Digital Forensics Investigation Report

Portfolio Sample

Will Kittredge

TABLE OF CONTENTS

BTK Final Investigation 3
Introduction 3
Imaging Process 4
Active File Review 7
Registry Data 10
Image and Video Analysis 21
Document Analysis 26
Internet Artifacts 32
Cached Images 32
Web Browsing 43
AXIOM Carved Cached Images 47
Deleted Material 54
Conclusion 59
References 61

BTK Final Investigation

Introduction

Dennis Rader, otherwise known as BTK (for "bind, torture, kill"), is an American serial killer known to have at least ten victims – most of them women. Rader was apprehended in 2005 after investigators were able to trace evidence discovered in the metadata of a Microsoft Word document back to him; this eventually led to the police obtaining incriminating DNA evidence (as testing revealed that Rader's daughter had DNA which closely matched that of BTK). BTK had been in communication with the police, who assured him that nothing could be traced back to his identity if he wanted to communicate with them via files stored on a floppy disk. Unbeknownst to Rader, investigators had the ability to recover the Word document that contained the metadata critical to their breakthrough in the case – despite him having deleted it. As discussed during class, the BTK case is considered significant in the history of the digital forensics field.

This report details the findings of a mock investigation assignment based on the real BTK case. The goal was to locate digital evidence that supports the conclusion of Dennis Rader being BTK. A forensic image file was provided in place of a physical drive, although they are functionally the same for the purposes of this assignment. The imaged file (which contains fabricated evidence) was examined using the forensic tools FTK Imager, Forensic Explorer, and Magnet AXIOM. Each piece of evidence that was located using the forensic software is presented and analyzed in this report. After all evidence artifacts have been presented, a conclusion is formulated at the end of the report.

Imaging Process

It is considered bad practice to work directly with original digital evidence. Instead, a forensic image of the original evidence should be captured and used as the working copy. A forensic image is a verifiable bit-for-bit copy of the information on a device (Gogolin, 2021, p. 33). Although a forensic image file was already provided for this assignment, it was treated like a physical drive (for educational purposes). This means that a forensic image must still be created from the already provided one, as that is our "original" in this scenario.

The forensic software FTK Imager was used to create a working-copy forensic image. As part of the image creation process, FTK Imager runs `MD5` and `SHA-1` hashing algorithms against both the original and the copy. A hashing algorithm creates a unique digital footprint from source data; furthermore, these "footprints" are fixed in length and cannot be reversed to determine what the original dataset was. Essentially, two files can only have identical hashes if they contain exactly the same data (Ciampa, 2017, p. 193). If FTK Imager finds that the hash of the original image and the working-copy image are the same, then we can be sure that the data contained in both is the same.

The `Create Disk Image` wizard was configured with the appropriate settings to create a new forensic image from an already existing one (see **Figure 1**). After the correct settings were configured, the imaging process was started. Upon completion of the imaging process, FTK Imager will display a summary of the results (see **Figure 2**) and save a complete report to a text file. A full copy of the report is visible on page 6. According to the results summary and the report, the copy forensic image is an exact duplicate of the provided one. At this point, the image file can now be loaded into other forensic software for processing and analysis.

Figure 1

FTK Imager: Create Disk Image Wizard

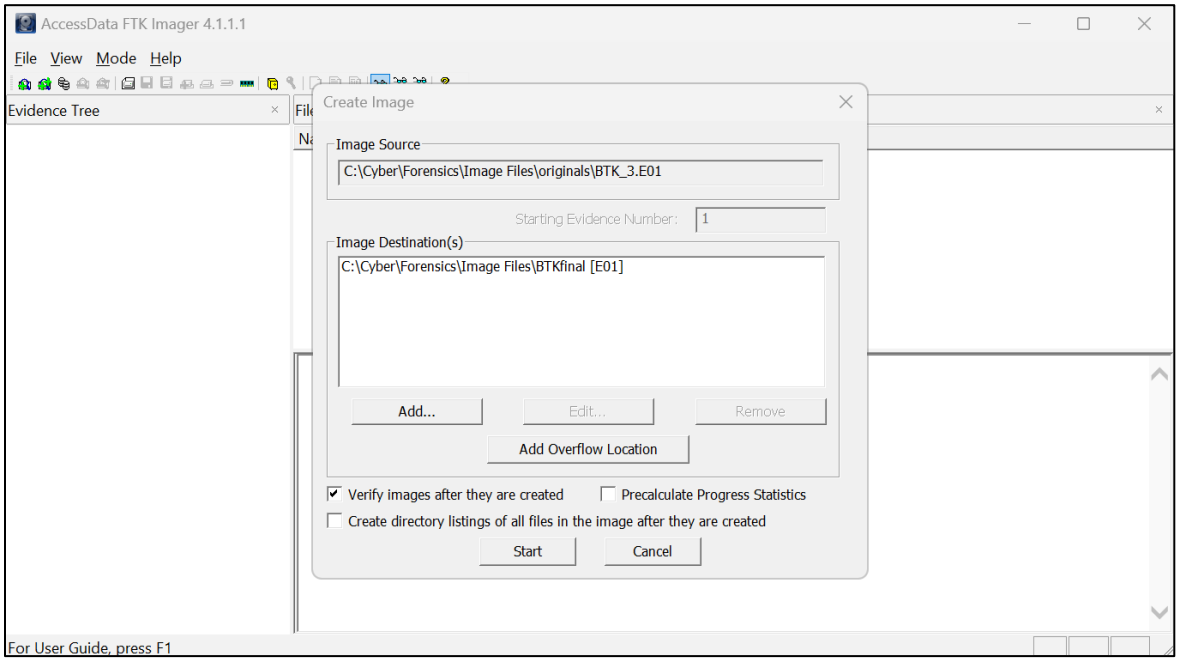
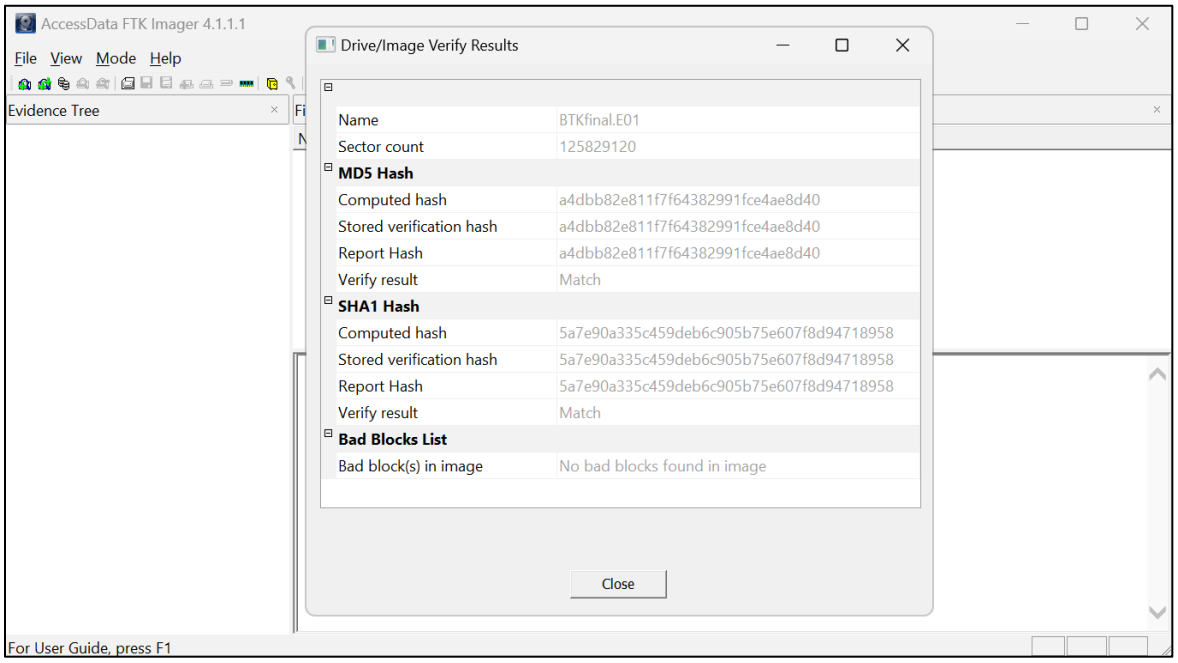


Figure 2

FTK Imager: Image Creation Results Summary



```
Created By AccessData® FTK® Imager 4.1.1.1

Case Information:
Acquired using: ADI4.1.1.1
Case Number: BTKfinal
Evidence Number: 0001
Unique description: A forensic image of BTK's hard drive
Examiner: Will Kittredge
Notes: Final exam practical

---------------------------------------------------------------

Information for C:\Cyber\Forensics\Image Files\BTKfinal:

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:   Thu Apr 18 22:08:47 2024
 Acquisition finished:  Thu Apr 18 22:11:50 2024
 Segment list:
  C:\Cyber\Forensics\Image Files\BTKfinal.E01

Image Verification Results:
 Verification started:  Thu Apr 18 22:11:50 2024
 Verification finished: Thu Apr 18 22:15:01 2024
 MD5 checksum:    a4dbb82e811f7f64382991fce4ae8d40 : verified
 SHA1 checksum:   5a7e90a335c459deb6c905b75e607f8d94718958 : verified
```

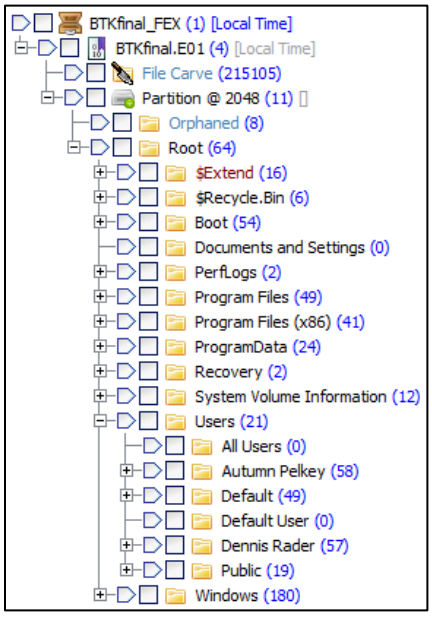
Active File Review

For this investigation, Forensic Explorer (FEX) was the primary forensic tool used to locate and examine evidence artifacts – though Magnet AXIOM was also utilized to gain an overview-level understanding of the evidence using its Artifacts and Media explorers. Within FEX, the File System, Artifacts, and Registry modules were used to further examine the image file as a whole and the artifacts identified by AXIOM.

Based on the structure and names of the folders (e.g., `Users` folder, an empty `Documents and Settings` folder) viewable in the File System module of FEX, the original forensic image appears to have been captured from a machine what was running at least Windows Vista (see **Figure 3**). This is supported by evidence presented later in the Registry Data section of this report. Nearly all of the evidence presented in this report comes from subfolders of the `Dennis Rader` user folder. In total, 50* significant artifacts were identified.

Figure 3

FEX: File System Module Folder Tree



Due to the nature of portions of the evidence (e.g., cached Internet images and Internet search history entries), some artifacts have been excluded from the total. Reasons for this include an overwhelming amount of them existing, the artifacts not having assigned filenames, or because I did not consider them as meaningfully different from previously identified artifacts. However, many excluded artifacts are still mentioned and/or visible in the Internet Artifacts section of this report; these artifacts are mainly ones that were only viewable in AXIOM.

Assume [Dennis Rader] folders to represent:

`\Root\Users\Dennis Rader`

Assume [IE Cache] folders to represent:

`[Dennis Rader]\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5`

Assume [Chrome Cache] folders to represent:

`[Dennis Rader]\AppData\Local\Google\Chrome\User Data\Default\Cache`

EVIDENCE ARTIFACTS TABLE		
#	**FILENAME**	**LOCATION**
01	Floppy.rtf	[Dennis Rader]\Documents\Communications\
02	Guilty.rtf	[Dennis Rader]\Documents\Communications\
03	How many.rtf	[Dennis Rader]\Documents\Communications\
04	Otero Family.rtf	[Dennis Rader]\Documents\Communications\
05	Shirley's Kids.rtf	[Dennis Rader]\Documents\Communications\
06	basic_knots.jpg	[Dennis Rader]\Documents\Kit\
07	filmcamera.jpg	[Dennis Rader]\Documents\Kit\
08	knife.jpg	[Dennis Rader]\Documents\Kit\
09	plasticbag-244x300.png	[Dennis Rader]\Documents\Kit\
10	rope.jpg	[Dennis Rader]\Documents\Kit\
11	springfield_armory_xd.jpg	[Dennis Rader]\Documents\Kit\
12	Project List.rtf	[Dennis Rader]\Documents\PL\
13	Death to Nancy.rtf	[Dennis Rader]\Documents\Poems\
14	Oh Anna Why Didn't You Appear.rtf	[Dennis Rader]\Documents\Poems\
15	Photo Diary.jpg	[Dennis Rader]\Pictures\
16	Yours Truly.jpg	[Dennis Rader]\Pictures\
17	Death.rtf	*N/A; Recovered/carved from disk*
18	anna.rtf	*N/A; Recovered/carved from disk*
19	Carved_JPG_63830984.jpg	*N/A; Recovered/carved from disk*
20	Carved_JPG_63831504.jpg	*N/A; Recovered/carved from disk*
21	Carved_JPG_63831632.jpg	*N/A; Recovered/carved from disk*
22	Carved_JPG_63831688.jpg	*N/A; Recovered/carved from disk*
23	Carved_JPG_63831816.jpg	*N/A; Recovered/carved from disk*
24	Carved_JPG_63831984.jpg	*N/A; Recovered/carved from disk*

EVIDENCE ARTIFACTS TABLE (CONTINUED)		
#	FILENAME	LOCATION
25	images[1].jpg	[IE Cache]\5JD6EV4A\
26	images[3].jpg	[IE Cache]\5JD6EV4A\
27	images[4].jpg	[IE Cache]\5JD6EV4A\
28	images[5].jpg	[IE Cache]\5JD6EV4A\
29	images[9].jpg	[IE Cache]\5JD6EV4A\
30	images[2].jpg	[IE Cache]\EGME2FHO\
31	images[5].jpg	[IE Cache]\EGME2FHO\
32	images[1].jpg	[IE Cache]\ERJIN6Q0\
33	images[2].jpg	[IE Cache]\ERJIN6Q0\
34	images[4].jpg	[IE Cache]\ERJIN6Q0\
35	images[10].jpg	[IE Cache]\ERJIN6Q0\
36	56e5bc7585b86.image[1].jpg	[IE Cache]\HFJN9M5H\
37	images[3].jpg	[IE Cache]\HFJN9M5H\
38	images[4].jpg	[IE Cache]\HFJN9M5H\
39	images[5].jpg	[IE Cache]\HFJN9M5H\
40	f_000045	[Chrome Cache]\
41	f_000132	[Chrome Cache]\
42	f_000134	[Chrome Cache]\
43	f_000114	[Chrome Cache]\
44	f_000116	[Chrome Cache]\
45	f_00011f	[Chrome Cache]\
46	f_000108	[Chrome Cache]\
47	f_00010a	[Chrome Cache]\
48	f_00010b	[Chrome Cache]\
49	f_0000d3	[Chrome Cache]\
50	f_000146	[Chrome Cache]\

Registry Data

Using the Registry module within FEX, the `SAM`, `SOFTWARE`, and `SYSTEM` registry hives, along with the `Dennis Rader` user's `NTUSER.DAT` file, were analyzed. Generally speaking, `SAM` contains user account information (machine-wide), `SOFTWARE` contains information about software installed on the machine (from the operating system or otherwise), `SYSTEM` contains information about the machine itself, and `NTUSER.DAT` contains information about a specific user (there is one `NTUSER.DAT` for every user). Analysis of these files revealed some evidence relevant to the case, but also some other information that I do not believe accurately reflects what one would expect to find during registry analysis of a real suspect or victim machine in the context of this case. This is due to the nature of the assignment as the forensic image file is a fabrication, however, I think it is still worthwhile to note these findings. Registry artifacts that are relevant to the case are presented in **Figure 4-Figure 6**, while the other artifacts are presented in **Figure 7**-**Figure 13**. Any comments on these findings are included in a note below their respective Figure.

Figure 4

FEX: NT USER Hive Explorer Recent Docs MRU (partial)

```
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:
BTKfinal.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
```

Note. The `Dennis Rader` user has recently accessed files and folders that contain evidence.

Figure 5

FEX: NT USER Hive Last Visited

```
Search for:
NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVis
itedMRU

Description:        Folder paths to recently used executable files.

Reference:          http://computer-
forensics.sans.org/blog/2010/04/02/openrunsavemru-lastvisitedmru/

================================================================================

Key Found:
BTKfinal.E01\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer
\ComDlg32\LastVisitedPidlMRU\


  Value               Data

  ~~~~~               ~~~~

  0                   {B5E83989-4076-4ED0-A33E-9B8E9870B07F},System Folder

  1                   chrome.exe,System Folder

  MRUListEx           0 1

--------------------------------------------------------------------------------

Registry Key Processor finished
```

Note. The Google Chrome executable (`chrome.exe`) was recently used by the `Dennis Rader` user. This is relevant because search history and cached content from the Google Chrome browser was discovered. That evidence is discussed in the Internet Artifacts section of this report.

Figure 6

FEX: SAM Hive Local Users (partial)

```
\\\
```

Figure 7

FEX: SYSTEM Hive Computer Name

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

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

Reference:          None.

=========================================================================

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


  Value                                         Data

  ~~~~~                                         ~~~~

  ComputerName                                  WIN-NGU8PA7DBCG

-------------------------------------------------------------------------

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


  Value                                         Data

  ~~~~~                                         ~~~~

  ComputerName                                  WIN-NGU8PA7DBCG

-------------------------------------------------------------------------

Registry Key Processor finished.
```

Note. The computer has a generic hostname.

Figure 8

FEX: SYSTEM Hive Disk Storage Devices

```
Search for:          SYSTEM\ControlSet###\Enum\SCSI\

Description:         Hard drives.

Reference:           None.

=========================================================================

Key Found:
BTKfinal.E01\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_VMware_&Prod_VMware_V
irtual_S\5&22be343f&0&000000\


  Value                          Data

  ~~~~~                          ~~~~

  FriendlyName                   VMware, VMware Virtual S SCSI Disk Device

-------------------------------------------------------------------------

Key Found:
BTKfinal.E01\SYSTEM\ControlSet002\Enum\SCSI\Disk&Ven_VMware_&Prod_VMware_V
irtual_S\5&22be343f&0&000000\


  Value                          Data

  ~~~~~                          ~~~~

  FriendlyName                   VMware, VMware Virtual S SCSI Disk Device

-------------------------------------------------------------------------

Registry Key Processor finished.
```

Note. There is a record of VMware virtual disks in the registry. I believe that this might indicate the original forensic image was captured from a virtual machine.

Figure 9

FEX: SYSTEM Hive Time Zone (partial)

```
Search for:          SYSTEM\ControlSet###\Control\TimeZoneInformation\
Description:         The time zone setting.
Reference:           None.
================================================================================
Key Found:
BTKfinal.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
```

Note. The time zone is set to Eastern. The expected time zone for this case would be Central.

Figure 10

FEX: SYSTEM Hive USB Storage 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.
```

Note. There is no record of USB storage devices being attached to the machine. This is entirely possible, but I believe it would be unusual. However, Rader was ultimately caught in real life due to using a floppy disk – so maybe his personal computer did not have USB ports, or he did not own any USB devices.

Figure 11

FEX: SOFTWARE Hive Default User Name

```
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:      BTKfinal.E01\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\


  Value                                         Data

  ~~~~~                                         ~~~~

  DefaultUserName                               Autumn Pelkey

--------------------------------------------------------------------------

Registry Key Processor finished.
```

Note. The default user is `Autumn Pelkey`. A Google search and LinkedIn profile reveal that this was a former Ferris State University MISI student with digital forensics experience, and therefore is possibly the creator of the original forensic image.

Figure 12

FEX: SOFTWARE Hive Product Name and ID

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

Description:        The name of the Operating System.

Reference:          None.

==========================================================================

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


  Value                         Data

  ~~~~~                         ~~~~

  ProductId                     00346-339-0000007-85733

  ProductName                   Windows 7 Home Basic

  BuildLabEx                    7601.17514.amd64fre.win7sp1_rtm.101119-1850

--------------------------------------------------------------------------

Registry Key Processor finished.
```

Note. The operating system of the machine was Windows 7, which did not exist at the time of Dennis Rader's arrest in 2005 (Microsoft, n.d.).

Figure 13

FEX: SOFTWARE Hive Registered Owner\Organization

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

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

Reference:          None.

==========================================================================

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


  Value                                         Data

  ~~~~~                                         ~~~~

  RegisteredOwner                               Windows User

  RegisteredOrganization

--------------------------------------------------------------------------

Registry Key Processor finished.
```

Note. The registered owner (`Windows User`) is generic. This is possible (the registered owner of my Windows PC is `Admin`, for example), but I believe it would be unlikely in the case of Dennis Rader.

Image and Video Analysis

Using the File System module within FEX, the forensic image file was searched for any images or videos that could be relevant to the case. In total, eight relevant images were discovered (see **Figure 14**-**Figure 21**) in subfolders of the `Dennis Rader` user folder (those being `[Dennis Rader]\Pictures\` and `[Dennis Rader]\Documents\Kit\`). Due to their locations within the filesystem, it is likely that these images would have been intentionally saved to these locations by Rader himself. Any comments on these findings are included in a note below their respective Figure.

Figure 14

filmcamera.jpg

Note. An image of a film camera. In the Deleted Material section of this report, recovered pictures of BTK victims that appear to have been taken by a film camera are presented. It is possible that those pictures could have been taken using this camera.

Figure 15

Photo Diary.jpg

Note. Dennis Rader has photos of BTK victims in a file called `Photo Diary`. This could suggest that Rader is BTK and that he is keeping a "diary" of his victims.

Figure 16

Yours Truly.jpg

Note. Dennis Rader has an image of BTK's signature with the filename `Yours Truly` on his computer. This could suggest that Dennis Rader has used BTK's signature to sign-off letters, which would support the conclusion that he is BTK.

Figure 17

springfield_armory_xd.jpg

Note. Rader has an image of a handgun saved to his computer. BTK is known to have held victims at gunpoint (Previch, 2004).

Figure 18

knife.jpg

Note. Rader also has an image of a knife saved to his computer. BTK is known to have stabbed victims (Previch, 2004).

Figure 19

rope.jpg

Note. Rader has an image of rope saved to his computer. There's nothing suspicious about this by itself, but it does not look good in the context of other evidence. The "B" in "BTK" stands for bind (as in binding someone), which is what one could use rope to do.

Figure 20

basic_knots.jpg

Note. Rader has images of knots on his computer. The connection between rope, knots, and binding is obvious.

Figure 21

plasticbag-244x300.png

Note. Rader has an image of a plastic bag saved to his computer. BTK is known to have put plastic bags over his victim's heads. The files `Otero Family.rtf` and `Shirley's Kids.rtf` presented in the Document Analysis section of this report mention the use of these bags. One of these documents is signed with " - `BTK`" at the end.

Document Analysis

Using the File System module within FEX, the forensic image file was searched for any documents that could be relevant to the case. In total, eight relevant documents were discovered (see **Figure 22-Figure 29**) in subfolders of the `Dennis Rader` user folder (those being `[Dennis Rader]\Documents\Communications\`, `[Dennis Rader]\Documents\PL\`, and `[Dennis Rader]\Documents\Poems\`). Like the images in the previous section, I think it is likely that these documents were intentionally saved to these locations by Rader himself due to their locations within the filesystem. Any comments on these findings are included in a note below their respective Figure.

Figure 22

Death to Nancy.rtf

```
Oh! Death to Nancy
What is this taht  I can see
Cold icy hands taking hold of me
for Death has come, you all can see.
Hell has open it,s  gate to trick me.
Oh! Death, Oh! Death, can't you spare me, over for another year!
I'll stuff your jaws till you can't talk
I'll blind  your leg's till you can't walk
I'll tie your hands till you can't make a stand.
And finally I'll close your eyes so you can't see
I'll bring sexual death unto you for me.
B.T.K.
```

Note. Rader has a poem that is likely referring to Nancy Fox, a BTK victim, on his computer.

Figure 23

Floppy.rtf

```
                                COMMUNICATION



Can I communicate with a Floppy and be traced to a computer. Be honest.
Under Miscellaneous Section, 494, (Rex, it will be OK), run it for a few
days in case I'm out of town-etc. I will try a floppy for a test run some
time in the near future-February or March.
```

Note. Rader has a copy of a communication from BTK on his computer where BTK asks if it is safe to use a floppy disk without it being traced back to his real identity. In the Deleted Material section of this report, a photocopy/scan of this document that was carved from the disk is presented.

Figure 24

How many.rtf

```
How many do I have to kill, before I get my name in the paper or some
national attention?  Do the cops think that all those deaths are not
related? Yes, the M.O. is different in each, but look at the pattern that
is developing. The victims are tied up _ most have been women _ phone cut
_ bring some bondage mater sadist tendencies _ no struggle, outside the
death spot _ no witnesses except the Vian's kids...



After a thing like Fox, I come home and go about life like anyone else.
And I will be like that until the urge hits me again...
```

Note. Another BTK communication that Rader has saved on his computer. “Fox” is likely referring to the BTK victim Nancy Fox.

Figure 25

Guilty.rtf

I write this letter to you for the sake of the tax payer as well as your time. Those three dude you have in custody are just talking to get publicity for the Otero murders. They know nothing at all. I did it by myself and with no ones help. There has been no talk either. Let's put this straight... .

I'm sorry this happen to society. They are the ones who suffer the most. It hard to control myself. You probably call me 'psychotic with sexual perversion hang-up.' When this monster enter my brain I will never know. But, it here to stay. How does one cure himself? If you ask for help, that you have killed four people they will laugh or hit the panic button and call the cops.

I can't stop it so the monster goes on, and hurt me as well as society. Society can be thankful that there are ways for people like me to relieve myself at time by day dreams of some victims being torture and being mine. It a big compicated game my friend of the monster play putting victims number down, follow them, checking up on them waiting in the dark, waiting, waiting... the pressure is great and sometimes he run the game to his liking. Maybe you can stop him. I can't. He has aready chosen his next victim or victims. I don't who they are yet. The next day after I read the paper, I will know, but it to late. Good luck hunting.

YOURS, TRULY GUILTILY

P.S. Since sex criminals do not change their M.O. or by nature cannot do so, I will not change mine. The code words for me will be... Bind them, toture them, kill them, BTK, you see he at it again. They will be on the next victim.

Note. BTK takes responsibility for multiple murders in this document. It is suspicious that Rader would have a copy of this on his computer.

Figure 26

Oh Anna Why Didn't You Appear.rtf

```
Oh, Anna Why Didn't You Appear

T' was perfect plan of deviant pleasure so bold on that Spring niteMy
inner felling hot with propension of the new awakening season

Warn, wet with inner fear and rapture, my pleasure of entanglement,like
new vines at night

Oh, Anna, Why Didn't You AppearDrop of fear fresh Spring rain would roll
down from your nakednessto scent to lofty fever that burns within,

In that small world of longing, fear, rapture, and desparation,the game we
play, fall on devil earsFantasy spring forth, mounts, to storm fury, then
winter clam atthe end.

Oh, Anna Why Didn't You AppearAlone, now in another time span I lay with
sweet enrapture garmentsacross most private thought

Bed of Spring moist grass, clean before the sun, enslaved withcontrol,
warm wind scenting the air, sun light sparkle tearsin eyes so deep and
clear.

Alone again I trod in pass memory of mirrors, and ponder why fornumber
eight was not.

Oh, Anna Why Didn't You Appear
```

Note. Another poem. Anna was a victim that BTK planned to kill, but she evaded him.

Figure 27

Shirley's Kids.rtf

```
They were very lucky; a phone call saved them. I was going to tape the
boys and put plastic bags over there heads like I did Joseph and Shirley -
and then hang the girl. God-oh God what a beautiful sexual relief this
would been
```

Note. Rader has a document on his computer detailing how BTK feels about not getting to kill Shirley's three children, and how he would have felt if he did.

Figure 28

Otero Family.rtf

Date: January 17, 1974

Location of Package: Stop sign at First and Kansas

I killed the Otero family on January 15, 1974 at their home. How, you wonder? I'll tell you.

I'd watched them carefully for some time, and then on the night of January 15, 1974, I snuck up to their detached garage. I saw dog prints outside the house, so I waited. At around 8:40 PM, the young boy unlocked the door and stepped outside.

It was time. I pulled my .22 gun on him and ordered him back inside. The family was inside, and I showed them my knife and gun, telling them it was a robbery and to cooperate. Josephine started to cry and the dog started barking obnoxiously.

After the dog was let out, I moved all four of them to a bedroom. There, I put bags over Joseph and the young boy. Finally, I used my rope to strangle Julie.

Josephine was next. I took my time with her and merely strangled her just enough to make her pass out. Then, I took her down to the basement and tied her to a sewer pipe. I had a bit more fun with her before finally killing her.

Joseph and young Joseph were next.

Now, they're all in heaven.

- BTK

Note. Rader has a document on his computer detailing how BTK committed the Otero family murders.

Figure 29

Project List.rtf

```
Julie Otero
Josephine Otero
Ashley Johnson
Katherine Bright
Kendra Smith
Sophia Delgado
Anna Williams
Kaylee Fisher
Shirley Vian
Nancy Fox
Anne Landing
Holi Johnson
Marine Hedge
Maria Perez
Vicky Wagerly
Delores Davis
Katherine Davis
```

Note. Rader has a list of names on his computer. Every victim known to have been killed by BTK is in this list, save for Joseph Otero and Joseph Otero Jr. All of these names seem to be women's names, which match what is known about BTK's motives.

Internet Artifacts

Internet artifacts in the form of Internet Explorer/Google Chrome search history and cached images were discovered in the forensic image file using the File System and Artifact modules within FEX. These evidence artifacts are organized into subsections in this report. Images are under the Cached Images subsection, while Internet searches are under the Web Browsing subsection. Additionally, there are some cached images that were not visible within FEX. These images are viewable in the AXIOM Carved Cached Images subsection in collections (rather than individually) due to the high number of them that exist.

Cached Images

A web browser cache is a performance feature that enhances the web browsing experience by saving parts of a webpage to a computer's disk so that the webpage loads faster when it is visited next (Google, 2024). In total, 26 relevant cached images (see **Figure 30-Figure 55**) were found in the Internet Explorer and Google Chrome browser caches using FEX. These could have been included in the Image and Video Analysis section of this report, but I believe that it makes more sense to classify cached images as Internet artifacts. Rather than commenting on each image individually, the images are organized into categories by Figure number and each category is then commented on.

CACHED IMAGES TABLE		
FIGURES	**CATEGORY**	**COMMENT**
30-43	Strangulation/ Suffocation Research	These images were likely cached when Rader was visiting webpages about strangulation or suffocation.
44-49	Binding Research	These images were likely cached when Rader was visiting webpages about binding and knots.
50-53	Weapons/Tools Research	These images were likely cached when Rader was visiting webpages about weapons and tools.
54 and 55	Miscellaneous	**See notes under figures*

Figure 30

56e5bc7585b86.image[1].jpg

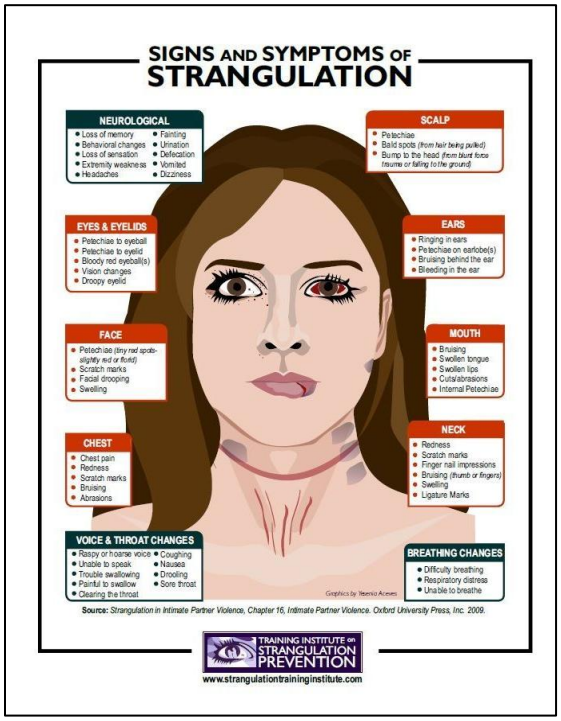


Figure 31

images[4].jpg (1)

Figure 32

images[5].jpg (1)

Figure 33

images[4].jpg (2)

Figure 34

images[4].jpg (3)

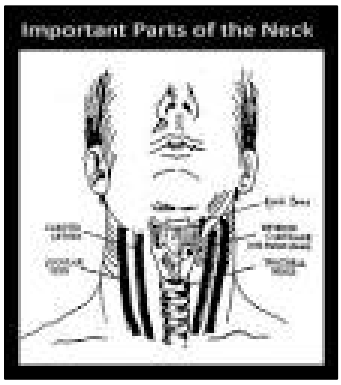


Figure 35

images[1].jpg (1)

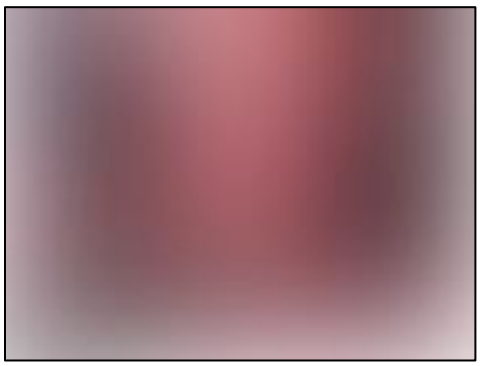


Figure 36

images[5].jpg (2)

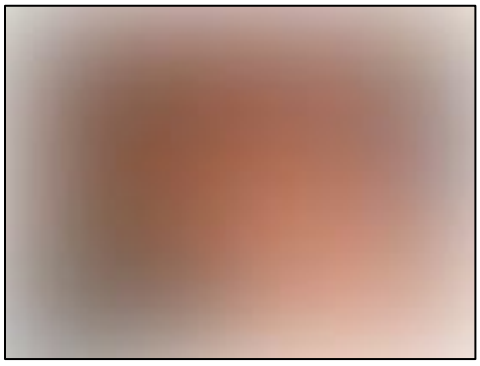


Figure 37

images[5].jpg (3)

Figure 38

images[2].jpg (1)

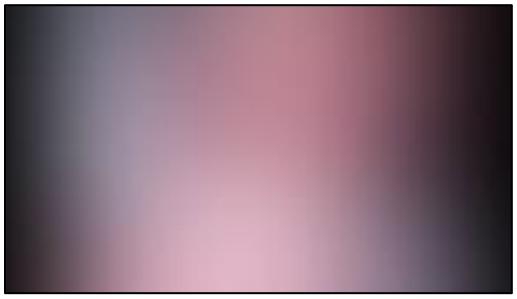


Figure 39

images[3].jpg (1)

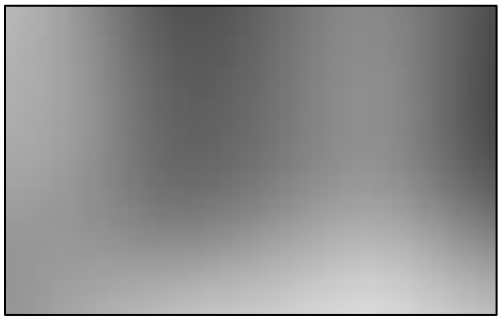


Figure 40

images[2].jpg (2)

Figure 41

images[3].jpg (2)

Figure 42

images[1].jpg (2)

Figure 43

f_00011f

Figure 44

f_000132

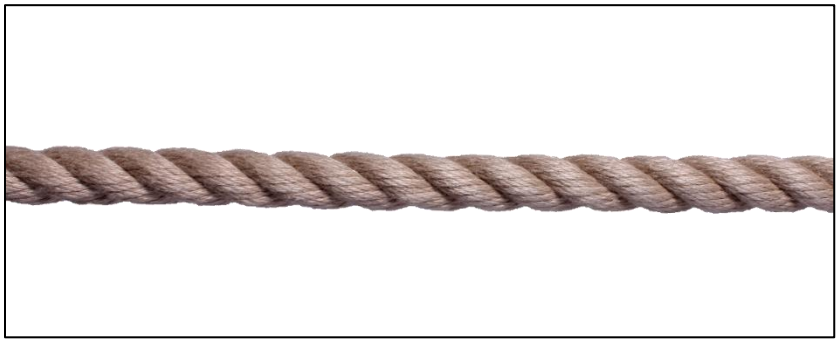


Figure 45

f_000134

Figure 46

images[10].jpg

Figure 47

f_000108

Figure 48

f_00010a

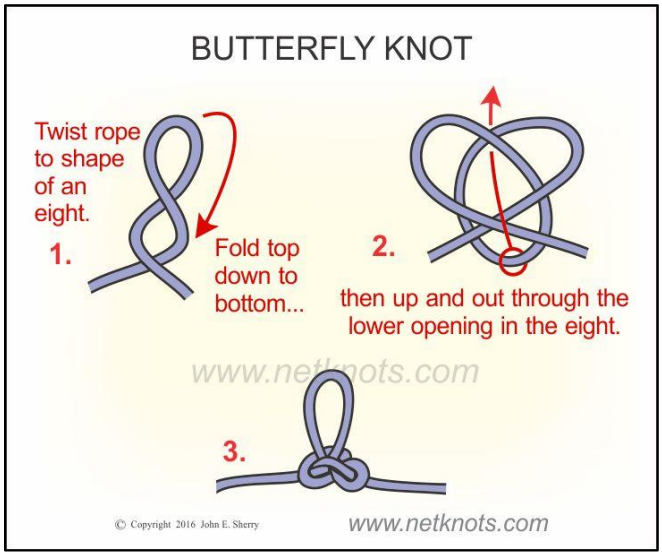


Figure 49

f_00010b

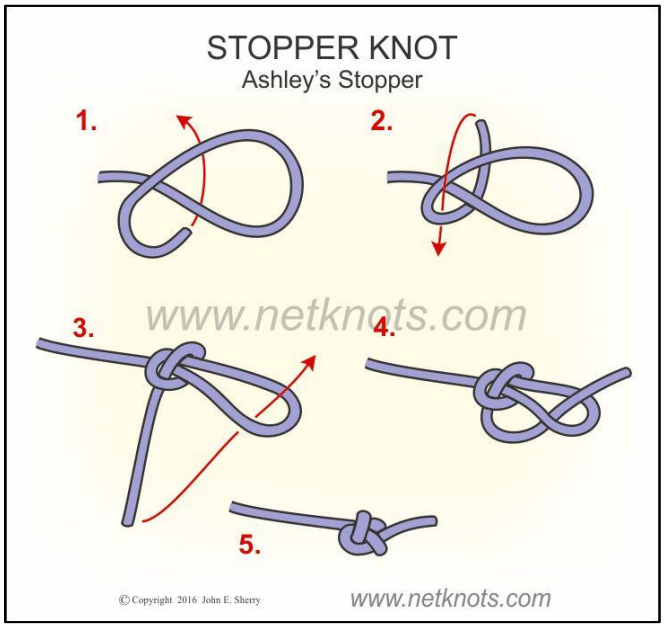


Figure 50

f_000114

Figure 51

f_000116

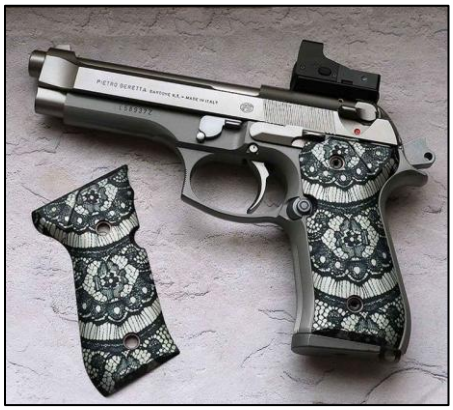


Figure 52

f_000146

Figure 53

images[9].jpg

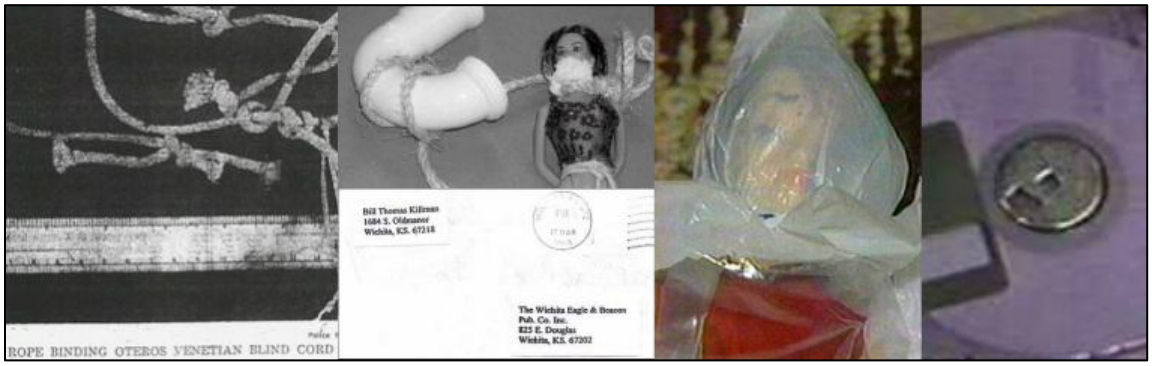
Figure 54

f_000045

Note. There were at least 20 other similar images of dolls in the Google Chrome cache located in a subfolder of the `Dennis Rader` user's home folder. BTK is known to have had dolls bound in ways that mimic his real-life victims.

Figure 55

f_0000d3



Note. A combined image of rope used in the Otero family murders, dolls bound and/or bagged, and the floppy disk that got BTK caught in real life.

Web Browsing

Using artifact processing scripts built into FEX, the forensic software can locate Internet search and browsing history data. As both Internet Explorer and Google Chrome were used, data was found for both of these browsers. FEX also attempts to extract Google queries from various different browsers and compile them into a single list. After FEX finished processing the web browsing data, it was exported into Microsoft Excel where extraneous and duplicate data was removed. Three detailing Google queries, Google Chrome browsing history, and Internet Explorer browsing history are visible on the next pages. From this data, we can see that Rader accessed various files that contain evidence, visited webpages related to torture or strangulation, researched silent killing methods, and made Google searches that are highly suspicious in the context of the case (e.g., “is a floppy disk anonymous” and “best ways to contact the police without getting caught”).

Google Queries.

Query	URL	Source
best ways to contact the police without getting caught	https://www.google.com/search?sclient=psy-ab&rlz=1C1CHBF_enUS741US741&espv=2&biw=1024&bih=662&q=best+ways+to+c	Browsers\Chrome Cache\
btk crime scene images	https://www.google.com/search?q=btk+crime+scene+images&rlz=1C1CHBF_enUS741US741&espv=2&source=lnms&tbm=isch&s	Browsers\Chrome History\
btk evidence	https://www.google.com/search?q=btk+evidence&rlz=1C1CHBF_enUS741US741&oq=btk+evidence&aqs=chrome..69i57.2360j0j7	Browsers\Chrome History\
btk victims	https://www.google.com/search?q=btk+victims&rlz=1C1CHBF_enUS741US741&espv=2&source=lnms&tbm=isch&sa=X&ved=0ah	Browsers\Chrome History\
guns	https://www.google.com/search?q=guns&rlz=1C1CHBF_enUS741US741&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjtz6D36Lb	Browsers\Chrome History\
is a floppy disk anonymous	https://www.google.com/search?q=is+a+floppy+disk+anonymous&oq=is+a+floppy+disk+anonymous&rlz=1C1CHBF_enUS741US7	Browsers\Chrome Cache\
ken lendwher	https://www.google.com/search?q=ken+lendwher&oq=ken+lendwher&rlz=1C1CHBF_enUS741US741&ie=UTF-8&aqs=chrome..69	Browsers\Chrome Cache\
knife	https://www.google.com/search?q=knife&rlz=1C1CHBF_enUS741US741&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjHgYTB6b	Browsers\Chrome History\
knot tying techniques	https://www.google.com/search?q=knot+tying+techniques&hl=en&gbv=2&oq=knot+tying+tec&gs_l=heirloom-serp.1.0.0j0i22i30l9	Browsers\Internet Explorer 4-9 URL (History)\
plastic bags	https://www.google.com/search?q=plastic+bags&rlz=1C1CHBF_enUS741US741&espv=2&source=lnms&tbm=isch&sa=X&ved=0a	Browsers\Chrome History\
quiet way to kill	https://www.google.com/search?q=quiet+way+to+kill&hl=en&gbv=2&source=lnms&sa=X&ved=0ahUKEwjlgLS5grHTAhWK6YMKHd	Browsers\Internet Explorer 4-9 URL (History)\
rope	https://www.google.com/search?q=rope&rlz=1C1CHBF_enUS741US741&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjp3dmX6b	Browsers\Chrome History\
rope tying knots	https://www.google.com/search?rlz=1C1CHBF_enUS741US741&espv=2&biw=1024&bih=662&tbm=isch&sa=1&q=rope+tying+kno	Browsers\Chrome Cache\
son of sam	https://www.google.com/search?sclient=psy-ab&rlz=1C1CHBF_enUS741US741&espv=2&biw=1024&bih=662&site=webhp&q=son	Browsers\Chrome Cache\
strangulation	https://www.google.com/search?q=strangulation&hl=en&gbv=2&prmd=ivns&source=lnms&tbm=isch&sa=X&ved=0ahUKEwj_kI2jg	Browsers\Internet Explorer 4-9 URL (History)\
ted bundy	https://www.google.com/search?sclient=psy-ab&rlz=1C1CHBF_enUS741US741&espv=2&biw=1024&bih=662&site=webhp&q=ted	Browsers\Chrome Cache\

Google Chrome Browsing History.

Title	URL	Last Visit Time	Visit Count	Source
joe otero - Google Search	https://www.google.com/#q=joe+otero	4/19/2017 17:17	1	History
how to strangle - Google Search	https://www.google.com/#q=how+to+strangle	4/19/2017 17:18	1	History
strangle - Google Search	https://www.google.com/#q=strangle	4/19/2017 17:18	1	History
Life and Death in Your Hands: Strangulation more co	https://www.strangulationtraininginstitute.com/life-and-death-in-your-hands-strangulation-more-common-in-domestic-abuse-cas	4/19/2017 17:19	1	History
torture - Google Search	https://www.google.com/#q=torture	4/19/2017 17:21	1	History
25 Most Brutal Torture Techniques Ever Devised In H	http://list25.com/25-most-brutal-torture-techniques-ever-devised/	4/19/2017 17:22	1	History
btk victims - Google Search	https://www.google.com/search?q=btk+victims&rlz=1C1CHBF_enUS741US741&espv=2&source=lnms&tbm=isch&sa=X&ved=0ah	4/21/2017 2:48	2	History
Activities	http://www.lutheranpioneers.org/activities.html	4/21/2017 3:01	1	History
Program Materials	http://www.lutheranpioneers.org/program.html	4/21/2017 3:01	1	History
servants in the afterlife - Google Search	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1CHBF_enUS741US741&ion=1&espv=2&ie=UTF-8#q=servants+	4/21/2017 3:03	1	History
BTK COMMUNICATIONS	http://www.christianityoasis.com/puritypublications/5003/BTK/BTKcommunications.htm	4/21/2017 3:23	1	History
KAKE.com | Wichita, Kansas News, Weather, Sports	http://www.kake.com/story/32113324/contact-us	4/21/2017 3:33	1	History
Dolls | The Barbie Collection	http://www.thebarbiecollection.com/shop	4/22/2017 0:22	1	History
Vintage Look Dolls | The Barbie Collection	http://www.thebarbiecollection.com/shop/vintage-look-dolls	4/22/2017 0:22	1	History
Fashion Dolls | The Barbie Collection	http://www.thebarbiecollection.com/shop/fashion-dolls	4/22/2017 0:23	1	History
Teresa® Doll and Shoes | for-girls | The Barbie Colle	http://www.thebarbiecollection.com/fashion-dolls/barbie-teresa-doll-shoe-dmp11	4/22/2017 0:23	1	History
btk evidence - Google Search	https://www.google.com/search?q=btk+evidence&rlz=1C1CHBF_enUS741US741&oq=btk+evidence&aqs=chrome..69i57.2360j0j7	4/22/2017 0:26	2	History
btk crime scene images - Google Search	https://www.google.com/search?q=btk+crime+scene+images&rlz=1C1CHBF_enUS741US741&espv=2&source=lnms&tbm=isch&s	4/22/2017 0:32	2	History
ROPE > Poly-Manila - WebRiggingSupply - Rope - Cal	http://webriggingsupply.com/pages/catalog/rope/poly-manila-rope-1.5inch.html?gclid=CICp65npttMCFQ2MaQodYJAIFA	4/22/2017 0:37	1	History
David Berkowitz - Murderer - Biography.com	http://www.biography.com/people/david-berkowitz-9209372	4/22/2017 0:45	1	History
best ways to contact the police without getting caugh	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1CHBF_enUS741US741&ion=1&espv=2&ie=UTF-8#q=best+way	4/22/2017 0:46	1	History

Internet Explorer Browsing History.

User	URL	Last Accessed (UTC)	Visit Count	Source
Dennis Rader	http://missoulian.com/search/?f=rss&t=article&c=news/local&l=50&s=start_time&sd=desc	4/19/2017 17:13	1	index.dat
Dennis Rader	http://missoulian.com/news/local/law-enforcement-medical-officials-discuss-increase-in-strangulation/article_90cf117e-2c42-	4/19/2017 17:13	5	index.dat
Dennis Rader	http://www.escapistmagazine.com/rss/news	4/19/2017 17:14	1	index.dat
Dennis Rader	http://www.escapistmagazine.com/forums/read/18.306368-the-REAL-way-to-make-a-silent-kill?page=2	4/19/2017 17:14	5	index.dat
Dennis Rader	http://www.animatedknots.com/indexbasics.php	4/19/2017 17:15	5	index.dat
Dennis Rader	file:///C:/Users/Dennis%20Rader/Documents/Communications/Otero%20Family.rtf	4/19/2017 17:43	1	index.dat
Dennis Rader	file:///C:/Users/Dennis%20Rader/Documents/Communications/How%20many.rtf	4/22/2017 0:28	1	index.dat
Dennis Rader	file:///C:/Users/Dennis%20Rader/Documents/Communications/Shirley's%20Kids.rtf	4/22/2017 0:30	1	index.dat
Dennis Rader	file:///C:/Users/Dennis%20Rader/Documents/Kit/basic_knots.jpg	4/22/2017 0:33	1	index.dat
Dennis Rader	file:///C:/Users/Dennis%20Rader/Documents/Kit/springfield_armory_xd.jpg	4/22/2017 0:36	1	index.dat
Dennis Rader	file:///C:/Users/Dennis%20Rader/Documents/Kit/plasticbag-244x300.png	4/22/2017 0:36	1	index.dat
Dennis Rader	file:///C:/Users/Dennis%20Rader/Documents/Kit/rope.jpg	4/22/2017 0:37	1	index.dat
Dennis Rader	file:///C:/Users/Dennis%20Rader/Documents/Kit/filmcamera.jpg	4/22/2017 0:38	1	index.dat
Dennis Rader	file:///C:/Users/Dennis%20Rader/Documents/Kit/knife.jpg	4/22/2017 0:38	1	index.dat
Dennis Rader	file:///C:/Users/Dennis%20Rader/Documents/PL/Project%20List.rtf	4/22/2017 0:43	1	index.dat

AXIOM Carved Cached Images

The following cached images were only viewable in AXIOM. They exist in high numbers and therefore have been organized into loose categories and presented in groups (see **Figure 56-Figure 64**).

Figure 56

Torture-Related Cached Images.

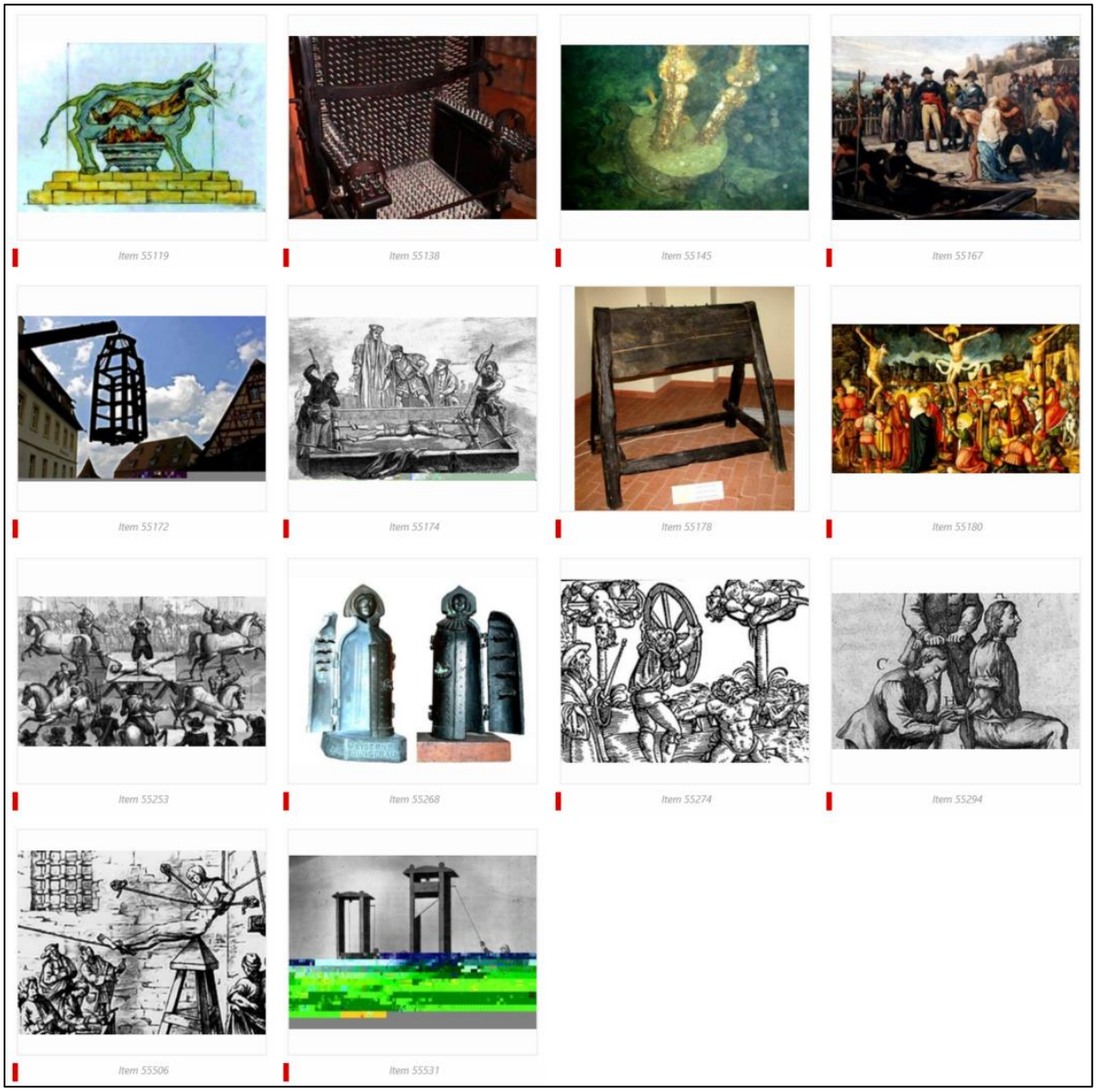


Figure 57

Firearms-Related Cached Images

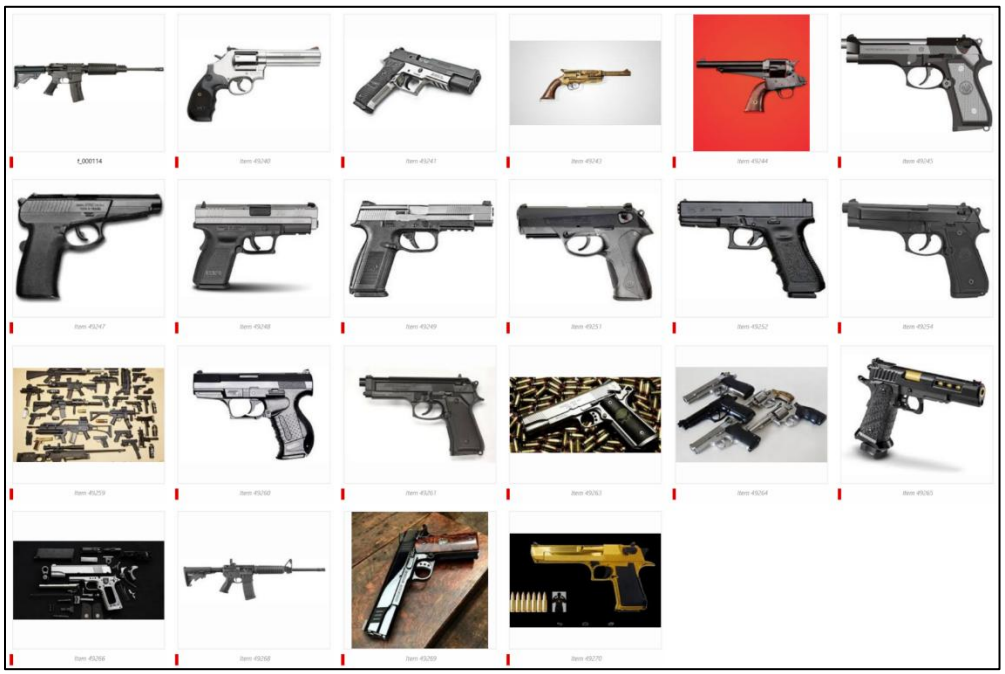


Figure 58

Knife-Related Cached Images

Figure 59

Camera-Related Cached Images

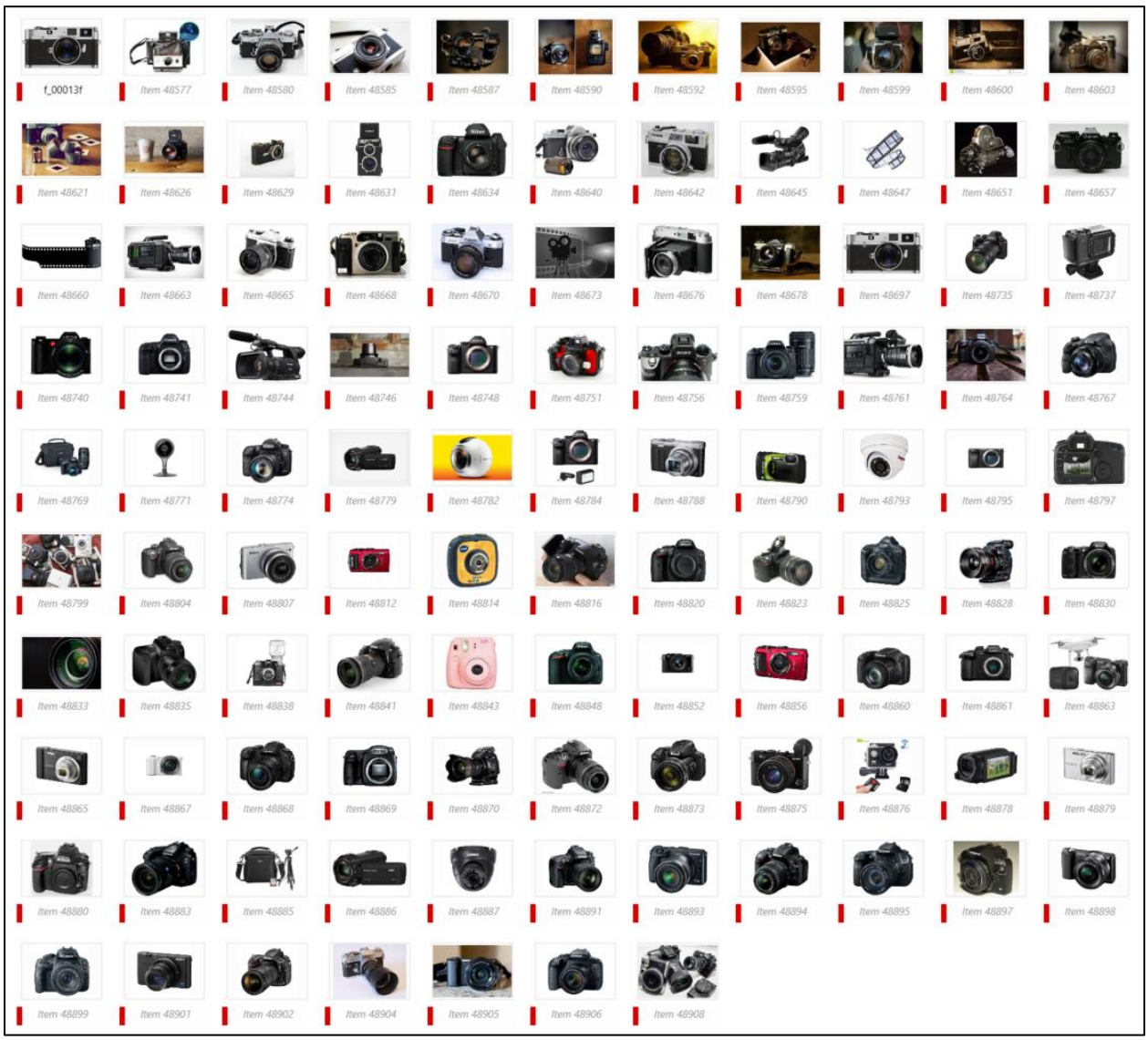


Figure 60

Rope and Knot-Related Cached Images

Figure 61

Plastic Bag-Related Cached Images

Figure 62

Crime Scene, Strangulation, and Binding-Related Cached Images

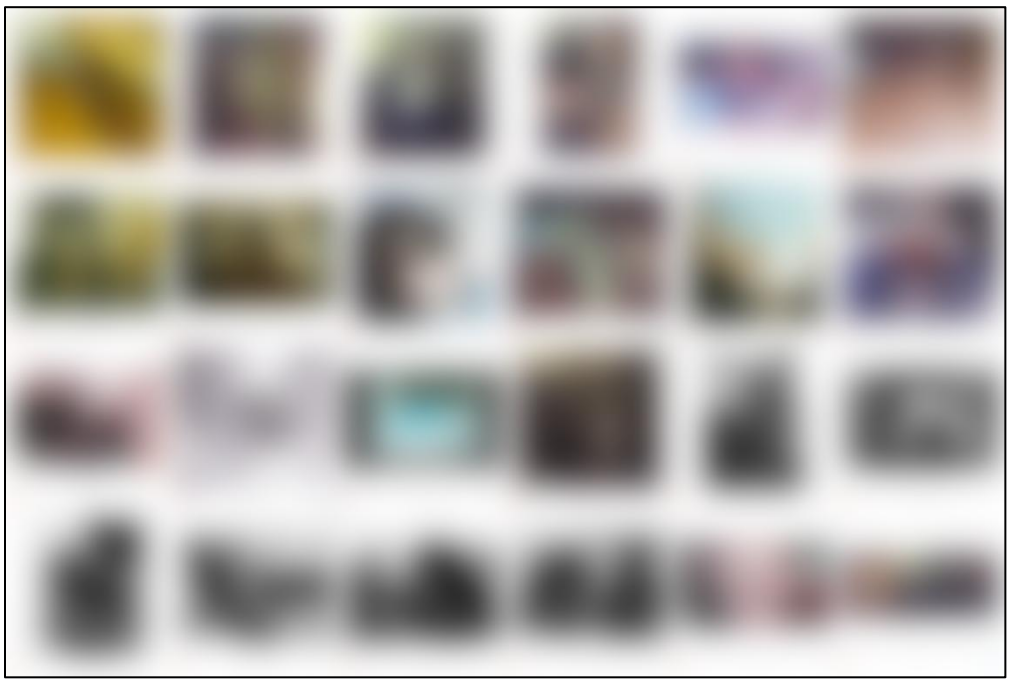
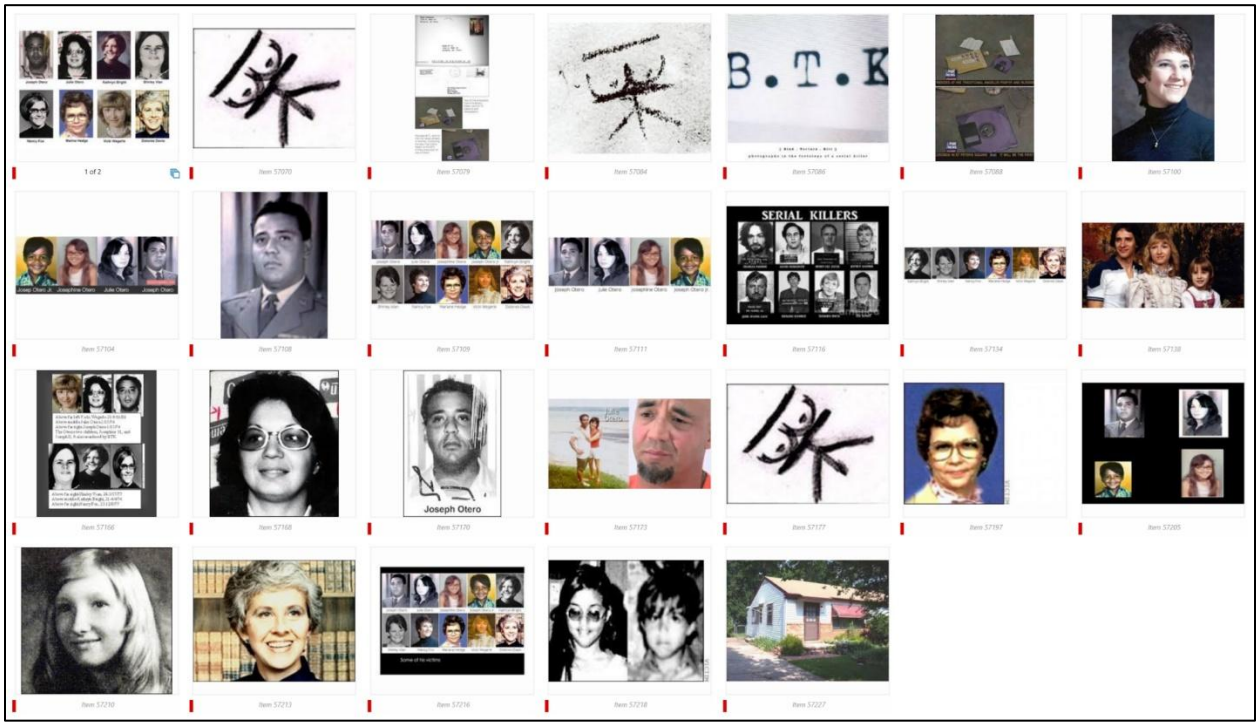


Figure 63

Dennis Rader-Related Cached Images

Figure 64

Other BTK-Related Cached Images



Deleted Material

Using FEX, eight relevant files were recovered from the Recycle Bin or carved from the disk. Two are documents (from the Recycle Bin, see **Figure 65** and **Figure 66**), and the remaining six are images (carved from the disk, see **Figure 67-Figure 72**). Any comments on these findings are included in a note below their respective Figure.

Figure 65

anna.rtf

```
Anna I can't wait to see you



Oh, Anna, any minute now

fear fresh Spring rain will roll down from your nakednessto scent to lofty
fever that burns within,

In that small world of longing, fear, rapture, and desparation,the game we
play, fall on devil earsFantasy spring forth, mounts, to storm fury, then
winter clam atthe end.

Oh, Anna Any minute, now

I lay with sweet enrapture garmentsacross most private thought

Bed of Spring moist grass, clean before the sun, enslaved withcontrol,
warm wind scenting the air, sun light sparkle tearsin eyes so deep and
clear.

Fornumber eight will be
```

Note. A recovered document that is similar to `Oh Anna Why Didn't You Appear.rtf`.

Figure 66

Death.rtf

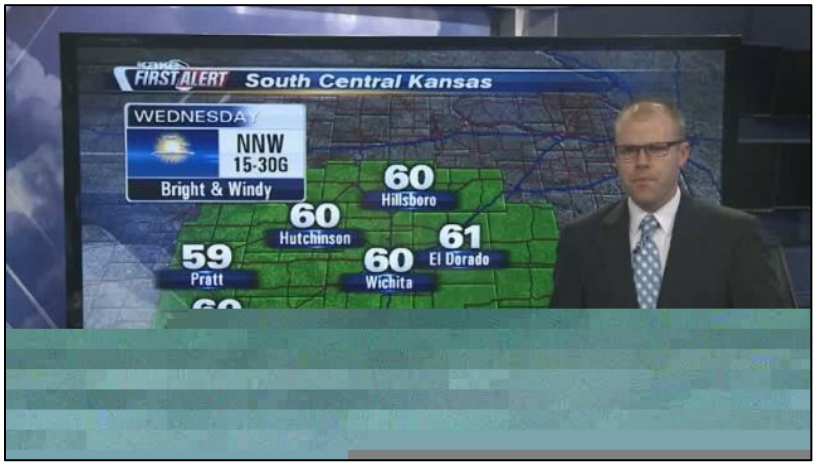
```
Oh! Death to Nancy
for Death has come, you all can see.
Hell has open it,s  gate to trick me.
Oh! Death, Oh! Death, can't you spare me, over for another year!
I'll stuff your jaws till you can't talk
I'll blind  your leg's till you can't walk
I'll tie your hands till you can't make a stand.

I'll bring sexual death unto you for me.
B.T.K.
```

Note. A recovered copy of the `Death to Nancy.rtf` document. The formatting is slightly different, and some lines are missing.

Figure 67

Carved_JPG_63830984.jpg



Note. A partially recovered image of what looks to be a weather report for the South-Central Kansas area. Wichita is visible in the image, which is where BTK is known to have been active.

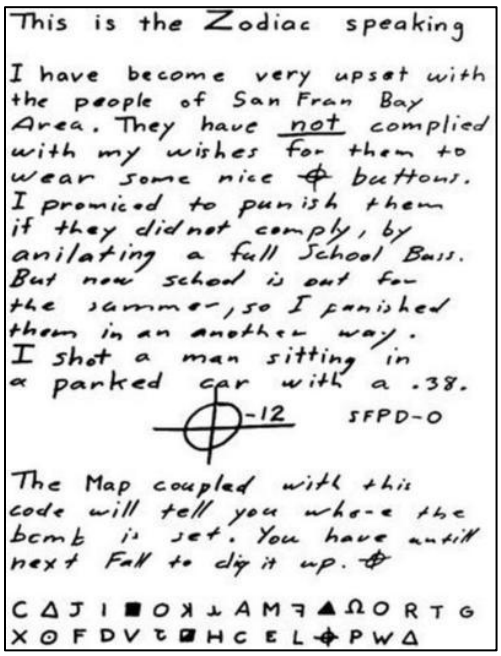
Figure 68

Carved_JPG_63831632.jpg

Note. A recovered photo of Dennis Rader. Clearly this is a stock photo, but I think it would be fair to ignore that fact due to the nature of this assignment (working with fabricated evidence for education/experience).

Figure 69

Carved_JPG_63831504.jpg


This is the Zodiac speaking

I have become very upset with the people of San Fran Bay Area. They have not complied with my wishes for them to wear some nice ⊕ buttons. I promised to punish them if they did not comply, by anilating a full School Bass. But now school is out for the summer, so I punished them in an another way. I shot a man sitting in a parked car with a .38.

-12 SFPD-O

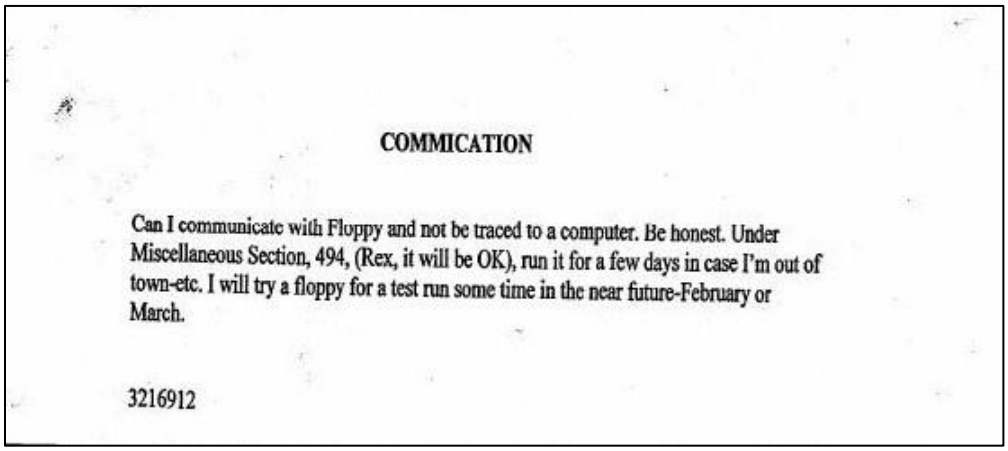
The Map coupled with this code will tell you where the bomb is set. You have until next Fall to dig it up. ⊕

C △ J I ■ O ✕ ⊥ A M ⅂ ▲ Ω O R T G
X ⊙ F D V ☾ ◪ H C E L ⊕ P W Δ

Note. A letter from the Zodiac Killer that dates to Summer 1970 (Bauer, 2023). Perhaps this could be a source of inspiration for Rader or indicate a connection between him and Zodiac.

Figure 70

Carved_JPG_63831984.jpg


COMMICATION

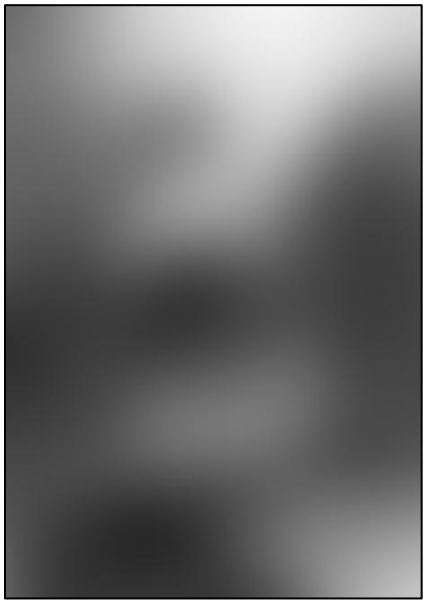
Can I communicate with Floppy and not be traced to a computer. Be honest. Under Miscellaneous Section, 494, (Rex, it will be OK), run it for a few days in case I'm out of town-etc. I will try a floppy for a test run some time in the near future-February or March.

3216912

Note. A recovered scan/photocopy of the `Floppy.rtf` document.

Figure 71

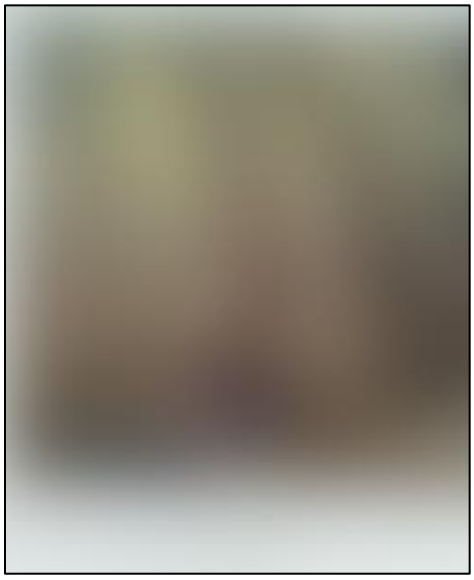
Carved_JPG_63831688.jpg



Note. A recovered photo of (presumably) a BTK victim.

Figure 72

Carved_JPG_63831816.jpg



Note. Another recovered photo of a victim.

Conclusion

After collecting and analyzing the evidence artifacts that were presented in this report, I believe it is highly likely that Dennis Rader is indeed BTK. Keeping in mind that the scenario states that investigators obtained a search warrant, this means that there must have already been a reason to suspect Rader of being BTK. Whatever evidence led to that suspicion will undoubtedly only be confirmed and strengthened by the digital evidence that was presented in this report.

Before reviewing this evidence, there are some findings from the registry that I would like to discuss first. According to the registry, The `Autumn Pelkey` user was the last to log in (see **Figure 11**), and the `Dennis Rader` user account is not password protected (nor has it ever been password protected in the past; see **Figure 6**). Rader is also not the registered owner of the machine (see **Figure 13**), which is one of the ways we discussed in class that digital evidence can be attributed to a real person in court. I'm uncertain of what this could mean for a real case, but my thought is that lawyers could potentially be able to argue that evidence was planted in the `Dennis Rader` user account by another person. However, I think these details are clearly meant to be ignored for the purposes of this assignment.

In any case, there was a veritable mountain of evidence in the forensic image file that strongly suggests Dennis Rader is BTK. Beginning with the registry, there was evidence that the `Dennis Rader` user had recently accessed some files/folders (see **Figure 4**) and used the Google Chrome executable (see **Figure 5**). Using those facts as guides, the recently accessed files and folders were located and analyzed along with Internet data from the Google Chrome and Internet Explorer web browsers.

Examination of the files and folders revealed documents containing information related to BTK such as poems about victims, a "project list" containing the names of prior and

prospective BTK victims, admissions of responsibility for murders (`Guilty.rtf`; see **Figure 25**), and communications between BTK and the police. Some of these documents are signed with " - BTK" (or something similar) at the end. Furthermore, Rader had images saved to his computer that closely match known details about BTK. These include images of items that BTK would have used such as a film camera, weapons, and rope/plastic bags for binding, strangulation, and suffocation. Additionally, the file `Photo Diary.jpg` contains images of all ten confirmed BTK victims. Deleted files, including pictures of victims and partial poems, were also recovered from the disk.

As far as Internet evidence artifacts go, a high number of cached images were discovered. These images depict things such as torture methods, weaponry, knots and rope, plastic bags, bound/strangled/suffocated victims, and known prior BTK victims. FEX was also able to extract Internet search and browsing history showing that Rader made multiple searches (e.g., "best ways to contact the police without getting caught," "is a floppy disk anonymous," "quiet ways to kill," and "strangulation") and visited websites (e.g., a forum page discussing silent ways to kill people) that are highly suspicious in the context of other evidence and the case as a whole. I believe that these are clear signs of Rader conducting research on the Internet to prepare for what he plans to do to a future victim.

In all, I don't think it is realistic that Rader would be found innocent of being BTK in the face of the overwhelming amount of digital evidence found on his computer in this scenario – especially when this evidence is combined with other evidence that investigators must have had beforehand if they were able to obtain a search warrant.

References

Bauer, C. P. (2023, September 12). *The Zodiac ciphers: What cryptologists know*. HISTORY. https://www.history.com/news/the-zodiac-ciphers-what-we-know

Ciampa, M. D. (2017). *Security awareness: Applying practical security in your world* (Fifth edition). Cengage Learning.

Gogolin, G. (Ed.). (2021). *Digital forensics explained* (2nd ed.). CRC Press. https://doi.org/10.1201/9781003049357

Google. (2024). *Clear cache & cookies*. Google Help. https://support.google.com/accounts/answer/32050?hl=en&co=GENIE.Platform%3DDesktop

Microsoft. (n.d.). *Windows 7 support ended on January 14, 2020*. Microsoft Support. Retrieved April 24, 2024, from https://support.microsoft.com/en-us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962

Previch, C. (2004, May 23). *Survivor recalls serial killer's attack*. The Oklahoman. https://www.oklahoman.com/story/news/2004/05/23/survivor-recalls-serial-killers-attack/61988446007/