

EXPERT INSIGHT

Learn Computer Forensics

Your one-stop guide to searching, analyzing,
acquiring, and securing digital evidence

Second Edition



William Oettinger

<packt>

Preface

Download the exercise files

You can download exercise files for this book from github.com/bill-lcf/Learn-Computer-Forensics.

Employed academic faculty can also download PowerPoints for each chapter and a question bank after validation. Send an email to verify@learncomputerforensics.com from an .edu email address requesting access. If you do not have an .edu email address, please send proof that you are an instructor.

Once the files are downloaded, please make sure that you unzip or extract the folder using the latest version of:

- WinRAR / 7-Zip for Windows
- Zipeg / iZip / UnRarX for Mac
- 7-Zip / PeaZip for Linux

We also have other code bundles from our rich catalog of books and videos available at <https://github.com/PacktPublishing/>. Check them out!

Chapter 1

Images

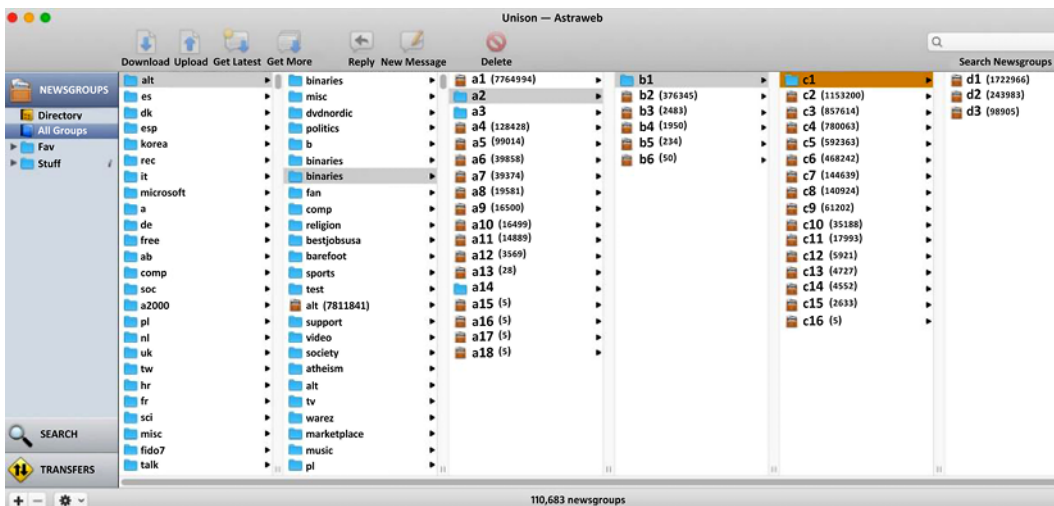


Figure 1.1: Unison application

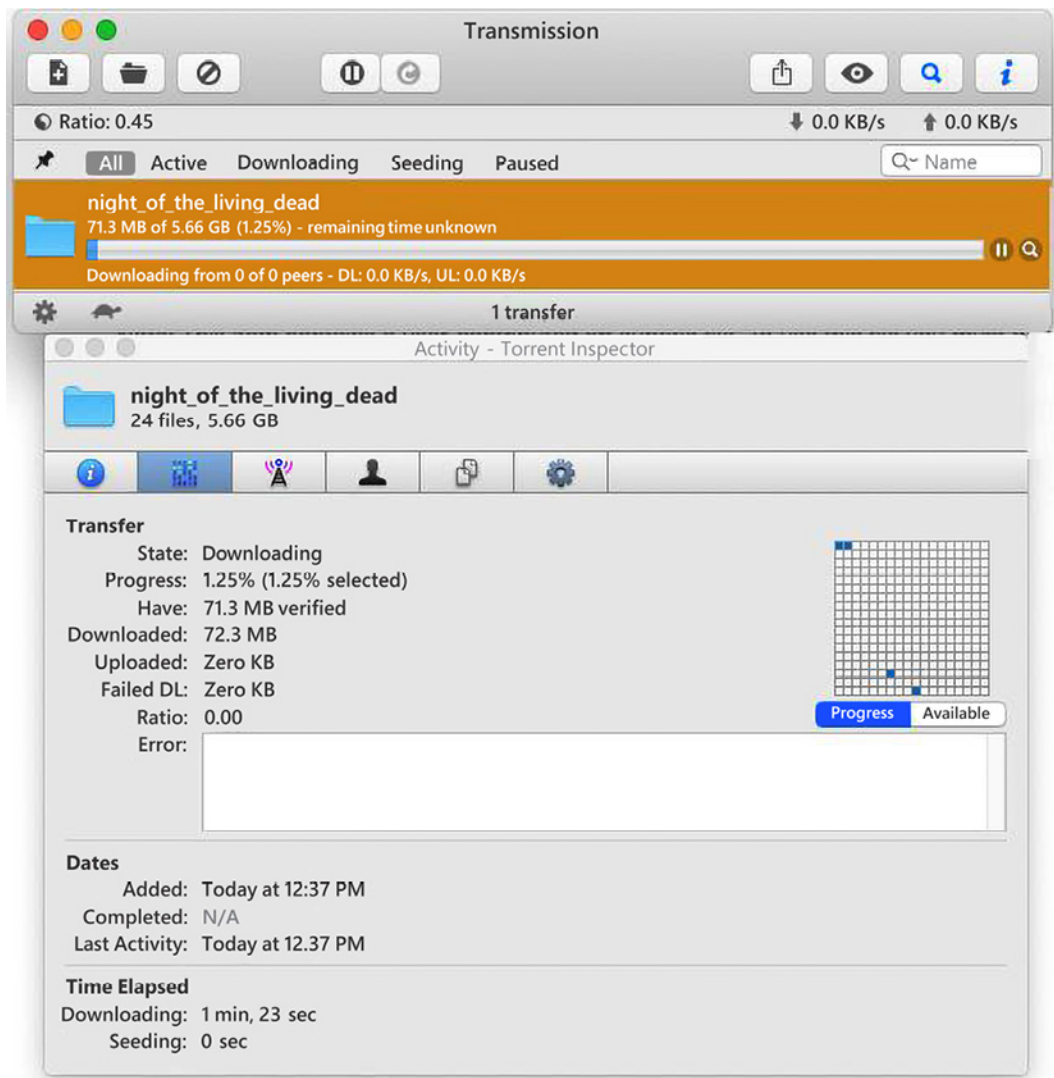


Figure 1.2: Transmission application



Please sign in

✔ You have successfully logged out

Sign in

Figure 1.3: Gophish login

New Group

×

Name:

Group name

+ Bulk Import Users

Download CSV Template

First Nam

Last Nam

Email

Position

+ Add

Show

10

entries

Search:

First Name

Last Name

Email

Position

No data available in table

Showing 0 to 0 of 0 entries

Previous

Next

Close

Save changes

Figure 1.4: Gophish import emails

Links

- Stalking information: <https://web.archive.org/web/20201028110630/https://members.victimsofcrime.org/our-programs/past-programs/stalking-resource-center/stalking-information>
- Computer Forensics: Computer Crime Scene Investigation, Charles River Media, 2002, available at: <https://www.amazon.com/Computer-Forensics-Investigation-CD-ROM-Networking/dp/1584500182>

Chapter 2

Images

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____ Location of Seizure: _____

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Figure 2.1: An evidence form

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
CD-001	1	Ultimate DVD contains server logs from AD001
HDD-001	1	Samsung SSD 1TB Ser#ABC9876
HDD-002	1	Samsung SSD 512 MB Ser#DEF4567
CP-001	1	Pixel XL 128 GB Ser# A5 12 D3 AC FD
TD-001	1	Generic Thumb drive 32GB (green) Unknown Serial Number
MD-001	1	Apple iPad 512 GB Ser# 09 E3 4D AB Rose Gold

Figure 2.2: A description of the evidence

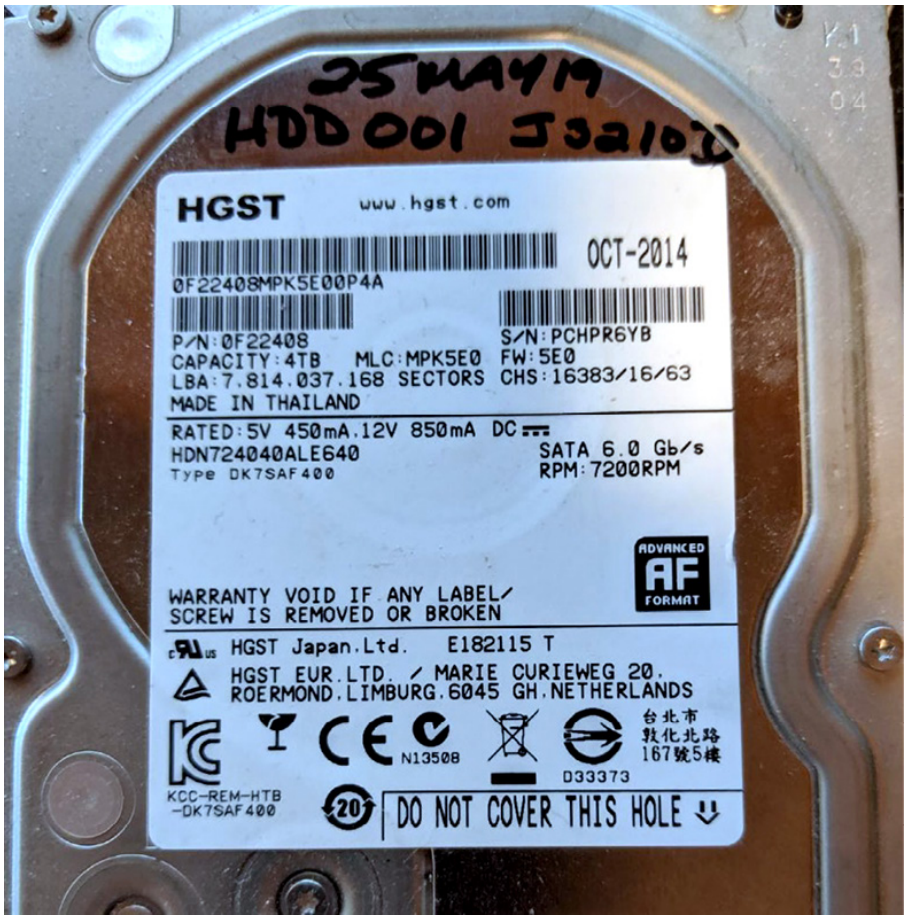


Figure 2.3: A hard drive

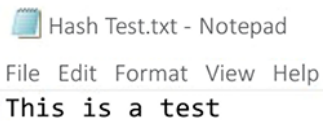


Figure 2.4: The hash text



Figure 2.5: The Jacksum values

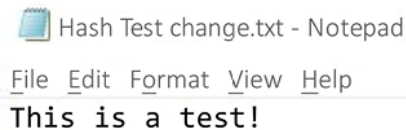


Figure 2.6: The change in the text



Figure 2.7: The change in the Jacksum values

Name	10534.gif
Type	jpg
Description	existing
Existent	✓
Size	3.0 KB (3,081)
Modified	07/12/2008 21:51:38 +0
Ext.	gif
Type status	mismatch detected, OK
Type descr.	JPEG

Figure 2.8: A file signature mismatch

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCIT
00000000	EF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿøÿà	JFIF

Figure 2.9: A file header

File Signatures

011001100110100101101100011001010010000001110011011010010110011101101110011000010111010001110101011100100110010101110011

66:69:6c:65:20:73:69:67:6e:61:74:75:72:65:73

Search

All Signatures

Submit Sigs

My Favorites

Control Panel

☐ Disable autocomplete

submit

Extension ☒ Signature ☐

Figure 2.10: filesignatures.net

File Signatures

011001100110100101101100011001010010000001110011011010010110011101101110011000010111010001110101011100100110010101110011

6 6 : 6 9 : 6 c : 6 5 : 2 0 : 7 3 : 6 9 : 6 7 : 6 e : 6 1 : 7 4 : 7 5 : 7 2 : 6 5 : 7 3

Search
All Signatures
Submit Sigs
My Favorites
Control Panel

☐ Disable autocomplete
 submit
 Extension ☒ Signature ☐

3 Results Found For JPG File Extension

Extension	Signature	Description
☆ <u>JPG</u>	<u>FF D8 FF E0</u> ASCII	JPEG IMAGE Sizet: 4 Bytes Offset: 0 Bytes
☆ <u>JPG</u>	<u>FF D8 FF E1</u> ASCII	Digital camera JPG using Exchangeable Image File Format (EXIF) Sizet: 4 Bytes Offset: 0 Bytes
☆ <u>JPG</u>	<u>FF D8 FF E8</u> ASCII	Still Picture Interchange File Format (SPIFF) Sizet: 4 Bytes Offset: 0 Bytes

Figure 2.11: The results for a JPG file signature

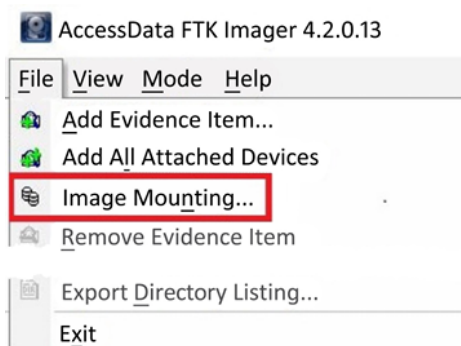


Figure 2.12: Image mounting

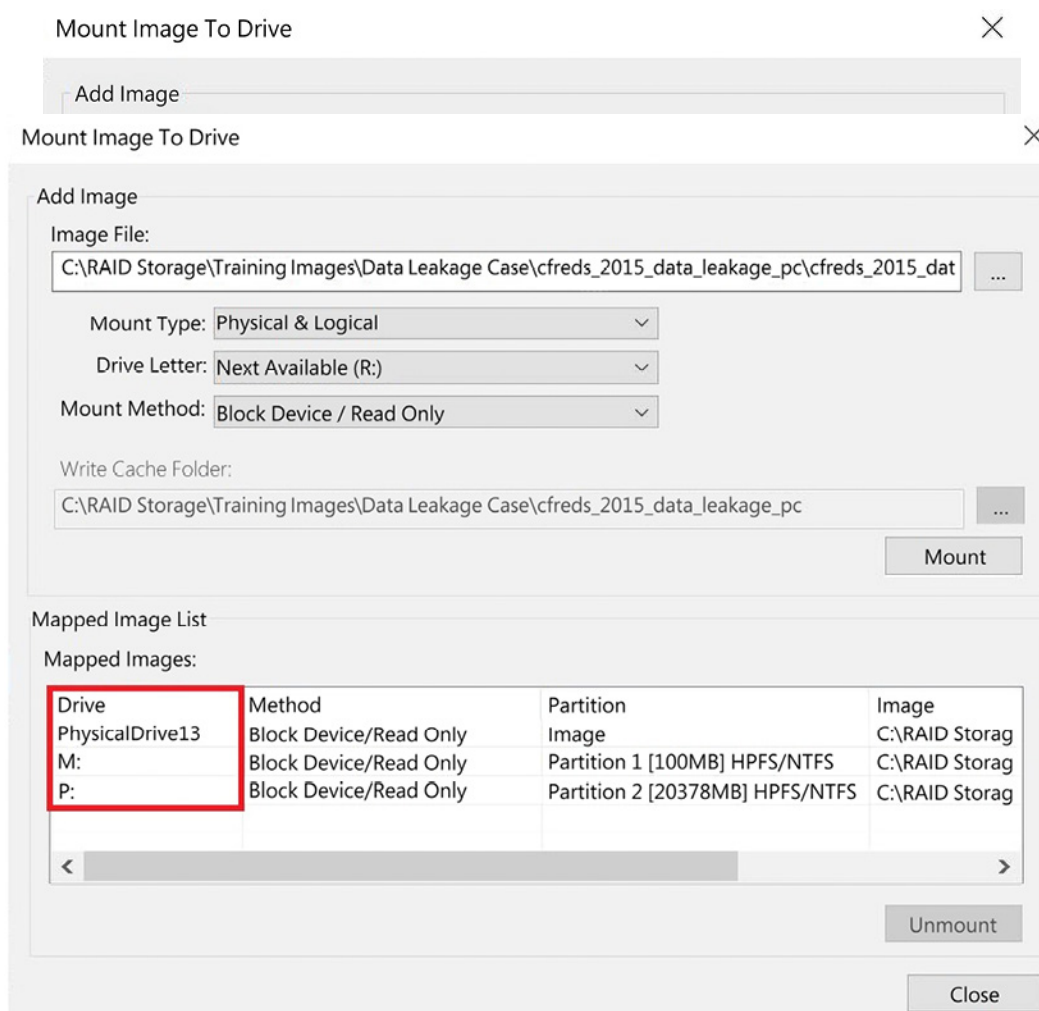


Figure 2.14: A mounted image

Links

- Tableau TK8u USB 3.0 forensic bridge: <https://security.opentext.com/tableau/hardware/details/t8u>
- CFTT: <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt>
- Some open-source forensic tools include the following:
 - Autopsy: <https://www.autopsy.com>.

- SIFT Workstation: <https://digital-forensics.sans.org/community/downloads>.
- PALADIN Forensic Suite: <https://sumuri.com/software/paladin/>.
- CAINE: <https://www.caine-live.net/>.
- Here are some commercial forensic tools available for Windows-based users:
 - X-Ways Forensics: <https://www.x-ways.net/>
 - EnCase: <https://www.guidancesoftware.com/encase-forensic>
 - Forensic Toolkit (FTK): <https://accessdata.com/products-services/forensic-toolkit-ftk>
 - Forensic Explorer (FEX): <http://www.forensicexplorer.com/>
 - Belkasoft Evidence Center: <https://belkasoft.com/ec>
 - Axion: <https://www.magnetforensics.com/products/magnet-axiom/>
- Here are some Macintosh-based tools:
 - Cellebrite Inspector: <https://cellebrite.com/en/inspector/>
 - RECON LAB: <https://sumuri.com/software/recon-lab/>
 - RECON ITR: <https://sumuri.com/software/recon-itr/>
- A Linux-based tool is SMART <http://www.asrdata.com/forensic-software/smart-for-linux/>)
- This is a list of some of the certifications available:
 - Certified Forensic Computer Examiner (CFCE) (Tool-Agnostic): <https://www.iacis.com/>
 - EnCase Certified Examiner (EnCE) (tool-specific): <https://www.opentext.com/products-and-solutions/services/training-and-learning-services/encase-training/certifications>
 - ACE (tool-specific): <https://training.accessdata.com/exams>
 - Computer Hacking Forensic Investigator (CHFI) (tool-agnostic): <https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/>
 - Global Information Assurance Certification (GIAC) (tool-agnostic): <https://www.giac.org/certifications>

- Certified Forensic Mac Examiner (CFME) (tool-agnostic): <https://sumuri.com/mac-training/>
- NIST chain of custody: <https://www.nist.gov/document/sample-chain-custody-formdocx>
- Free Jacksum utility: <https://jacksum.loefflmann.net/en/index.html>
- FTK Imager: <https://accessdata.com/product-download/ftk-imager-version-4.2.0>
- Warren Kruse and Jay Heiser, Computer Forensics: Incident Response Essentials (Addison Wesley, 2001). You can purchase the book from <https://www.amazon.com/Computer-Forensics-Incident-Response-Essentials/dp/0201707195>

Chapter 3

Images

```
URI: file:///media/bob/Picture Drive/New
```

Figure 3.1: URI from thumbnail

```
URI: file:///media/bobby/Picture Drive/
```

Figure 3.2: URI image: bobby

The following non-system files should be present on the logical level of the disk:

```
039C8A00 Scientific control.mp3 MD5: e73a608dfb422a206ce7a62deb90ff9b
029D4A00 Export_me.JPG MD5: c0c3892606849fd76a8534ef80956705
```

Figure 3.3: DCFL control image hash values

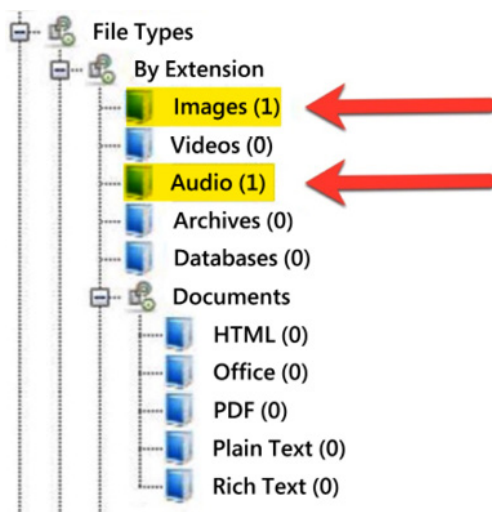


Figure 3.4: DCFL control image – file types

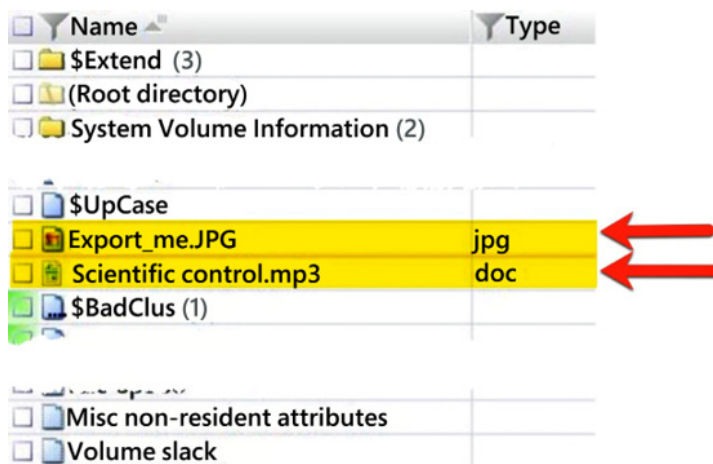


Figure 3.5: DCFL control image – X-Ways logical files

Name	/img_control.dd/Export_me.JPG
Type	File System
MIME Type	image/jpeg
Size	21165
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2007-08-20 06:10:23 PDT
Accessed	2007-08-20 07:21:37 PDT
Created	2007-08-20 06:10:23 PDT
Changed	2007-08-20 07:21:47 PDT
MD5	c0c3892606849fd76a8534ef80956705

Figure 3.6: DCFL control image – metadata of jpg

Evidence object	control
Name	Export_me.JPG
Type	jpg
Description	existing
Existent	✓
Size	20.7 KB (21,165)
Created	08/20/2007 13:10:23 +0
Modified	08/20/2007 13:10:23 +0
Accessed	08/20/2007 14:21:37 +0
Record changed	08/20/2007 14:21:47 +0
Record changed ²	08/20/2007 13:10:23 +0
Ext.	JPG
Pixels	0.4 MP
Analysis	0% skin tones
Hash ¹ (MD5)	C0C3892606849FD76A8534EF80956705
Hash ² (SHA-1)	4F90640F999271C41A1E77804FD7AAA4F0340D9D
Generator signature	60F38468 (U:Standard 75 Edited)
Device type	unknown
Relevance	3.59

Figure 3.7: DCFL control image – X-Ways metadata of JPG

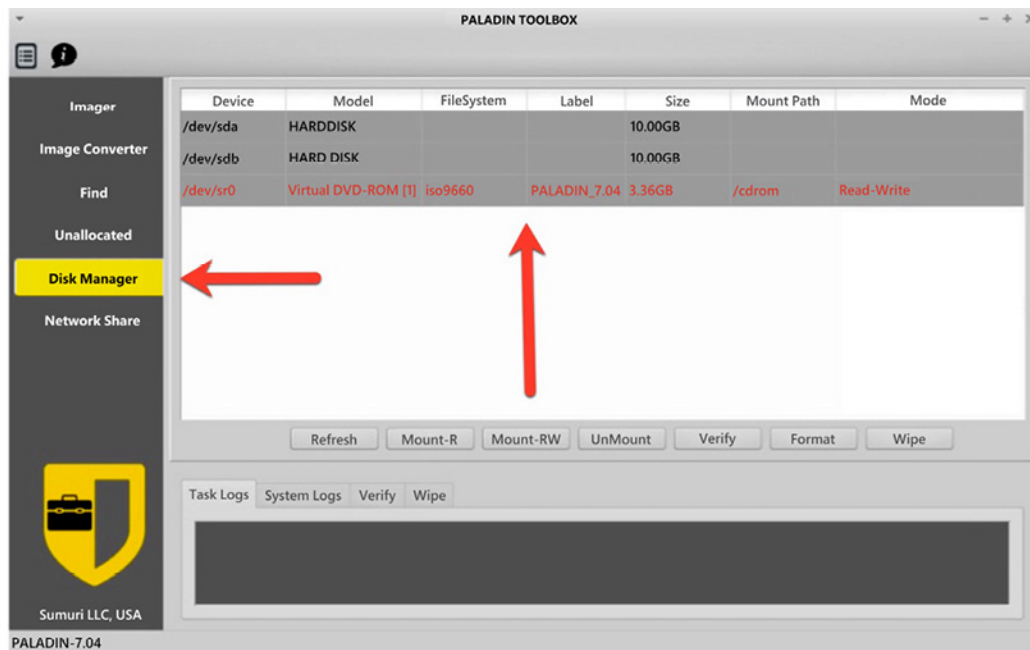


Figure 3.8: PALADIN toolbox

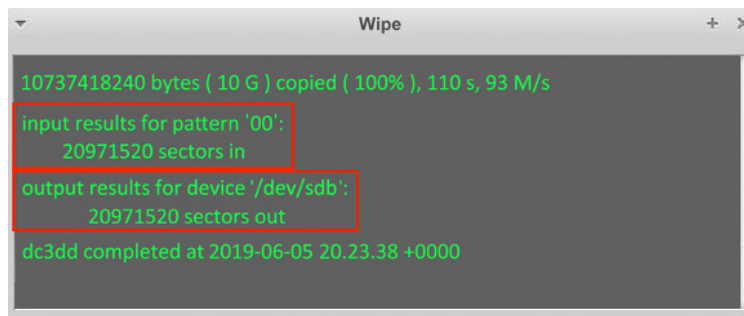


Figure 3.9: PALADIN toolbox – Results of wiping

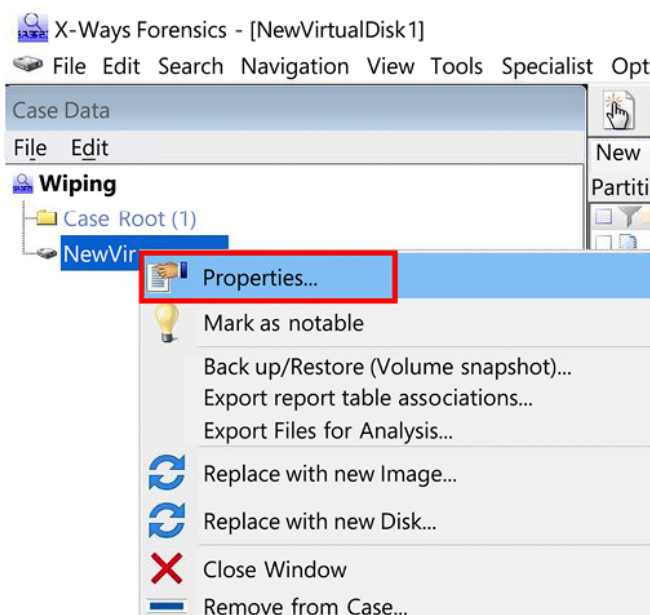


Figure 3.10: X-Ways – Properties menu

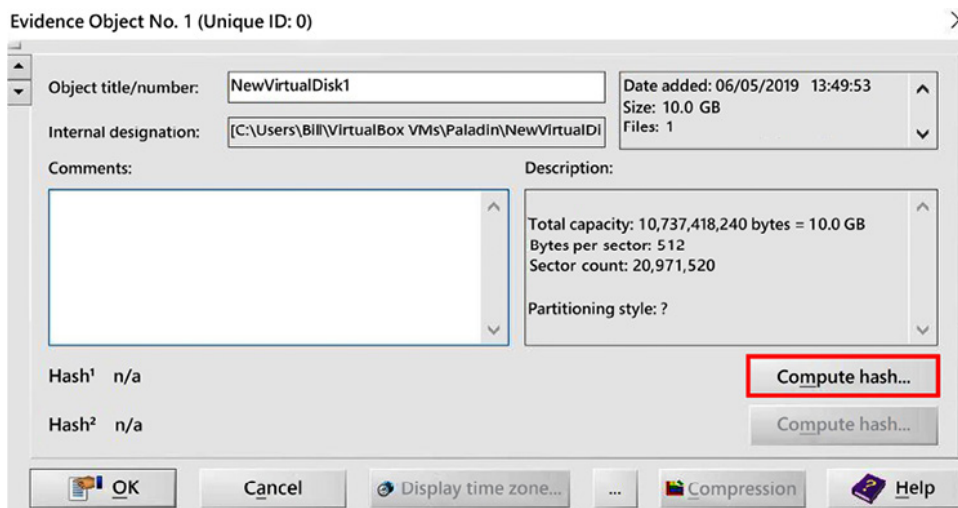


Figure 3.11: X-Ways – Hashing configuration

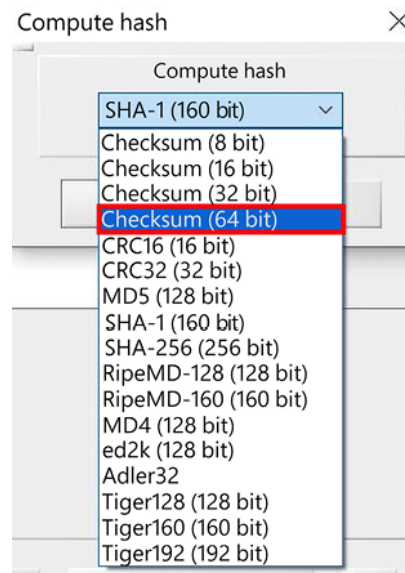


Figure 3.12: X-Ways – Selecting Checksum (64 bit)

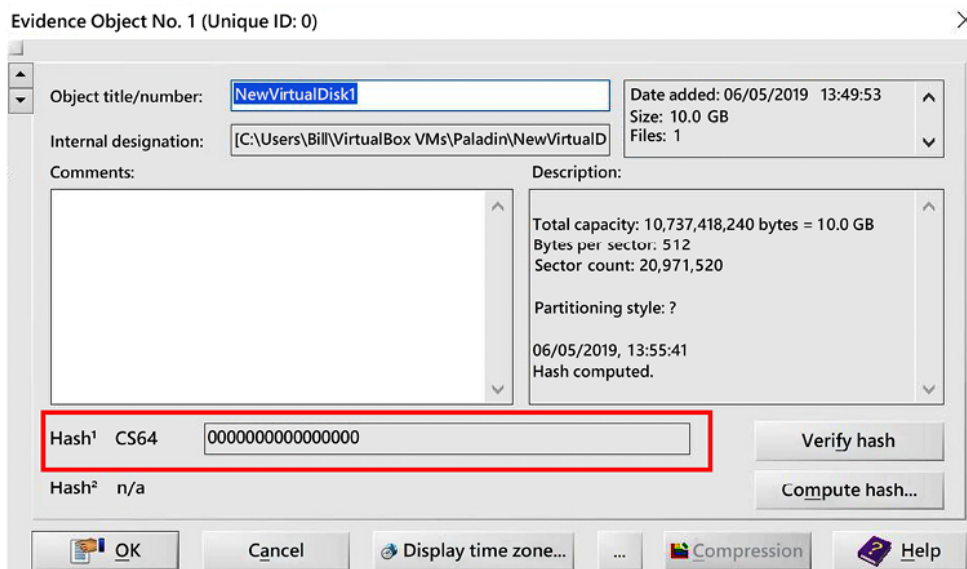


Figure 3.13: X-Ways – Checksum result

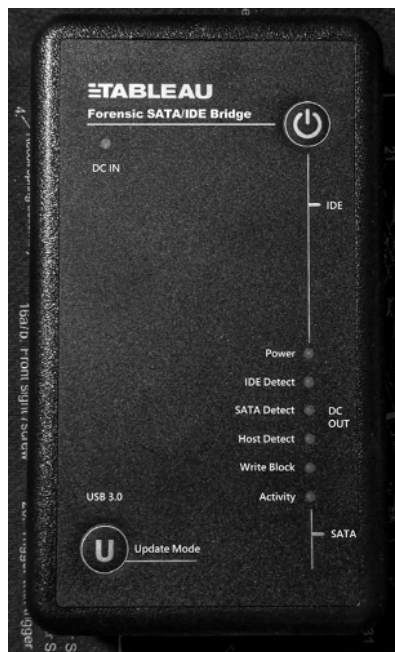


Figure 3.14: Tableau Writeblocker

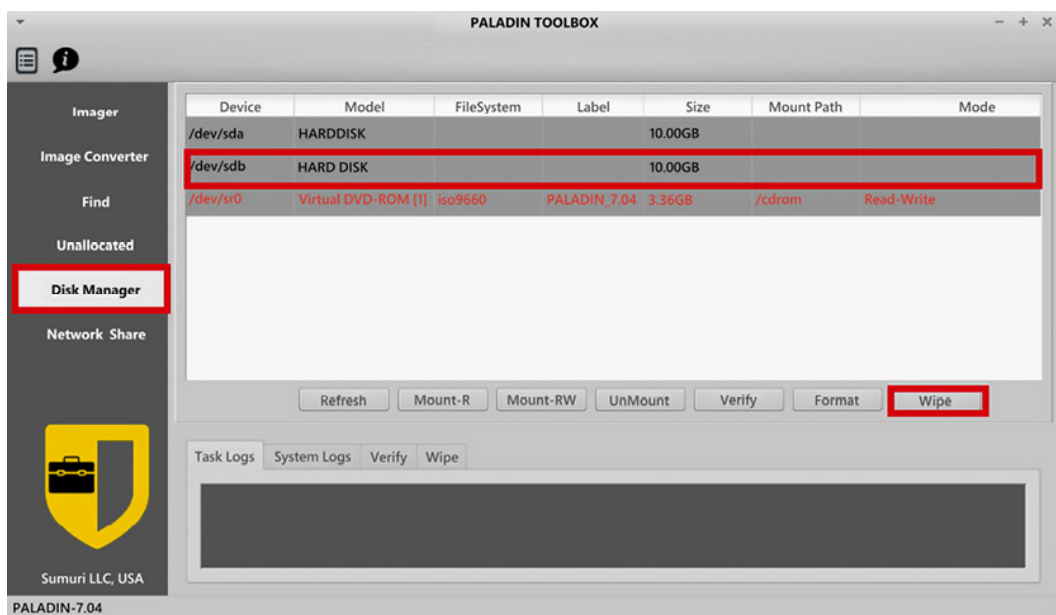
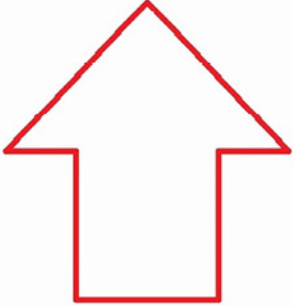


Figure 3.15: PALADIN toolbox – Disk Manager

Device	Model	FileSystem	Label	Size	Mount Path	Mode
/dev/sdb	VBOX HARDDISK			10.00GB		
/dev/sda1	VBOX HARDDISK	ext4	OS	10.00GB	/media/OS	Read Only
/dev/sdb	VBOX HARDDISK			10.00GB		
/dev/sr0	VBOX CD-ROM	iso9660	PALADIN_7.04	3.36GB	/cdrom	Read-Write



Refresh Mount-R Mount-RW UnMount Verify Format Wipe

Figure 3.16: PALADIN toolbox – Disk Manager Mode status

 cfreds_2015_data_leakage_pc.dd	4/21/2015 11:17 AM	DD File	20,971,520 KB
--	--------------------	---------	---------------

Figure 3.17: DD image example

Case Information	CRC	Data	CRC	Data	CRC	Data	CRC	MD5
------------------	-----	------	-----	------	-----	------	-----	-----

Figure 3.18: Expert Witness Format file layout

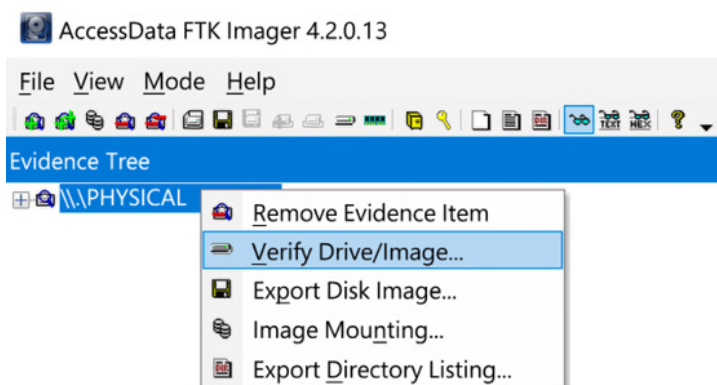


Figure 3.19: FTK Imager – Creating a hash value

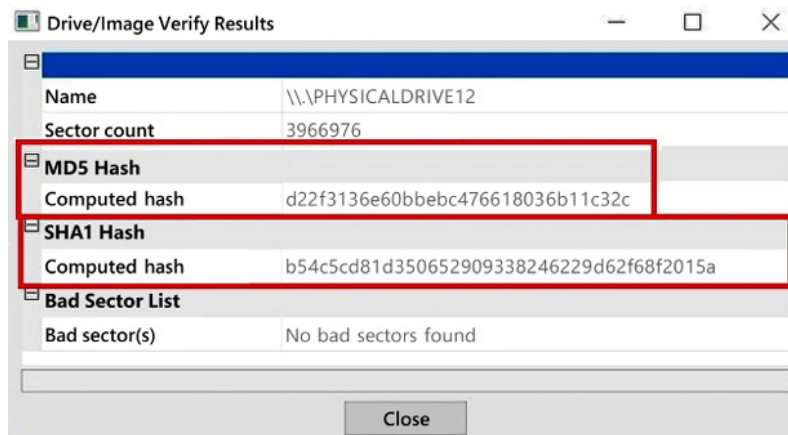


Figure 3.20: FTK Imager – Drive/Image Verify Results

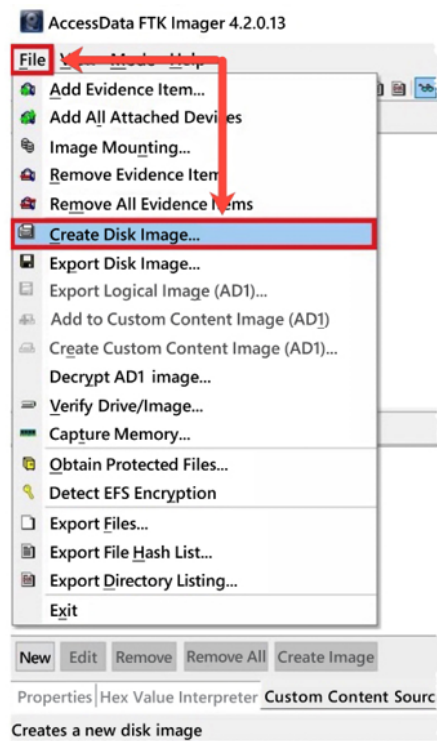


Figure 3.21: FTK Imager – Create Disk Image menu

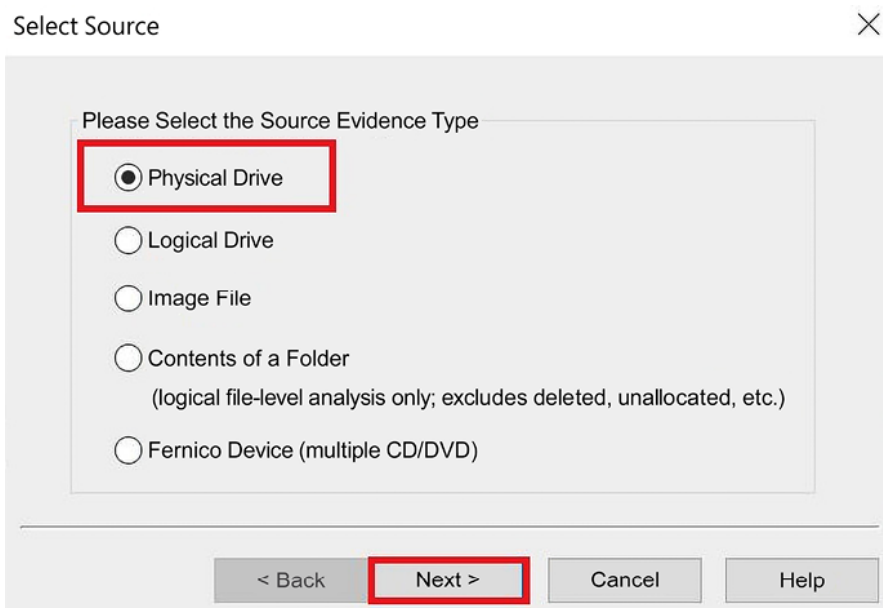


Figure 3.22: FTK Imager – Select Source menu

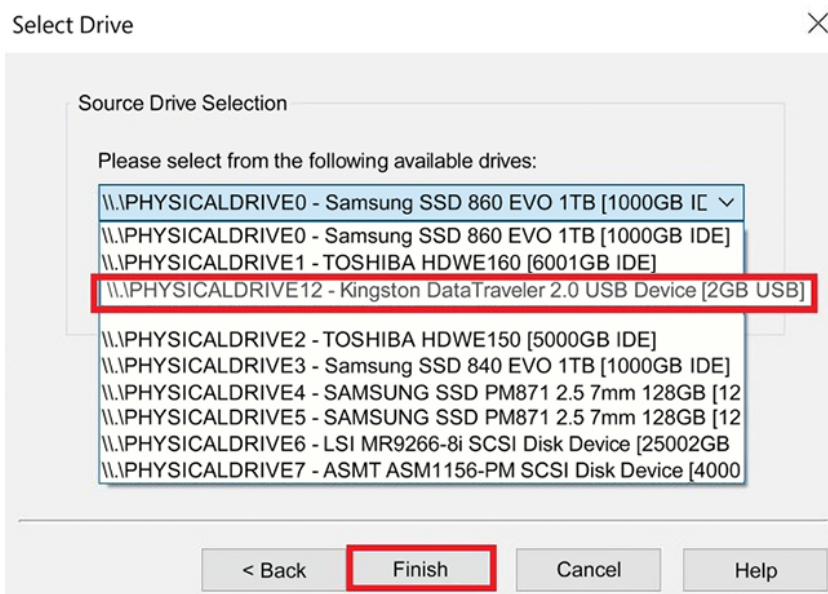


Figure 3.23: FTK Imager – Select Drive menu

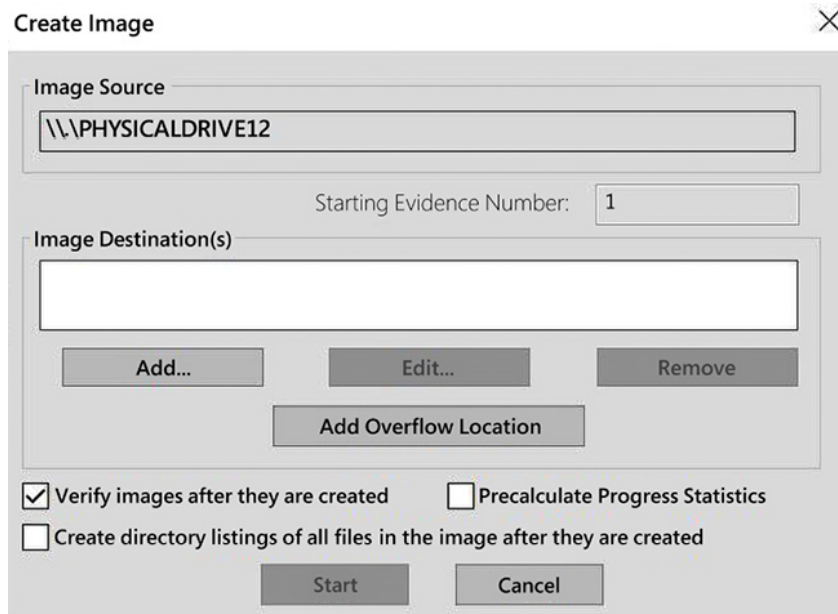


Figure 3.24: FTK Imager – Create Image menu

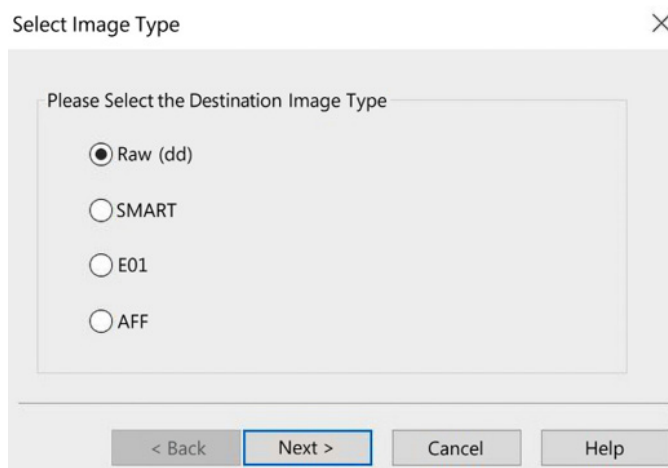
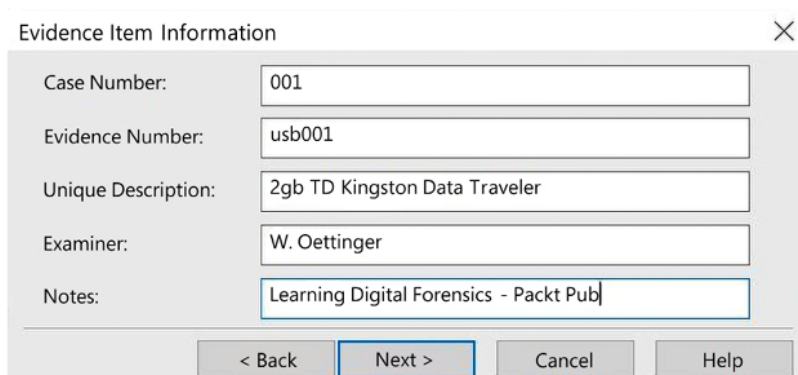


Figure 3.25: FTK Imager – Select Image Type menu

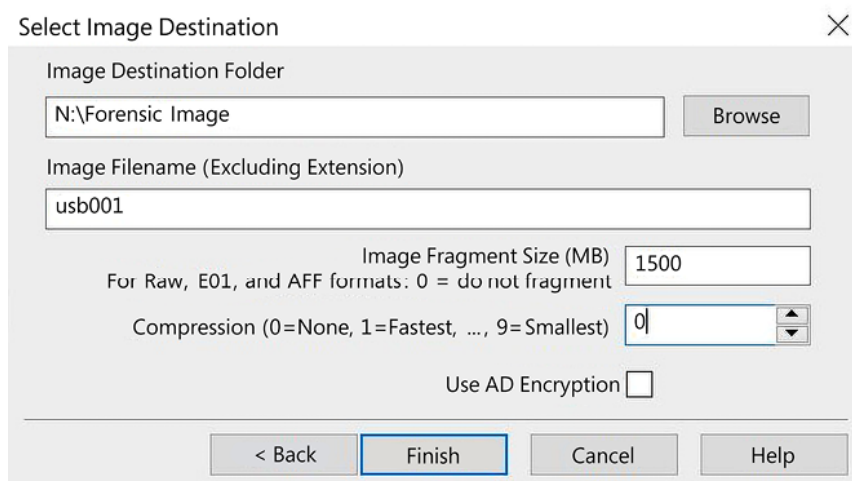


The 'Evidence Item Information' window in FTK Imager contains the following fields and values:

Field	Value
Case Number:	001
Evidence Number:	usb001
Unique Description:	2gb TD Kingston Data Traveler
Examiner:	W. Oettinger
Notes:	Learning Digital Forensics - Packt Pub

At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

Figure 3.26: FTK Imager – Evidence Item Information window



The 'Select Image Destination' window in FTK Imager contains the following fields and values:

Field	Value
Image Destination Folder	N:\Forensic Image
Image Filename (Excluding Extension)	usb001
Image Fragment Size (MB)	1500
Compression (0=None, 1=Fastest, ..., 9=Smallest)	0
Use AD Encryption	<input type="checkbox"/>

At the bottom, there are four buttons: '< Back', 'Finish', 'Cancel', and 'Help'. The 'Finish' button is highlighted with a blue border.

Figure 3.27: FTK Imager – Select Image Destination window

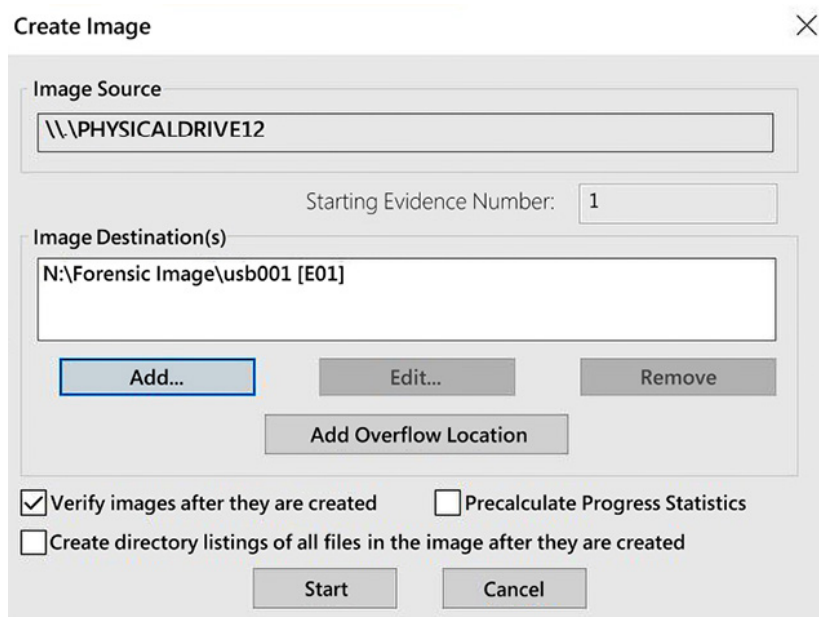


Figure 3.28: FTK Imager – Create Image window

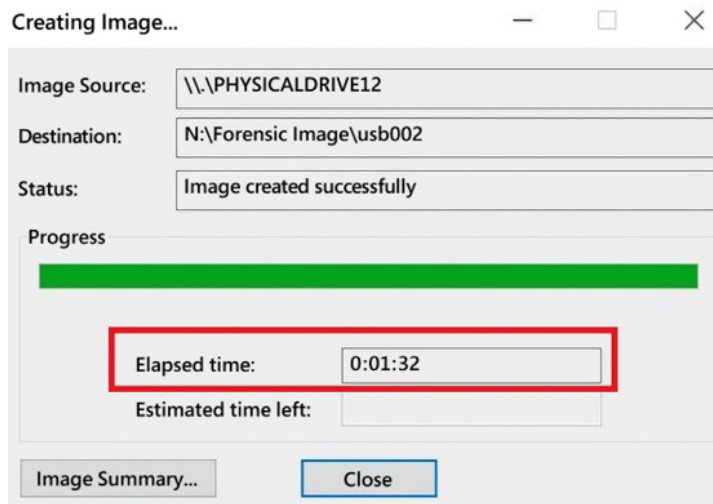


Figure 3.29: FTK Imager – Completed Creating Image window

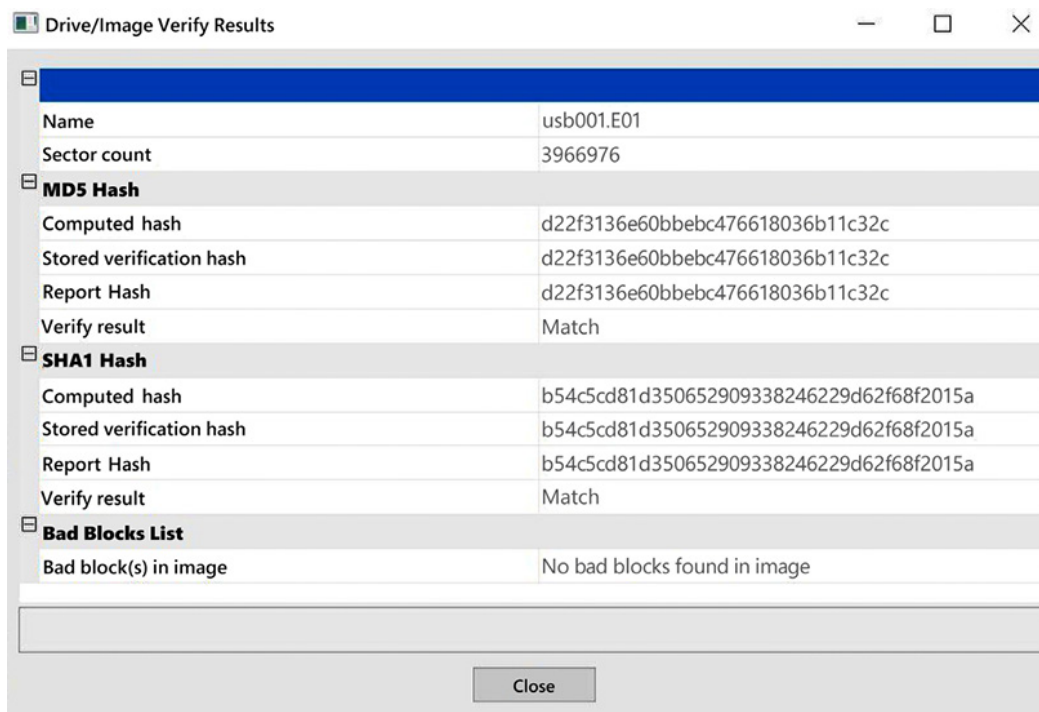


Figure 3.30: FTK Imager – Final verification window



Figure 3.31: PALADIN – Desktop



Figure 3.31: PALADIN – Desktop

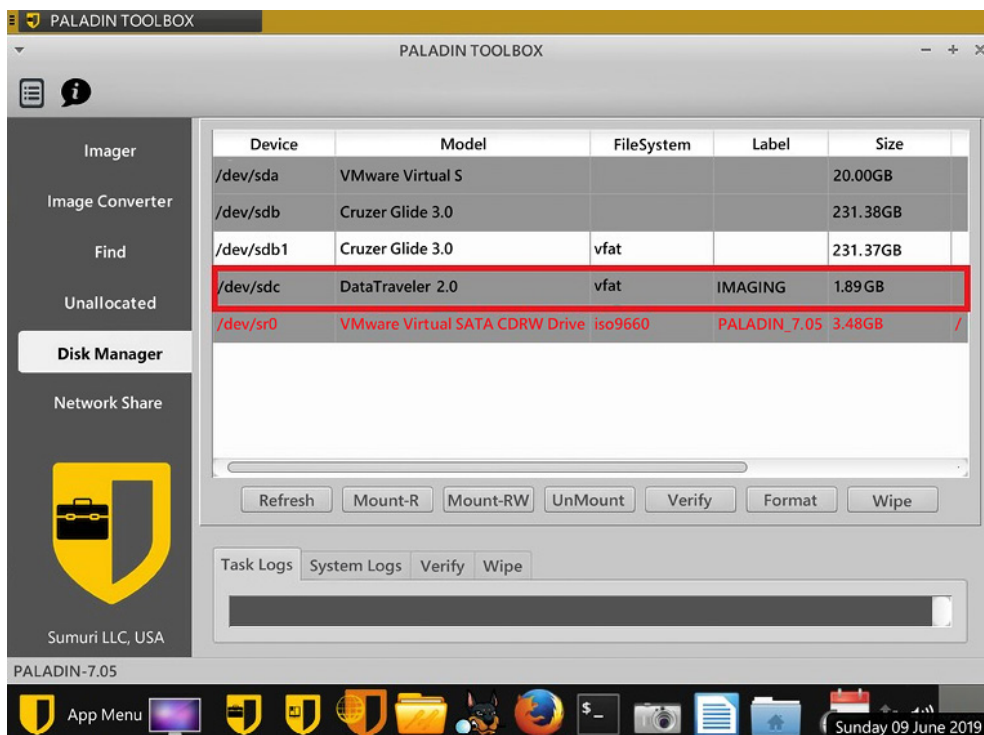


Figure 3.32: PALADIN toolbox

```
dc3dd 7.2.641 started at 2019-06-09 16:43:43 +0000
compiled options:
command line: dc3dd of=/dev/null hash=md5 hash=sha1 if=/dev/sdc hlog=/tmp/
000AEBFFB4C45B8903020517_06-09-2019-16-43-43_verify.log

input results for device '/dev/sdc':
  d22f3136e60bbebc476618036b11c32c (md5)
  b54c5cd81d350652909338246229d62f68f2015a (sha1)

output results for file '/dev/null':
```

Figure 3.33: PALADIN – Hash results

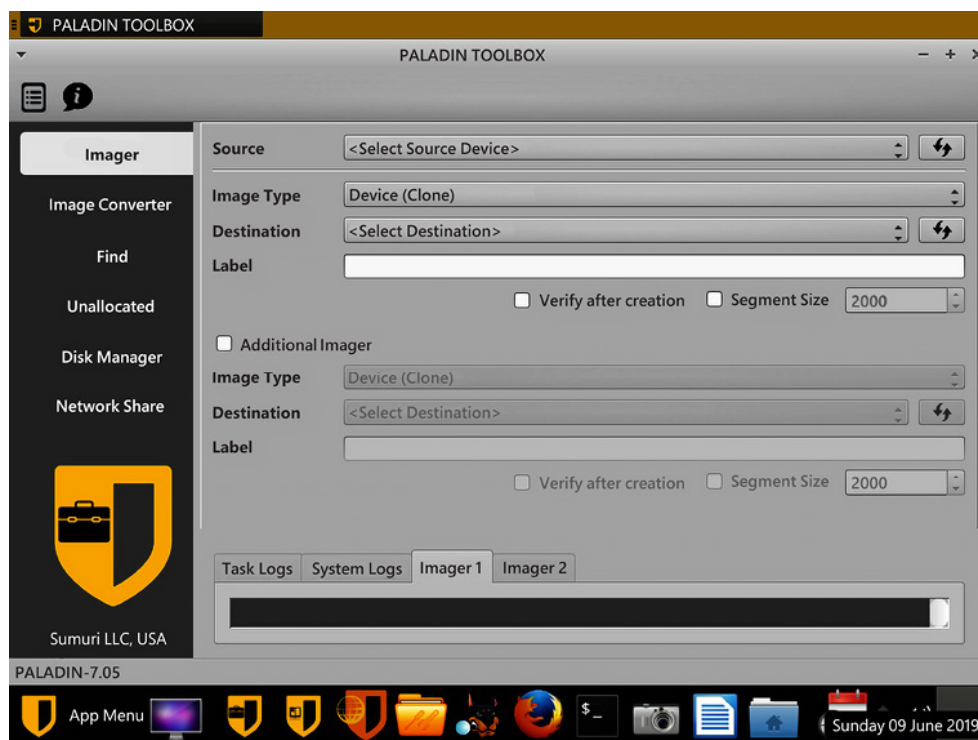


Figure 3.34: PALADIN – Toolbox imaging screen

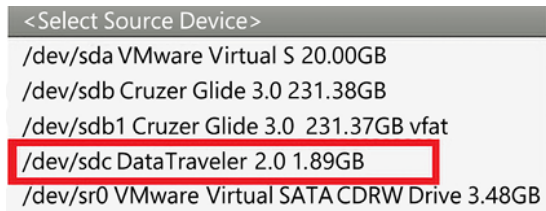


Figure 3.35: PALADIN – Toolbox Select Source Device drop-down menu

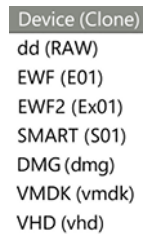


Figure 3.36: PALADIN – Toolbox Image Format drop-down menu



Figure 3.37: PALADIN – Toolbox Destination drop-down menu

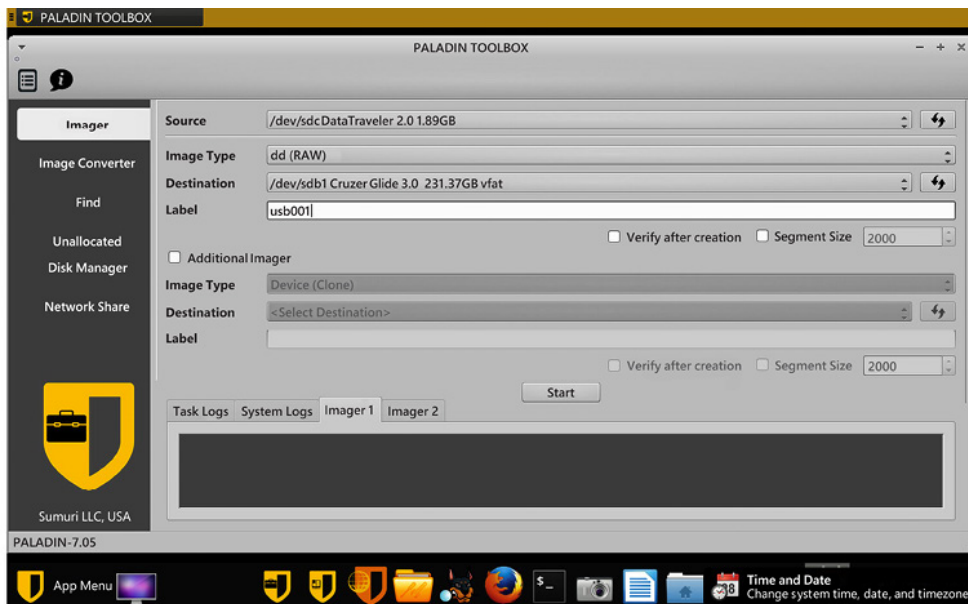


Figure 3.38: PALADIN – Toolbox imager

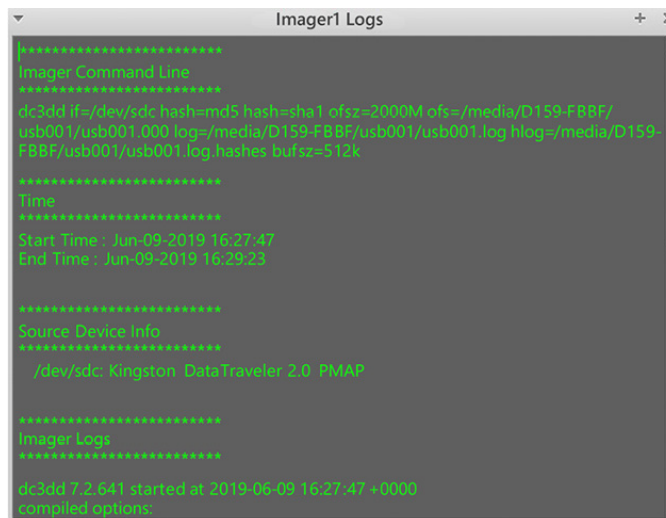


Figure 3.39: PALADIN – Completed imaging screen

Links

Zatyko, K., 2011. Commentary: Defining Digital Forensics. Retrieved from <http://www.forensicmag.com/>

Chapter 4

Images

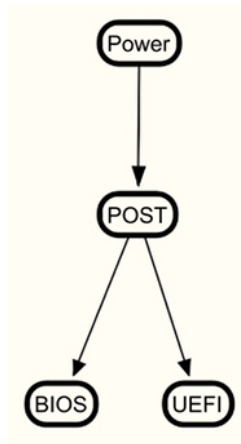


Figure 4.1: Boot process

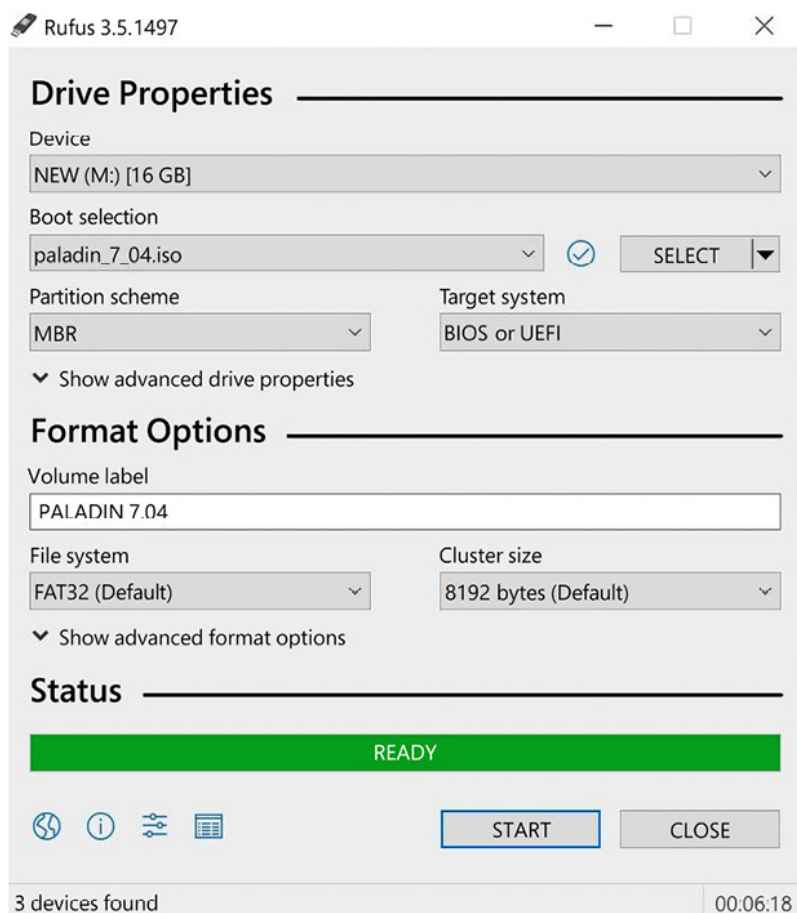


Figure 4.2: Rufus



Figure 4.3: Hard drive

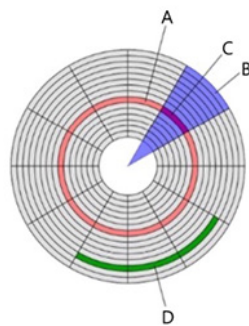


Figure 4.4: Drive diagram

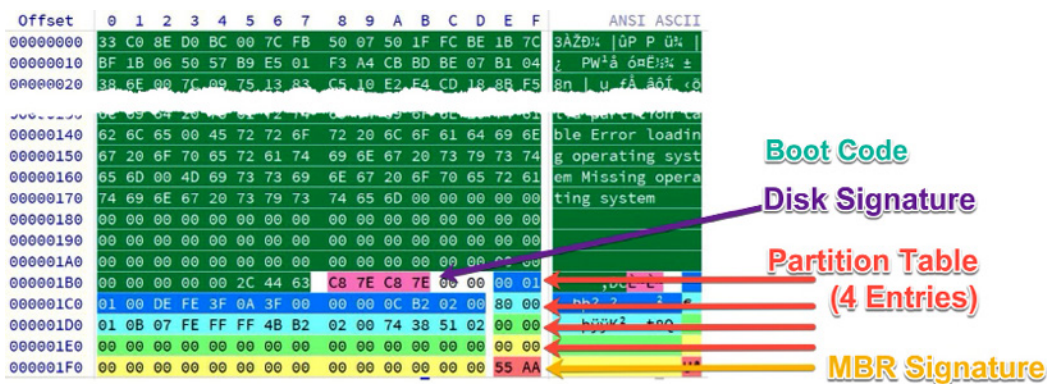


Figure 4.5: MBR map

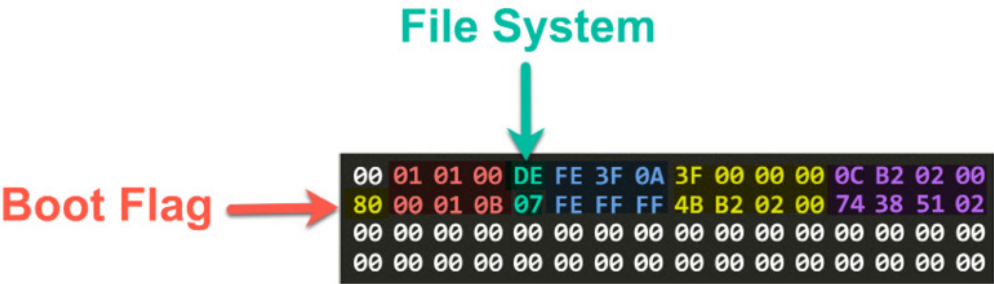


Figure 4.6: Partition tables



Figure 4.7: Partition map

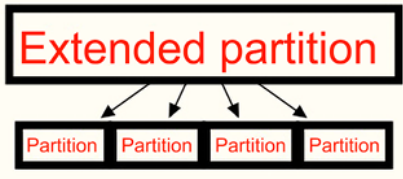


Figure 4.8: Extended partition map

000000001B0	65 6D 00 00 00 63 7B 9A 00 00 00 00 00 00 00 00
000000001C0	02 00 EE FE FF 33 01 00 00 00 FF FF FF FF 00 00
000000001D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000001E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000001F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA

Figure 4.9: GPT hex

00000000200	45 46 49 20 50 41 52 54 00 00 01 00 5C 00 00 00	EFI PART \
00000000210	6C D3 30 12 00 00 00 00 01 00 00 00 00 00 00 00	100
00000000220	80 00 00 00 80 00 00 00 04 00 00 00 00 00 00 00	0- 00
00000000230	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Figure 4.10: EFI PART

GPT header format

Offset	Length	Contents
0 (0x00)	8 bytes	Signature ("EFI PART", 45h 46h 49h 20h 50h 41h 52h 54h)
8 (0x08)	4 bytes	Revision (for GPT version 1.0 (through at least UEFI version 2.7 (May 2017)), the value is 00h 00h 01h 00h)
12 (0x0C)	4 bytes	Header size
16 (0x10)	4 bytes	CRC32 checksum of the GPT header
20 (0x14)	4 bytes	Reserved; must be zero
24 (0x18)	8 bytes	Current LBA (location of this header copy)
32 (0x20)	8 bytes	Backup LBA (location of the other header copy)
40 (0x28)	8 bytes	First usable LBA for partitions (primary partition table last LBA + 1)
48 (0x30)	8 bytes	Last usable LBA (secondary partition table first LBA – 1)
56 (0x38)	16 bytes	Disk GUID in mixed endian
72 (0x48)	8 bytes	Starting LBA of array of partition entries (always 2 in primary copy)
80 (0x50)	4 bytes	Number of partition entries in array
84 (0x54)	4 bytes	Size of a single partition entry (usually 80h or 128)
88 (0x58)	4 bytes	CRC32 checksum of the of the partition table
92 (0x5C)	*	Reserved; must be zeroes for the rest of the block (420 bytes for a sector size of 512 bytes; but can be more with larger sector sizes)

Figure 4.11: GPT header format

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0000000400	A4	BB	94	DE	D1	06	40	4D	A1	6A	BF	D5	01	79	D6	AC	»"bÑ @M;jzÖ yÖ-
0000000410	C4	04	7F	C0	41	4E	2D	46	9C	B1	AA	A1	9A	A8	07	FC	Ä ÄAN-Fœ±*;š" ü
0000000420	00	08	00	00	00	00	00	00	FF	9F	0F	00	00	00	00	00	ÿÿ
0000000430	01	00	00	00	00	00	00	80	42	00	61	00	73	00	69	00	€B a s i
0000000440	63	00	20	00	64	00	61	00	74	00	61	00	20	00	70	00	c d a t a p
0000000450	61	00	72	00	74	00	69	00	74	00	69	00	6F	00	6E	00	a r t i t i o n
0000000460	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000470	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000480	28	73	2A	C1	1F	F8	D2	11	BA	4B	00	A0	C9	3E	C9	3B	(s*Á øÒ °K É>É;
0000000490	4A	0C	5D	1C	1C	51	E1	4F	94	D5	FC	6D	48	0F	27	86	J] Qáo"ÖümH '†
00000004A0	00	A0	0F	00	00	00	00	00	FF	B7	12	00	00	00	00	00	ÿ·
00000004B0	00	00	00	00	00	00	00	80	45	00	46	00	49	00	20	00	€E F I
00000004C0	73	00	79	00	73	00	74	00	65	00	6D	00	20	00	70	00	s y s t e m p
00000004D0	61	00	72	00	74	00	69	00	74	00	69	00	6F	00	6E	00	a r t i t i o n
00000004E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000004F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000500	16	E3	C9	E3	5C	0B	B8	4D	81	7D	F9	2D	F0	02	15	AE	ãÉä\ ,M }ù-ø °
0000000510	C2	6D	C0	11	34	28	79	4E	87	FA	CD	56	0B	1D	F1	C3	ÄmÄ 4(yN†úÍV ñÄ
0000000520	00	B8	12	00	00	00	00	00	FF	37	13	00	00	00	00	00	, ÿ7
0000000530	00	00	00	00	00	00	00	80	4D	00	69	00	63	00	72	00	€M i c r
0000000540	6F	00	73	00	6F	00	66	00	74	00	20	00	72	00	65	00	o s o f t r e
0000000550	73	00	65	00	72	00	76	00	65	00	64	00	20	00	70	00	s e r v e d p
0000000560	61	00	72	00	74	00	69	00	74	00	69	00	6F	00	6E	00	a r t i t i o n
0000000570	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000580	A2	A0	D0	EB	E5	B9	33	44	87	C0	68	B6	B7	26	99	C7	¢ Ðëä¹3D†Àh¶·&™Ç
0000000590	21	1F	93	09	AF	7F	A9	44	81	D8	1E	73	C1	4B	9E	AF	! " °D Ø sÁKž~
00000005A0	00	38	13	00	00	00	00	00	FF	0F	9E	3B	00	00	00	00	8 ÿ ž;
00000005B0	00	00	00	00	00	00	00	00	42	00	61	00	73	00	69	00	B a s i
00000005C0	63	00	20	00	64	00	61	00	74	00	61	00	20	00	70	00	c d a t a p
00000005D0	61	00	72	00	74	00	69	00	74	00	69	00	6F	00	6E	00	a r t i t i o n
00000005E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000005F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Figure 4.12: GPT sector 2

GUID partition entry format		
Offset	Length	Contents
0 (0x00)	16 bytes	Partition type GUID
16 (0x10)	16 bytes	Unique partition GUID
32 (0x20)	8 bytes	Starting LBA
40 (0x28)	8 bytes	Ending LBA
48 (0x30)	8 bytes	Attribute flags
56 (0x38)	72 bytes	Partition name

Figure 4.13: GUID

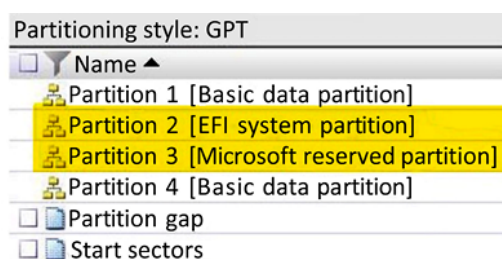


Figure 4.14: How HPA may appear in X-Ways

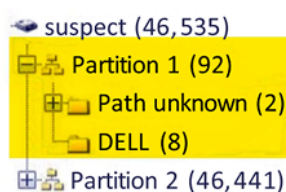


Figure 4.15: How HPA may appear in FTK Imager



Figure 4.16: FAT areas

EB 58 90	4D 53 44 4F 53	35 2E 30	00 02 08 2A 20
02 00 00 00 00 F8 00 00	3F 00 FF 00 80 00 00 00		
00 E8 3F 00 EB 0F 00 00	00 00 00 00 02 00 00 00		
01 00 06 00 00 00 00 00	00 00 00 00 00 00 00 00		
80 00 29 D9 7C BE FC 4E	4F 20 4E 41 4D 45 20 20		
20 20 46 41 54 33 32 20	20 20 33 C9 8E D1 BC F4		
7B 8E C1 8E D9 BD 00 7C	88 56 40 88 4E 02 8A 56		
61 72 74 0D 0A 00 00 00	00 00 00 00 00 00 00 00		
00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00 00 00 00 00 00 00 00	AC 01 B9 01 00 00 55 AA		

Figure 4.17: VBR

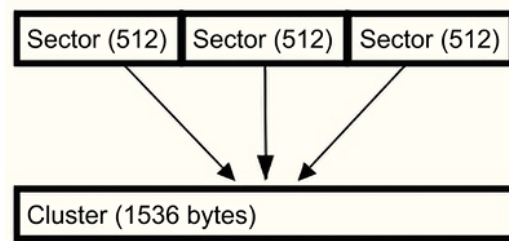


Figure 4.18: Cluster example

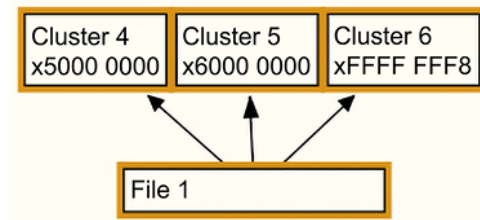


Figure 4.19: Non-fragmented file entry

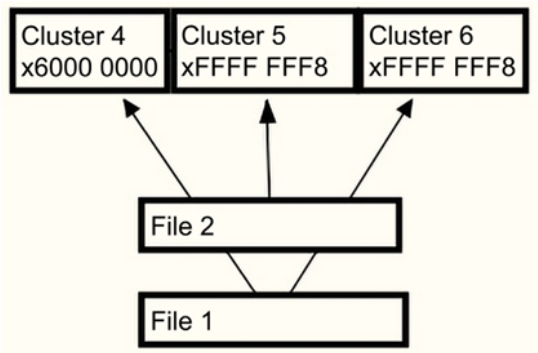


Figure 4.20:Fragmented file entry

Unused Entry	E5 6C 00 6F 00 6E 00 67 00 66 00 0F 00 D4 69 00	ál.o.n.g.f...Öi.
	6C 00 65 00 6E 00 61 00 6D 00 00 00 65 00 2E 00	l.e.n.a.m...e...
	E5 4F 4E 47 46 49 7E 31 54 58 54 20 00 6B B0 6D	ãONGFI~1TXT .k°m
	D3 4E D3 4E 00 00 B1 6D D3 4E 00 00 00 00 00 00	ÓNÓN...±mÓN.....
	53 48 4F 52 54 20 20 20 54 58 54 20 18 6B B0 6D	SHORT TXT .k°m
	D3 4E D3 4E 00 00 93 6D D3 4E 00 00 00 00 00 00	ÓNÓN...mÓN.....
	24 52 45 43 59 43 4C 45 42 49 4E 16 00 30 B5 6D	\$RECYCLEBIN..0µm
	D3 4E D3 4E 00 00 B6 6D D3 4E 06 00 00 00 00 00	ÓNÓN...¶mÓN.....
	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00 00 00 00 00 00 00 00 00 00 00 00 00 00

Figure 4.21: FAT directory entry

Offset (hex)	Size (Bytes)	Description
x00	1	The first character of the file name or status byte
x01	7	Filename (padded with spaces if required)
x08	3	Three characters of the file extension
x0B	1	Attributes
x0C	1	Reserved
x0D	1	Created time and date of the file
x0E	2	File creation time
x10	2	File creation date
x12	2	Last accessed date
x14	2	Two high bytes of FAT32 starting cluster
x16	2	Time of the Last Write to File (last modified or when created)
x18	2	Date of the Last Write to File (last modified or when created)
0x1A	2	Two low bytes of the starting cluster for FAT32
0X1C	4	File size (zero for a directory)

53 48 4F 52 54 20 20 20

54 58 54 20

18 6B B0 6D

SHORT TXT.k°m

D3 4E D4 4E 00 00 E9 5E D4 4E 08 00 27 00 00 00

ONON..é~ON..'...

Figure 4.22: FAT directory map

0000 0001	READ ONLY
0000 0010	HIDDEN FILE
0000 0100	SYSTEM FILE
0000 1000	VOLUME LABEL
0000 1111	LONG FILENAME
0001 0000	DIRECTORY
0010 0000	ARCHIVE

Figure 4.23: Packed byte

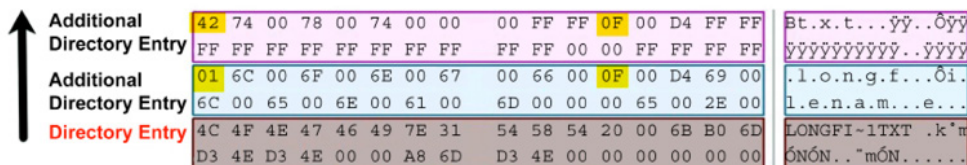


Figure 4.24: LFN

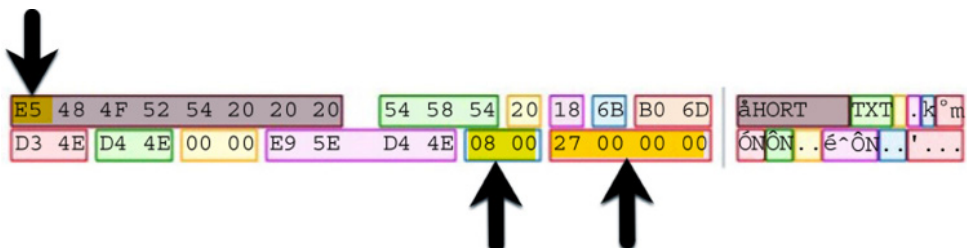


Figure 4.25: Deleted entry

Bytes per sector	011	512	15
Sectors per cluster	013	8	114

Figure 4.26: Boot record

```
00 00 00 00 FF FF FF 0F 0B 00 00 00 0C 00 00 00
0D 00 00 00 0E 00 00 00 0F 00 00 00 10 00 00 00
```

Figure 4.27: Deleted FAT

\$MFT	Describes all files on the volume, including file names, timestamps, stream names, and lists of cluster numbers where data streams reside, indexes, security identifiers, and file attributes.
\$MFTMirr	Duplicate of the first vital entries of \$MFT, usually 4 entries (4 kb).
\$LogFile	Contains transaction log of file system metadata changes.
\$Volume	Contains information about the volume, namely the volume object identifier, volume label, file system version, and volume flags.
\$AttrDef	A table of MFT attributes that associates numeric identifiers with names.
\$ (Root file name index)	The root folder.
\$Bitmap	Tracks the allocation status of all clusters in the partition.
\$Boot	Volume boot record.
\$BadClus	A file that contains all the clusters marked as having bad sectors.
\$Secure	Access control list database.
\$UpCase	Converts lowercase characters to matching Unicode uppercase characters.
\$Extend	A file system directory containing various optional extensions, such as \$Quota, \$ObjId, \$Reparse, or \$UsnJrnl.

Figure 4.28: NTFS table

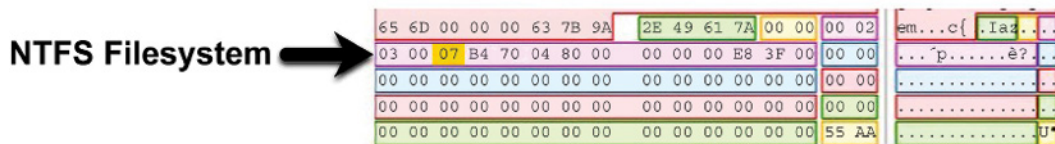


Figure 4.29: NTFS MBR

EB 52 90	4E 54 46 53 20	20 20 20	00 02 08 00 00	ER.NTFS
00 00 00 00 00 F8 00 00	3F 00 FF 00 80 00 00 00		ø..?.ý
00 00 00 00 80 00 80 00	FF E7 3F 00 00 00 00 00		ÿç?
AA A9 02 00 00 00 00 00	02 00 00 00 00 00 00 00			*@.....
F6 00 00 00 01 00 00 00	66 20 92 02 61 92 02 7C			ö.....f ..a..
00 00 00 00	FA 33 C0 8E	D0 BC 00 7C FB 68 C0 07	ú3Ä.Ð¼. ûhÄ.
0A 50 72 55 73 75 20 45	74 72 6C 2B 41 6C 74 2B			.press Ctrl+Alt+
44 65 6C 20 74 6F 20 72	65 73 74 61 72 74 0D 0A			Del to restart..
00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00 00 00 00 00 00 8A 01	A7 01 BF 01 00 00	55 AA	\$.¿...U°

Figure 4.30: NTFS VBR

JMP instruction	000	EB 52 90
OEM ID	003	NTFS
▼ BIOS Parameter Block	00B	
Bytes per sector	00B	512
Sectors per cluster	00D	8
Reserved sectors	00E	0
(always zero)	010	00 00 00
(unused)	013	00 00
Media descriptor	015	248
(unused)	016	00 00
Sectors per track	018	63
Number of heads	01A	255
Hidden sectors	01C	128
(unused)	020	00 00 00 00
Signature	024	80 00 80 00
Total sectors	028	4,188,159
SMFT cluster number	030	174,506
SMFTMirr cluster number	038	2
Clusters per File Record Segment	040	246
Clusters per Index Block	044	1
Volume serial number	048	66 20 92 02 61 92 02 7C
Checksum	050	0
Bootstrap code	054	FA 33 C0 8E D0 BC 00 7C
Signature (55 AA)	1FE	55 AA

Figure 4.31: \$Boot record

46 49 4C 45	30 00	03 00	39 6B 20 00 00 00 00 00	FILE0...9k
01 00	01 00	38 00	01 00	...8...Ø.....
00 00 00 00 00 00 00 00	04 00	00 00	28 00 00 00 00 (...)
03 00	00 00 00 00	00 00	10 00 00 00 60 00 00 00`
00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	00 00 00 00 00 00 00 00	30 00 00 00 80 00 00 00H.....
00 00 00 00 08 01 00 00	00 00 00 00 00 00 00 00	30 00 00 00 80 00 00 00	62 00 00 00 18 00 01 000.....
00 00 00 00 00 00 00 00	10 00 6C 00 6F 00 6E 00	67 00 66 00 69 00 6C 00	65 00 2E 00 74 00 78 00b.....
74 00 00 00 00 00 00 00	80 00 00 00 18 00 00 00	00 00 00 00 18 00 00 00	00 00 00 00 18 00 00 00	..l.o.n.g.f.i.l.
00 00 18 00 00 00 01 00	00 00 00 00 18 00 00 00	00 00 00 00 18 00 00 00	00 00 00 00 18 00 00 00	e.n.a.m.e...t.x.
80 00 00 00 A0 00 00 00	00 16 18 00 00 00 03 00	00 16 18 00 00 00 03 00	00 16 18 00 00 00 03 00	t.....
F3 D0 1C A7 50 97 F4 8A	E2 74 67 93 FC 80 74 47	E2 74 67 93 FC 80 74 47	E2 74 67 93 FC 80 74 47
5B 5B A5 DA DA 5A 00 CB	B7 1C B0 00 00 00 00 00	B7 1C B0 00 00 00 00 00	B7 1C B0 00 00 00 00 00	6Ð.SP.ð.â tg.û.tG
FF FF FF FF	82 79 47 11	82 79 47 11	82 79 47 11	[[¥ÚÚZ.E . °
				yyyy

Figure 4.32: NTFS file record

Signature (must be 'FILE')	000	FILE
Offset to the update sequence	004	0x30
Update sequence size in words	006	3
\$LogFile Sequence Number (LSN)	008	2,124,601
Sequence number	010	1
Hard link count	012	1
Offset to the first attribute	014	0x38
Flags	016	01 00
Real size of the FILE record	018	472
Allocated size of the FILE record	01C	1,024
Base FILE record	020	0
Next attribute ID	028	4
ID of this record	02C	40
Update sequence number	030	03 00
Update sequence array	032	00 00 00 00
Attribute \$10	038	
Attribute \$30	098	
Attribute \$80	118	
Attribute \$80	130	
End marker	1D0	0xFFFFFFFF

Figure 4.33: NTFS file record map

\$Standard Information - 0x10	Includes information such as timestamp and link count.
\$Attribute List - 0x20	Lists the location of all attribute records that do not fit in the MFT record.
\$File Name - 0x30	<p>A repeatable attribute for both long and short file names. The long name of the file can be up to 255 Unicode characters.</p> <p>The short name is the 8.3 case-insensitive name for the file. Additional names, or hard links, required by POSIX can be included as additional file name attributes.</p>
\$Security Descriptor - 0x50	Describes who owns the file and who can access it.
\$Data - 0x80	Contains file data. NTFS allows multiple data attributes per file. Each file type has one unnamed data attribute. A file can also have one or more named data attributes.

Figure 4.34: File attributes table

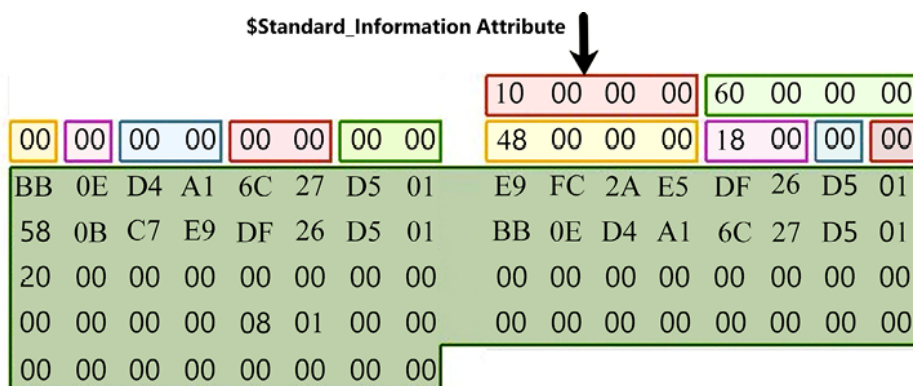


Figure 4.35: \$Standard_Information Attribute

Attribute \$10	038	
Attribute type	038	0x10
Length (including header)	03C	96
Non-resident flag	040	0
Name length	041	0
Name offset	042	0x00
➤ Flags	044	00 00
Attribute ID	046	0
Length of the attribute	048	72
Offset to the attribute data	04C	0x18
Indexed flag	04E	0
Padding	04F	0
▼ \$STANDARD_INFORMATION	050	
File created (UTC)	050	6/20/2019 1:32 PM
File modified (UTC)	058	6/19/2019 8:45 PM
Record changed (UTC)	060	6/19/2019 8:45 PM
Last access time (UTC)	068	6/20/2019 1:32 PM
➤ File Permissions	070	20 00 00 00
Maximum number of versions	074	0
Version number	078	0
Class Id	07C	0
Owner Id	080	0
Security Id	084	264
Quota Charged	088	0
Update Sequence Number	090	0

Figure 4.36: File attribute map

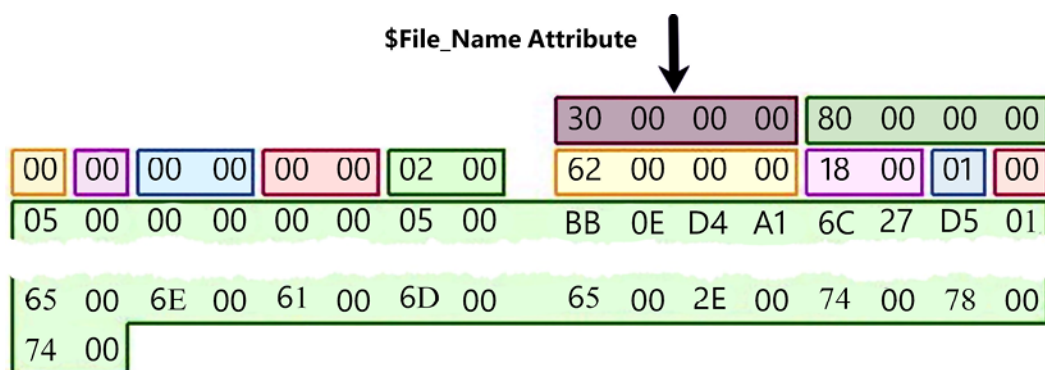


Figure 4.37: \$File_Name Attribute

Attribute \$30		098	
Attribute type	098	0x30	
Length (including header)	09C	128	
Non-resident flag	0A0	0	
Name length	0A1	0	
Name offset	0A2	0x00	
➤ Flags	0A4	00 00	
Attribute ID	0A6	2	
Length of the attribute	0A8	98	
Offset to the attribute data	0AC	0x18	
Indexed flag	0AE	1	
Padding	0AF	0	
▼ \$FILE_NAME	0B0		
Parent directory file record number	0B0	5	
Parent directory sequence number	0B6	5	
File created (UTC)	0B8	6/20/2019 1:32 PM	
File modified (UTC)	0C0	6/20/2019 1:32 PM	
Record changed (UTC)	0C8	6/20/2019 1:32 PM	
Last access time (UTC)	0D0	6/20/2019 1:32 PM	
Allocated size	0D8	0	
Real size	0E0	0	
➤ File attributes	0E8	20 00 00 00	
(used by EAs and reparse)	0EC	0	
File name length	0F0	16	
File name namespace	0F1	0	
File name	0F2	longfilename.txt	

Figure 4.38: Filename attribute map

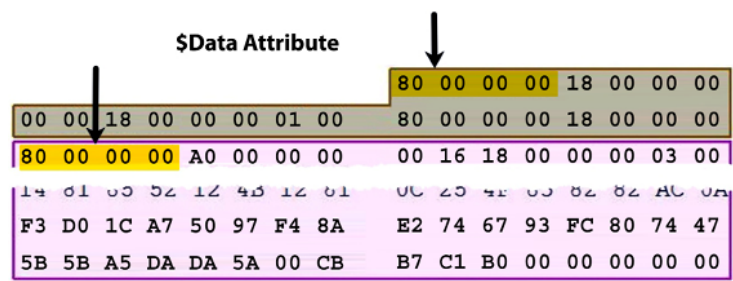


Figure 4.39: \$Data Attribute

Attribute \$80	130	
Attribute type	130	0x80
Length (including header)	134	160
Non-resident flag	138	0
Name length	139	22
Name offset	13A	0x18
> Flags	13C	00 00
Attribute ID	13E	3
Length of the attribute	140	83
Offset to the attribute data	144	0x48
Indexed flag	146	0
Padding	147	0
Attribute Name	148	com.dropbox.attributes
▼ \$DATA	178	
Data	178	78 9C AB 56 4A 29 CA 2F 48
End marker	1D0	0xFFFFFFFF

Figure 4.40: Data attribute map

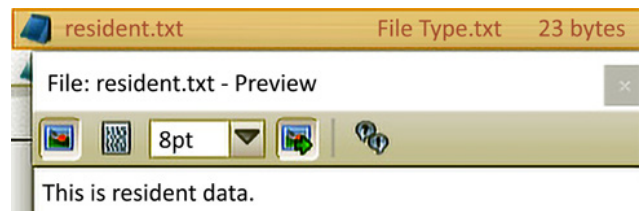


Figure 4.41: Resident data file

\$Data Attribute

00 00 18 00 00 00 01 00	80 00 00 00	30 00 00 000...
54 68 69 73 20 69 73 20	17 00 00 00	18 00 00 00
20 64 61 74 61 2E 20 00	72 65 73 69 64 65 6E 74		This is resident data. .

Figure 4.42: Resident data example

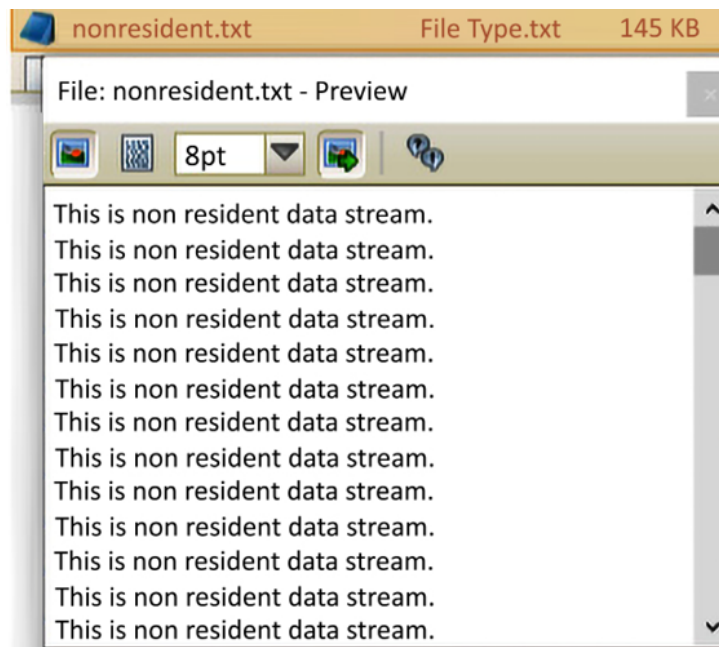


Figure 4.43: Non-resident data

01 00 00 00 00 00 06 00	80 00 00 00	48 00 00 00H...
24 00 00 00 00 00 00 00	00 00 00 00	00 00 00 00
00 50 02 00 00 00 00 00	40 00 00 00	00 00 00 00	\$.....@.....
30 43 02 00 00 00 00 00	30 43 02 00	00 00 00 00	.P.....0C.....
	11 25 26 00	00 00 00 00	0C.....%&.....

Figure 4.44: Non-resident data example

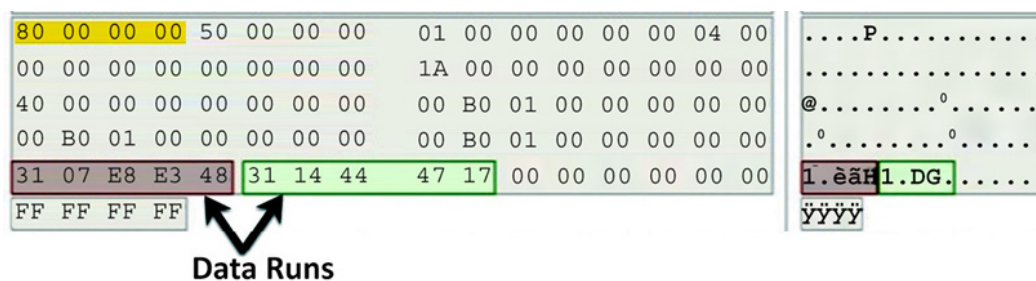


Figure 4.45: Run list

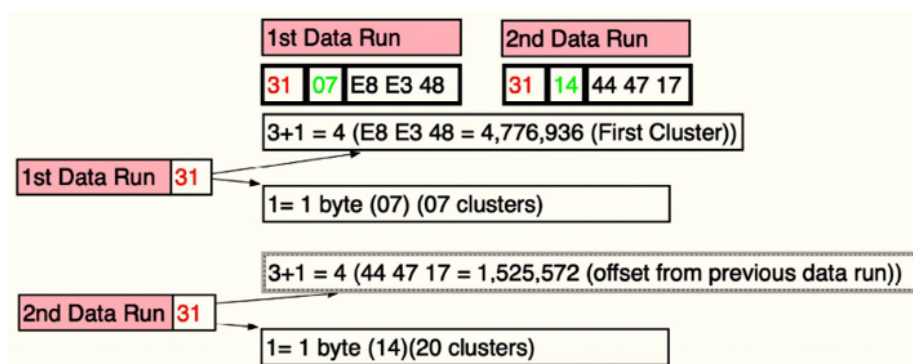


Figure 4.46: Run list map

Links

- You can find a full list of partition identifiers at https://www.win.tue.nl/~aeb/partitions/partition_types-1.html
- Carrier, B. File System Forensic Analysis. Addison-Wesley, Reading, PA., Mar. 2005 (available at <https://www.kobo.com/us/en/ebook/file-system-forensic-analysis-1>)

Chapter 5

Images

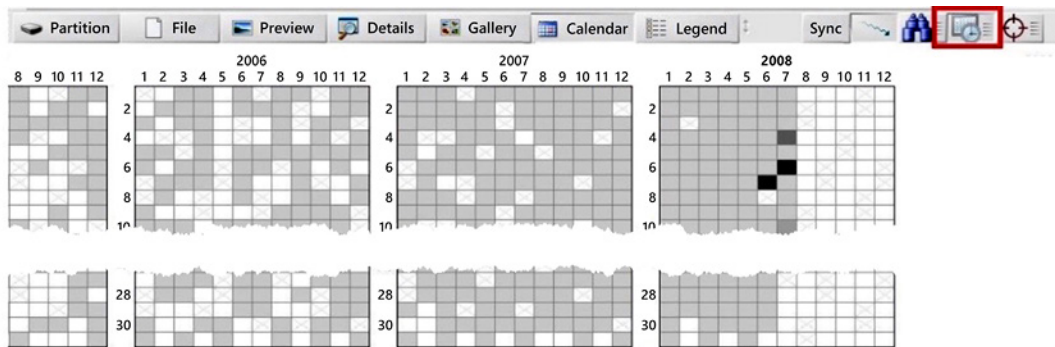


Figure 5.1: X-Ways

07/20/2008 01:27:42.0	Access	Internal file...	C:\Documents and Sett...	Temp.LNK	lnk	0.5 KB	07/20/2008 01:27:42.5
07/20/2008 01:27:42.1	Key changed	Registry	\Software\Microsoft\Int...	REGISTRY_USER_NTUSER_5-1-5-21-484763869-796845957...	registry	660 KB	07/20/2008 02:00:13.0
07/20/2008 01:27:42.5 +0	Creation	File system		m57biz.LNK	lnk	408 B	07/20/2008 01:27:42.5 +0
07/20/2008 01:27:42.5	Access	File system		desktop.ini	ini1	62 B	07/06/2008 06:11:22.7

Figure 5.2: Filter results

07/20/2008 01:27:59.7 +0	Key changed	Registry	\Software\Microsoft\Offi...	REGISTRY_USER_NTUSER_5-1-5-21-484763869-796845957...	registry	768 KB	07/06/2008 06:11:22.3 +0
07/20/2008 01:27:59.7 +0	Key changed	Registry	\Software\Microsoft\Offi...	REGISTRY_USER_NTUSER_5-1-5-21-484763869-796845957...	registry	768 KB	07/06/2008 06:11:22.3 +0
07/20/2008 01:28:00 +0	Record chan...	Messaging		RE: Please send me the information now.eml (2)	eml	1.0 KB	07/20/2008 01:28:47.8 +0

Figure 5.3: Jean's email

Subject	RE: Please send me the information now
Date	07/20/2008 01:28:47 +0
Sender	Jean User <jean@m57.biz>
Recipients	tuckgorge@gmail.com
Attachments	m57biz.xls

I've attached the information that you have requested to this email message.

----- Original Message -----

From: alison@m57.biz [mailto:tuckgorge@gmail.com]

Sent: Sunday, July 20, 2008 2:23 AM

To: jean@m57.biz

Subject: Please send me the information now

Hi, Jean.

I'm sorry to bother you, but I really need that information now --- this VC guy is being very insistent. Can you please reply to this email with the information I requested --- the names, salaries, and social security numbers (SSNs) of all our current employees and intended hires?

Thanks.

Alison

E-mail Header
Date: 20 Jul 2008 01:28:47 -0000 From: Jean User <jean@m57.biz> Sender: Jean User <jean@m57.biz> To: <tuckgorge@gmail.com> Subject: RE: Please send me the information now Importance: Normal Mime-Version: 1.0 Content-Type: multipart/mixed; boundary="-----_NextPart_0"

Figure 5.4: Jean's email header

```
c:\tools\plaso>image_export.exe -h
usage: image_export.exe [-h] [--troubles] [-V] [-d] [-q]
                        [--artifact_definitions PATH]
                        [--custom_artifact_definitions PATH] [--data PATH]
                        [--logfile FILENAME] [--partitions PARTITIONS]
                        [--volumes VOLUMES] [--no_vss] [--vss_only]
                        [--vss_stores VSS_STORES]
                        [--artifact_filters ARTIFACT_FILTERS]
                        [--artifact_filters_file PATH]
                        [--date-filter TYPE_START_END] [-f FILE_FILTER]
                        [-x EXTENSIONS] [--names NAMES]
                        [--signatures IDENTIFIERS] [-w PATH]
                        [--include_duplicates]
                        [IMAGE]
```

Figure 5.5: image_export

```
image_export --names 'm57biz.xls' C:\tools\plaso\image\jean.001 -w C:\tools\plaso\export\files
```

command

modifier

source

destination

Figure 5.6: CLI map

```
c:\tools\plaso>log2timeline.exe -h
usage: log2timeline.exe [-h] [--troubles] [-V] [--artifact_definitions PATH]
                        [--custom_artifact_definitions PATH] [--data PATH]
                        [--artifact_filters ARTIFACT_FILTERS]
                        [--artifact_filters_file PATH] [--preferred_year YEAR]
                        [--process_archives] [--skip_compressed_streams]
                        [-f FILE_FILTER] [--hasher_file_size_limit SIZE]
                        [--hashers HASHER_LIST]
                        [--parsers PARSER_FILTER_EXPRESSION]
                        [--yara_rules PATH] [--partitions PARTITIONS]
                        [--volumes VOLUMES] [-z TIMEZONE] [--no_vss]
                        [--vss_only] [--vss_stores VSS_STORES]
                        [--credential TYPE:DATA] [-d] [-q] [--info]
                        [--use_markdown] [--no_dependencies_check]
                        [--logfile FILENAME] [--status_view TYPE] [-t TEXT]
                        [--buffer_size BUFFER_SIZE] [--queue_size QUEUE_SIZE]
                        [--single_process] [--temporary_directory DIRECTORY]
                        [--worker_memory_limit SIZE] [--workers WORKERS]
                        [--sigsegv_handler] [--profilers PROFILERS_LIST]
                        [--profiling_directory DIRECTORY]
                        [--profiling_sample_rate SAMPLE_RATE]
                        [--storage_format FORMAT]
                        [--task_storage_format FORMAT]
                        [STORAGE_FILE] [SOURCE]
```

Figure 5.7: log2timeline

```

***** Parser Presets *****
Name : Description
-----
android : android_app_usage, chrome_cache, filestat, sqlite/android_calls,
          sqlite/android_sms, sqlite/android_webview,
          sqlite/android_webviewcache, sqlite/chrome_27_history,
          sqlite/chrome_8_history, sqlite/chrome_cookies, sqlite/skype
linux : bash_history, bencode, czip/oxml, dockerjson, dpkg, filestat,
        gdrive_synclog, olecf, pls_recall, popularity_contest, selinux,
        sqlite/google_drive, sqlite/skype, sqlite/zeitgeist, syslog,
        systemd_journal, utmp, webhist, xchatlog, xchatscrollback,
        zsh_extended_history
macos : asl_log, bash_history, bencode, bsm_log, cups_ipp, czip/oxml,
        filestat, fseventsd, gdrive_synclog, mac_appfirewall_log,
        mac_keychain, mac_securityd, macwifi, olecf, plist,
        sqlite/appusage, sqlite/google_drive, sqlite/imessage,
        sqlite/ls_quarantine, sqlite/mac_document_versions,
        sqlite/mac_notes, sqlite/mackeeper_cache, sqlite/mac_knowledge,
        sqlite/skype, syslog, utmpx, webhist, zsh_extended_history
webhist : binary_cookies, chrome_cache, chrome_preferences,
          esedb/msie_webcache, firefox_cache, java_idx, msiecf,
          opera_global, opera_typed_history, plist/safari_history,
          sqlite/chrome_27_history, sqlite/chrome_8_history,
          sqlite/chrome_autofill, sqlite/chrome_cookies,
          sqlite/chrome_extension_activity, sqlite/firefox_cookies,
          sqlite/firefox_downloads, sqlite/firefox_history
win7 : amcache, custom_destinations, esedb/file_history,
       olecf/olecf_automatic_destinations, recycle_bin, winevtx, win_gen
win7_slow : mft, win7
win_gen : bencode, czip/oxml, esedb, filestat, gdrive_synclog, lnk,
          mcafee_protection, olecf, pe, prefetch, sccm, skydrive_log,
          skydrive_log_old, sqlite/google_drive, sqlite/skype,
          symantec_scanlog, usnjournal, webhist, winfirewall, winjob, winreg
winxp : recycle_bin_info2, rplog, win_gen, winevt
winxp_slow : mft, winxp
-----

```

Figure 5.8: Results of the info modifier

```

c:\tools\plaso>log2timeline C:\tools\plaso\export\files\jean.plaso C:\tools\plaso\image\jean.001
2022-02-02 13:00:51,847 [INFO] (MainProcess) PID:15324 <data_location> Determined data location: c:\tools\plaso\data
2022-02-02 13:00:51,862 [INFO] (MainProcess) PID:15324 <artifact_definitions> Determined artifact definitions path: c:\tools\plaso\artifacts
Checking availability and versions of dependencies.
[OPTIONAL] missing: lz4.
[OK]

```

Figure 5.9: Output

```
c:\tools\plaso>log2timeline -f filter_windows.txt C:\tools\plaso\export\files\jeanfilter.plaso C:\tools\plaso\image\jean.001
2022-02-02 13:10:51.785 [INFO] (MainProcess) PID:7896 <data_location> Determined data location: c:\tools\plaso\data
2022-02-02 13:10:51.799 [INFO] (MainProcess) PID:7896 <artifact_definitions> Determined artifact definitions path: c:\tools\plaso\artifacts
Checking availability and versions of dependencies.
[OPTIONAL] missing: lz4.
[OK]
```

Figure 5.10: Filter

```
c:\tools\plaso>pinfo -h
usage: pinfo [-h] [--troubles] [-V] [--compare STORAGE_FILE]
             [--output_format FORMAT] [-V] [-w OUTPUTFILE]
             [STORAGE_FILE]

Shows information about a Plaso storage file, for example how it was collected, what information was extracted from a source, etc.

positional arguments:
  STORAGE_FILE          Path to a storage file.

optional arguments:
  -h, --help            Show this help message and exit.
  --troubles            Show troubleshooting information.
  -V, --version         Show the version information.
  --compare STORAGE_FILE
                        The path of the storage file to compare against.
  --output_format FORMAT, --output-format FORMAT
                        Format of the output, the default is: text. Supported
                        options: json, text.
  -v, --verbose         Print verbose output.
  -w OUTPUTFILE, --write OUTPUTFILE
                        Output filename.
```

Figure 5.11: pinfo

```
c:\tools\plaso>psort -h
usage: psort [-h] [--troubles] [-V] [--analysis PLUGIN_LIST]
             [--temporary_directory DIRECTORY] [--worker-memory-limit SIZE]
             [--logfile FILENAME] [-d] [-q] [--status_view TYPE]
             [--slice DATE] [--slice_size SLICE_SIZE] [--slicer] [--data PATH]
             [-a] [--language LANGUAGE] [-z TIMEZONE] [-o FORMAT]
             [-w OUTPUT_FILE] [--fields FIELDS]
             [--additional_fields ADDITIONAL_FIELDS]
             [--profilers PROFILERS_LIST] [--profiling_directory DIRECTORY]
             [--profiling_sample_rate SAMPLE_RATE]
             [STORAGE_FILE] [FILTER]
```

Figure 5.12: psort

***** Analysis Plugins *****	
Name	Description
browser_search	Analyze browser search entries from events. [Summary/Report plugin]
chrome_extension	Convert Chrome extension IDs into names, requires Internet connection. [Summary/Report plugin]
file_hashes	A plugin for generating a list of file paths and corresponding hashes. [Summary/Report plugin]
nsrslvr	Analysis plugin for looking up hashes in nsrslvr. [Summary/Report plugin]
sessionize	Analysis plugin that labels events by session. [Summary/Report plugin]
tagging	Analysis plugin that tags events according to rules in a tagging file. [Summary/Report plugin]
unique_domains_visited	A plugin to generate a list all domains visited. [Summary/Report plugin]
viper	An analysis plugin for looking up SHA256 hashes in Viper. [Summary/Report plugin]
virustotal	An analysis plugin for looking up hashes in VirusTotal. [Summary/Report plugin]
windows_services	Provides a single list of for Windows services found in the Registry. [Summary/Report plugin]

Figure 5.13: List of analysis plugins

```
c:\tools\plaso>psteal -h
usage: psteal [-h] [--troubles] [-V] [--preferred_year YEAR]
             [--process_archives] [--skip_compressed_streams]
             [--storage_file PATH] [--partitions PARTITIONS]
             [--volumes VOLUMES] [--credential TYPE:DATA]
             [--status_view TYPE] [--source SOURCE] [--data PATH]
             [--language LANGUAGE] [-z TIMEZONE] [-o FORMAT] [-w OUTPUT_FILE]
             [--fields FIELDS] [--additional_fields ADDITIONAL_FIELDS]
             [--buffer_size BUFFER_SIZE] [--queue_size QUEUE_SIZE]
             [--single_process] [--temporary_directory DIRECTORY]
             [--worker_memory_limit SIZE] [--workers WORKERS]

psteal is a command line tool to extract events from individual
files, recursing a directory (e.g. mount point) or storage media
image or device. The output events will be stored in a storage file.
This tool will then read the output and process the events into a CSV
file.
```

Figure 5.14: psteal

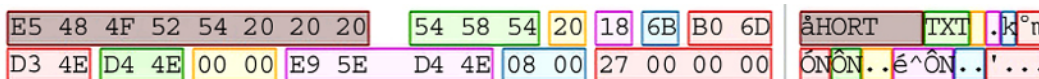


Figure 5.15: Deleted entry

Bytes per sector	011	512	15
Sectors per cluster	013	8	114

Figure 5.16: Boot record

```

00 00 00 00 FF FF FF 0F 0B 00 00 00 0C 00 00 00
0D 00 00 00 0E 00 00 00 0F 00 00 00 10 00 00 00

```

Figure 5.17: Deleted FAT

Tables

Index.dat file(s)	Browser history
LNK file(s)	USNJrnl
Registry	Event log(s)
Metadata of Microsoft Office file(s)	Email message(s)
Recycle Bin file(s)	Shadow copy file(s)
Prefetch file(s)	Restore point(s)
Cookie(s)	MAC timestamp(s)

Table 5.1 – Sources of information for the event list feature

Name	Description
dynamic	Output events to a delimiter (comma by default) separated value output format, that supports a dynamic selection of fields.
elastic	Output events to an Elasticsearch database. Requires elasticsearch-py.
elastic_ts	Output events to an Elasticsearch database for use with Timesketch. Requires elasticsearch-py. Solely intended to be used by the Timesketch backend.
json	Output events to JSON format.
json_line	Output events to JSON line format.
kml	Output events with geography data into a KML format.
l2tcsv	Output events to log2timeline.pl legacy CSV format, with 17 fixed fields.
l2ttln	Output events to log2timeline.pl extended TLN format, with 7 fixed fields.
null	Do not output events.
rawpy	Output events in “raw” (or native) Python format.
tln	Output events to TLN format, with 5 fixed fields.
xlsx	Output events to an Excel spreadsheet (XLSX).

Table 5.2 – List of available output formats

Path

MD5 hash value of m57plan.xls: e23a4eb7f2562f53e88c9dca8b26a153

Further down the screen, you will see detailed explanations for the modifiers. Note that I will only cover the most used options; there is additional documentation that we will not discuss here.

- `--names NAMES`. The filter on filenames. This option accepts a comma-separated string denoting all filenames, for example, `x enn-tee-user.dat,UsrClass.dat`.
- `-w PATH`, `--write PATH`. The directory in which extracted files should be stored.
- `--data PATH`. The path to a directory containing the data files.
- `-x EXTENSIONS`, `--extensions EXTENSIONS`. The filter on filename extensions. This option accepts multiple comma-separated values, for example, `csv, docx, and pst`.

- The info modifier: `c:\tools\plaso>log-2-timeline.exe --info`
- Output file of log-2-timeline: `log2timeline C:\tools\plaso\export\files\jean.plaso C:\tools\plaso\image\jean.001`
- Plaso installation folder: `log2timeline -f filter_windows.txt C:\tools\plaso\export\files\jeanfilter.plaso C:\tools\plaso\image\jean.001`
- To search for an IP address, you can use the following regular expression: `\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`. The `\d` specifies that the following will match on a digit (number). The curly brackets, `{1,3}`, indicate the number can be from one to three digits. `\.` specifies a search for the `.` character. The `\d{1,3}` pattern then repeats an additional three times until it has the value for an IPv4 address.
- To search for a US phone number, you can use the following expression: `((\d{3}\d{3}) | (\d{3}-)?) \d{3}-\d{4}`. The `\(` will match the open bracket. `\d{3}` will match on a three-digit number. `\)` will match on the closed bracket. This pattern will give you the area code, `(###)`, in this format. The remaining regular expression will give you the first three digits, `\d{3}`, the dash, `-`, and the final four digits, `\d{4}`, of the US phone number. If the phone number is not formatted as `(###) ###-####` or `###-###-####`, you will not get a hit.

Commands and outputs

Command 5.1

```
image underscore export --names 'm57plan.xls'
C:\tools\plaso\image\jean.001 -w C:\tools\plaso\export\files
```

Command 5.2

```
log-2-timeline OUTPUT INPUT
```

Command 5.3

```
psort -q --slice '2008-07-20 01:26:17'
:/tools/plaso/export/files/jean.plaso -w
:/tools/plaso/export/files/jeansliceoutput.csv
```

The command will create a `.csv` file, which contains events 5 minutes before and 5 minutes after the timestamp placed in the CLI.

Command 5.4

```
psteal --source C:/tools/plaso/image/jean.001 -o l2tcsv -w
:/tools/plaso/export/files/jean.csv
```

Here's the command. It creates a .csv file that is almost 1 GB in size. However, if I change the output to .xlsx, it reduces the size to 35 MB. So, keep in mind that you are processing and analyzing your datasets.

output 5.1: Output of the ping command

```
-----
***** Plaso Storage Information
*****
Filename: jeanfilter.plaso
Format version: 20190309
Serialization format: JSON
-----
***** Sessions
*****
276a7520-999e-428b-a6b4-11fcf9cf987d :
2019-07-19T22:19:36.092703Z
-----
```

Output 5.2 System information

```
-----
-----
***** System configuration: 276a7520-999e-428b-a6b4-
11fcf9cf987d *****
Hostname: N/A
Operating system: Windows NT
Operating system product: Microsoft Windows XP
Operating system version: 5.1
Code page : cp1252
Keyboard layout: N/A
Time zone: GMT
-----
-----
```

Output 5.3

```
***** Analysis report: 0
*****
String: Report generated from tagging
Generated on:2019-07-20T20:04:46.000000Z
Report text: Tagging plugin produced 9754 tags
-----
```

Links

- Belkasoft Evidence Center: belkasoft.com/ec
- Autopsy: www.sleuthkit.org/autopsy
- Recon Lab: sumuri.com/software/recon-lab
- Paladin: sumuri.com/software/paladin

Plaso: <https://github.com/log-2-timeline/plaso>

- If you want to download some premade filters, you can do so at https://github.com/mark-hallman/plaso_filters.
- Plaso Documentation: <https://buildmedia.readthedocs.org/media/pdf/plaso/latest/plaso.pdf>
- Windows forensic analysis toolkit: Advanced analysis techniques for Windows 8; Waltham, MA: Syngress: https://www.abebooks.com/servlet/SearchResults?sts=t&cm_sp=SearchF-_-home-_-Results&an=&tn=Windows+forensic+analysis+toolkit&kn=&isbn=

Output

Output 5.1

```
-----
***** Plaso Storage Information
*****
Filename. jeanfilter.plaso
Format version. 20190309
Serialization format. Jason
-----
```

```
***** Sessions
*****
```

```
276a7520-999e-428b-a6b4-11fcf9cf987d .
2019-07-19T22.19.36.092703Z
```

```
-----
```

Output 5.2

```
-----
-----
```

```
***** System configuration. 276a7520-999e-428b-a6b4-
11fcf9cf987d *****
```

```
Hostname. N/A
```

```
Operating system. Windows NT
```

```
Operating system product. Microsoft Windows XP
```

```
Operating system version. 5.1
```

```
Code page . cp1252
```

```
Keyboard layout. N/A
```

```
Time zone. G.M.T
```

```
-----
-----
```

Output 5.3

```
***** Analysis report. 0
*****
```

```
String. Report generated from tagging
```

```
Generated on.2019-07-20T20.04.46.000000Z
```

```
Report text. Tagging plugin produced 9754 tags
```

```
-----
```

Exercise

Data set

Chapter 5 Emails.xlsx

Chapter 5 Carving.dee-dee

Software needed

Timeline Explorer - <https://ericzimmerman.github.io/#!index.md>

Microsoft .NET 6 or newer is required. You will get errors without at least .NET 6. When in doubt, install it! Make sure you get the Desktop runtime if you plan on running any of the gooey programs.

Autopsy - <https://www.autopsy.com/>

Email exercise

An individual outside of m57.biz purchased a laptop from Craigslist. The laptop the individual purchased contained child pornography and they decided to inform the police about it.

Investigators were able to trace the laptop back to m57.biz. When the police contacted the CEO of m57.biz, the CEO reported that the laptop, as well as other items, had been stolen from the m57 inventory.

The m57 CEO gave consent for the police investigators to search m57.biz and image all of the m57.biz computers, company phones, as well as U.S.B drives.

Analyze the emails found in the Chapter 5 emails.xlsx spreadsheet and identify potential suspects and a timeline of their activity.

Data carving exercise

- Load Autopsy and start a new case.
- Select Disk Image or VM file for the data source.
- Navigate to the folder where you stored the image Chapter 5 Carving.dee-dee. Select only the following Ingest Modules.
- PhotoRec Carver Embedded File Extractor
- From the drop-down menu, select All files, Directory, and Unallocated Space.

Analyze the results.

Chapter 6

Images

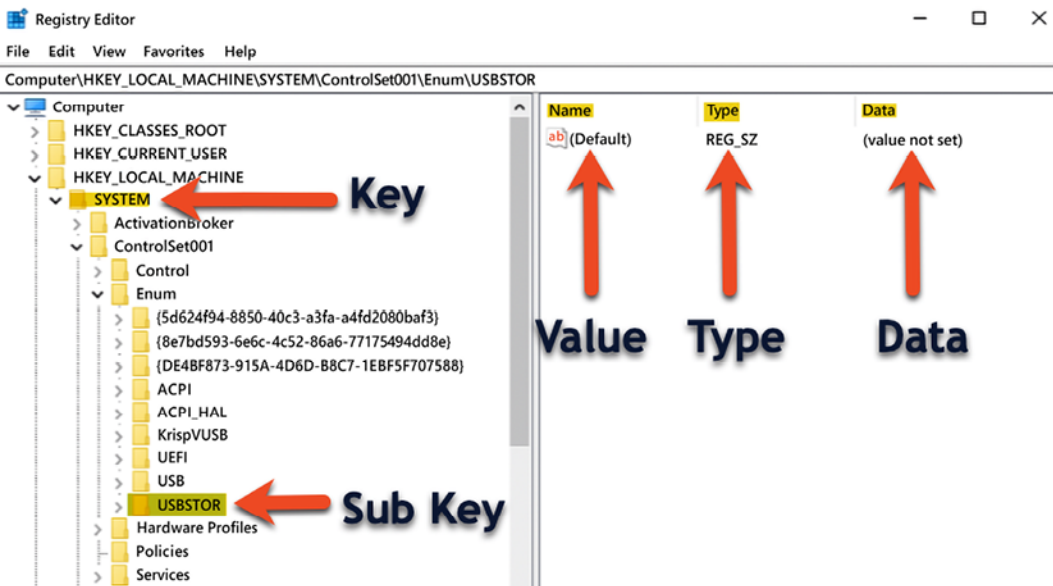


Figure 6.1: Registry Editor showing the USBSTOR registry key


```
Username      : jcloudy [1001]
SID           : S-1-5-21-2734969515-1644526556-1039763013-1001
Full Name     :
User Comment  :
Account Type  :
Account Created : Tue Mar 27 09:18:58 2018 Z
Name         :
Password Hint : It's me you idiot!
Last Login Date : Fri Apr 6 12:26:27 2018 Z
Pwd Reset Date : Tue Mar 27 09:18:58 2018 Z
Pwd Fail Date  : Fri Apr 6 03:30:52 2018 Z
Login Count   : 23
--> Password does not expire
--> Password not required
--> Normal user account
```

Figure 6.4: RegRipper output for the jcloudy account

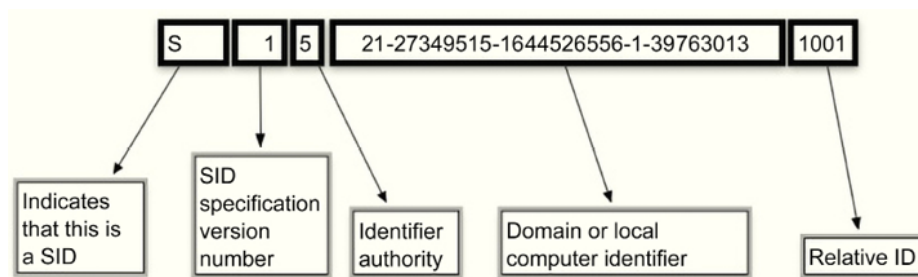


Figure 6.5: Breakdown of the SID

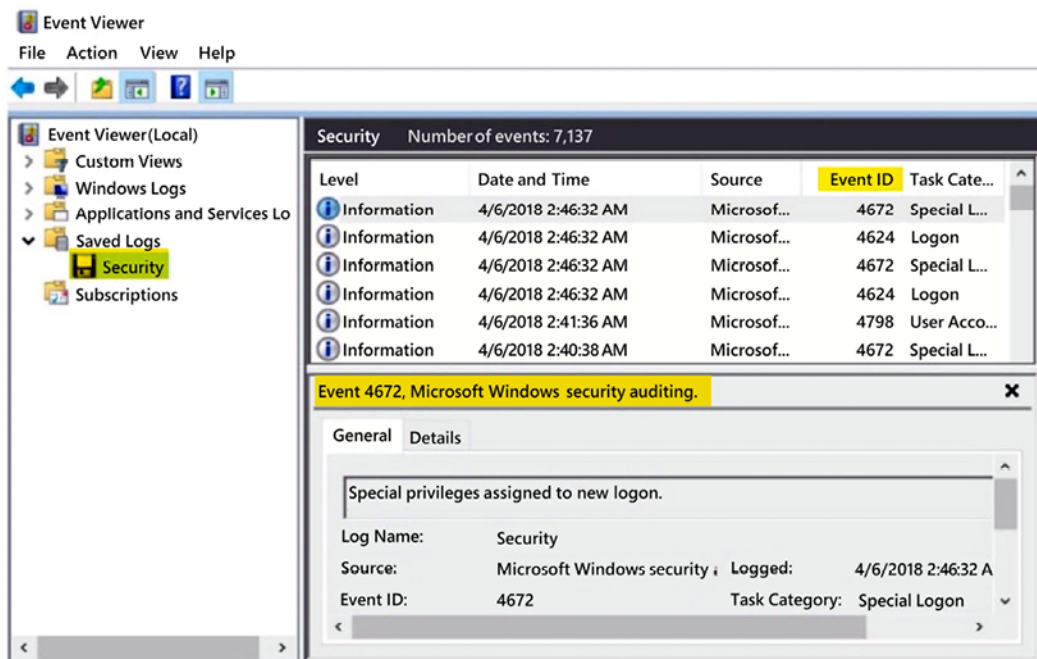


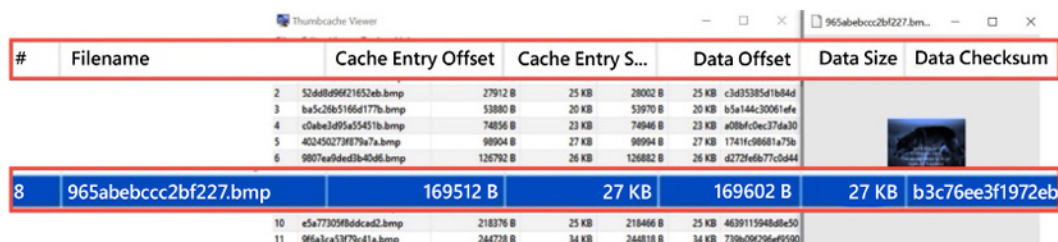
Figure 6.6: Event Viewer displaying event information

Subject:			
Security ID:	SYSTEM		
Account Name:	DESKTOP-PM6C56D\$		
Account Domain:	WORKGROUP		
Logon ID:	0x3E7		
Logon Information:			
Logon Type:	2		
Restricted Admin Mode:	-		
Virtual Account:	No		
Elevated Token:	No		
Impersonation Level:	Impersonation		
New Logon:			
Security ID:	S-1-5-21-2734969515-1644526556-1039763013-1001		
Account Name:	jcloudy		
Account Domain:	DESKTOP-PM6C56D		
Logon ID:	0x11F43947		
Linked Logon ID:	0x11F4390D		
Network Account Name:	-		
Log Name: Security			
Source:	Microsoft Windows security :	Logged:	4/6/2018 05:26
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-PM6C56D
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 6.7: Event Viewer showing the logon type

Logon Types	Description
Interactive	Logon to the local host by the user.
Network	A network logon to the local host by the user.
Batch	Allows processes to be started without user input.
Service	Automated process. No user input needed.
Unlock	The local host was unlocked via user input.
NetworkCleartext	Network logon to the local host by the user. The password was sent in cleartext to the authentication package. The password was then encrypted before it was sent on the network.
NewCredentials	The user account was duplicated and received new credentials for the network connection leaving the secure network.
RemoteInteractive	A logon to the local host by the user using a remote application.
CachedInteractive	A network logon to the local host by the user, using the network credentials on the local host.

Figure 6.8: Microsoft logon types



#	Filename	Cache Entry Offset	Cache Entry S...	Data Offset	Data Size	Data Checksum
2	52d68d96f21652eb.bmp	27912 B	25 KB	28002 B	25 KB	c3d35385d1b84d
3	ba5c26b5166d177b.bmp	53880 B	20 KB	53970 B	20 KB	b5e144c30061efe
4	c0abe3d95a55451b.bmp	74856 B	23 KB	74946 B	23 KB	a08bf0ec37da30
5	4024502778f79a7a.bmp	98904 B	27 KB	98994 B	27 KB	1741fc98681a75b
6	9807ea9ded1b40d6.bmp	126792 B	26 KB	126882 B	26 KB	d272f6f677c0d44
8	965abebccc2bf227.bmp	169512 B	27 KB	169602 B	27 KB	b3c76ee3f1972eb
10	e5a7705f8ddca2.bmp	218376 B	25 KB	218466 B	25 KB	4639115948d8e50
11	9f6a3ca53f79c41a.bmp	244728 B	34 KB	244818 B	34 KB	739b09c296ef9590

Figure 6.9: Thumbcache Viewer output

SystemIndex_PropertyStore [Table ID = 17, 575 Columns]		
Quick Filter		
27 f2 2b cc bc be 5a 96		
WorkID	27F-System_Search_Rank	4612F-System_Search_GatherTime
673	707406378	7F 8E 63 8C D7 C7 D3 01

Figure 6.10: Filtered database results

4421-System_ItemFolderPathDisplay:	C:\Users\jcloudy\Desktop
4234-System_Contact_HomeAddress1Locality:	
4222-System_Contact_EmailAddress2:	
4428-System_ItemPathDisplay:	C:\Users\jcloudy\Desktop\MyTiredHead.jpg
4236-System_Contact_HomeAddress1Region:	
4614-System_Search_LastIndexedTotalTime:	
4233-System_Contact_HomeAddress1Country:	
4235-System_Contact_HomeAddress1PostalCode:	
4155-System_Communication_AccountName:	
33-System_ItemUrl:	file:C:/Users/jcloudy/Desktop/MyTiredHead.jpg`

Figure 6.11: Filename display in the database

4105-System_Activity_AppldKind:	
4655-System_ThumbnailCacheld:	27 F2 2B CC BC BE 5A 96 00
4469-System_Media_EpisodeNumber:	

Figure 6.12: Thumbnail name in the database

Name		Type
Windows (351)		
WebCache (24)		
V01res00001.jrs		jrs
V01res00002.jrs		jrs
V01.chk		chk
V01.log		edblog
V0100016.log		edblog
V0100017.log		edblog
V0100018.log		edblog
V01tmp.log		edblog
WebCacheV01.dat (1)		edb
WebCacheV01.jfm		jfm
V01.log		log
V01tmp.log		log
WebCacheV01.dat		dat
WebCacheV01.dat		hxx
V01.chk		chk
V01.chk		chk

Figure 6.14: File Explorer showing the WebCacheV01.dat file

30.03.18 04:29:48	Visited: jcloudy@file:///C:/Users/jcloudy/Desktop/Larry%20King_%20Time%20to%20Repeal%20the%20Poorly%20Written%20Second%20Amendment.html
27.03.18 09:51:12	Visited: jcloudy@file:///C:/Users/jcloudy/OneDrive/Getting%20started%20with%20OneDrive.pdf
06.04.18 03:55:00	Visited: jcloudy@file:///C:/Users/jcloudy/Desktop/AMEN.pdf
03.04.18 06:11:21	Visited: jcloudy@file:///C:/Users/jcloudy/Desktop/The%20Cloudy%20Manifesto.docx
31.03.18 04:19:35	Visited: jcloudy@file:///C:/Users/jcloudy/Desktop/DemLogic.jpg
06.04.18 08:29:08	Visited: jcloudy@file:///C:/Users/jcloudy/Downloads/DemGun.jpg

Figure 6.15: X-Ways display of the contents of the WebCache

OpenSavePidlMRU*

LastWrite Time: Fri Apr 6 03:56:31 2018

Note: All value names are listed in MRUListEx order.

My Computer\CLSID_Desktop\LeftUsesBoycotts.pdf
 My Computer\CLSID_Desktop\AMEN.pdf
 My Computer\CLSID_Desktop\UKknifeBan.pdf
 My Computer\CLSID_Desktop\SelfDefenseisMurder.pdf
 My Computer\C:\Users\jcloudy\Desktop\Cloudy thoughts (4apr).docx
 My Computer\CLSID_Desktop
 My Computer\CLSID_Desktop\Operation 2nd Hand Smoke.pptx
 My Computer\CLSID_Desktop\The Cloudy Manifesto.docx
 My Computer\C:\Users\jcloudy\Desktop\The Cloudy Manifesto.docx
 My Computer\CLSID_Desktop\Huckleberry.png
 My Computer\CLSID_Desktop\DemLogic.jpg
 My Computer\CLSID_Desktop\RedGuns.jpg

Figure 6.16: Content of NTUSER.DAT key - OpenSavePidlMRU

```
recentdocs v.20100405 (NTUSER.DAT)

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

LastWrite Time Fri Apr 6 12:27:08 2018 (UTC)

37 = rootkey.csv
36 = Hardware and Sound
10 = DemGun.jpg
34 = LeftUsesBoycotts.pdf
33 = AMEN.pdf
12 = Planning.docx
32 = UKknifeBan.pdf
31 = SelfDefenseisMurder.pdf
30 = Cloudy thoughts (4apr).docx
```

Figure 6.17: Recent Docs entries

```
LastWrite Time Fri Apr 6 12:27:08 2018 (UTC)

MRUListEx = 0

0 = rootkey.csv
```

Figure 6.18: Content of NTUSER.DAT key - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs for CSV files

```
LastWrite Time Thu Apr 5 08:32:48 2018 (UTC)

MRUListEx = 0,3,1,2

0 = Planning.docx
3 = Cloudy thoughts (4apr).docx
1 = AIRPORT INFORMATION.docx
2 = The Cloudy Manifesto.docx
```

Figure 6.19: Content of NTUSER.DAT key - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\docx

```
LastWrite Time Fri Mar 30 04:32:26 2018 (UTC)
MRUListEx = 1,0
1 = Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'.html
0 = Larry King_ Time to Repeal the 'Poorly Written' Second Amendment.html
```

Figure 6.20: Content of NTUSER.DAT key - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\html

```

LastWrite Time Fri Apr 6 12:27:08 2018 (UTC)
MRUListEx = 4,5,1,3,2,0

4 = Downloads
5 = Hardware and Sound
1 = The Internet
3 = OneDrive
2 = System and Security
0 = CloudLog (D:)

```

Figure 6.21: Content of NTUSER.DAT key - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folders

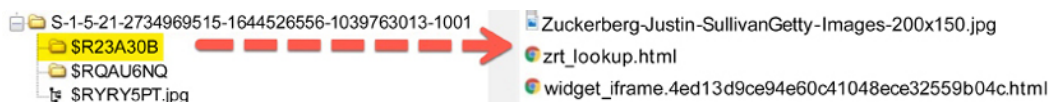


Figure 6.22: Deleted directory

Target attributes	A
Target file size	172684
Show Window	SW_NORMAL
Target created	03/30/2018 02:29:57 +0
Last written	04/04/2018 04:59:32 +0
Last accessed	04/04/2018 04:59:32 +0
ID List	Desktop\AIRPORT INFORMATION.docx
	C=03/30/2018 02:29:58
	M=04/04/2018 04:59:34
	Size=172684
Volume type	Fixed
Volume serial	0xAA920881
Local path	C:\Users\jcloudy\Desktop\AIRPORT INFORMATION.docx
Relative path	..\..\..\..\..\Desktop\AIRPORT INFORMATION.docx
Working directory	C:\Users\jcloudy\Desktop
Known Folder Tracking	false
Host name	desktop-pm6c56d
Volume ID	{BC7539BE-7B5B-4E04-9F8D-1C0D9B3AFF21}
Object ID	{30D25F11-3208-11E8-9B15-28E347017777}
MAC Address	28 E3 47 01 77 77
Timestamp	03/27/2018 21:45:39 +0, Seq: 6933
PROPERTYSTORAGE	{446D16B1-8DAD-4870-A748-402EA43D788C}
Size	29
propID	104

Figure 6.23: Link File contents

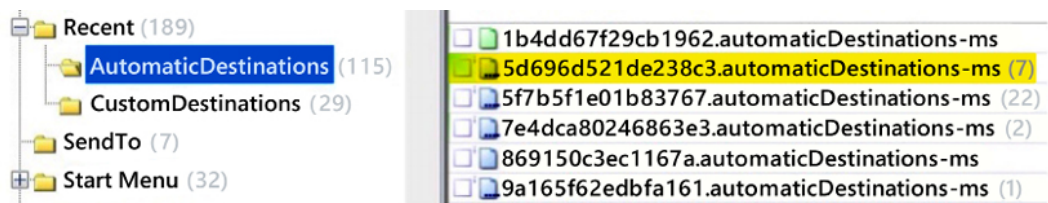


Figure 6.24: JumpList display

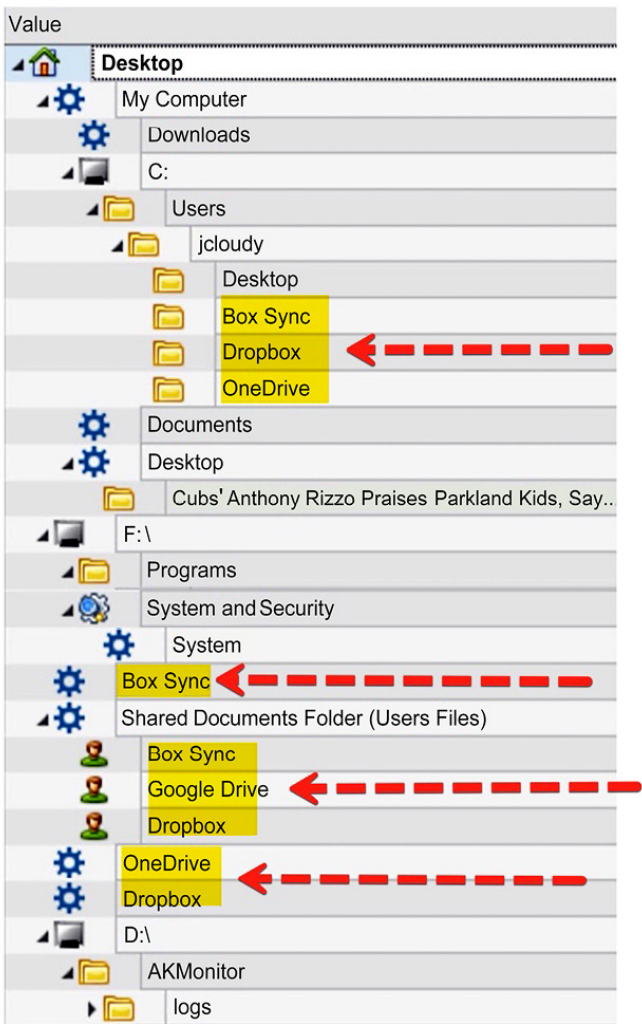


Figure 6.25: Shellbag Explorer: a graphical representation of shellbags


```

Name: Google Drive
Absolute path: Desktop\Shared Documents Folder (Users Files)\Google Drive
Key-Value name path: BagMRU\7-1
Registry last write time: 2018-04-05 02:05:13.581

Target timestamps
Created on: 2018-03-28 00:43:24.000
Modified on: 2018-03-28 00:43:24.000
Last accessed on: 2018-03-28 00:43:24.000

Miscellaneous
Shell type: Users Files Folder
Node slot: 14
MRU position: 1
# of child bags: 0

First interacted with: 2018-03-28 00:43:25.373

```

Figure 6.26: RegRipper output Google Drive

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run ...	Last Run Time
SETUP.EXE-45616327.d...	4/6/2018 05:26	4/6/2018 05:26	21,083	SETUP.EXE	(VOLUME{D1d3cscf78a333-a920881})\PROGRAM FILES\ANALISA CORPORATION\INSTALLED\INSTALLCORE\SETUP.EXE	1	4/6/2018 05:26
SVCHOST.EXE-7628D...	4/6/2018 05:46	4/6/2018 05:46	10,728	SVCHOST.EXE	(VOLUME{D1d3cscf78a333-a920881})\WINDOWS\SYSTEM32\SVCHOST.EXE	1	4/6/2018 05:46
SPEECHRUNTIME.EXE...	4/6/2018 05:46	4/6/2018 05:46	13,000	SPRINTLITE.MT...	(VOLUME{D1d3cscf78a333-a920881})\WINDOWS\SYSTEM32\SPRINTLITE.MT...	1	4/6/2018 05:46
FTK IMAGER.EXE-437E...	4/6/2018 05:41	4/6/2018 05:41	4,382	FTK IMAGER.EXE	(VOLUME{0000000000000000-407f6516})\PROGRAMS\IMAGER_LITE_3.1.1\FTK IMAGER.EXE	1	4/6/2018 05:41
FTK IMAGER.EXE-DED...	4/6/2018 05:40	4/6/2018 05:40	4,382	FTK IMAGER.EXE	(VOLUME{0000000000000000-407f6516})\PROGRAMS\IMAGER_LITE_3.1.1\FTK IMAGER.EXE	1	4/6/2018 05:40
RUNDLL32.EXE-87E3F...	4/6/2018 05:39	4/6/2018 05:39	4,382	RUNDLL32.EXE	(VOLUME{D1d3cscf78a333-a920881})\WINDOWS\SYSTEM32\RUNDLL32.EXE	1	4/6/2018 05:39
WMAPRVSX.EXE-OCBA...	4/6/2018 05:35	4/6/2018 05:35	4,771	WMAPRVSX.EXE	(VOLUME{D1d3cscf78a333-a920881})\WINDOWS\SYSTEM32\WMAPRVSX.EXE	1	4/6/2018 05:35
EXCEL.EXE-9231AABD...	4/6/2018 05:27	4/6/2018 05:27	47,159	EXCEL.EXE	(VOLUME{D1d3cscf78a333-a920881})\PROGRAM FILES (X86)\MICROSOFT OFFICE\ROOT\OFFICE\EXCEL.EXE	1	4/6/2018 05:27
RUNDLL32.EXE-25212...	4/6/2018 05:26	4/6/2018 05:26	8,705	RUNDLL32.EXE	(VOLUME{D1d3cscf78a333-a920881})\WINDOWS\SYSTEM32\RUNDLL32.EXE	1	4/6/2018 05:26
DLHOST.EXE-AEB615...	4/6/2018 01:31	4/6/2018 01:31	10,012	DLHOST.EXE	(VOLUME{D1d3cscf78a333-a920881})\WINDOWS\SYSTEM32\DLHOST.EXE	1	4/6/2018 01:31

Figure 6.27: Prefetch files displayed by WinPrefetchView

```

-----
timezone v.20160318
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time Tue Mar 27 09:56:27 2018 (UTC)
  DaylightName    -> @tzres.dll,-111
  StandardName    -> @tzres.dll,-112
  Bias            -> 300 (5 hours)
  ActiveTimeBias  -> 240 (4 hours)
  TimeZoneKeyName-> Eastern Standard Time
-----

```

Figure 6.28: RegRipper output - SYSTEM\CurrentControlSet\Control\TimeZoneInformation

```
<WLANProfile xmlns='http://www.microsoft.com/networking/WLAN/profile/v1'>
<name>Net 2.4</name><SSIDConfig><SSID><hex>4E657420322E34</hex>
<name>Net 2.4</name><MSM><security><authEncryption><authentication>
WPA2PSK</authentication><encryption>AES</encryption>
```

Figure 6.29: XML Output of WLAN Profile

```
Launching networklist v.20190128
(Software) Collects network info from Vista+ NetworkList key

Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles
Net 2.4
  DateLastConnected: Fri Mar 30 17:09:01 2018
  DateCreated       : Tue Mar 27 05:15:58 2018
  DefaultGatewayMac: 5C-8F-E0-2A-1C-68
  Type              : wireless
Nla\Wireless
Net 2.4
```

Figure 6.30: RegRipper output - SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList

```
3/27/2018 12:15:58 +0
Microsoft-Windows-WLAN-AutoConfig
EventID: 11000
Computer: SYSTEM

Adapter=Broadcom 802.11n Network Adapter DeviceGuid={4B0AE068-B350-4BD4-85AB-77E0E581863}
LocalMac=EC:0E:C4:20:7F:0E
SSID=Net 2.4
BSSType=Infrastructure
Auth=WPA2-Personal Cipher=AES-CCMP OnexEnabled=0
IhvConnectivitySetting= ConnectionId=0000000000000002
```

Figure 6.31: Event log for WIFI access

```

UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Tue Mar 27 09:19:59 2018 (UTC)

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Fri Apr 6 12:41:20 2018 Z
F:\Programs\Imager_Lite_3.1.1\FTK Imager.exe (1)
Fri Apr 6 12:27:04 2018 Z
{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Root\Office16\EXCEL.EXE (1)
Thu Apr 5 07:02:25 2018 Z
{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Root\Office16\WINWORD.EXE (1)
Thu Apr 5 06:06:42 2018 Z
{6D809377-6AF0-444B-8957-A3773F02200E}\S3 Browser\s3browser-win32.exe (4)
Thu Apr 5 02:32:31 2018 Z
Microsoft.Office.WINWORD.EXE.15 (2)
Thu Apr 5 02:05:01 2018 Z
{6D809377-6AF0-444B-8957-A3773F02200E}\Box\Box Sync\BoxSync.exe (2)

```

Figure 6.32: Contents of NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist

```

shimcache v.20190112
(System) Parse file refs from System hive AppCompatCache data

*** ControlSet001 ***
ControlSet001\Control\Session Manager\AppCompatCache
LastWrite Time: Tue Mar 27 21:45:28 2018 Z
|
C:\Windows\system32\MRT-KB890830.exe Tue Mar 27 09:38:12 2018 Z
C:\Windows\system32\attrib.exe Fri Sep 29 13:41:33 2017 Z
C:\Program Files\NVIDIA Corporation\DRS\DRSInstaller.exe Tue Mar 14 14:07:18 2017 Z
C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE Sat Mar 3 12:03:10 2018 Z
C:\Users\jcloudy\AppData\Local\Microsoft\OneDrive\Update\OneDriveSetup.exe Tue Mar 27 09:21:57 2018 Z
C:\Windows\system32\OpenWith.exe Fri Sep 29 13:42:00 2017 Z
C:\Windows\system32\SnippingTool.exe Fri Sep 29 14:43:00 2017 Z

```

Figure 6.33: Shimcache output

```

usbdevices v.20140416
(System) Parses Enum\USB key for USB & WPD devices

VID_0781&PID_5580
LastWrite: Tue Mar 27 09:22:21 2018
SN : AA010215170355310594
LastWrite: Tue Mar 27 12:13:16 2018

VID_0781&PID_5580
LastWrite: Tue Mar 27 09:22:21 2018
SN : AA010603160707470215
LastWrite: Tue Mar 27 21:45:44 2018

```

Figure 6.34: Content of Registry key - SYSTEM\CurrentControlSet\Enum\USB

```

usbstor v.20141111
(System) Get USBStor key info
USBStor
ControlSet001\Enum\USBStor

Disk&Ven_SanDisk&Prod_Extreme&Rev_0001 [Tue Mar 27 09:22:21 2018]
S/N: AA010215170355310594&0 [Tue Mar 27 12:11:44 2018]
Device Parameters LastWrite: [Tue Mar 27 12:11:42 2018]
Properties LastWrite : [Tue Mar 27 09:16:45 2018]
FriendlyName : SanDisk Extreme USB Device

S/N: AA010603160707470215&0 [Tue Mar 27 09:22:21 2018]
Device Parameters LastWrite: [Tue Mar 27 09:22:21 2018]
Properties LastWrite : [Tue Mar 27 09:23:58 2018]
FriendlyName : SanDisk Extreme USB Device

```

Figure 6.35: Content of Registry key - SYSTEM\CurrentControlSet\Enum\USBSTOR

```

mountdev v.20130530

(System) Return contents of System hive MountedDevices key

MountedDevices

LastWrite time = Tue Mar 27 09:22:21 2018Z
Device: _??_USBSTOR#Disk&Ven_SanDisk&Prod_Extreme&Rev_0001#AA010603160707470215&0#
{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\
DosDevices\D:\??\Volume{3869c27a-31b8-11e8-9b12-ecf4bb487fed}

Device: _??_USBSTOR#Disk&Ven_SanDisk&Prod_Extreme&Rev_0001#AA010215170355310594&0#
{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\
DosDevices\E:\??\Volume{5c3108bf-31c0-11e8-9b10-806e6f6e6963}

```

Figure 6.36: Content of Registry key - SYSTEM\MountedDevices

```

mp2 v.20120330
(NTUSER.DAT) Gets user's MountPoints2 key contents

MountPoints2
Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
LastWrite Time Fri Apr 6 12:35:08 2018 (UTC)

Remote Drives:

Volumes:
Fri Apr 6 12:35:08 2018 (UTC)
    {76d45981-0000-0000-0000-100000000000}
Tue Mar 27 21:45:54 2018 (UTC)
    {3869c27a-31b8-11e8-9b12-ecf4bb487fed}
Tue Mar 27 09:32:09 2018 (UTC)
    {09931f21-7faf-44a9-81d8-1e73c14b9eaf}
    {5c3108bb-31c0-11e8-9b10-806e6f6e6963}

```

Figure 6.37: Content of Registry key - Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

Links

- A full list of Microsoft Windows Event IDs can be found at: <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>
- RegRipper available for download from: <https://github.com/keydet89/RegRipper3.0>
- Eric Zimmerman's work is available for download from: <https://ericzimmerman.github.io/#!index.md>
- SANS catalog descriptions of the artifacts: <https://digital-forensics.sans.org/community/posters>
- Thumbcache Viewer: <https://thumbcacheviewer.github.io/>
- ESEDatabaseView: https://www.nirsoft.net/utils/ese_database_view.html
- JumpLists ID list: <https://community.malforensics.com/t/list-of-jump-list-ids/158>
- WinPrefetchViewtool: https://www.nirsoft.net/utils/win_prefetch_view.html
- Altheide, C., Carvey, H. A., and Davidson, R. (2011). Digital Forensics with Open

Source Tools. Amsterdam: Elsevier/Syngress: <https://www.amazon.com/Digital-Forensics-Open-Source-Tools/dp/1597495867>)

- Carvey, H. A. (2005). Windows forensics and incident recovery. Boston: Addison-Wesley: <https://www.amazon.com/Windows-Forensics-Incident-Recovery-Harlan/dp/0321200985>)
- Bunting, S. (2012). EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner; Study Guide. Indianapolis, IN: Wiley: <https://www.amazon.com/EnCase-Computer-Forensics-Official-EnCE/dp/0470901063>

Static URLs

This section contains static URLs such as path URLs and keys.

- Folders within Roaming folder:
 - \Users\%USER%\AppData\Roaming\Microsoft\Windows\Cookies
 - \Users\%USER%\AppData\Roaming\Microsoft\Windows\Network Shortcuts
 - \Users\%USER%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
 - \Users\%USER%\AppData\Roaming\Microsoft\Windows\Recent
 - \Users\%USER%\AppData\Roaming\Microsoft\Windows\SendTo
 - \Users\%USER%\AppData\Roaming\Microsoft\Windows\Start Menu
 - \Users\%USER%\AppData\Roaming\Microsoft\Windows\Templates
- Folders within Local folder:
 - \Users\%USER%\AppData\Local
 - \Users\%USER%\AppData\Local\Microsoft\Windows\History
 - \Users\%USER%\AppData\Local\Microsoft\Windows\Temporary Internet Files
- The following path will contain information about the user accounts on the system: C:\windows\system32\config\Sam\Domains\Account\Users
- In Windows Vista through Windows 10, we can find the event logs at the following path: C:\Windows\System32\winevt\logs

- The thumbcache can be found in the user's profile at the following path: AppData\Local\Microsoft\Windows\Explorer
- Windows Search Indexing database can be found at the following path: C.\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb
- JumpLists can be found at the following paths:
 - %UserProfile%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
 - %UserProfile%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations
- The following is the information contained in the file. You can see that the user was using Chrome to view PDF files and offline HTML files. It also contains the date/time the user opened the files.
 - 7 04/06/2018 03.56.32 +0 C.\Users\jcloudy\Desktop\LeftUsesBoycotts.pdf
 - 6 04/06/2018 03.55.00 +0 C.\Users\jcloudy\Desktop\AMEN.pdf
 - 5 04/05/2018 05.51.41 +0 C.\Users\jcloudy\Desktop\UKknifeBan.pdf
 - 4 04/05/2018 05.48.40 +0 C.\Users\jcloudy\Desktop\SelfDefenseisMurder.pdf
 - 3 03/30/2018 04.32.25 +0 C.\Users\jcloudy\Desktop\Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'.html
 - 2 03/30/2018 04.29.48 +0 C.\Users\jcloudy\Desktop\Larry King_ Time to Repeal the 'Poorly Written' Second Amendment.html
 - 1 03/27/2018 09.51.18 +0 C.\Users\jcloudy\OneDrive\Getting started with OneDrive.pdf desktop-pm6c56d
- Another key to view most recently used files: NT-user.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
- This is an example of the file extension subkeys I described earlier, and it shows the recently used C.S.V files: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.csv

- This is an example of the file extension subkeys I described earlier, and it shows the recently used DOCX files: `Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx`
- This is an example of the file extension subkeys I described earlier, and it shows the recently used HTML files: `Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.html`
- There is also an additional subkey, `\Folder`, that lists when the user opened folders on the system, which is shown as follows: `Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder`

Exercise

Data set

Chapter 6 Owl Exercise.e01

Software needed

Autopsy - <https://www.autopsy.com/>

Scenario

In a jurisdiction where owls are illegal to trade and buy, two users are discussing the illegal trade of owls. A computer is taken into evidence belonging to a user who is attempting to purchase owls illegally. It has been requested that you conduct an analysis of the digital evidence. A forensic image has been obtained and is ready for you. You may use Autopsy or any other tool.

Some artifacts you may want to look for include.

- Web searches
- Shopping searches
- Chat clients
- Email
- Documents
- Social networks
- Oh-ess artifacts
- ell-enn-kay files

- Recycle Bin
- Shellbag

Potential keywords.

- Owl
- Owlet
- Feathers
- Eggs
- Crossbreeding
- Nocturnal
- Nest
- Hoot
- Conservation
- Wingspan

Chapter 7

Images

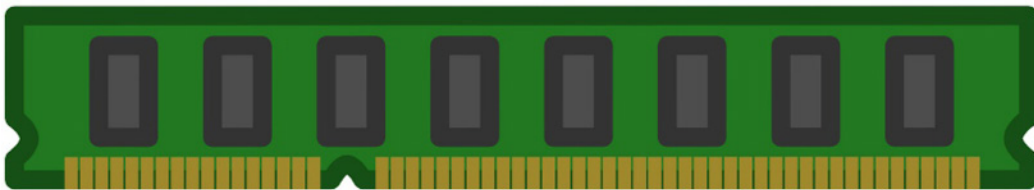


Figure 7.1: DRAM image

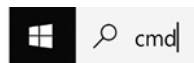


Figure 7.2: Search bar

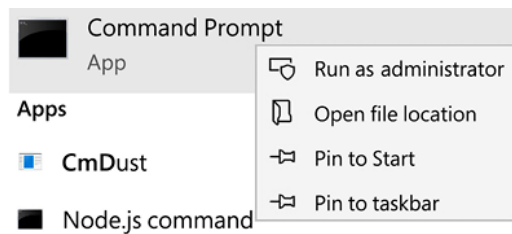


Figure 7.3: Run as administrator

```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msliche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      35945185280 bytes ( 34280 Mb)
Free space size:         369265610752 bytes ( 352159 Mb)

* Destination = \\?\C:\tools\MSI-20220214-221822.raw

--> Are you sure you want to continue? [y/n]
```

Figure 7.4: DumpIt screen

```
* Destination = \\?\C:\tools\MSI-20220214-221822.raw

--> Are you sure you want to continue? [y/n] y
+ Processing... Success.
```

Figure 7.5: DumpIt successful

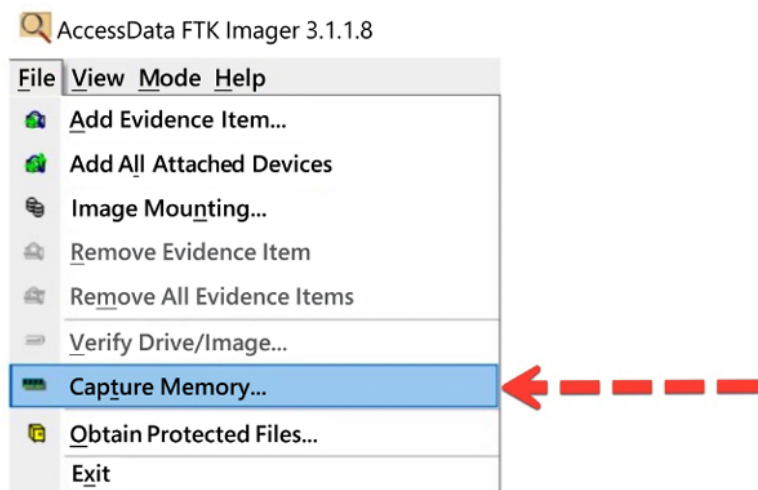


Figure 7.6: FTK Imager menu

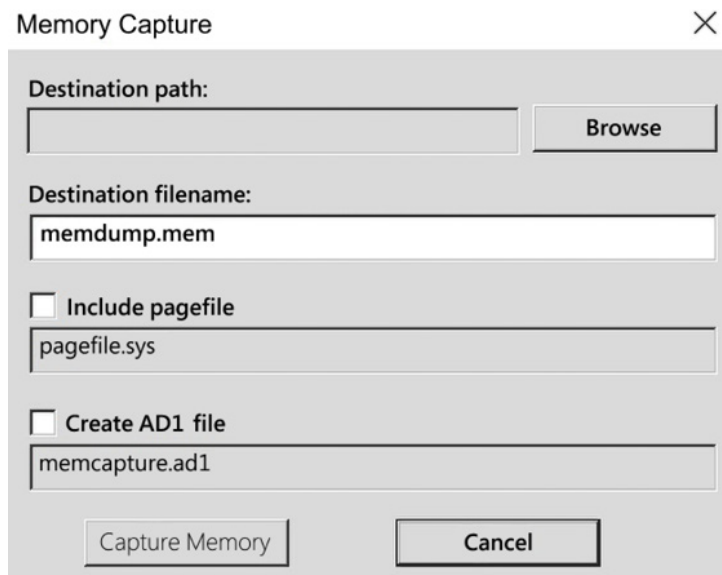


Figure 7.7: FTK Imager memory capture

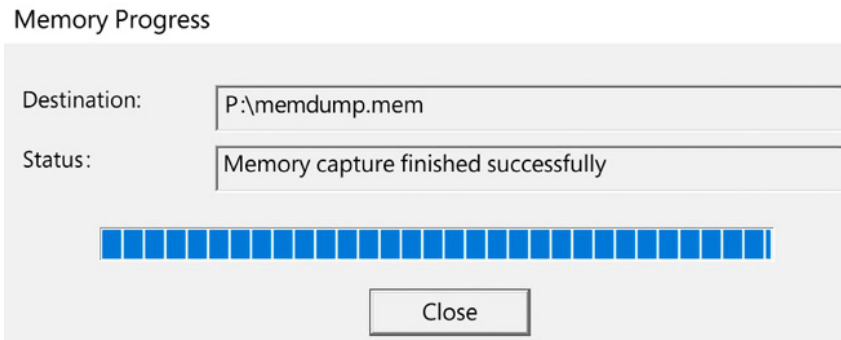


Figure 7.8: FTK Image successful

alerts.txt	Processing errors recorded in a text file.
ccn.txt	Processes credit card numbers recorded in a text file.
ccn_track2.txt	Processes credit card "track 2" information, which has been found in some bank card fraud cases recorded in a text file.
domain.txt	Processes Internet domains found on the drive, including dotted-quad addresses found in the text recorded in a text file.
email.txt	Processes email addresses recorded in a text file.
ether.txt	Processes Ethernet MAC addresses found through IP packet carving of swap files and compressed system hibernation files and file fragments recorded in a text file.
exif.txt	Processes EXIFs from JPEGs and video segments. This feature file contains all the EXIF fields, expanded as XML records recorded in a text file.
find.txt	Processes the results of specific regular expression search requests recorded in a text file.
identified_blocks.txt	Processes block hash values that match hash values in a hash database that the scan was run against recorded in a text file.
ip.txt	Processes IP addresses found through IP packet carving recorded in a text file.
rfc822.txt	Processes email message headers including the Date, Subject, and Message-ID: fields recorded in a text file.
tcp.txt	Processes TCP flow information found through IP packet carving recorded in a text file.
telephone.txt	Processes US and international telephone numbers recorded in a text file.
url.txt	Processes URLs, typically found in browser caches, email messages, and pre-compiled into executables recorded in a text file.
url_searches.txt	Processes a histogram of terms used in internet searches from services such as Google, Bing, Yahoo, and others recorded in a text file.
url_services.txt	Processes a histogram of the domain name portion of all the URLs found on the media recorded in a text file.
wordlist.txt	Processes a list of all "words" extracted from the disk, useful for password cracking recorded in a text file.
wordlist_*.text	Processes the wordlist with duplicates, removed, formatted in a form that can be easily imported into a popular password-cracking program recorded in a text file.
zip.txt	Processes information regarding every ZIP file component found on the media. This is exceptionally useful as ZIP files include internal structure and ZIP is increasingly the compound file format of choice for a variety of products such as Microsoft Office recorded in a text file.

Figure 7.9: Bulk Extractor output options

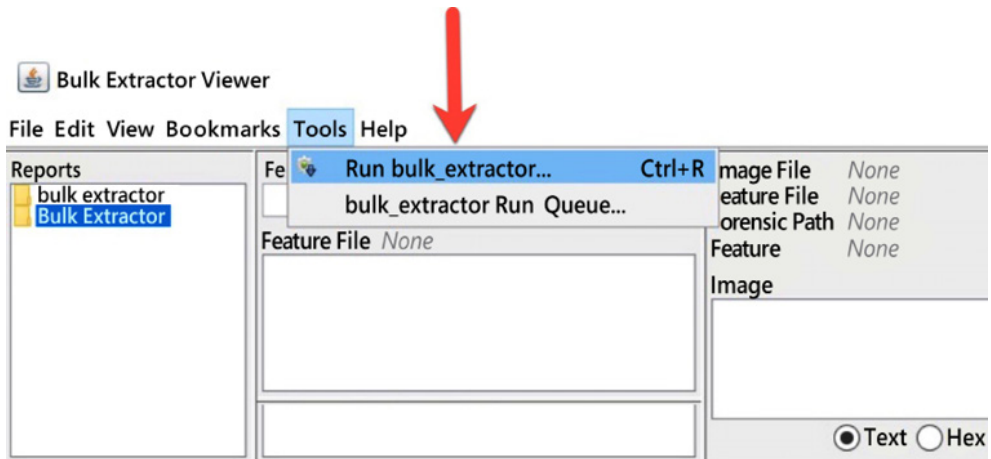



Figure 7.10: Bulk Extractor menu – the run bulk extractor option

 Run bulk_extractor ✕

Required Parameters

Scan: ☒ Image File ☐ Raw Device ☐ Directory of Files

Image file: ...

Output Feature Directory: ...

General Options

☐ Use Banner File ...

☐ Use Alert List File ...

☐ Use Stop List File ...

☐ Use Find Regex Text File ...

☐ Use Find Regex Text

☐ Use Random Sampling

Tuning Parameters

☐ Use Context Window Size

☐ Use Page Size

☐ Use Margin Size

☐ Use Block Size

☐ Use Number of Threads

☐ Use Maximum Recursion Depth

☐ Use Wait Time

Parallelizing

☐ Use start processing at offset

☐ Use process range offset o1-o2

☐ Use add offset to reported feature offsets

Debugging Options

☐ Start on Page Number

☐ Use Debug Mode Number

☐ Erase Output Directory

Scanner Controls

☐ Use Plugin Directories ...


☐ Use Settable Options

Scanners

- ☒ base16
- ☒ facebook
- ☒ hashdb
- ☒ outlook
- ☒ sceanan
- ☒ wordlist
- ☒ xor
- ☒ accts
- ☒ aes
- ☒ base64
- ☒ elf
- ☒ email
- ☒ exif
- ☒ find
- ☒ gps
- ☒ gzip
- ☒ hiberfile
- ☒ httplogs
- ☒ json
- ☒ kml
- ☒ msxml
- ☒ net
- ☒ pdf
- ☒ rar
- ☒ sqlite
- ☒ vcard
- ☒ windirs
- ☒ winlnk
- ☒ winpe
- ☒ winprefetch
- ☒ zip

Manage Queue...
Import...
Submit Run
Cancel

Figure 7.11: Bulk Extractor menu options to run

 Run bulk_extractor ✕

Required Parameters

Scan: ☒ Image File ☐ Raw Device ☐ Directory of Files

Image file: ...

Output Feature Directory: ...

General Options

☐ Use Banner File ...

☐ Use Alert List File ...

☐ Use Stop List File ...

☐ Use Find Regex Text File ...

☐ Use Find Regex Text

☐ Use Random Sampling

Tuning Parameters

☐ Use Context Window Size

☐ Use Page Size

☐ Use Margin Size

☐ Use Block Size

☐ Use Number of Threads

☐ Use Maximum Recursion Depth

☐ Use Wait Time

Parallelizing

☐ Use start processing at offset

☐ Use process range offset o1-o2

☐ Use add offset to reported feature offsets

Debugging Options

☐ Start on Page Number

☐ Use Debug Mode Number

☐ Erase Output Directory

Scanner Controls

☐ Use Plugin Directories ...

☐ Use Settable Options

Scanners

- ☒ base16
- ☒ facebook
- ☒ hashdb
- ☒ outlook
- ☒ sceadan
- ☒ wordlist
- ☒ xor
- ☒ accts
- ☒ aes
- ☒ base64
- ☒ elf
- ☒ email
- ☒ exif
- ☒ find
- ☒ gps
- ☒ gzip
- ☒ hiberfile
- ☒ httplogs
- ☒ json
- ☒ kml
- ☒ msxml
- ☒ net
- ☒ pdf
- ☒ rar
- ☒ sqlite
- ☒ vcard
- ☒ windirs
- ☒ winlnk
- ☒ winpe
- ☒ winprefetch
- ☒ zip

Manage Queue...
Import...
Submit Run
Cancel

Figure 7.11: Bulk Extractor menu options to run

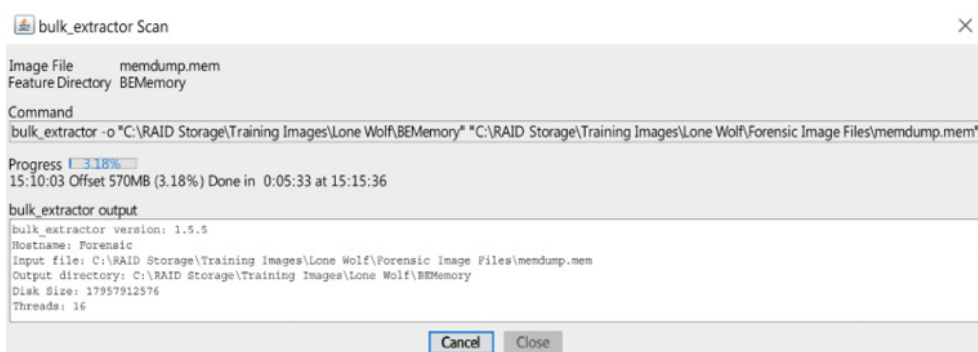


Figure 7.12: Bulk Extraction window

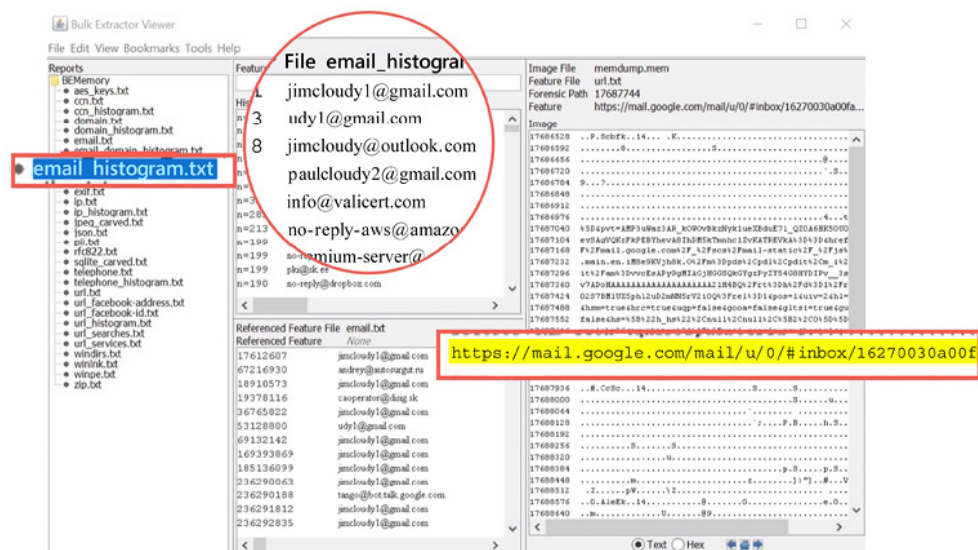


Figure 7.13: Bulk Extractor Viewer – extracted content

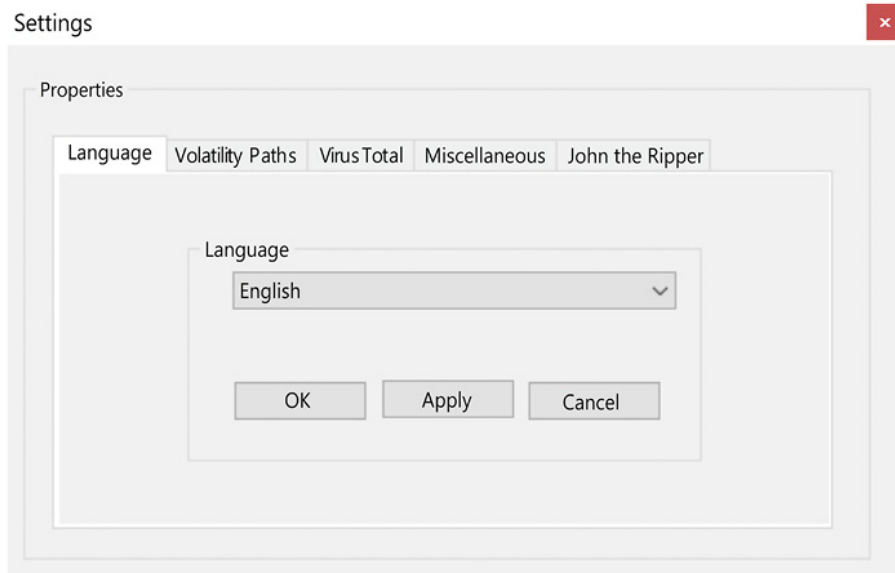


Figure 7.14: Volix settings

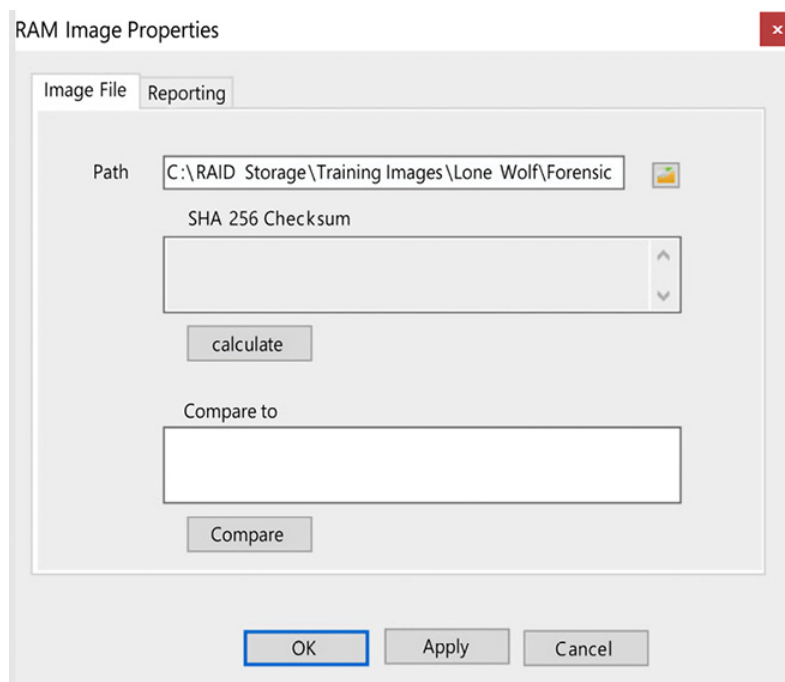


Figure 7.15: Volix RAM location

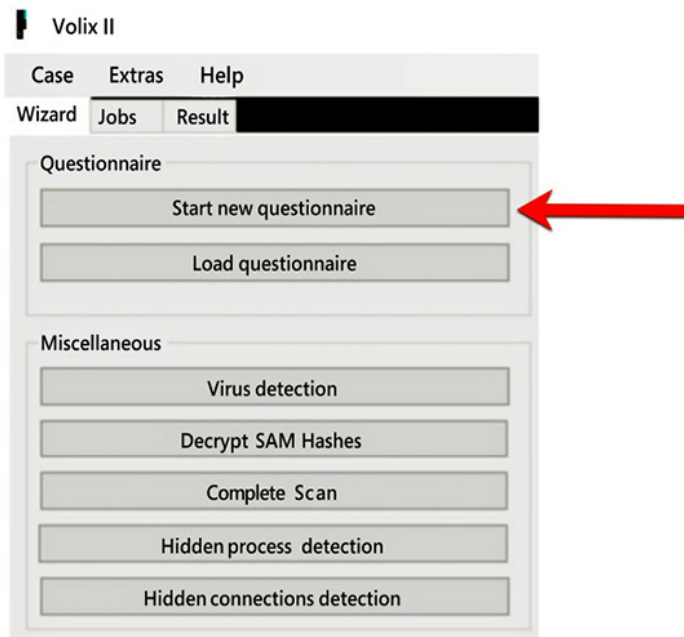


Figure 7.16: VOLIX wizard

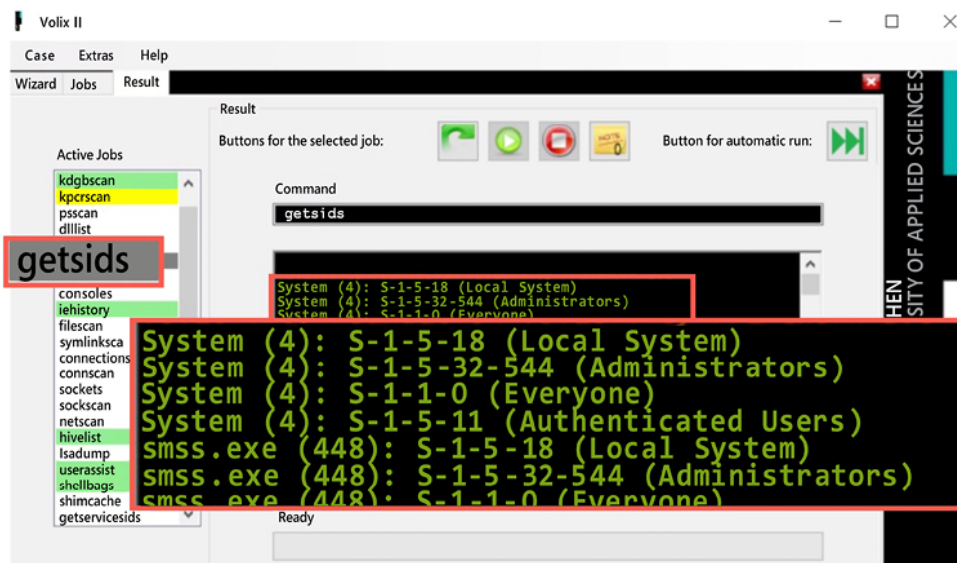


Figure 7.17: Volix scan results

Links

- Converting dump files: <https://www.comae.com>
- DumpIt: <https://github.com/thimbleweed/All-In-USB/tree/master/utilities/DumpIt>
- Bulk Extractor: http://digitalcorpora.org/downloads/bulk_extractor
- Volatility: <https://www.volatilityfoundation.org>
- VOLIX II v2: <https://www.fh-aachen.de/en/people/schuba/forschung/it-forensik/projekte/volix-en>
- Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linu. John Wiley & Sons: <https://www.amazon.com/Art-Memory-Forensics-Detecting-Malware/dp/1118825098>

Static URLs

This section contains static URLs such as path URLs and keys.

- Crash dump enable: `SYSTEM\CurrentControlSet\Control\CrashControl\CrashDumpEnable`

Chapter 8

Images

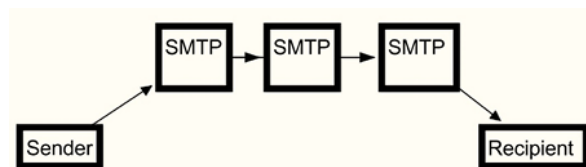


Figure 8.1: Diagram of an email sent by SMTP

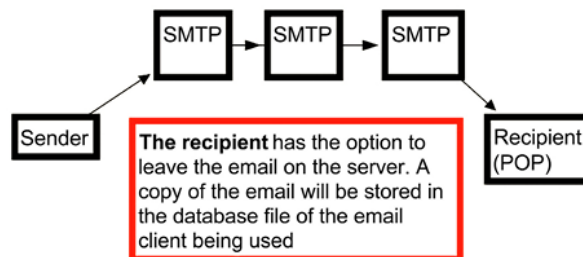


Figure 8.2. SMTP-POP map

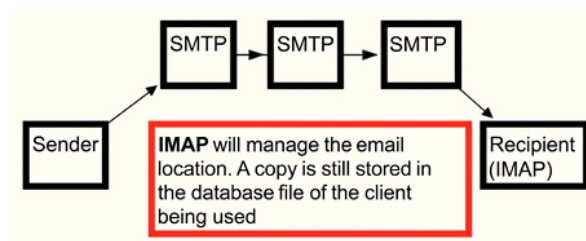


Figure 8.3: IMAP map

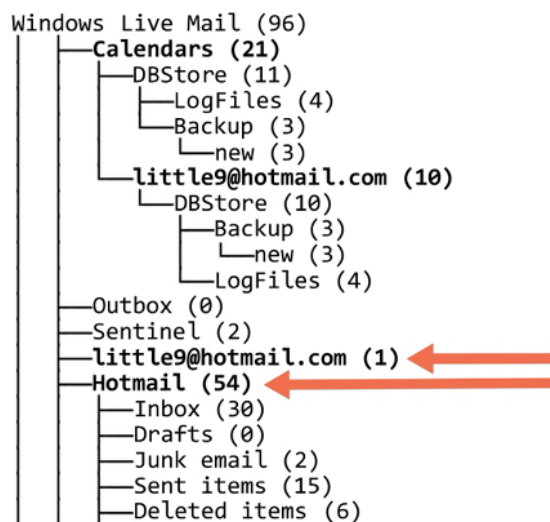


Figure 8.4: Windows Live Mail folder

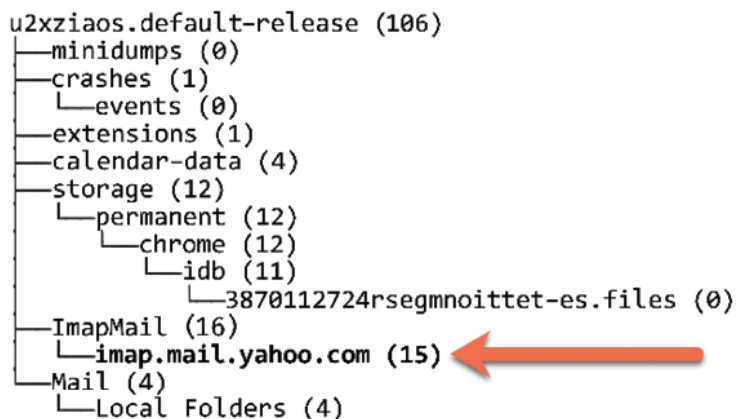


Figure 8.5: Thunderbird folder structure

Name ▲	Type
imap.mail.yahoo.com (15)	
INBOX (3)	mbox
Banks.eml	eml
New sign in on thunderbird.eml	eml
Re: midgets.eml	eml

Figure 8.6: Thunderbird inbox

08/28/2019 Inbox (2) -
 19 22:19:39 badguynneedslove@gmail.com - https://mail.google.com/mail/?pc=topnav-about-n-en
 +0 Gmail

Figure 8.7. Email, History

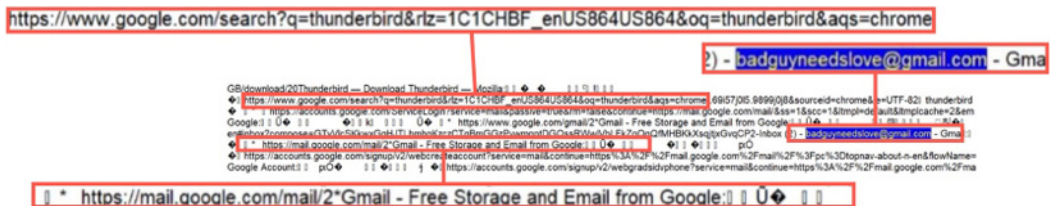


Figure 8.8. Chrome cache displayed

```

Mozilla (1,505)
├── Firefox (1,505)
│   └── Profiles (1,504)
│       ├── 55abhq00.default-release (1,504)
│       │   ├── safebrowsing (50)
│       │   │   ├── google4 (10)
│       │   │   ├── jumplistCache (5)
│       │   │   ├── startupCache (236)
│       │   │   ├── cache2 (1,162)
│       │   │   │   ├── entries (1,160)
│       │   │   │   └── doomed (0)
│       │   │   ├── thumbnails (0)
│       │   │   ├── OfflineCache (1)
│       │   │   ├── safebrowsing-updating (49)
│       │   │   │   └── google4 (9)
│       │   └── cqr6ioib.default (0)
  
```

Figure 8.9: Firefox folder structure

```

"matches": [
  {
    "lookupId": "badguynneedslove@gmail.com",
    "personId": [
      "114987255021342983529"
    ]
  }
],
"people": {
  "114987255021342983529": {
    "personId": "114987255021342983529",
    "metadata": {
      "lastUpdateTimeMicros": "1567030765000",
      "identityInfo": {
        "originalLookupToken": [
          "badguynneedslove@gmail.com"
        ],
        "sourceIds": [
          {
            "container": "PROFILE",
            "id": "114987255021342983529",
            "sourceEtag": "#3koZ3UbbbsLY=",
            "containerType": "PROFILE"
          }
        ]
      }
    }
  }
}

```



Figure 8.10: Firefox Cache

Emails and messages

Content of the email:

Jean,
One of the potential investors that I've been dealing with has asked me to get a background check of our current employees. Apparently they recently had some problems at some other company they funded.
Could you please put together for me a spreadsheet specifying each of our employees, their current salary, and their S.S.N? Please do not mention this to anybody.
Thanks.
(P.S. because of the sensitive nature of this, please do not include the text of this email in your message to me. Thanks.)

The following is the email header for the email Jean received from Alison:

-----HEADERS-----

Return-Path: simsong@xy.dreamhostps.com

X-Original-To: jean@m57.biz

Delivered-To: x2789967@spunkymail-mx8.g.dreamhost.com

Received: from smarty.dreamhost.com (sd-green-bigip-81.dreamhost.com [208.97.132.81]) by spunkymail-mx8.g.dreamhost.com (Postfix) with ESMTP id E32634D80F for <jean@m57.biz>; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)

Received: from xy.dreamhostps.com (apache2-xy.xy.dreamhostps.com [208.97.188.9]) by smarty.dreamhost.com (Postfix) with ESMTP id 6E408EE23D for <jean@m57.biz>; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)

Received: by xy.dreamhostps.com (Postfix, from userid 558838) id 64C683B1DAE; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)

To: jean@m57.biz From: alison@m57.biz

subject: background checks

Message-Id: 20080719233957.64C683B1DAE@xy.dreamhostps.com

Date: Sat, 19 Jul 2008 16:39:57 -0700 (PDT)

The Message field

Message-Id: <20080719233957.64C683B1DAE@xy.dreamhostps.com>

The first server the email touched:

Received: by xy.dreamhostps.com (Postfix, from userid 558838) id 64C683B1DAE; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)

The received lines from subsequent servers:

Received: from smarty.dreamhost.com (sd-green-bigip-81.

```
dreamhost.com [208.97.132.81])
```

```
by spunkymail-mx8.g.dreamhost.com (Postfix) with ESMTP id  
E32634D80F for <jean@m57.biz>;
```

```
Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
```

```
Received: from xy.dreamhostps.com (apache2-xy.xy.dreamhostps.  
com [208.97.188.9])
```

```
by smarty.dreamhost.com (Postfix) with ESMTP id 6E408EE23D for  
<jean@m57.biz>;
```

```
Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
```

The return path field:

```
Return-Path: <simsong@xy.dreamhostps.com>
```

Optional fields:

```
X-Priority: 3
```

```
X-Mailer: PHPMailer 5.2.9 (https://github.com/PHPMailer/  
PHPMailer/)
```

```
Message-Id: ff176aaf06e2f6958ada6e2d3c43b095@x3.netcomlearning.  
com
```

```
X-Report-Abuse: Please forward a copy of this message,  
including all headers, to abuse@mandrill.com
```

```
X-Report-Abuse: You can also report abuse  
here: http://mandrillapp.com/contact/  
abuse?id=30514476.1925a088d66f450cb25a4034f3ec6942 X-Mandrill-  
User: md_30514476
```

MIME version email attachment:

```
MIME-Version. 1.0
```

```
Content-Type. text/html; charset=us-ascii
```

```
Content-Transfer-Encoding. 7bit
```

Artifacts

```
{ "endpoint_info_list" : [ { "endpoint" : "smtp.badguy27@yahoo.com",  
  "c_eye-dee" : "d24c.2d00",  
  "c_name" : "Joe Badguy Smith" },  
  { "endpoint" : "smtp.bad-guy-needs-love@gmail.com",  
    "c_eye-dee" : "e80f.5b71", "c_name" : "John Badguy Smith" },  
  { "endpoint" : "smtp.yahoo@mail.comms.yahoo.net",  
    "c_eye-dee" : "624f.10f0", "c_name" : "Yahoo! Inc." } ] }
```

Links

Jones, R. (2006). Internet forensics: Beijing: Oreilly: <http://shop.oreilly.com/product/9780596100063.do>

Exercise

Data set

Jean outlook.pst

Software needed

Autopsy - <https://www.autopsy.com/>

Scenario

A company, XYZ L.L.C, finds that a spreadsheet containing confidential information was Posted as an attachment in the “technical support” forum of a competitor’s website.

The spreadsheet came from the CFO of XYZ L.L.C, Jean’s computer.

Interviews

You are tasked with investigating the leak of confidential information. To that end, you conduct interviews with the President and Chief Financial Officer of XYZ L.L.C, Alison and Jean respectively. Here are excerpts from their interviews.

Alison (President).

- I don't know what Jean is talking about.
- I never asked Jean for the spreadsheet.
- I never received the spreadsheet by email.

Jean (CFO).

- Alison asked me to prepare the spreadsheet as part of a new funding round.
- Alison asked me to send the spreadsheet to her by email.
- That's all I know.

Email accounts

Alison (President).

`alison@m57.biz`

Jean (CFO).

`jean@m57.biz`

Question to answer

Examining Jean's email, How did the documents get on the competitor's website? Use Autopsy (or your tool of choice) to analyze the emails contained in the `.pst` file.

Chapter 9

Images

```
"date_added": "13105251021405925",
"id": "110",
"meta_info": {
  "last_visited_desktop": "13197567715245509"
},
"name": "BBC News",
"sync_transaction_version": "592"
"type": "url",
"url": "http://news.bbc.co.uk/"
, {
  "date_added": "13105251021408611",
  "id": "111",
  "meta_info": {
    "last_visited_desktop": "13197950930217586"
  },
  "name": "CNN",
  "sync_transaction_version": "592",
  "type": "url",
  "url": "http://www.cnn.com/"
```

Figure 9.1: JSON BBC bookmark

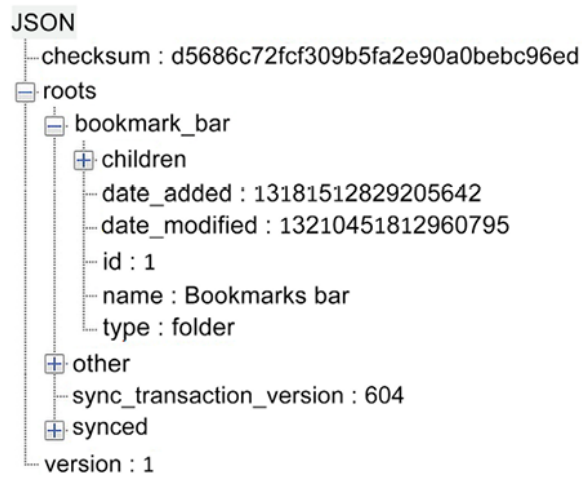


Figure 9.2: JSON root folder

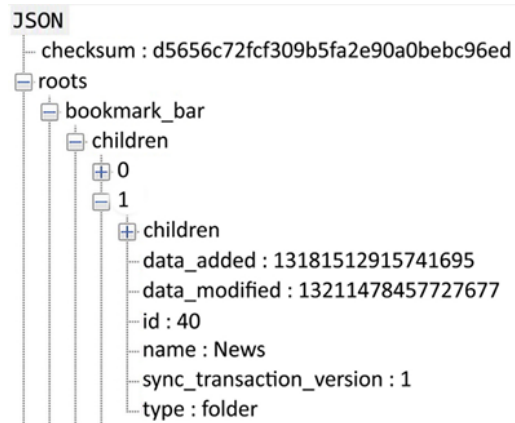


Figure 9.3: JSON children



Figure 9.4: JSON bookmarks

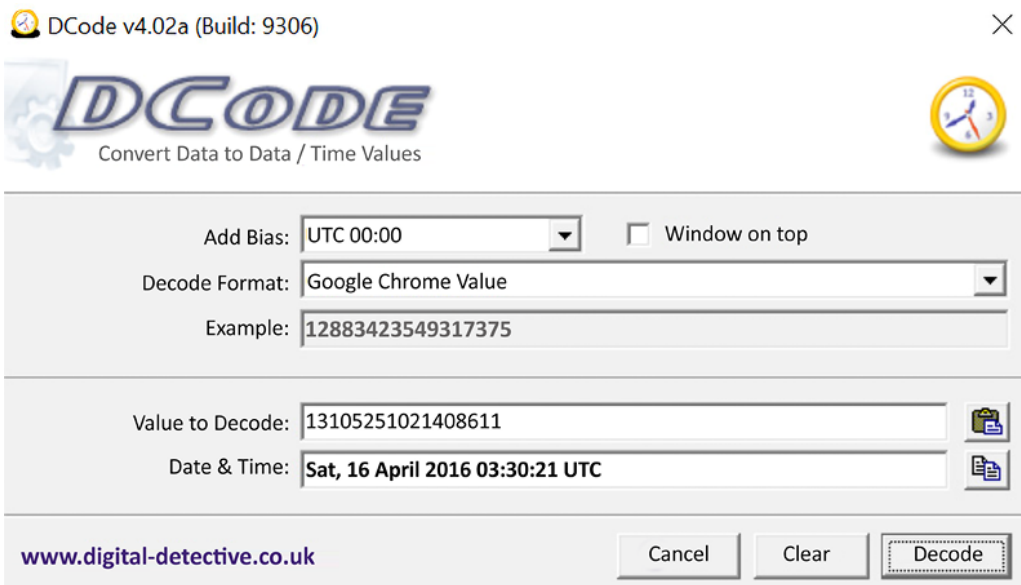


Figure 9.5: DCode tool used for translating the Google Chrome Value

C:\Users\IEUser\Downloads\Thunderbird Setup 68.0.exe
https://www.thunderbird.net/en-GB/download/
08/29/2019 16:14:38 +0
08/29/2019 16:14:40 +0

Figure 9.6: User's Chrome History

gmail
https://www.google.com/search? q=**gmail**& (REDACTED)
08/28/2019 22:17:04 +0
thunderbird
https://www.google.com/search?q=**thunderbird**& (REDACTED)
08/29/2019 16:14:29 +0

Figure 9.7: User's Search History

08/28/2019 22:22:08 +0
(2 unread) - **badguy27@yahoo.com** - Yahoo Mail
https://mail.yahoo.com/d/REDACTED)
08/28/2019 22:22:36 +0
Banks - **badguyneedslove@gmail.com** - Gmail
https://mail.google.com/mail/ (REDACTED)
08/29/2019 16:14:29 +0
thunderbird - Google Search
https://www.google.com/search?q=thunderbird&REDACTED)
08/29/2019 16:14:33 +0
Thunderbird - Download Thunderbird - Mozilla
https://www.thunderbird.net/en-GB/download/ 1

Figure 9.8: User's Internet History

creation_utc	host_key	name	value	path	expires_utc	is_secure	is_httponly	last_access_utc	has_expires	is_pe
13211504229653934	.google.com	_ga		/gmail/about	13274576231000000	0	0	13211504229653934	1	1
13211504229654926	.google.com	_gid		/gmail/about	13211590631000000	0	0	13211504229654926	1	1
13211504361869670	.google.com	APISID		/	13274576361869670	0	0	13211568843104513	1	1
13211504373193089	mail.google.com	COMPASS		/mail/u/0			13212368374193089	1	1	13211504554421139

Figure 9.9: Cookies

Host Name	Path	Name	Value	Secure	HTTP Only	Last Access...	Created On	Expires
.google.com	/gmail/about	_ga		No	No	8/28/2019 22:17	8/28/2019 22:17	8/27/2019 22:17
mail-ads.google.com	/mail/u/0	COMPASS		Yes	Yes	8/28/2019 22:19	8/28/2019 22:19	9/7/2019 22:19
www.yahoo.com	/	flash_enabled		No	No	8/28/2019 22:21	8/28/2019 22:21	9/27/2019 22:21

Figure 9.10: Cookie View

gmail.html	https://www.google...text.html	0	8/28/2019 15:17	8/28/2019 15:17		stfc	HTTP/1.1 302		private	172.217.14.100	
s2	https://www.google...text/javascript	14,665	8/28/2019 15:17	8/27/2019 14:17	8/27/2019 14:27	8/26/2020 14:47	stfc	HTTP/1.1 200 br	data_3 [253952]	public, max-age=31536000	172.217.14.100
about.html	https://mail.google...	0	8/28/2019 15:17	8/27/2019 21:40		8/28/2019 21:40	stfc	HTTP/1.1 301		public, max-age=86400	172.217.11.105
about.html	https://www.google...text.html	0	8/28/2019 15:17	8/28/2019 04:21		8/29/2019 04:21	stfc	HTTP/1.1 301		public, max-age=86400	172.217.14.100
about.html	https://www.google...text.html	15,504	8/28/2019 15:17	8/28/2019 15:17	7/19/2019 00:30	8/28/2019 15:17	stfc	HTTP/1.1 200 gdp	data_3 [303104]	private, max-age=3000	172.217.14.100

Figure 9.11: Cache view

Miniature Schnauzer Dog Breed Information.url	url	2.5 KB	09/02/2019	18:01:11	+0	09/02/2019	18:01:13	+0
schnauzers - Bing images.url	url	1.1 KB	09/02/2019	18:01:30	+0	09/02/2019	18:01:30	+0
Salt and Pepper Miniature Schnauzer - Bing images.url	url	1.3 KB	09/02/2019	18:01:47	+0	09/02/2019	18:01:47	+0
Christen's Miniature Schnauzers - Las Vegas, NV.url	url	180 B	09/02/2019	18:02:11	+0	09/02/2019	18:02:11	+0

Figure 9.12: IE bookmarks

```
[DEFAULT]
BASEURL=http://christensminischnauzers.com/
{000214A0-0000-0000-C000-000000000046}
Prop3=19,2
[InternetShortcut]
URL=http://christensminischnauzers.com/IDList=
```

Figure 9.13

ContainerId	LastAccessTime	Name	Directory
1	132119207925900830	Content	C:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
2	132115040805283385	feedplat	C:\Users\IEUser\AppData\Local\Microsoft\Feeds\Cache\
3	131594261121527040	ietld	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\IETIdCache\
4	132119207924265464	History	C:\Users\IEUser\AppData\Local\Microsoft\Windows\History\History.1IE5\
5	132119207926189424	Cookies	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Cookies\
6	132119207925419840	iecompat	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\IECompatCache\
7	132119207925516038	iecompatua	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\iecompatuaCache\
8	132119207913683684	DNTException	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\DNTException\
9	132119207925131246	EmieSiteList	C:\Users\IEUser\AppData\Local\Microsoft\Internet Explorer\EmieSiteList\
10	132119207925131246	EmieUserList	C:\Users\IEUser\AppData\Local\Microsoft\Internet Explorer\EmieUserList\
11	132119207944659440	DOMStore	C:\Users\IEUser\AppData\Local\Microsoft\Internet Explorer\DOMStore\
12	132119207959858724	MSHist012019082820190829	C:\Users\IEUser\AppData\Local\Microsoft\Windows\History\History.1E5\MSHist012019082820190829\
13	132115041147334574	iedownload	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\
14	132119207959762526	MSHist012019082920190830	C:\Users\IEUser\AppData\Local\Microsoft\Windows\History\History.1E5\MSHist012019082920190830\
15	132119207959762526	MSHist012019082620190902	C:\Users\IEUser\AppData\Local\Microsoft\Windows\History\History.1E5\MSHist012019082620190902\
16	132119207959954922	MSHist012019090220190903	C:\Users\IEUser\AppData\Local\Microsoft\Windows\History\History.1E5\MSHist012019090220190903\

Figure 9.14: ESE database showing the Containers table

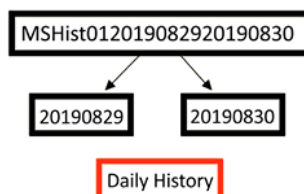


Figure 9.15: The Daily history folder naming convention

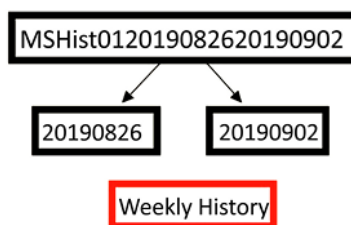


Figure 9.16: Weekly history naming convention. This data spans the time period from August 26, 2019, to September 2, 2019.

EntryId	SyncTime	ExpiryTime	ModifiedTime	AccessedTime	Url
1	132115734791679663	132138198789360361	132115482789355131	132115734791679663	:2019082920190830: IEUser@file:///C:/Program%20Files/Windows%20Mail/MOERES.dll
2	132115734793861687	0	132115482789355131	132115734793861687	:2019082920190830: IEUser@Host: Computer
3	132115735348103202	132138195053033732	132115483347995798	132115735348103202	:2019082920190830: IEUser@file:///C:/Users/IEUser/Downloads/EnableWinMailWin7/msoe_64.zip
4	132115735669898689	132138195374936623	132115483669890000	132115735669898689	:2019082920190830: IEUser@file:///C:/Program%20Files/Windows%20Mail/msoe.dll
5	132115736325813786	132138196030768150	132115484325730216	132115736325813786	:2019082920190830: IEUser@file:///C:/Users/IEUser/Downloads/EnableWinMailWin7/msoe_32.zip

Figure 9.17: Contents of table 12

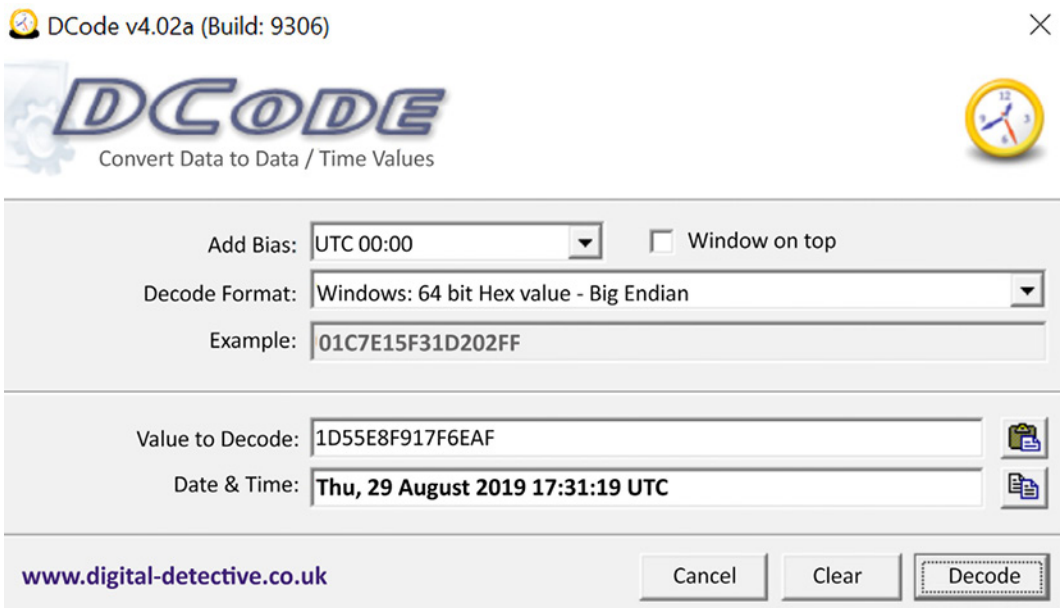


Figure 9.18: DCode tool used to convert the Windows Time value

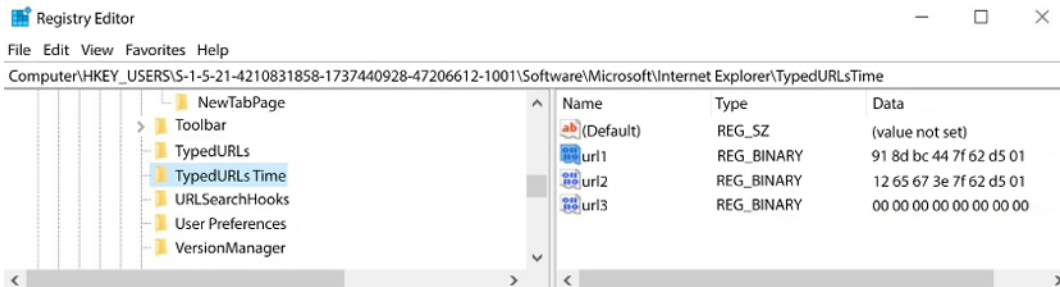


Figure 9.19: TypedURLsTime registry entry

Filename	Content Type	URL	Last Accessed	Last Modified	Expiration Time
acquire-80[1].png	image/png	https://f6ef4eacbe624ae1083a-b3d937de523d4a3...	9/2/2019 11:27	12/5/2018 13:05	9/2/2019 11:42
update_2_19_0_1...	text/html	https://f6ef4eacbe624ae1083a-b3d937de523d4a3...	9/2/2019 11:27	8/22/2019 09:59	9/2/2019 11:42
AAGEZp5[1].jpg	image/jpeg	https://static-global-s-msn-com.akamaized.net/i...	9/2/2019 11:23	9/2/2019 04:57	9/7/2019 04:56
AAesHLQ[1].png	image/png	https://static-global-s-msn-com.akamaized.net/i...	9/2/2019 11:23	8/30/2019 00:28	9/4/2019 00:28
AAGHCg4[1].png	image/jpeg	https://static-global-s-msn-com.akamaized.net/i...	9/2/2019 11:23	9/2/2019 10:27	9/7/2019 10:27

Figure 9.20: The output of cache view

ContainerId	LastAccessTime	Name	PartitionId	Directory
1	132119207925900830	Content	M	C:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
2	132115040805283385	feedplat	M	C:\Users\IEUser\AppData\Local\Microsoft\Feeds\Cache\
3	131594261121527040	ietid	M	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\IETIdCache\
4	132119207924265464	History	M	C:\Users\IEUser\AppData\Local\Microsoft\Windows\History\History.IE5\
5	132119207926189424	Cookies	M	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Cookies\
6	132119207925419840	iecompat	M	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\IECompatCache\
7	132119207925516038	iecompatua	M	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\iecompatuaCache\
8	132119207913683684	DNTException	M	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\DNTException\
9	132119207925131246	EmieSiteList	M	C:\Users\IEUser\AppData\Local\Microsoft\Internet Explorer\EmieSiteList\
10	132119207925131246	EmieUserList	M	C:\Users\IEUser\AppData\Local\Microsoft\Internet Explorer\EmieUserList\
11	132119207944659440	DOMStore	M	C:\Users\IEUser\AppData\Local\Microsoft\Internet Explorer\DOMStore\
12	132119207959858724	MSHist012019082820190829	M	C:\Users\IEUser\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012019082820190829\
13	132115041147334574	iedownload	M	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\

Figure 9.21: Content of the Containers table

EntryId	AccessCount	SyncTime	CreationTime	ExpiryTime	ModifiedTime	AccessedTime	Url	File name
36	18	132119208683123513	132119208683098765	132435432680000000	132119208683098765	132119208683123513	Cookie: euser@yahoo.com/	ff00A\K.txt
41	2	132115040834588757	132115040834204478	132452000840000000	132115040834204478	132119208675537727	Cookie: euser@www2.bing.com/	02VC\RVN.txt
21	17	132119208670850307	132119208670850307	132496048706000000	132119208670850307	132119208670850307	Cookie: euser@www.msn.com/	061C9W\T.txt
47	3	132115044434921485	132115044434921485	132115988430000000	132115044434921485	132115044436695875	Cookie: euser@www.mca.com/	YP2L4CQ.txt
45	4	132115040938395120	132115040938395120	132192800940000000	132115040938395120	132119208656572465	Cookie: euser@www.google.com/	U095\SR9.txt
88	1	132119208810385392	13211920881037806	132426479285000000	13211920881037806	132119208810385393	Cookie: euser@www.bing.com/images	8MC55C\B.txt
28	6	132115040768554247	132115040768554247	132452000760000000	132115040768554247	13211920865615988	Cookie: euser@www.bing.com/	11SCA0L.txt
80	20	132119208580379897	132119208580379897	132496000870000000	132119208580379897	132119208586593995	Cookie: euser@www.akc.com/	0W2Y\W.txt
74	8	132119208601371321	132119208601342395	132461352650000000	132119208601342395	132119208601351321	Cookie: euser@bbc.net/	XTRRX\N.txt
50	1	132119208670631033	132119208670631033	132434568060000000	132119208670631033	132119208670631033	Cookie: euser@optonline.com/	0L\CK0K0.txt

Figure 9.22: Content of the Cookies table

```

MR
0
c.msn.com/
1024
3308281856
30796639
4095225949
30760429

```

Figure 9.23: Example of contents of cookie file

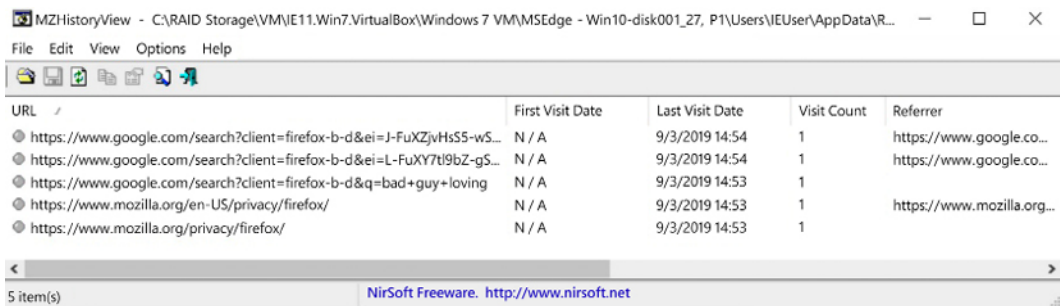


Figure 9.24. Firefox history is shown in MZHistoryView

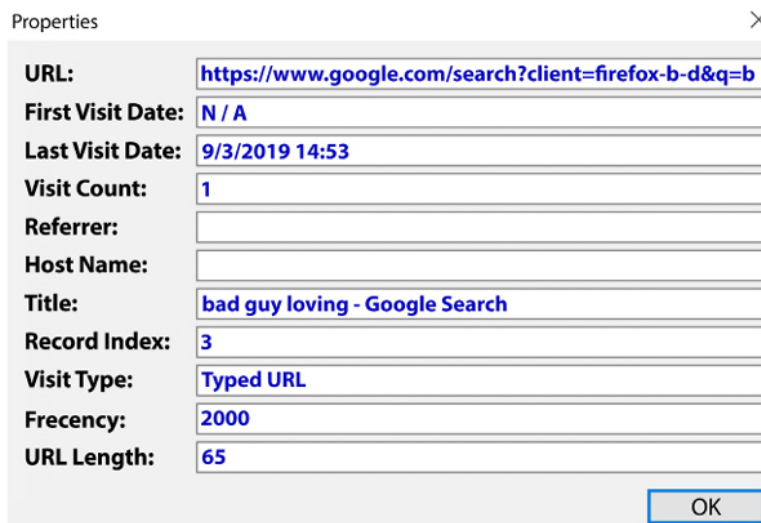


Figure 9.25. Typed URL is shown in record 3

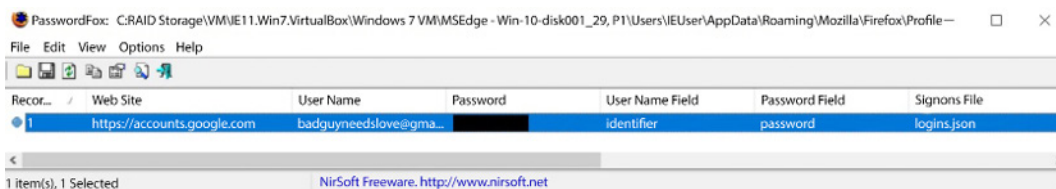


Figure 9.26. Password shown in PasswordFox

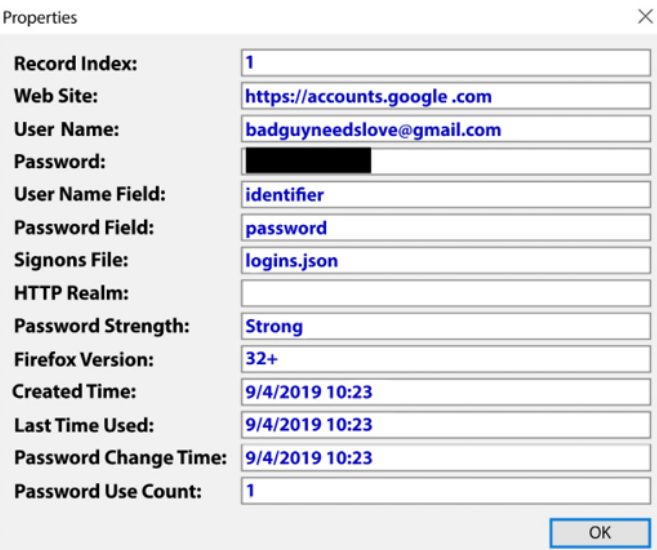


Figure 9.27: Password properties in Password Fox

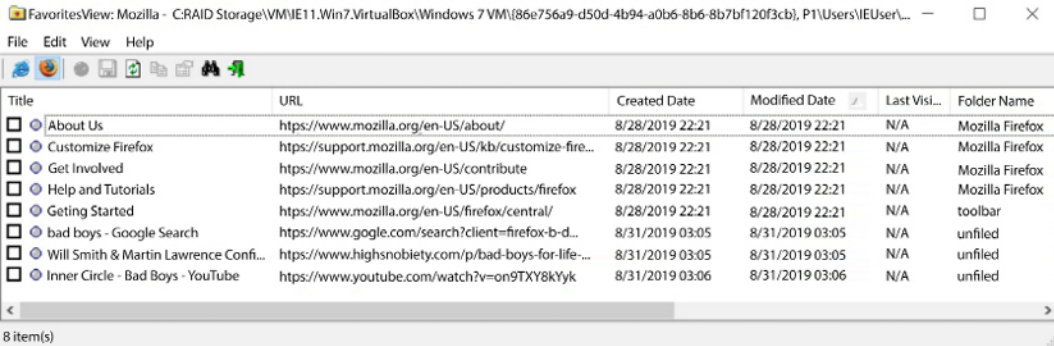


Figure 9.28: Favorites are shown in FavoritesView



Figure 9.29: Facebook URL

Bulk Extractor	
● alerts.txt	
● ccn.txt	
● ccn_histogram.txt	
● domain.txt	
● domain_histogram.	
● elf.txt	
● email.txt	
● email_domain_hist	
● email_histogram.tx	
● ether.txt	
● ether_histogram.txt	
● exif.txt	
● hex.txt	
● jpeg_carved.txt	
● json.txt	
● rfc822.txt	
● sqlite_carved.txt	

Histogram File url_facebook-id.txt	
n=12	1398069580413568
n=12	1819946191667827
n=7	296280873867140
n=5	990491837629352
n=2	1243316582352556
n=1	1661729067442897
n=1	1835684153362700
n=1	282409338764678
n=1	307729452976042
n=1	382649952068500
n=1	520255291469580
n=1	658500157678938

Figure 9.30: Bulk Extractor output for Facebook

bulk extractor	
Bulk Extractor	
● alerts.txt	
● ccn.txt	
● ccn_histogram.txt	
● domain.txt	
● domain_histogram.	
● elf.txt	
● email.txt	
● email_domain_hist	
● email_histogram.tx	
● ether.txt	
● ether_histogram.txt	
● exif.txt	
● hex.txt	
● jpeg_carved.txt	
● json.txt	
● rfc822.txt	

twitter	
Histogram File domain_histogram.txt	
n=412	twitter.com
n=66	platform.twitter.com
n=27	syndication.twitter.com
n=25	analytics.twitter.com
n=24	www.twitter.com
n=10	api.twitter.com
n=7	static.ads-twitter.com
n=7	twitter.github.com
n=1	caps.twitter.com
n=1	cdn.api.twitter.com
n=1	twitter
n=1	urls.api.twitter.com

Figure 9.31: Bulk Extractor output for Twitter



Figure 9.32: Twitter ID

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
00000000	14	C2	B6	08	E8	AA	0E	5A	EA	26	35	5C	BB	56	F5	6F	Â	è
00000016	4C	2C	00	00	00	00	00	00	00	01	00	00	00	FF	FF	FF	L,	ÿÿÿ
00000032	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	0A	00	00	ÿÿÿÿÿÿÿÿÿÿÿÿ	
00000048	00	0A	00	00	00	1F	03	00	00	58	02	00	00				X	

Figure 9.33: eMule User ID

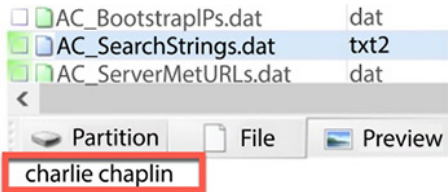
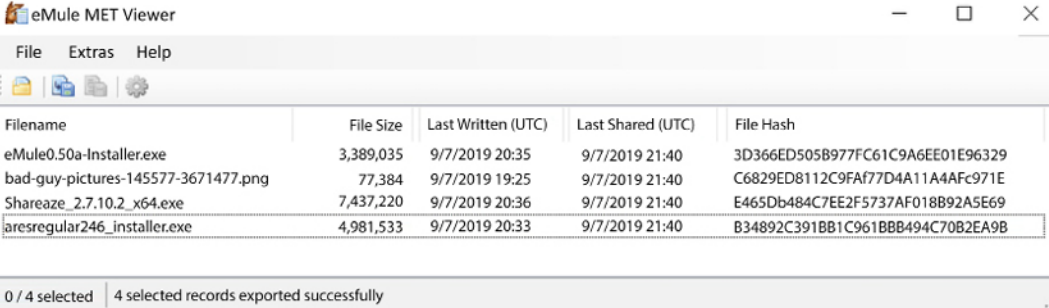


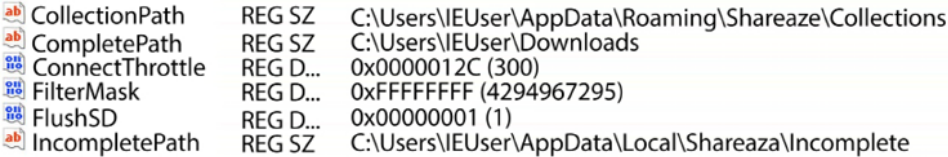
Figure 9.34: eMule Search Terms



The screenshot shows the 'eMule MET Viewer' application window. It has a menu bar with 'File', 'Extras', and 'Help'. Below the menu is a toolbar with icons for file operations. The main area displays a table with the following columns: 'Filename', 'File Size', 'Last Written (UTC)', 'Last Shared (UTC)', and 'File Hash'. The table contains four rows of data. At the bottom, a status bar indicates '0 / 4 selected' and '4 selected records exported successfully'.

Filename	File Size	Last Written (UTC)	Last Shared (UTC)	File Hash
eMule0.50a-Installer.exe	3,389,035	9/7/2019 20:35	9/7/2019 21:40	3D366ED505B977FC61C9A6EE01E96329
bad-guy-pictures-145577-3671477.png	77,384	9/7/2019 19:25	9/7/2019 21:40	C6829ED8112C9FAf77D4A11A4AFc971E
Shareaze_2.7.10.2_x64.exe	7,437,220	9/7/2019 20:36	9/7/2019 21:40	E465Db484C7EE2F5737AF018B92A5E69
aresregular246_installer.exe	4,981,533	9/7/2019 20:33	9/7/2019 21:40	B34892C391BB1C961BBB494C70B2EA9B

Figure 9.35: MetViewer



The screenshot shows the 'Shareaza path' settings. It lists several registry values with their types and paths.

CollectionPath	REG_SZ	C:\Users\IEUser\AppData\Roaming\Shareaze\Collections
CompletePath	REG_SZ	C:\Users\IEUser\Downloads
ConnectThrottle	REG_D...	0x0000012C (300)
FilterMask	REG_D...	0xFFFFFFFF (4294967295)
FlushSD	REG_D...	0x00000001 (1)
IncompletePath	REG_SZ	C:\Users\IEUser\AppData\Local\Shareaza\Incomplete

Figure 9.36: Shareaza path



The screenshot shows the 'Shareaza Search' settings. It lists four search entries with their types and values.

Search.01	REG_SZ	charlie tuna
Search.02	REG_SZ	charlie
Search.03	REG_SZ	john
Search.04	REG_SZ	charlie chaplin

Figure 9.37: Shareaza Search

Links

- Dcode: <https://www.digital-detective.net/dcode/>
- Chrome Pass: <https://www.nirsoft.net/utils/chromepass.html>
- Internet Explorer Cache Viewer: https://www.nirsoft.net/utils/ie_cache_viewer.html
- Mzcacheview: https://www.nirsoft.net/utils/mozilla_cache_viewer.html
- MZCookiesView: <https://www.nirsoft.net/utils/mzcv.html>

- MZHistoryView: https://www.nirsoft.net/utils/mozilla_history_view.html
- Password Fox: <https://www.nirsoft.net/utils/passwordfox.html>
- FavoritesView: <https://www.nirsoft.net/utils/faview.html>
- Facebook URL for analyzing: https://www.facebook.com/photo.php?fbid=10215539711464494&set=a.1627301761019&type=3&source=11&referrer_profile_id=1190817474
- Kik: <https://web.archive.org/web/20201224090043/https://lawenforcement.kik.com/hc/en-us>
- How to use Python to convert Base32 values into Base16: <https://github.com/qbittorrent/qBittorrent/wiki/How-to-convert-base32-to-base16-info-hashes>
- Ares Galaxy: <https://sourceforge.net/projects/aresgalaxy/>
- Magnet Forensics AXIOM forensic tool: <https://www.magnetforensics.com>
- eMule MET Viewer: <https://www.gaijin.at/en/software/emulemetviewer>
- Casey, E. (2017). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Vancouver, B.C.: Langara College. This is available at <https://www.amazon.com/Digital-Evidence-Computer-Crime-Computers/dp/0123742684>.

Static URLs

This section contains static URLs such as path URLs and keys.

- The Google Chrome history file will be found in the following path: %USERS%/AppData/Local/Google/Chrome/User Data/
- The Google Chrome cookie file can be found at the following path: %USERS%/AppData/Local/Google/Chrome/User Data/Default
- You can find the bookmarks file at the following path: %USERS%/AppData/Local/Google/Chrome/User Data/Default/Bookmarks
- The Google Chrome cookie file can be found at the following path: %USERS%/AppData/Local/Google/Chrome/User Data/Default
- The Google Chrome password file can be found at the following path: %USERS%/

AppData/Local/Google/Chrome/User Data/Default

- The default location of the artifacts for the Chromium-based Edge browser is at the following path: C:\Users\%USER%\AppData\Local\Microsoft\Edge\User Data\Default
- The default path Internet Explorer keeps the bookmarks in is at the following path: %USER%/Favorites
- The Edge and Internet Explorer version 10 and higher use an ESE database that can be found at the following path: %User%\AppData\Local\Microsoft\Windows\WebCache
- The system stores cache these files in the following path(s):
 - For a Windows 7-based system: %USER%/AppData/Local/Microsoft/Windows/Temporary Internet Files\Content.IE5
 - ♦ Temporary Internet Files
 - Content.IE5
 - OPDYBC4P
 - S97WTYG7
 - Q67FIXJT
 - 4MNQZMD8
 - SCD1EGFC
 - 34UZLM61
 - V2I5AL1G
 - 5S4OGUTD
 - For a Windows 8/10-based system: %USERS%/AppData/LocalLow/Microsoft/Windows/AppCache
 - ♦ Windows
 - AppCache
 - 0Z1ZMDEH
 - ♦ %USERS%/AppData/Local/Microsoft/Windows/INetCache/IE
 - ♦ INetCache
 - Low

IE

4TENJ512

9SKPYC9A

QMIGA2MM

EP19S3JV

- For the Microsoft Edge browser: %USER%/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/AC
 - ♦ MicrosoftEdge

Cache

9CG3K1S3

IHCXX8UB

OOW222LO

CENY1YGT

- The cookie files of Microsoft Edge are stored in the following path(s): %USER%/AppData/Roaming/Microsoft/Windows/Cookies/
- The cookie files of Microsoft Edge are stored in the following path(s): %USER%/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/AC/MicrosoftEdge/Cookies
- The path where you can find the profiles is as follows: %USER%/AppData/Local/Mozilla/Firefox
- The file tree of three Firefox profiles are as follows:
 - The Bad guy's profile

Firefox

Profiles

tszci9zh.Badguy

thumbnails

safebrowsing

google4

startupCache

cache2

entries

doomed

OfflineCache

- BadGuy Needs Love's profile

fd8rnyou.BadGuy Needs Love

startupCache

cache2

entries

doomed

thumbnails

safebrowsing

google4

OfflineCache

- Default user's profile

30nh3g6c.default-release

startupCache

cache2

doomed

entries

thumbnails

OfflineCache

- The profiles.ini file can be found at the following path: %USER%/AppData/Roaming/Mozilla/Firefox/profiles.ini
- The contents of the profiles.ini file is shown here:

```
[Install1308046B0AF4A39CB]
```

```
Default=Profiles/fd8rnyou.Badguy Needs Love
```

```
Locked=1
```

```
[Profile2]
```

```
Name=Badguy
```

IsRelative=1
Path=Profiles/tszci9zh.Badguy
Default=1
[Profile1]
Name=default
IsRelative=1
Path=Profiles/9wofgs9f.default
[Profile0]
Name=default-release
IsRelative=1
Path=Profiles/30nh3g6c.default-release
[General]
Startwithlastprofile=1
Version=2
[Profile3]
Name=Badguy Needs Love
IsRelative=1
Path=Profiles/fd8rnyou.Badguy Needs Love

- The cache files are stored at the following path: %USER%/AppData/Local/Mozilla/Firefox/Profiles/%Profile%
- The file tree of the cache files looks like the following:

Firefox

Profiles

tszci9zh.Badguy

thumbnails

safebrowsing

google4

startupCache

cache2

entries

doomed

OfflineCache

- You can find the cookie database at the following path: %USER%/AppData/Roaming/Mozilla/Firefox/Profiles/%Profile%
- You can find the history database at the following path: %USER%/AppData/Roaming/Mozilla/Firefox/Profiles/%Profile%
- You can find the password files at the following path: %USER%/AppData/Roaming/Mozilla/Firefox/Profiles/%Profile%
- You can find the bookmark database file at the following path: %USER%/AppData/Roaming/Mozilla/Firefox/Profiles/%Profile%
- The Shareaza folder structure(s) can be seen in the user profile as follows:
 - %USER%\AppData\Local\Shareaza
 - %USER%\AppData\Local\Shareaza\Incomplete
 - %USER%\AppData\Roaming\Shareaza
 - %USER%\AppData\Roaming\Shareaza\Collections
 - %USER%\AppData\Roaming\Shareaza\Data
 - %USER%\AppData\Roaming\Shareaza\Torrents
- eMule stores its configuration files in the user's local profile, as follows: %USER%\AppData\Local\eMule

Code

Code 9.1: The following is the Python code that Chris Hurst provided:

```
>>> import base64
>>> b32Hash = "WRN7ZT6NKMA6SSXYKAFRUGDDIFJUNKI2"
>>> b16Hash = base64.b16encode(base64.b32decode(b32Hash))
>>> b16Hash = b16Hash.lower()
>>> print (b16Hash)
```

Output

Output 9.1

```
Filename      : gmail.html
URL           : https://www.google.com/gmail
Content Type  : text/html
File Size     : 0
Last Accessed : 8/28/2019 15:17
Server Time   : 8/28/2019 15:17
Server Last Modified:
Expire Time   :
Server Name   : sffe
Server Response : HTTP/1.1 302
Content Encoding :
Cache Name    :
Cache Control : private
ETag          :
Server IP Address : 172.217.14.100
URL Length    : 28 =====
```

Output 9.2

TypedURLs

Software\Microsoft\Internet Explorer\TypedURLs

LastWrite Time Tue Sep 3 17:29:58 2019 (U.T.C)

url1 -> http://bankrobbery.com/

url2 -> http://yahoo.com/

url3 -> http://gmail.com/

Output 9.3

Name	Created	Modified
06PC9CZM.txt	09/03/2019 17:29:48	09/03/2019 17:29:48
09BHTXJM.txt	09/02/2019 18:00:59	09/02/2019 18:00:59
09WSNIHD.txt	09/03/2019 17:29:27	09/03/2019 17:29:27
0W6YLVUJ.txt	09/02/2019 18:01:08	09/02/2019 18:01:08
0WBQAB4E.txt	09/02/2019 18:23:51	09/02/2019 18:23:51
16SUYNBJ.txt	09/03/2019 17:29:51	09/03/2019 17:29:51
1983DVP6.txt	09/02/2019 18:23:46	09/02/2019 18:23:46
28Z2GM8G.txt	09/03/2019 17:29:49	09/03/2019 17:29:49
2CM18GNC.txt	09/03/2019 17:29:38	09/03/2019 17:29:38

Output 9.4

```
Software\Ares
LastWrite Time Sat Sep 7 21:48:04 2019 (UTC)
Stats.LstConnect: Mon Sep 8 15:51:07 2019 UTC
Personal.Nickname: Badguy27
General.Language: English
PrivateMessage.AwayMessage: This is an automatic away message generated by Ares program, user isn't here now.
Search Terms: Badguy movies
```

Output 9.5

```
C:\Users\IEUser\Downloads\aresregular246_installer.exe
```

```
C:\Users\IEUser\Downloads\bad-guy-pictures-145577-3671477.png
```

```
C:\Users\IEUser\Downloads\eMule0.50a-Installer.exe
```

```
C:\Users\IEUser\Downloads\Shareaza_2.7.10.2_x64.exe
```

Chapter 10

Images



Figure 10.1: Guerrilla Mail interface


✓ Random
Male
Female

✓ American
Arabic
Australian
Brazil
Chechen (Latin)
Chinese
Chinese (Traditional)
Croatian
Czech
Danish
Dutch
England/Wales
Eritrean
Finnish
French
German
Greenland
Hispanic
Hobbit
Hungarian
Icelandic
Igbo
Italian
Japanese
Japanese (Anglicized)
Klingon
Ninja
Norwegian
Persian
Polish
Russian
Russian (Cyrillic)
Scottish
Slovenian

Your Randomly Generated Identity

Gender Random
Name set American
Country United States

Generate Advanced Options



Logged in users can view full social security numbers and can save their fake names to use later.

g+ Sign in

Paul D. Walker
135 Meadowcrest Lane
Harold, KY 41635

Curious what **Paul** means? [Click here to find out!](#)

Mother's maiden name Thompson
SSN 404-28-XXXX
You should [click here](#) to find out if your SSN is online.

Geo coordinates 37.470508, -82.715889

PHONE
Phone 606-478-1020
Country code 1

BIRTHDAY
Birthday January 3, 1947
Age 75 years old
Tropical zodiac Capricorn

ONLINE
Email Address PaulDWalker@teleworm.us
This is a real email address. [Click here to activate it!](#)
Username Iming1947
Password OoleiN5l
Website anhuilulu.com
Browser user agent Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Safari/605.1.15

New Zealand
Norway
Poland
Portugal
Slovenia
South Africa
Spain
Sweden
Switzerland
Tunisia
United Kingdom
✓ United States
Uruguay

Figure 10.2: Fake Name Generator persona creation

FINANCE

Visa	4916 4096 8823 0356
Expires	7/2026
CVV2	818

EMPLOYMENT

Company	Father & Son
Occupation	Oxygen therapist

PHYSICAL CHARACTERISTICS

Height	5' 11" (180 centimeters)
Weight	205.9 pounds (93.6 kilograms)
Blood type	O-

TRACKING NUMBERS

UPS tracking number	1Z 44F 355 58 6760 719 9
Western Union MTCN	6208789813
MoneyGram MTCN	38098536

OTHER

Favorite color	Blue
Vehicle	2001 Nissan GT-R
GUID	daed7db8-9bab-43a5-b21b-528841a83cab
QR Code	Click to view the QR code for this identity

Figure 10.3: Remainder of the person's information



Figure 10.4: Random set of images from <https://thispersondoesnotexist.com>

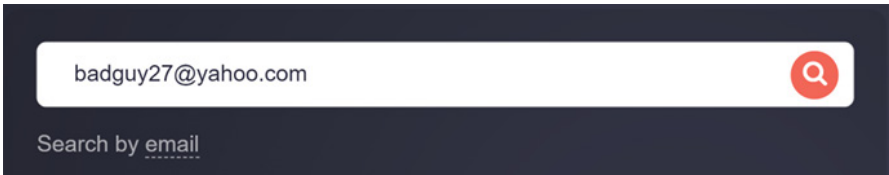


Figure 10.5: WhoisXML API input badguy27@yahoo.com

badguy27@yahoo.com verification details

Check email by syntax	Valid
SMTP check	The email address exists and can receive email over SMTP.
Domain name system check	The domain in the email address has passed DNS check.
Free email address check	The email address is free.
Check email provider for abuse	The email address isn't disposable.
Catch all emails address	The mail server has a "catch-all" address.

Figure 10.6: WhoisXML API response for badguy27@yahoo.com

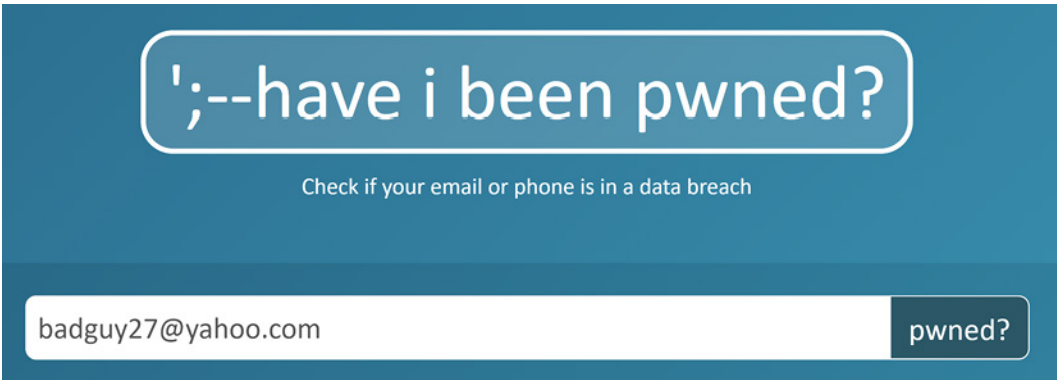
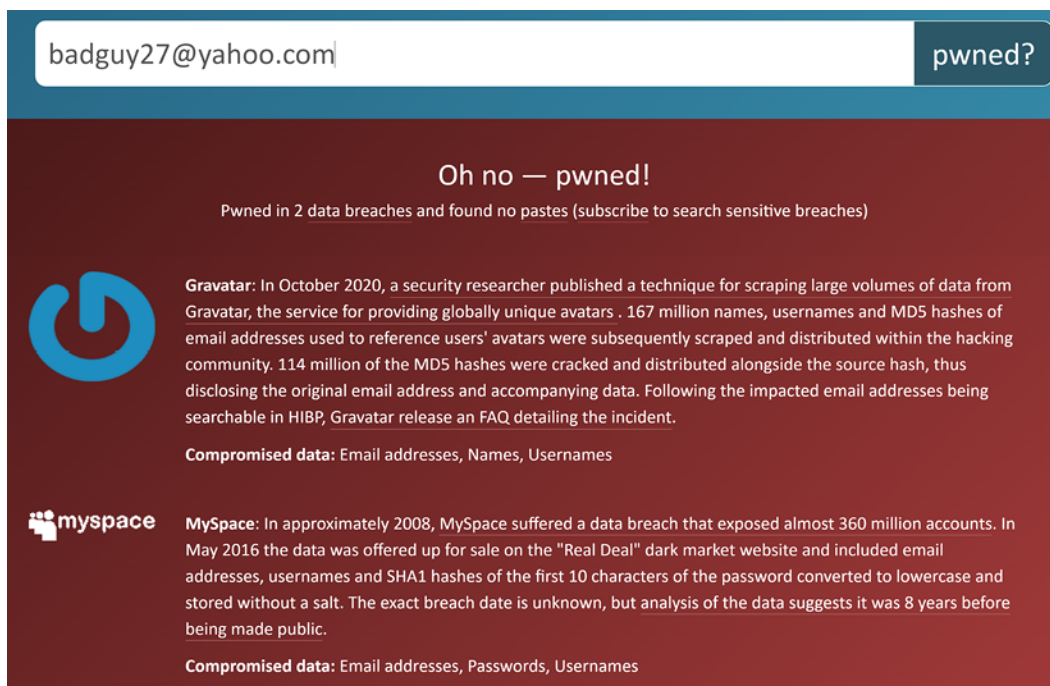



Figure 10.7: have i been pwned? search for badguy27@yahoo.com




badguy27@yahoo.com pwned?

Oh no — pwned!

Pwned in 2 data breaches and found no pastes ([subscribe to search sensitive breaches](#))

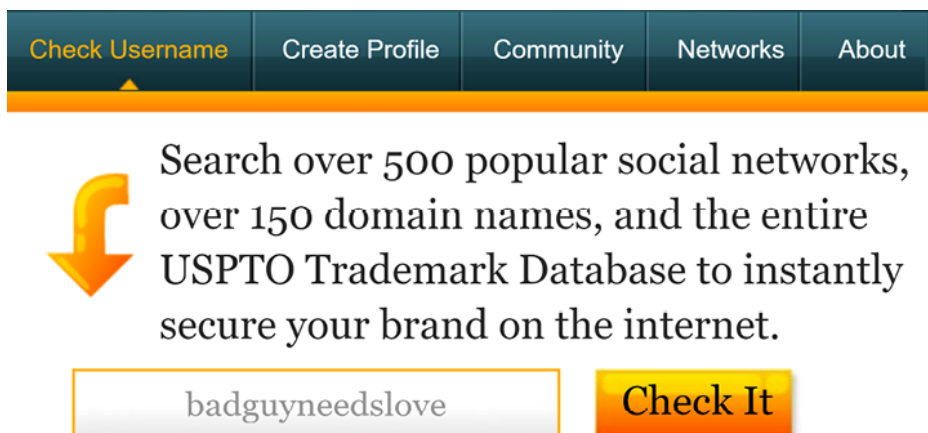
 **Gravatar:** In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars. 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an [FAQ](#) detailing the incident.

Compromised data: Email addresses, Names, Usernames

 **MySpace:** In approximately 2008, MySpace suffered a data breach that exposed almost 360 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years before being made public.

Compromised data: Email addresses, Passwords, Usernames

Figure 10.8: have i been pwned? results for badguy27@yahoo.com



Check Username Create Profile Community Networks About

Search over 500 popular social networks, over 150 domain names, and the entire USPTO Trademark Database to instantly secure your brand on the internet.

badguyneedslove Check It

Figure 10.9: Knowem search for badguyneedslove

Preview Search of Top 25 Most Popular Social Networks

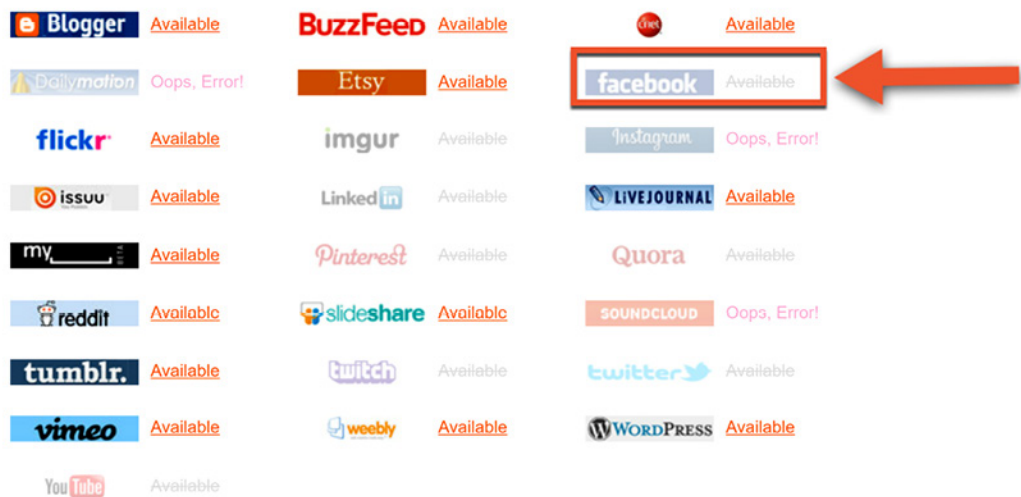


Figure 10.10: Knowem search results for badguyneedslove



Figure 10.11: Facebook and Twitter results

TruePeopleSearch


Name	Reverse Phone	Reverse Address
<input type="text" value="e.g John Smith"/>	<input type="text" value="City, State or Zip"/>	<input type="text" value=""/>

Figure 10.12: True People Search – search screen


John Smith

Age

Full Background Report Available → Ad

 Current Address

Narrows, VA 24124

 Phone Numbers

(405) - Landline

(314) - Landline

(248) - Landline

Figure 10.13: True People Search – results (name)



Previous Addresses

██████████

Edmond, OK 73012

(Dec 1969 - Jan 2021)

Map

██████████

Las Vegas, NV 89110

(Nov 2017 - May 2020)

Map

██████████


Marionville, MO 65705

(Sep 2004 - Jan 2020)

Map

View All Addresses

Figure 10.14: True People Search – results (address)



Email Addresses


j.a.smith@██████████.edu

mynonnie@██████████.net


jalexandersmith@██████████.com

View All Email Addresses

Figure 10.15: True People Search – results (email)




Darci R ██████████, Amanda L ██████████, Angelica R ██████████, Brenton E ██████████, Carneous



Possible Associates

Donna ██████████, Kimberly ██████████, Dishonne ██████████, Lawrence ██████████



Possible Businesses

██████████
██████████ Mi 48336

Figure 10.16: True People Search – results (possible)

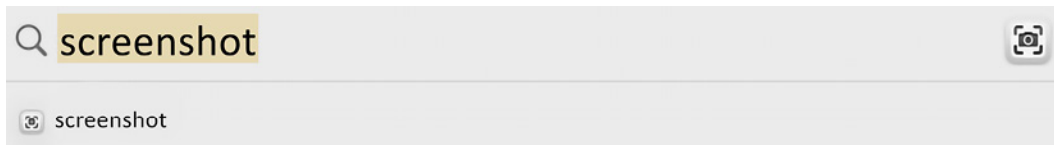


Figure 10.17: Spotlight Search – “screenshot”

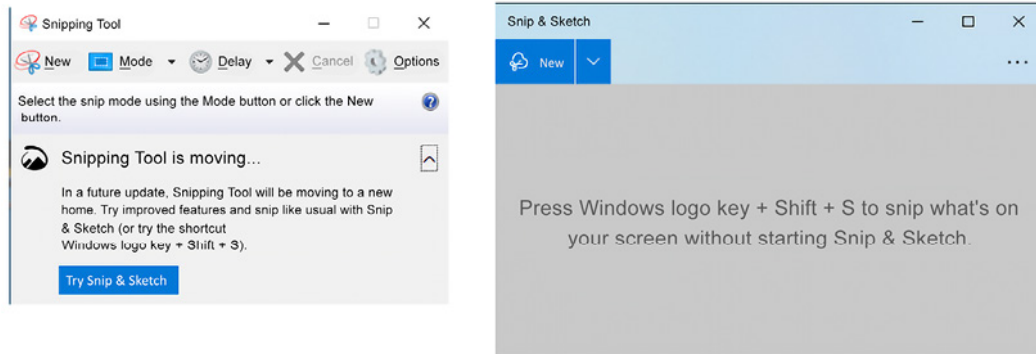


Figure 10.18: MS Windows – Snipping Tool and Snip and Sketch

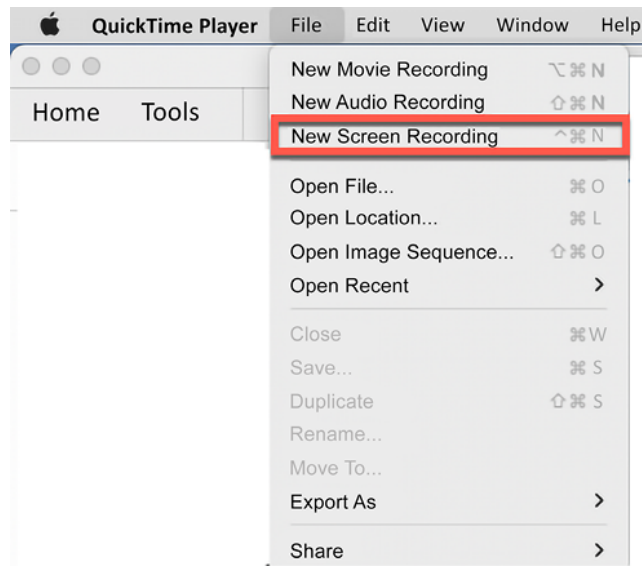


Figure 10.19: QuickTime Player menu

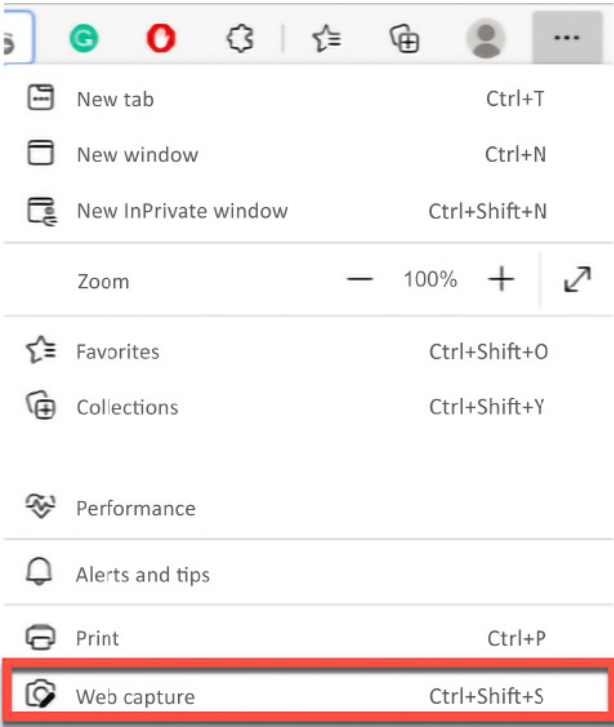


Figure 10.20: Edge browser capture menu

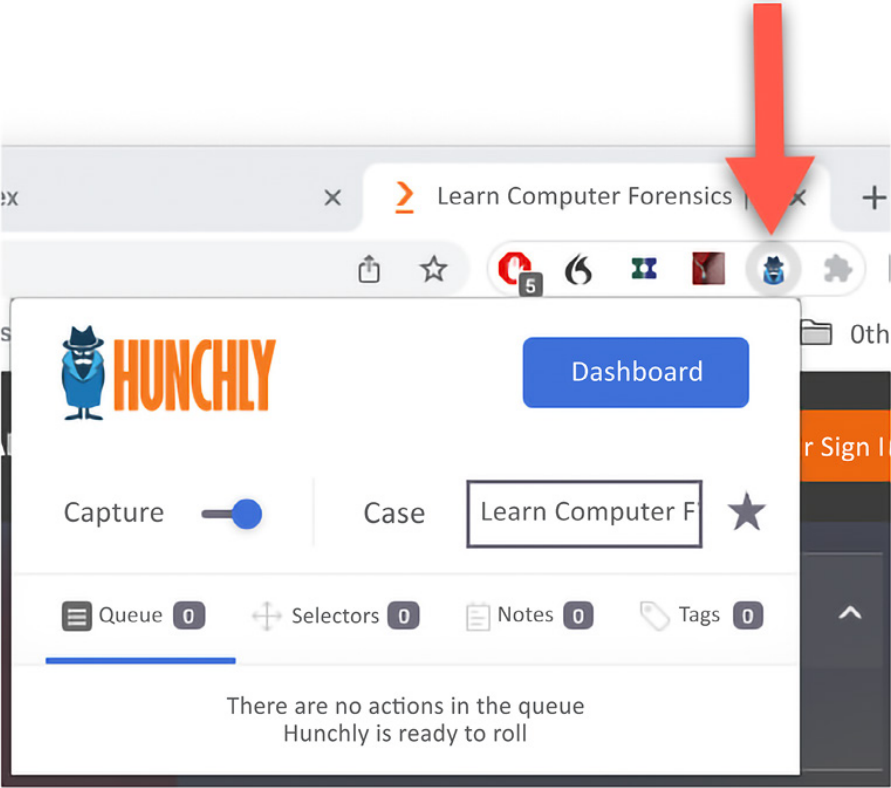


Figure 10.21: Hunchly extension menu

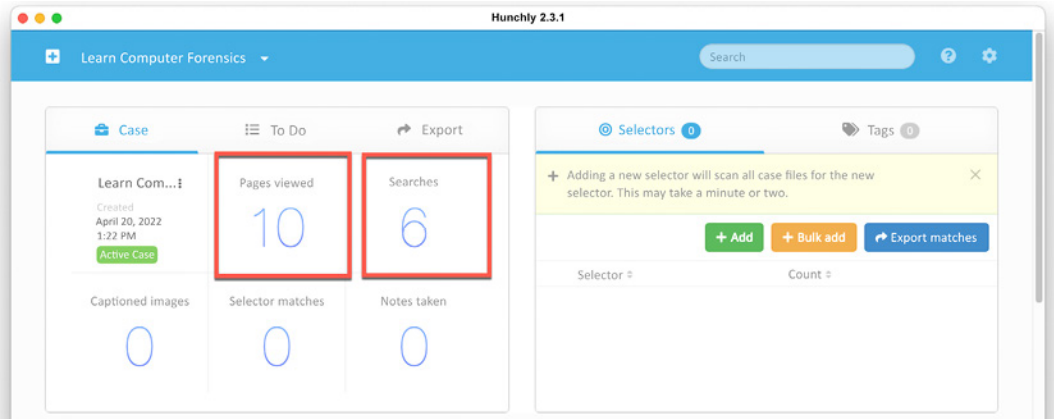


Figure 10.22: Hunchly desktop

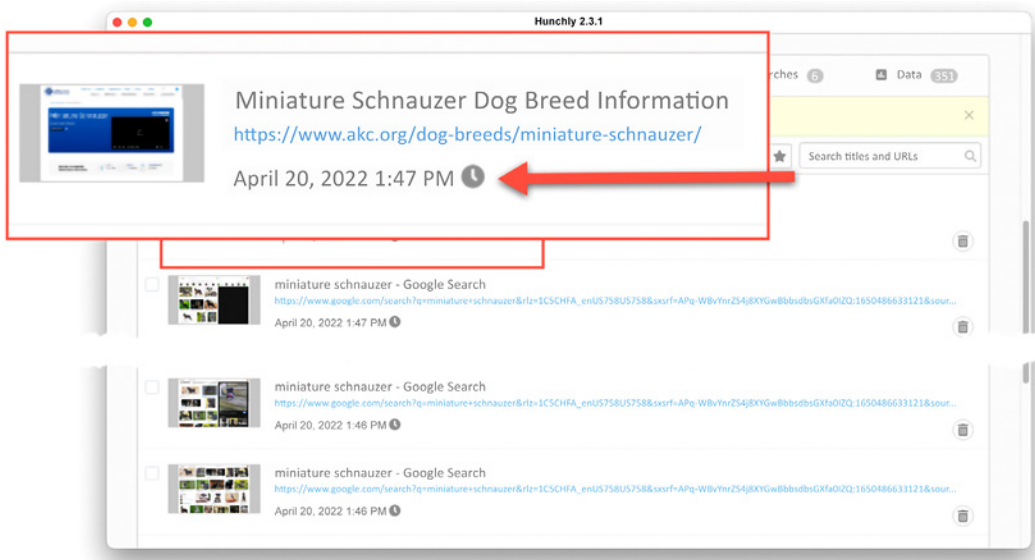


Figure 10.23: Hunchly history

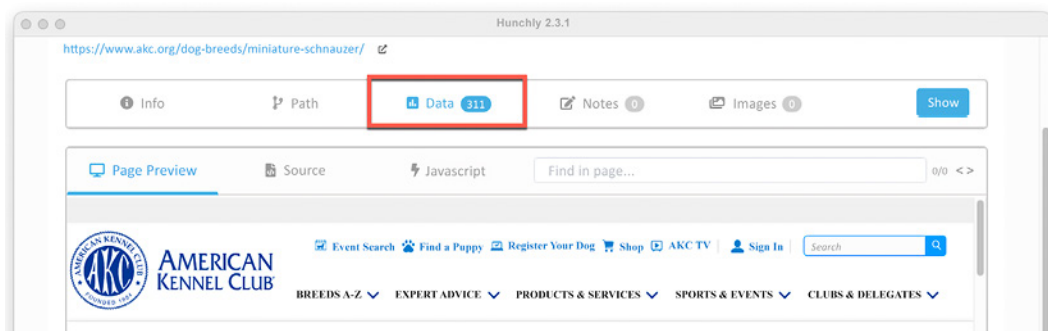


Figure 10.24: Hunchly preview

Type	Category	Value
Tracking Code	Google Analytics	UA-36985312-37
Accounts	Email Address	g@yahoo.com
Accounts	Email Address	ds8@gmail.com
Accounts	Email Address	USA@gmail.com

Tracking Code	Infrastructure	Facebook Tracking Pixel ID	IPv4 IP Address
		98709637134806	1.4.3.7
			1.3.2.5
			6.1.1.1
			2.1.3.2

Figure 10.25 Hunchly Data view

Links

- Temp Mail: <https://temp-mail.org/en/>
- Guerrilla Mail: <https://www.guerrillamail.com/>
- Tutanota: <https://tutanota.com/>
- ProtonMail: <https://protonmail.com/>
- Fake Name Generator: <https://www.fakenamegenerator.com>
- This Person Does Not Exist: <https://thispersondoesnotexist.com>
- Fake Caller ID: <https://fakecallerid.io>
- Email Hippo: <https://tools.emailhippo.com/>
- Hunter: <https://hunter.io/>
- Verify Email: <https://verify-email.org/>
- DeBounce: <https://debounce.io/>
- Emailable: <https://emailable.com/>

- Reacher: <https://reacher.email/>
- WhoisXML API: <https://geekflare.com/email-verification-api/>
- Pastebin: <https://pastebin.com/>
- PSBDMP (<https://psbdmp.ws/>)
- have i been pwned?: <https://haveibeenpwned.com/>
- SpyCloud: <https://spycloud.com/>
- Knowem: knowem.com
- Target's username URL: www.facebook.com/badguynneedslove
- True People Search: <https://truepeoplesearch.com/>
- Whitepages: <https://www.whitepages.com/>
- ZabaSearch: <https://zabasearch.com/>
- People Search Now: <https://peoplesearchnow.com/>
- Spokeo: <https://www.spokeo.com/>
- Hunchly: <https://www.hunch.ly/>
- FireShot: <https://getfireshot.com/>
- HTTrack: <https://www.httrack.com/>
- Web2Disk: <http://www.web2disk.com/>
- SiteSucker: <https://ricks-apps.com/osx/sitesucker/index.html>
- X1 Social Discovery: <https://www.x1.com/products/x1-social-discovery/>
- EyeWitness: <https://github.com/FortyNorthSecurity/EyeWitness>
- FAW: <https://en.fawproject.com>
- Open source intelligence techniques: Resources for searching and analyzing online information: [Inteltechniques.com](https://inteltechniques.com).
- Hunting cyber criminals: A hacker's guide to online intelligence gathering tools and techniques. Indianapolis, Indiana: John Wiley & Sons Inc.

Chapter 11

Images

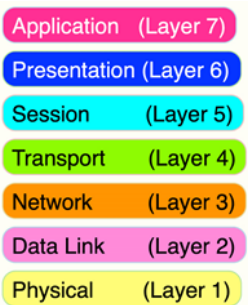


Figure 11.1: OSI model

Application (Layer 7)	User Interaction
Presentation (Layer 6)	Data Formatting, Encryption
Session (Layer 5)	Controls Ports and Sessions
Transport (Layer 4)	Data Transmission Protocols
Network (Layer 3)	Routing
Data Link (Layer 2)	Formatting of the data
Physical (Layer 1)	Physical medium of the network

Figure 11.2: OSI model – layer functions

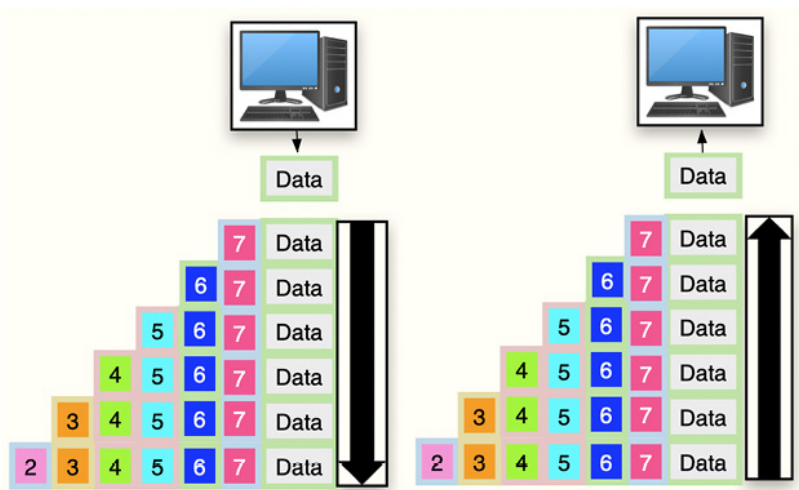


Figure 11.3: Encapsulation

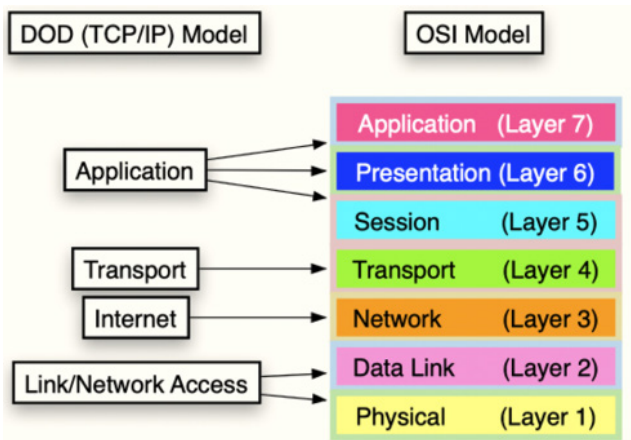


Figure 11.4: The TCP/IP model compared to the OSI model

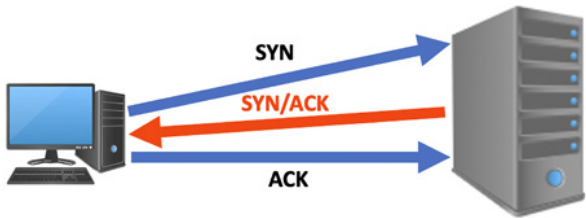


Figure 11.5: TCP three-way handshake

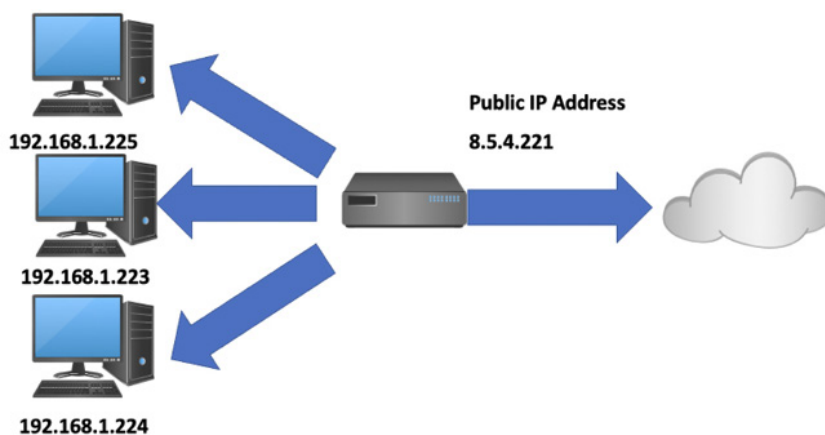


Figure 11.6: Example of NAT

2001:0db8:0000:0000:0000:8a2e:0370:7334

Figure 11.7: IPv6 address

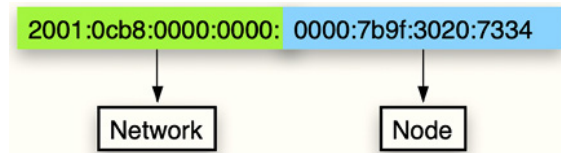


Figure 11.8: IPv6 address separated

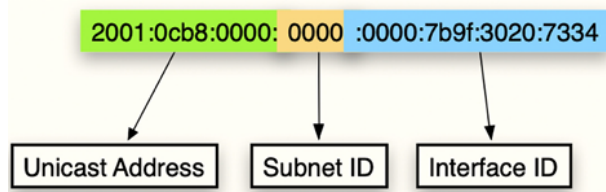


Figure 11.9: IPv6



Figure 11.10: IPv6 shorthand example

Table

Class	Address Range	Max Number of Hosts	Private eye-pee Range
Class A	1.0.0.1 - 126.255.255.254	16,777,214 Hosts	10.0.0.0, 10.255.255.255
Class B	128.1.0.1 - 191.255.255.254	65,532 Hosts	176.16.0.0, 172.31.255.255
Class C	192.0.1.1 - 223.255.254.254	256 Hosts	192.168.0.0, 192.168.255.255
Class D	224.0.0.0 - 239.255.255.255	Reserved for Multicast	
Class E	240.0.0.0 - 254.255.255.254	Reserved for Research	

Table 11.1. eye-pee-version-four eye-pee address classes

Examples

Example 11.1

```
User@Server ~ % ping packtpub.com
PING packtpub.com (104.22.1.175): 56 data bytes
64 bytes from 104.22.1.175: icmp_seq=0 ttl=60 time=10.270 ms
64 bytes from 104.22.1.175: icmp_seq=1 ttl=60 time=9.949 ms
64 bytes from 104.22.1.175: icmp_seq=2 ttl=60 time=14.081 ms
64 bytes from 104.22.1.175: icmp_seq=3 ttl=60 time=13.323 ms
64 bytes from 104.22.1.175: icmp_seq=4 ttl=60 time=9.048 ms
64 bytes from 104.22.1.175: icmp_seq=5 ttl=60 time=9.077 ms
64 bytes from 104.22.1.175: icmp_seq=6 ttl=60 time=9.254 ms
```

Example 11.2

```
User@Server ~ % ping 192.168.86.22
PING 192.168.86.22 (192.168.86.22): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
ping: sendto: No route to host
```

Appendix

Neil, I. (2018). *Comptia Security+ Certification Guide: Master It security essentials and exam topics for Comptia security+ sy0-501 certification*. Packt Publishing Ltd.

Davies, G. (2019). *Networking fundamentals: Develop the networking skills required to pass the Microsoft Mta Networking Fundamentals Exam 98-366*. Packt Publishing Ltd.

Chapter 12

Images

Item Name	Tag Number	Description
Compaq Presario	Tag1	Compaq Presario Laptop Computer
Toshiba HD	Tag1 HD001	256 GB Toshiba SATA Hard Drive from the Compaq Presario Laptop Computer
SanDisk Cruzer	Tag1 TD001	128 GB SanDisk Cruzer Glide Thumb drive

Figure 12.1: Evidence Tag example

Compaq Presario (Tag1 HD001)	
Product Name	Windows 10
Computer Name	BadGuy Laptop
Registered Owner	BadGuy27
Install Date	August 13, 2018, 08:52:58 (Local)
Last Shutdown	October 12, 2018, 23:44:11 (Local)
Time Zone	Pacific Standard Time

Figure 12.2: Evidence example

Links

For more information, you can refer to Forensic Examination of Digital Evidence, A Guide for Law Enforcement, from <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>.

Chapter 13

Links

- IACIS's Code of Ethics: <https://www.iacis.com/wp-content/uploads/2019/11/IACIS-Code-of-Ethics-and-Professional-Conduct-Ver-1.4.pdf>
- IFSCE's Code of Ethics: <https://www.isfce.com/ethics2.htm>
- Smith, F. C., and Bace, R. G. (2003). A guide to forensic testimony: the art and practice of presenting testimony as an expert technical witness. Boston, MA: Addison-Wesley: <https://www.amazon.com/Guide-Forensic-Testimony-Presenting-Technical/dp/0201752794>
- Poynter, D. (2012). Expert witness handbook: tips and techniques for the litigation consultant. Santa Barbara, CA: Para Pub: <https://www.amazon.com/Expert-Witness-Handbook-Techniques-Litigations/dp/1568601522>