BTK Killer Investigation

Ferris State University

DFOR 310

Zachary C. Schulte

Table of Contents

BTK Investigation.

This week I have my practical final-exam for DFOR-310, and I am investigating the suspect serial killer BTK's hard drive. The investigators have obtained a search warrant and have confiscated the hard drive of BTK.

Imaging the Hard Drive

FTK Imager

I am using a software known as FTK Imager® to capture an image of the hard drive from the laptop obtained from the suspected serial killer known at BTK. After the laptop is removed from the suspect's home from the search warrant, I take it into the lab testing environment where we remove the hard drive from the device. Following this, we take the hard drive and capture the BIOS system date and time. This will be used throughout this investigation to create timestamps of the files on the system.

Following the documentation of the BIOS system date and time, the hard drive is installed back into the laptop. From here I connect a write blocker on the laptop. The write blocker allows me to capture an image of the hard drive without altering any of the files. It will create a bit-by-bit copy of all information found on the drive. Figure 1.0 shows the information that is provided before we image the drive.

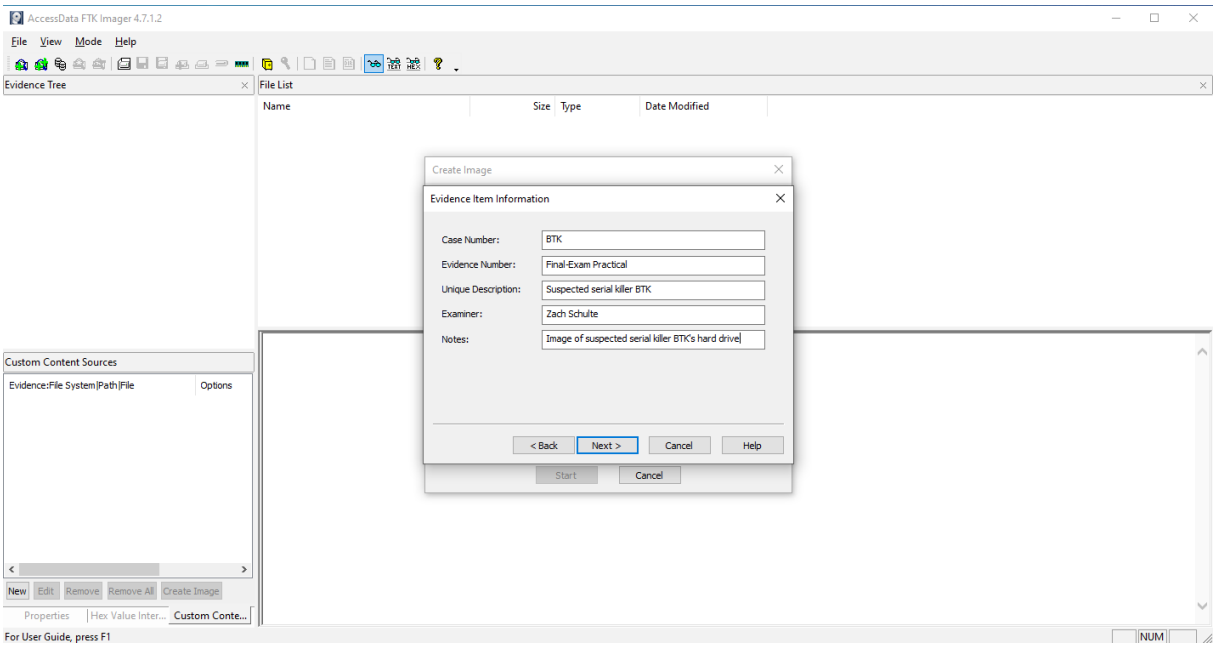


Figure 1.0

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

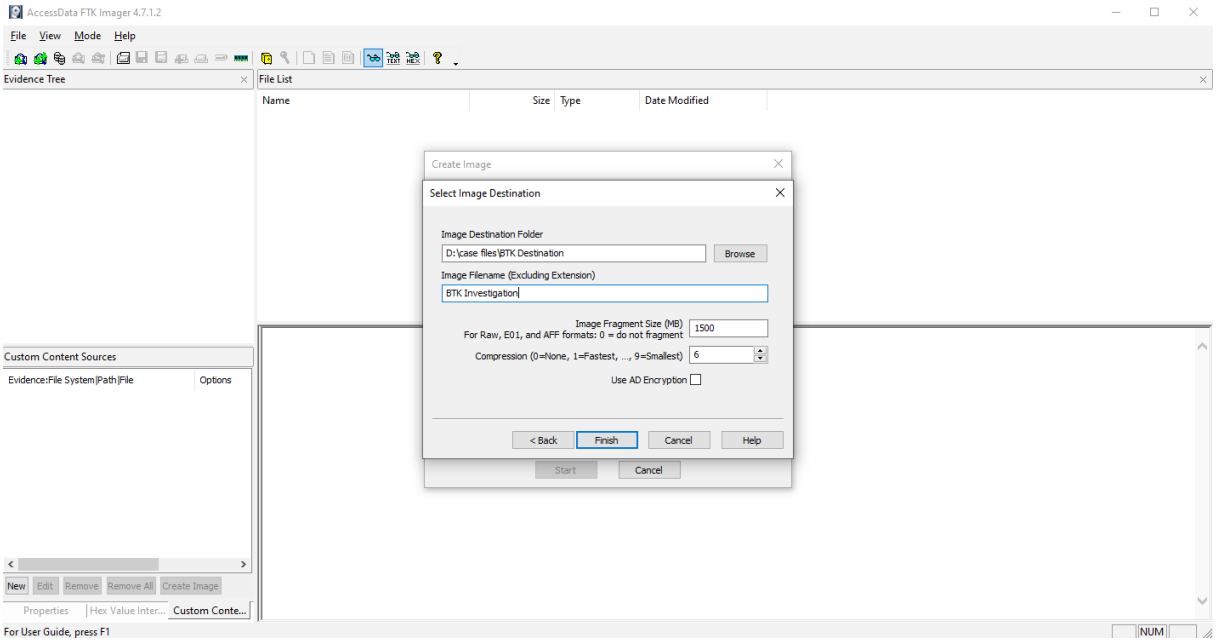


Figure 1.1

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

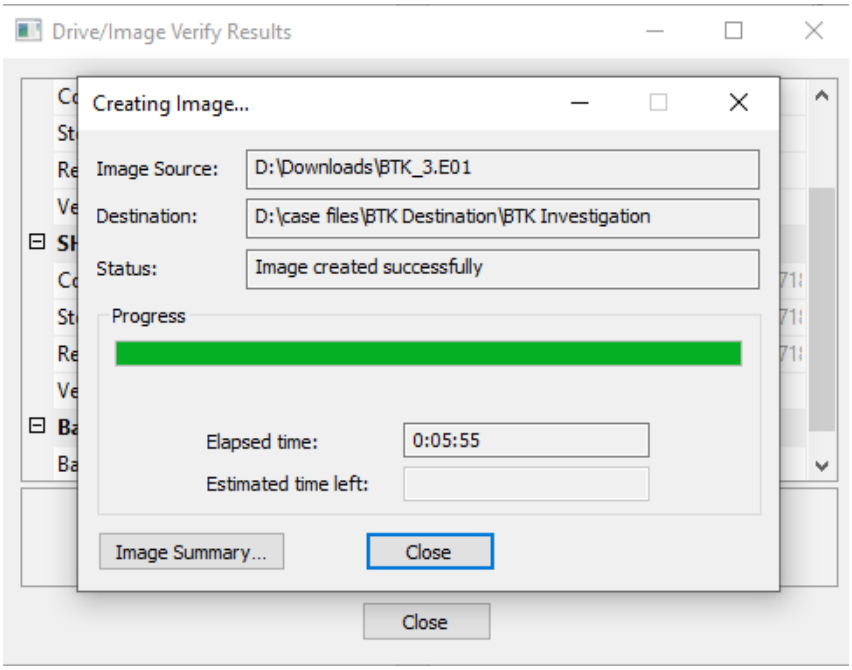


Figure 1.2

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

After the image is finished creating, it will provide a .txt document that provides an image summary in the destination folder. This gives information relevant to case number, evidence number, who the investigator is, and any notes created on the case. This information was copied from the summary.

Created By AccessData® FTK® Imager 4.7.1.2

Case Information:

Acquired using: ADI4.7.1.2

Case Number: BTK

Evidence Number: Final-Exam Practical

Unique description: Suspected serial killer BTK

Examiner: Zach Schulte

Notes: Image of suspected serial killer BTK's hard drive

Information for D:\case files\BTK Destination\BTK Investigation:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Verification Hashes]

MD5 verification hash: a4dbb82e811f7f64382991fce4ae8d40

SHA1 verification hash: 5a7e90a335c459deb6c905b75e607f8d94718958

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 125,829,120

[Image]

Image Type: E01

Case number: BTK_3

Evidence number: Laptop 3

Examiner: Prof.Otting

Notes:

Acquired on OS: Win 201x

Acquired using: ADI3.4.2.6

Acquire date: 8/31/2017 4:54:20 PM

System date: 8/31/2017 4:54:20 PM

Unique description: untitled

Source data size: 61440 MB

Sector count: 125829120

[Computed Hashes]

MD5 checksum: a4dbb82e811f7f64382991fce4ae8d40

SHA1 checksum: 5a7e90a335c459deb6c905b75e607f8d94718958

Image Information:

Acquisition started: Fri Apr 28 13:08:20 2023

Acquisition finished: Fri Apr 28 13:14:15 2023

Segment list:

D:\case files\BTK Destination\BTK Investigation.E01

D:\case files\BTK Destination\BTK Investigation.E02

D:\case files\BTK Destination\BTK Investigation.E03

D:\case files\BTK Destination\BTK Investigation.E04

D:\case files\BTK Destination\BTK Investigation.E05

Image Verification Results:

Verification started: Fri Apr 28 13:14:15 2023

Verification finished: Fri Apr 28 13:17:58 2023

MD5 checksum: a4dbb82e811f7f64382991fce4ae8d40 : verified

SHA1 checksum: 5a7e90a335c459deb6c905b75e607f8d94718958 : verified

When looking at downloading a file or taking an image of a hard drive or file, you want to look at the hash values presented 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 we can proceed with the investigation of the suspected serial killer BTK's hard drive.

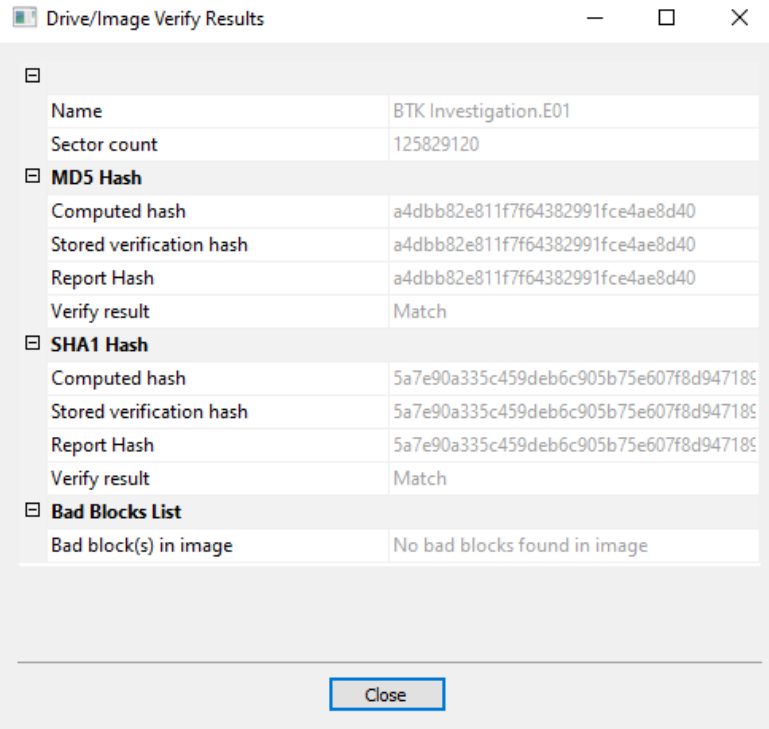


Figure 1.4

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

Presentation of Evidence

Forensic Explorer

The software I am using is called Forensic Explorer® V5.6.8. This software allows me to look at the image of the drive that was created. This software also allows us to look at the Windows Registry of the image. Figures 1.5-1.8 show the initial setup process of Forensic Explorer including investigator information and time zone.

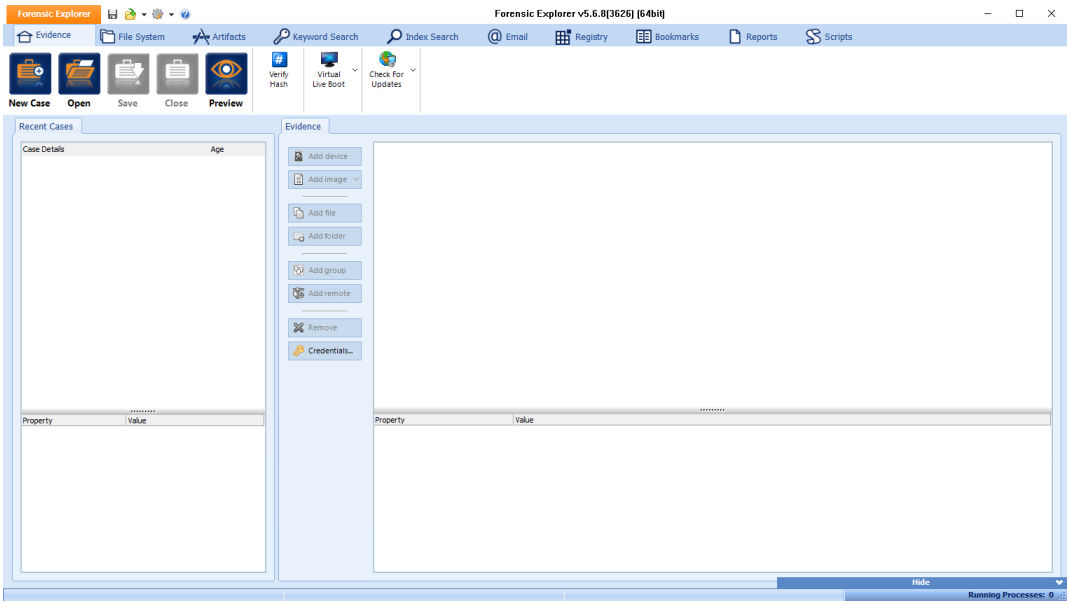


Figure 1.5

Figure 1.5 shows the software opening up of Forensic Explorer

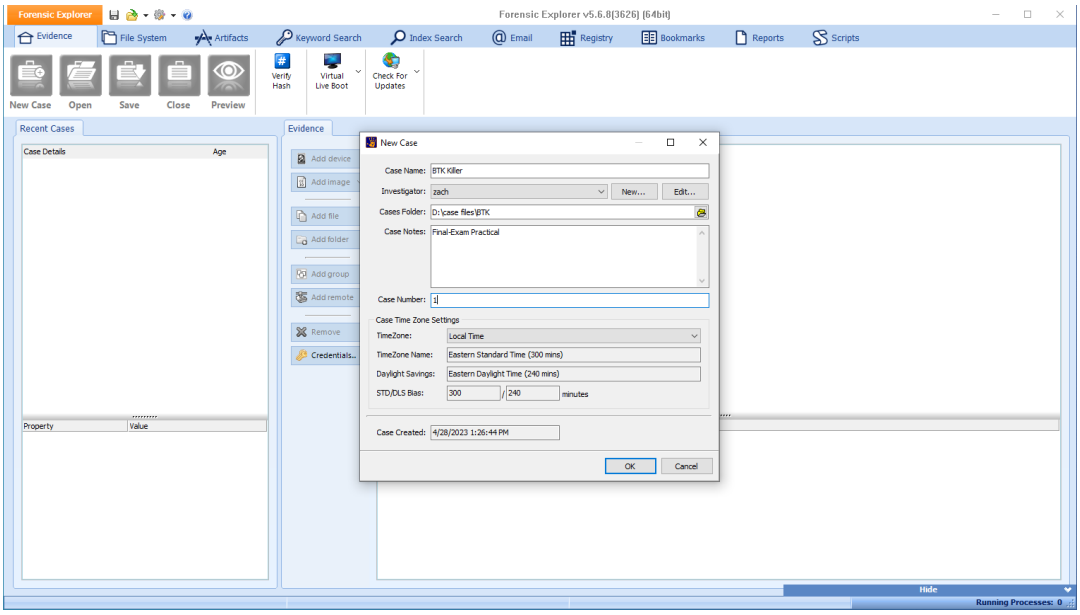


Figure 1.6

Figure 1.6 shows the creation of the new case that includes information like Case Name, Investigator information, and time zone.

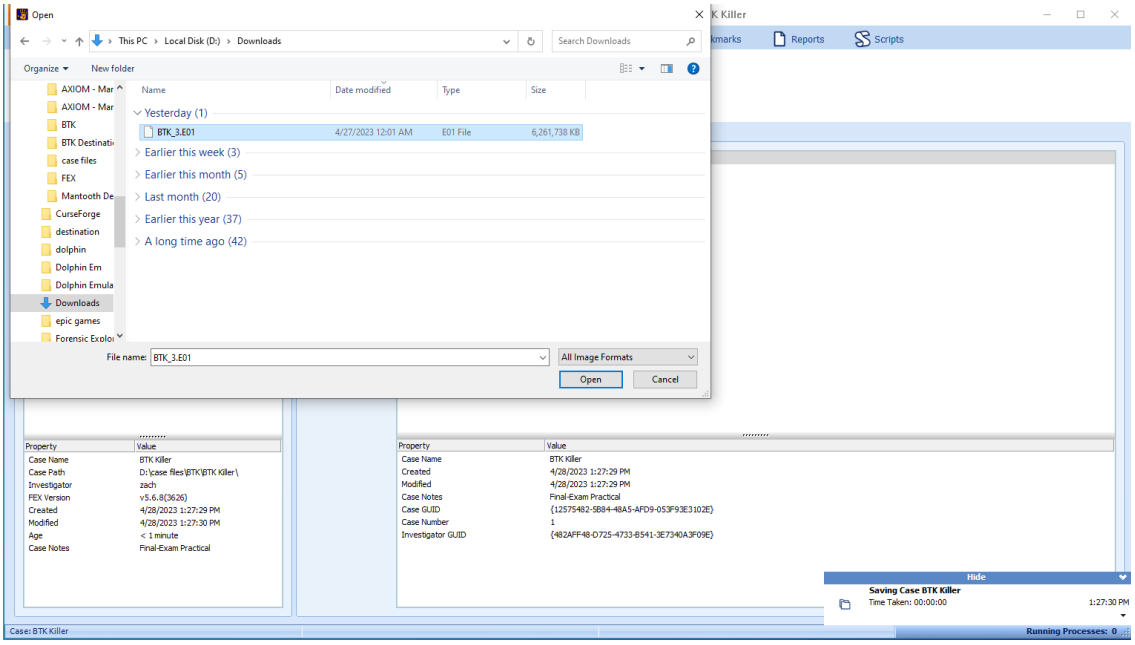


Figure 1.7

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

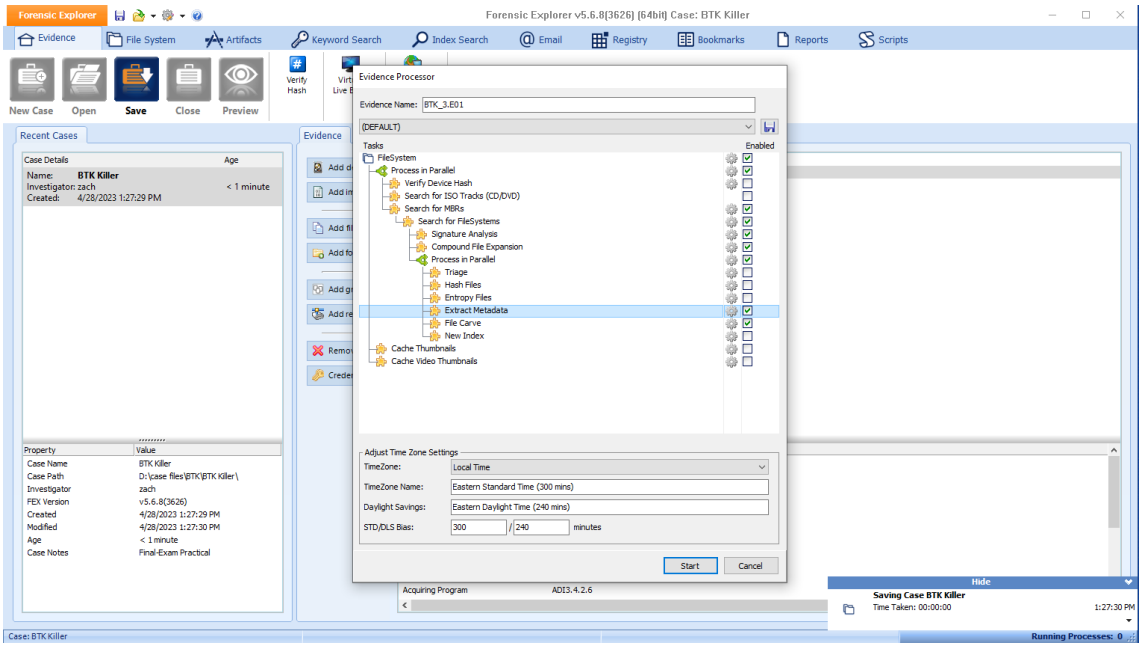


Figure 1.8

Figure 1.8 shows what data Forensic Explorer looks at. This is what I chose for this case.

Registry

The registry is found on the Windows Operating systems, and for this investigation 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, and Security Account Manager (SAM). In order to obtain the registry information, I need to import it from the File System to the registry in Forensic Explorer. There is one image that has been loaded into Forensic Explorer. Figures 1.9-2.0 show the image as well as where the registry information is found.

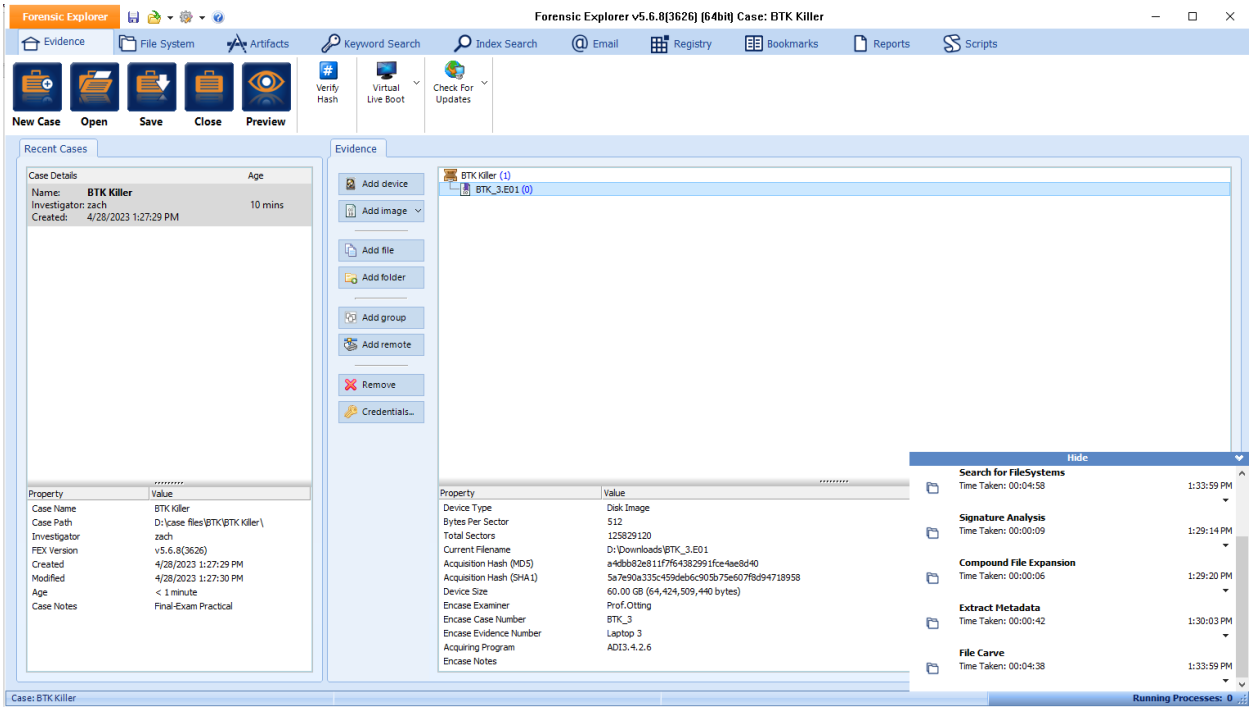


Figure 1.9

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

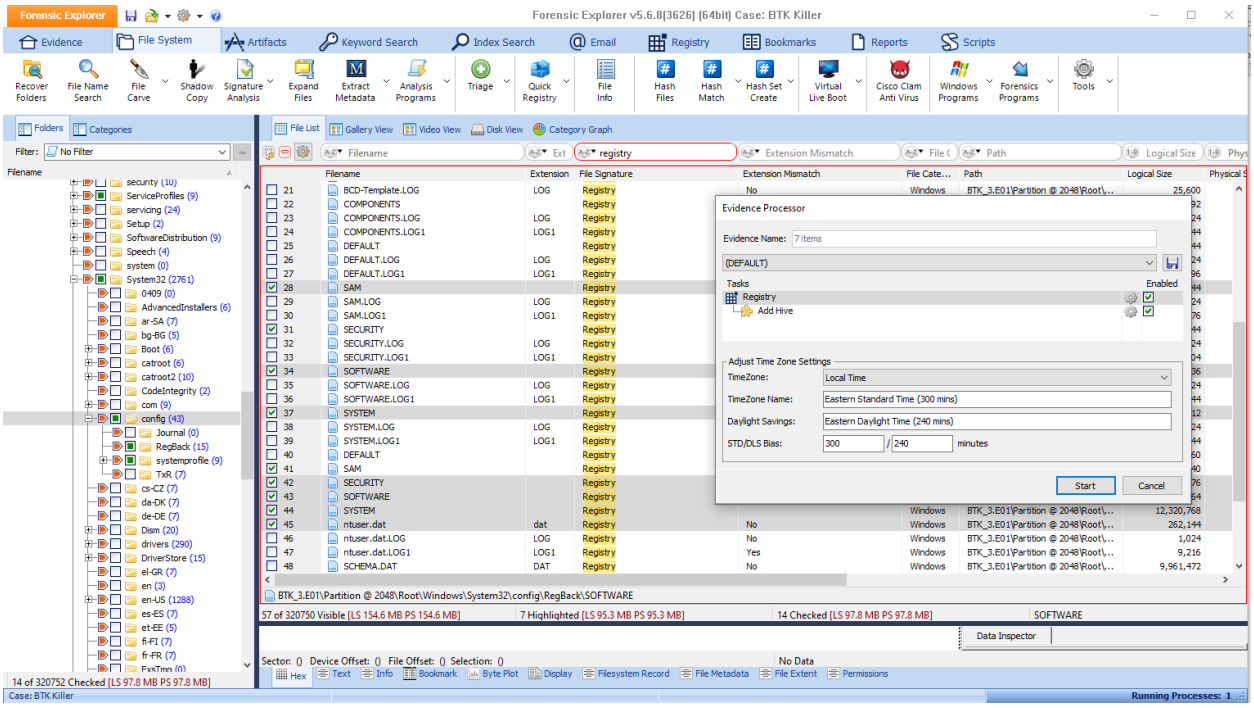


Figure 2.0

Figure 2.0 shows that the registry data is being sent to the registry module to be analyzed.

Security Accounts Manager

The Security Accounts Manager (SAM) is the first hive of the registry I will be analyzing. This hive contains information related to usernames as well as passwords for all accounts on this device. There are four user accounts within the SAM hive registry. Copied and pasted below is the information related to all users located within the SAM hive.

Parse: \SAM\Domains\Account\Users

User Name: Administrator

Full Name:

User ID: 500($01F4)

Account Created: 19-Apr-2017 17:04:38 [UTC]

Account Last Modified: 19-Apr-2017 20:03:50 [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: 6

Last Login: 21-Nov-2010 03:47:20 [UTC]

Password Required: True

Password Last Set: 21-Nov-2010 03:57:24 [UTC]

Last Password Fail: {Never}

Invalid Password Count: 0

Country Code: 0 (Default)

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

Source: BTK_3.E01\Partition @ 2048\Root\Windows\System32\config\SAM > SAM\SAM\SAM\Domains\Account\Users\000001F4

User Name: Guest

Full Name:

User ID: 501($01F5)

Account Created: 19-Apr-2017 17:04:38 [UTC]

Account Last Modified: 19-Apr-2017 20:03:50 [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: BTK_3.E01\Partition @ 2048\Root\Windows\System32\config\SAM > SAM\SAM\SAM\Domains\Account\Users\000001F5

User Name: Autumn Pelkey

User ID: 1000($03E8)

Account Created: 19-Apr-2017 17:04:29 [UTC]

Account Last Modified: 22-Apr-2017 00:30:36 [UTC]

Account Expires: {Never}

Account Type: ($0000)

Account Status: Normal user account

Number Logins: 5

Last Login: 22-Apr-2017 00:30:36 [UTC]

Password Required: True

Password Last Set: 19-Apr-2017 17:04:29 [UTC]

Last Password Fail: 19-Apr-2017 17:10:09 [UTC]
~~~~~~~~~~~~~~~~

Invalid Password Count: 0

Country Code: 1 (USA)

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

Source: BTK_3.E01\Partition @ 2048\Root\Windows\System32\config\SAM > SAM\SAM\SAM\Domains\Account\Users\000003E8

User Name: Dennis Rader

User ID: 1001($03E9)

Account Created: 19-Apr-2017 17:10:09 [UTC]

Account Last Modified: 22-Apr-2017 00:20:51 [UTC]

Account Expires: {Never}

Account Type: ($0000)

Account Status: Normal user account

Password does not expire

Number Logins: 4

Last Login: 22-Apr-2017 00:20:51 [UTC]

Password Required: False

Password Last Set: {Never}

Last Password Fail: {Never}
~~~~~~~~~~~~~~~~

Invalid Password Count: 0

Country Code: 0 (Default)

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

Source: BTK_3.E01\Partition @ 2048\Root\Windows\System32\config\SAM > SAM\SAM\SAM\Domains\Account\Users\000003E9

End of results.

System

The next hive I am looking at is called System. This hive has information related to the system or computer. The information pasted below is information about the computer name that was entered at installation.

Computer name.

The computer name was the standard information name given to the computer at creation of WIN-NGU8PA7DBCG.

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

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

Reference: None.
~~~~~~~~~~~~~~~~

==========

==========

Key Found: BTK_3.E01\SYSTEM\ControlSet001\Control\ComputerName\ComputerName\

Value Data

~~~~~ ~~~~

ComputerName WIN-NGU8PA7DBCG

Key Found: BTK_3.E01\SYSTEM\ControlSet002\Control\ComputerName\ComputerName\

Value Data

~~~~~ ~~~~

ComputerName WIN-NGU8PA7DBCG

Key Found: BTK_3.E01\SYSTEM\ControlSet001\Control\ComputerName\ComputerName\

Value Data

~~~~~ ~~~~

ComputerName WIN-NGU8PA7DBCG

Key Found: BTK_3.E01\SYSTEM\ControlSet002\Control\ComputerName\ComputerName\

Value Data

~~~~~ ~~~~

ComputerName WIN-NGU8PA7DBCG

Registry Key Processor finished.

Shutdown Time.

There appears to be a shutdown time last recorded on 4/22/2017 1:01:38 AM

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

Description: Last computer shutdown time.

Reference: None.

==========

==========

Key Found: BTK_3.E01\SYSTEM\ControlSet001\Control\Windows\

Value	Data
ShutdownTime	4/22/2017 1:01:38 AM

Key Found: BTK_3.E01\SYSTEM\ControlSet002\Control\Windows\

Value Data

~~~~~ ~~~~

ShutdownTime 4/19/2017 8:04:07 PM

Key Found: BTK_3.E01\SYSTEM\ControlSet001\Control\Windows\

Value Data

~~~~~ ~~~~

ShutdownTime 4/19/2017 5:59:31 PM

Key Found: BTK_3.E01\SYSTEM\ControlSet002\Control\Windows\

Value Data

~~~~~ ~~~~

ShutdownTime 4/19/2017 8:04:07 PM
~~~~~

Registry Key Processor finished.

Time Zone.

The time zone appears to be recorded in Eastern Standard Time.

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

Description: The time zone setting.

Reference: None.

==========

==========

Key Found: BTK_3.E01\SYSTEM\ControlSet001\Control\TimeZoneInformation\

Value	Data
ActiveTimeBias	0x00F0
Bias	0x012C

DaylightBias 0xFFFFFFC4

DaylightName @tzres.dll,-111

DaylightStart .....

DynamicDaylightTimeDisabled 0x0000

StandardBias 0x0000

StandardName @tzres.dll,-112

StandardStart .....

TimeZoneKeyName Eastern Standard Time

Key Found: BTK_3.E01\SYSTEM\ControlSet002\Control\TimeZoneInformation\

Value Data

~~~~ ~~~~

ActiveTimeBias 0x00F0

Bias 0x012C

DaylightBias 0xFFFFFFC4

DaylightName @tzres.dll,-111
~~~~

DaylightStart .....

DynamicDaylightTimeDisabled 0x0000

StandardBias 0x0000

StandardName @tzres.dll,-112

StandardStart .....

TimeZoneKeyName Eastern Standard Time

Key Found: BTK_3.E01\SYSTEM\ControlSet001\Control\TimeZoneInformation\

Value Data

~~~~ ~~~~

ActiveTimeBias 0x00F0

Bias 0x012C

DaylightBias 0xFFFFFFC4

DaylightName @tzres.dll,-111

DaylightStart .....

DynamicDaylightTimeDisabled 0x0000
~~~~

StandardBias 0x0000

StandardName @tzres.dll,-112

StandardStart .....

TimeZoneKeyName Eastern Standard Time

Key Found: BTK_3.E01\SYSTEM\ControlSet002\Control\TimeZoneInformation\

Value Data

~~~~~ ~~~~

ActiveTimeBias 0x00F0

Bias 0x012C

DaylightBias 0xFFFFFFC4

DaylightName @tzres.dll,-111

DaylightStart .....

DynamicDaylightTimeDisabled 0x0000

StandardBias 0x0000

StandardName @tzres.dll,-112
~~~~~

StandardStart .....

TimeZoneKeyName Eastern Standard Time

Registry Key Processor finished.

USB Devices.

The next set of information I want to look at within the System hive is the Universal Serial Bus (USB) storage devices found within this laptop previously. According to Forensic Explorer there have been zero USB devices.

Search for: SYSTEM\ControlSet001\Enum\USBSTOR\...\FriendlyName

Description: List of installed USB storage devices using "FriendlyName" key.

Reference: None.

==========

==========

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

Registry Key Processor finished.

Software

The next main hive I want to look at is called Software. This hive registry contains information related to what is installed on the device, the original install date of the OS, network cards, and the default user name.

Default username.

The default user name found on this device is Autumn Pelkey.

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

==========

==========

Key Found: BTK_3.E01\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\

Value Data

~~~~~ ~~~~

DefaultUserName Autumn Pelkey

DefaultUserName Autumn Pelkey

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

==========

==========

BTK_3.E01\SOFTWARE\Clients\Mail\Hotmail\

BTK_3.E01\SOFTWARE\Clients\Mail\Hotmail\Protocols\mailto\
~~~~~

BTK_3.E01\SOFTWARE\Clients\Mail\Hotmail\Protocols\mailto\

BTK_3.E01\SOFTWARE\Clients\Mail\Hotmail\Protocols\mailto\DefaultIcon\

BTK_3.E01\SOFTWARE\Clients\Mail\Hotmail\Protocols\mailto\shell\open\command\

BTK_3.E01\SOFTWARE\Clients\Mail\Hotmail\shell\open\command\

BTK_3.E01\SOFTWARE\Clients\Mail\Windows Mail\Envelope\CLSID\

BTK_3.E01\SOFTWARE\Clients\Mail\Windows Mail\Envelope\CurVer\

BTK_3.E01\SOFTWARE\Clients\Mail\Hotmail\

BTK_3.E01\SOFTWARE\Clients\Mail\Hotmail\Protocols\mailto\

BTK_3.E01\SOFTWARE\Clients\Mail\Hotmail\Protocols\mailto\

BTK_3.E01\SOFTWARE\Clients\Mail\Hotmail\Protocols\mailto\DefaultIcon\

BTK_3.E01\SOFTWARE\Clients\Mail\Hotmail\Protocols\mailto\shell\open\command\

BTK_3.E01\SOFTWARE\Clients\Mail\Hotmail\shell\open\command\

BTK_3.E01\SOFTWARE\Clients\Mail\Windows Mail\Envelope\CLSID\

BTK_3.E01\SOFTWARE\Clients\Mail\Windows Mail\Envelope\CurVer\

Registry Key Processor finished.

OS Install Date.

What I am looking for next is the original date the Operating System was installed on, or also the (OS Install Date) which is April 19th, 2017, at 5:04:39 PM.

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

Description: Installation date of the Operating System.

Reference: None.

==========

==========

Key Found: BTK_3.E01\SOFTWARE\Microsoft\Windows NT\CurrentVersion\

Value	Data
~~	~~~~
InstallDate	4/19/2017 5:04:39 PM
InstallDate	4/19/2017 5:04:39 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: BTK_3.E01\SOFTWARE\Microsoft\Windows NT\CurrentVersion\

Value Data

~~~~~ ~~~~

RegisteredOwner Windows User

RegisteredOwner Windows User

RegisteredOrganization

RegisteredOrganization

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:

BTK_3.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0C479F34-8E0D-4C1C-9DAC-C1071A6C5007}\

Value	Data
DisplayName	VMware Tools
DisplayVersion	10.0.10.4301679
Publisher	VMware, Inc.
URLInfoAbout	

Key Found:

BTK_3.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}\

Value	Data

DisplayName Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161

DisplayVersion 9.0.30729.6161

Publisher Microsoft Corporation

URLInfoAbout

Key Found: BTK_3.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{925E7EEB-6D38-492E-A238-1933644DF1C0}\

Value Data

~~~~ ~~~~

DisplayName LibreOffice 5.3 Help Pack (English (United States))

DisplayVersion 5.3.2.2

Publisher The Document Foundation

URLInfoAbout http://www.documentfoundation.org
~~~~

Key Found:

BTK_3.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132} - 1033\

Value	Data
DisplayName	Microsoft .NET Framework 4.6
DisplayVersion	4.6.00081
Publisher	Microsoft Corporation
URLInfoAbout	http://go.microsoft.com/fwlink/?LinkId=286133

Key Found:

BTK_3.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{94A631D5-B30A-3DD8-B65C-1117C09DA73E}\

Value	Data

~~~~~ ~~~~

DisplayName Microsoft .NET Framework 4.6

DisplayVersion 4.6.00081

Publisher Microsoft Corporation

URLInfoAbout http://go.microsoft.com/fwlink/?LinkId=286133

Key Found:

BTK_3.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0C479F34-8E0D-4C1C-9DAC-C1071A6C5007}\

Value Data

~~~~~ ~~~~

DisplayName VMware Tools

DisplayVersion 10.0.10.4301679

Publisher VMware, Inc.

URLInfoAbout

Key Found:

BTK_3.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}\

Value	Data
~~	~~~~
DisplayName	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161
DisplayVersion	9.0.30729.6161
Publisher	Microsoft Corporation
URLInfoAbout	

Key Found:

BTK_3.E01\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{925E7EEB-6D38-492E-A238-1933644DF1C0}\

Value	Data
~~	~~~~
DisplayName	LibreOffice 5.3 Help Pack (English (United States))
DisplayVersion	5.3.2.2
Publisher	The Document Foundation
URLInfoAbout	http://www.documentfoundation.org

Registry Key Processor finished.

NTUser.Dat

The final registry I am looking at for information is NTUser.dat. This hive registry has information related to 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:

BTK_3.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg\

Value	Data
~~	~~~~
0	Photo Diary.jpg,File
1	Yours Truly.jpg,File
2	basic_knots.jpg,File
3	springfield_armory_xd.jpg,File
4	rope.jpg,File

5 filmcamera.jpg,File

6 knife.jpg,File

MRUListEx 6 5 4 3 2 1 0

Key Found:
BTK_3.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\
.png\

Value Data

~~~~~ ~~~~

0 plasticbag-244x300.png,File

MRUListEx 0

Key Found:
BTK_3.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\
.rtf\
~~~~~

Value	Data
0	Project List.rtf,File
1	Death to Nancy.rtf,File
2	Oh Anna Why Didn't You Appear.rtf,File
3	Floppy.rtf,File
4	Death.rtf,File
5	anna.rtf,File
6	Guilty.rtf,File
7	Wyatt's poem.rtf,File
8	How many.rtf,File
9	Shirley's Kids.rtf,File
MRUListEx	0 9 8 7 6 5 2 4 1 3

Key Found:

BTK_3.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\

Value	Data
0	PL,File
1	Communications,File
10	anna.rtf,File
11	Guilty.rtf,File
12	Wyatt's poem.rtf,File
13	How many.rtf,File
14	Shirley's Kids.rtf,File
15	basic_knots.jpg,File
16	Kit,File
17	springfield_armory_xd.jpg,File
18	plasticbag-244x300.png,File
19	rope.jpg,File
2	Death to Nancy.rtf,File
20	filmcamera.jpg,File
21	knife.jpg,File

22 Project List.rtf,File

3 Oh Anna Why Didn't You Appear.rtf,File

4 Photo Diary.jpg,File

5 Pictures,File

6 Yours Truly.jpg,File

7 Floppy.rtf,File

8 Poems,File

9 Death.rtf,File

Key Found:

BTK_3.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder\

Value	Data
0	Communications,File
1	Pictures,File

2 Poems,File

3 Kit,File

4 PL,File

MRUListEx 4 3 0 2 1

Key Found:

BTK_3.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\

Value Data

~~~~~ ~~~~

MRUListEx 0 22 16 21 20 19 18 17 15 1 14 13 12 11 8 10 3 9 2 7 5 6 4

Registry Key Processor finished.
~~~~~

Disk Structure

Partition Size

On this device there is one image. This image contains one partition. Partition one is Partition @ 2048 and has a logical size of 64,422,411,776 bytes, or around ~60 gigabytes of data in total.

Format

Partition one (Partition @ 2048) is formatted with NTFS.

Active File Review

Axiom

The next software I am using for this case is called AXIOM Process and AXIOM Examine. Figures 2.1-2.3 show how the case is loaded into the software.

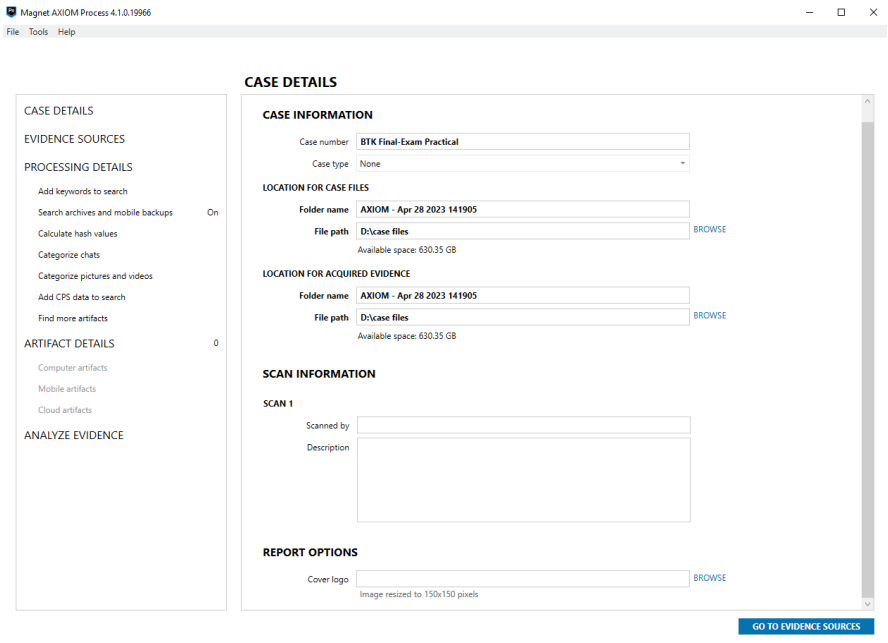


Figure 2.1

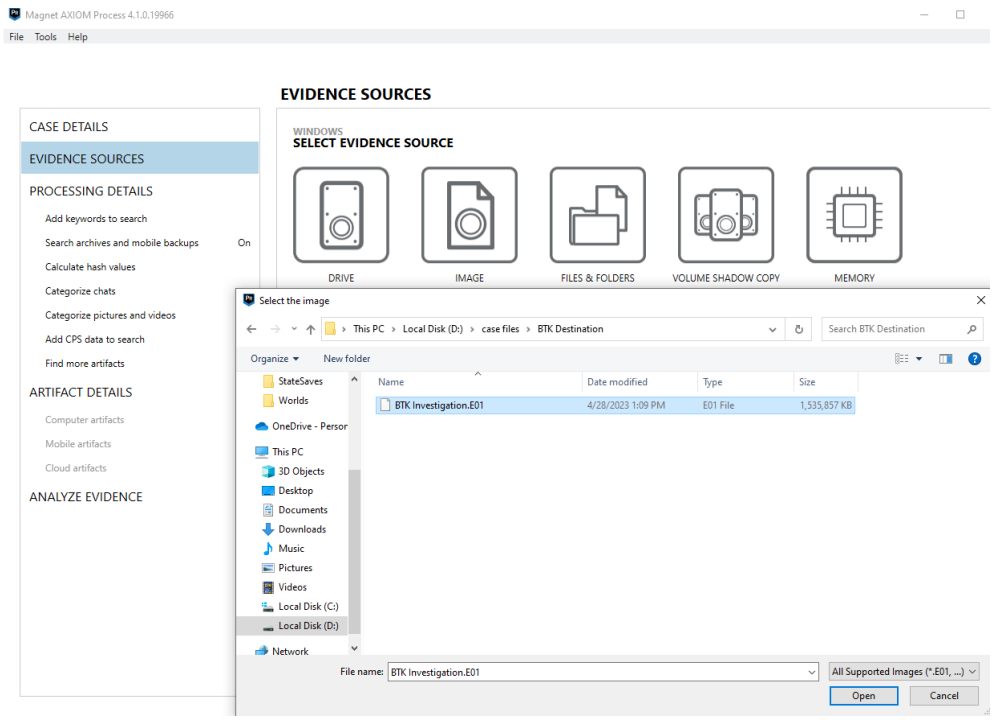


Figure 2.2

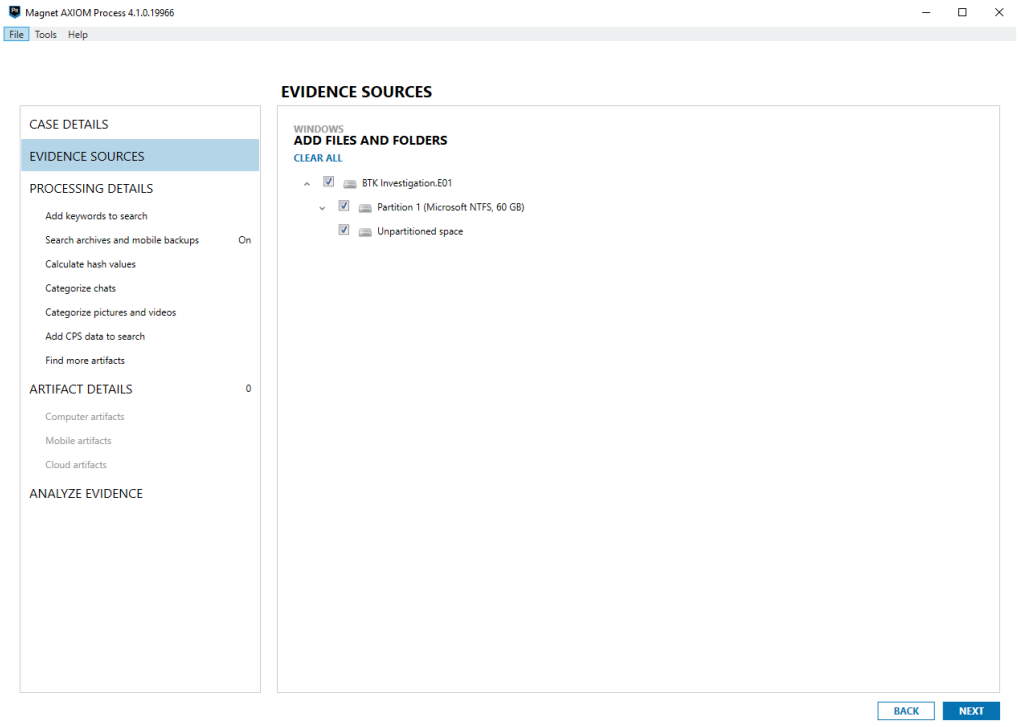


Figure 2.3

Web Related

Main History

The main history includes searches in Internet Explorer as well as Google Chrome. This includes downloads, keyword searches, and the main google searches found on this device. Figures 2.4-5.4 show this information.

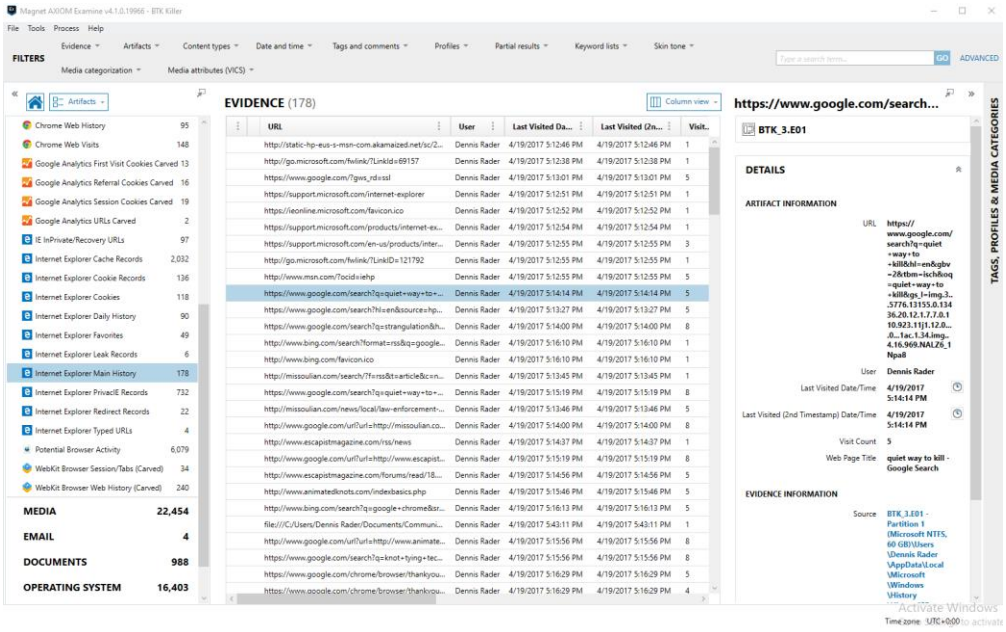


Figure 2.4

Figure 2.4 shows a google search for “quiet way to kill”

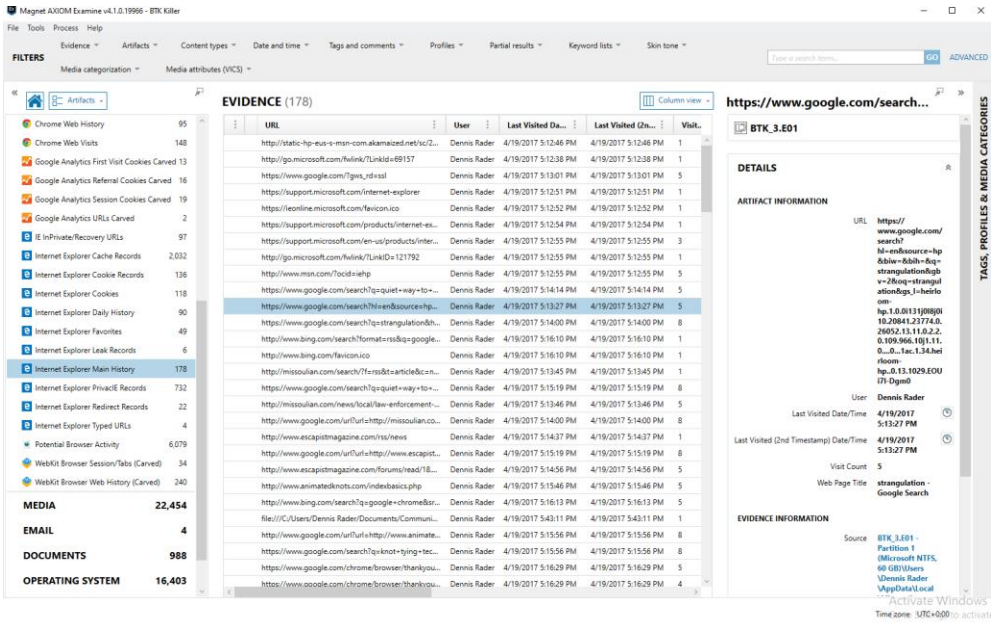


Figure 2.5

Figure 2.5 shows a search for “strangulation”

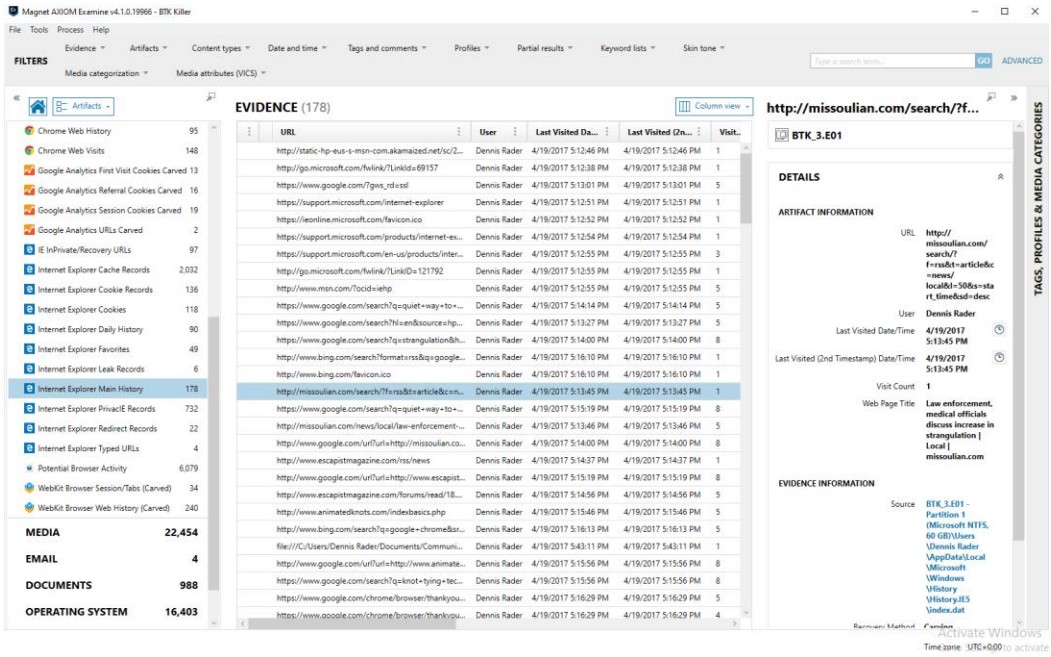


Figure 2.6

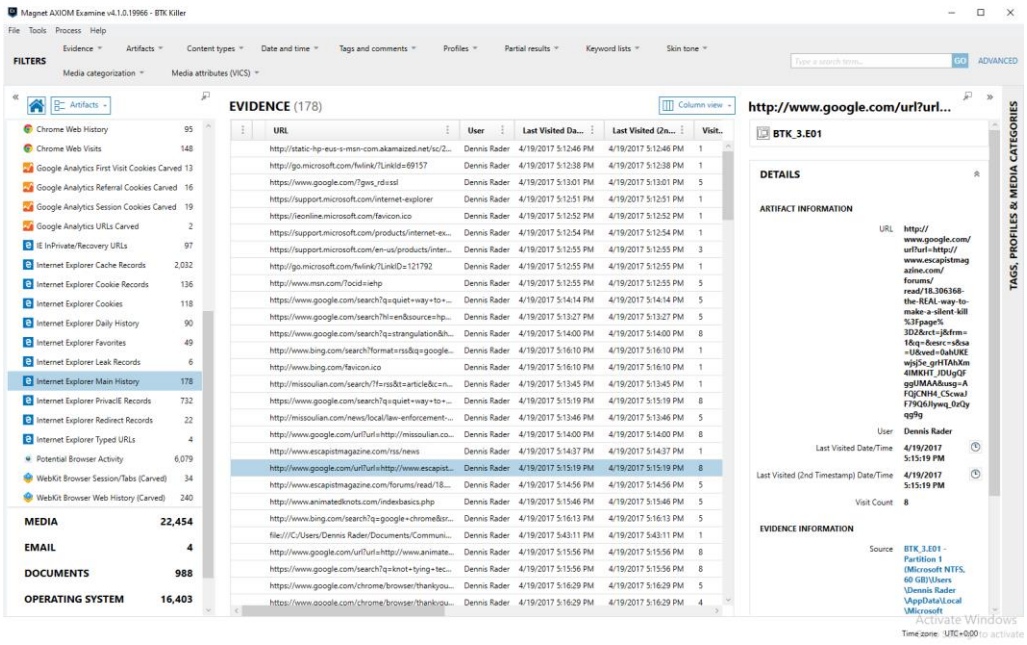


Figure 2.7

Figure 2.7 shows a search result for “the REAL way to make a silent kill”

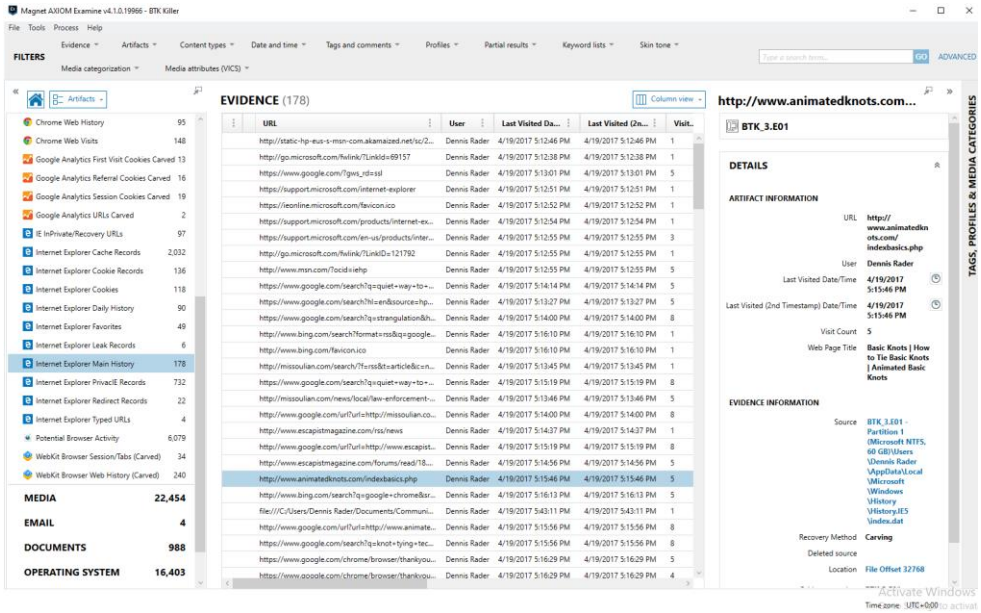
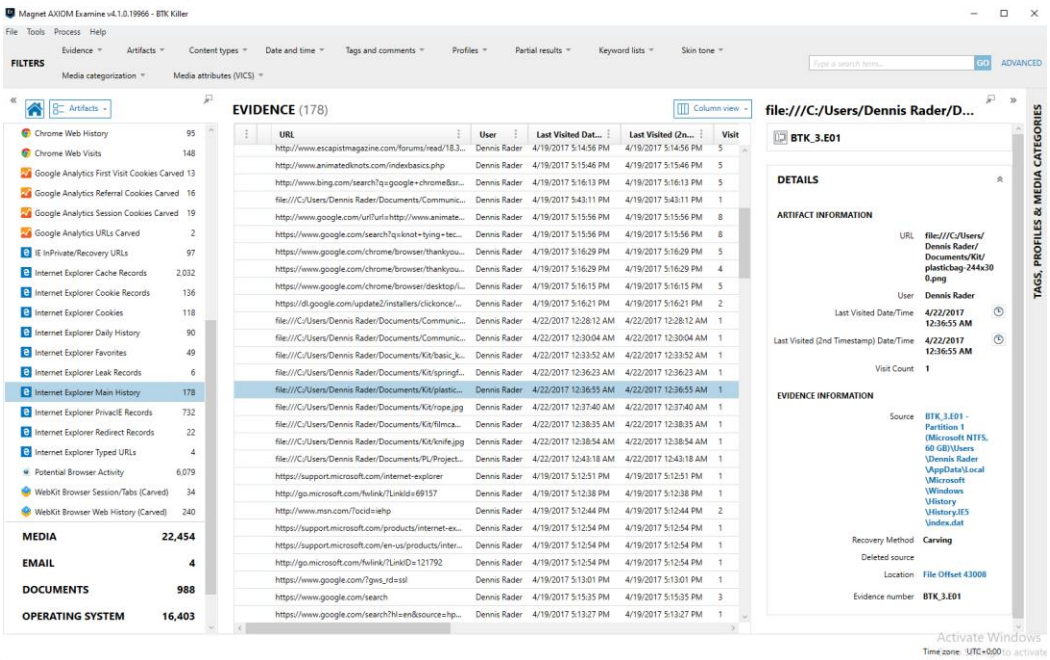


Figure 2.8

Figure 2.8 search for basic knots.



.

Figure 2.9

Figure 2.9 file titled “plastic bag”.

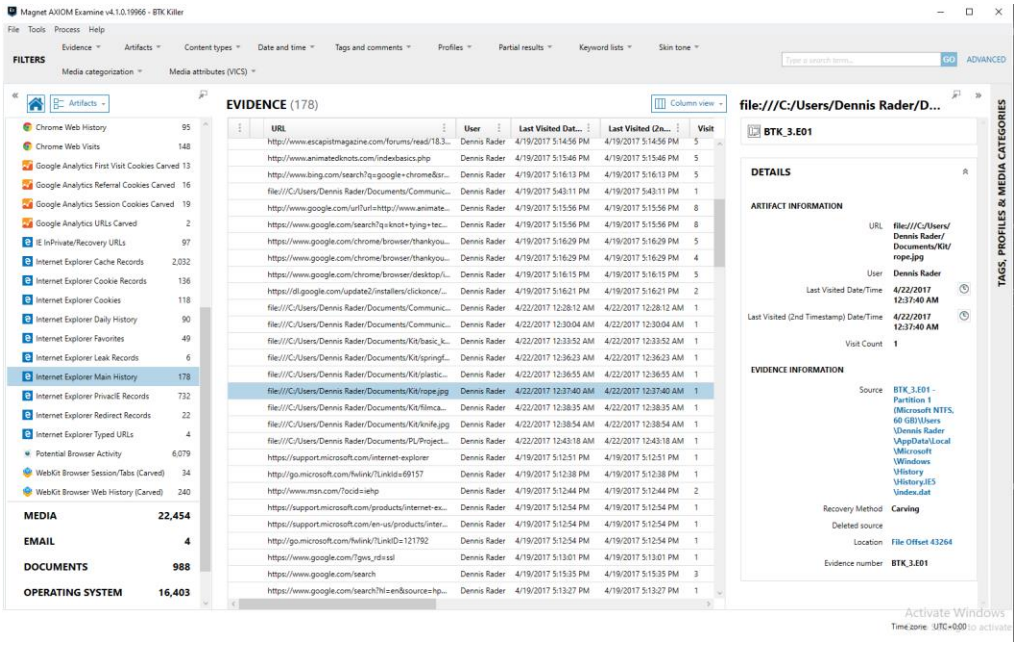


Figure 3.0

Figure 3.0 file titled “rope.jpg”

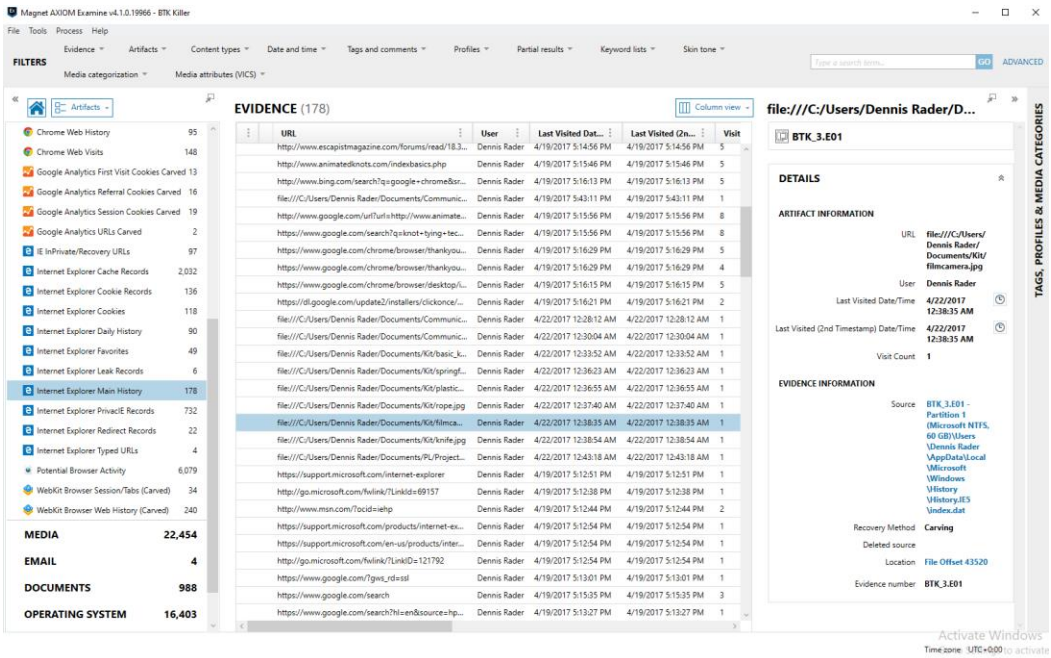


Figure 3.1

Figure 3.1 file titled “filmcamera.jpg”

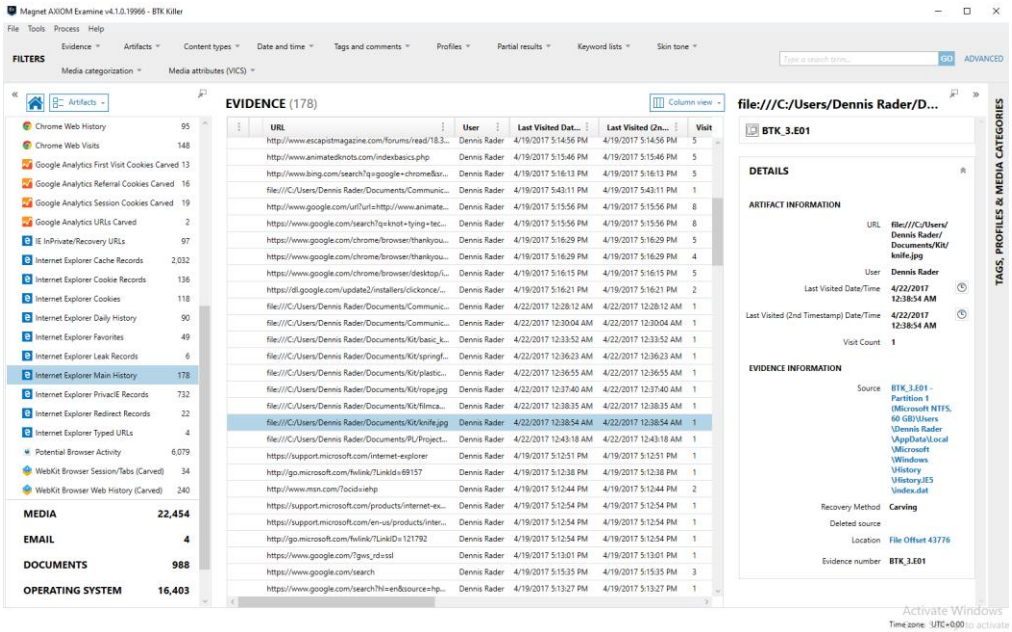


Figure 3.2

Figure 3.2 file titled “knife.jpg”

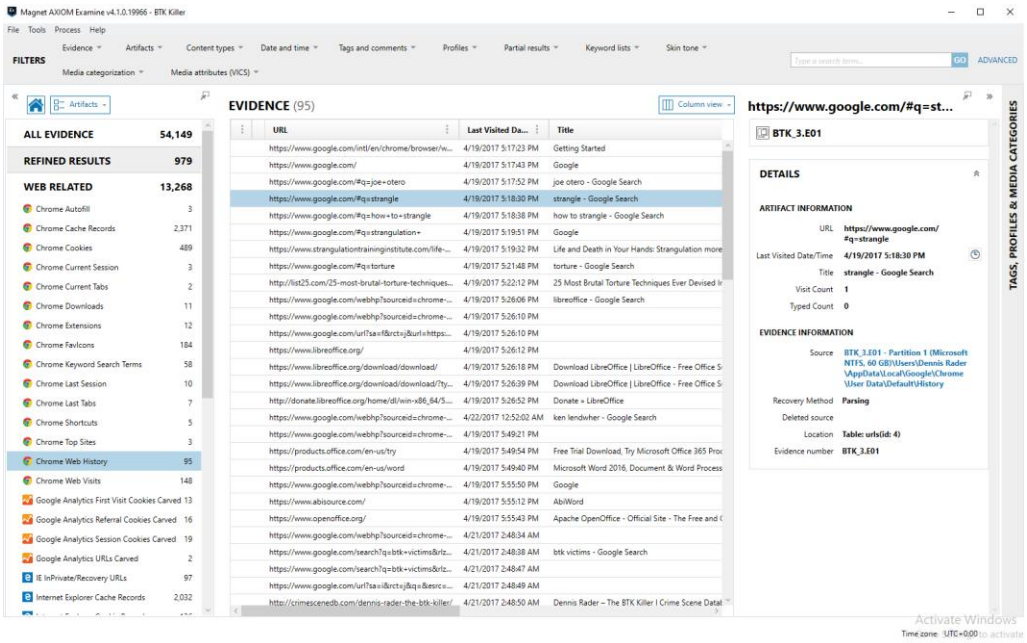


Figure 3.3

Figure 3.3 search result for “strangle.”

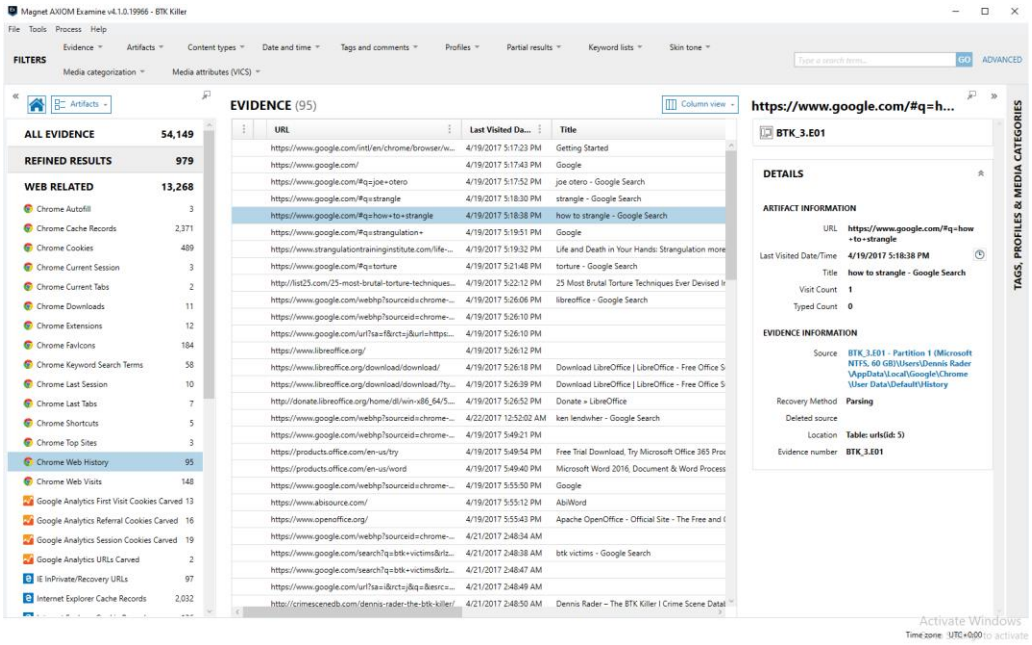
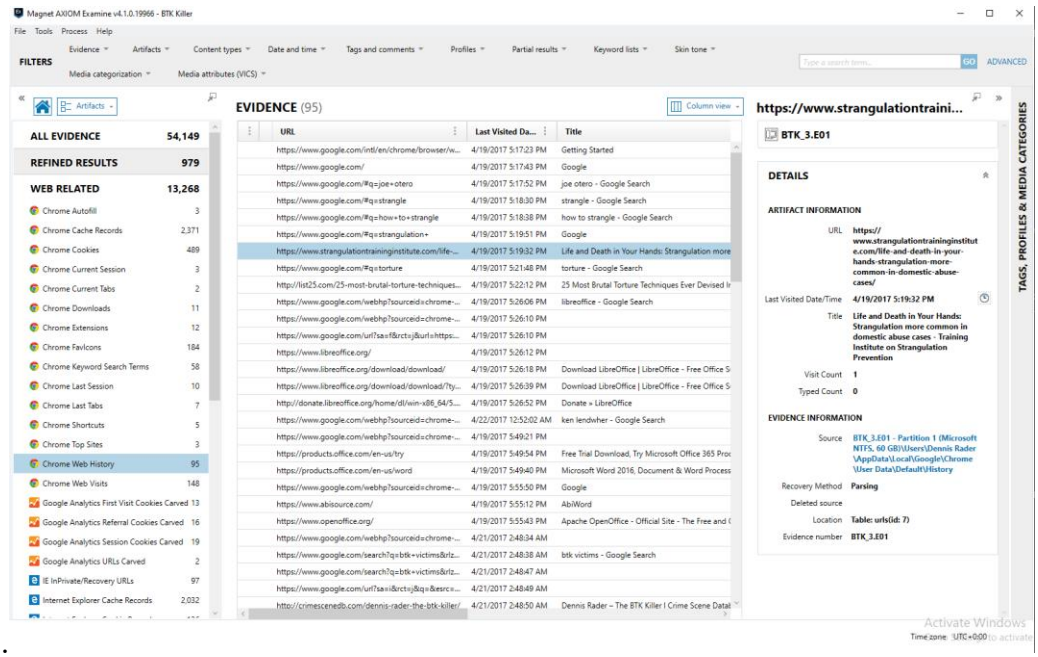


Figure 3.4

Figure 3.4 search result for “how to strangle”



.

Figure 3.5

Figure 3.5 search for “strangulation more common in domestic abuse cases.”

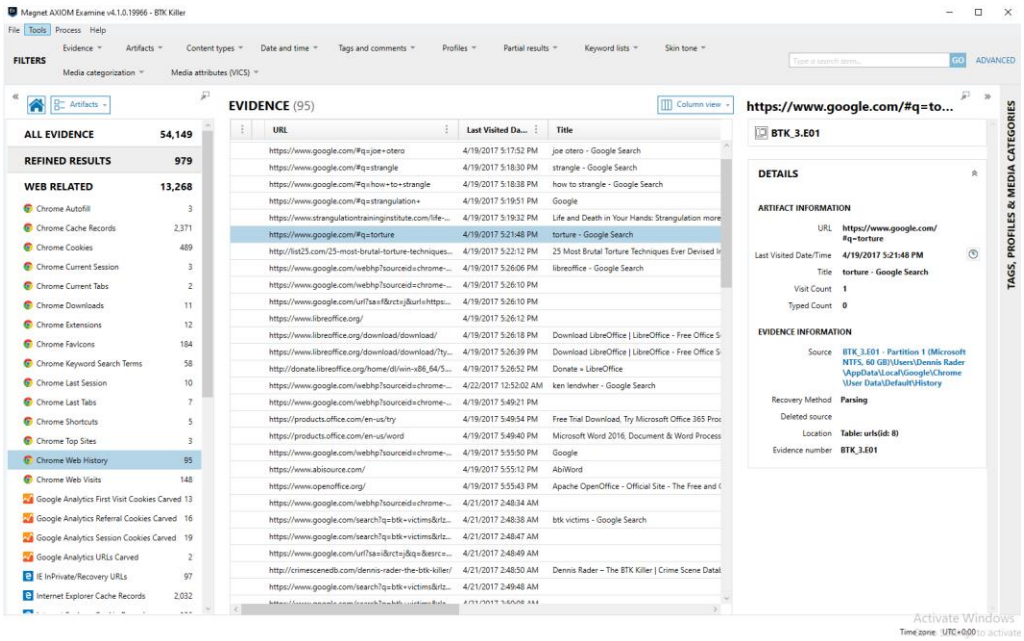


Figure 3.6

Figure 3.6 search for “torture”

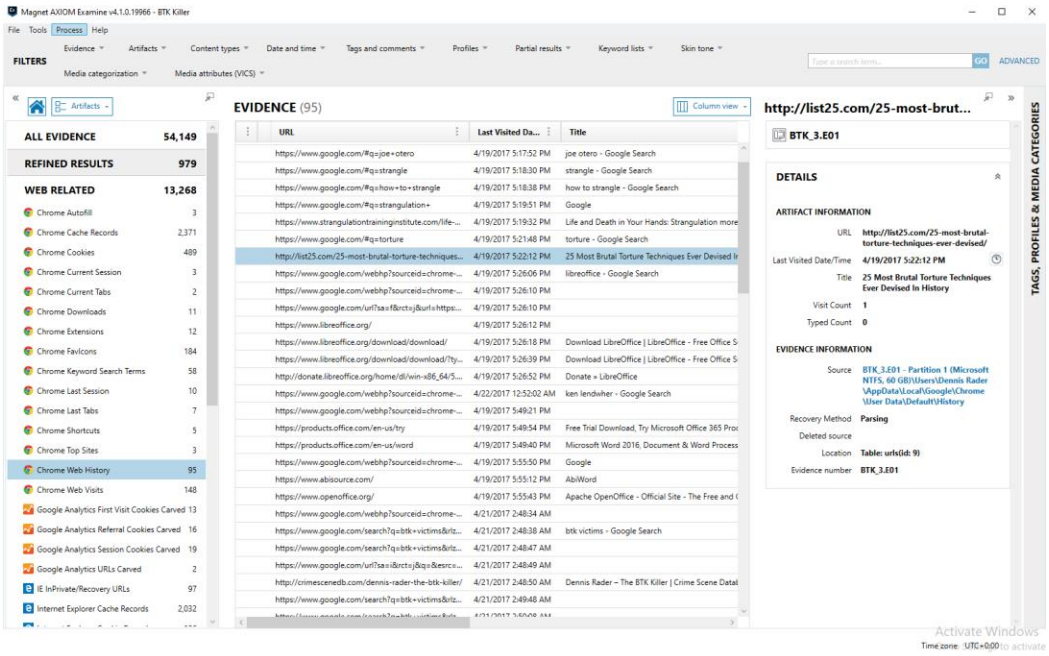


Figure 3.7

Figure 3.7 “search for 25 most brutal torture techniques ever devised in history.”

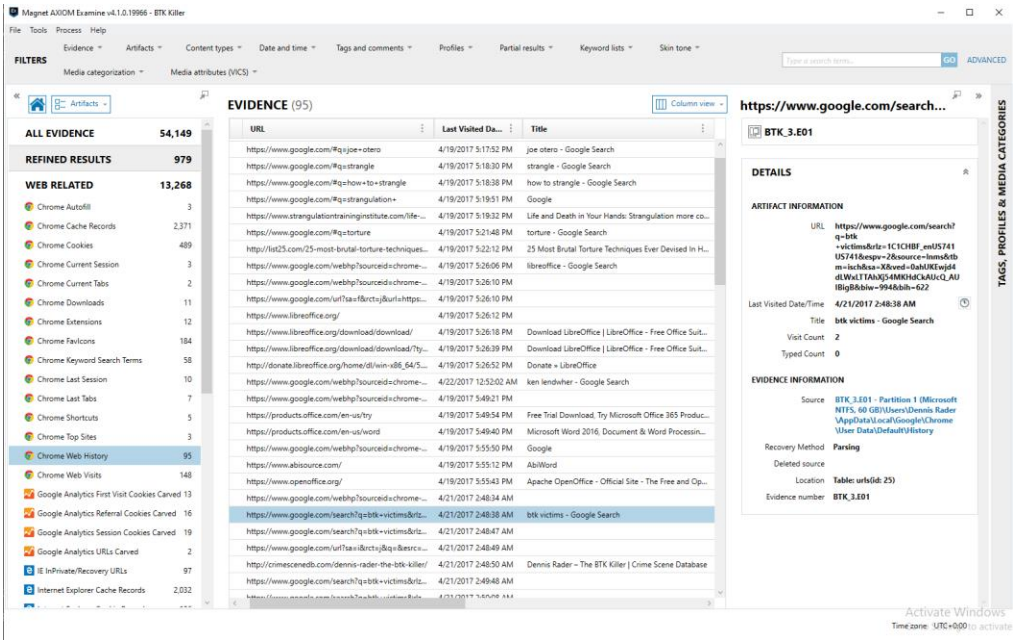


Figure 3.8

Figure 3.8 search for “btk victims”.

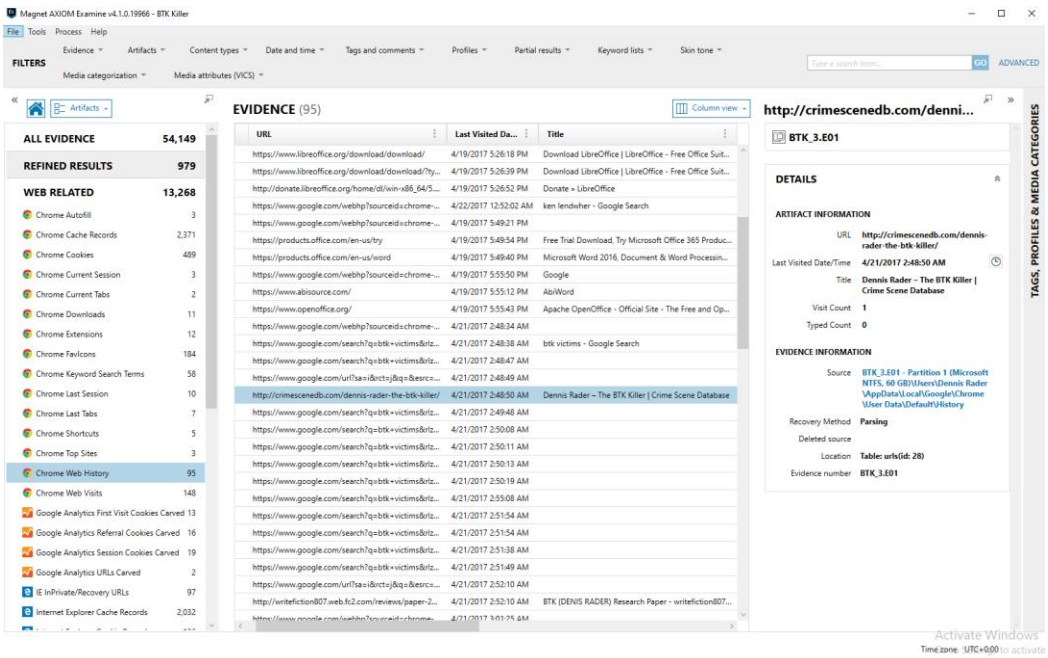


Figure 3.9

Figure 3.9 search for “Dennis Rader crime scene database”.

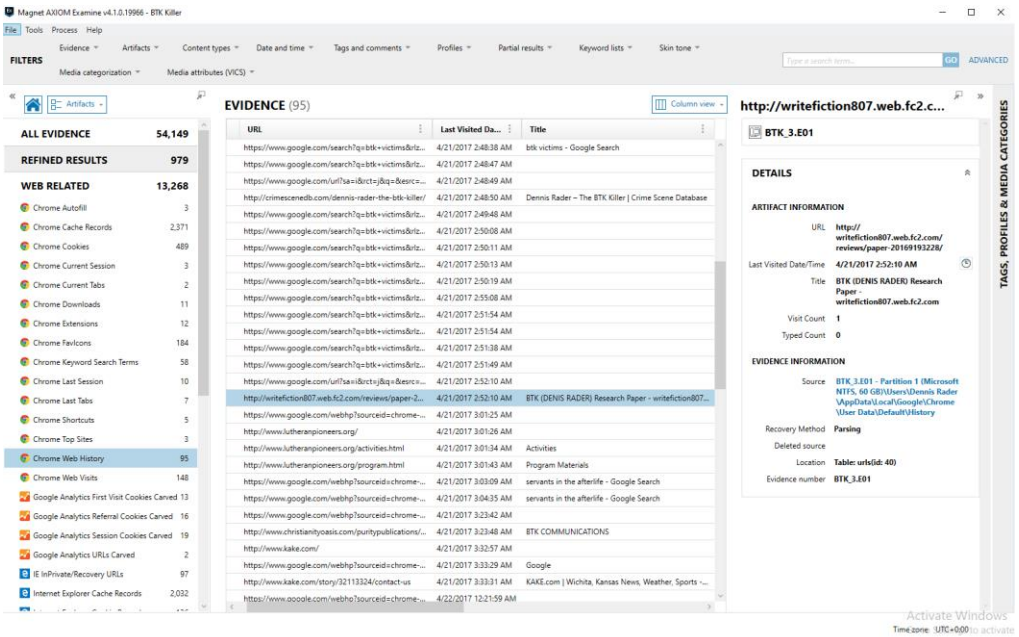


Figure 4.0

Figure 4.0 search for “BTK (DENNIS RADER) Research Paper.”

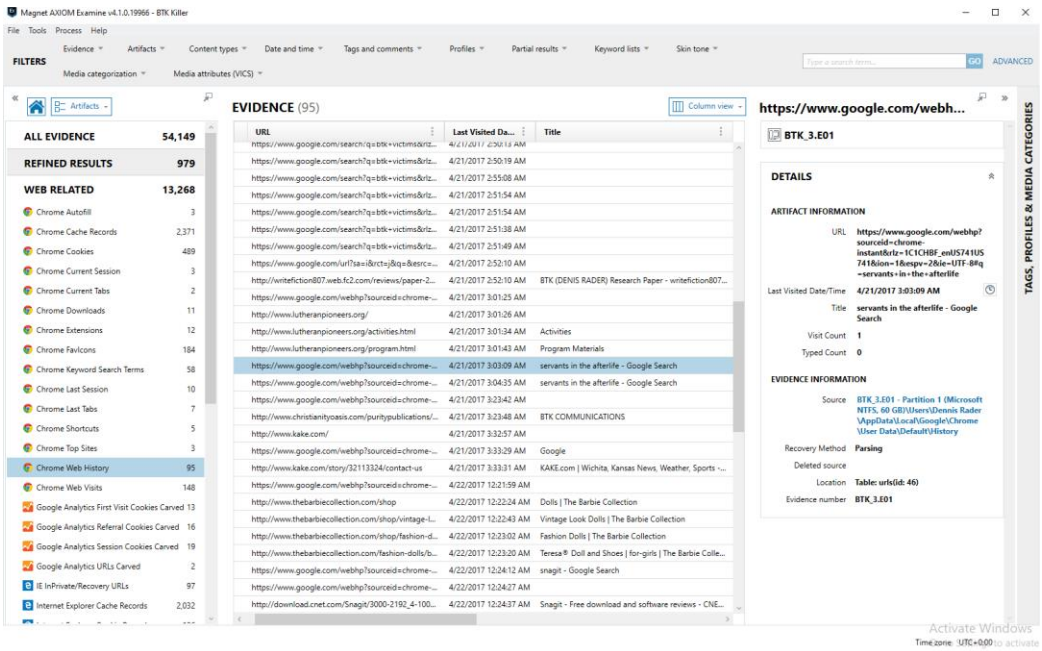


Figure 4.1

Figure 4.1 search for “servants in the afterlife.”

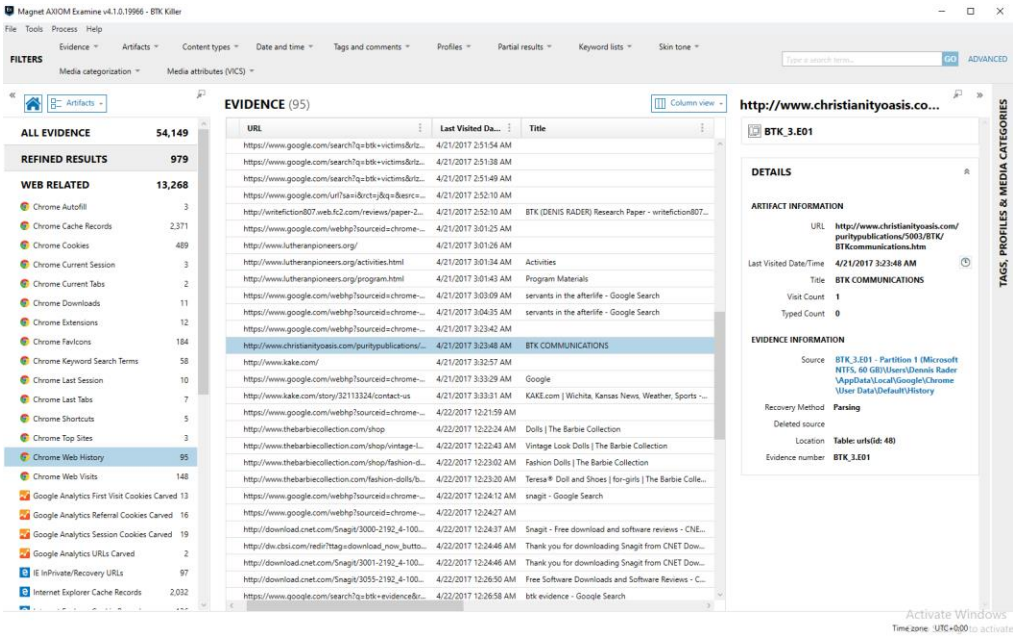


Figure 4.2

Figure 4.2 search for “christianityoasis.com”

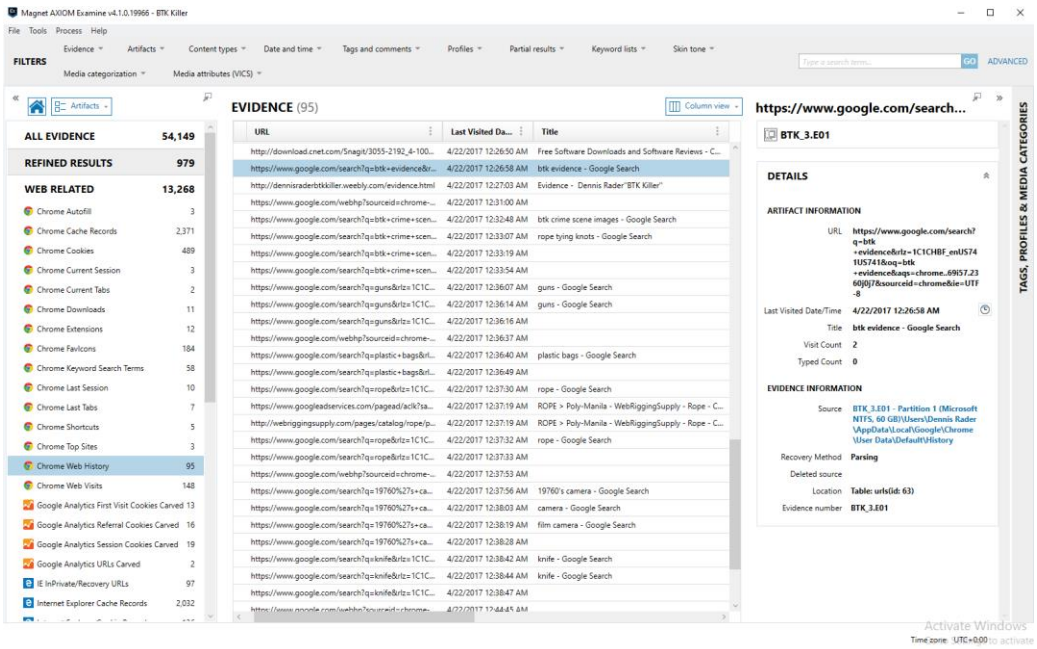


Figure 4.3

Figure 4.3 search for “btk evidence.”

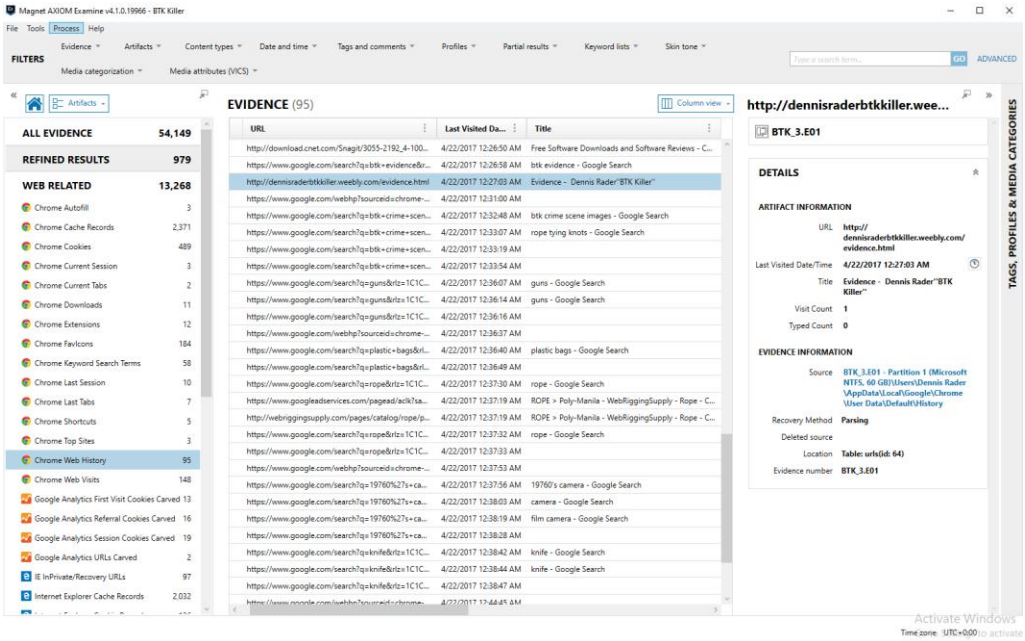


Figure 4.4

Figure 4.4 search for evidence on BTK killer.

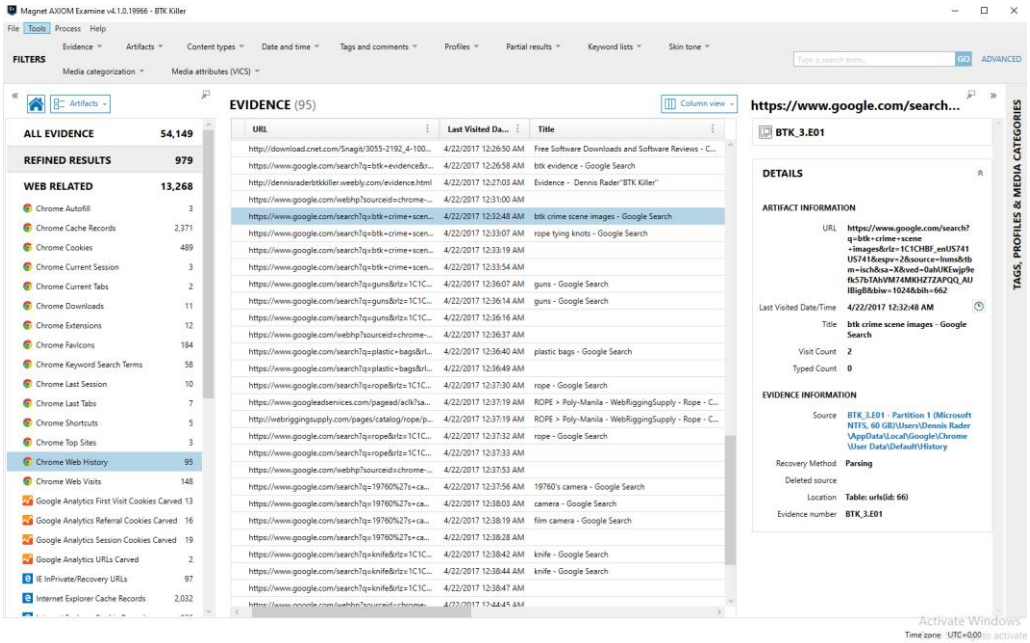


Figure 4.5

Figure 4.5 search for “btk crime scene images.”

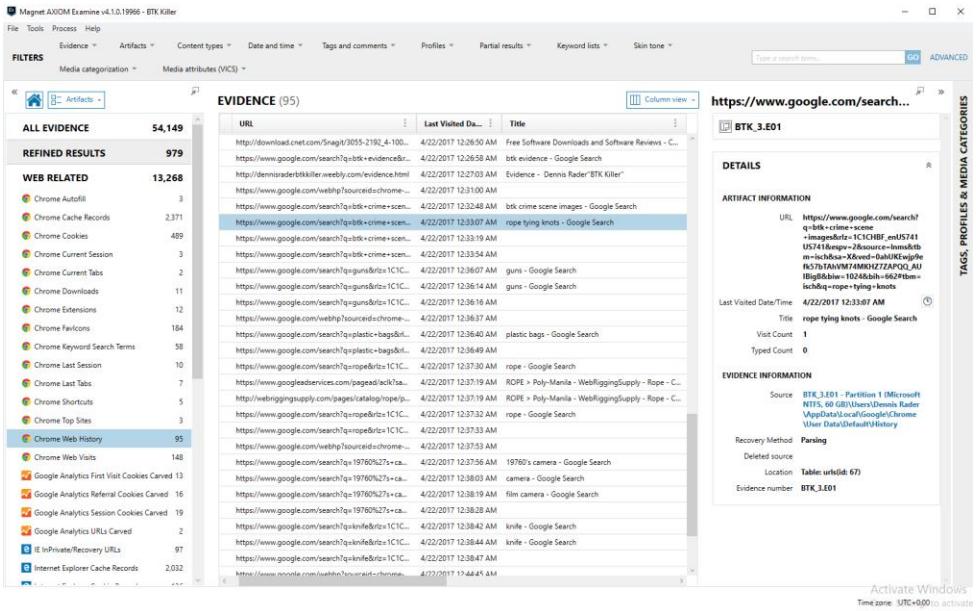


Figure 4.6

Figure 4.6 search for “rope tying knots.”

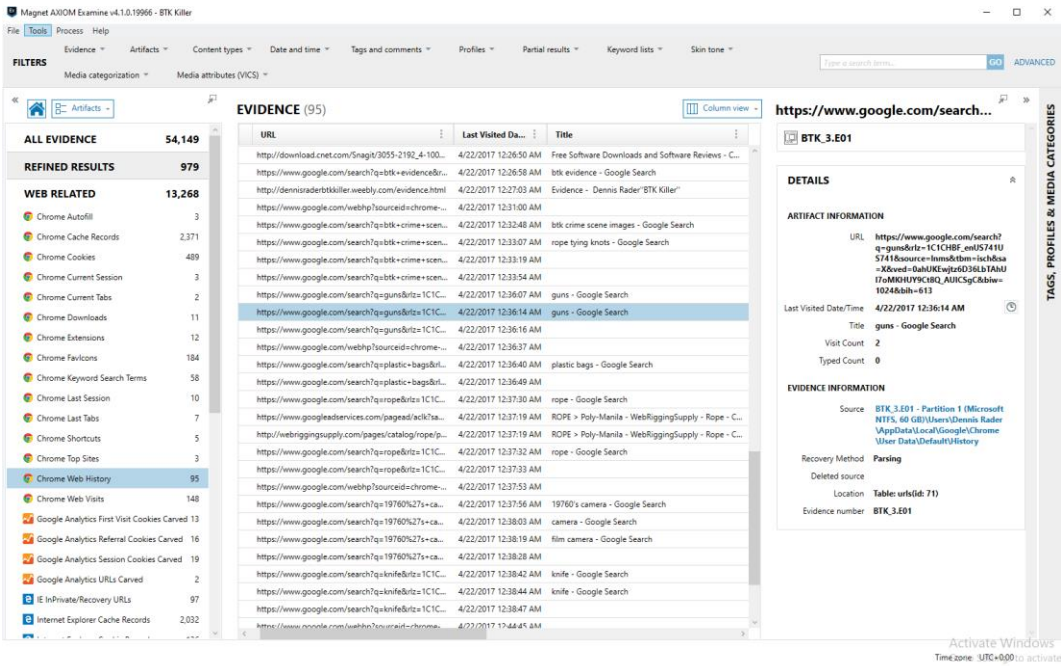


Figure 4.7

Figure 4.7 search for “guns.”

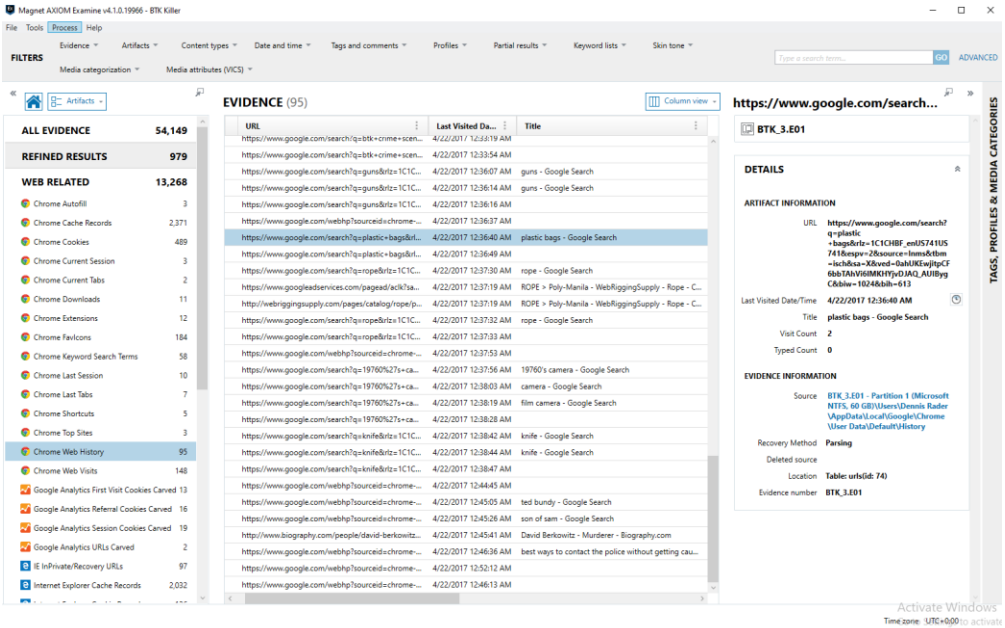


Figure 4.8

Figure 4.8 search for “plastic bags.”

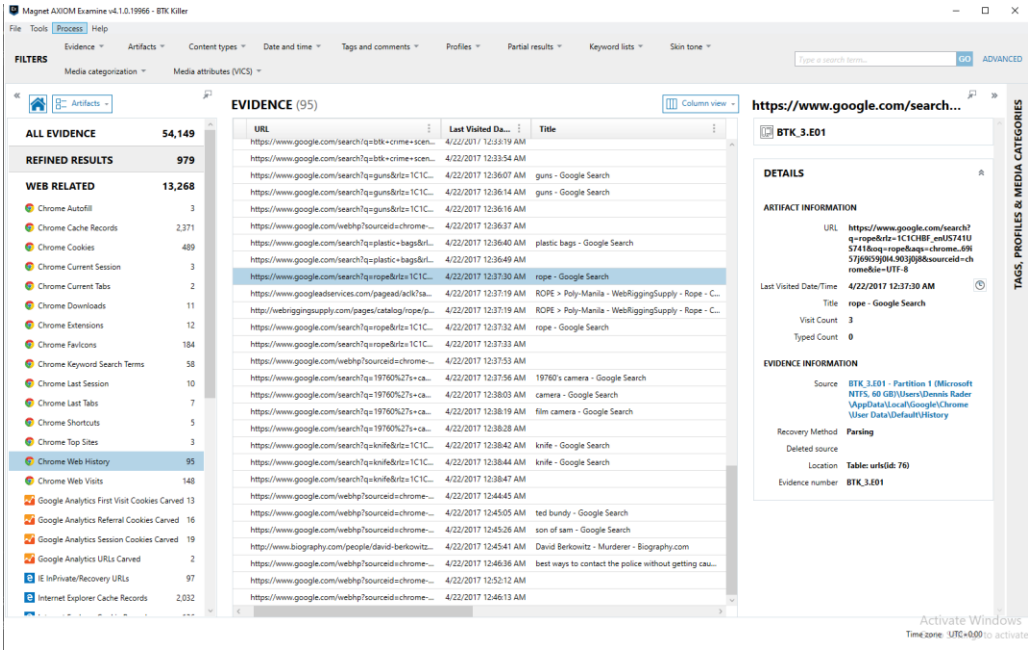


Figure 4.9

Figure 4.9 search for “rope.”

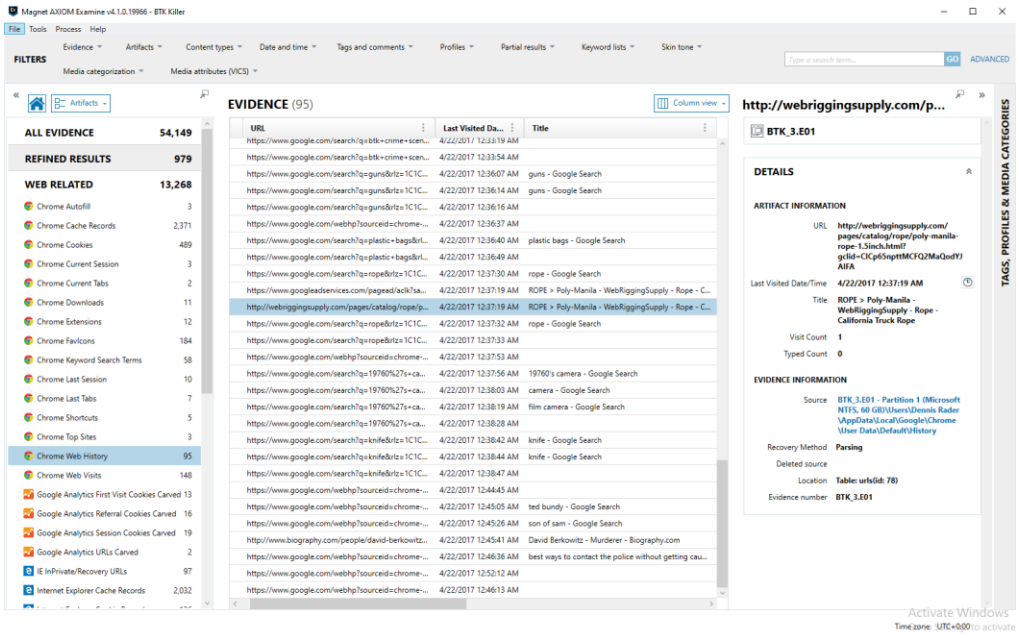


Figure 5.0

Figure 5.0 search for “rope” again.

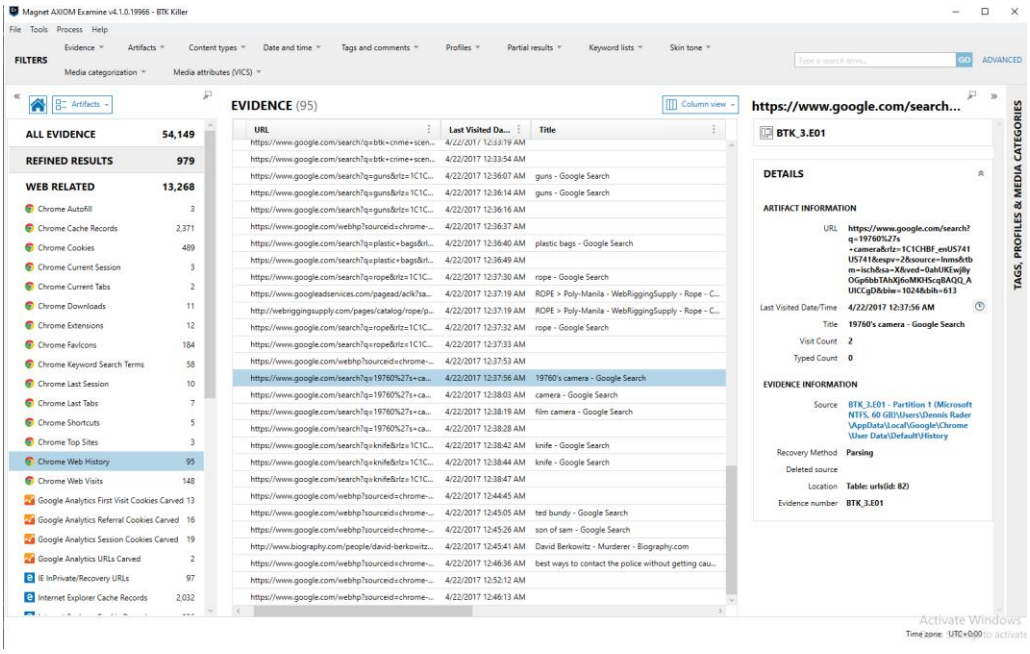


Figure 5.1

Figure 5.1 search for “19760’s camera.”

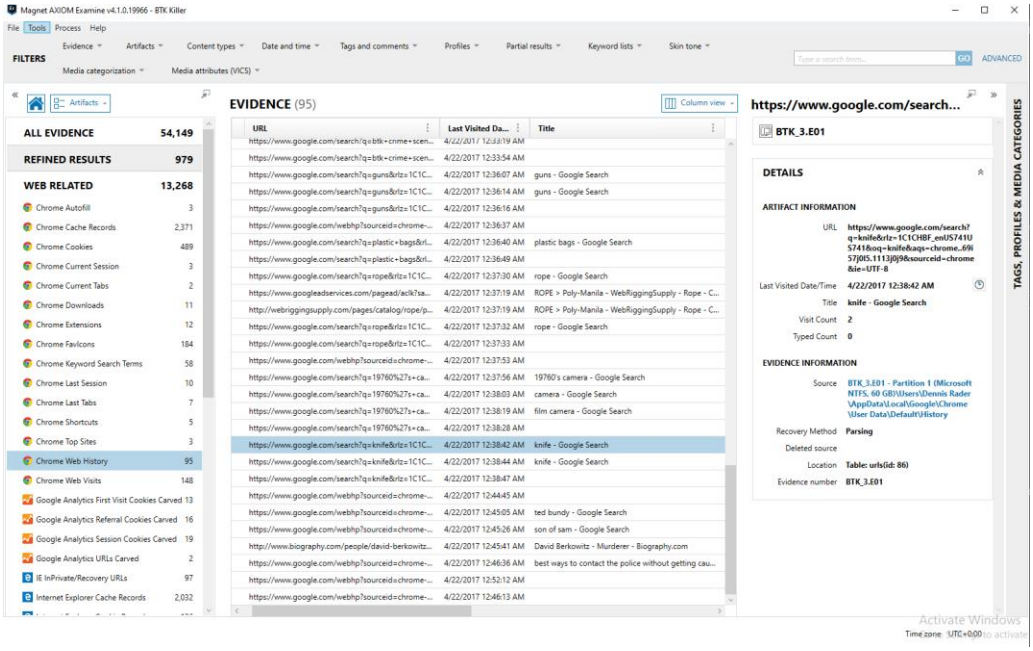


Figure 5.2

Figure 5.2 search for “knife.”

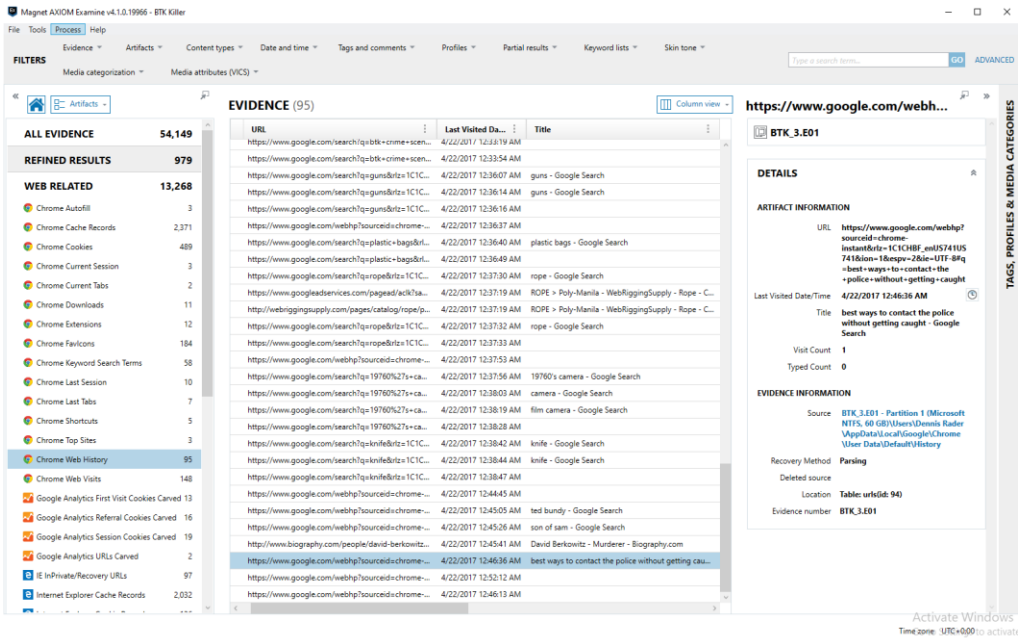


Figure 5.3

Figure 5.3 search for “best ways to contact the police without getting caught.”

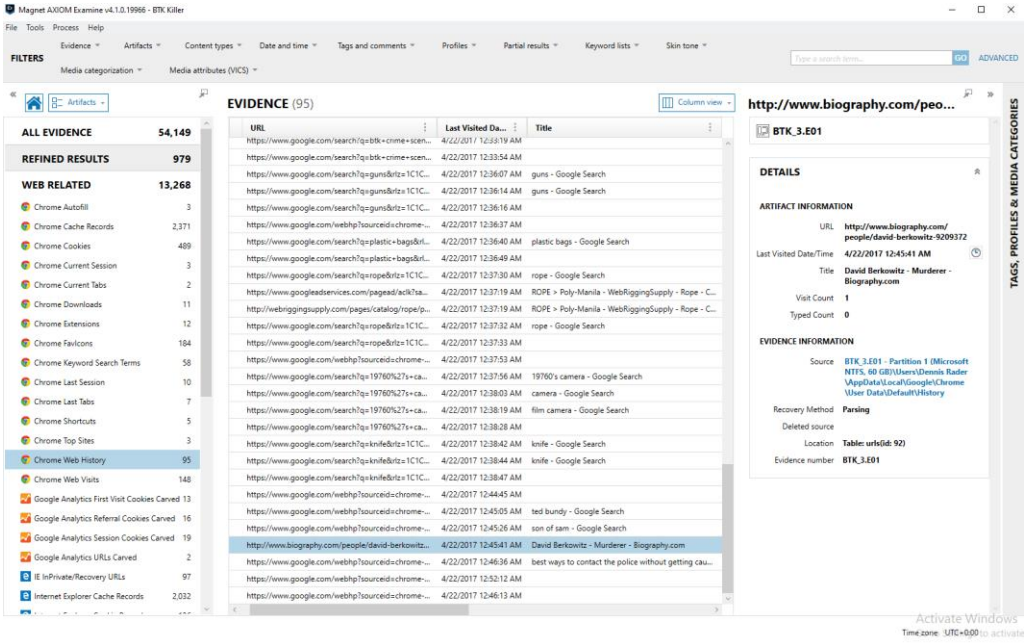


Figure 5.4

Figure 5.4 search for “David Berkowitz – Murderer – Biography.com”

Daily History

This is the daily history and the lab tabs opened on the suspect serial killer BTK's laptop. Figures 5.5-6.2 show this information.

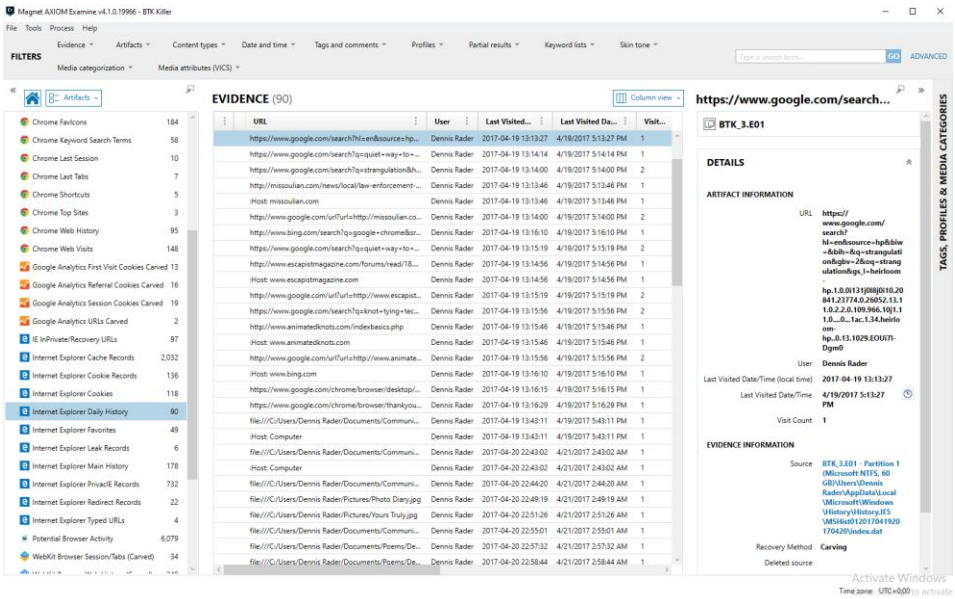


Figure 5.5

Figure 5.5 shows a search result for "strangulation."

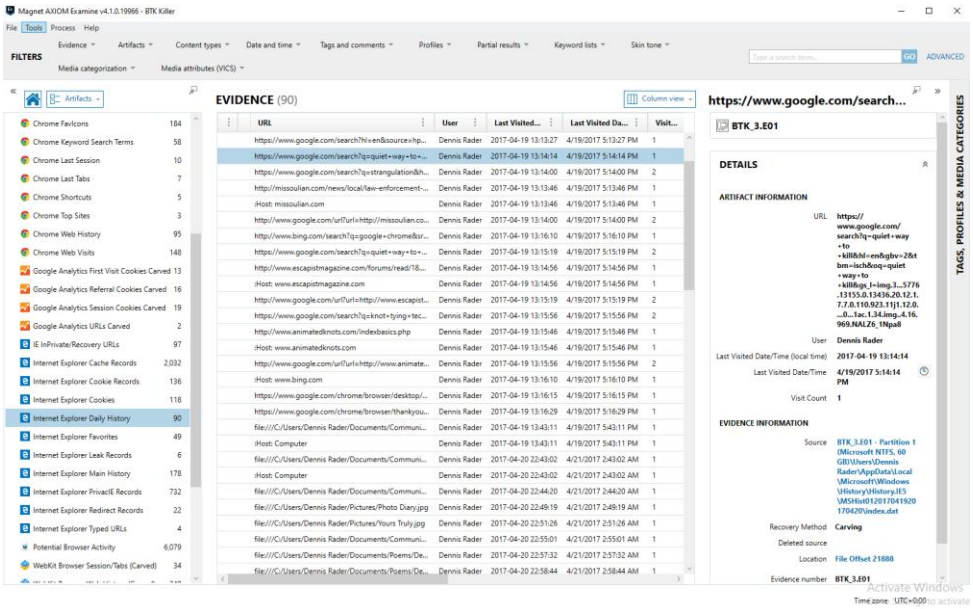


Figure 5.6

Figure 5.6 search for how to quietly kill.

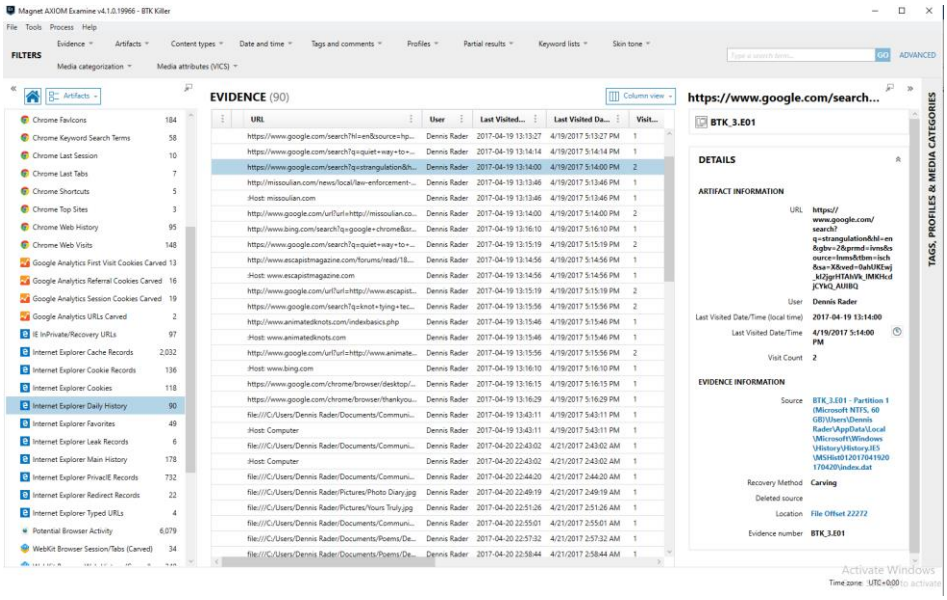


Figure 5.7

Figure 5.7 search for strangulation.

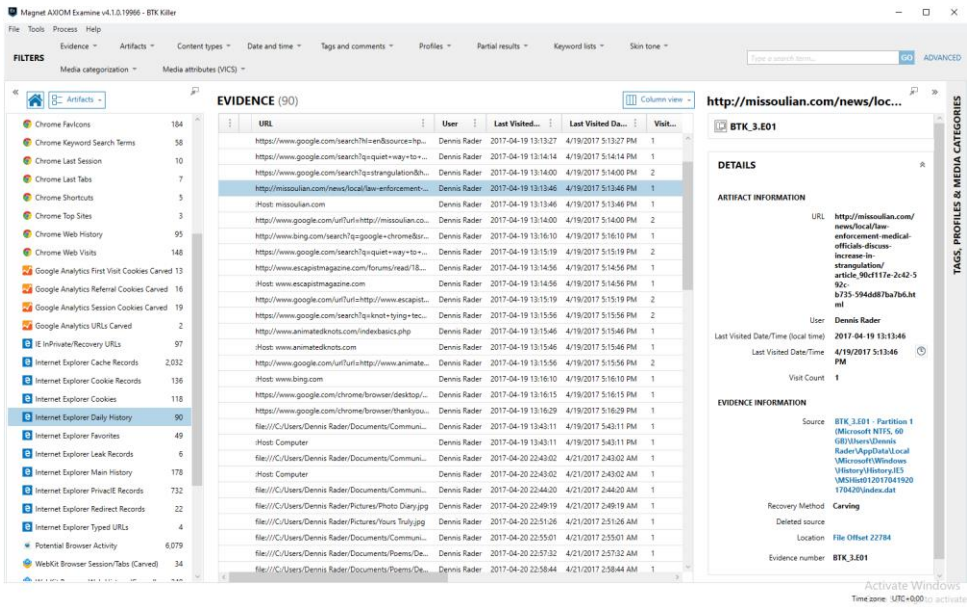


Figure 5.8

Figure 5.8 search for law enforcement in strangulation.

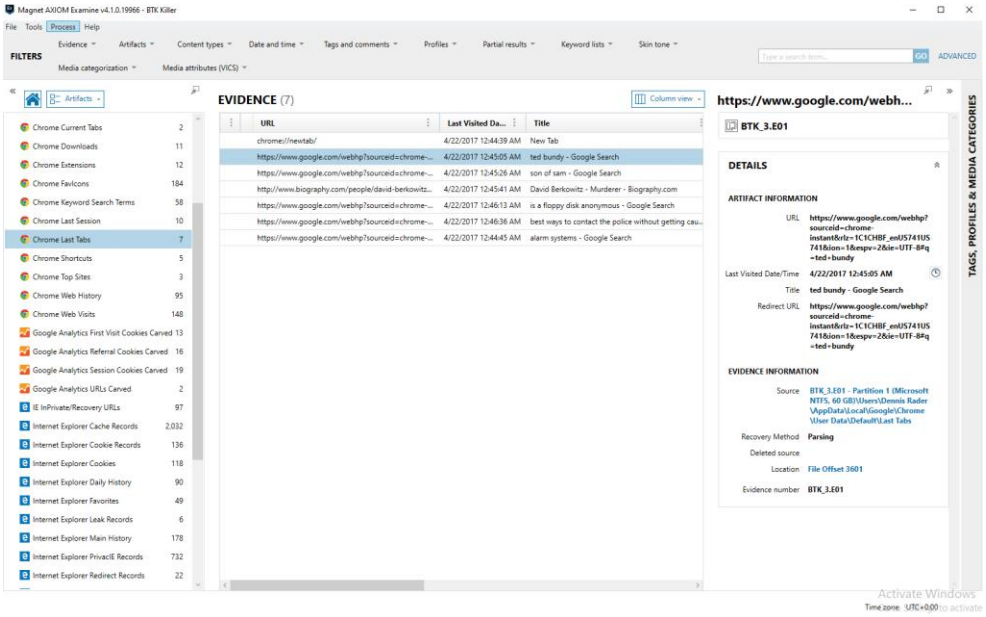


Figure 5.9

Figure 5.9 search for ted bundy.

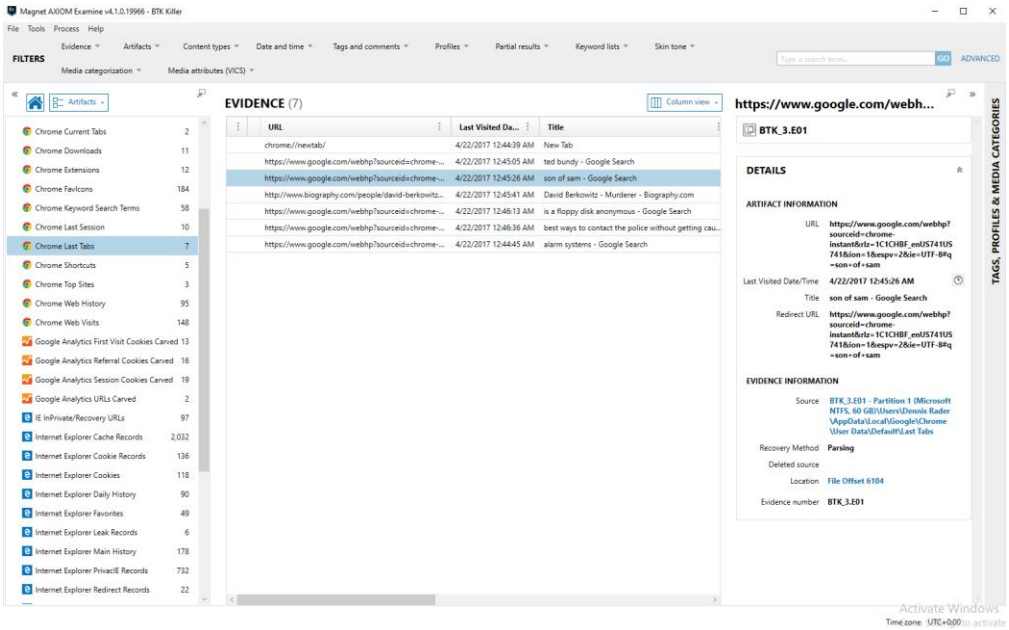


Figure 5.9

Figure 5.9 search for son of sam.

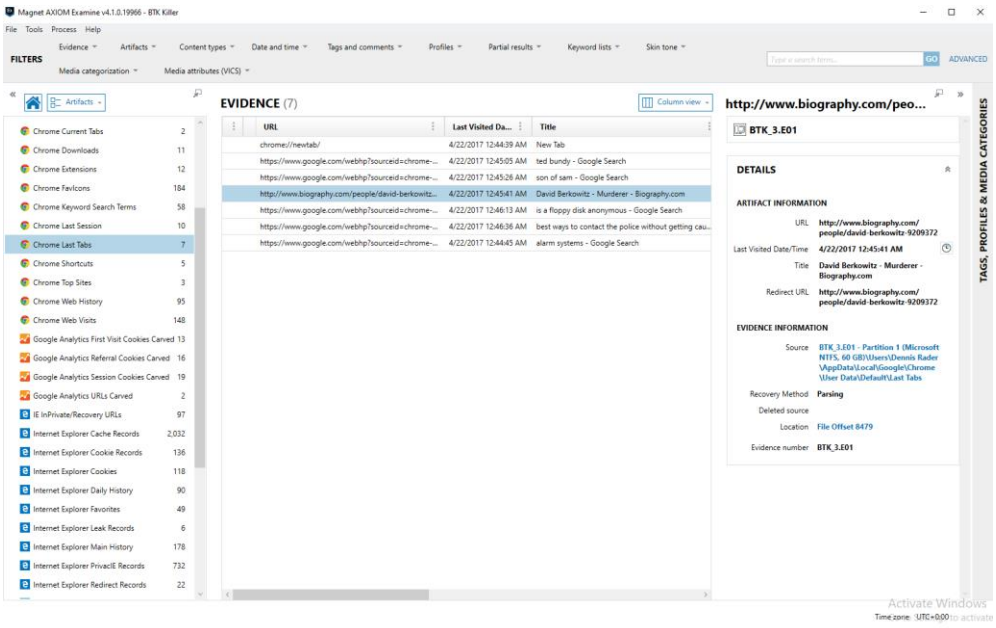


Figure 6.0

Figure 6.0 search for David Berkowitz again.

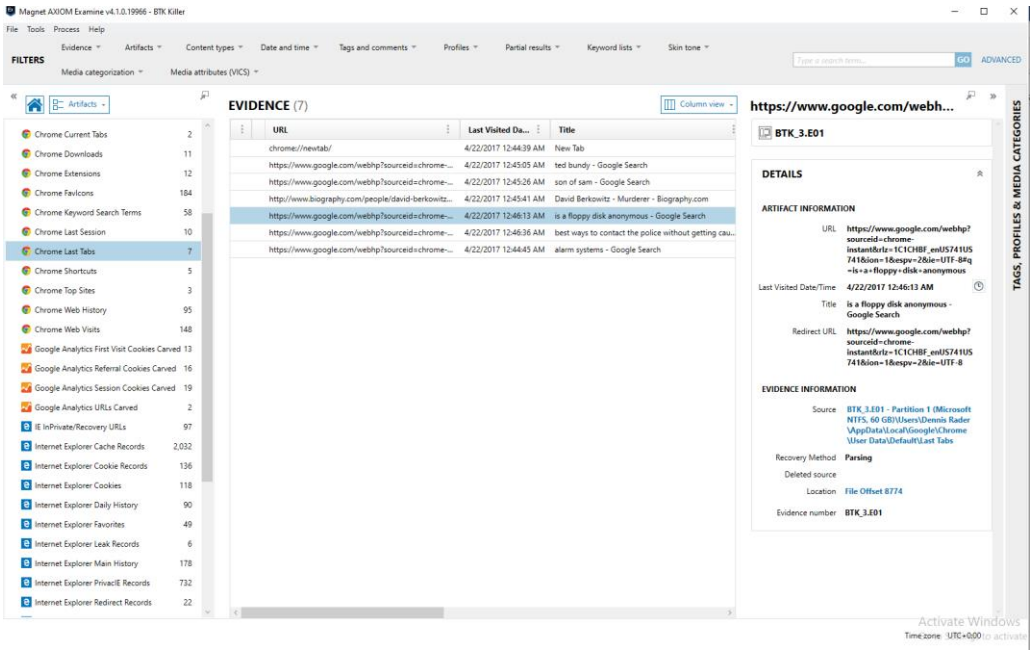


Figure 6.1

Figure 6.1 search for “is a floppy disk anonymous.”

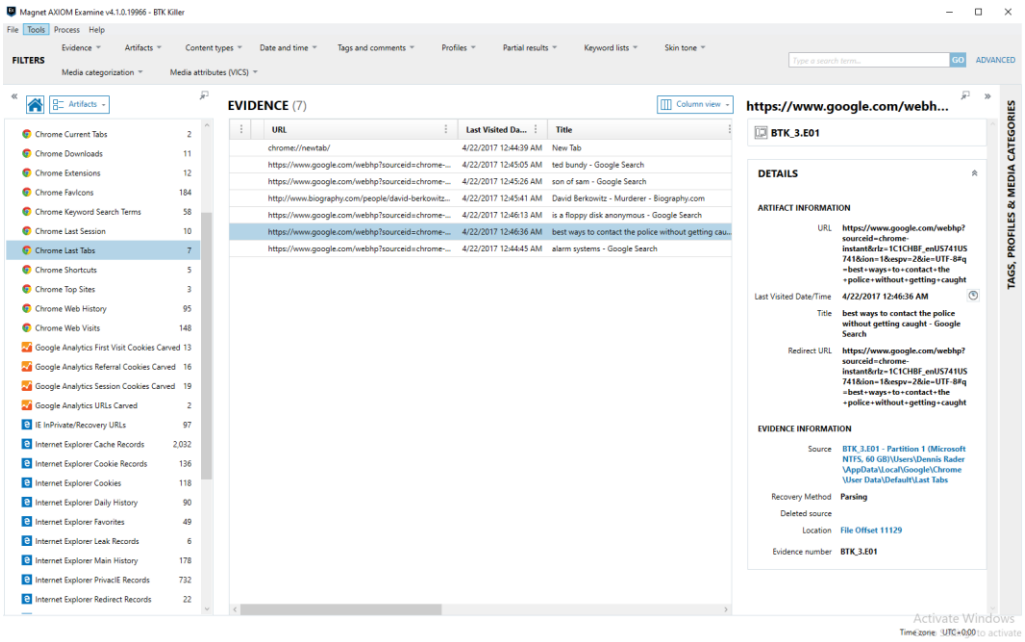


Figure 6.2

Figure 6.2 search for “best ways to contact the police without getting caught.” Again.

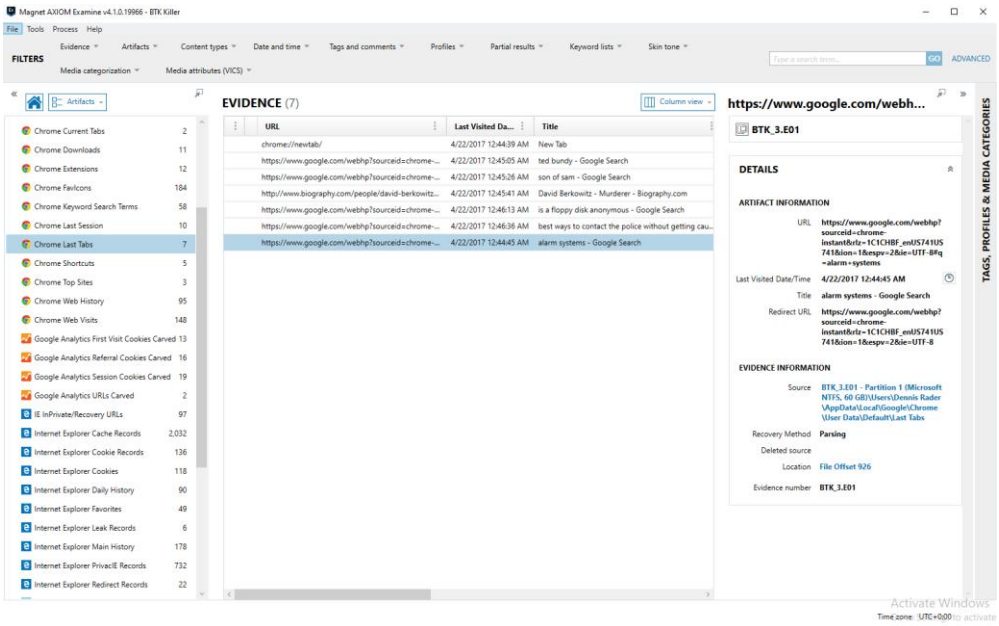


Figure 6.3

Figure 6.3 search for “alarm systems.”

Media

Photos.

All the following pictures that I have found relate to the web search history results. These photos contain images of: ropes, strangulation, weapons, dead bodies, BTK killer related images such as photos of victims before and after events took place. Figures 6.4-13.1

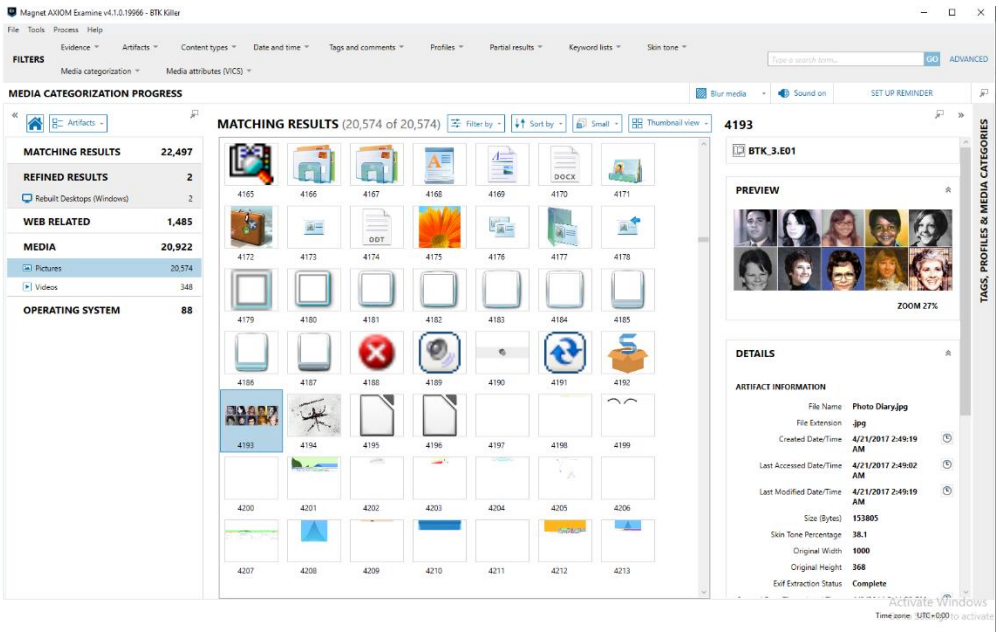


Figure 6.5

Figure 6.5 picture of list of victims.

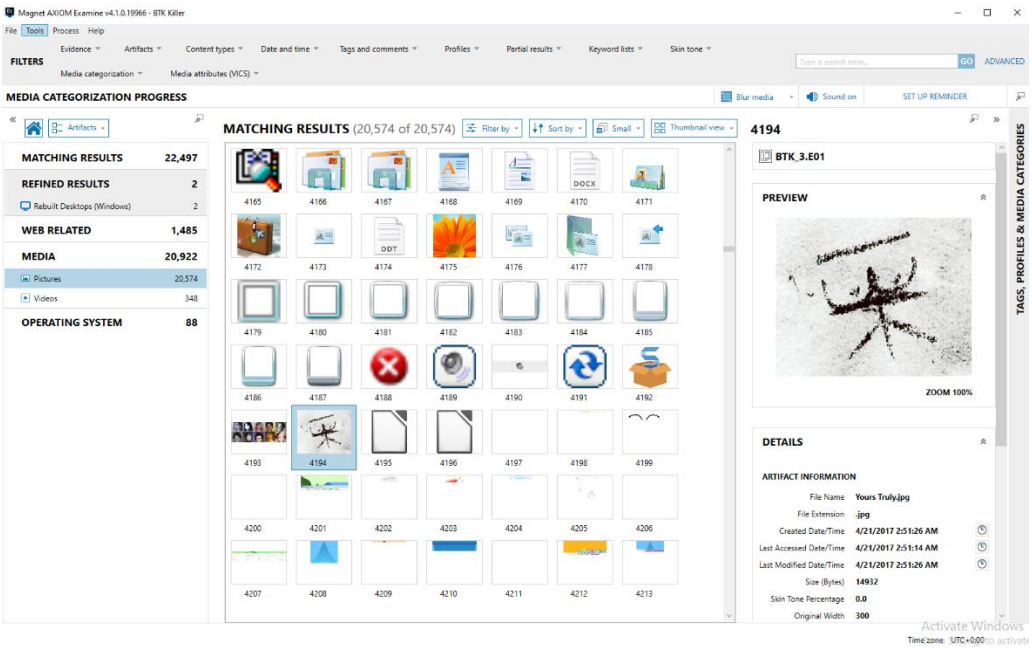


Figure 6.5

Figure 6.5 picture of his signature.

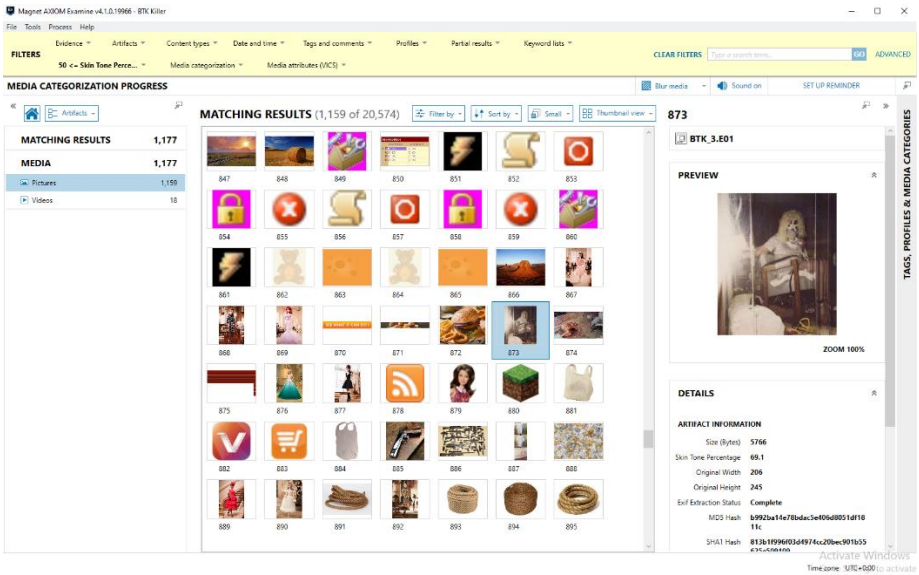


Figure 6.6

Figure 6.6 picture of weird mask person.

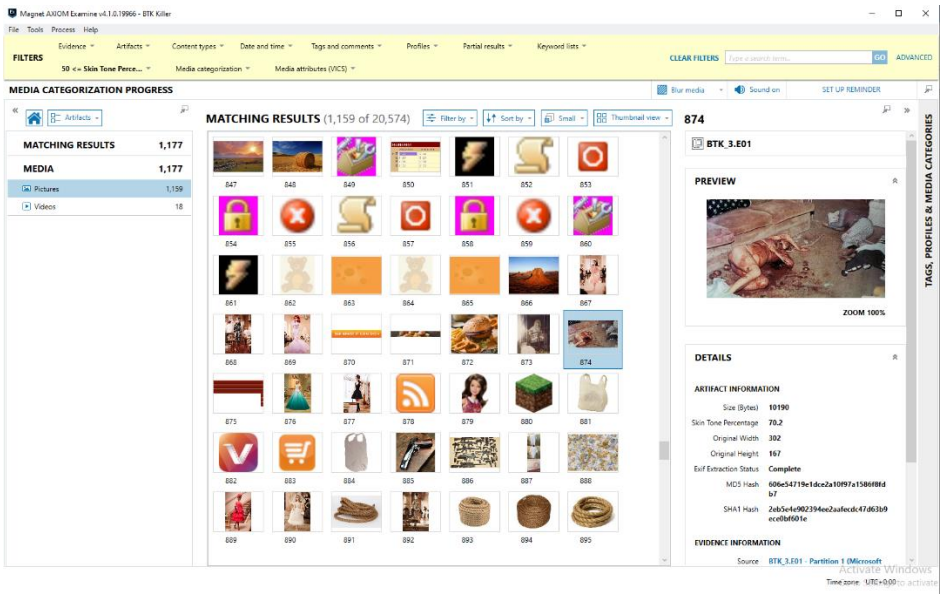


Figure 6.7

Figure 6.7 picture of a crime scene victim.

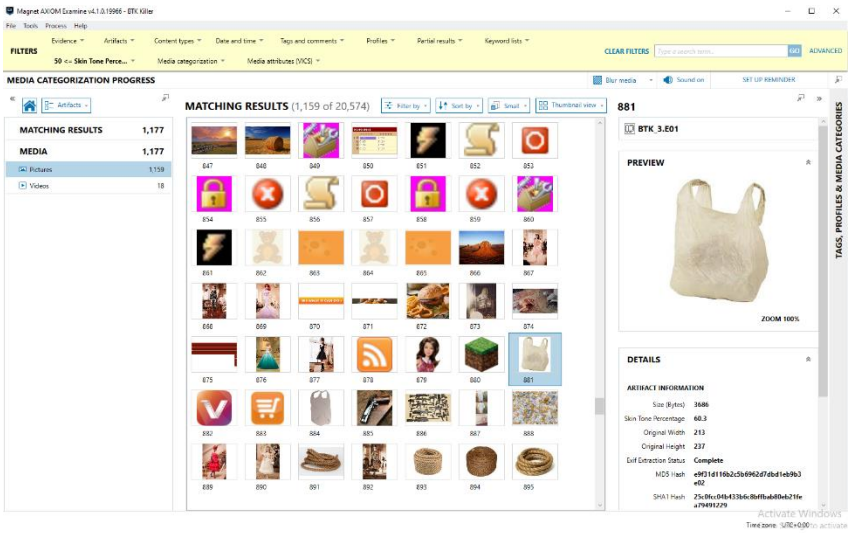


Figure 6.8

Figure 6.8 picture of a plastic bag.

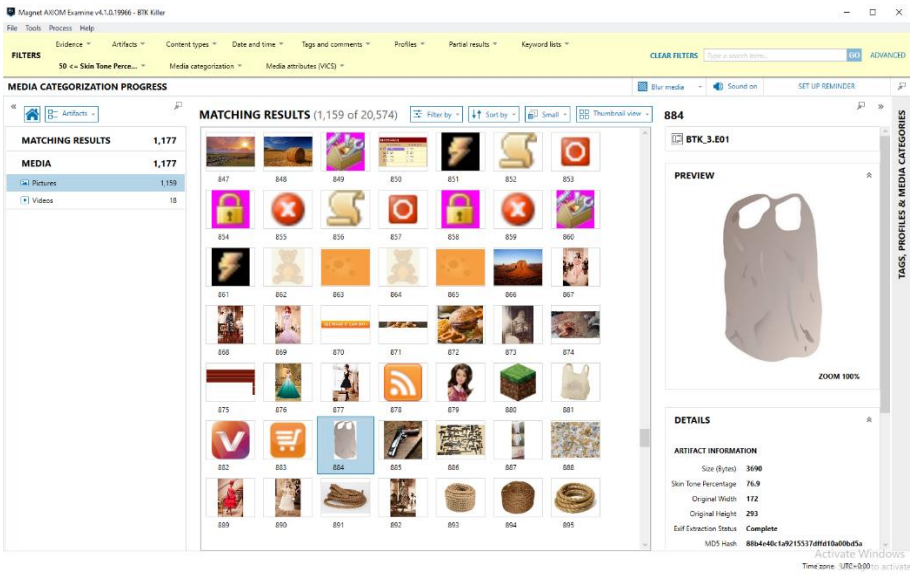


Figure 6.9

Figure 6.9

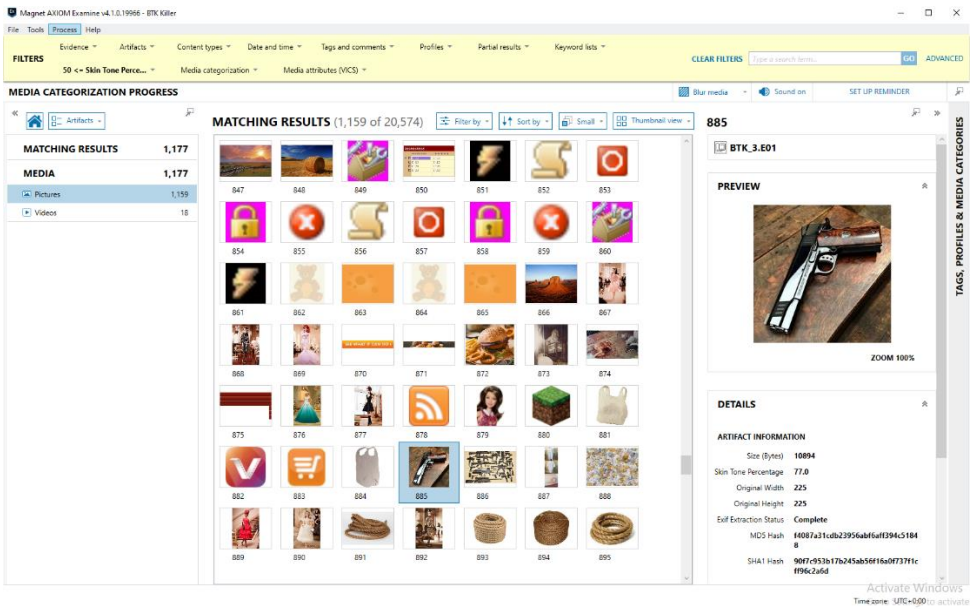


Figure 7.0

Figure 7.0 picture of a gun.

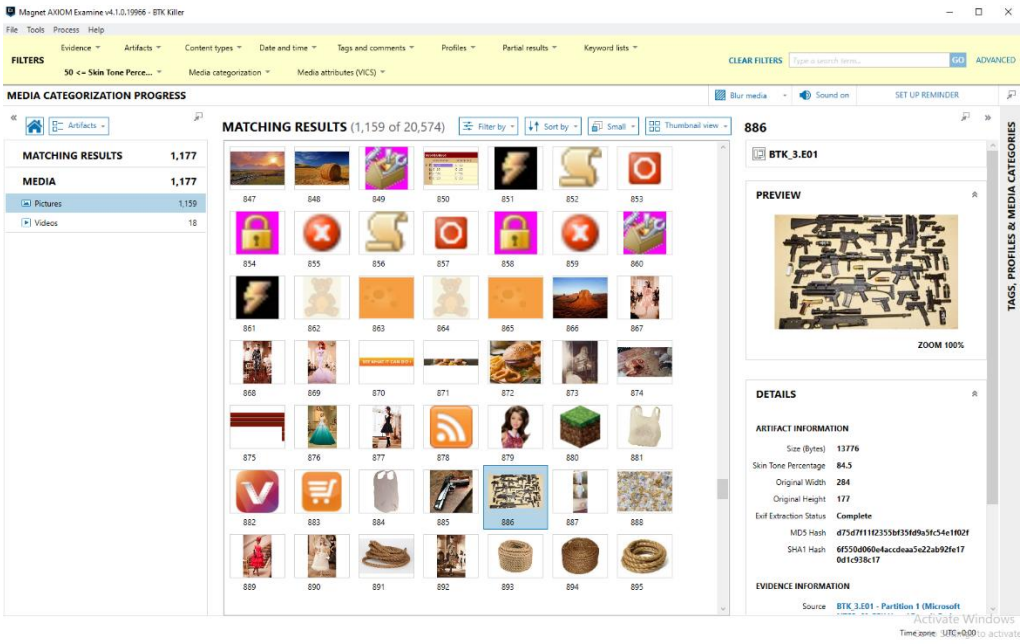


Figure 7.1

Figure 7.1

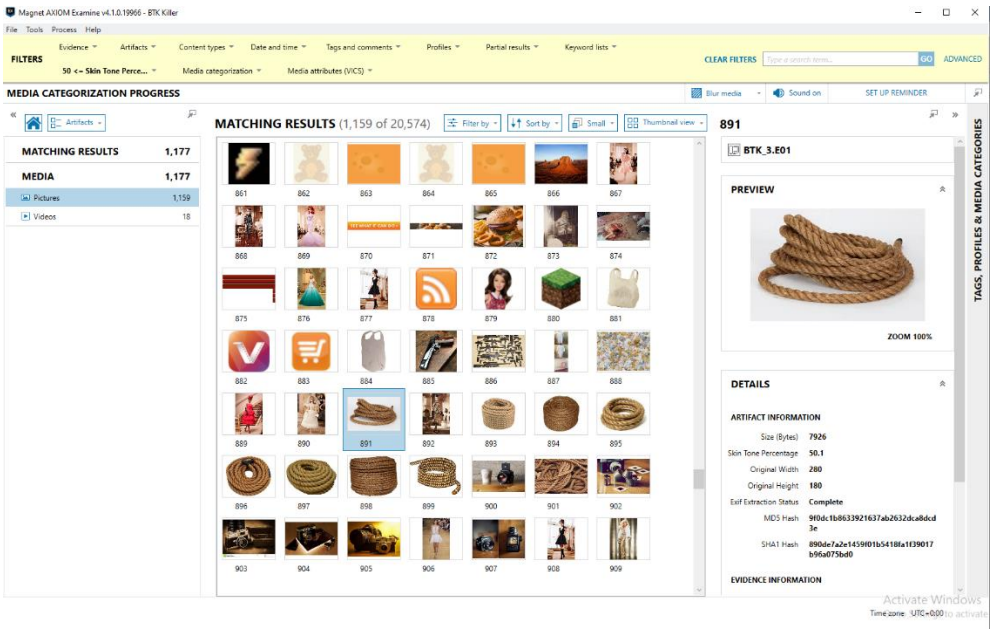


Figure 7.2

Figure 7.2 multiple pictures of rope.

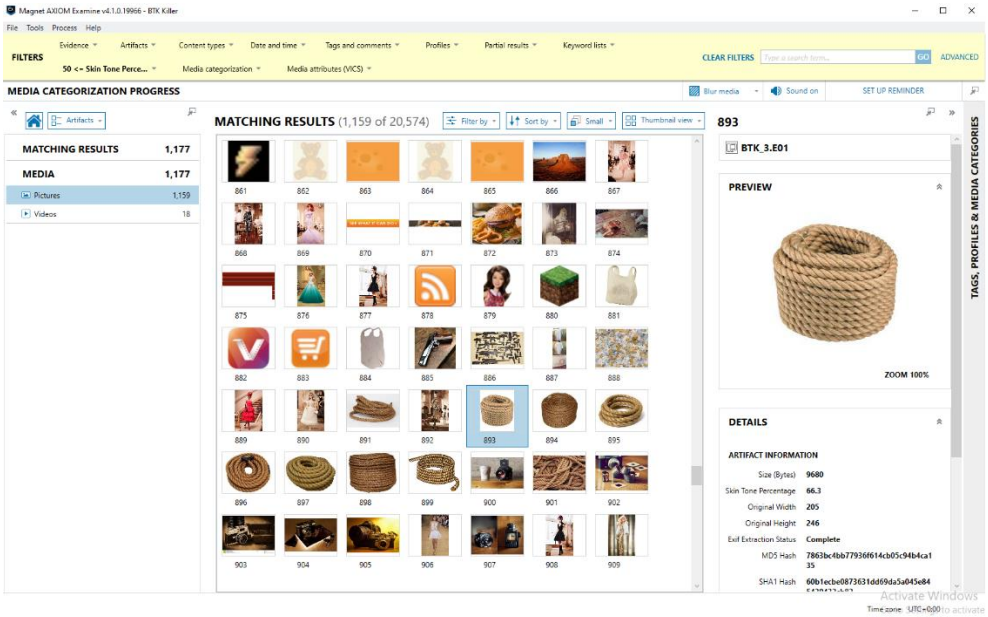


Figure 7.3

Figure 7.3

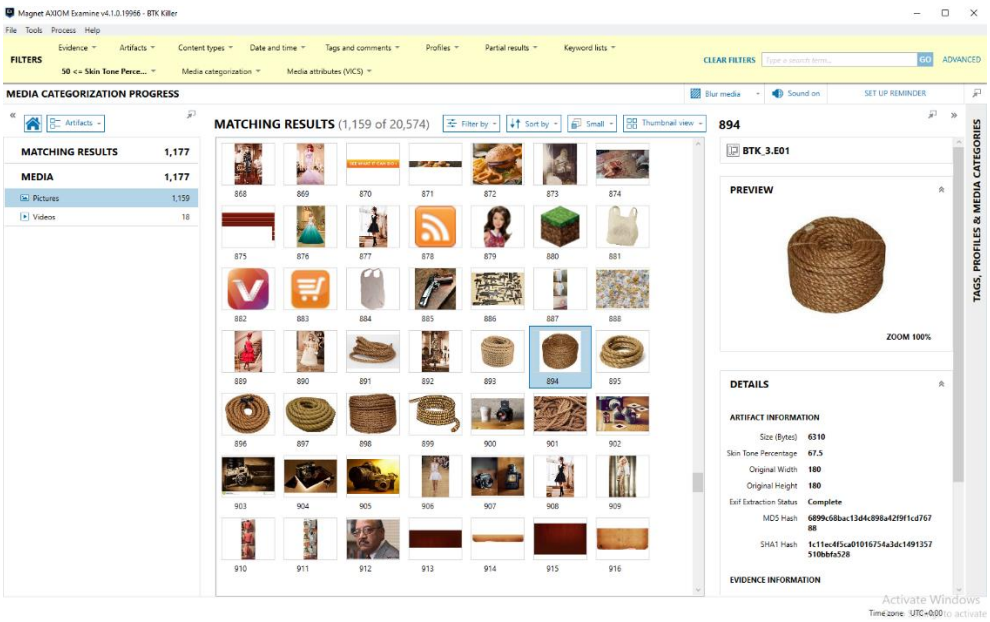


Figure 7.4

Figure 7.4

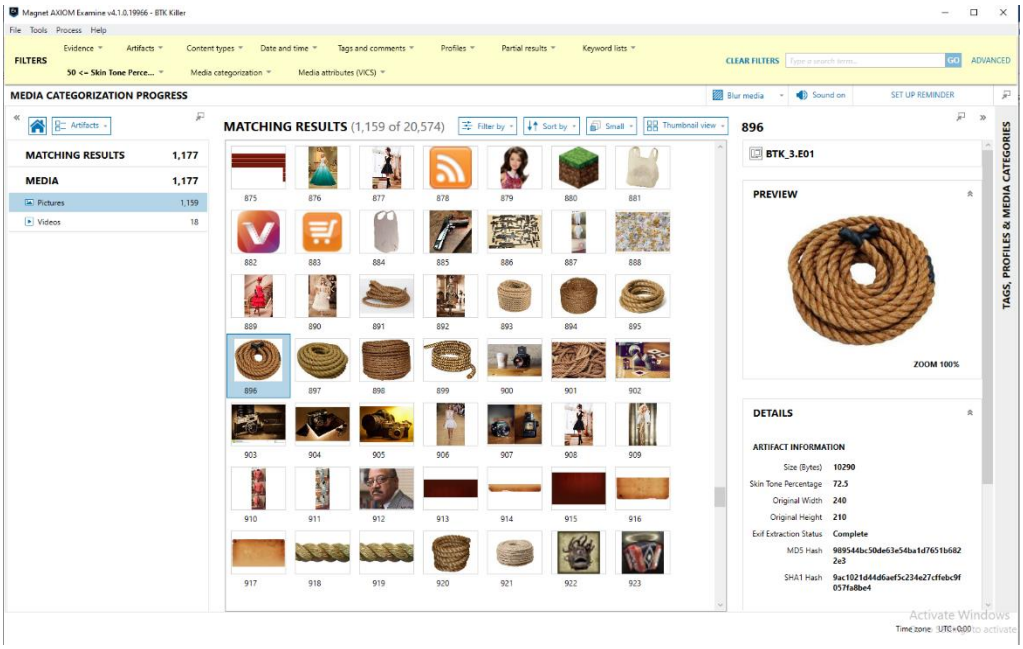


Figure 7.5

Figure 7.5

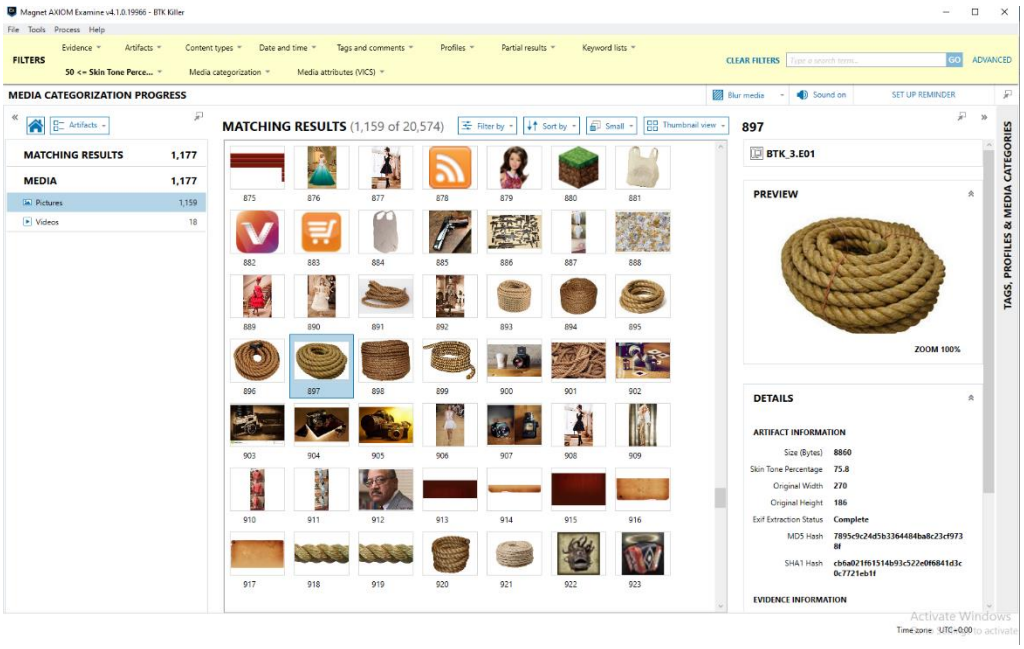


Figure 7.6

Figure 7.6

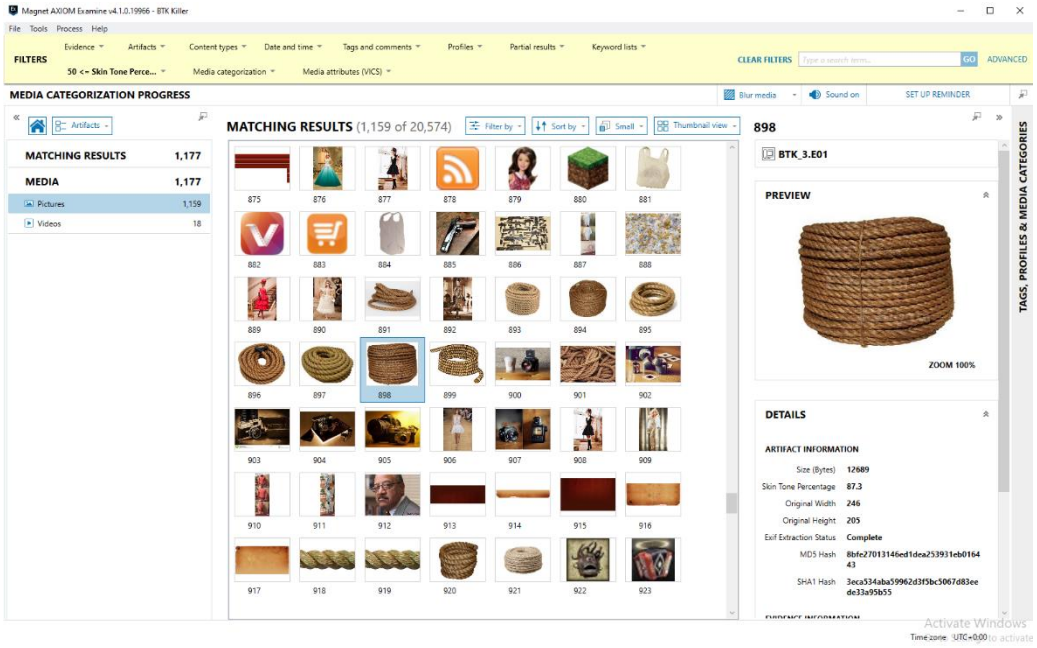


Figure 7.7

Figure 7.7

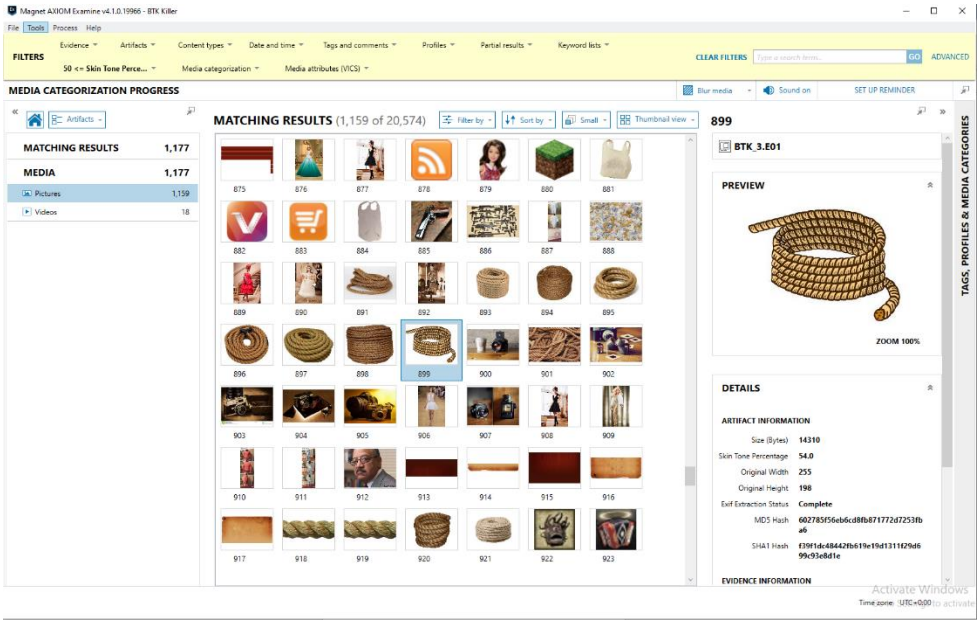


Figure 7.8

Figure 7.8

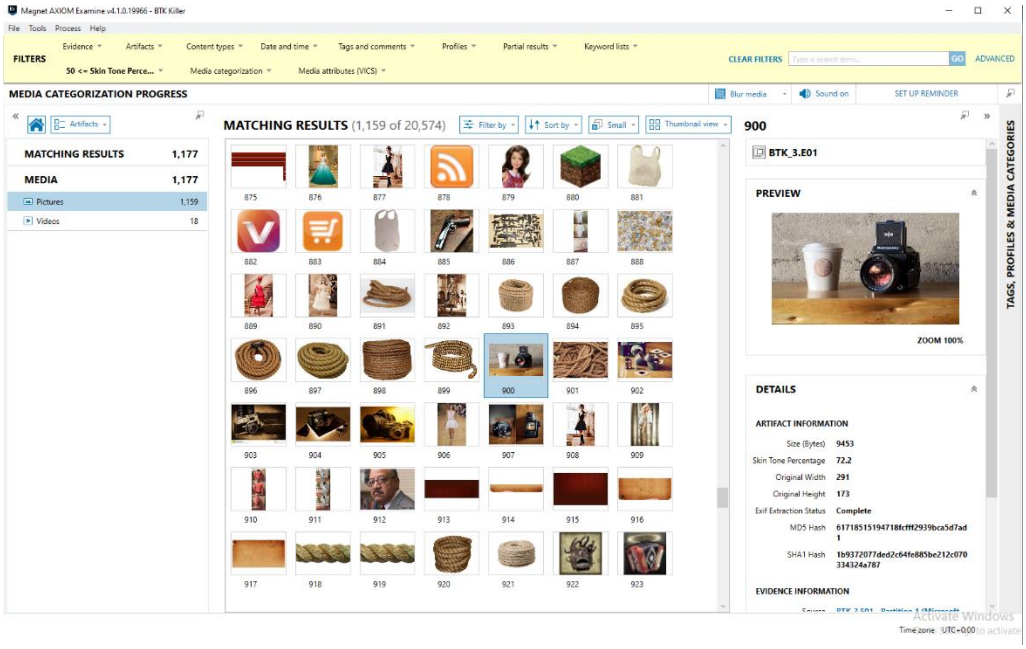


Figure 7.9

Figure 7.9 multiple pictures of camera he used.

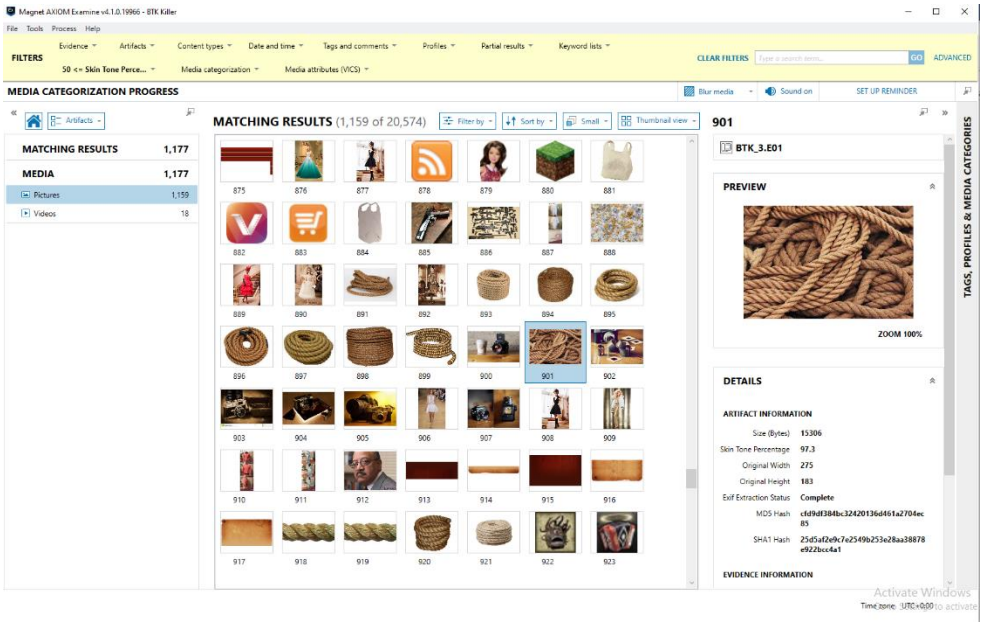


Figure 8.0

Figure 8.0

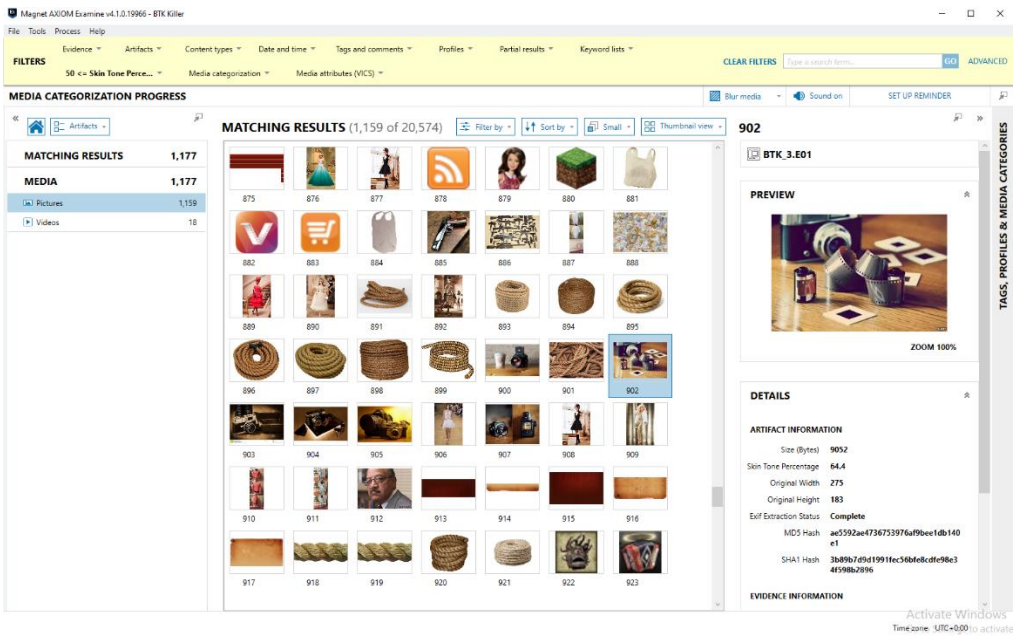


Figure 8.1

Figure 8.1

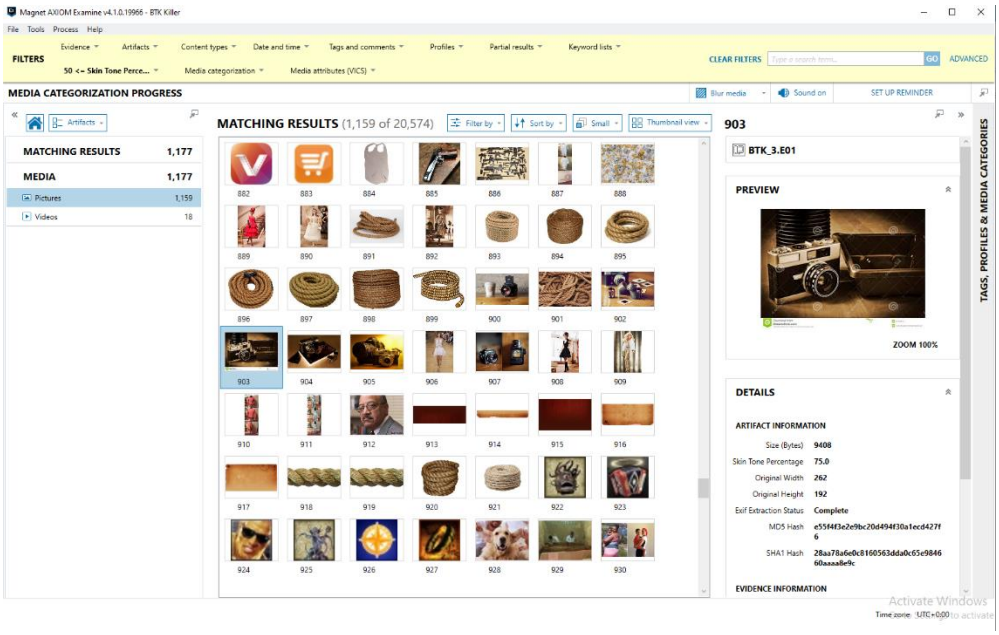


Figure 8.2

Figure 8.2

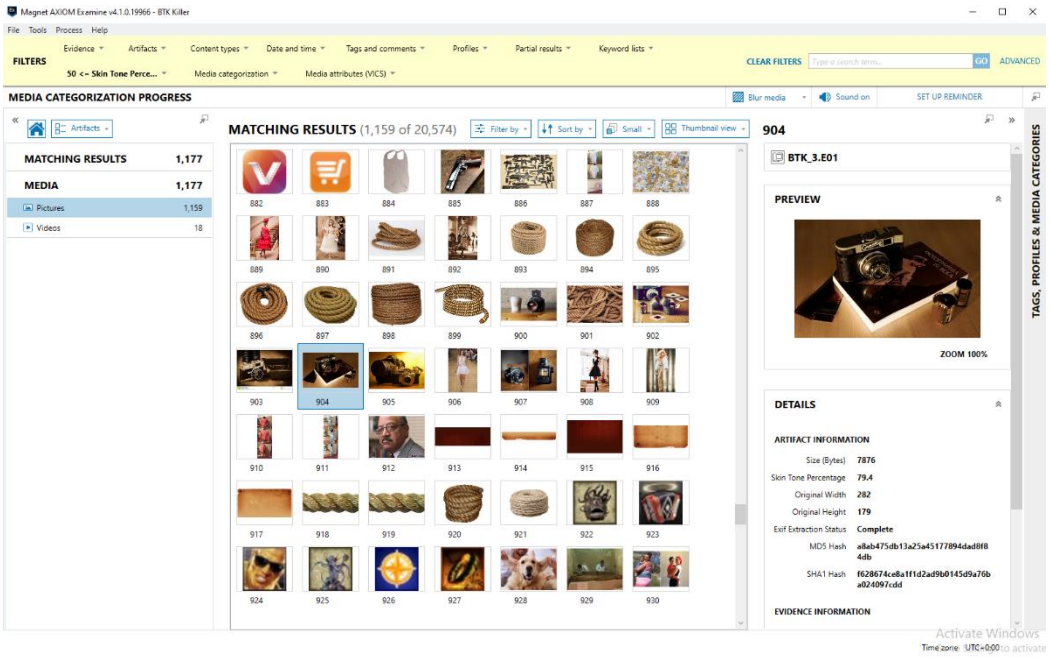


Figure 8.3

Figure 8.3

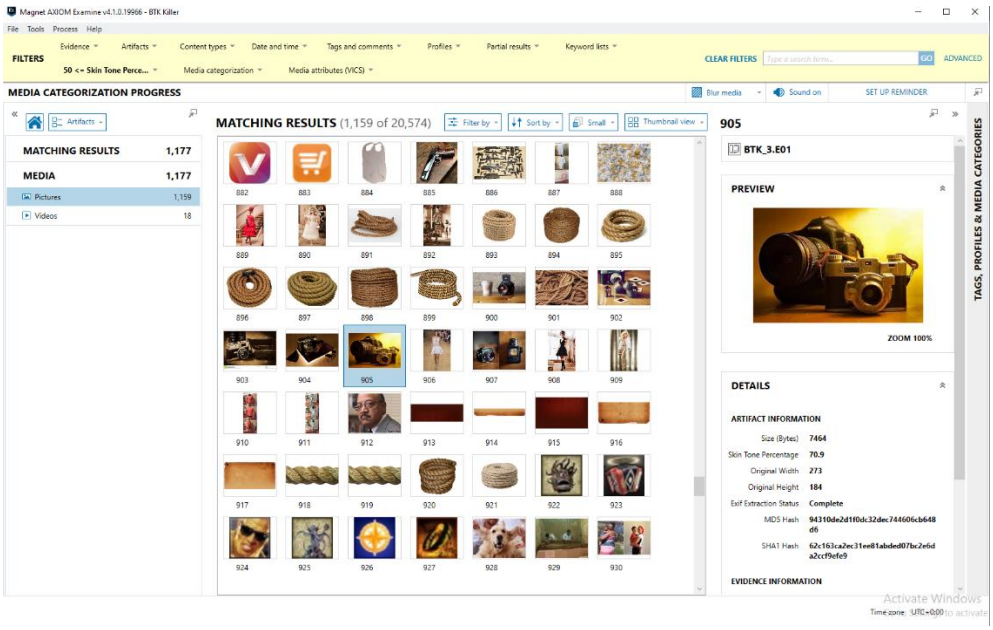


Figure 8.4

Figure 8.4

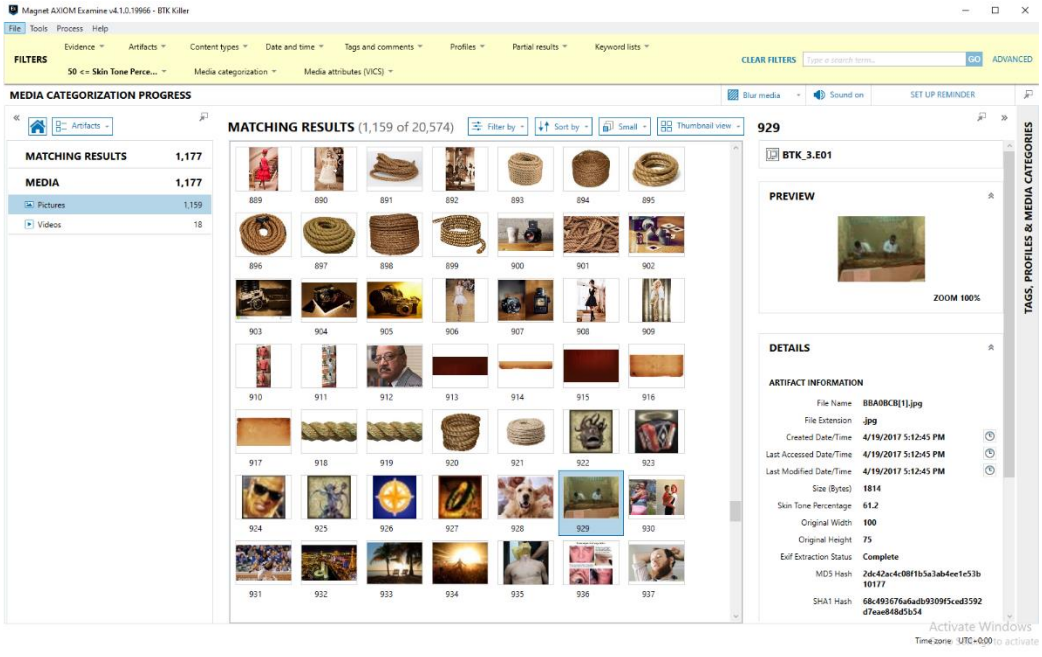


Figure 8.5

Figure 8.5 photo of victims.

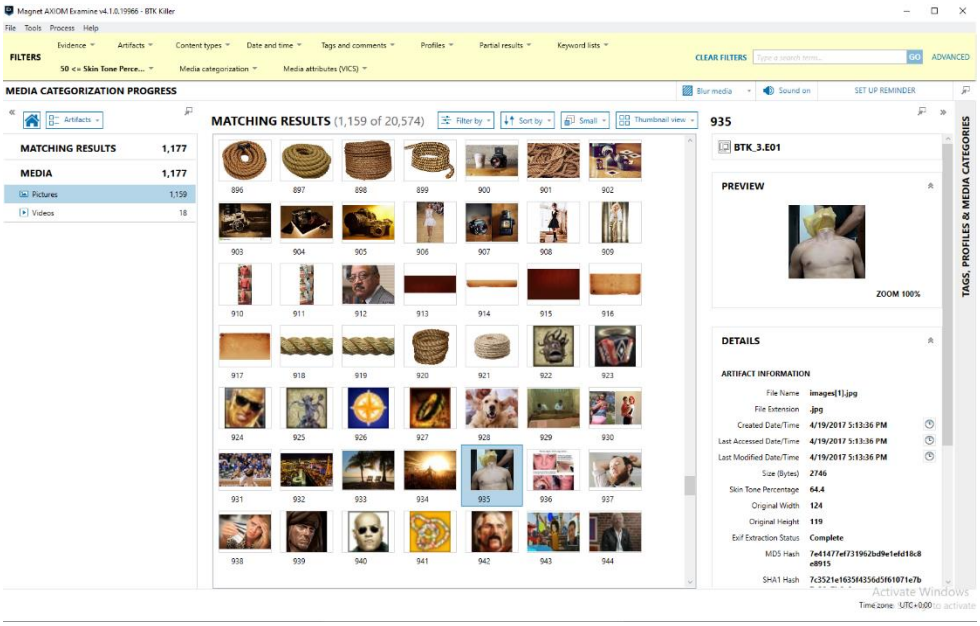


Figure 8.6

Figure 8.6 photo of victim with plastic bag on the head.

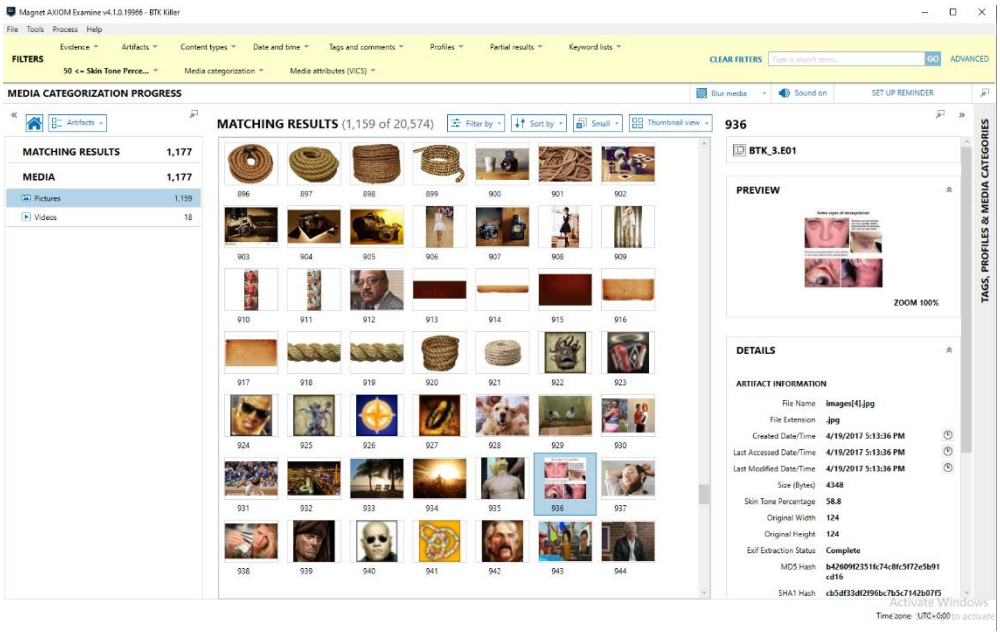


Figure 8.7

Figure 8.7 picture of what strangulation looks like.

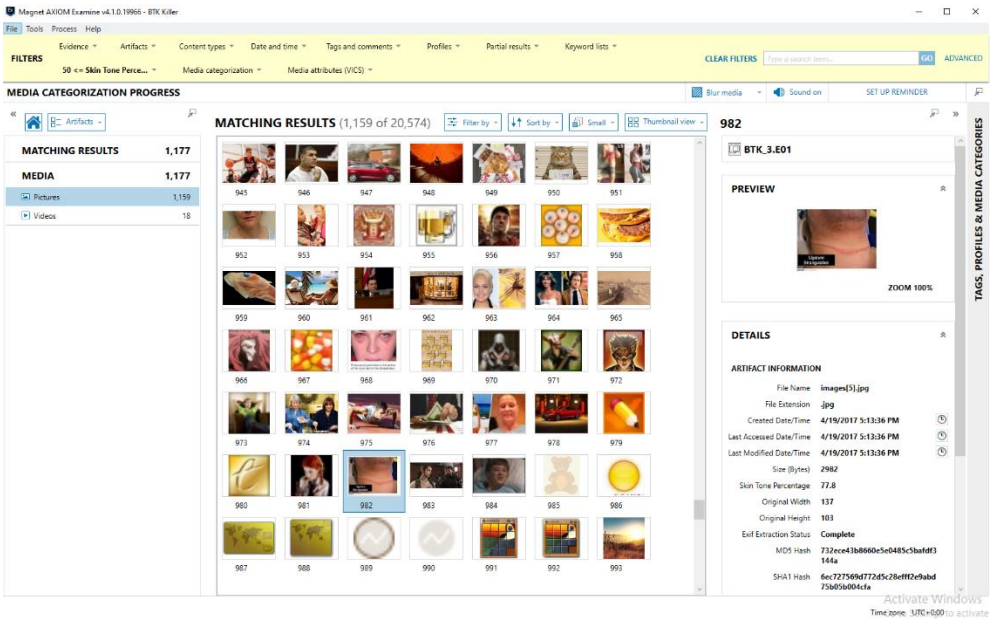


Figure 8.8

Figure 8.8 another picture of strangulation line.

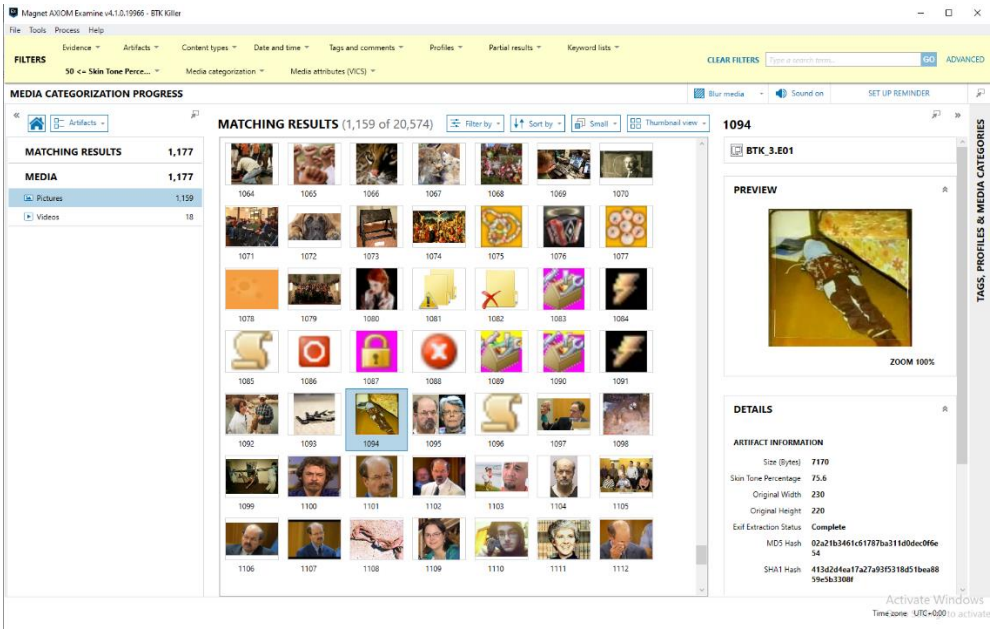


Figure 8.9

Figure 8.9 picture of victim wrapped up.

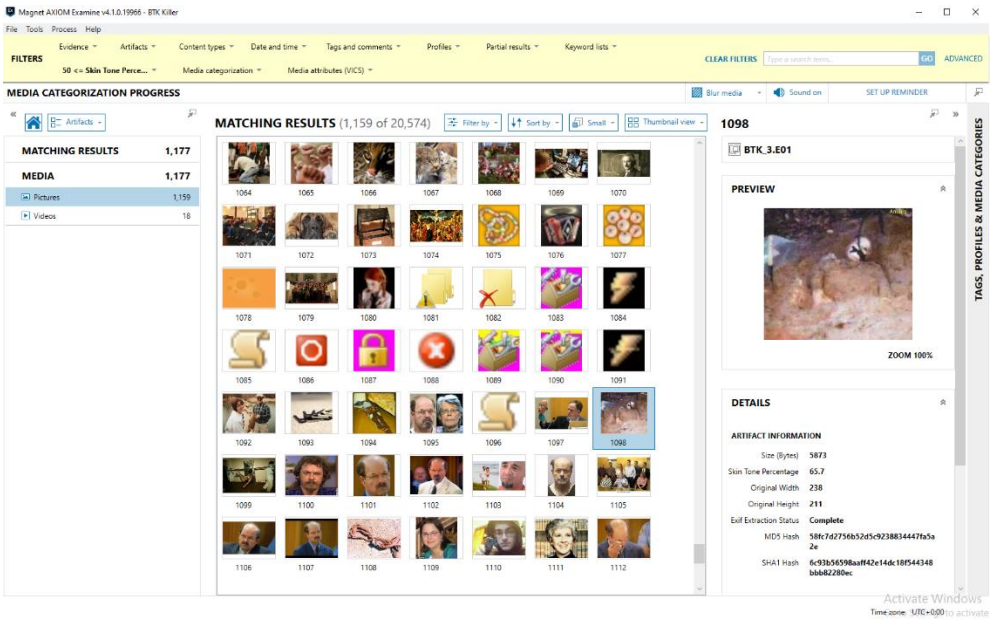


Figure 9.0

Figure 9.0 picture of victim.

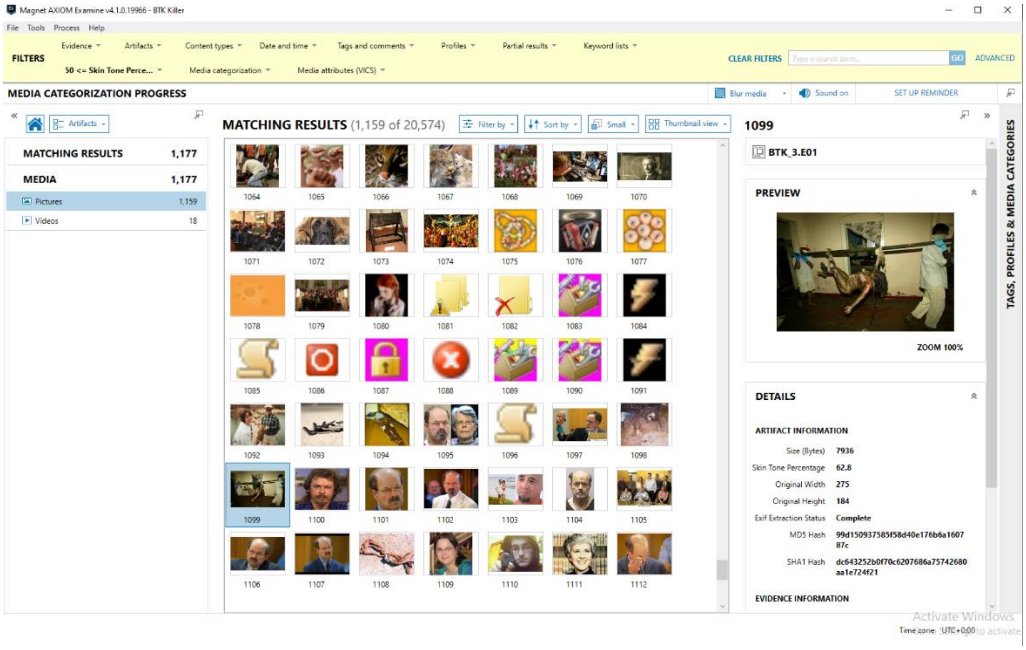


Figure 9.1

Figure 9.1 picture of victim tied up on some wooden ladder.

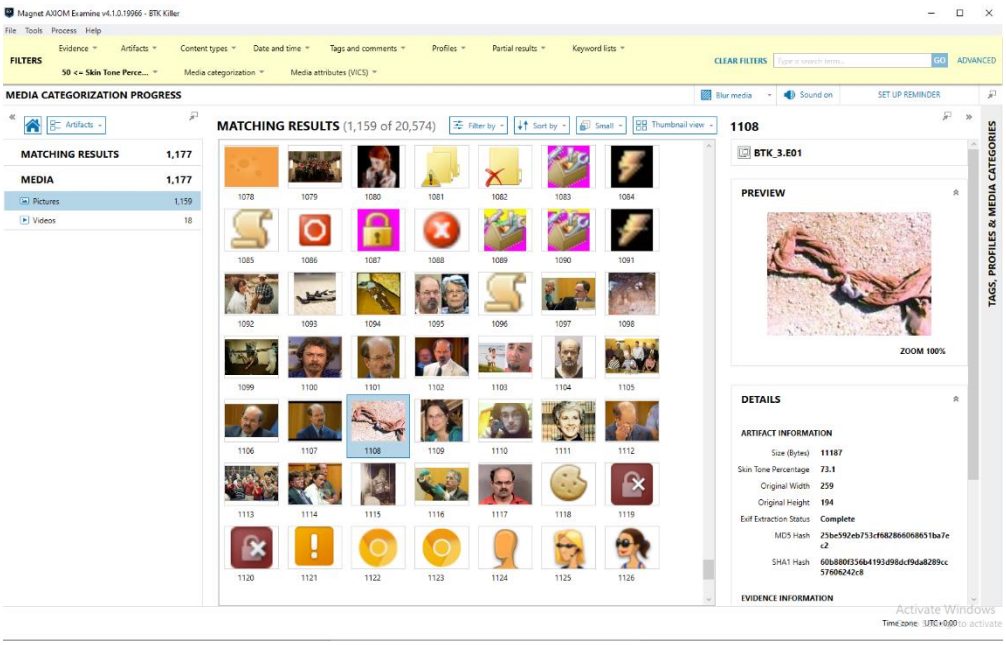


Figure 9.2

Figure 9.2 picture of some type of knot.

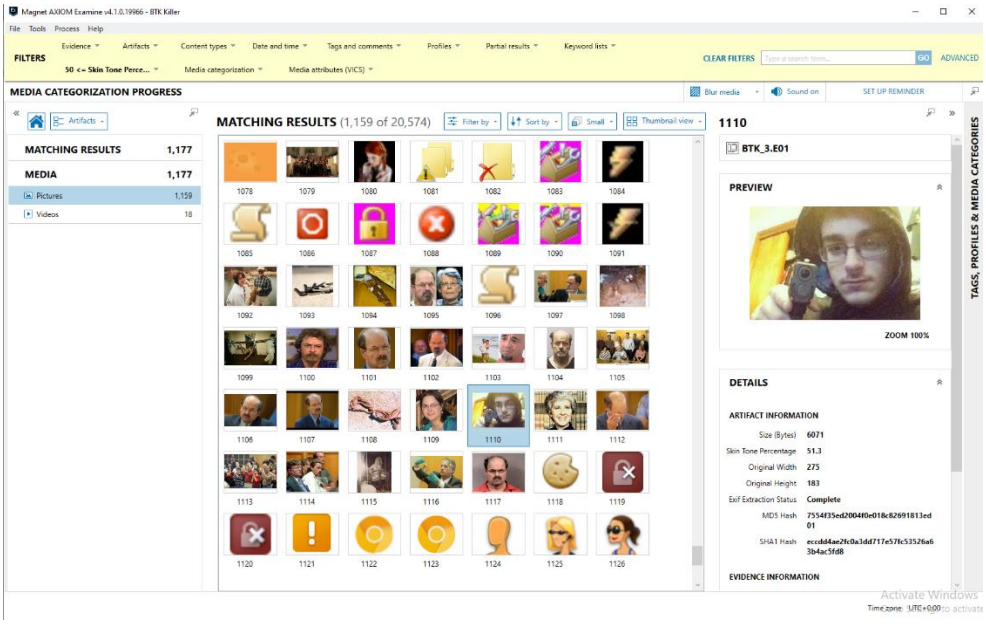


Figure 9.3

Figure 9.3 picture of a person pointing a gun at the camera.

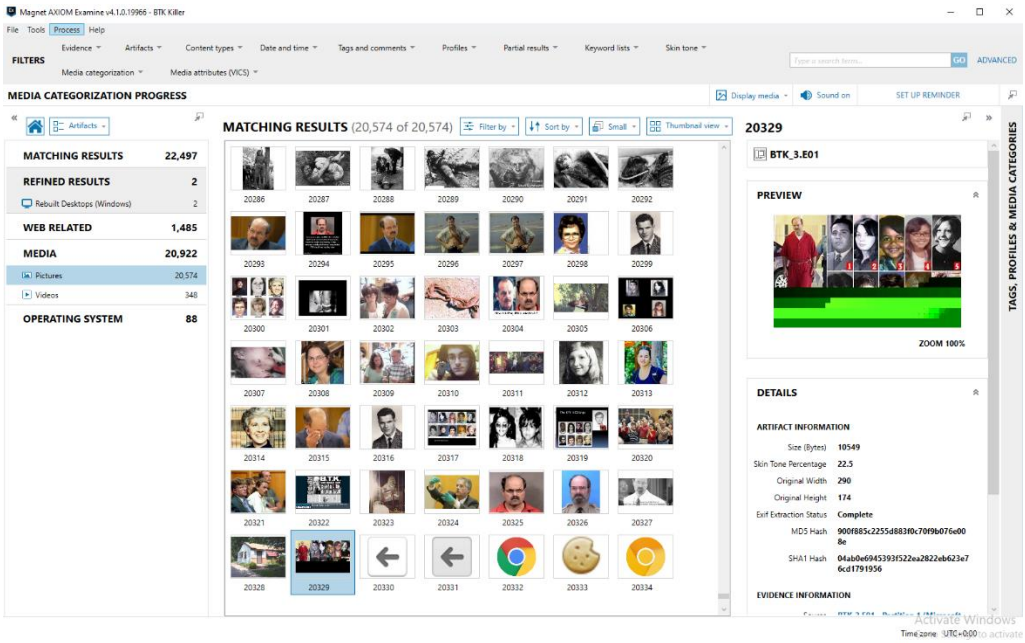


Figure 9.4

Figure 9.4 another picture of the btk killer and list of his victims.

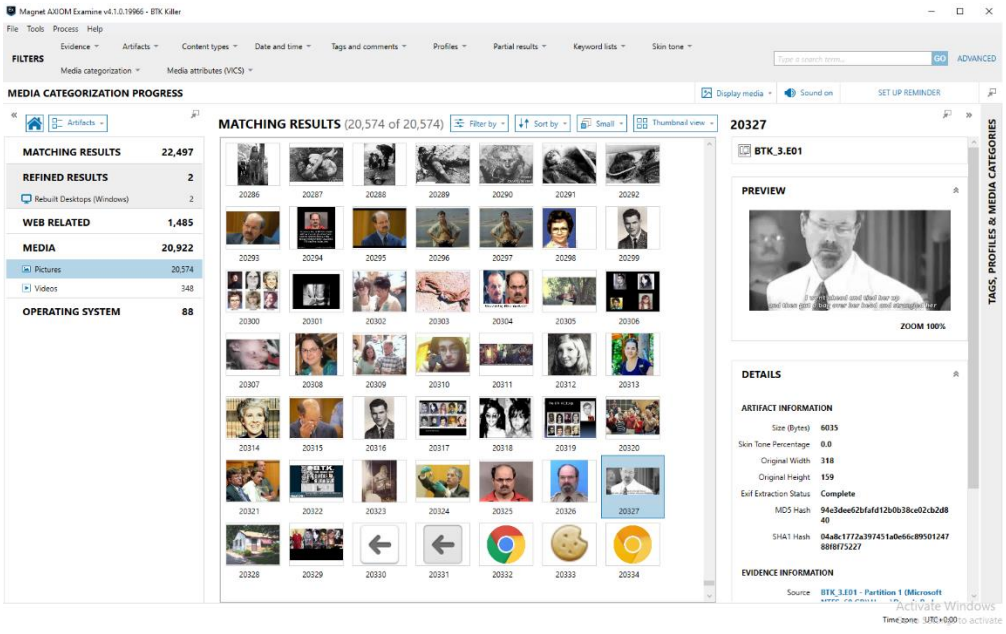


Figure 9.5

Figure 9.5 picture of captioned photograph of confession.

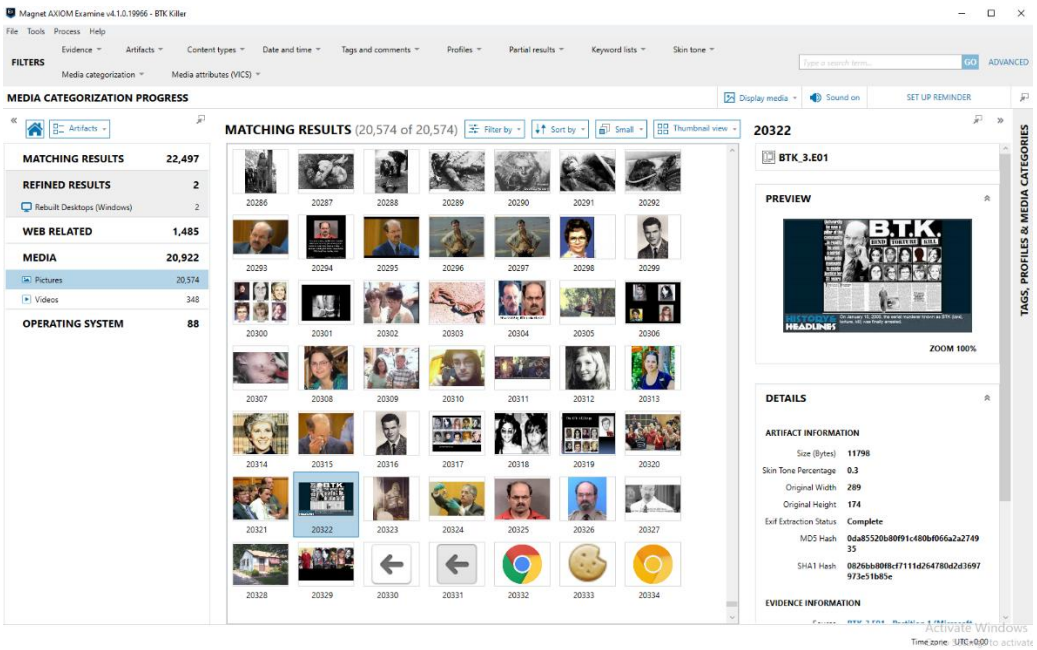


Figure 9.6

Figure 9.6 news article of the btk killer.

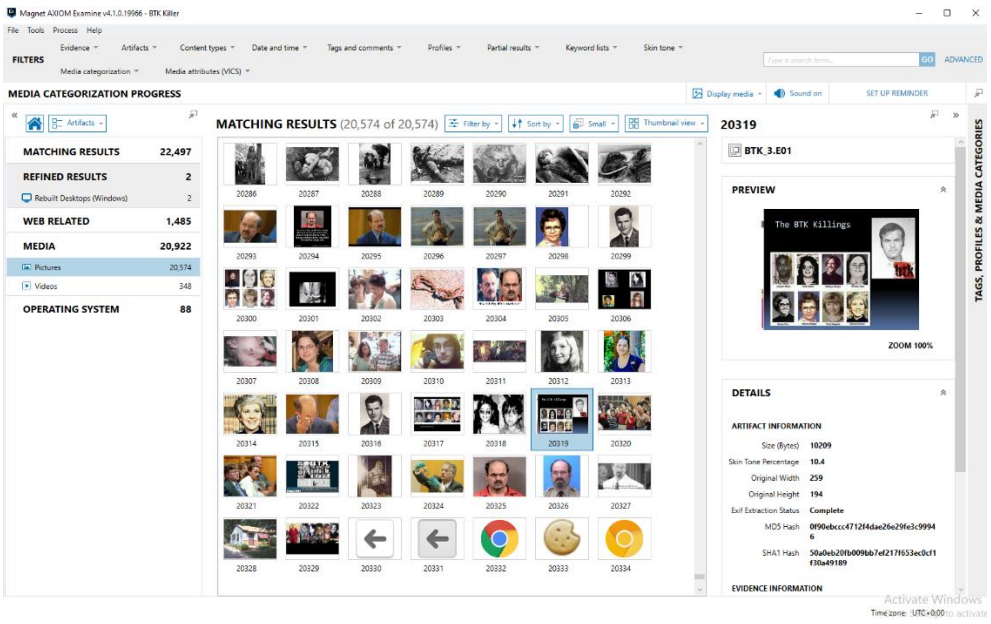


Figure 9.7

Figure 9.7 another picture of btk killer and the victims.

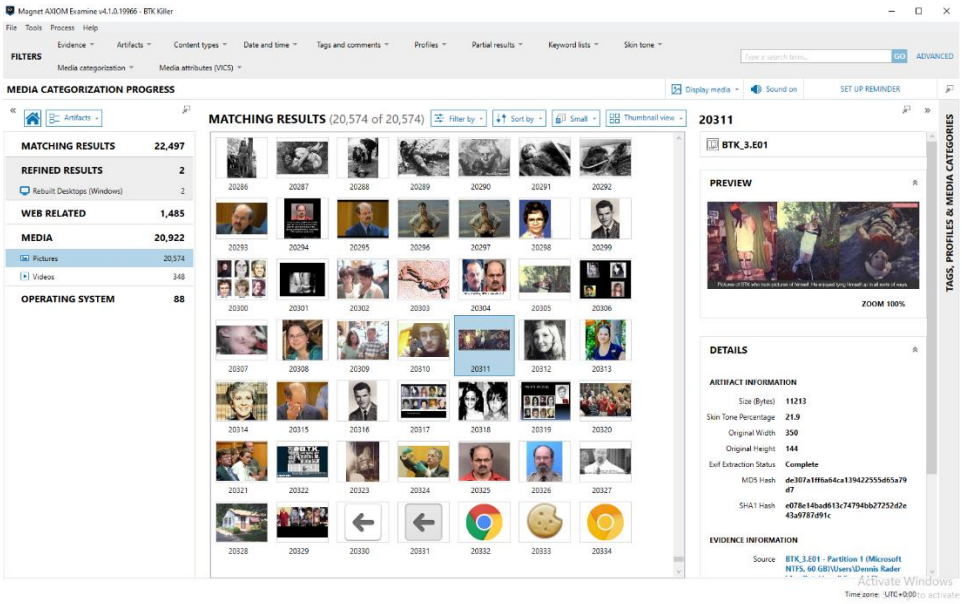


Figure 9.8

Figure 9.8 news article or crime scene photograph of the btk killer victims.

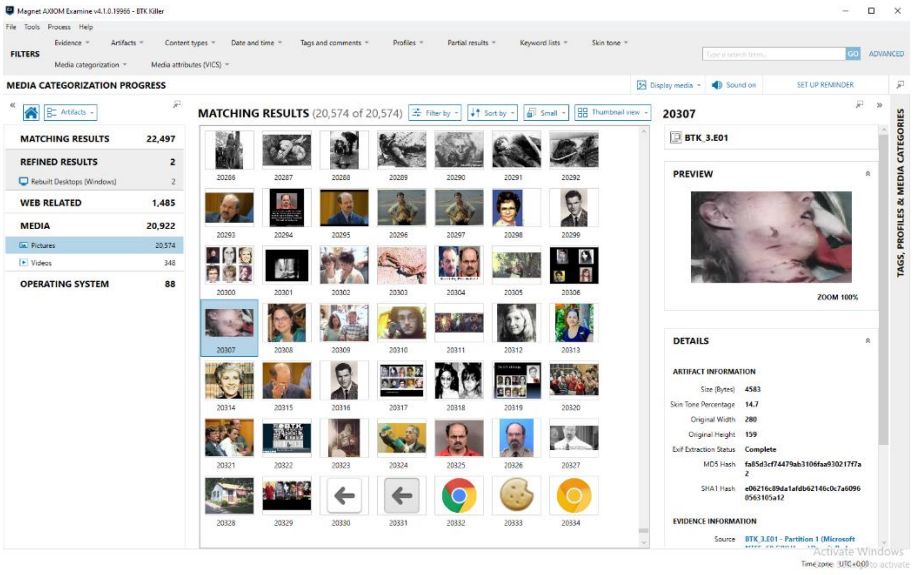


Figure 9.9

Figure 9.9 crime scene strangulation photograph.

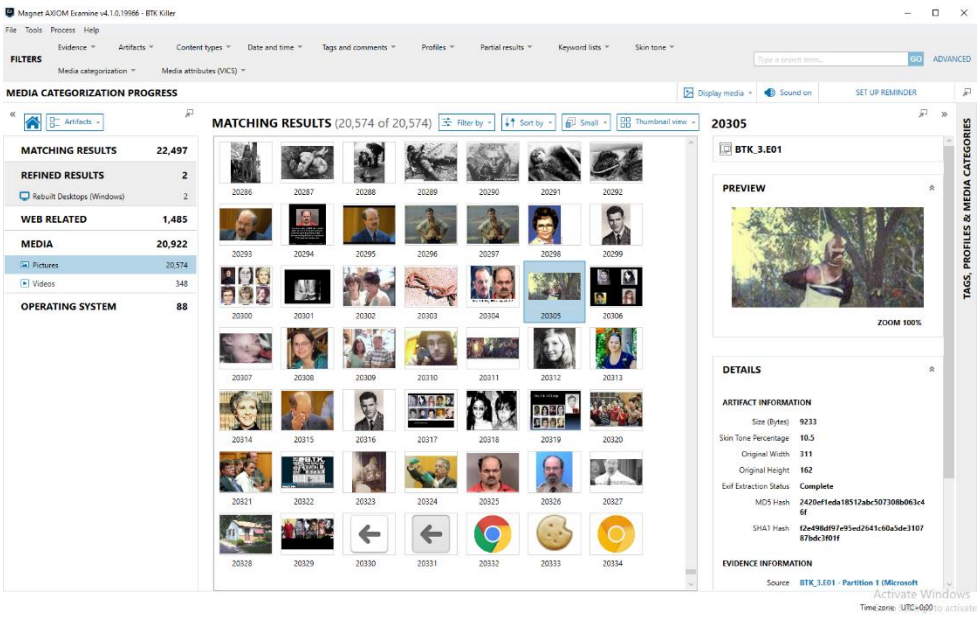


Figure 10.0

Figure 10.0 image of btk killer hanging victim.

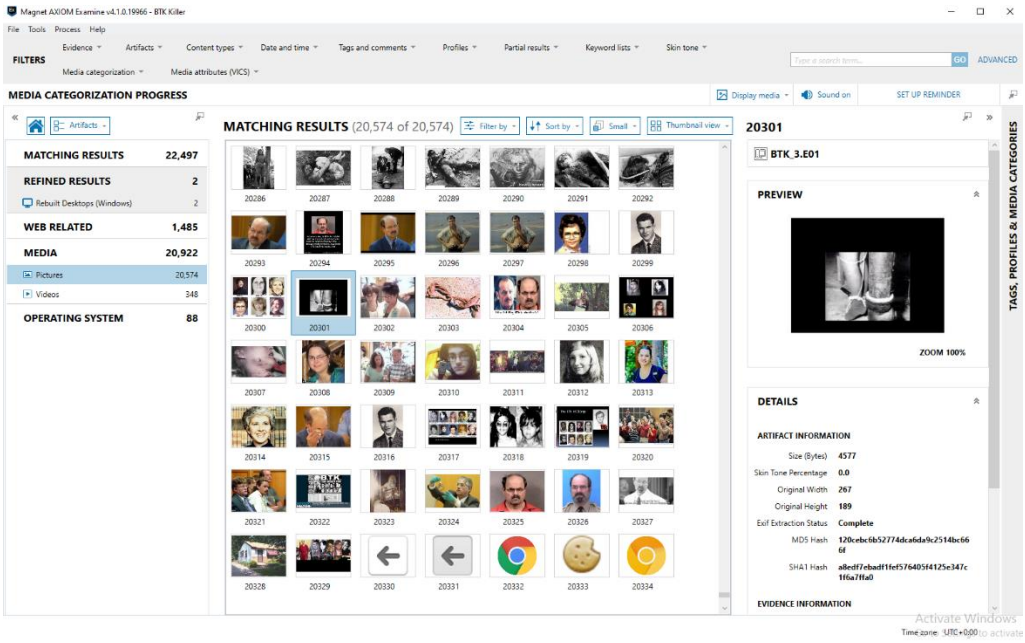


Figure 10.1

Figure 10.1 legs taped up of one of his victims.

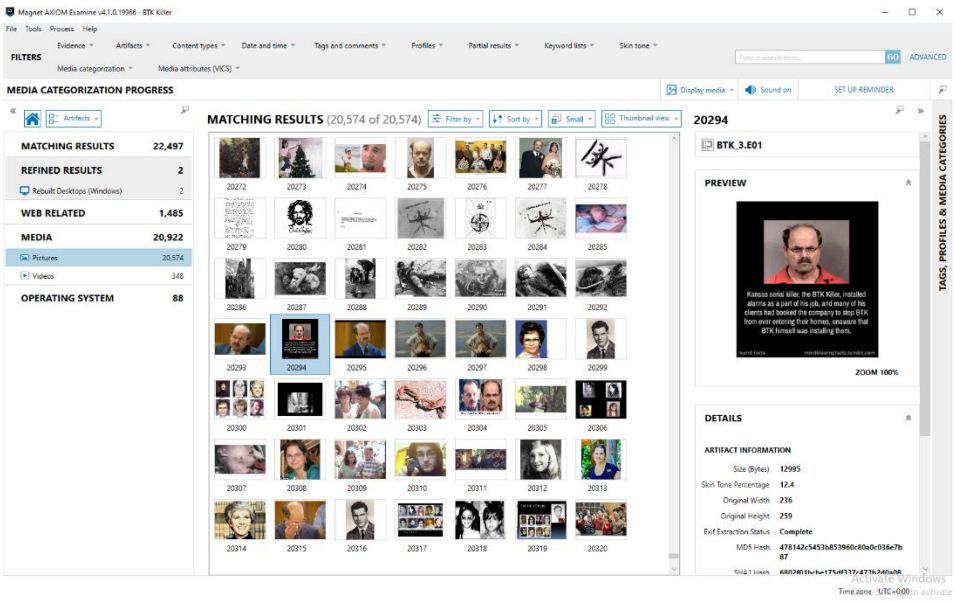


Figure 10.2

Figure 10.2 image of the serial killer with captions.

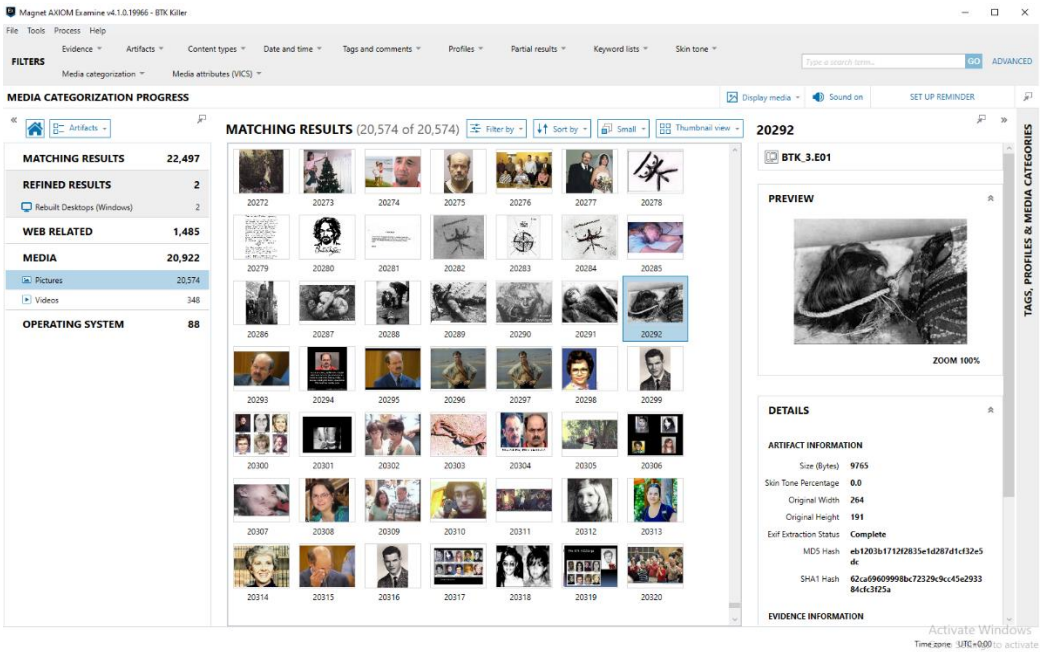


Figure 10.3

Figure 10.3 image of strangled victim.

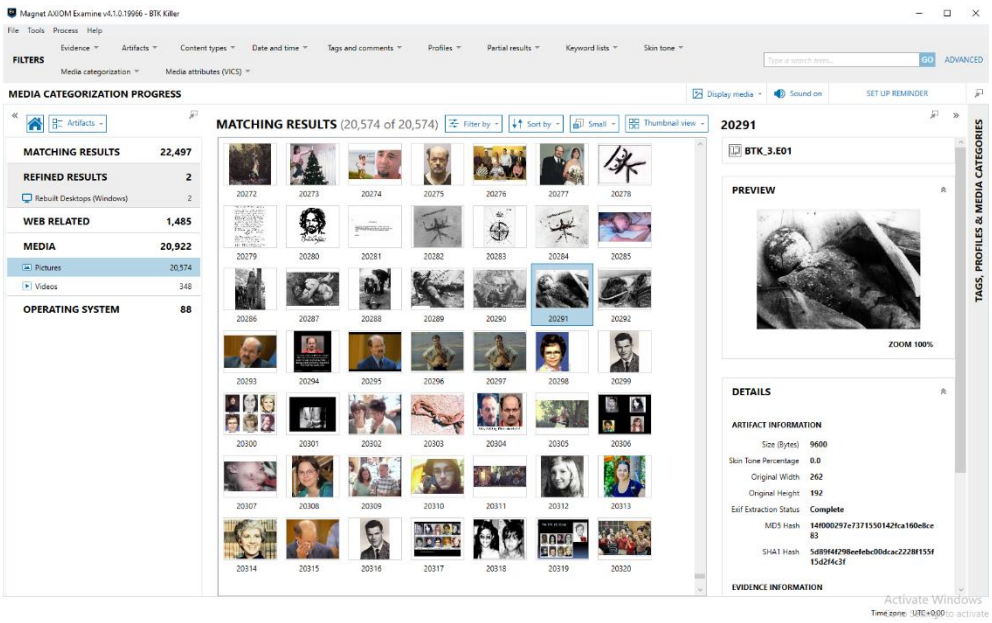


Figure 10.4

Figure 10.4 image of victim.

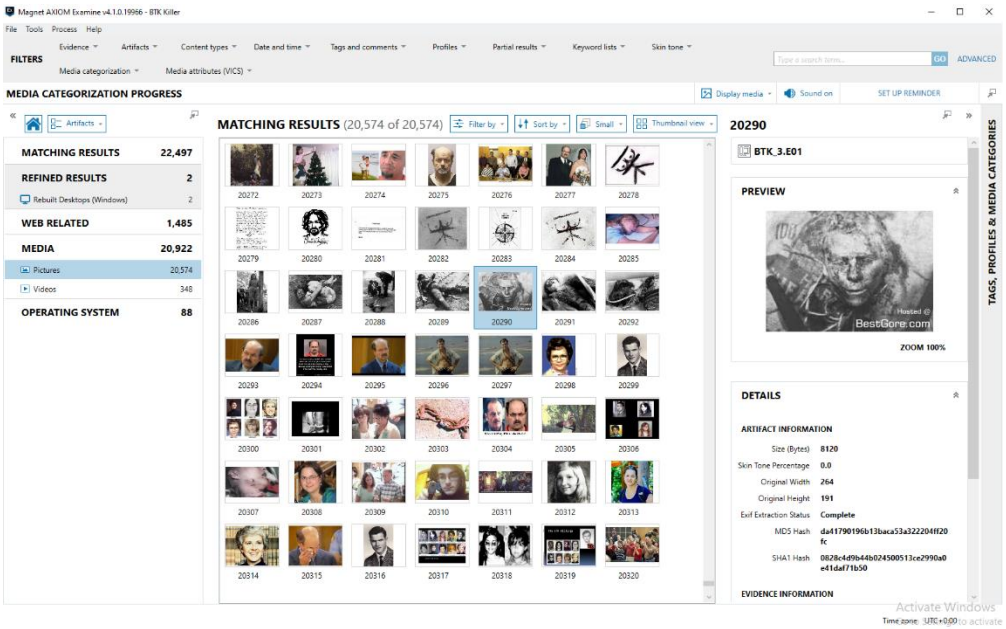


Figure 10.5

Figure 10.5 image of victim.

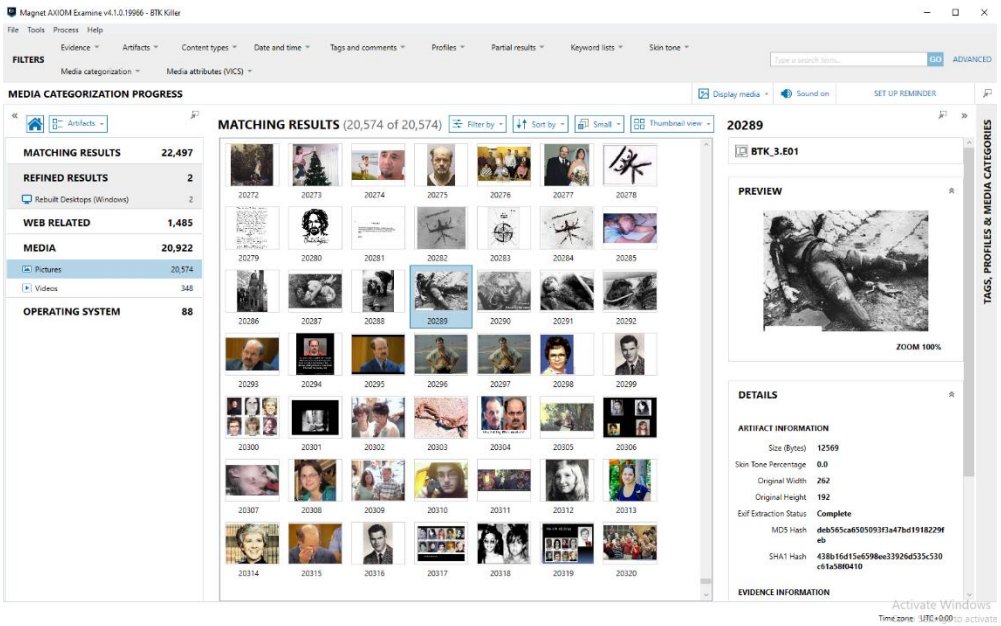


Figure 10.6

Figure 10.6 image of victim.

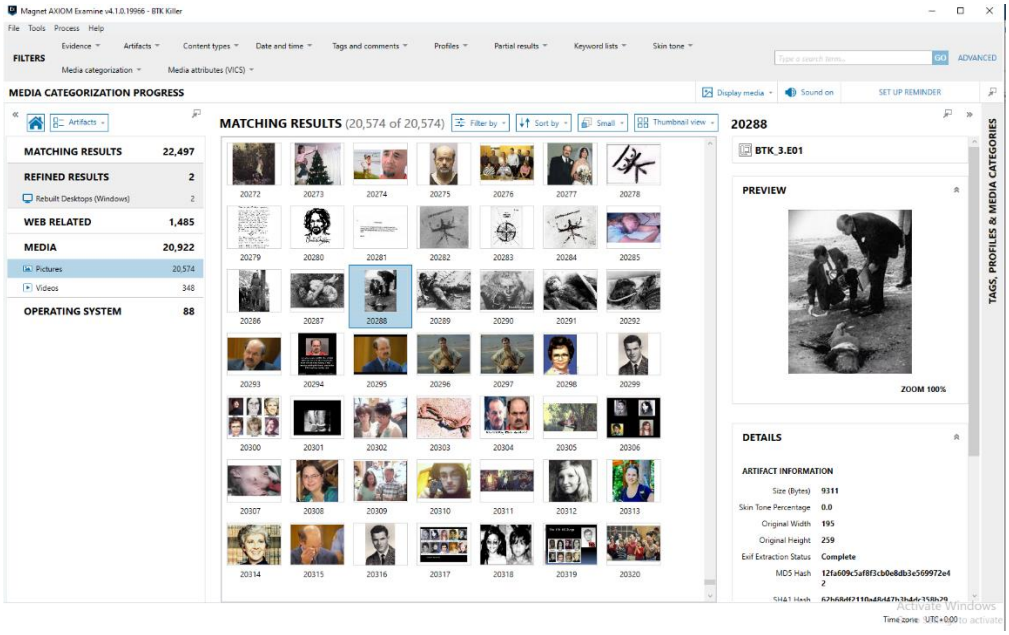


Figure 10.7

Figure 10.7 crime scene image of victim.

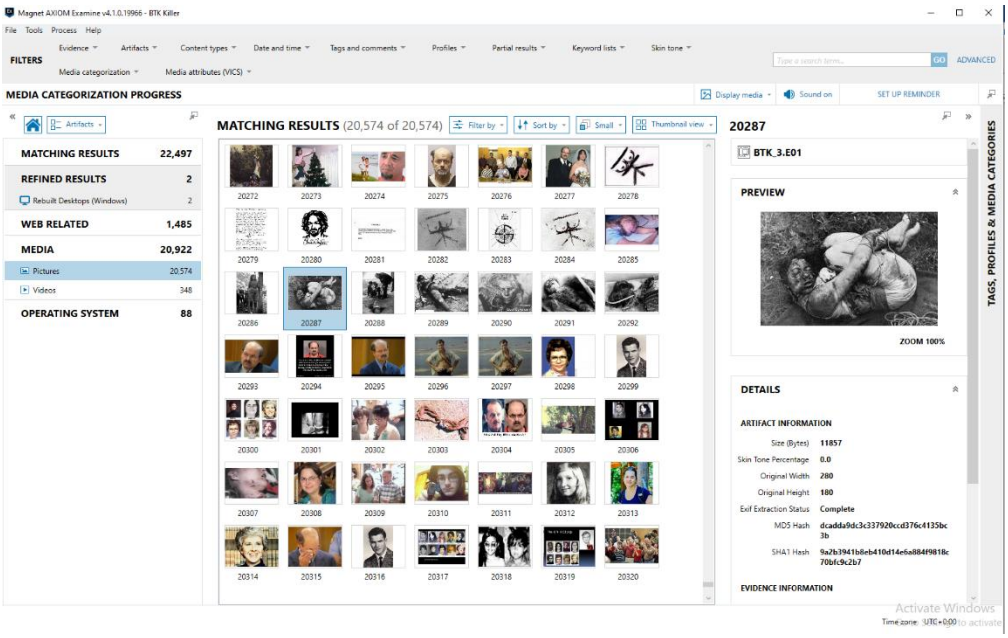


Figure 10.8

Figure 10.8 crime scene image of victim.

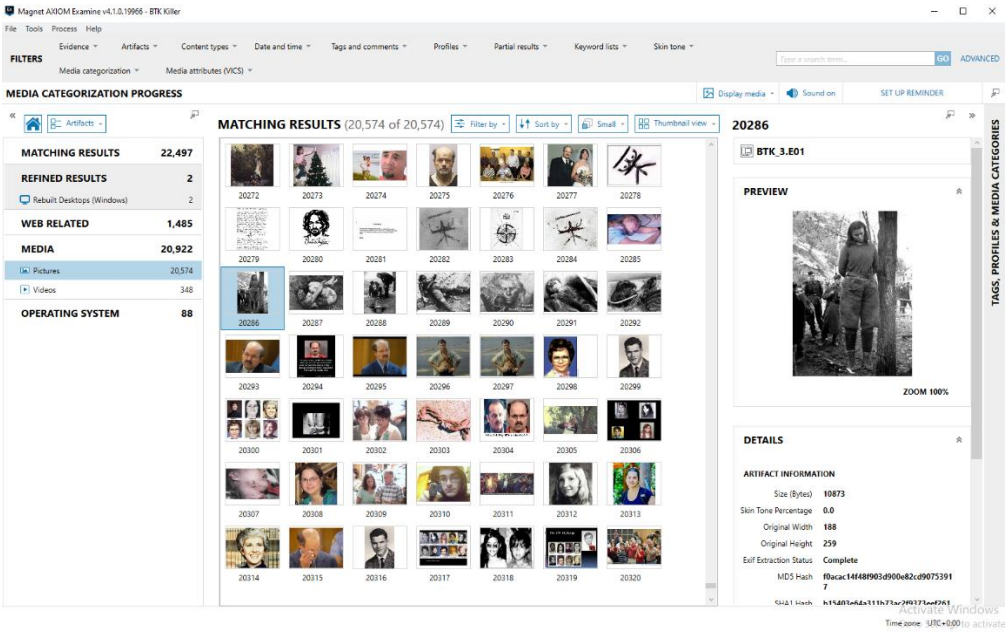


Figure 10.9

Figure 10.9 crime scene image of victim.

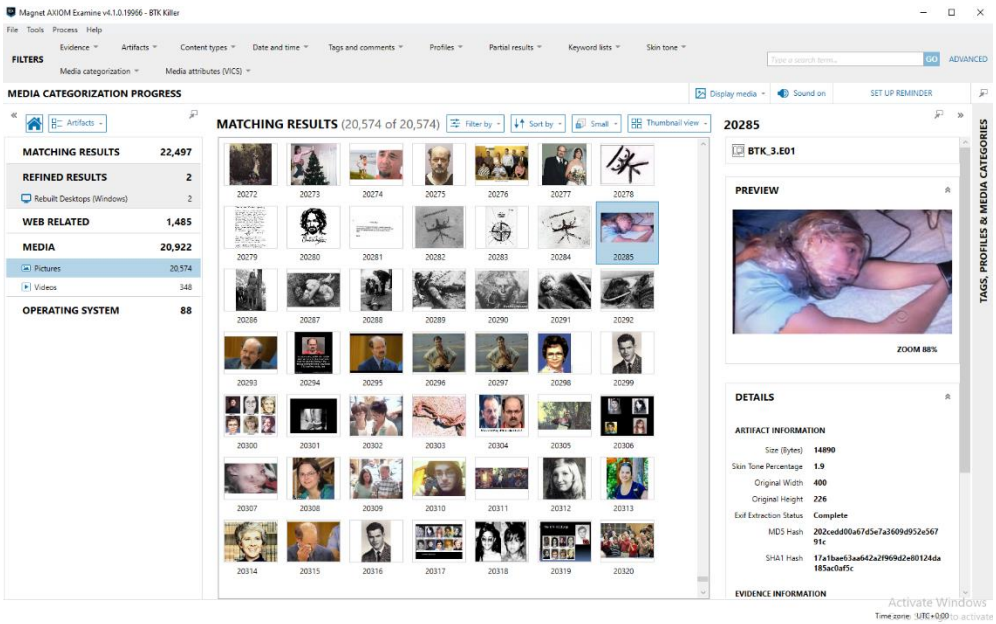


Figure 11.0

Figure 11.0 crime scene image of victim strangled with plastic bag.

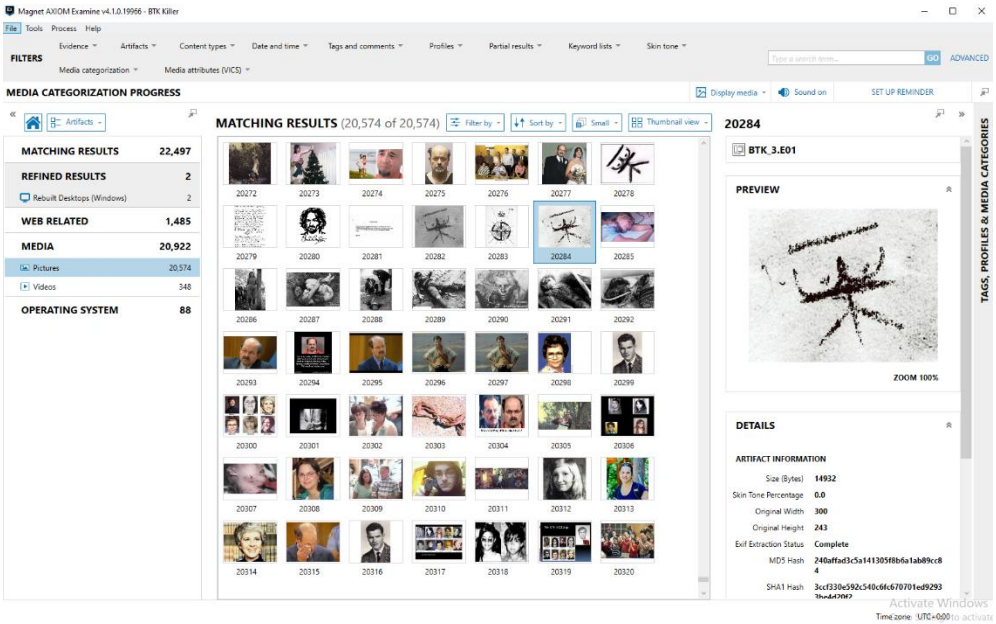


Figure 11.1

Figure 11.1 another btk killer signature image.

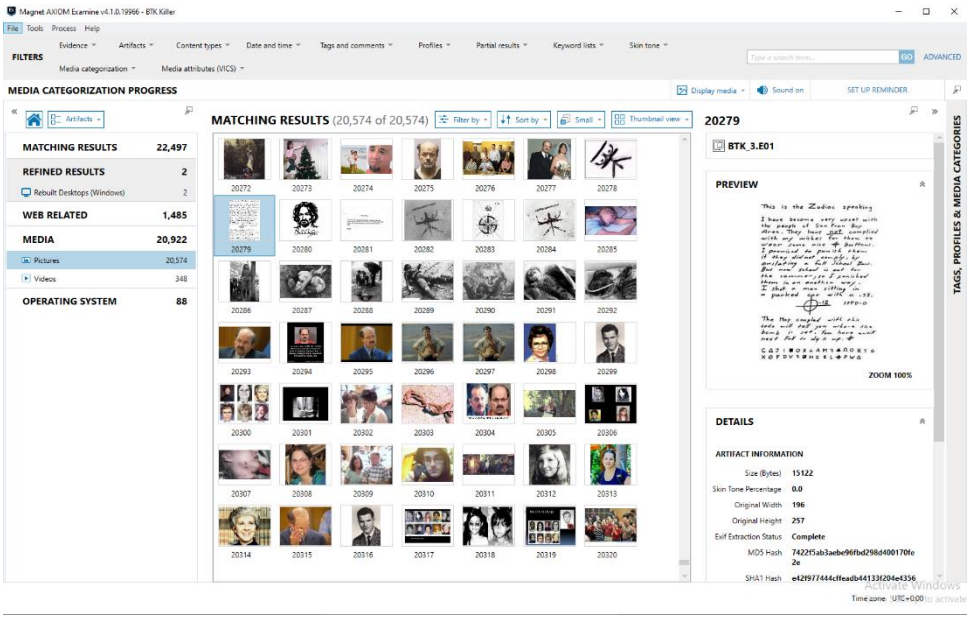


Figure 11.2

Figure 11.2 note by the Zodiac killer.

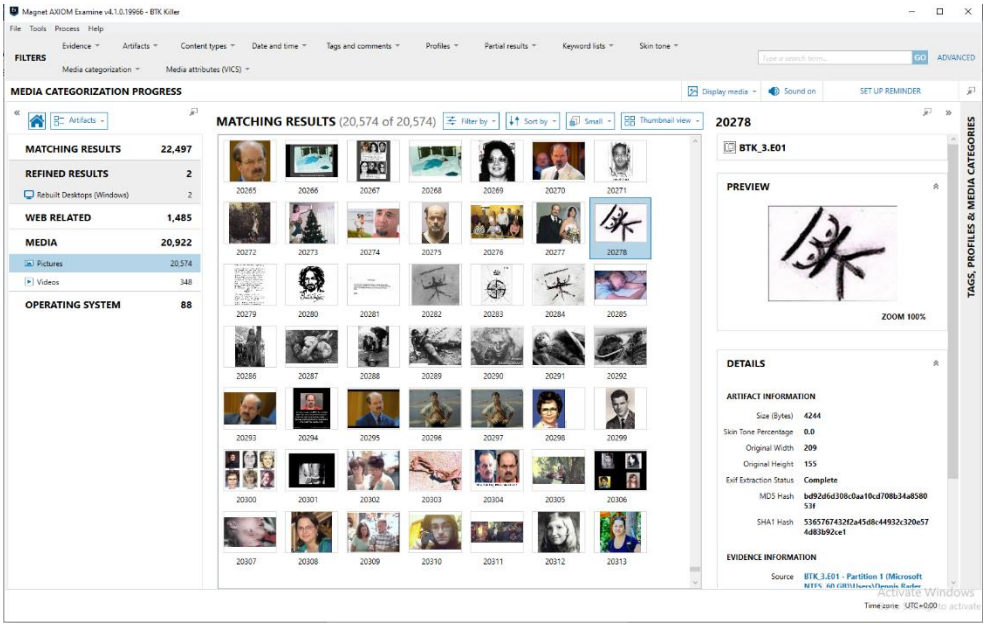


Figure 11.3

Figure 11.3 another picture of the btk killer's signature.

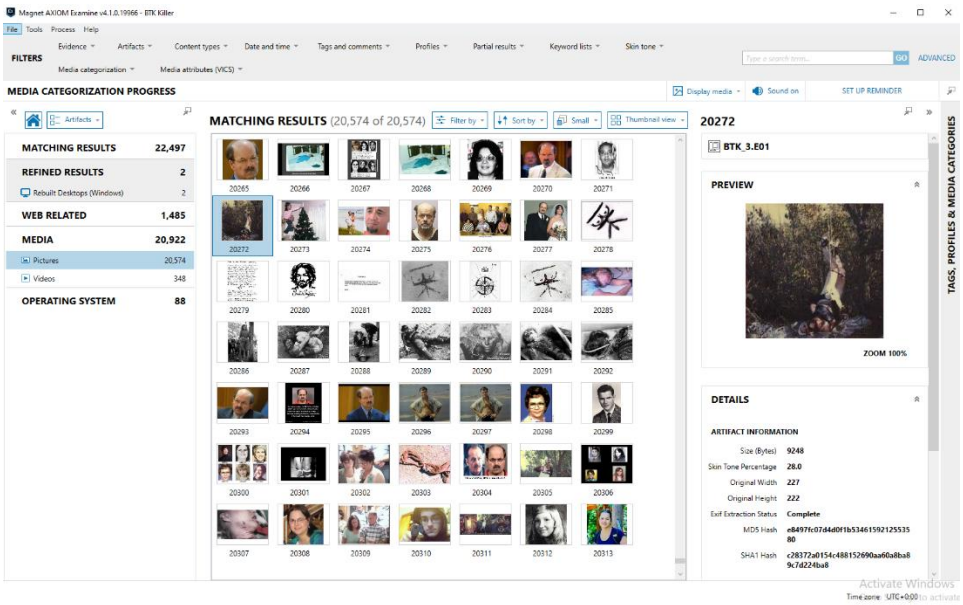


Figure 11.4

Figure 11.4 victim of btk killer.

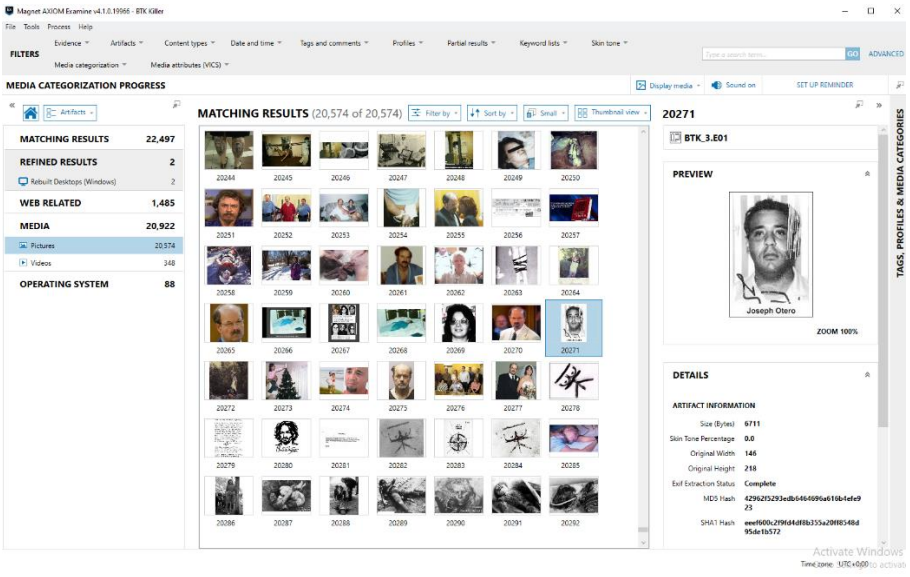


Figure 11.5

Figure 11.5 victim of btk killer.

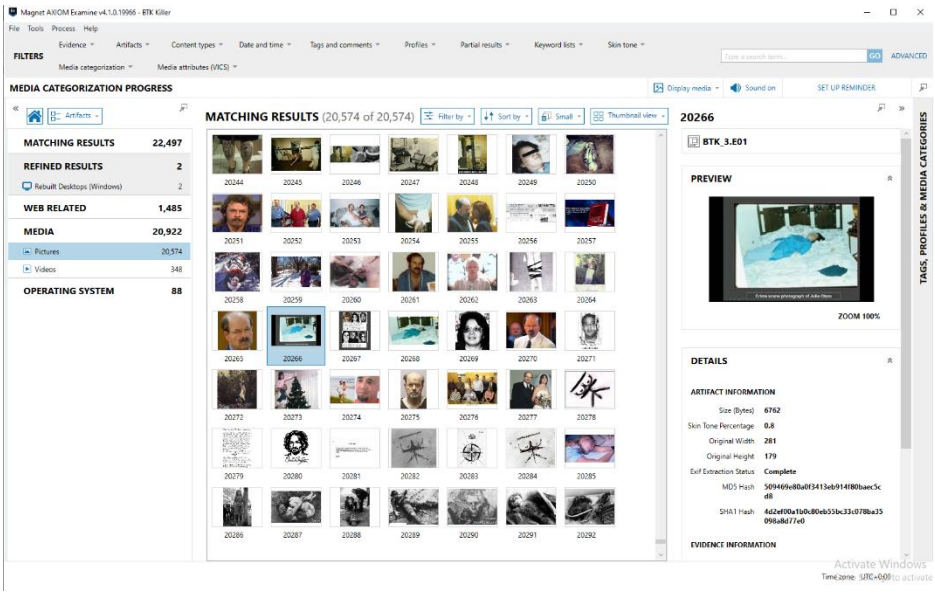


Figure 11.6

Figure 11.6 photograph of victim of btk killer.

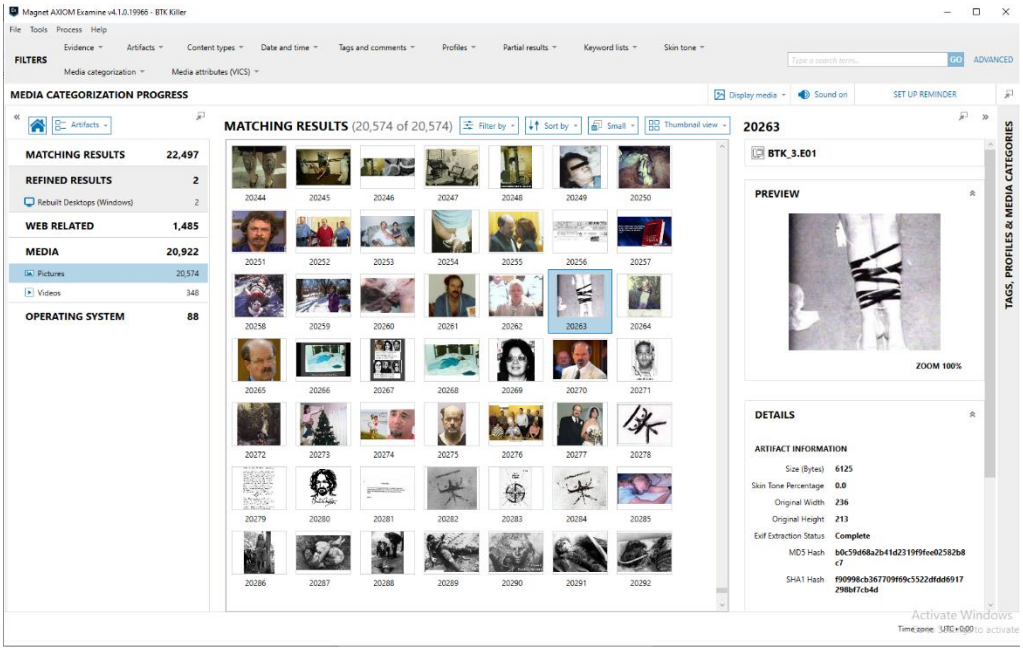


Figure 11.7

Figure 11.7 photograph of a victim with their legs tied up with black tape.

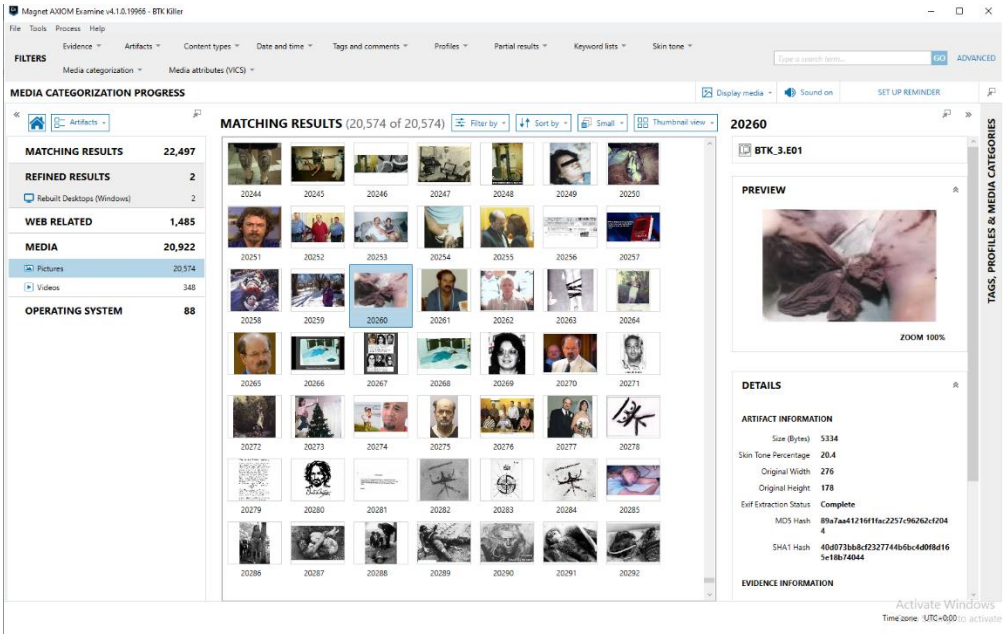


Figure 11.8

Figure 11.8 a knot created by the btk killer stained with blood.

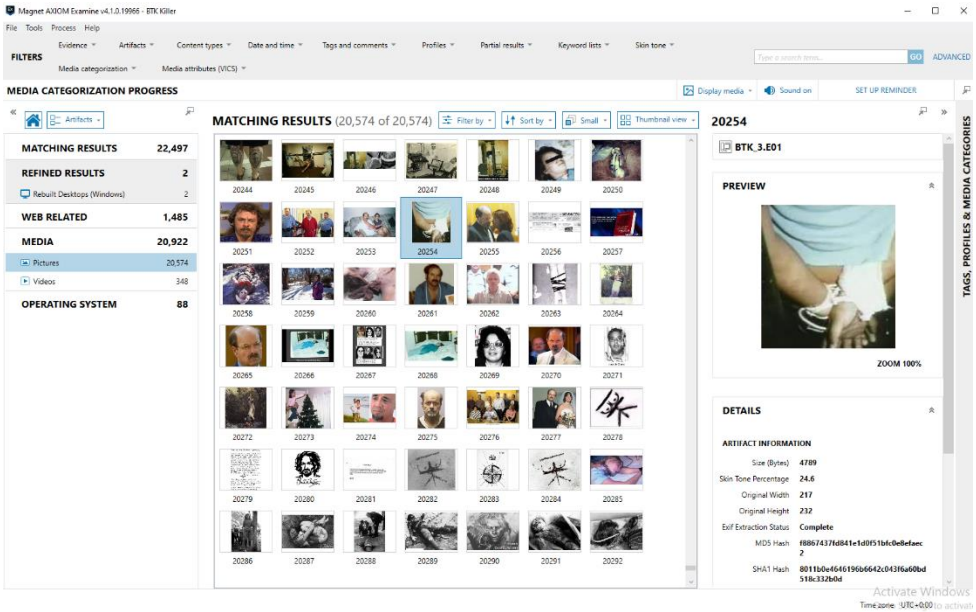


Figure 11.9

Figure 11.9 victims' hands tied with a knot by the btk killer.

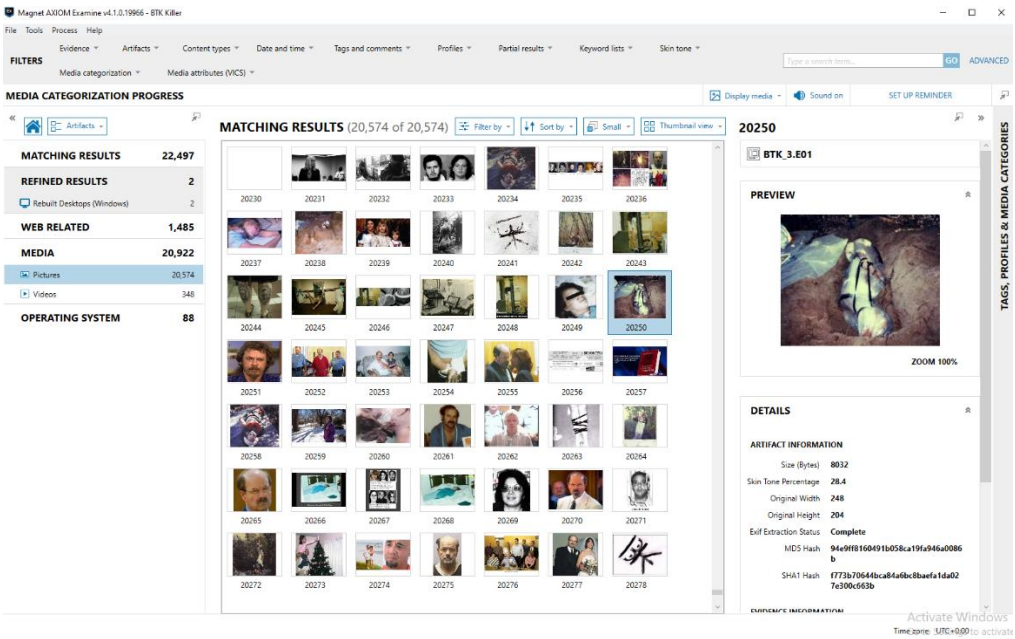


Figure 12.0

Figure 12.0 victim of the btk killer wrapped up.

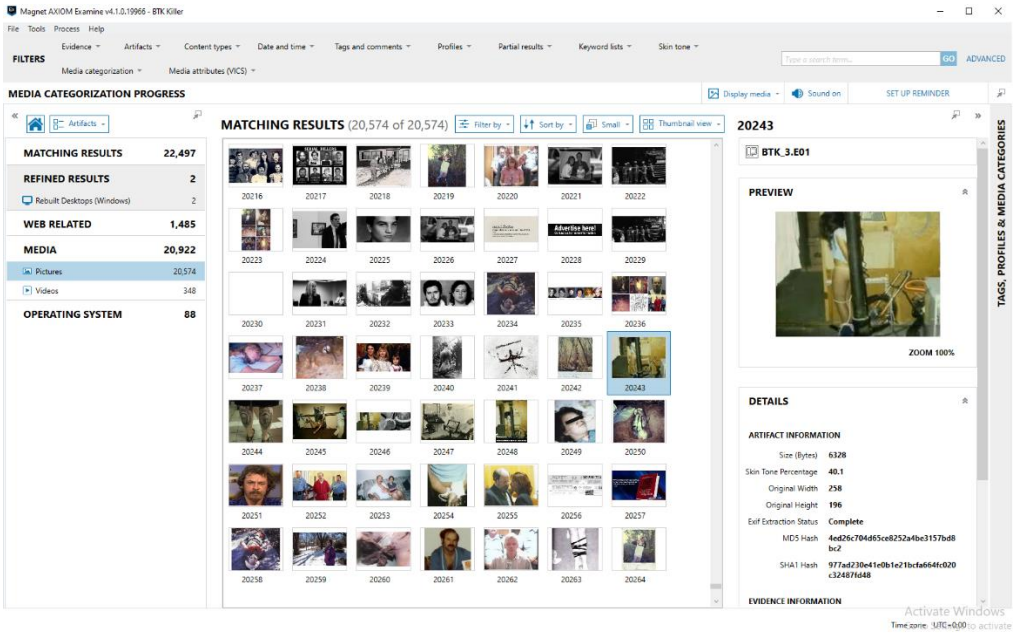


Figure 12.1

Figure 12.1 photograph of a victim tied to a pole.

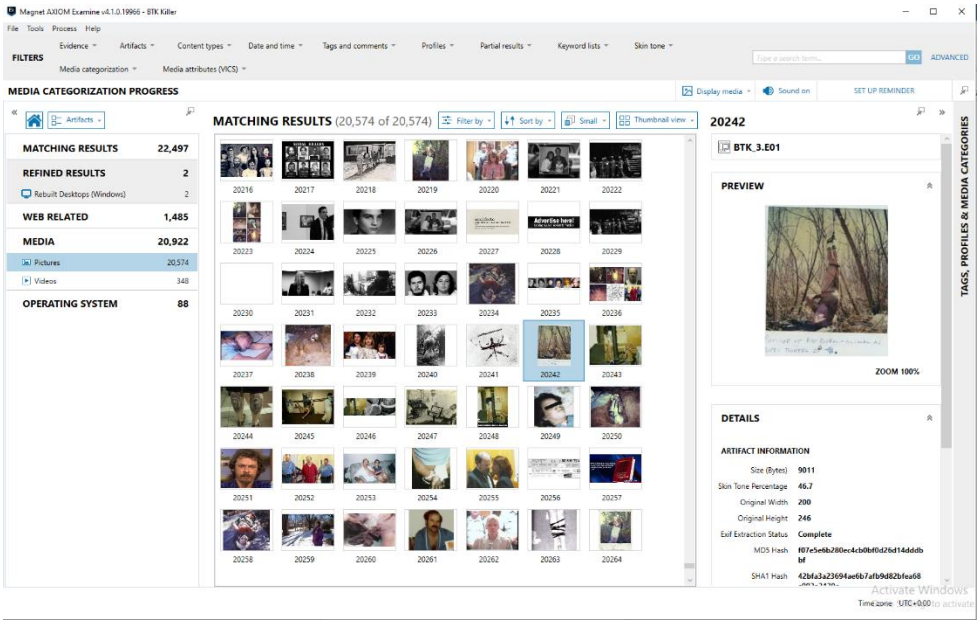


Figure 12.2

Figure 12.2 picture of victim being hung by their feet.

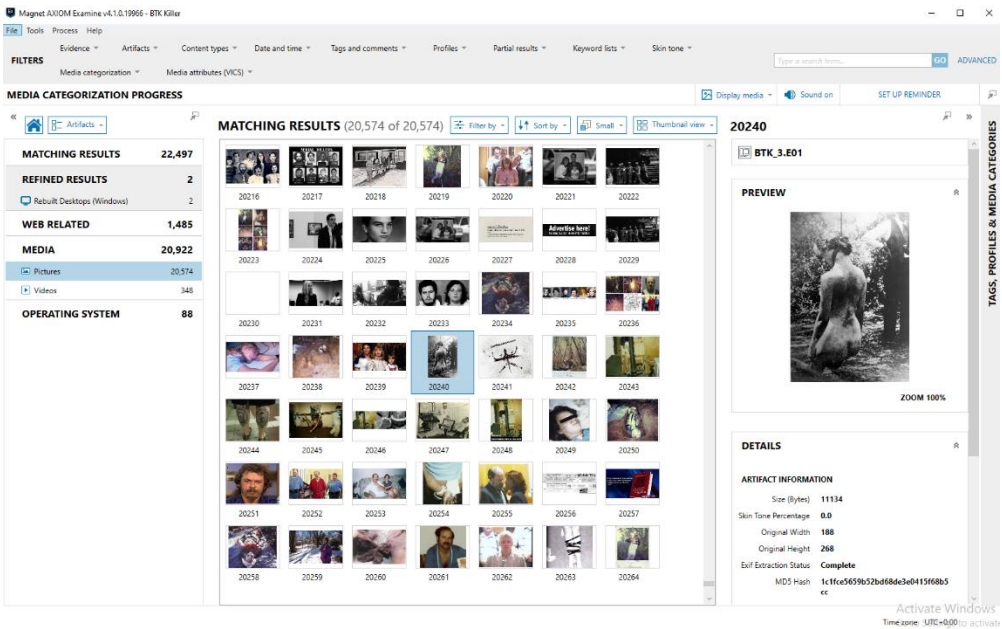


Figure 12.3

Figure 12.3 photograph of victim being hung by their neck.

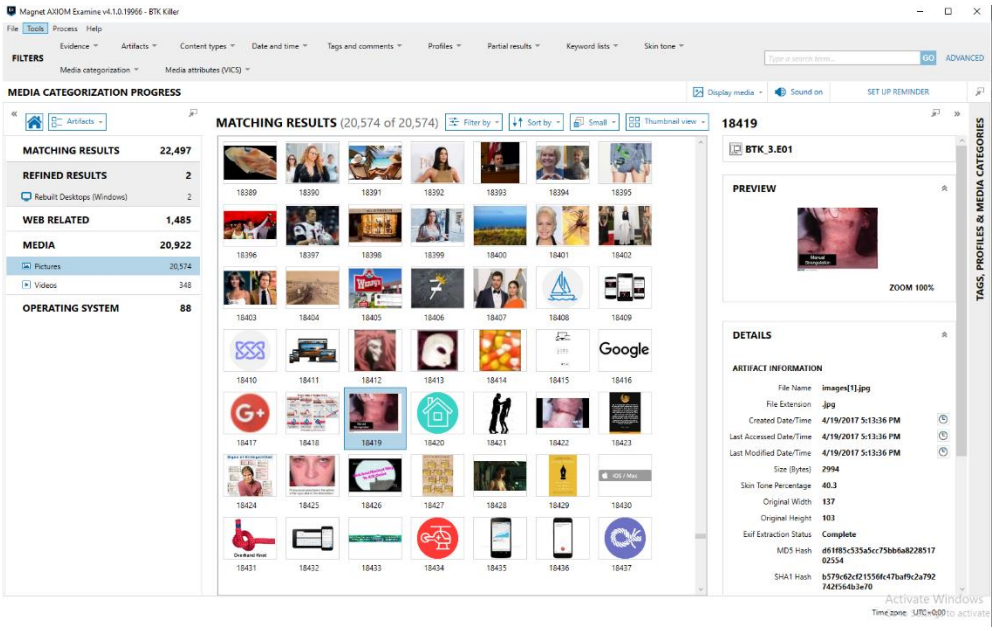


Figure 12.4

Figure 12.4 picture of strangulation marks.

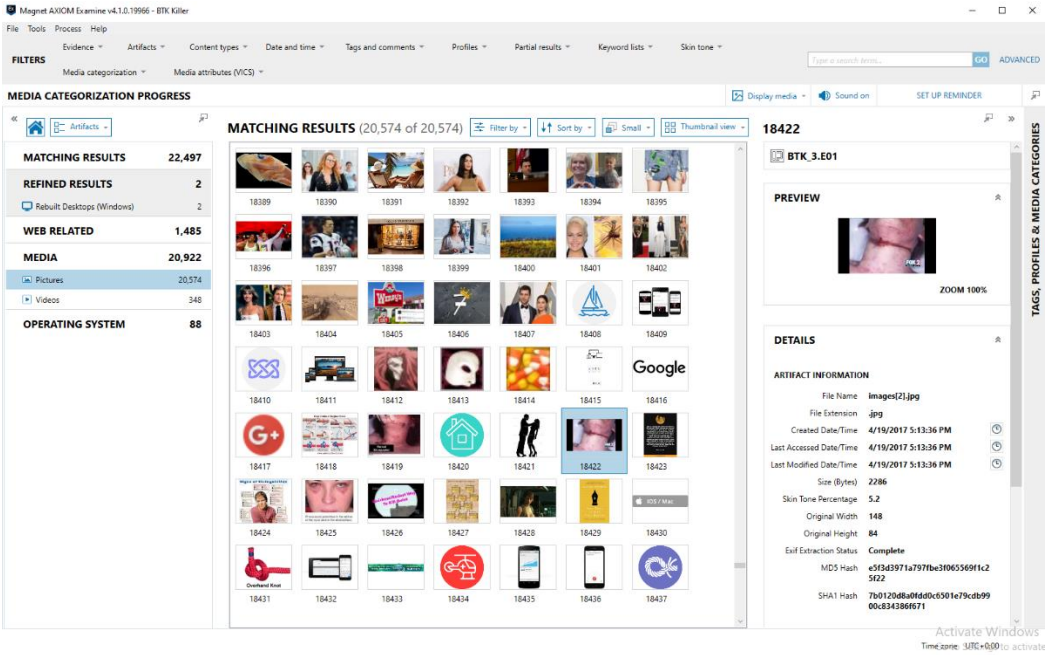


Figure 12.5

Figure 12.5 picture of strangulation line.

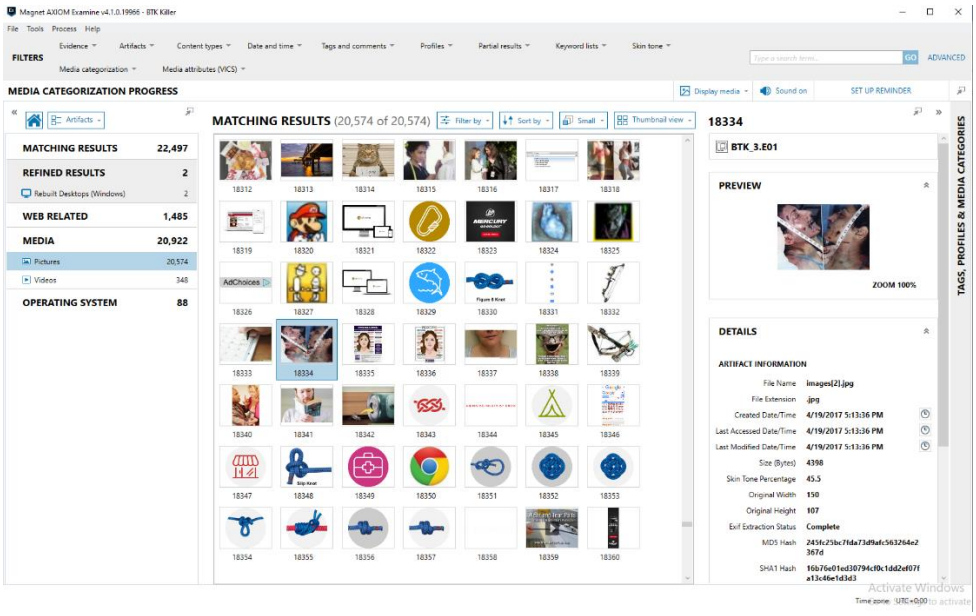


Figure 12.6

Figure 12.6 picture of crime scene victim measurements.

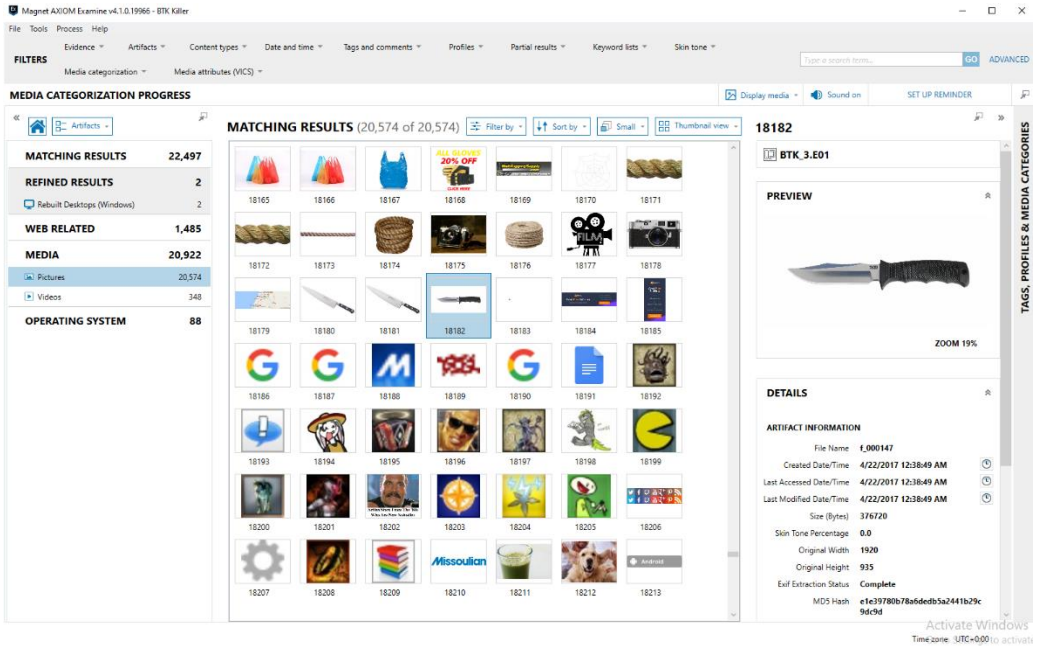


Figure 12.7

Figure 12.7 photograph of knife.

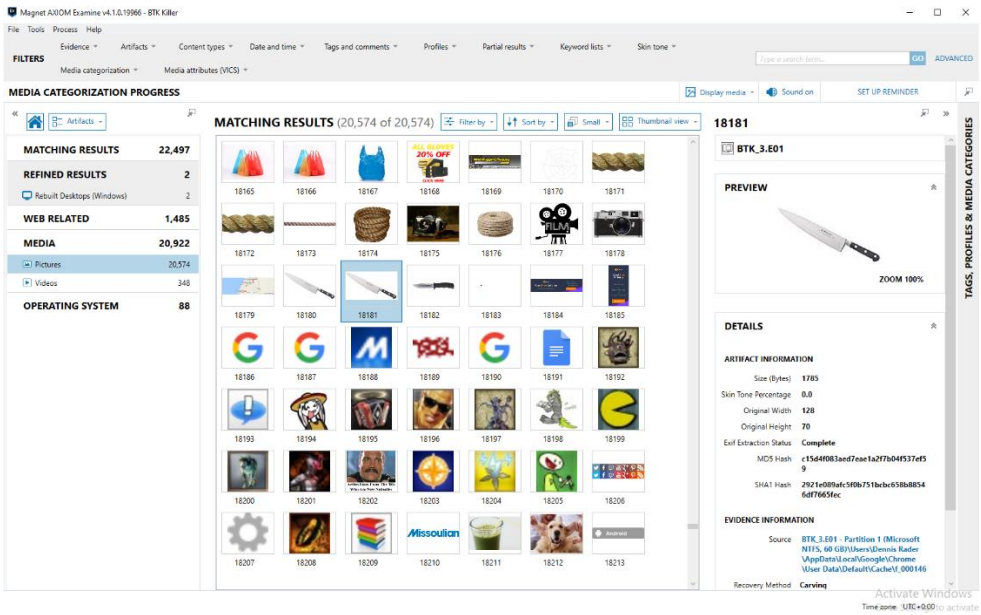


Figure 12.8

Figure 12.8 photograph of knife.

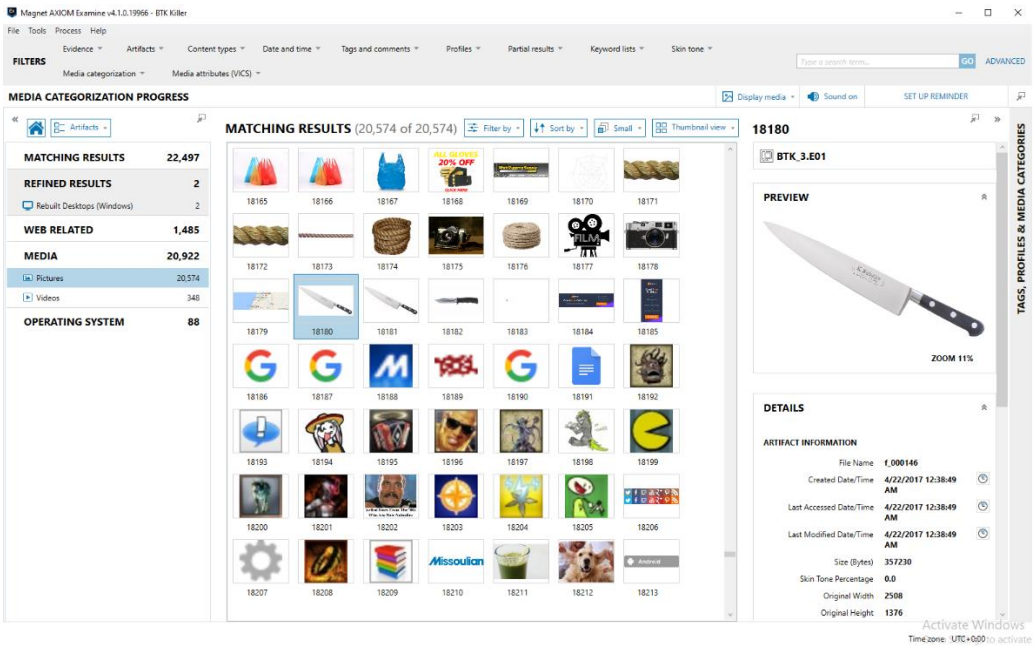


Figure 12.9

Figure 12.9 photograph of knife.

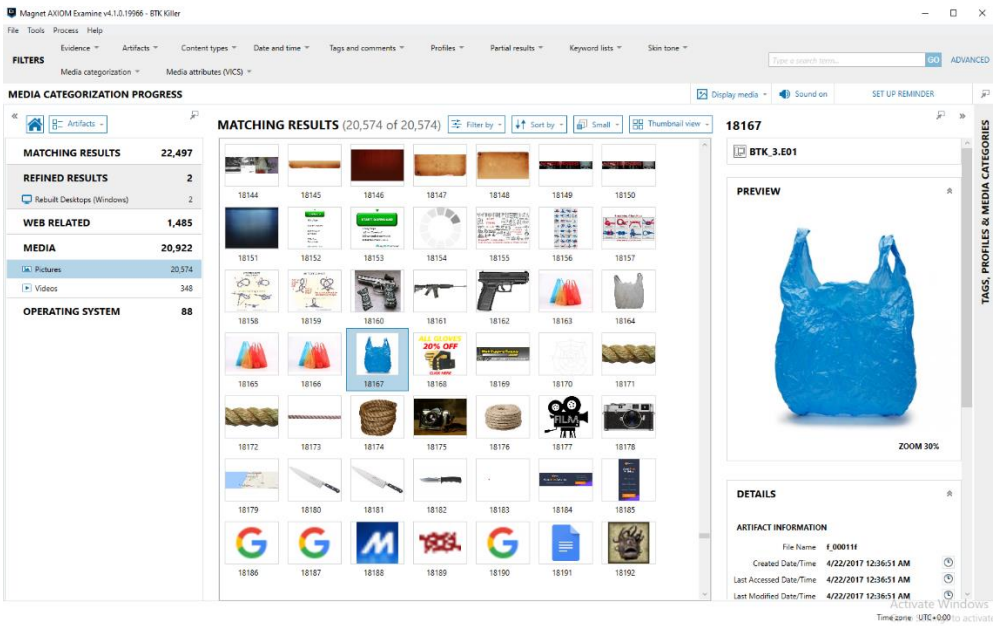


Figure 13.0

Figure 13.0 photograph of plastic bag.

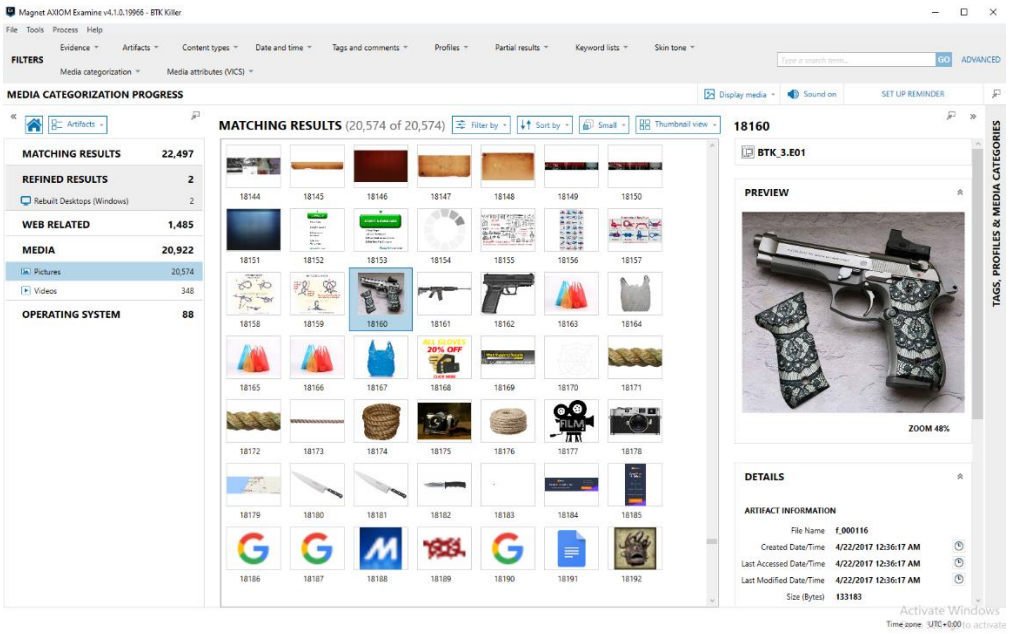


Figure 13.1

Figure 13.1 photograph of pistol.

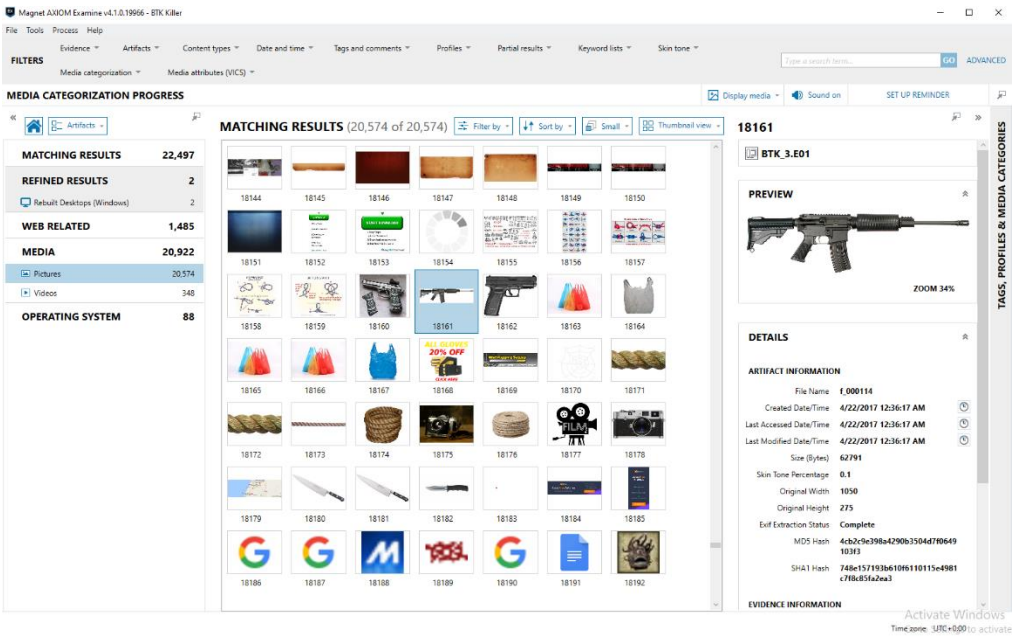


Figure 13.2

Figure 13.2 photograph of AR.

Documents

Rtf documents.

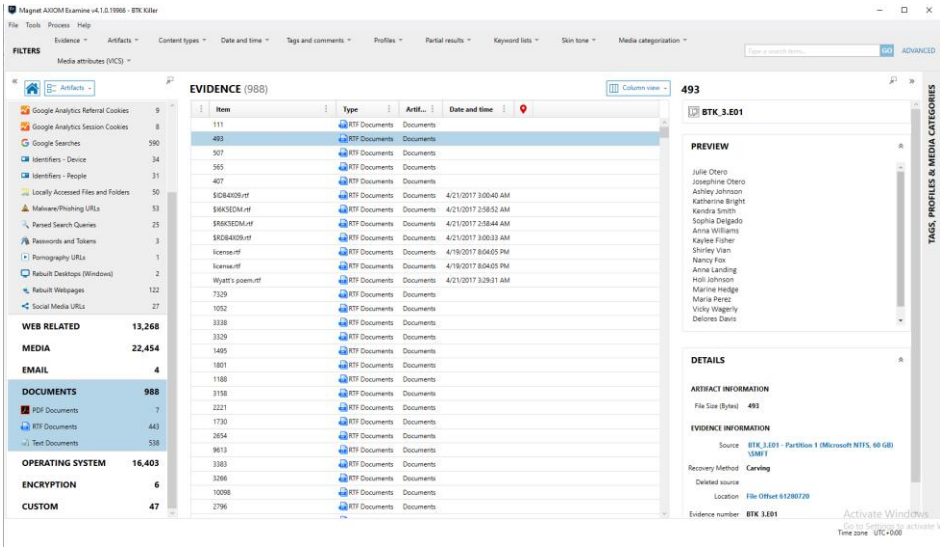


Figure 13.3

Figure 13.3 list of victims of the btk killer.

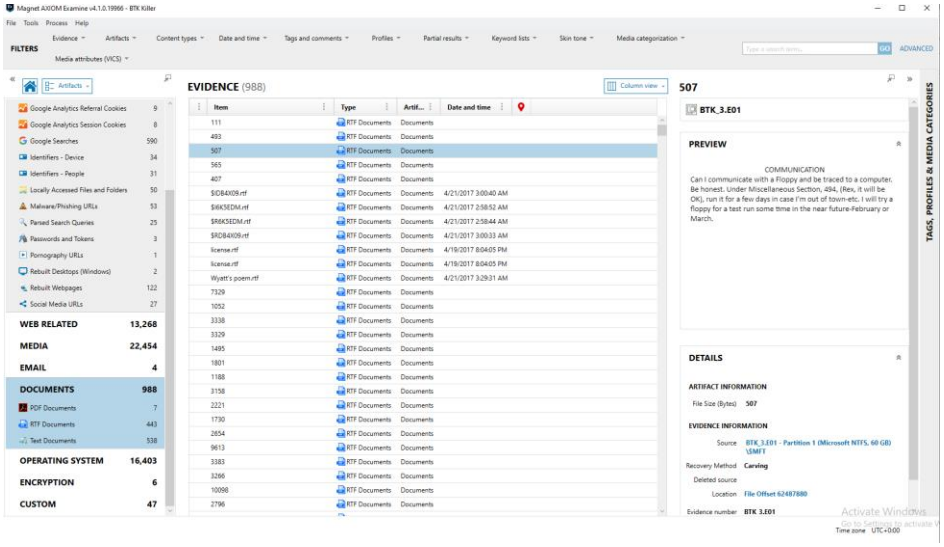


Figure 13.4

Figure 13.4 question about being traced with a floppy disk.

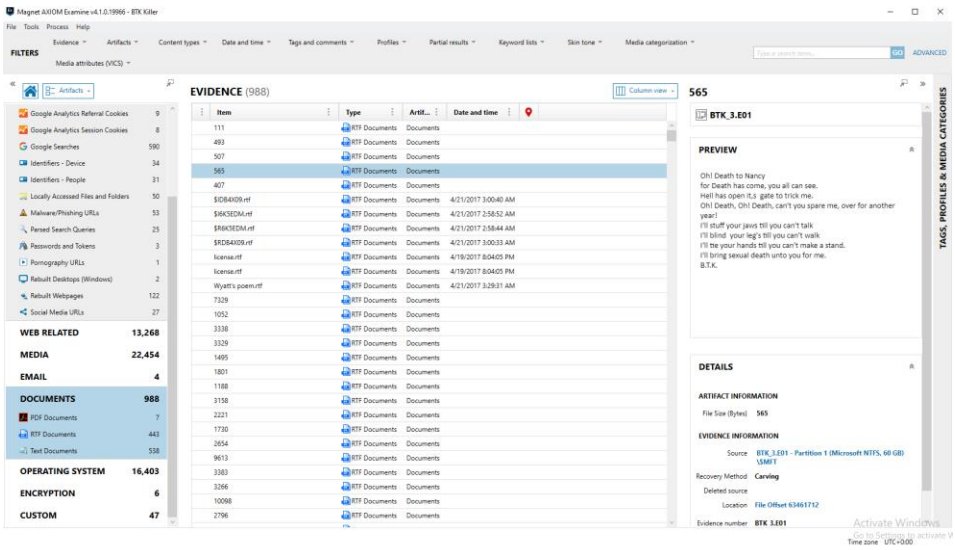


Figure 13.5

Figure 13.5 poem about Nancy by the BTK killer.

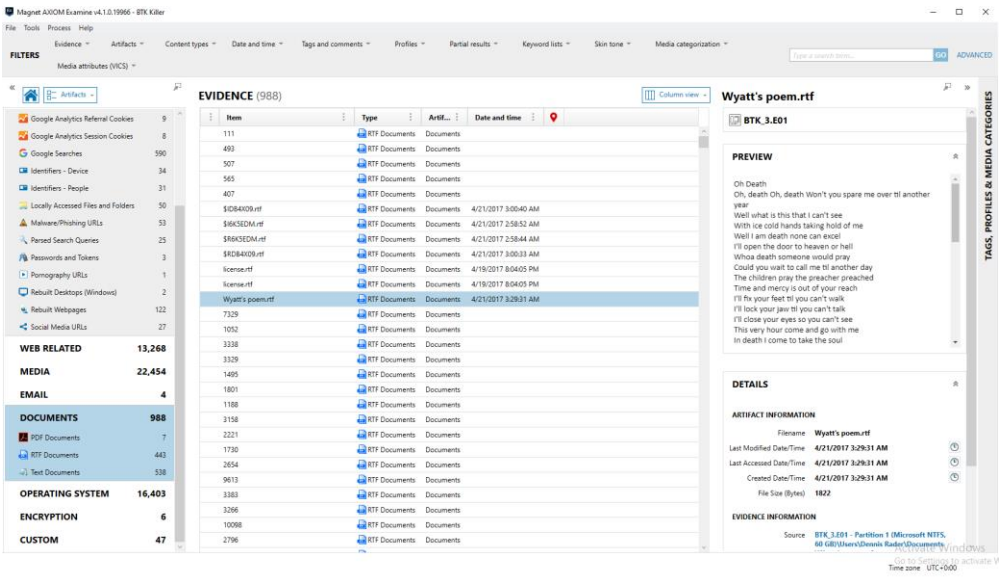


Figure 13.6

Figure 13.6 Another poem about death by the BTK killer.

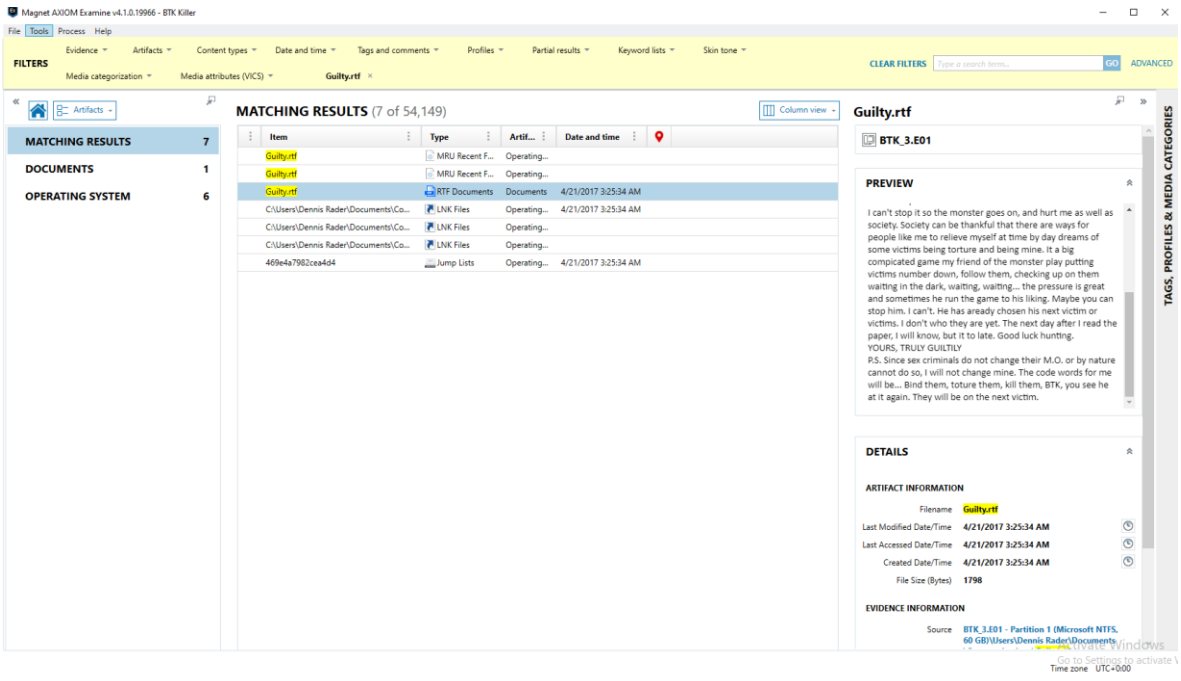


Figure 13.7

Figure 13.7 poem about being guilty by the BTK killer.

Encryption

This device does include encryption / anti-forensic tools. I was not able to access any of the six files that were encrypted.

Conclusion

The image of the hard drive that I took was around six gigabytes of information to process in both AXIOM Process, and Forensic Explorer.

The suspect in this case was Dennis Rader or the BTK Killer. From the device that we seized legally from the BTK killers' home, there are multiple evidence files on the device. The computer name was the default one provided during installation of WIN-NGU8PA7DBCG. The computer owner information however belonged to Autumn Pelkey.

When looking through the registry data with Forensic Explorer, there are multiple evidence points that gave reason to believe that this laptop was the BTK killers. One of the user names was Dennis Rader. The time zone was set in Eastern Standard Time but the current evidence suggests they are in Kansas which runs on Central Standard Time.

When looking through AXIOM Examine there was numerous search results in Internet Explorer and Google Chrome relating to strangulation, ropes, how to kill quietly, victim names of the BTK killer, guns, weapons, plastic bags, and other search results based on or around the BTK killer. There were also more obscure search results such as christianityoasis.com and thebarbiecollection.com. There is no clear connection between these but there were also pictures relating to barbie dolls.

Looking at AXIOM Examine there is many photographs relating to each of these items of interest. There were dozens of photographs of ropes, knots, and various other uses for it in possible strangulation means or to tie up his victims. There were pictures of plastic bags, including pictures of using these plastic bags on his victims. There were images of guns. Furthermore, there were dozens of images of Dennis Rader, images of the BTK killer crime

scenes, pictures of his victims being mutilated, tortured, along with other illegal activities. There were also pictures of victims with tape around their legs and their hands tied up with knots. Furthermore, there were many images relating to Dennis Rader actively searching for information about the BTK killer, including his victims, the family of his victims, crime scenes, news articles, and other media content relating to it.

There were also Rtf files about the BTK killer. These included various poems located within the device. It is not clear whether these letters or poems were letters to his victims, to himself, or any other fixation. There was one particular rtf document which stood out and that was “Guilty.rtf” which talks about how the other suspects are just doing it for attention and he has the help of no-one and that there is a possible monster in his head and he cannot get help for it.

There seems to also be a common picture found within AXIOM of a possible signature that belongs to him at the crime scenes. It seems to represent the letters B.T.K.

This case in general was very interesting. Dennis Rader seemed to want to be caught based on the letters, the google results, and the floppy disk. Furthermore, he wanted to communicate with the police without being caught, so it was not a clean-cut confession. This also proves a sign of guilt though.

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