: #000000;"> |
- TAGS AND COMMENTS**

Figure 8.8

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

The screenshot shows the Magnet AXIOM interface with the following details:

- EVIDENCE (54)** table:
 

|    | To              | From         | Date... | Subject                                        | Body                                                   | Cc | Bcc | Headers                                     |
|----|-----------------|--------------|---------|------------------------------------------------|--------------------------------------------------------|----|-----|---------------------------------------------|
| 1  | <Saved by...    | 3/6/2007...  |         | <DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0..." |                                                        |    |     | From: <Saved by Windows Internet Explor...  |
| 2  | <Saved by...    | 3/6/2007...  |         | Google Image Result for http://glossary....    | <DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0..."         |    |     | From: <Saved by Windows Internet Explor...  |
| 3  | <dollarhyde...> | 7/11/2007... |         | Returned mail: delivery problems encoun...     | A message from <dollarhyde86@comcast.net> wa...        |    |     | Received: from nvcrmhc13.comcast.net        |
| 4  | <t0phfair...>   | 7/12/2007... |         | Hey Mom                                        | <DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0..."         |    |     | Received: from nvcrmhc13.comcast.net        |
| 5  | dollarhyde...>  | 4/13/2007... |         | Publish Your PGP Key - Trial Encryption S...   | <DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01..."        |    |     | Received: from go-mkt89.verticalresponse... |
| 6  | "mr smee...>    | 4/10/2007... |         | It's easy to switch to Gmail!                  | <html> <font face="Arial, Helvetica, sans-serif"> <... |    |     | Received: by 10.78.52.10; Tue, 10 Apr 2     |
| 7  | "mr smee...>    | 4/10/2007... |         | Gmail is different. Here's what you need ...   | <html> <font face="Arial, Helvetica, sans-serif"> <... |    |     | Received: by 10.78.52.10; Tue, 10 Apr 2     |
| 8  | <txkidd...>     | 7/23/2007... |         | Stuff                                          | <DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0..."         |    |     | Received: from trainingken (c-24-8-18)      |
| 9  | "John Wa...>    | 7/24/2007... |         | Girlfriend                                     | <html xmlns="urn:schemas-microsoft-com:offic...        |    |     | Received: from smtp110.sbc.mail.mud...      |
| 10 | "John Wa...>    | 7/24/2007... |         | Forgot photo                                   | <html xmlns="urn:schemas-microsoft-com:offic...        |    |     | Received: from smtp103.sbc.mail.mud...      |
| 11 | dollarhyde...>  | 5/11/2007... |         | PGP Encryption Software Rated "Best Buy"       | <DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01..."        |    |     | Received: from mkt89.verticalresponse...    |
| 12 | "Mr Smee...>    | 4/12/2007... |         | HEY                                            | <DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0..."         |    |     | Delivered-To: smee.rox@gmail.com            |
- ARTIFACT INFORMATION** for the selected email:
 

|           |                                                                                                                                                                                            |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To        | dollarhyde86@comcast.net                                                                                                                                                                   |
| From      | "PGP Corporation - Laura Lee" <PGP_Corporation_Laura_Le@mail.vresp.com>                                                                                                                    |
| Date/Time | 5/11/2007 8:05:29 AM                                                                                                                                                                       |
| Subject   | PGP Encryption Software Rated "Best B                                                                                                                                                      |
| Body      | <DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01..."><br>"http://www.w3.org/TR/html4/loose.dtd"<br><html><br><head><br><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"> |

Figure 8.9

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

The screenshot shows the Magnet AXIOM interface with the following details:

- EVIDENCE (54)** table:
 

|    | To                           | From         | Date... | Subject                                      | Body                                                      | Cc | Bcc | Headers                                  |
|----|------------------------------|--------------|---------|----------------------------------------------|-----------------------------------------------------------|----|-----|------------------------------------------|
| 1  | "mr smee...>                 | 4/10/2007... |         | Gmail is different. Here's what you need ... | <html> <font face="Arial, Helvetica, sans-serif"> <...    |    |     | Received: by 10.78.52.10; Tue, 10 Apr 2  |
| 2  | <txkidd...>                  | 7/23/2007... |         | Stuff                                        | <DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0..."            |    |     | Received: from trainingken (c-24-8-18)   |
| 3  | "John Wa...>                 | 7/24/2007... |         | Girlfriend                                   | <html xmlns="urn:schemas-microsoft-com:offic...           |    |     | Received: from smtp110.sbc.mail.mud...   |
| 4  | "John Wa...>                 | 7/24/2007... |         | Forgot photo                                 | <html xmlns="urn:schemas-microsoft-com:offic...           |    |     | Received: from smtp103.sbc.mail.mud...   |
| 5  | dollarhyde...>               | 5/11/2007... |         | PGP Encryption Software Rated "Best Buy"     | <DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01..."           |    |     | Received: from mkt89.verticalresponse... |
| 6  | "Mr Smee...>                 | 4/12/2007... |         | HEY                                          | <DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0..."            |    |     | Delivered-To: smee.rox@gmail.com         |
| 7  | trialware...>                | 4/12/2007... |         | PGP Trial Software Order Confirmation: 8...  | Thank you for registering for our free 30-day trial of... |    |     | Received: from mta.mpg.com (63.251.1)    |
| 8  | "Wes Mantooth" <Rasco Ba...> | 7/23/2007... |         | RE: Stuff                                    | <html xmlns="urn:schemas-microsoft-com:vml" x...          |    |     | Received: from smtp113.sbc.mail.mud...   |
| 9  | John Wash...>                | 7/24/2007... |         | Re: Stuff                                    |                                                           |    |     | From: Wes Mantooth [mailto:dollarhyd...  |
| 10 | "New Win...>                 | 2/27/2007... |         | Welcome to Windows Mail                      | <html xmlns:s2="urn:DocumentPartTemplate"> ...            |    |     | From: "Microsoft Windows Mail Team"      |
| 11 | "Wes Man...>                 | 7/1/2007...  |         | Re: New Venture                              | <DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0..."            |    |     | Delivered-To: smee.rox@gmail.com         |
- ARTIFACT INFORMATION** for the selected email:
 

|           |                                                                                                                                                                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To        | "Wes Mantooth" <dollarhyde86@comcast.net>                                                                                                                                                                                                                      |
| From      | "Rasco Badguy" <txkidd@swbell.net>                                                                                                                                                                                                                             |
| Date/Time | 7/23/2007 6:27:11 PM                                                                                                                                                                                                                                           |
| Subject   | RE: Stuff                                                                                                                                                                                                                                                      |
| Body      | <html xmlns="urn:schemas-microsoft-com:vml" xmlns="urn:schemas-microsoft-com:office" xmlns="urn:schemas-microsoft-com:officeword" xmlns="http://www.w3.org/TR/REC-html40"><br><head><br><meta http-equiv="Content-Type" content="text/html; charset=us-ascii"> |

Figure 9.0

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

The screenshot shows the Magnet AXIOM interface with the following details:

- EVIDENCE (54):** A table listing 54 pieces of evidence. The first few entries are:
  - Google Analytics Referral Cookies (14)
  - Google Analytics Session Cookies (12)
  - Google Searches (390)
  - Identifiers - Device (244)
  - Identifiers - People (252)
  - Locally Accessed Files and Folders (48)
  - Parsed Search Queries (2)
  - Passwords and Tokens (6)
  - Rebuilt Desktops (Windows) (2)
  - Rebuilt Webpages (52)
  - Social Media URLs (16)
- WEB RELATED:** Total 1,992
- MEDIA:** Total 1,172
- EMAIL:** Total 188
  - Email Attachments (60)
  - EMDQ Files (54):** Selected in the sidebar.
  - Outlook Appointments (22)
  - Outlook Contacts (16)
  - Outlook Emails (18)
  - Outlook Notes (8)
  - Outlook Tasks (10)
- DOCUMENTS:** Total 180
- OPERATING SYSTEM:** Total 8,414
- ENCRYPTION:** Total 12

**PREVIEW:** Shows an email from "Wes Mantooth" to "John Washer" on 7/11/2007. The subject is "Re: New Venture". The body contains a message about a pin and card, and an attachment named "ATM\_THEFTS1.ppt".

**EMAIL ATTACHMENTS:** Shows the file "ATM\_THEFTS1.ppt".

**TAGS AND COMMENTS:** Shows the comment "Time zone UTC+000 Activate Windows".

Figure 9.1

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

The screenshot shows the Magnet AXIOM interface with the following details:

- EVIDENCE (54):** A table listing 54 pieces of evidence. The first few entries are:
  - Google Analytics Referral Cookies (14)
  - Google Analytics Session Cookies (12)
  - Google Searches (390)
  - Identifiers - Device (244)
  - Identifiers - People (252)
  - Locally Accessed Files and Folders (48)
  - Parsed Search Queries (2)
  - Passwords and Tokens (6)
  - Rebuilt Desktops (Windows) (2)
  - Rebuilt Webpages (52)
  - Social Media URLs (16)
- WEB RELATED:** Total 1,992
- MEDIA:** Total 1,172
- EMAIL:** Total 188
  - Email Attachments (60)
  - EMDQ Files (54):** Selected in the sidebar.
  - Outlook Appointments (22)
  - Outlook Contacts (16)
  - Outlook Emails (18)
  - Outlook Notes (8)
  - Outlook Tasks (10)
- DOCUMENTS:** Total 180
- OPERATING SYSTEM:** Total 8,414
- ENCRYPTION:** Total 12

**PREVIEW:** Shows an email from "John Washer" to "chkwasher" and "txkidd" on 7/24/2007. The subject is "Re: Stuff". The body contains a message about a trade and an attachment named "2003 Cigarette Gladiator powerboat for s...".

**ARTIFACT INFORMATION:** Shows the artifact information for the selected email.

**TAGS AND COMMENTS:** Shows the comment "Time zone UTC+000 Activate Windows".

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

Magnet AXIOM Examine v4.1.0.1996 - Mantooth

File Tools Process Help

Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

FILTERS Media categorization Media attributes (VICS)

Type a search term... GO ADVANCED

Classic view

**EVIDENCE (22)**

| To | From | Date... | Subject                                     | Body                                                    | Cc | Bcc | Headers |
|----|------|---------|---------------------------------------------|---------------------------------------------------------|----|-----|---------|
|    |      |         | Meet with Seth about boat                   |                                                         |    |     |         |
|    |      |         | Go check stealing                           |                                                         |    |     |         |
|    |      |         | Ribbon Cutting - Texas Star Pharmacy        | (\rtf1\ansi\ansicpg1252\deff0\deflang1033\fonttbl\{\... |    |     |         |
|    |      |         | Y.M.                                        | (\rtf1\ansi\ansicpg1252\deff0\deflang1033\fonttbl\{\... |    |     |         |
|    |      |         | Communion Sunday -- bring non-perishable    | (\rtf1\ansi\ansicpg1252\deff0\deflang1033\fonttbl\{\... |    |     |         |
|    |      |         | Collecting and Processing Intelligence Inf. | (\rtf1\ansi\ansicpg1252\deff0\deflang1033\fonttbl\{\... |    |     |         |
|    |      |         | Credentialing and Identity Assurance Con... | (\rtf1\ansi\ansicpg1252\deff0\deflang1033\fonttbl\{\... |    |     |         |
|    |      |         | Combating Fraud and Corruption in the...    | (\rtf1\ansi\ansicpg1252\deff0\deflang1033\fonttbl\{\... |    |     |         |
|    |      |         | Pharmacy                                    | (\rtf1\ansi\ansicpg1252\deff0\deflang1033\fonttbl\{\... |    |     |         |
|    |      |         | Pharmasolutions Expo 2007                   | (\rtf1\ansi\ansicpg1252\deff0\deflang1033\fonttbl\{\... |    |     |         |

Go check stealing

**Ribbon Cutting - Texas Star Pharmacy**

**PREVIEW**

Subject: Ribbon Cutting - Texas Star Pharmacy  
Importance: Normal

Texas Star Pharmacy  
3033 W. Parker, Ste 100  
(NE corner of Parker & Independence)

**DETAILS**

**ARTIFACT INFORMATION**

Subject: Ribbon Cutting - Texas Star Pharmacy  
Start Date/Time: 7/27/2006 4:30:00 PM  
End Date/Time: 7/27/2006 5:00:00 PM  
Body: (\rtf1\ansi\ansicpg1252\deff0\deflang1033\fonttbl\{\font\swiss V\charset0 Arial\})  
(^generator Riched20 5.50.30.2002;)\\viewkind4uc1pard\l0\f20  
Texas Star Pharmacy\par  
3033 W. Parker, Ste 100 \par

**TAGS AND COMMENTS**

Figure 9.3

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

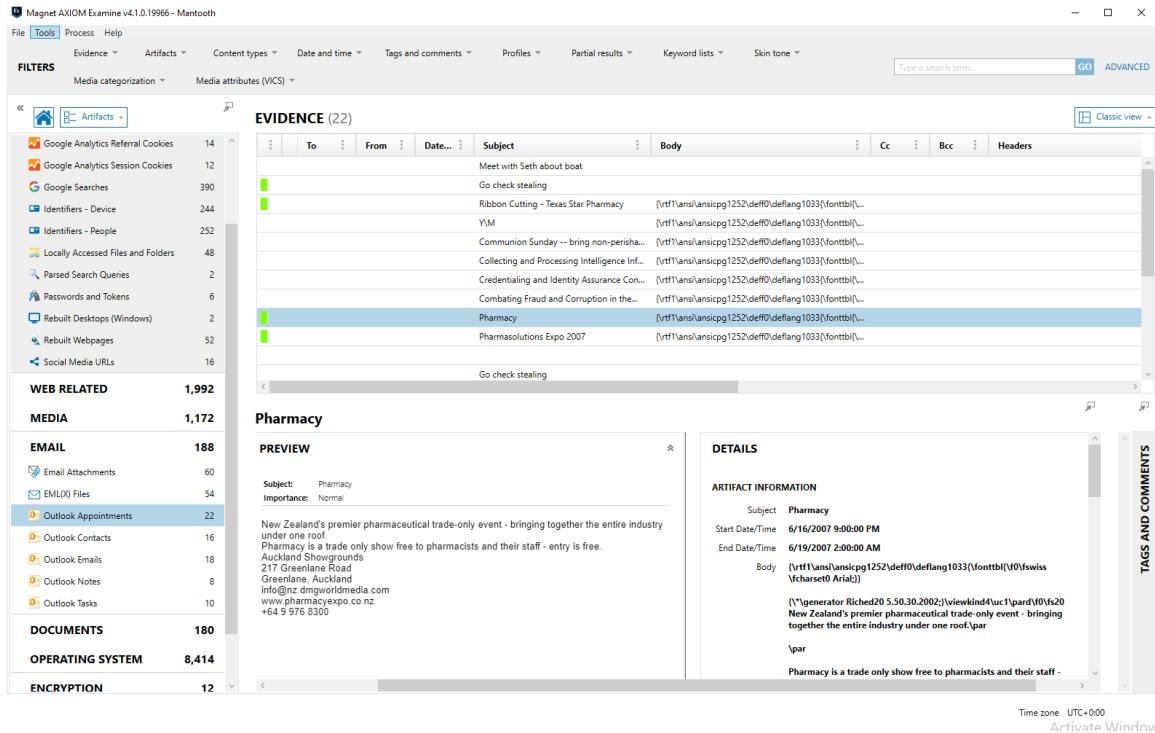


Figure 9.4

Figure 9.4 contains information about a pharmacy selling drugs illegally.

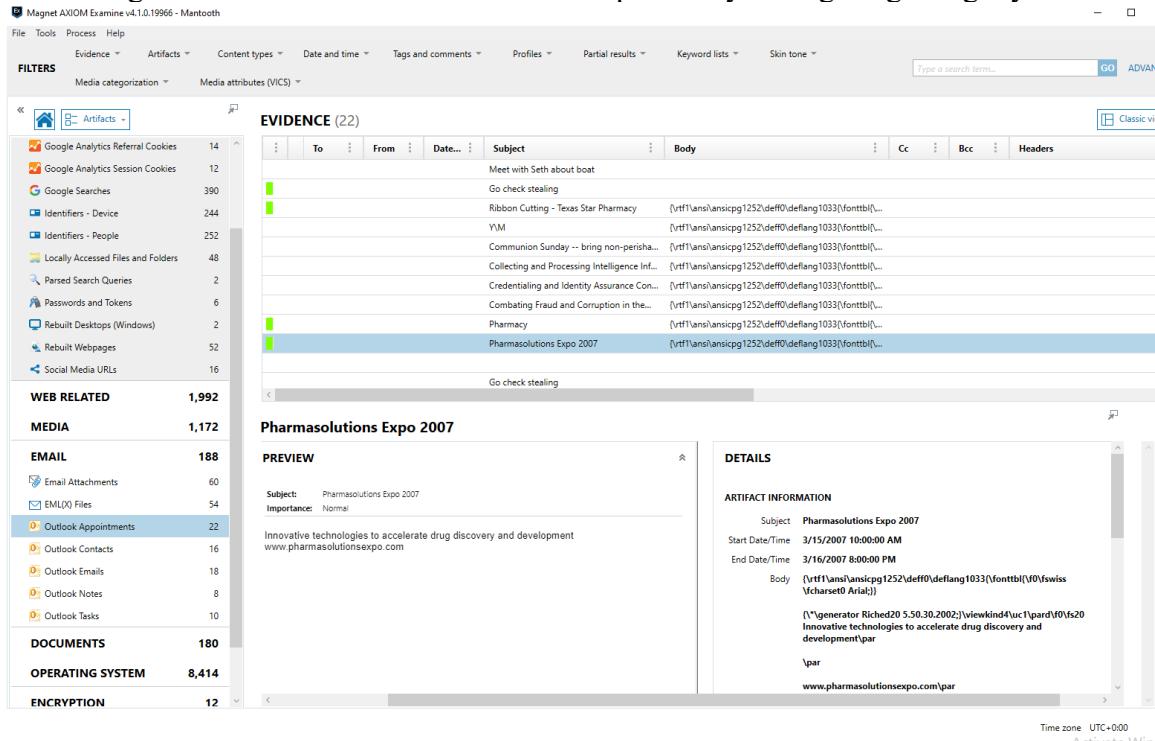


Figure 9.5

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

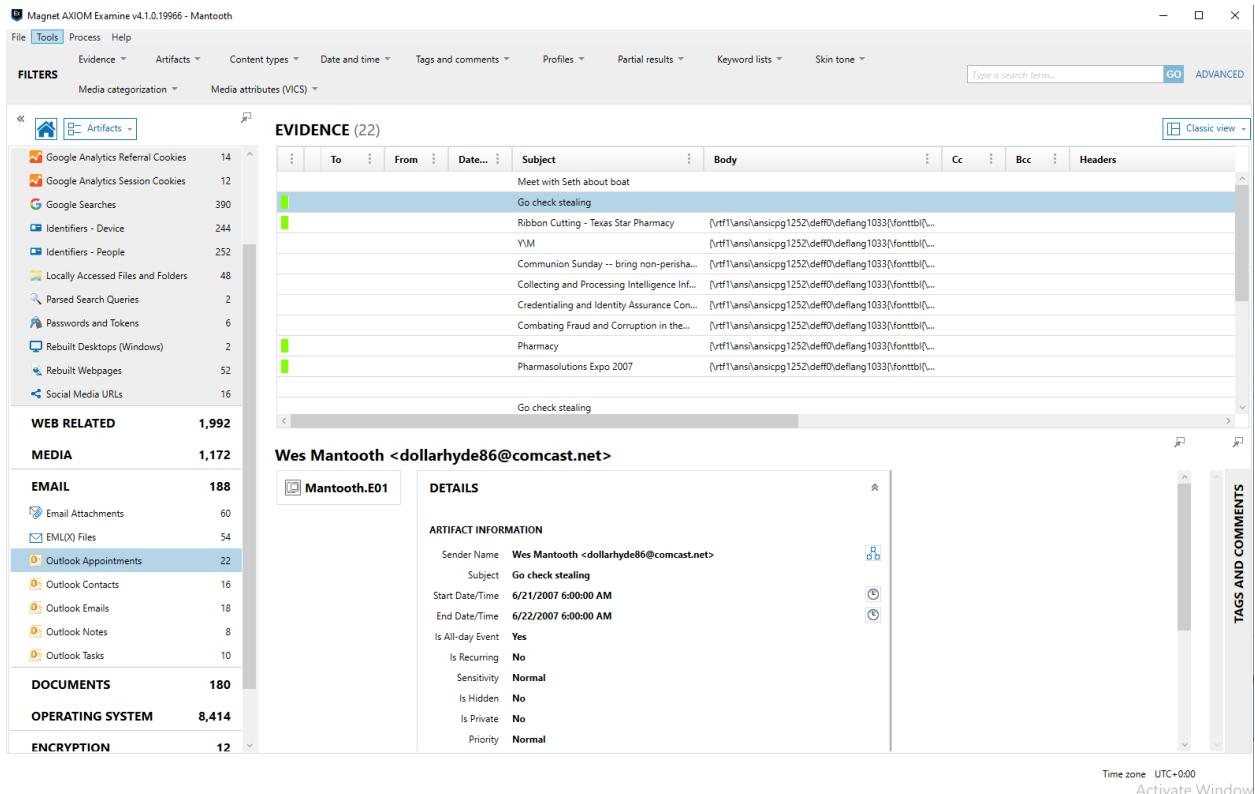


Figure 9.6

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

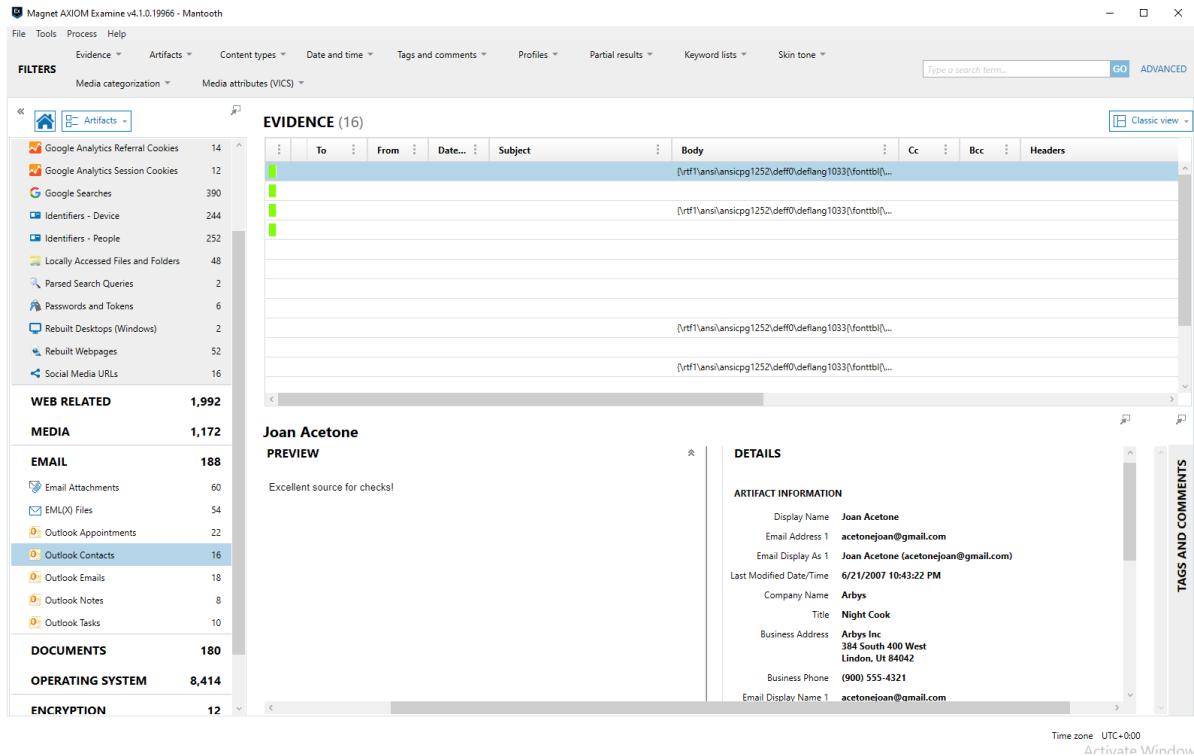


Figure 9.7

Figure 9.7 talks about a source for fraudulent cashier checks.

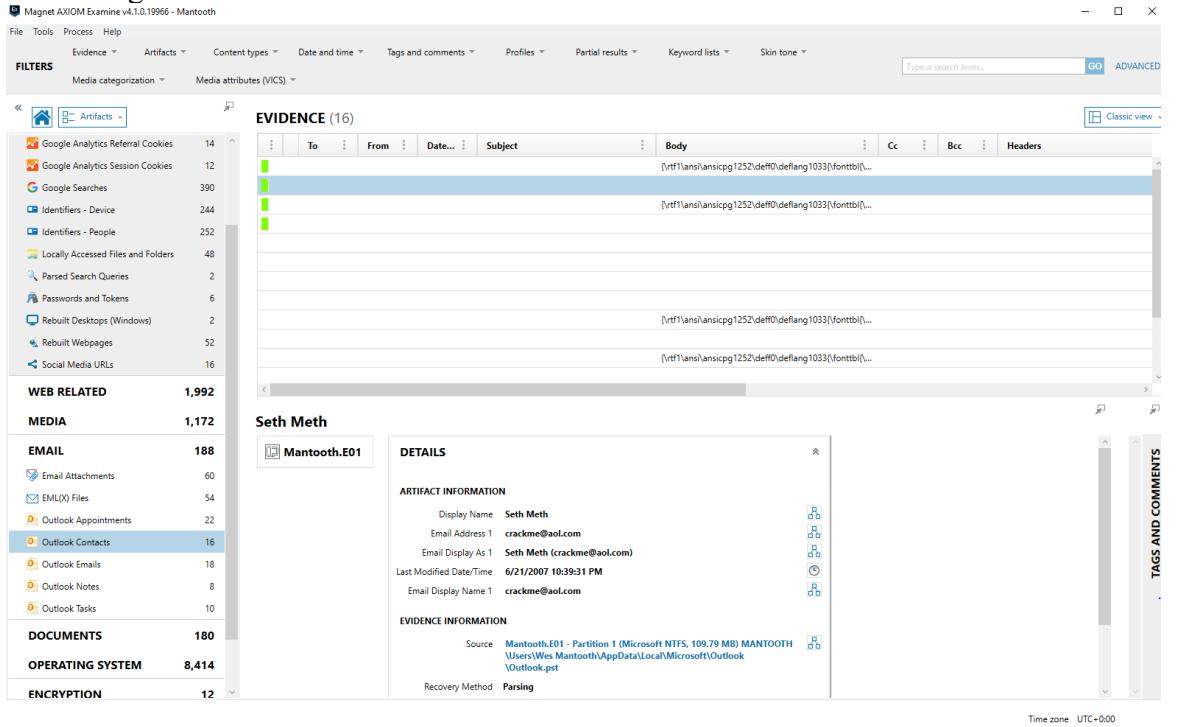


Figure 9.8

Figure 9.8 contains an email labeled "Seth Meth".

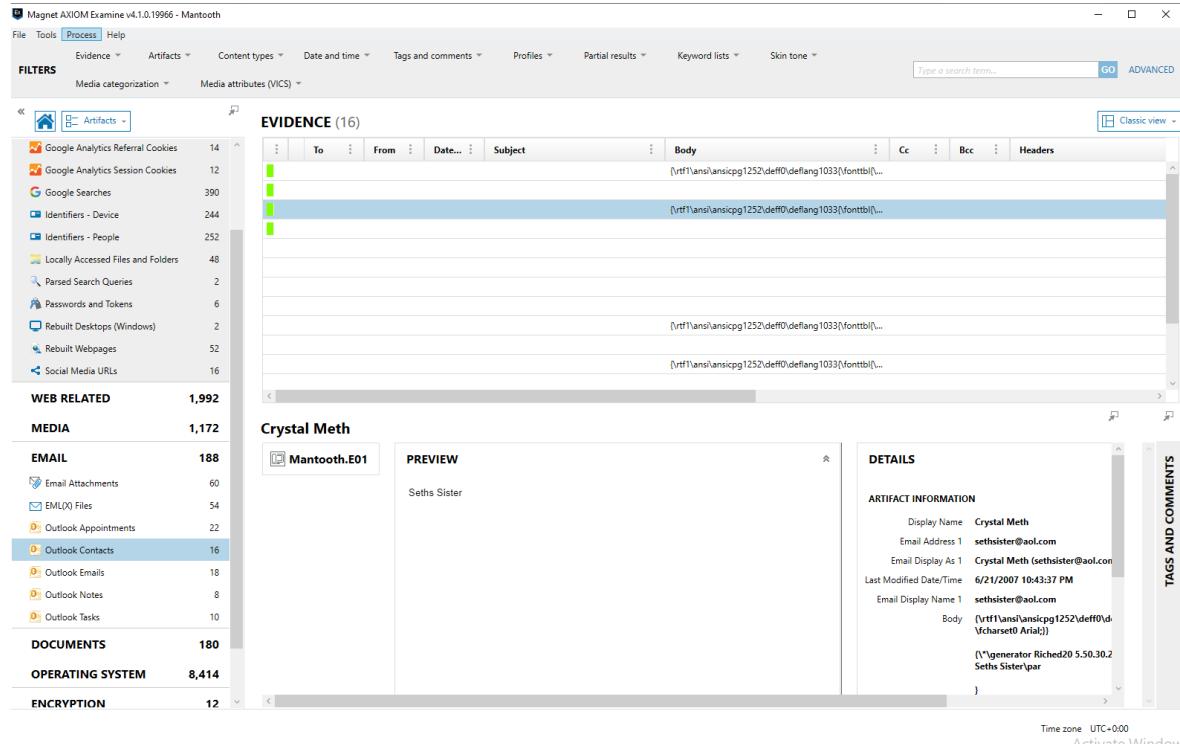


Figure 9.9

Figure 9.9 contains another email labeled "Crystal Meth".

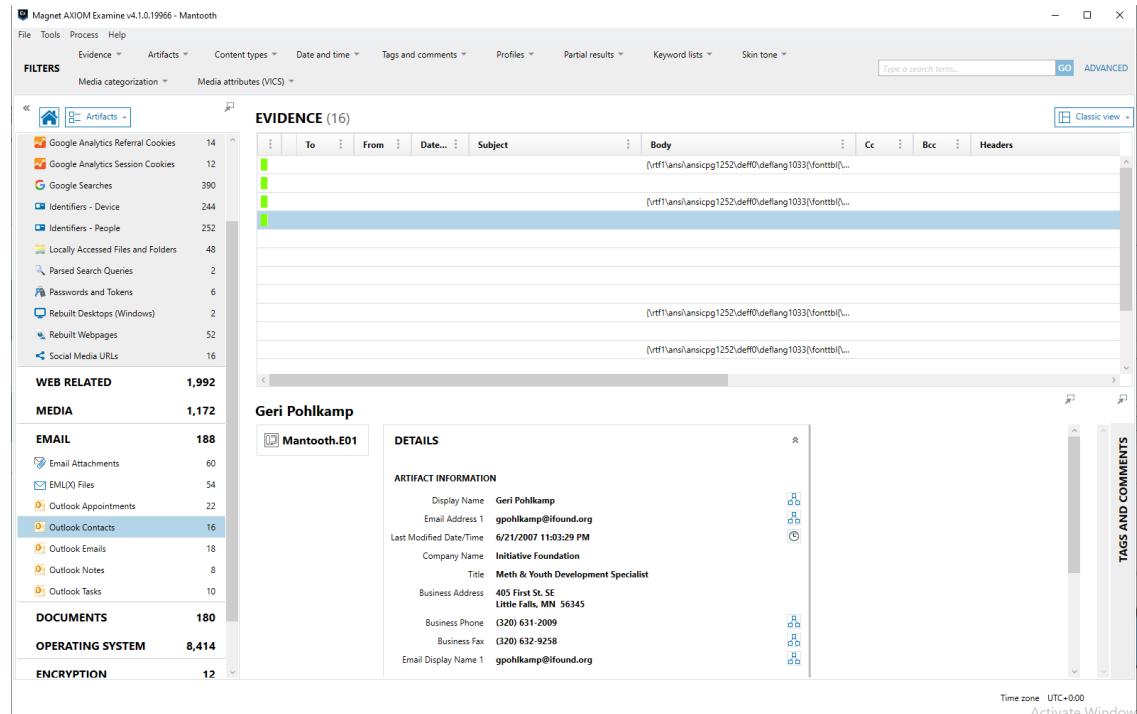


Figure 10.0

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

The screenshot shows the Magnet AXIOM Examine software interface. The top navigation bar includes File, Tools, Process, Help, Evidence, Artifacts, Content types, Date and time, Tags and comments, Profiles, Partial results, Keyword lists, Skin tone, and a search bar. Below the navigation is a 'FILTERS' section with Media categorization and Media attributes (VICS) dropdowns.

The main area displays the 'EVIDENCE (18)' list. The columns are To, From, Date..., Subject, Body, Cc, Bcc, and Headers. The list contains several entries, including:

- Microsoft Office Outlook Test Message
- Re: What's up in D town?
- Letter
- RE: What's up in D town?
- RE: What's up in D town?
- Welcome to Microsoft Office Outlook 2003
- Welcome to Microsoft Office Outlook 2003
- Microsoft Office Outlook Test Message
- What's up in D town?

On the left, there is a sidebar with category counts: Google Analytics Referral Cookies (14), Google Analytics Session Cookies (12), Google Searches (390), Identifiers - Device (244), Identifiers - People (252), Locally Accessed Files and Folders (48), Parsed Search Queries (2), Passwords and Tokens (6), Rebuilt Desktops (Windows) (2), Rebuilt Webpages (52), and Social Media URLs (16). Below this is a breakdown of evidence types: WEB RELATED (1,992), MEDIA (1,172), EMAIL (188), DOCUMENTS (180), OPERATING SYSTEM (8,414), and ENCRYPTION (12).

A specific email entry for John Washer (<chkwasher@comcast.net>) is selected. The 'PREVIEW' tab shows the raw HTML of the email message. The 'DETAILS' tab provides artifact information, including Sender Name (John Washer <chkwasher@comcast.net>), Recipients (Web Mantooh), Subject (Re: What's up in D town?), Creation Date/Time (6/21/2007 6:02:19 PM), Delivery Date/Time (6/20/2007 6:01:59 PM), and the full body of the email message.

Figure 10.1

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

The screenshot shows the Magnet AXIOM interface with the title bar "Magnet AXIOM Examine v4.1.0.19966 - Mantooth". The main window displays the "EVIDENCE (18)" section. On the left, a sidebar lists various artifact types with their counts: Google Analytics Referral Cookies (14), Google Analytics Session Cookies (12), Google Searches (390), Identifiers - Device (244), Identifiers - People (252), Locally Accessed Files and Folders (48), Parsed Search Queries (2), Passwords and Tokens (6), Rebuilt Desktops (Windows) (2), Rebuilt Webpages (52), and Social Media URLs (16). Below these are sections for WEB RELATED (1,992), MEDIA (1,172), EMAIL (188), DOCUMENTS (180), OPERATING SYSTEM (8,414), and ENCRYPTION (12). The central area shows a list of 18 email messages. One message from "John Washer <chkwasher@comcast.net>" is selected, showing its preview and details. The preview shows a message body with HTML code and a link to a ClickLane project. The details pane shows the recipient as "John Washer <chkwasher@comcast.net>", subject as "Re: Whats up in D town?", and body content including the HTML code and the ClickLane link.

Figure 10.2

Figure 10.2 contains another email from John Washer about meth.

The screenshot shows the Magnet AXIOM interface with the title bar "Magnet AXIOM Examine v4.1.0.19966 - Mantooth". The main window displays the "EVIDENCE (18)" section. The sidebar is identical to Figure 10.2. The central area shows a list of 18 email messages. One message from "Rasco Badguy <txkidd@swbell.net>" is selected, showing its preview and details. The preview shows a message body with HTML code and attachments. The details pane shows the recipient as "Rasco Badguy <txkidd@swbell.net>", subject as "Letter", and body content including the HTML code and the attachment "Confidential Business Letter.doc".

Figure 10.3

Figure 10.3 contains an email from Rasco Badguy about meth.

**EVIDENCE (18)**

| Google Analytics Referral Cookies  | 14           | To | From | Date... | Subject                                  | Body                                                   | Cc | Bcc | Headers                               |  |  |
|------------------------------------|--------------|----|------|---------|------------------------------------------|--------------------------------------------------------|----|-----|---------------------------------------|--|--|
| Google Analytics Session Cookies   | 12           |    |      |         | Microsoft Office Outlook Test Message    | This is an e-mail message sent automatically by Mic... |    |     | Date: Wed, 20 Jun 2007 17:50:35 +000  |  |  |
| Google Searches                    | 390          |    |      |         | Whats up in D town?                      | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18 |  |  |
| Identifiers - Device               | 244          |    |      |         | Re: Whats up in D town?                  | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18 |  |  |
| Identifiers - People               | 252          |    |      |         | Re: Whats up in D town?                  | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18 |  |  |
| Locally Accessed Files and Folders | 48           |    |      |         | Letter                                   | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from smtp122.sbc.mail.re3.y |  |  |
| Parsed Search Queries              | 2            |    |      |         | RE: Whats up in D town?                  | <html xmlns:v="urn:schemas-microsoft-com:vml" x...     |    |     |                                       |  |  |
| Passwords and Tokens               | 6            |    |      |         |                                          | <html xmlns:v="urn:schemas-microsoft-com:vml" x...     |    |     |                                       |  |  |
| Rebuilt Desktops (Windows)         | 2            |    |      |         |                                          | <html xmlns:v="urn:schemas-microsoft-com:vml" x...     |    |     |                                       |  |  |
| Rebuilt Webpages                   | 52           |    |      |         | Welcome to Microsoft Office Outlook 2003 | <HTML> <HEAD> <TITLE> <STYLE TY...                     |    |     |                                       |  |  |
| Social Media URLs                  | 16           |    |      |         | Welcome to Microsoft Office Outlook 2003 | <HTML> <HEAD> <TITLE> <STYLE TY...                     |    |     |                                       |  |  |
| <b>WEB RELATED</b>                 | <b>1,992</b> |    |      |         | Microsoft Office Outlook Test Message    | This is an e-mail message sent automatically by Mic... |    |     | Date: Wed, 20 Jun 2007 17:50:35 +000  |  |  |
| <b>MEDIA</b>                       | <b>1,172</b> |    |      |         | Whats up in D town?                      | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18 |  |  |
| <b>EMAIL</b>                       | <b>188</b>   |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| Email Attachments                  | 60           |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| EML(X) File                        | 54           |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| Outlook Appointments               | 22           |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| Outlook Contacts                   | 16           |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| Outlook Emails                     | 18           |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| Outlook Notes                      | 8            |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| Outlook Tasks                      | 10           |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| <b>DOCUMENTS</b>                   | <b>180</b>   |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| OPERATING SYSTEM                   | 8,414        |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| ENCRYPTION                         | 12           |    |      |         |                                          |                                                        |    |     |                                       |  |  |

**PREVIEW**

From: Wes Mantooth <dollarhyde86@comcast.net>  
Received: 6/21/2007 6:00:00 PM  
To: [John Washer]  
Subject: RE: Whats up in D town?  
Importance: Normal  
Sensitivity: Normal  
Attachments: Prescription2.gif

Sorry man.  
I have been a little under the weather lately. Too much party!  
Yea, I am going to go... same time and place.  
I am still on the trail of some good scripts...  
Check the one out.  
I need to do a little editing on the type and quantity... but it shouldn't be a problem.  
Later

**EMAIL ATTACHMENTS**

Prescription2.gif

**TAGS AND COMMENTS**

Time zone UTC+000

Figure 10.4 – 10.6 contain messages from dollarhyde.

Figure 10.4 contains a message from dollarhyde about meth.

**EVIDENCE (18)**

| Google Analytics Referral Cookies  | 14           | To | From | Date... | Subject                                  | Body                                                   | Cc | Bcc | Headers                               |  |  |
|------------------------------------|--------------|----|------|---------|------------------------------------------|--------------------------------------------------------|----|-----|---------------------------------------|--|--|
| Google Analytics Session Cookies   | 12           |    |      |         | Microsoft Office Outlook Test Message    | This is an e-mail message sent automatically by Mic... |    |     | Date: Wed, 20 Jun 2007 17:50:35 +000  |  |  |
| Google Searches                    | 390          |    |      |         | Whats up in D town?                      | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18 |  |  |
| Identifiers - Device               | 244          |    |      |         | Re: Whats up in D town?                  | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18 |  |  |
| Identifiers - People               | 252          |    |      |         | Re: Whats up in D town?                  | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18 |  |  |
| Locally Accessed Files and Folders | 48           |    |      |         | Letter                                   | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from smtp122.sbc.mail.re3.y |  |  |
| Parsed Search Queries              | 2            |    |      |         | RE: Whats up in D town?                  | <html xmlns:v="urn:schemas-microsoft-com:vml" x...     |    |     |                                       |  |  |
| Passwords and Tokens               | 6            |    |      |         |                                          | <html xmlns:v="urn:schemas-microsoft-com:vml" x...     |    |     |                                       |  |  |
| Rebuilt Desktops (Windows)         | 2            |    |      |         |                                          | <html xmlns:v="urn:schemas-microsoft-com:vml" x...     |    |     |                                       |  |  |
| Rebuilt Webpages                   | 52           |    |      |         | Welcome to Microsoft Office Outlook 2003 | <HTML> <HEAD> <TITLE> <STYLE TY...                     |    |     |                                       |  |  |
| Social Media URLs                  | 16           |    |      |         | Welcome to Microsoft Office Outlook 2003 | <HTML> <HEAD> <TITLE> <STYLE TY...                     |    |     |                                       |  |  |
| <b>WEB RELATED</b>                 | <b>1,992</b> |    |      |         | Microsoft Office Outlook Test Message    | This is an e-mail message sent automatically by Mic... |    |     | Date: Wed, 20 Jun 2007 17:50:35 +000  |  |  |
| <b>MEDIA</b>                       | <b>1,172</b> |    |      |         | Whats up in D town?                      | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18 |  |  |
| <b>EMAIL</b>                       | <b>188</b>   |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| Email Attachments                  | 60           |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| EML(X) File                        | 54           |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| Outlook Appointments               | 22           |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| Outlook Contacts                   | 16           |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| Outlook Emails                     | 18           |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| Outlook Notes                      | 8            |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| Outlook Tasks                      | 10           |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| <b>DOCUMENTS</b>                   | <b>180</b>   |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| OPERATING SYSTEM                   | 8,414        |    |      |         |                                          |                                                        |    |     |                                       |  |  |
| ENCRYPTION                         | 12           |    |      |         |                                          |                                                        |    |     |                                       |  |  |

**PREVIEW**

From: Wes Mantooth <dollarhyde86@comcast.net>  
Received: 6/21/2007 9:00:00 PM  
To: [John Washer]  
Subject: RE: Whats up in D town?  
Importance: Normal  
Sensitivity: Normal  
Attachments: doc-prescription.jpg

Your crazy!  
You are going to blow your self up!  
I am sticking with my method.  
I hooked another today from the pharm counter... this lady is a mess. She just leaves this stuff lying around!  
©

**EMAIL ATTACHMENTS**

doc-prescription.jpg

**TAGS AND COMMENTS**

Time zone UTC+000

Figure 10.5

**EVIDENCE (18)**

| To | From | Date... | Subject                                  | Body                                                   | Cc | Bcc | Headers                                  |
|----|------|---------|------------------------------------------|--------------------------------------------------------|----|-----|------------------------------------------|
|    |      |         | Microsoft Office Outlook Test Message    | This is an e-mail message sent automatically by Mic... |    |     | Date: Wed, 20 Jun 2007 17:50:35 +000     |
|    |      |         | Whats up in D town?                      | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18)   |
|    |      |         | Re: Whats up in D town?                  | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18)   |
|    |      |         | Re: Whats up in D town?                  | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18)   |
|    |      |         | Letter                                   | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from smtp122.sbc.mail.re3.y... |
|    |      |         | RE: Whats up in D town?                  | <html xmlns:v="urn:schemas-microsoft-com:vml" ...      |    |     |                                          |
|    |      |         | RE: Whats up in D town?                  | <html xmlns:v="urn:schemas-microsoft-com:vml" ...      |    |     |                                          |
|    |      |         | RE: Whats up in D town?                  | <html xmlns:v="urn:schemas-microsoft-com:vml" ...      |    |     |                                          |
|    |      |         | Welcome to Microsoft Office Outlook 2003 | <HTML><HEAD> <TITLE> <STYLE TY...                      |    |     | Date: Wed, 20 Jun 2007 17:50:35 +000     |
|    |      |         | Welcome to Microsoft Office Outlook 2003 | <HTML><HEAD> <TITLE> <STYLE TY...                      |    |     | Received: from trainingken (c-24-8-18)   |
|    |      |         | Microsoft Office Outlook Test Message    | This is an e-mail message sent automatically by Mic... |    |     |                                          |
|    |      |         | Whats up in D town?                      | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     |                                          |

**PREVIEW**

From: Wes Mantooth <dollarhyde86@comcast.net>  
Received: 6/20/2007 11:28:00 PM  
To: ["John Washer"]  
Subject: RE: Whats up in D town?  
Importance: Normal  
Sensitivity: Normal  
Attachments: Pharmacy.vcs

It works EXACTLY the same. I have been doing quit a bit of research on it. You would be amazed what information you can get from those who would try and stop you! I am going to NZ for a trade show. Lots of free schwag! You should come! See the attached cal event. Later

From: John Washer [mailto:chkwasher@comcast.net]

**EMAIL ATTACHMENTS**

Pharmacy.vcs

**TAGS AND COMMENTS**

Time zone UTC+0:00 Activate Window

Figure 10.6

**EVIDENCE (18)**

| To | From | Date... | Subject                                  | Body                                                   | Cc | Bcc | Headers                                  |
|----|------|---------|------------------------------------------|--------------------------------------------------------|----|-----|------------------------------------------|
|    |      |         | Microsoft Office Outlook Test Message    | This is an e-mail message sent automatically by Mic... |    |     | Date: Wed, 20 Jun 2007 17:50:35 +000     |
|    |      |         | Whats up in D town?                      | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18)   |
|    |      |         | Re: Whats up in D town?                  | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18)   |
|    |      |         | Re: Whats up in D town?                  | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from trainingken (c-24-8-18)   |
|    |      |         | Letter                                   | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     | Received: from smtp122.sbc.mail.re3.y... |
|    |      |         | RE: Whats up in D town?                  | <html xmlns:v="urn:schemas-microsoft-com:vml" ...      |    |     |                                          |
|    |      |         | RE: Whats up in D town?                  | <html xmlns:v="urn:schemas-microsoft-com:vml" ...      |    |     |                                          |
|    |      |         | RE: Whats up in D town?                  | <html xmlns:v="urn:schemas-microsoft-com:vml" ...      |    |     |                                          |
|    |      |         | Welcome to Microsoft Office Outlook 2003 | <HTML><HEAD> <TITLE> <STYLE TY...                      |    |     | Date: Wed, 20 Jun 2007 17:50:35 +000     |
|    |      |         | Welcome to Microsoft Office Outlook 2003 | <HTML><HEAD> <TITLE> <STYLE TY...                      |    |     | Received: from trainingken (c-24-8-18)   |
|    |      |         | Microsoft Office Outlook Test Message    | This is an e-mail message sent automatically by Mic... |    |     |                                          |
|    |      |         | Whats up in D town?                      | <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0...         |    |     |                                          |

**PREVIEW**

From: John Washer <chkwasher@comcast.net>  
Received: 6/20/2007 5:56:25 PM  
To: ["Mantooth"]  
Subject: Whats up in D town?  
Importance: Normal  
Sensitivity: None

Dude!  
You been laying a little low these days?  
I have been trying to call you almost daily and we can't hook up!  
I have the "Special K" your looking for... but it is going to cost you!  
Give me a buzz! But hurry... this stuff ain't gonna last!

**ARTIFACT INFORMATION**

Sender Name: John Washer <chkwasher@comcast.net>  
Recipients: Mantooth  
Subject: Whats up in D town?  
Creation Date/Time: 6/20/2007 5:56:37 PM  
Delivery Date/Time: 6/20/2007 5:56:25 PM  
Body: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"><HTML><HEAD><META http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><META content="MSHTML 6.0.2900.3132" name=GENERATOR><STYLE></STYLE>

**DETAILS**

**TAGS AND COMMENTS**

Time zone UTC-0:00 Activate Window

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

The screenshot shows the Magnet AXIOM Examine interface. On the left, there's a sidebar with filters for Evidence, Artifacts, Content types, Date and time, Tags and comments, Profiles, Partial results, Keyword lists, and Skin tone. Below that is a tree view of evidence categories: ALL EVIDENCE (13,018), Refined Results (1,056), WEB RELATED (1,992), and MEDIA (1,172). Under Refined Results, several items are listed, including Classified URLs (2), Google Analytics First Visit Cookies (16), Google Analytics Referral Cookies (14), Google Analytics Session Cookies (12), Google Searches (390), Identifiers - Device (244), Identifiers - People (252), Locally Accessed Files and Folders (48), Posed Search Queries (2), Passwords and Tokens (6), Rebuilt Desktops (Windows) (2), Rebuilt Webpages (52), and Social Media URLs (16). The Outlook Notes category is highlighted.

The main pane displays the EVIDENCE (8) table with columns: Creation Date/Time, Last Modified..., and Body. The table shows eight entries from June 21, 2007, at various times between 11:14:45 PM and 11:15:22 PM. The body of the first entry is visible:

```

6/21/2007 11:14:45 PM 6/21/2007 11:14:45 PM (\rtf1\ansi\ansicpg1252\def0\deflang1033\fonttbl{\...
6/21/2007 11:15:01 PM 6/21/2007 11:15:01 PM (\rtf1\ansi\ansicpg1252\def0\deflang1033\fonttbl{\...
6/21/2007 11:15:14 PM 6/21/2007 11:15:14 PM (\rtf1\ansi\ansicpg1252\def0\deflang1033\fonttbl{\...
6/21/2007 11:15:22 PM 6/21/2007 11:15:22 PM (\rtf1\ansi\ansicpg1252\def0\deflang1033\fonttbl{\...
6/21/2007 11:14:45 PM 6/21/2007 11:14:45 PM (\rtf1\ansi\ansicpg1252\def0\deflang1033\fonttbl{\...
6/21/2007 11:15:01 PM 6/21/2007 11:15:01 PM (\rtf1\ansi\ansicpg1252\def0\deflang1033\fonttbl{\...
6/21/2007 11:15:14 PM 6/21/2007 11:15:14 PM (\rtf1\ansi\ansicpg1252\def0\deflang1033\fonttbl{\...
6/21/2007 11:15:22 PM 6/21/2007 11:15:22 PM (\rtf1\ansi\ansicpg1252\def0\deflang1033\fonttbl{\...

```

The right side of the interface shows a preview of the note, which reads "Go to KMart and buy Acetone". Below it is a details section for the artifact, showing creation and last modified dates/times, and the full body of the note:

```

(\rtf1\ansi\ansicpg1252\def0\deflang1033\fonttbl{\...
\deflang1033\fonttbl{\...
\defcharset0 Comic Sans MS})\...
\generator Riched20
5.50.30.2002;\viewkind4\uc1
\pard\ql\fs20 Go to KMart and
buy Acetone\par
\par

```

At the bottom right, it says "Time zone: UTC+000" and "Active OS: Windows".

Figure 10.8

Figure 10.8 contains information about buying Acetone at Kmart.

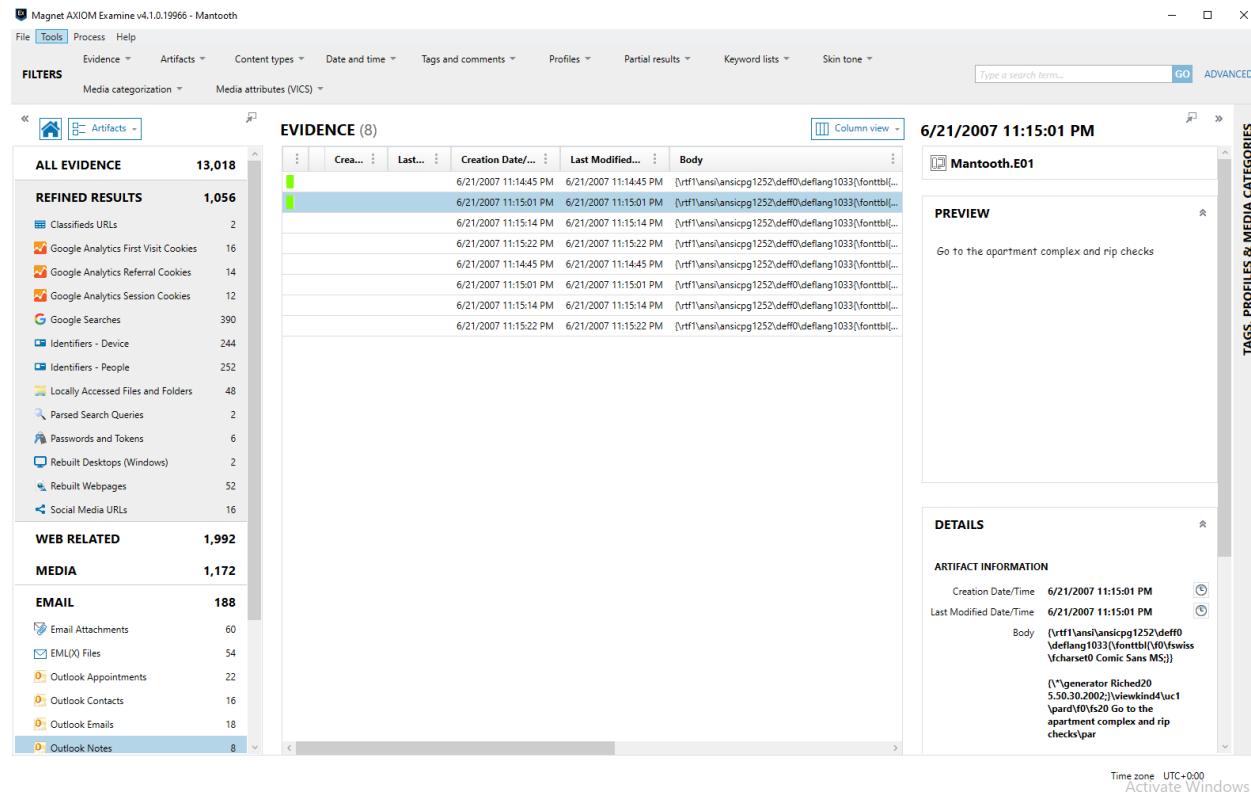


Figure 10.9

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

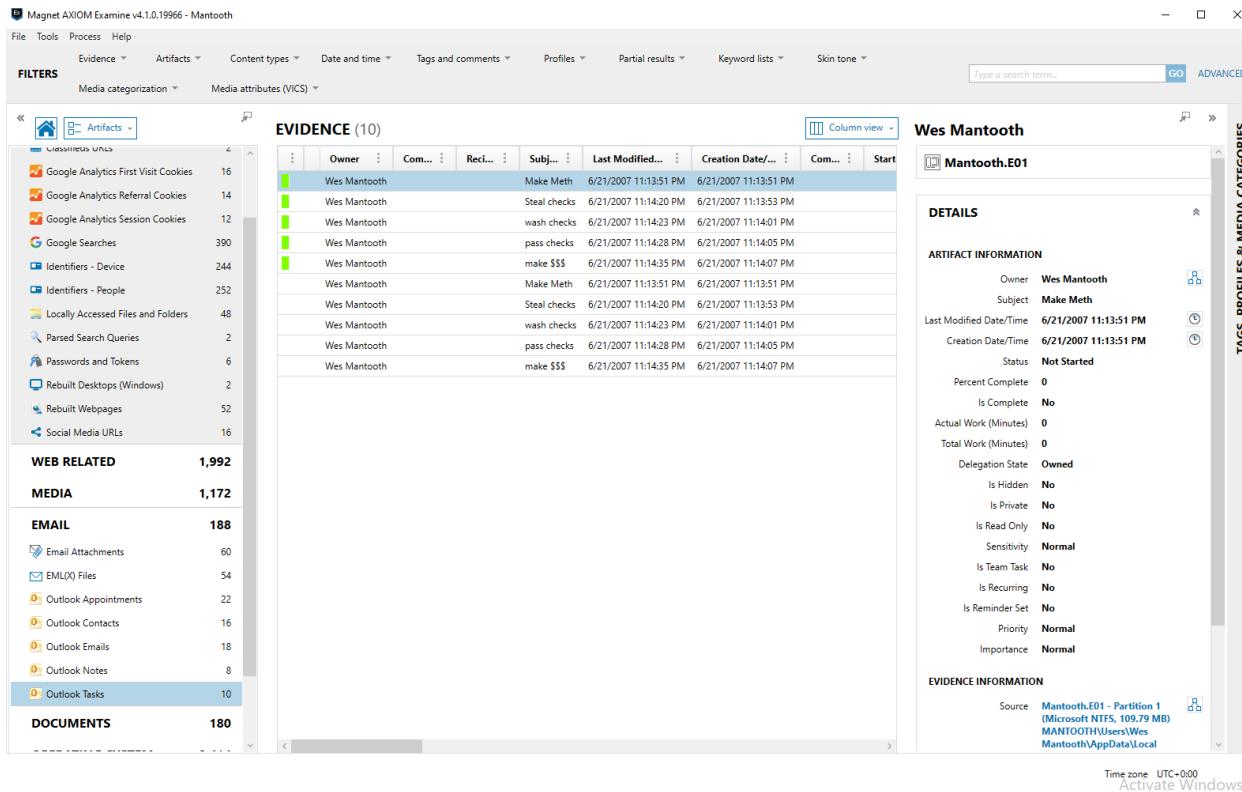


Figure 11.0

## 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

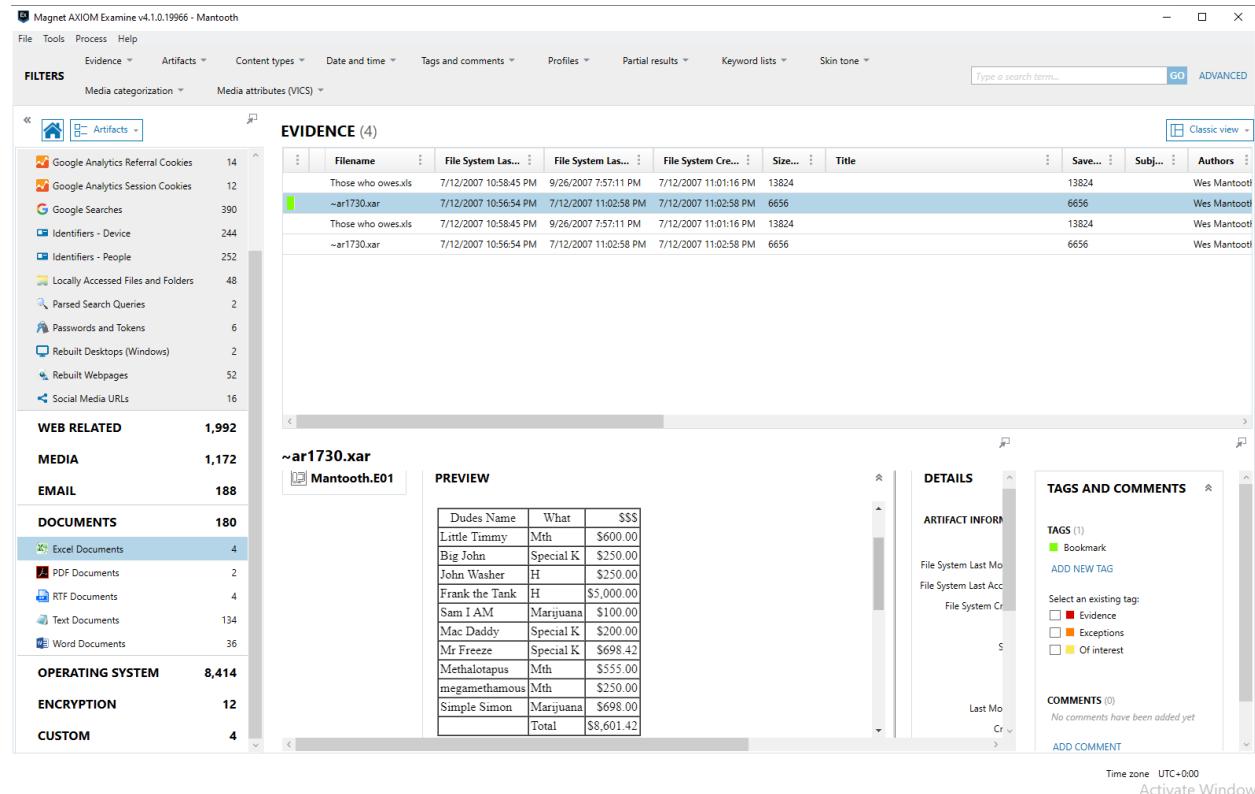


Figure 11.1

## Text Documents

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

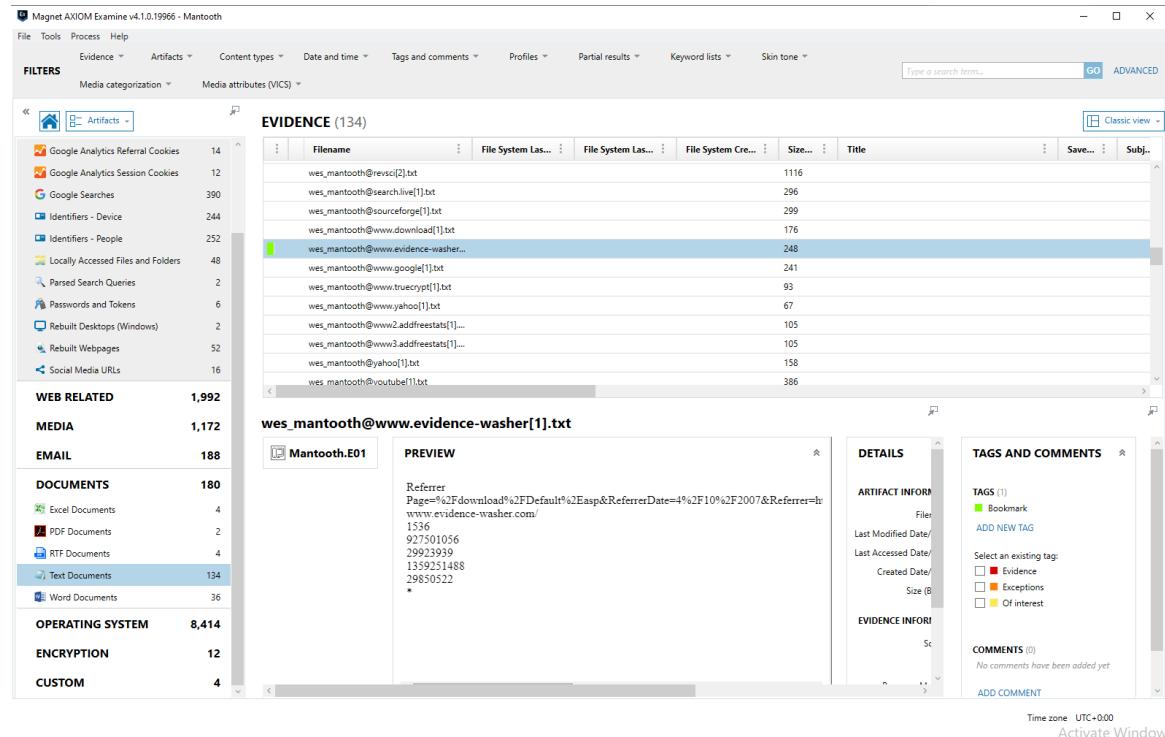


Figure 11.2

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

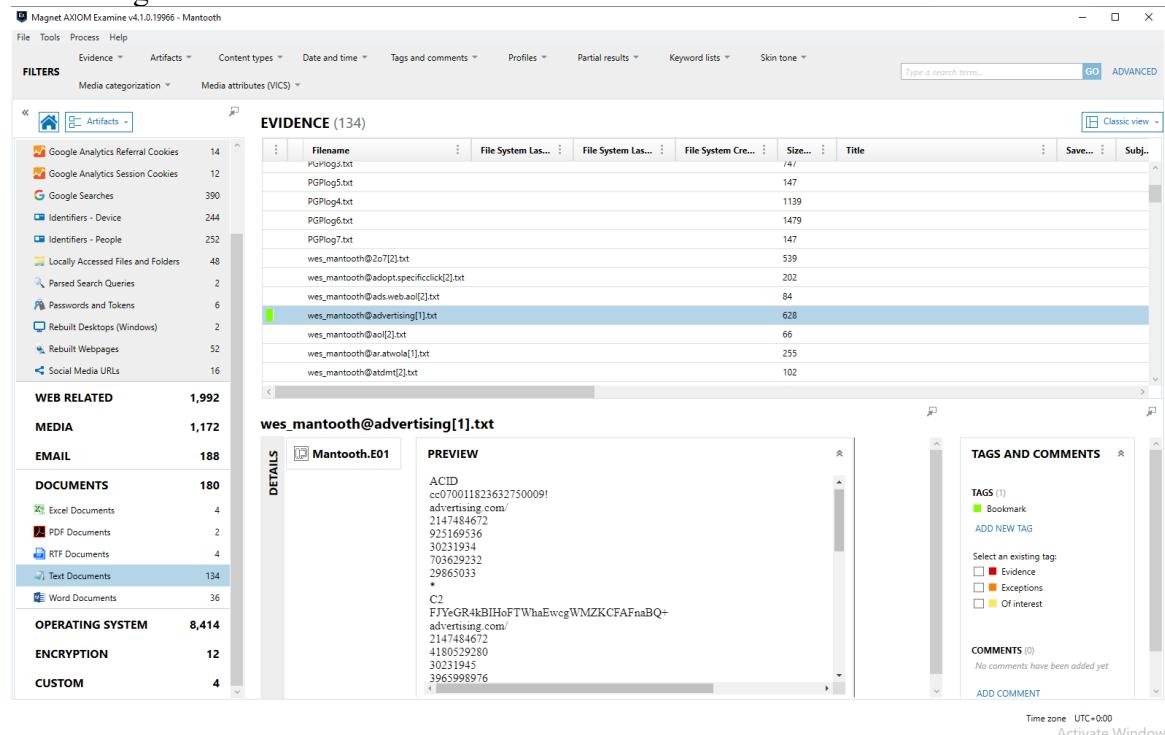


Figure 11.3

Figure 11.3 is an advertising board for his drugs.

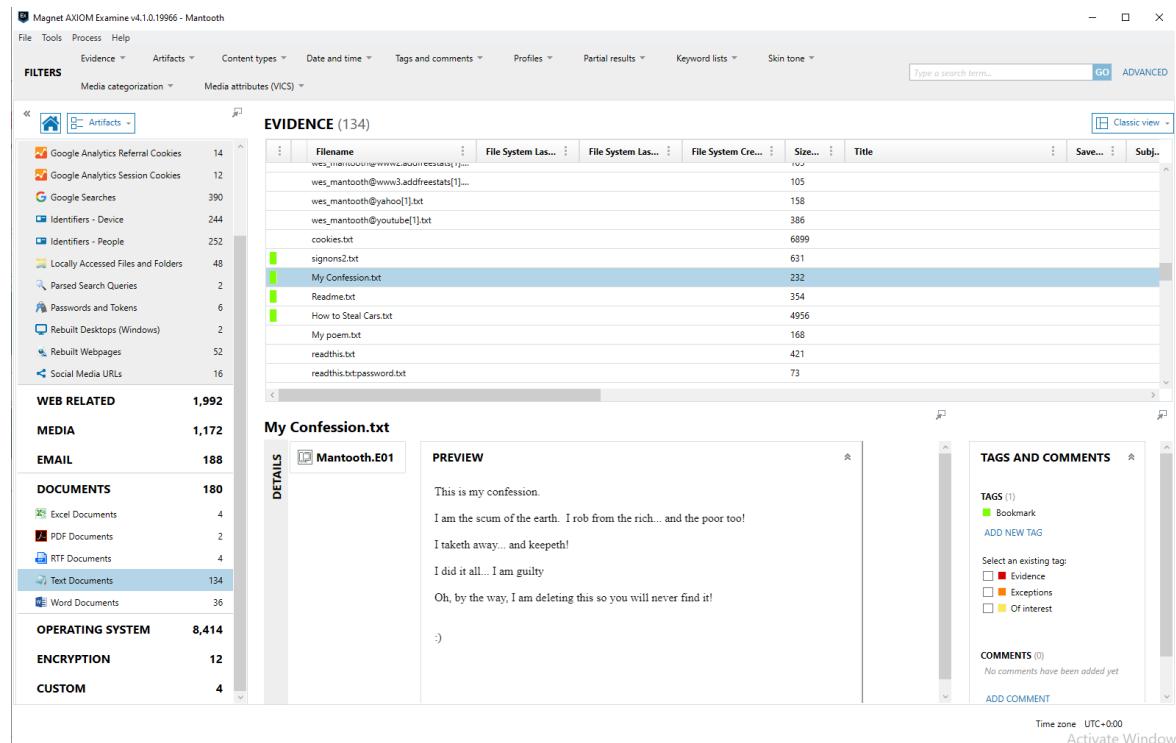


Figure 11.4

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

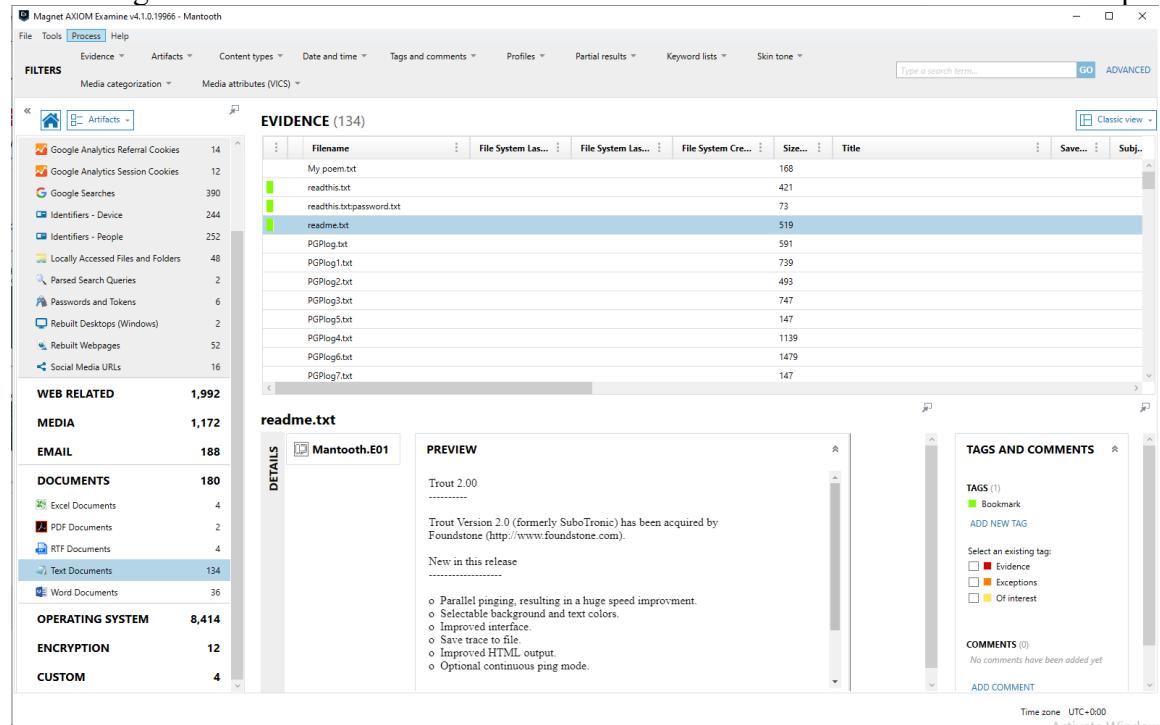


Figure 11.5

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

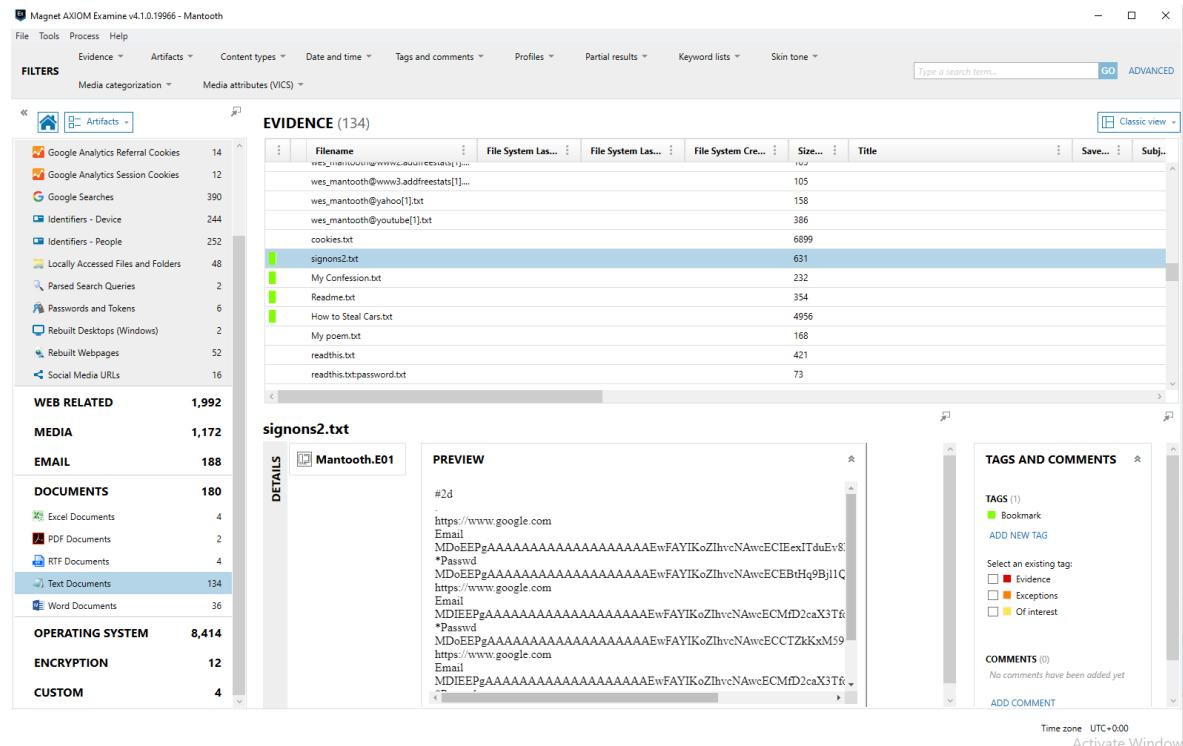


Figure 11.6

Figure 11.6 is a list of sign ons and passwords.

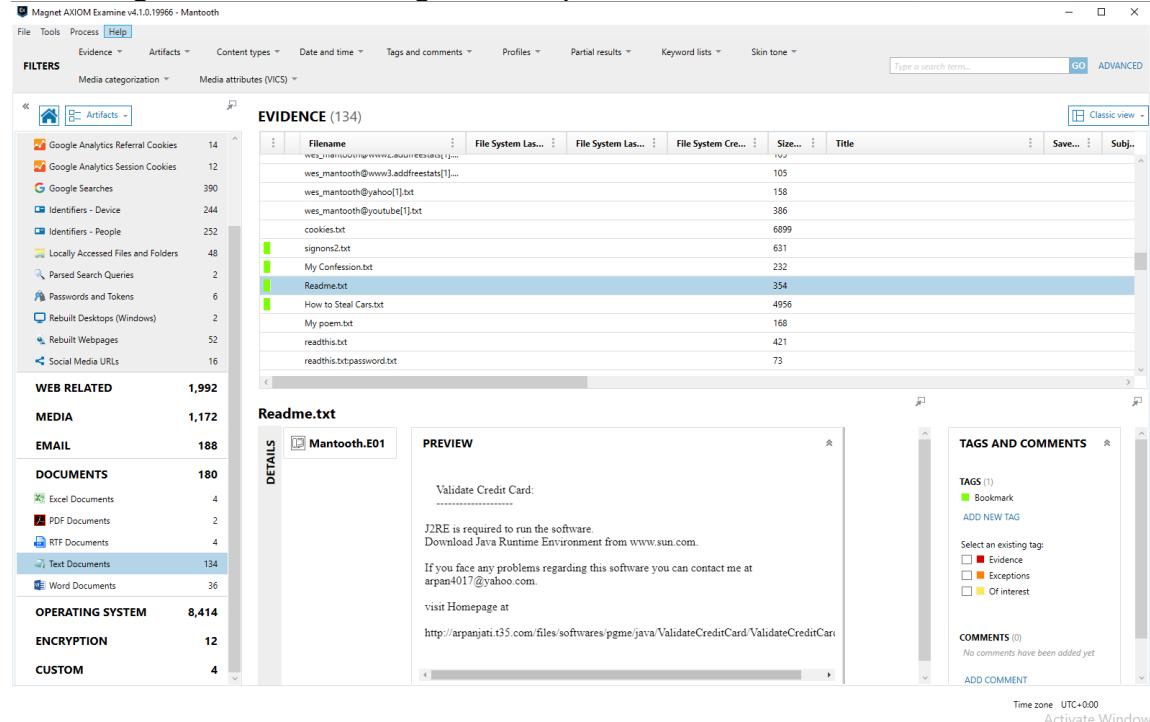


Figure 11.7

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

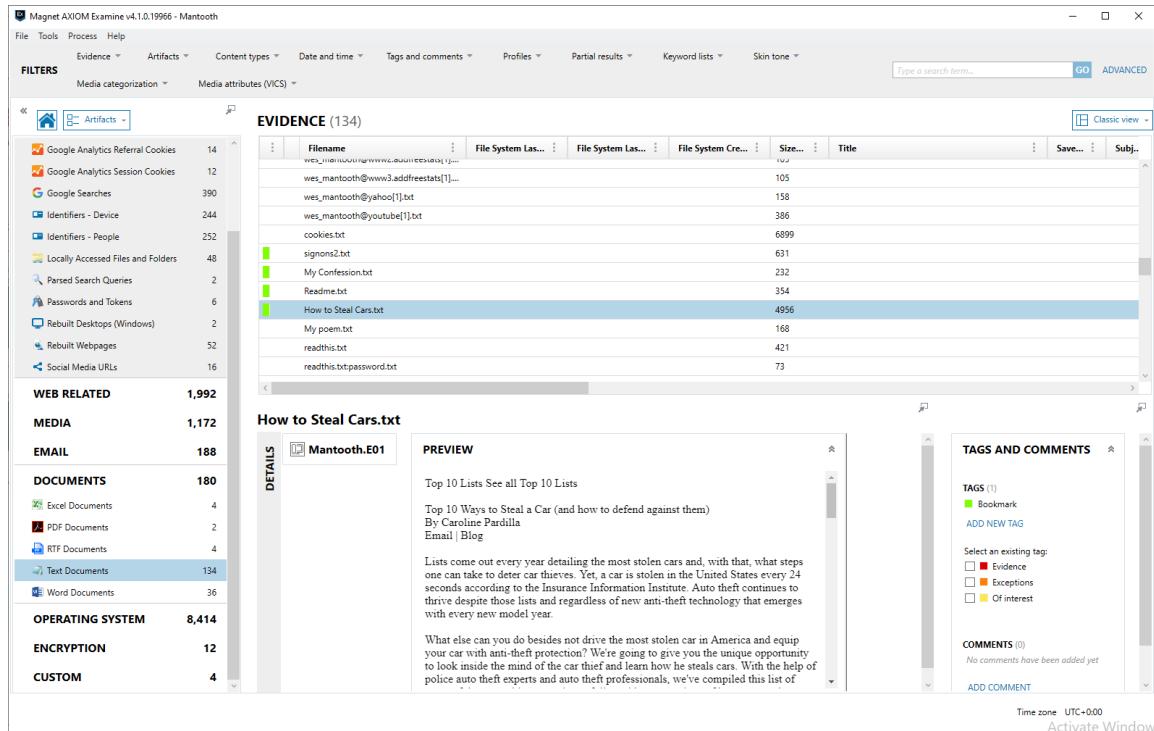


Figure 11.8

Figure 11.8 is a .txt file about stealing cars.

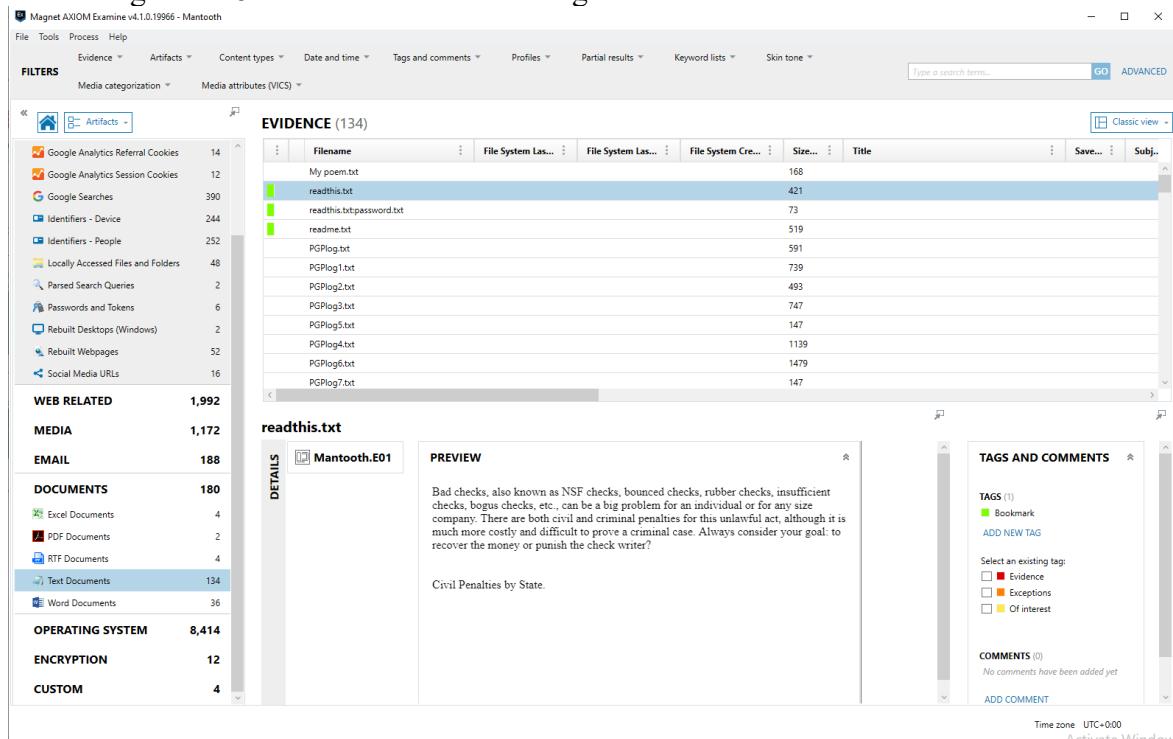


Figure 11.9

Figure 11.9 is a .txt file about bad checks.

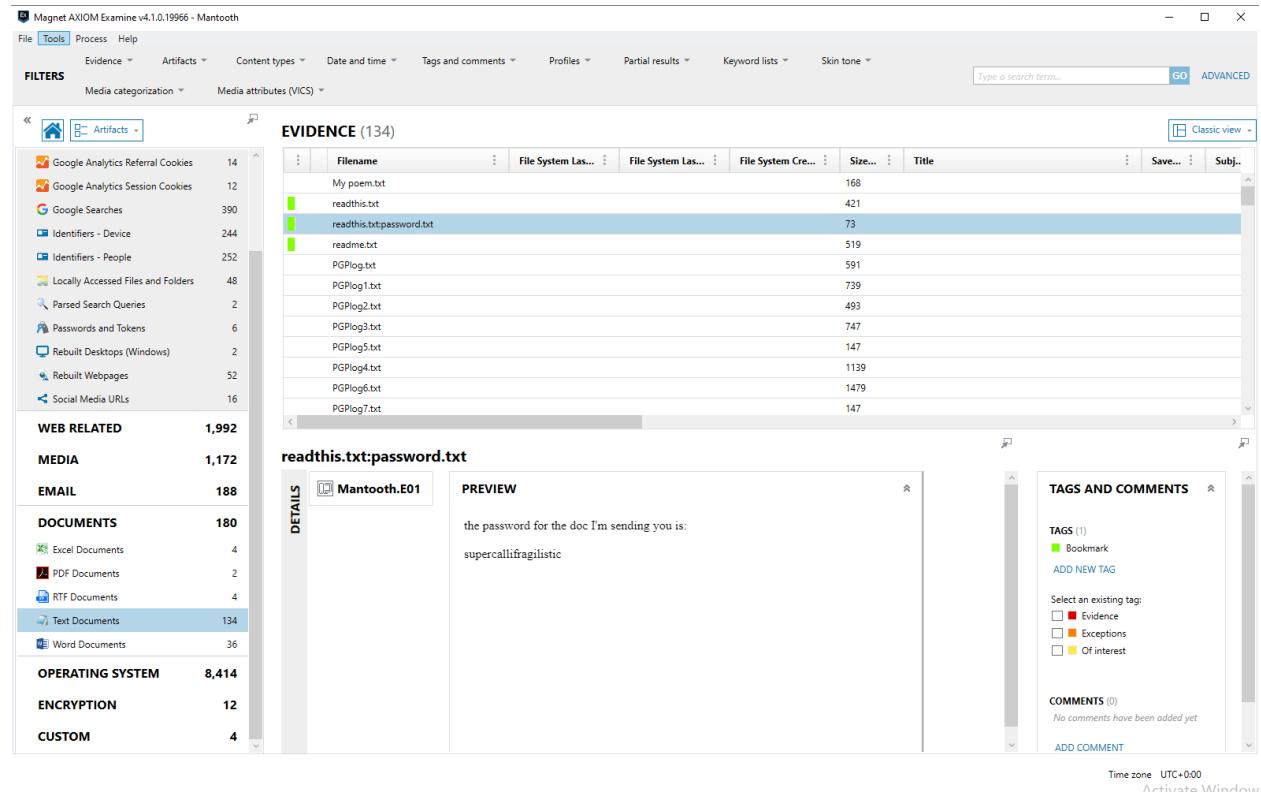


Figure 12.0

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 WESMANTOOOTH-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>