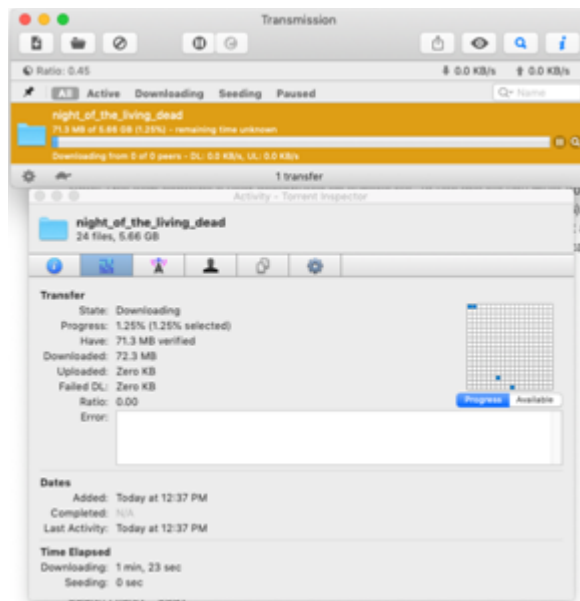


Chapter 1: Types of Computer-Based Investigations



Please sign in

You have successfully logged out

Username
Password
Sign in

Dashboard

No campaigns created yet. Let's create one!

New 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](#)

Chapter 2: The Forensic Analysis Process

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)

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



Hash Test.txt - Notepad

File Edit Format View Help
This is a test

startjacksum.txt - Notepad

File Edit Format View Help

|ce114e4501d2f4e2dcea3e17b546f339 F:\Hash Test.txt

a54d88e06612d820bc3be72877c74f257b561b19 F:\Hash Test.txt

Created with Jacksum 1.7.0, algorithm=md5 and sha-1

Hash Test change.txt - Notepad

File Edit Format View Help
This is a test!

702edca0b2181c15d457eacac39de39b F:\Hash Test change.txt

8b6ccb43dca2040c3cfbcd7bfff0b387d4538c33 F:\Hash Test change.txt

Created with Jacksum 1.7.0, algorithm=md5 and sha-1

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

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

File Signatures

01 * 001 1001 101 00101 1 01 10001 1001010010000001 * 1001 101 10100101 1001 * 101 101 * 1001 100000101 1010001 1 1010101 1 0010001 10010101 10001 1
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

Extension Signature

File Signatures

68:68:60:68:20:73:69:67:66:61:74:75:72:68:73

[Search](#) [All Signatures](#) [Submit Sigs](#) [My Favorites](#) [Control Panel](#)

Disable autocomplete

Extension Signature

3 Results Found For JPG File Extension

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

AccessData FTK Imager 4.2.0.13

File View Mode Help

- Add Evidence Item...
- Add All Attached Devices
- Image Mounting...**
- Remove Evidence Item
- Remove All Evidence Items
- Create Disk Image...
- Export Disk Image...
- Export Logical Image (AD1)...
- Add to Custom Content Image (AD1)...
- Create Custom Content Image (AD1)...
- Decrypt AD1 image...
- Verify Drive/Image...
- Capture Memory...
- Obtain Protected Files...
- Detect EFS Encryption
- Export Files...
- Export File Hash List...
- Export Directory Listing...
- Exit

Mount Image To Drive

Add Image

Image file:

Mount Type:

Drive Letter:

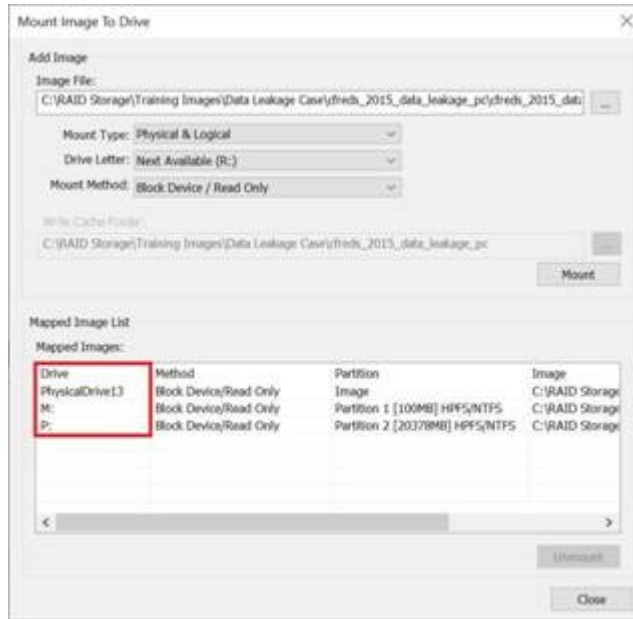
Mount Method:

Write Cache Policy:

Mapped Image List

Mapped Images:

Drive	Method	Partition	Image



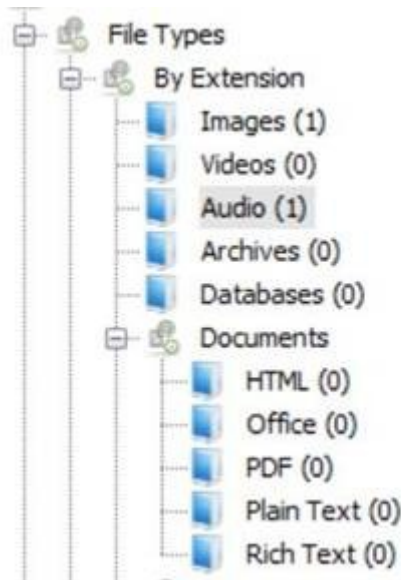
Chapter 3: Acquisition of Evidence

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

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

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

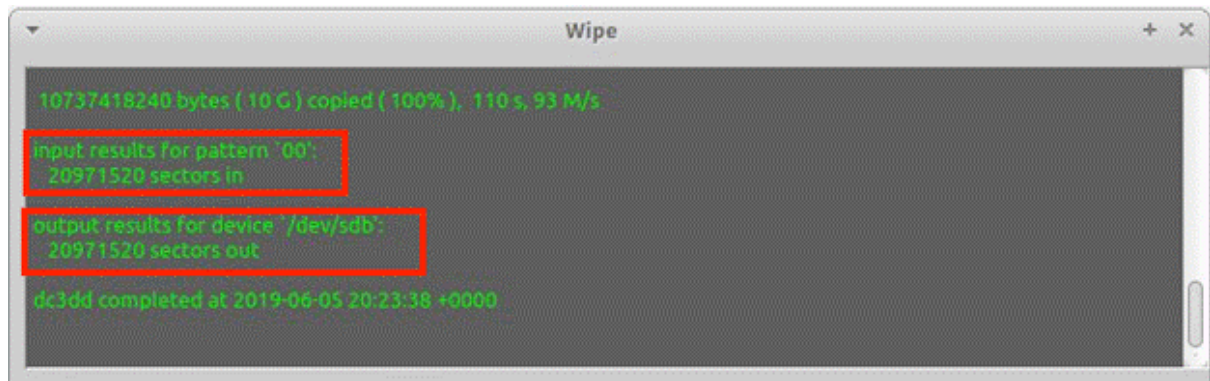
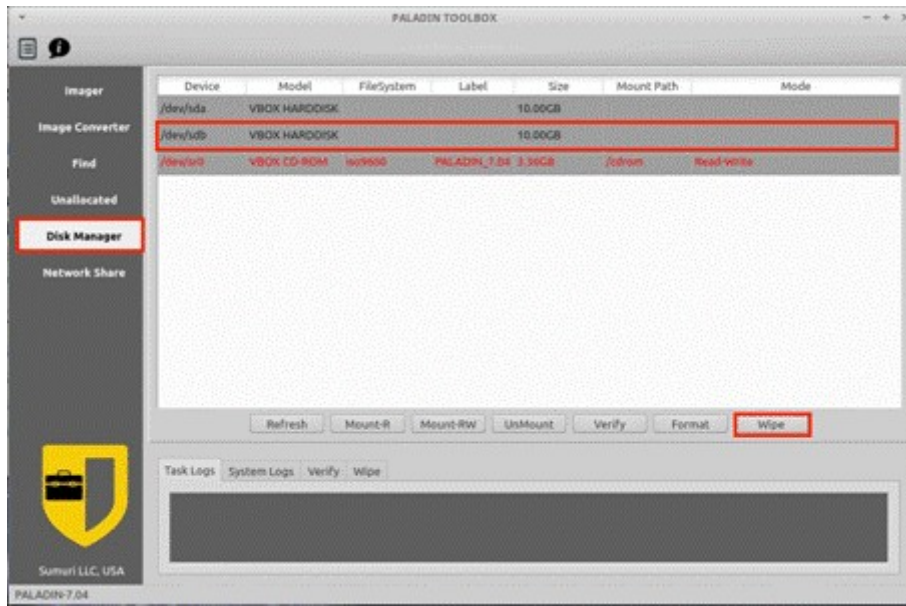
```
039C8A00 Scientific control.mp3 MD5: e73a608dfb422a206ce7a62deb90ff9b  
029D4A00 Export_me.JPG MD5: c0c3892606849fd76a8534ef80956705
```

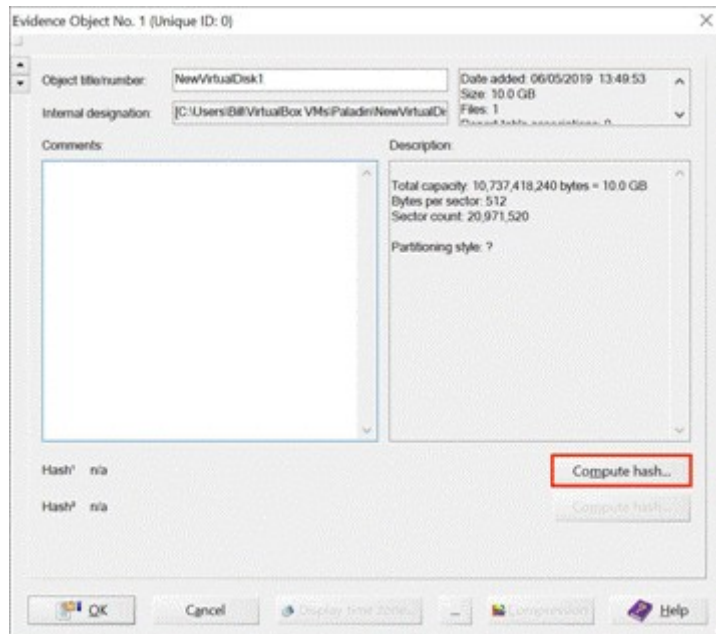
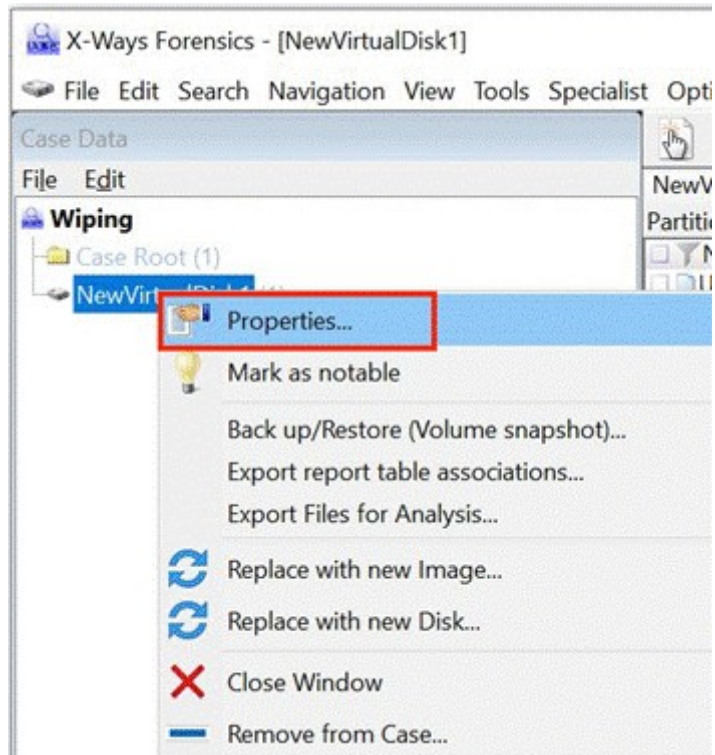


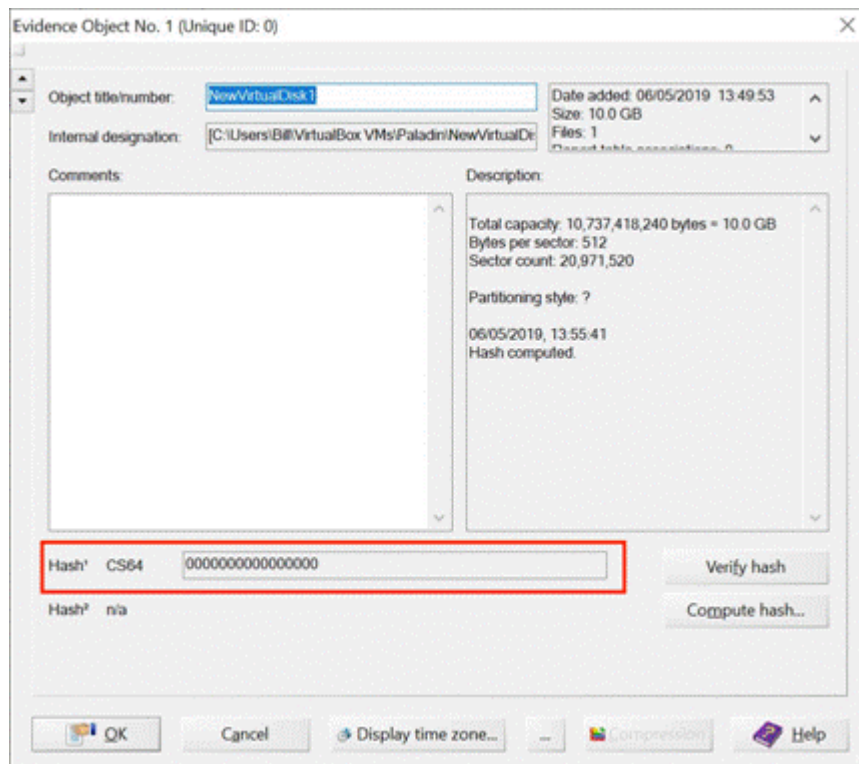
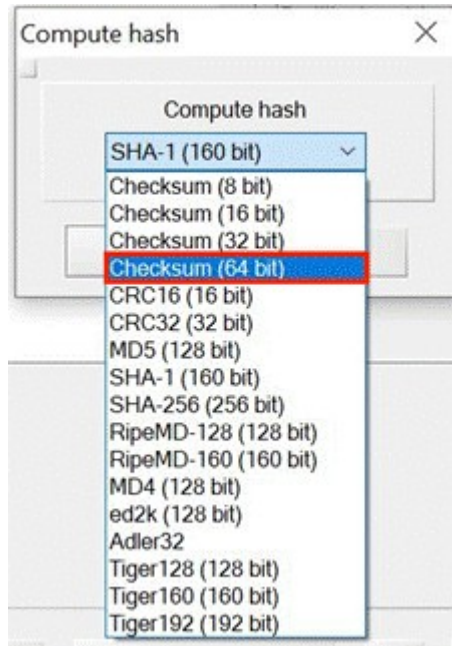
Name	Type
\$Extend (3)	
(Root directory)	
System Volume Information (2)	
RECYCLER (2)	
\$AttrDef	
\$Bitmap	
\$Boot	
\$LogFile	
\$MFT (1)	
\$MFTMirr	
\$UpCase	
Export_me.JPG	jpg
Scientific control.mp3	doc
\$BadClus (1)	
\$Secure (3)	
\$Volume	
deleted.JPG	jpg
MVC-577V.MPG	mpg
Free space (not)	
Idle space	
Misc non-resident attributes	
Volume slack	

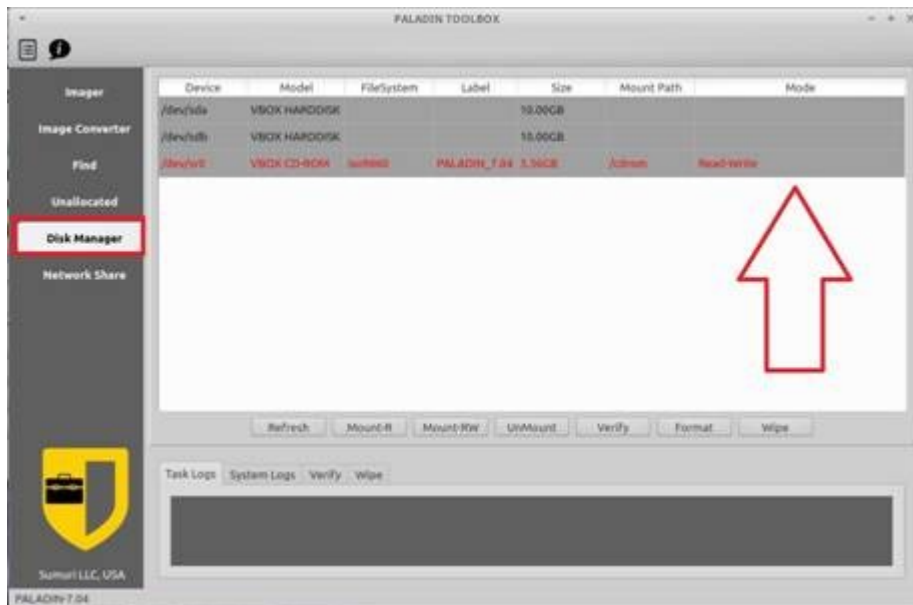
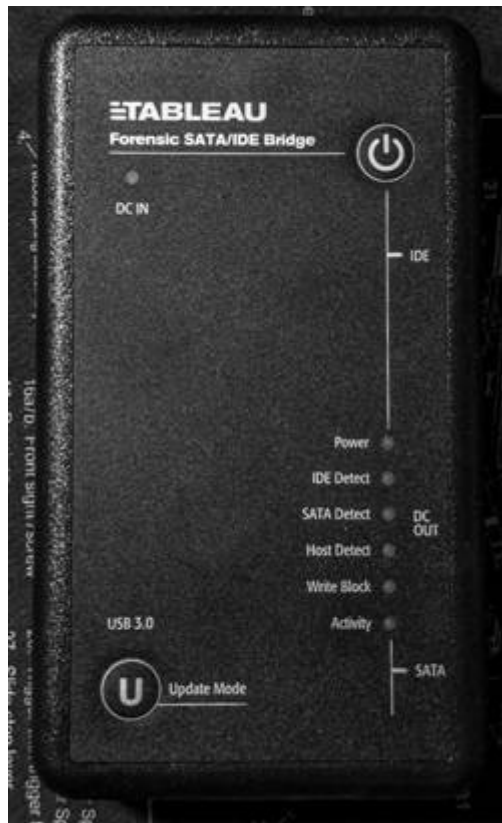
Name /img_control.dd/Export_me.JPG
 Type File System
 MIME Type image/jpeg
 Size 21165
 File Name Allocation Allocated
 Metadata Allocation Allocated
 Modified 2007-08-20 06:10:23 PDT
 Accessed 2007-08-20 07:21:37 PDT
 Created 2007-08-20 06:10:23 PDT
 Changed 2007-08-20 07:21:47 PDT
 MD5 c0c3892606849fd76a8534ef80956705

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 changed¹	08/20/2007 13:10:23 +0
Ext.	JPG
Type status	confirmed, OK
Type descr.	JPEG
Category	Pictures
Path	\
Full path	\Export_me.JPG
Parent name	\
Attr.	A
1st sector	85,669
FS offset	43897856
ID	29
Int. ID	22
Int. parent	6
Unique ID	0-22
Unique ID as GUID	00000016-0000-4000-B0E330CC71024E5F
Owner	S-1-5-21-3958095517-222395546-2225589205-500
Link count	'1
Pixels	0.4 MP
Analysis	0% skin tones
Hash¹ (MD5)	C0C3892606849FD76A8534EF80956705
Hash¹ (SHA-1)	4F90640F999271C41A1E77804FD7AAA4F0340D9D
Generator signature	60F38468 (U-Standard 75 Edited)
Device type	unknown
Relevance	3.59









Device	Model	FileSystem	Label	Size	Mount Path	Mode
/dev/sda	VBOX HARDDISK			10.00GB		
/dev/sda1	VBOX HARDDISK	ext4	OS	10.00GB	/media/OS	Read Only
/dev/sdb	VBOX HARDDISK			10.00GB		
/dev/ur0	VBOX CD-ROM	iso9660	PALADIN_7.04	3.36GB	/cdrom	Read-Write

↑

Refresh Mount-R Mount-RW UnMount Verify Format Wipe

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

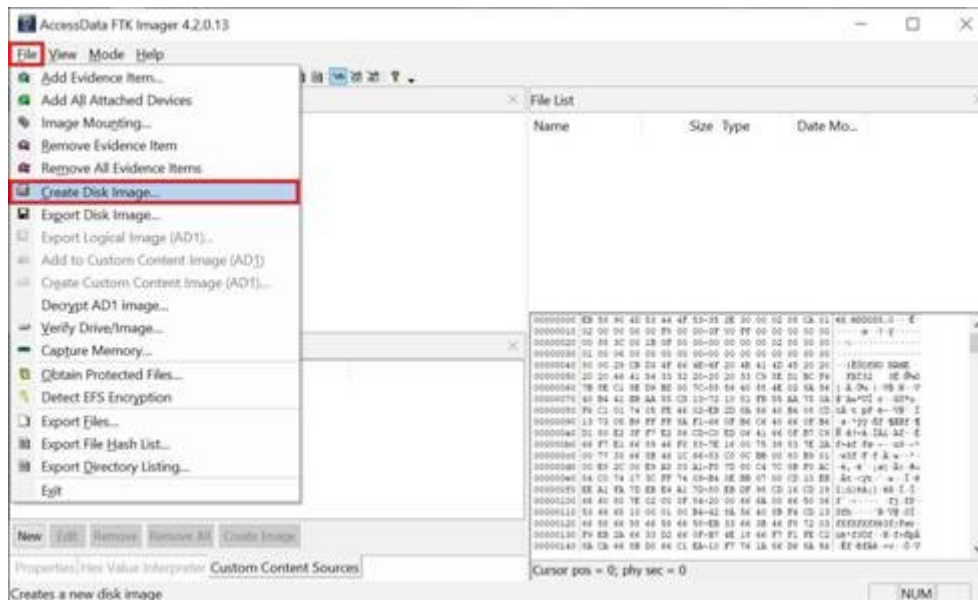
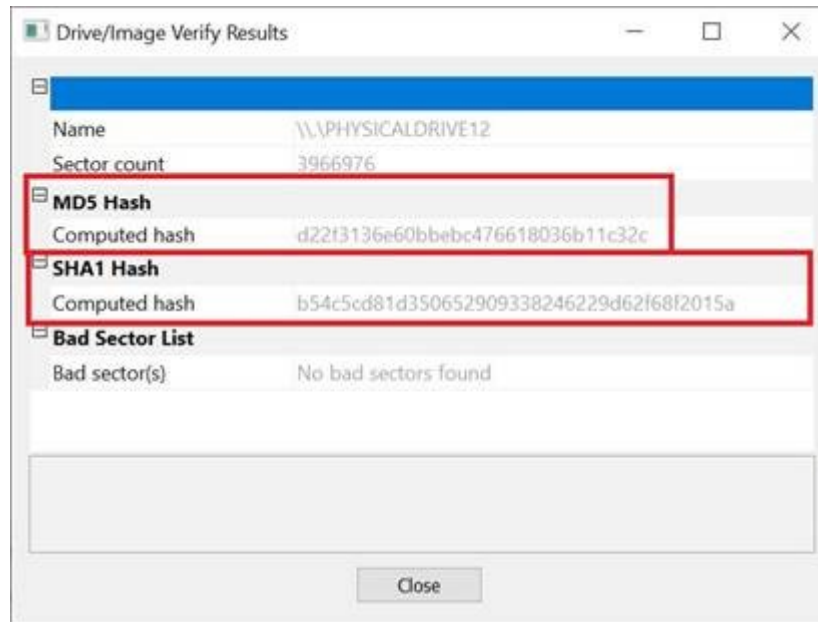
- Case Information
- CRC
- Data
- CRC
- Data
- CRC
- Data
- CRC
- MD5

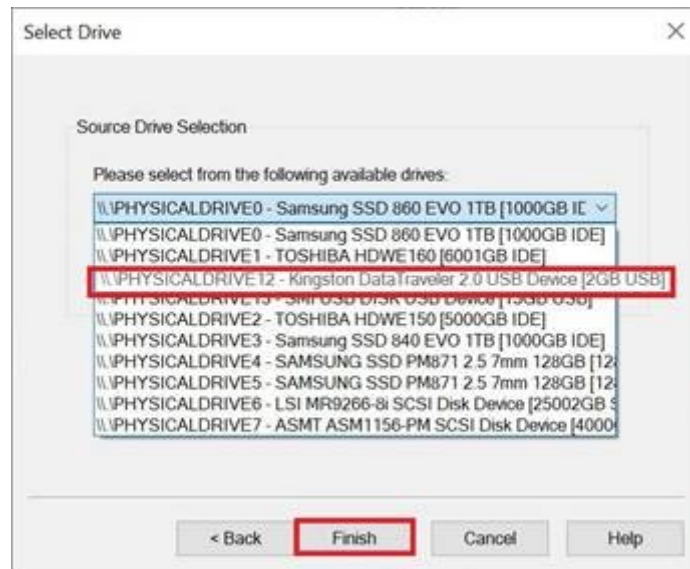
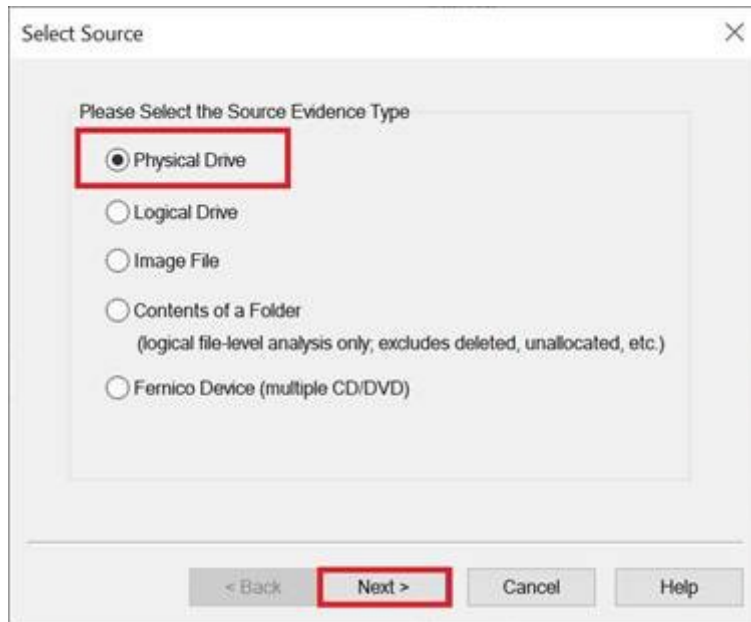
AccessData FTK Imager 4.2.0.13

File View Mode Help

Evidence Tree

- \\PHYSICAL
 - Remove Evidence Item
 - Verify Drive/Image...
 - Export Disk Image...
 - Image Mounting...
 - Export Directory Listing...





Select Image Type

Please Select the Destination Image Type

Raw (dd)
 SMART
 E01
 AFF

< Back Next > Cancel Help

Evidence Item Information

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

< Back Next > Cancel Help

Select Image Destination

Image Destination Folder
N:\Forensic Image Browse

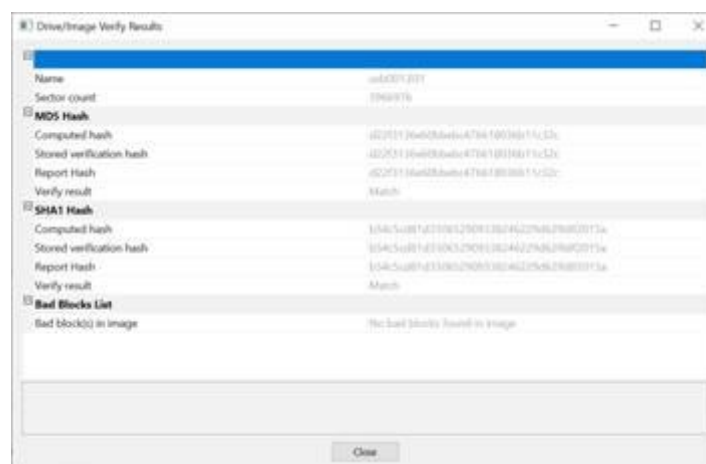
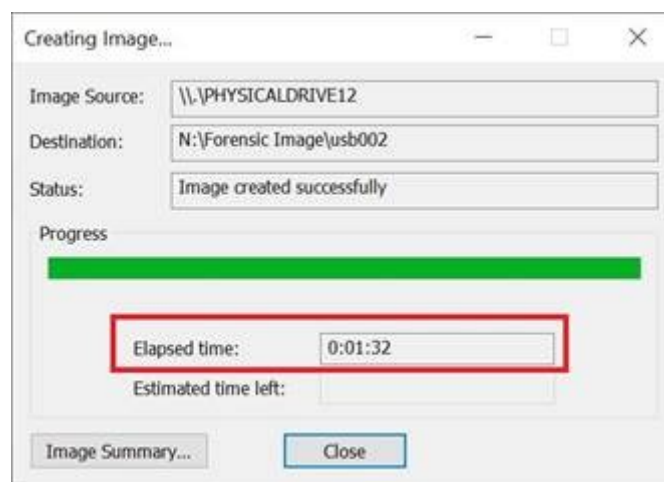
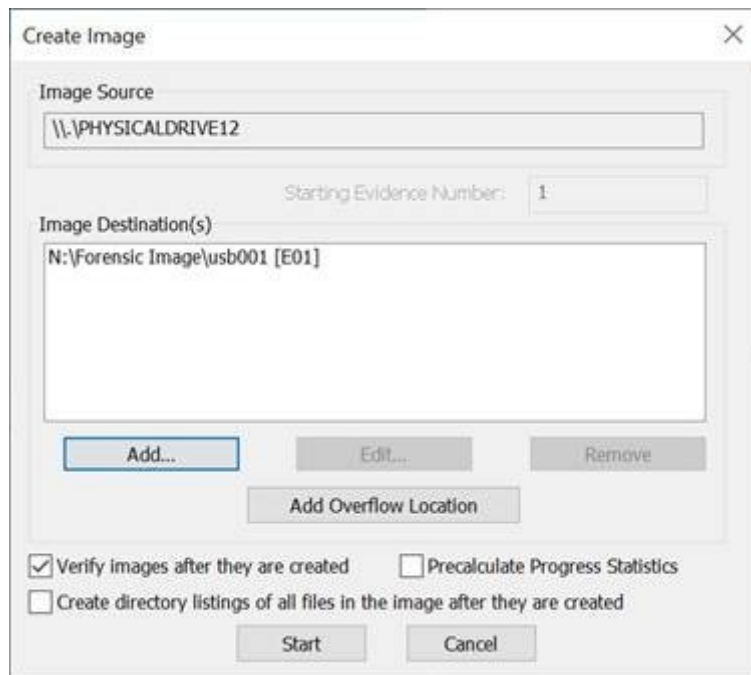
Image Filename (Excluding Extension)
usb001

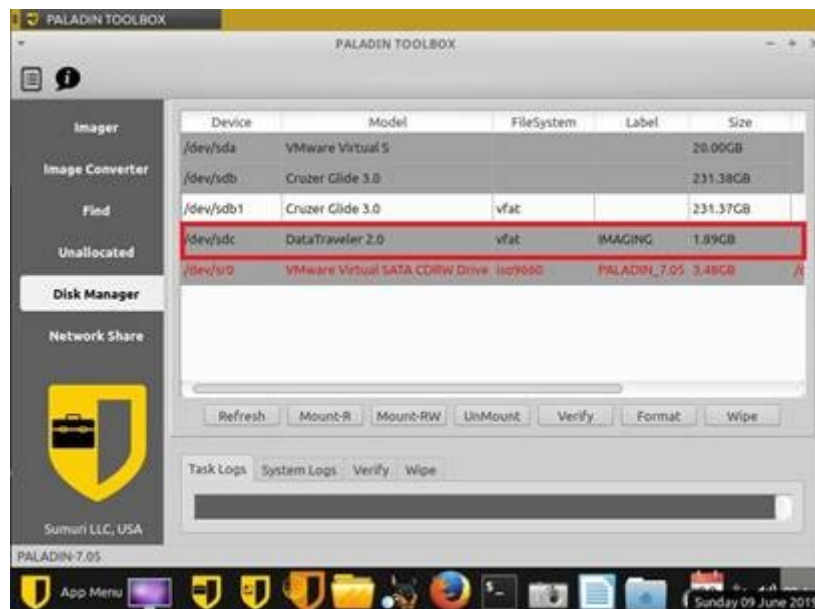
Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

Use AD Encryption

< Back Finish Cancel Help





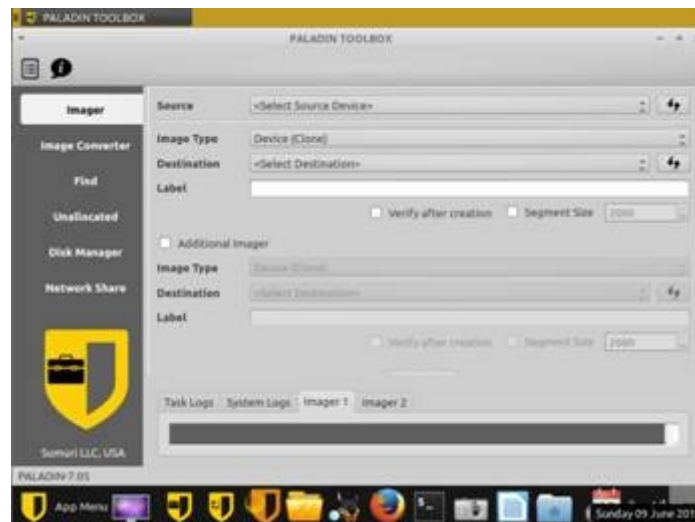
```

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':

```



<Select Source Device>

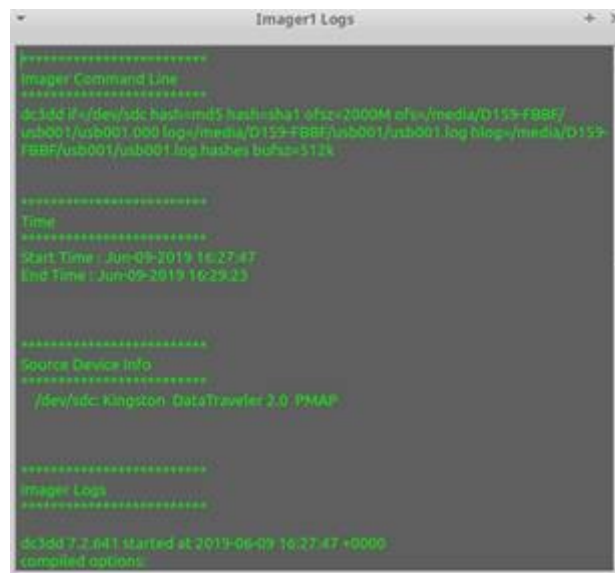
/dev/sda VMware Virtual S 20.00GB
/dev/sdb Cruzer Glide 3.0 231.38GB
/dev/sdb1 Cruzer Glide 3.0 231.37GB vfat
/dev/sdc DataTraveler 2.0 1.89GB
/dev/sr0 VMware Virtual SATA CDRW Drive 3.48GB

Device (Clone)

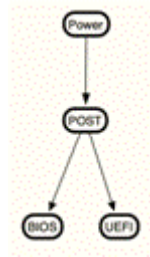
dd (RAW)
EWF (E01)
EWF2 (Ex01)
SMART (S01)
DMG (dmg)
VMDK (vmdk)
VHD (vhd)

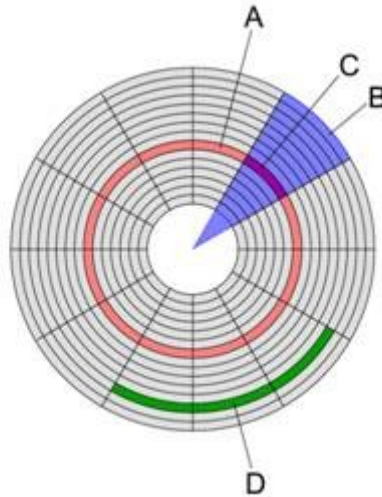
<Select Destination>

/dev/sdb1 Cruzer Glide 3.0 231.37GB vfat



Chapter 4: Computer Systems





Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	13	C0	8E	D0	BC	00	7C	FB	50	07	50	1F	FC	BE	10	7C	hAZ0n jGp P UN
00000010	BF	10	96	50	57	89	E5	01	F3	A4	C6	BD	BE	07	B1	94	l Pw'A 0mEsh x
00000020	38	8E	00	7C	89	75	13	83	C5	10	E2	F4	CD	18	88	F9	ln j u jA a0i .0
00000030	E3	C6	10	49	74	19	38	2C	T4	F6	A0	B5	97	B4	87	8B	/A It s, to y
00000040	F0	AC	3C	00	74	FC	8B	0T	00	B4	9E	CD	10	EB	F2	88	o<c t0> I 60
00000050	4E	10	E8	46	00	T2	2A	FE	46	10	00	7E	04	0B	74	0B	N eF s+bF e- t
00000060	80	7E	94	0C	74	05	A0	90	07	75	D2	00	46	02	06	03	e- t *u0eF f
00000070	46	08	06	83	96	0A	00	E8	21	00	73	05	A0	06	07	EB	F jV 6i s * 4
00000080	0C	81	3E	FE	7D	55	AA	74	0B	80	7E	10	0B	74	C8	A6	u 0p]U*t e- 1E
00000090	87	07	EB	A9	8B	FC	1E	57	8B	F5	CB	BF	05	00	8A	56	r 88:0 w:0Ej 5V
000000A0	00	B4	08	CD	13	72	23	8A	C1	24	3F	98	8A	DE	8A	FC	I re5A57 5p50
000000B0	43	F7	E3	8B	D1	86	D6	B1	06	D2	FE	42	F7	E2	39	58	C+r:8f0s 0fB+r9V
000000C0	0A	77	23	72	05	39	46	08	73	1C	88	01	02	88	00	7C	wer 9f s =
000000D0	88	4E	02	8B	56	00	CD	13	73	51	4F	74	4C	32	E4	8A	N v I s00tN285
000000E0	96	00	CD	13	EB	E4	8A	56	08	68	BB	AA	55	84	41	CD	V I aa5V *u AI
000000F0	13	72	36	81	FB	55	AA	75	30	F6	C1	01	74	2B	61	80	r8 00*u00A t+a
00000100	8A	00	8A	00	FF	76	0A	FF	76	0B	0A	00	00	00	7C	8A	j jv jv j h j
00000110	01	6A	10	84	42	88	F4	CD	13	61	61	73	0E	4F	74	0B	j B:0I was 0s
00000120	32	E4	8A	56	00	CD	13	FB	D6	61	F9	C3	49	8E	76	61	285V I 80wuAImv
00000130	9C	69	64	20	70	61	72	74	69	74	69	6F	8E	20	74	61	lid partition ta
00000140	62	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E	ble Error loadin
00000150	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	g operating syst
00000160	65	60	00	40	69	73	73	69	6E	67	20	6F	70	65	72	61	em Missing opera
00000170	74	69	6E	67	20	73	79	73	74	65	60	00	00	00	00	00	ting system
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001B0	00	08	00	00	00	2C	44	63	C8	7E	C8	7E	00	00	00	01	,0cE-E-
000001C0	01	90	DE	FE	3F	0A	3F	00	00	00	8C	B2	02	00	00	00	0p? ? * k
000001D0	01	00	07	FE	FF	4B	82	02	00	T4	30	51	02	00	00	00	pp9K^2 t8Q
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55 AA

```

00 01 01 00 DE FE 3F 0A 3F 00 00 00 0C B2 02 00
80 00 01 0B 07 FE FF FF 4B B2 02 00 74 38 51 02
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

```

Partition Partition Partition **Extended partition**

Extended partition

Partition Partition Partition Partition

```
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
```

```
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 lÓ0
00000000220 AF 12 9E 3B 00 00 00 00 22 00 00 00 00 00 00 00 - ž; "
00000000230 8E 12 9E 3B 00 00 00 00 A2 60 8A D3 0D 63 00 43 Ž ž; €`ŠÓ c C
00000000240 9F 9D 39 BD FB 81 B3 9E 02 00 00 00 00 00 00 00 Ÿ 9!ú ³ž
00000000250 80 00 00 00 80 00 00 00 64 96 AF 89 00 00 00 00 € € d-~%
00000000260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```


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

Partitioning style: GPT

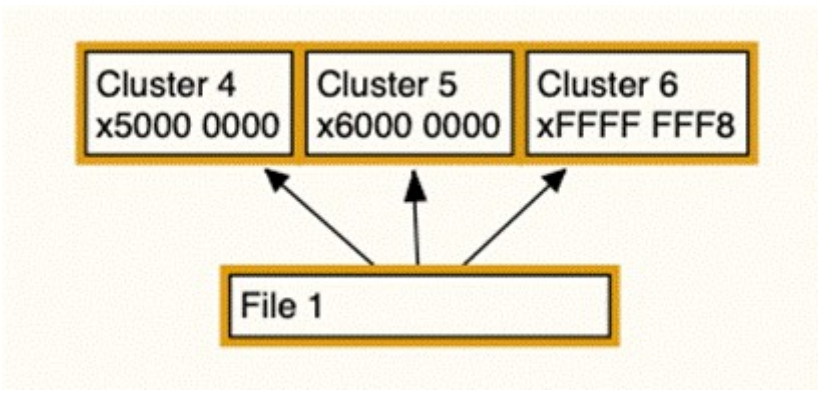
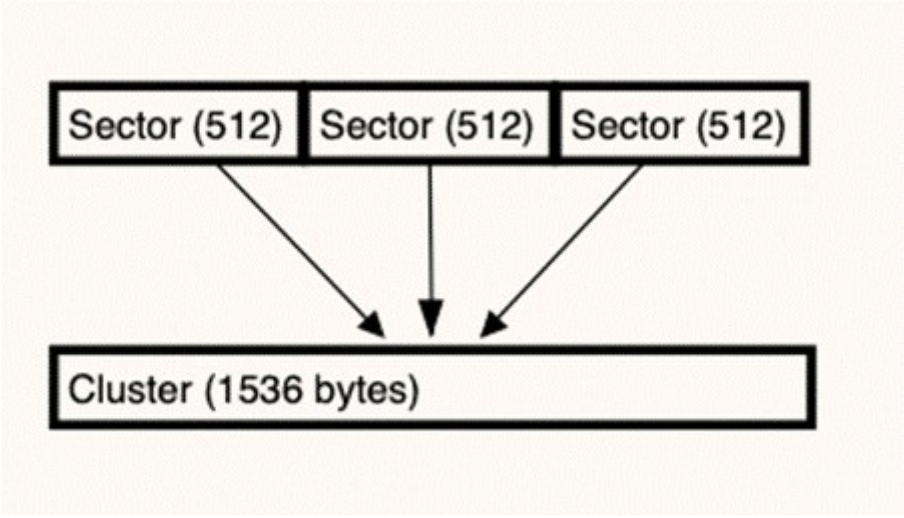
- Name ▲
 - Partition 1 [Basic data partition]
 - Partition 2 [EFI system partition]
 - Partition 3 [Microsoft reserved partition]
 - Partition 4 [Basic data partition]
- Partition gap
- Start sectors

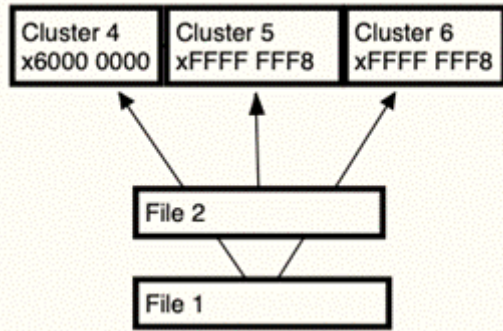
suspect (46,535)

- Partition 1 (92)
 - Path unknown (2)
 - DELL (8)
- Partition 2 (46,441)



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 00 00 00 02 00 00 00	01 00 06 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	40 B4 41 BB AA 55 CD 13	72 10 81 FB 55 AA 75 0A
F6 C1 01 74 05 FE 46 02	EB 2D 8A 56 40 B4 08 CD	13 73 05 B9 FF FF 8A F1	66 0F B6 C6 40 66 0F B6
D1 80 E2 3F F7 E2 86 CD	C0 ED 06 41 66 0F B7 C9	66 F7 E1 66 89 46 F8 83	7E 16 00 75 39 83 7E 2A
00 77 33 66 8B 46 1C 6E	83 C0 0C BB 00 80 B9 01	00 E8 2C 00 E9 A8 03 A1	F9 7D 80 C4 7C 8B F0 AC
84 C0 74 17 3C FF 74 09	B4 0E BB 07 00 CD 10 EB	EE A1 FA 7D EB E4 A1 7D	80 EB DF 98 CD 16 CD 19
66 60 80 7E 02 00 0F 84	20 00 66 6A 00 66 50 06	53 66 68 10 00 01 00 B4	42 8A 56 40 8B F4 CD 13
66 58 66 58 66 58 66 58	EB 33 66 3B 46 F8 72 03	F9 EB 2A 66 33 D2 66 0F	B7 4E 18 66 F7 F1 FE C2
8A CA 66 8B D0 66 C1 EA	10 F7 76 1A 86 D6 8A 56	40 8A E9 C0 E4 06 0A CC	B8 01 02 CD 13 66 61 0F
82 74 FF 81 C3 00 02 66	40 49 75 94 C3 42 4F 4F	54 4D 47 52 20 20 20 20	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 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 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
73 6B 20 65 72 72 6F 72	FF 0D 0A 50 72 65 73 73	20 61 6E 79 20 6B 65 79	20 74 6F 20 72 65 73 74
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	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	





E5 6C 00 6F 00 6E 00 67 00 66 00 0F 00 D4 69 00	l.o.n.g.f...01.
6C 00 65 00 6E 00 61 00 6D 00 00 00 65 00 2E 00	l.e.n.a.m.....
E5 4F 4E 47 46 49 7E 31 54 58 54 20 00 6B B0 6D	LONGFI-1TXT .k*m
D3 4E D3 4E 00 00 B1 6D D3 4E 00 00 00 00 00 00	ÓNÓN..tmÓN.....
E5 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 B1 6D D3 4E 00 00 00 00 00 00	ÓNÓN..tmÓN.....
42 74 00 78 00 74 00 00 00 FF FF 0F 00 D4 FF FF	St.x.t...yy..0yy
FF FF FF FF FF FF FF FF FF FF 00 00 FF FF FF FF	yyyyyyyyyy..yyyy
01 6C 00 6F 00 6E 00 67 00 66 00 0F 00 D4 69 00	l.o.n.g.f...01.
6C 00 65 00 6E 00 61 00 6D 00 00 00 65 00 2E 00	l.e.n.a.m.....
4C 4F 4E 47 46 49 7E 31 54 58 54 20 00 6B B0 6D	LONGFI-1TXT .k*m
D3 4E D3 4E 00 00 A8 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	SRECYCLEBIN..0pm
D3 4E D3 4E 00 00 B6 6D D3 4E 06 00 00 00 00 00	ÓNÓN..tmÓN.....
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

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 D3 4E 00 00 B6 6D D3 4E 06 00 00 00 00 00	ÓNÓN..tmÓN.....

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

42 74 00 78 00 74 00 00	00 FF FF 0F 00 D4 FF FF	Bt.x.t...yy..ôyy
FF FF FF FF FF FF FF FF	FF FF 00 00 FF FF FF FF	yyyyyyyyyy..yyyy
01 6C 00 6F 00 6E 00 67	00 66 00 0F 00 D4 69 00	.l.o.n.g.f...ôi.
6C 00 65 00 6E 00 61 00	6D 00 00 00 65 00 2E 00	l.e.n.a.m...e...
4C 4F 4E 47 46 49 7E 31	54 58 54 20 00 6B B0 6D	LONGFI~lTXT .k°m
D3 4E D3 4E 00 00 A8 6D	D3 4E 00 00 00 00 00 00	ÓNÓN...mÓN.....

E5 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	ÓNÓN...é^ÓN...'

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

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

EB 52 90	4E 54 46 53 20	20 20 20	00 02 08 00 00	00 NTFS
00 00 00 00 00	F0 00 00	3F 00 FF	00 80 00 00 00
00 00 00 00 80 80 00	FF 87 3F	00 00 00 00 00	00 00 00
AA A9 02 00 00 00 00	02 00 00	00 00 00 00 00	00 00 00	*B.....
F4 00 00 00 01 00 00 00	46 20 92	02 41 92 02 7C	
00 00 00 00	FA 33 C0 8E	D0 BC 00 7C	F8 68 C0 07
1F 1E 60 64 00 C8 88 16	0E 05 44 81 8E 03 00 4E		
54 46 53 75 15 B4 41 80	AA 55 CD 13 72 0C 81 F8		
55 AA 75 04 F7 C1 01 00	75 03 E9 00 00 1E 83 8C		
18 69 1A 00 B4 48 4A 16	0E 00 88 F4 14 1F CD 13		
9F 83 C4 18 9E 58 1F 72	81 38 04 08 00 75 D8 A3		
0F 00 C1 2E 0F 00 04 1E	5A 33 D8 B9 00 20 2B C0		
66 FF 06 11 00 03 16 0F	00 8E C2 FF 04 14 00 E8		
68 00 28 C8 77 EF 88 00	88 CD 1A 66 23 C0 75 20		
66 81 F8 54 43 50 41 75	24 81 89 02 01 72 18 16		
68 07 88 14 68 52 11 16	68 09 00 64 53 64 53 64		
55 16 14 14 68 89 01 46	41 0E 07 CD 1A 33 C0 B9		
0A 13 89 F6 0C FC F3 AA	89 8E 01 90 90 66 60 1E		
06 64 A1 11 00 66 03 04	1C 00 1E 66 68 00 00 00		
00 66 50 04 53 68 01 00	68 10 00 B4 42 8A 14 00		
05 14 1F 88 F4 CD 13 46	59 58 5A 66 59 64 59 1F		
0F 82 14 00 66 FF 06 11	00 03 16 0F 00 8E C2 FF		
0E 16 00 75 8C 07 1F 44	41 C3 A1 F4 01 E8 09 00		
A1 FA 01 88 03 00 F4 8B	FD 88 FD AC 3C 00 74 09		
84 0E 88 07 00 CD 10 8B	F2 C3 00 0A 41 20 64 69		
73 68 20 72 65 61 44 20	65 72 72 6F 72 20 6F 63		
63 75 72 72 65 64 00 00	0A 42 4F 4F 54 40 47 52		
20 69 73 20 63 6F 4D 70	72 65 73 73 65 64 00 00		
0A 50 72 65 73 73 20 43	74 72 6C 28 41 6C 74 28		
44 65 6C 20 74 6F 20 72	65 73 74 61 72 74 00 0A		
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	

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

46 49 4C 45	30 00 03 00	39 6B 20 00 00 00 00 00	FILE 0 . . 0k
01 00 01 00	39 00 01 00	D8 01 00 00 00 04 00 00 0
00 00 00 00 00 00 00 00	04 00 00 00 28 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	R
BB 0E D4 A1 6C 27 D5 01	E9 FC 2A E5 DF 26 D5 01		w.0;l'0.eu*88&0
58 0B C7 E9 DF 26 D5 01	BB 0E D4 A1 6C 27 D5 01		X.ç&8&0.w.0;l'0
20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00 00 00 00 08 01 00 00	00 00 00 00 00 00 00 00	
00 00 00 00 00 00 00 00	30 00 00 00 80 00 00 00	0
00 00 00 00 00 00 02 00	62 00 00 00 18 00 01 00	b
05 00 00 00 00 00 05 00	BB 0E D4 A1 6C 27 D5 01	w.0;l'0
BB 0E D4 A1 6C 27 D5 01	BB 0E D4 A1 6C 27 D5 01		w.0;l'0.w.0;l'0
BB 0E D4 A1 6C 27 D5 01	00 00 00 00 00 00 00 00		w.0;l'0
00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	
10 00 6C 00 6F 00 6E 00	67 00 66 00 69 00 6C 00		. . l . o . n . g . f . i . l .
65 00 6E 00 61 00 6D 00	65 00 2E 00 74 00 78 00		e . n . a . m . e . . t . x .
74 00 00 00 00 00 00 00	80 00 00 00 18 00 00 00		t
00 00 18 00 00 00 01 00	00 00 00 00 18 00 00 00	
80 00 00 00 A0 00 00 00	00 16 18 00 00 00 03 00	
53 00 00 00 48 00 00 00	63 00 6F 00 6D 00 2E 00		B . . . H . . . c . o . m . .
64 00 72 00 6F 00 70 00	62 00 6F 00 78 00 2E 00		d . r . o . p . b . o . x . . .
61 00 74 00 74 00 72 00	69 00 62 00 75 00 74 00		a . t . t . r . i . b . u . t .
65 00 73 00 00 00 00 00	78 9C AB 56 4A 29 CA 2F		w . s x . e . v . j . E /
48 CA AF 88 4F CB CC 49	CD 4C 89 CF C9 4F 4E CC		H E ~ . o E I I I L . I f o n I
51 B2 52 A8 56 CA 4D 4C	CE C8 CC 03 89 26 96 94		Q * R ~ V E M L I E I . . 4 . .
14 81 85 52 12 4B 12 81	0C 25 4F 83 82 82 AC 0A		. . . R . K . . . 40 . . . ~
F3 D0 1C A7 50 97 F4 8A	E2 74 67 93 FC 80 74 47		0 B . S P . o . A t g . d . t g
5B 5B A5 DA DA 5A 00 CB	B7 1C B0 00 00 00 00 00		[[V 0 0 z . E ' . *
FF FF FF FF	82 79 47 11 00 00 00 00 00 00 00 00		0 9 9 9 . y G

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

\$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	A repeatable attribute for both long and short file names. The long name of the file can be up to 255 Unicode characters. 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.
\$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.

03 00	00 00 00 00	00 00	10 00 00 00	60 00 00 00
00 00	00 00	00 00	48 00 00 00	18 00 00 00
BB 0E D4 A1 6C 27 D5 01	E9 FC 2A E5 DF 26 D5 01	BB 0E D4 A1 6C 27 D5 01	BB 0E D4 A1 6C 27 D5 01	BB 0E D4 A1 6C 27 D5 01
58 0B C7 E9 DF 26 D5 01	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
20 00 00 00 00 00 00 00	00 00 00 00 08 01 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	30 00 00 00 80 00 00 00			

Attribute \$10	03B	
Attribute type	03B	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

00 00 00 00 00 00 00 00	30 00 00 00	80 00 00 00
00 00 00 00 00 00 02 00	62 00 00 00	18 00 01 00
05 00 00 00 00 00 05 00	BB 0E D4 A1 6C 27 D5 01	BB 0E D4 A1 6C 27 D5 01
BB 0E D4 A1 6C 27 D5 01	BB 0E D4 A1 6C 27 D5 01	BB 0E D4 A1 6C 27 D5 01
BB 0E D4 A1 6C 27 D5 01	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00
10 00 6C 00 6F 00 6E 00	67 00 66 00 69 00 6C 00	67 00 66 00 69 00 6C 00
65 00 6E 00 61 00 6D 00	65 00 2E 00 74 00 78 00	65 00 2E 00 74 00 78 00
74 00	80 00 00 00 18 00 00 00	80 00 00 00 18 00 00 00
00 00 18 00 00 00 01 00	00 00 00 00 18 00 00 00	00 00 00 00 18 00 00 00

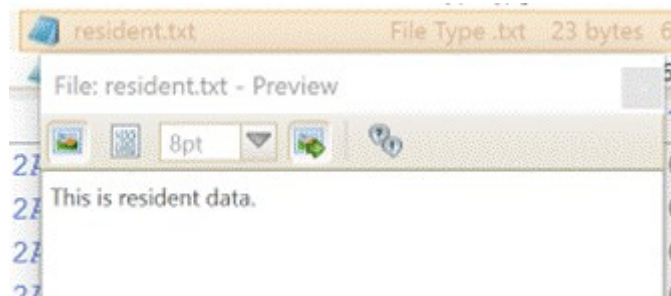
Attribute \$30	098	
Attribute type	098	0x30
Length (including header)	09C	128
Non-resident flag	0A0	0
Name length	0A1	0
Name offset	0A2	0x00
> Flags	0A4	00 00
Attribute ID	0A6	2
Length of the attribute	0A8	98
Offset to the attribute data	0AC	0x18
Indexed flag	0AE	1
Padding	0AF	0
▼ \$FILE_NAME	0B0	
Parent 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

```

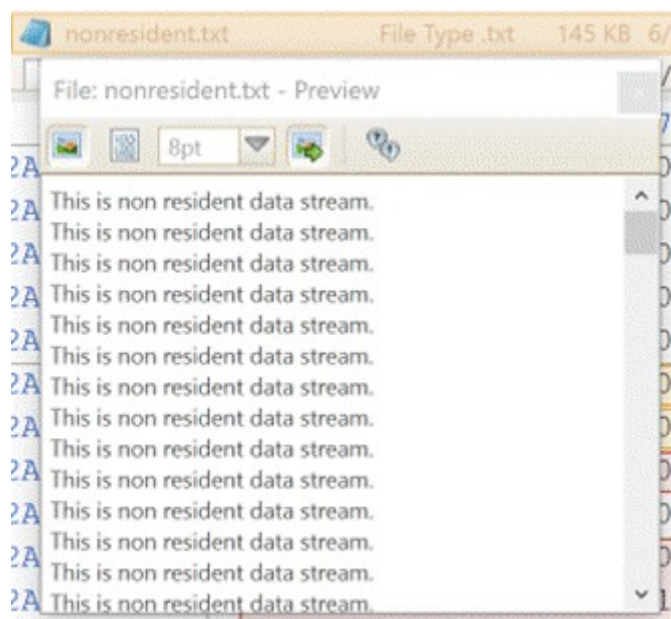
74 00 00 00 00 00 00 00 80 00 00 00 18 00 00 00
00 00 18 00 00 00 01 00 00 00 00 00 18 00 00 00
80 00 00 00 A0 00 00 00 00 16 18 00 00 00 03 00
53 00 00 00 48 00 00 00 63 00 6F 00 6D 00 2E 00
64 00 72 00 6F 00 70 00 62 00 6F 00 78 00 2E 00
61 00 74 00 74 00 72 00 69 00 62 00 75 00 74 00
65 00 73 00 00 00 00 00 78 9C AB 56 4A 29 CA 2F
48 CA AF 88 4F CB CC 49 CD 4C 89 CF C9 4F 4E CC
51 B2 52 A8 56 CA 4D 4C CE C8 CC 03 89 25 96 94
14 81 85 52 12 4B 12 81 0C 25 4F 83 82 82 AC 0A
F3 D0 1C A7 50 97 F4 8A E2 74 67 93 FC 80 74 47
5B 5B A5 DA DA 5A 00 CB B7 1C B0 00 00 00 00
FF FF FF FF 82 79 47 11 00 00 00 00 00 00 00

```

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

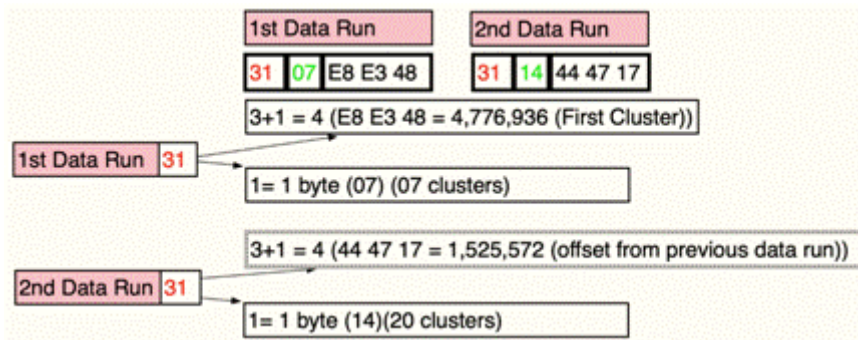


96 6A E0 D5 5E A7 04 37	80 00 00 00 30 00 00 00	.jàÔ^s.7.....0...
00 00 18 00 00 00 01 00	17 00 00 00 18 00 00 00
54 68 69 73 20 69 73 20	72 65 73 69 64 65 6E 74	This is resident
20 64 61 74 61 2E 20 00	80 00 00 00 A0 00 00 00	data.



96 6A E0 D5 5E A7 04 37	80 00 00 00 48 00 00 00	.jãŒ^s.7....H...
01 00 00 00 00 00 06 00	00 00 00 00 00 00 00 00
24 00 00 00 00 00 00 00	40 00 00 00 00 00 00 00	\$......@.....
00 50 02 00 00 00 00 00	30 43 02 00 00 00 00 00	.P.....0C.....
30 43 02 00 00 00 00 00	11 25 26 00 00 00 00 00	0C.....%&.....

80 00 00 00 50 00 00 00	01 00 00 00 00 00 04 00P.....
00 00 00 00 00 00 00 00	1A 00 00 00 00 00 00 00
40 00 00 00 00 00 00 00	00 B0 01 00 00 00 00 00	@.....°.....
00 B0 01 00 00 00 00 00	00 B0 01 00 00 00 00 00	.°.....°.....
31 07 E8 E3 48 31 14 44 47 17	00 00 00 00 00 00 00 00	l.ëãHl.DG.....
FF FF FF FF 82 79 47 11	00 00 00 00 00 00 00 00	ÿÿÿÿ.yG.....



Subject	RE: Please send me the information now
Date	07/20/2008 01:28:47 +0
Sender	Jean User <jean@m57.biz>
Recipients	luckgong@gmail.com
Attachments	ms1764.xls

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

Original Message
 From: alex@ms17.biz (mailto:luckgong@gmail.com)
 Date: Sunday, July 20, 2008 2:22 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

Alex

E-mail Header	
Date	20 Jul 2008 01:28:47 -0000
From	jean user <jean@m57.biz>
Sender	jean user <jean@m57.biz>
To	luckgong@gmail.com
Subject	RE: Please send me the information now
Importance	Normal
MIME-Version	1.0
Content-Type	multipart/mixed
Boundary	====_NextPart_07

```
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]
```

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

Command

modifier

source

destination

```
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]
```



```

***** 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/is_quarantine, sqlite/mac_document_versions,
        sqlite/mac_notes, sqlite/mackeeper_cache, sqlite/mac_knowledgec,
        sqlite/skype, syslog, utmpx, webhist, zsh_extended_history
webhist : binary_cookies, chrome_cache, chrome_preferences,
          esedb/msie_webcache, firefox_cache, java_idx, mslecf,
          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 : eft, 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, usnjrn, webhist, winfirewall, winjob, winreg
winxp : recycle_bin_info2, rplg, win_gen, winevt
winxp_slow : eft, winxp
-----

```

```

C:\tools\plaso>log2timeline C:\tools\plaso\export\files\jean.plaso C:\tools\plaso\image\jean.001
2019-08-07 11:25:34,830 [INFO] (MainProcess) PID:5324 <data_location> Determined data location: C:\tools\plaso\data
2019-08-07 11:25:34,848 [INFO] (MainProcess) PID:5324 <artifact_definitions> Determined artifact definitions path:
C:\tools\plaso\artifacts
Checking availability and versions of dependencies.
[OPTIONAL] missing: lz4.
[OK]

```

```

C:\tools\plaso>log2timeline -f filter_windows.txt C:\tools\plaso\export\files\jeanfilter.plaso C:\tools\plaso\image\jean.001
2019-07-19 15:19:35,018 [INFO] (MainProcess) PID:23288 <data_location> Determined data location: c:\tools\plaso\data
2019-07-19 15:19:35,034 [INFO] (MainProcess) PID:23288 <artifact_definitions> Determined artifact definitions path: c:\tools\plaso\artifacts
Checking availability and versions of dependencies.
[OPTIONAL] missing: lz4.
[OK]

```

```

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.

```



```
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]

Application to read, filter and process output from a plaso storage file.
```

```
***** 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]
-----
```

```
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.
```

E5	48	4F	52	54	20	20	20	54	58	54	20	18	6B	B0	6D	ã	H	O	R	T	.	k	°	m
D3	4E	D4	4E	00	00	E9	5E	D4	4E	08	00	27	00	00	00	Ó	Ô	..	é	Ô	..	'	...	

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

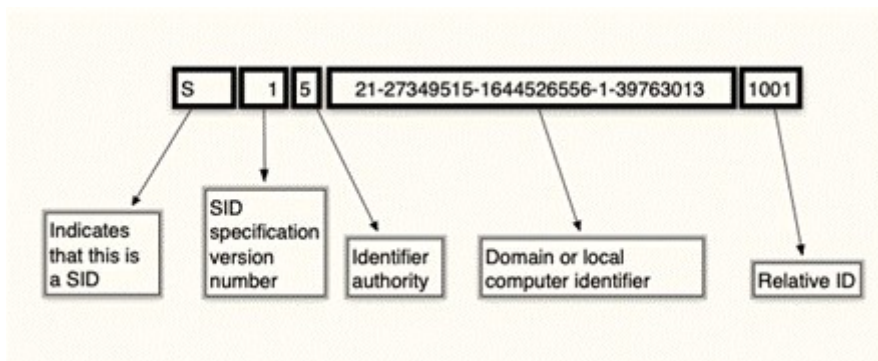
00 00 00 00 FF FF FF 0F 0B 00 00 00 0C 00 00 00
0D 00 00 00 0E 00 00 00 0F 00 00 00 10 00 00 00

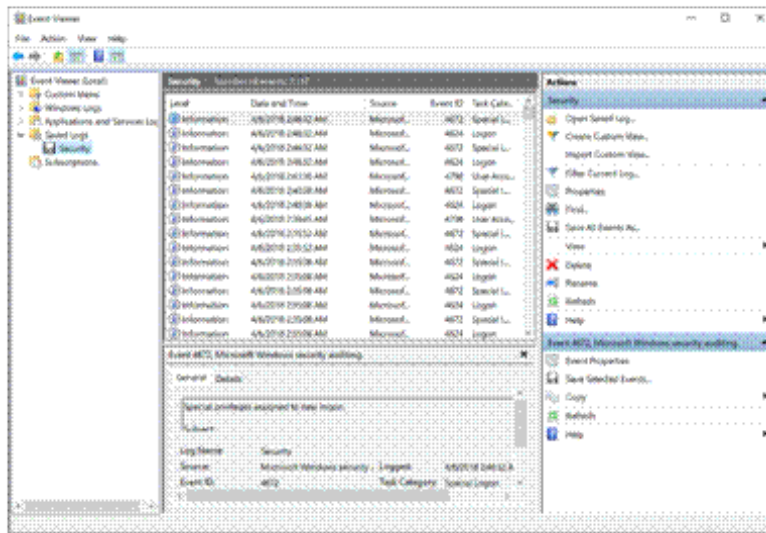
Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Del...	Data Record...
+	+	+	+	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
F	RegBinary	03-00-01-00-00-00-00-9A...	00-00-00-05	<input type="checkbox"/>	<input type="checkbox"/>
V	RegBinary	00-00-00-00-F4-00-00-03...	02-00-02-00-00-00-00-AA-85-55-DA-8D-77-23-F5-08...	<input type="checkbox"/>	<input type="checkbox"/>
ForcePasswordReset	RegBinary	00-00-00-00		<input type="checkbox"/>	<input type="checkbox"/>
UserPasswordHint	RegBinary	49-00-74-00-27-00-73-00-20...		<input type="checkbox"/>	<input type="checkbox"/>
UserTile	RegBinary	01-00-00-00-03-00-00-01...	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-...	<input type="checkbox"/>	<input type="checkbox"/>

```

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
  
```





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](#)

#	Filename	Cache Entry Offset	Cache Entry S...	Data Offset	Data Size	Data Checksum
1	14b707546180c86c.bmp	24 B	27 KB	114 B	27 KB	b52628b2db47c2e
2	52dd8d96f21652eb.bmp	27912 B	25 KB	28002 B	25 KB	c3d35385d1b84d6
3	ba5c26b5166d177b.bmp	53880 B	20 KB	53970 B	20 KB	b5a144c30061efe4
4	c0abe3d95a55451b.bmp	74856 B	23 KB	74946 B	23 KB	a08bfc0ec37da30e
5	402450273f879a7a.bmp	98904 B	27 KB	98994 B	27 KB	1741fc98681a75b2
6	9807ea9ded3b40d6.bmp	126792 B	26 KB	126882 B	26 KB	d272fe6b77c0d44f
7	77e0f5f51e9964d9.bmp	154296 B	14 KB	154386 B	14 KB	3e967a62194806c
8	965abebccc2bf227.bmp	169512 B	27 KB	169602 B	27 KB	b3c76ee3f1972eb
9	a02881907609c89.bmp	197400 B	20 KB	197486 B	20 KB	ce7266b0af7e59ec
10	e5a77305f8d0cad2.bmp	218376 B	25 KB	218466 B	25 KB	4639115948d8e50
11	9f6a3ca53f79c41a.bmp	244728 B	34 KB	244818 B	34 KB	739b09f296ef9590

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

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`

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

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

30.03.18 04:29:48	Visited: jcloudy@file:///C:/Users/jcloudy/Desktop/Larry%20Kng_%20Time%20to%20Repea%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

- S-1-5-21-2734969515-1644526556-1039763013-1001
- \$R23A30B
- \$RQAU6NQ
- \$RYRY5PT.jpg

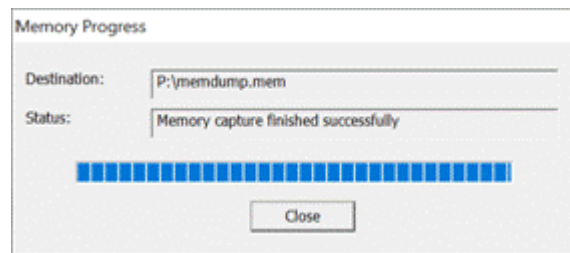
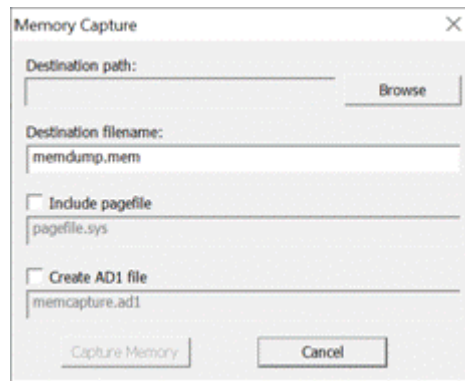
- Zuckerberg-Justin-SullivanGetty-Images-200x150.jpg
- zrt_lookup.html
- widget_iframe.4ed13d9ce94e60c41048ece32559b04c.html

- Recent (189)
- AutomaticDestinations (115)
- CustomDestinations (29)
- SendTo (7)
- Start Menu (32)

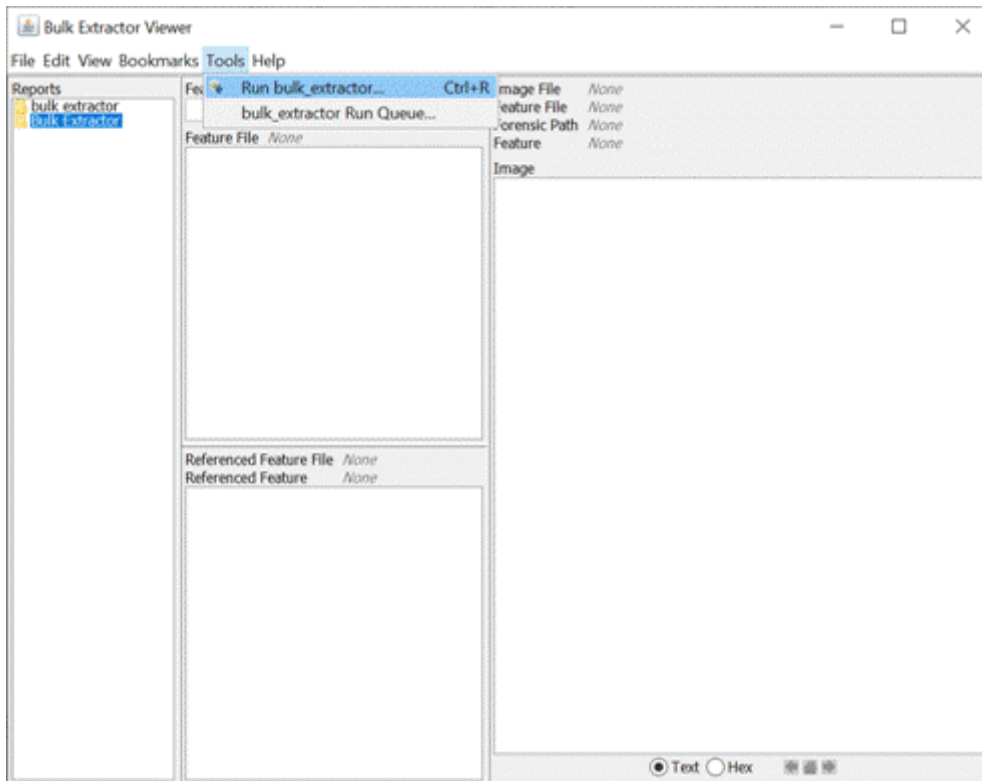
- 1b4dd67f29cb1962.automaticDestinations-ms
- 5d696d521de238c3.automaticDestinations-ms (7)
- 5f7b5f1e01b83767.automaticDestinations-ms (22)
- 7e4dca80246863e3.automaticDestinations-ms (2)
- 869150c3ec1167a.automaticDestinations-ms
- 9a165f62edbfa161.automaticDestinations-ms (1)

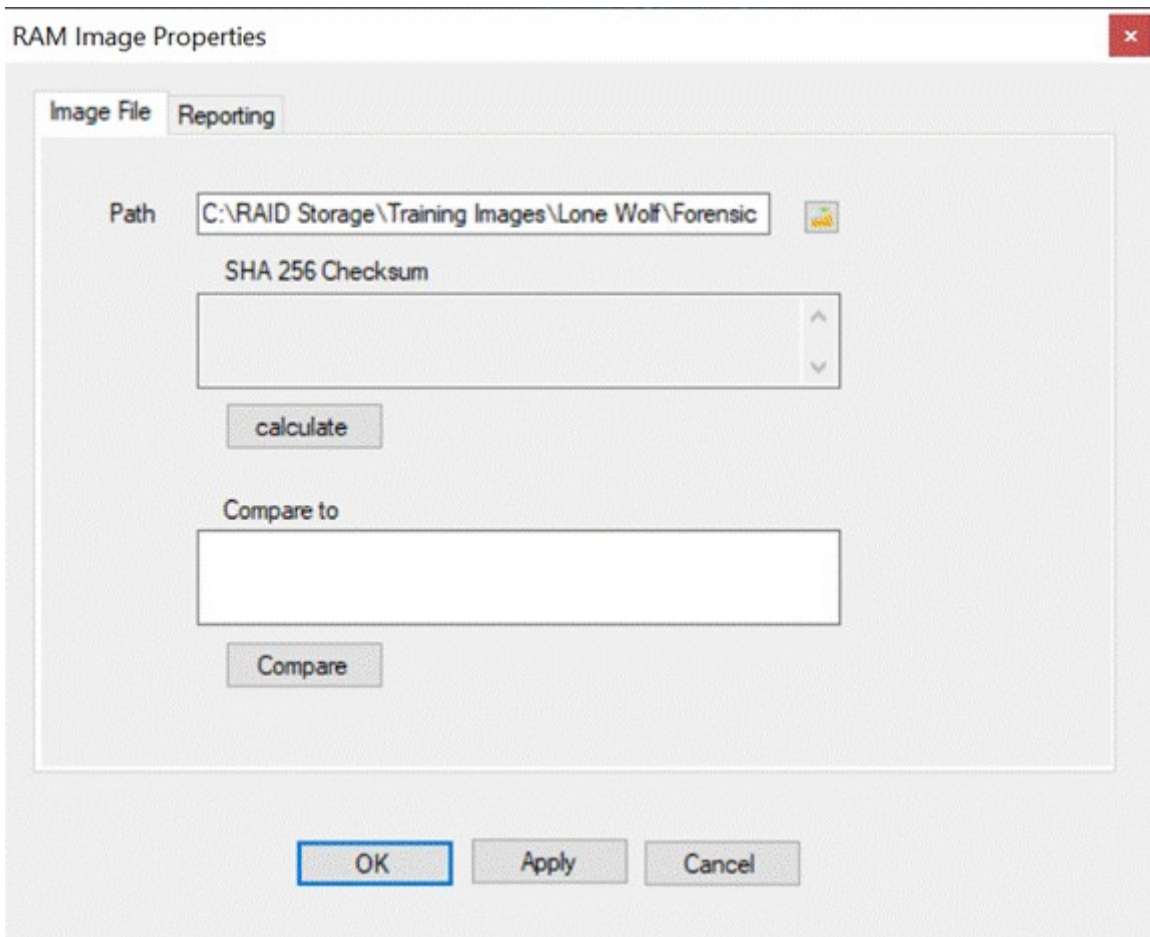
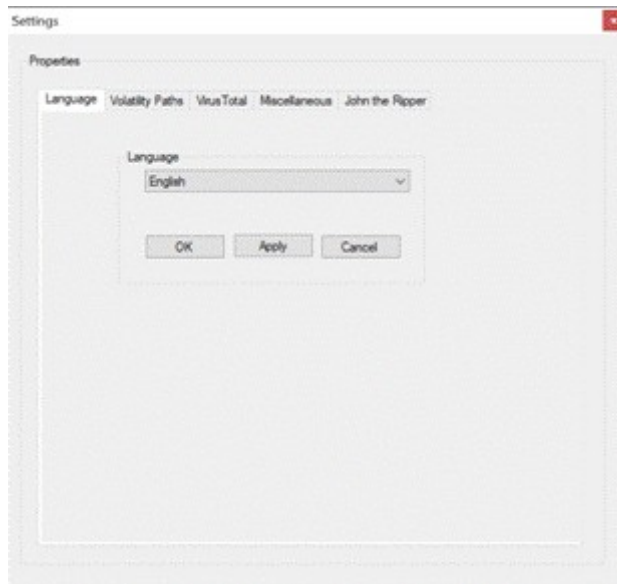


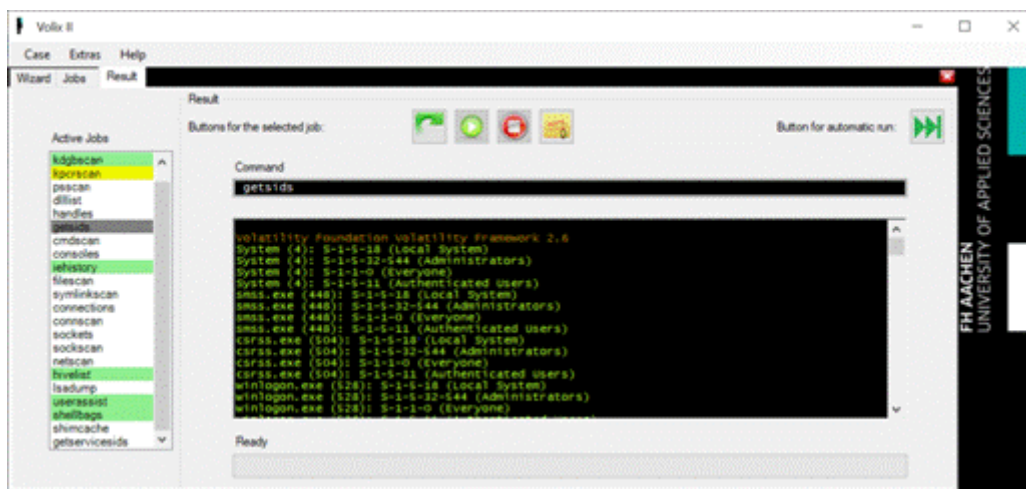
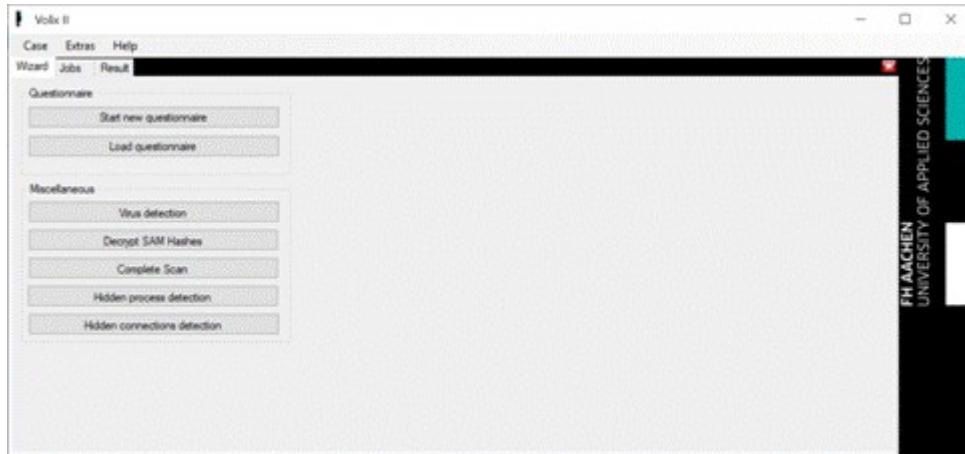
Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run ...	Last Run Time
SETUP.EXE-4919107...	4/6/2018 05:26	4/6/2018 05:26	25,000	SETUP.EXE	WOLLM014b3c9f14ba113-ae020801\PROGRAM FILES\AVIDA CORPORATION\INSTALLED\INSTALLCORE\SETUP.EXE	1	4/6/2018 05:26
SVOHOST.EXE-7030...	4/6/2018 05:48	4/6/2018 05:48	10,728	SVOHOST.EXE	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\SVOHOST.EXE	1	4/6/2018 05:48
SPEECHRUNTIME.E...	4/6/2018 05:48	4/6/2018 05:48	13,808	SPEECHRUNTIME...	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\SPEECH_ONECORE\COMMON\SPEECHRUNTIME.E...	1	4/6/2018 05:48
FTK IMAGER.EXE-437...	4/6/2018 05:41	4/6/2018 05:41	23,978	FTK IMAGER.EXE	WOLLM0300000000000000-407601\PROGRAMS\IMAGER_LITE_3.1.1\FTK IMAGER.EXE	1	4/6/2018 05:41
FTK IMAGER.EXE-060...	4/6/2018 05:40	4/6/2018 05:40	3,386	FTK IMAGER.EXE	WOLLM0300000000000000-407601\CPS 780 LONE WOLF SCENARIO\FTK IMAGER_4_2_P\FTK IMAGER\FTK IMAGER.EXE	1	4/6/2018 05:40
RUNDLL32.EXE-87CF...	4/6/2018 05:39	4/6/2018 05:39	4,382	RUNDLL32.EXE	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\RUNDLL32.EXE	1	4/6/2018 05:39
WMPRVSE.EXE-0C3A...	4/6/2018 05:35	4/6/2018 05:35	4,771	WMPRVSE.EXE	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\WMPRVSE.EXE	1	4/6/2018 05:35
SVOHOST.EXE-7339...	4/6/2018 05:35	4/6/2018 05:35	2,981	SVOHOST.EXE	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\SVOHOST.EXE	1	4/6/2018 05:35
SVOHOST.EXE-48719...	4/6/2018 05:35	4/6/2018 05:35	4,478	SVOHOST.EXE	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\SVOHOST.EXE	1	4/6/2018 05:35
EXCLE.EXE-621A4A8...	4/6/2018 05:27	4/6/2018 05:27	42,159	EXCLE.EXE	WOLLM014b3c9f14ba113-ae020801\PROGRAM FILES (X86)\MICROSOFT OFFICE\OFFICE16\EXCLE.EXE	1	4/6/2018 05:27
RUNDLL32.EXE-2521...	4/6/2018 05:26	4/6/2018 05:26	8,705	RUNDLL32.EXE	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\RUNDLL32.EXE	1	4/6/2018 05:26
RUNDLL32.EXE-0A4H...	4/6/2018 05:26	4/6/2018 05:26	6,410	RUNDLL32.EXE	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\RUNDLL32.EXE	1	4/6/2018 05:26
RUNDLL32.EXE-405L...	4/6/2018 05:26	4/6/2018 05:26	8,707	RUNDLL32.EXE	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\RUNDLL32.EXE	1	4/6/2018 05:26
RUNDLL32.EXE-FA42...	4/6/2018 05:26	4/6/2018 05:26	6,409	RUNDLL32.EXE	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\RUNDLL32.EXE	1	4/6/2018 05:26
RUNDLL32.EXE-880A...	4/6/2018 05:26	4/6/2018 05:26	8,705	RUNDLL32.EXE	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\RUNDLL32.EXE	1	4/6/2018 05:26
RUNDLL32.EXE-9C7B...	4/6/2018 05:26	4/6/2018 05:26	6,408	RUNDLL32.EXE	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\RUNDLL32.EXE	1	4/6/2018 05:26
DLHOST.EXE-488015...	4/6/2018 05:21	4/6/2018 05:21	10,312	DLHOST.EXE	WOLLM014b3c9f14ba113-ae020801\WINDOWS\SYSTEM32\DLHOST.EXE	1	4/6/2018 05:21



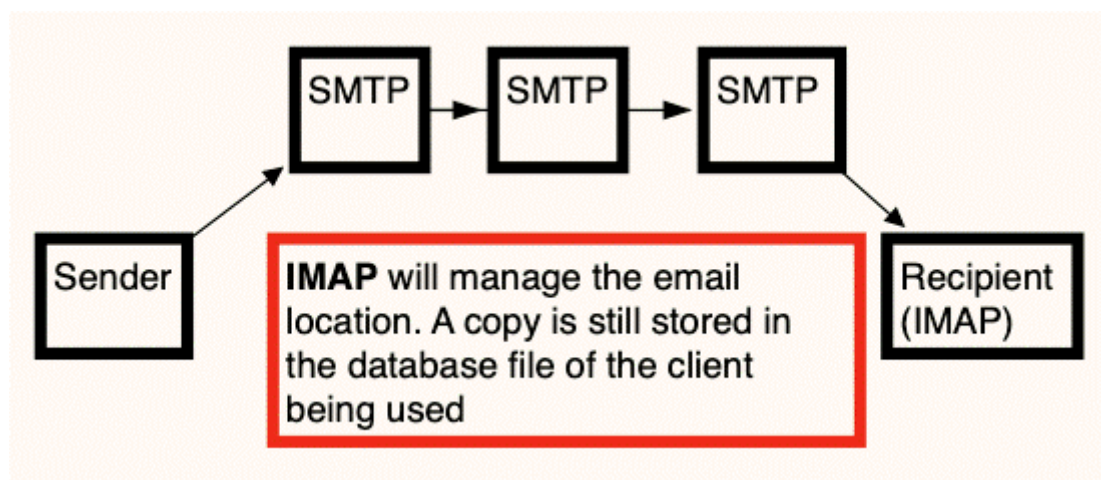
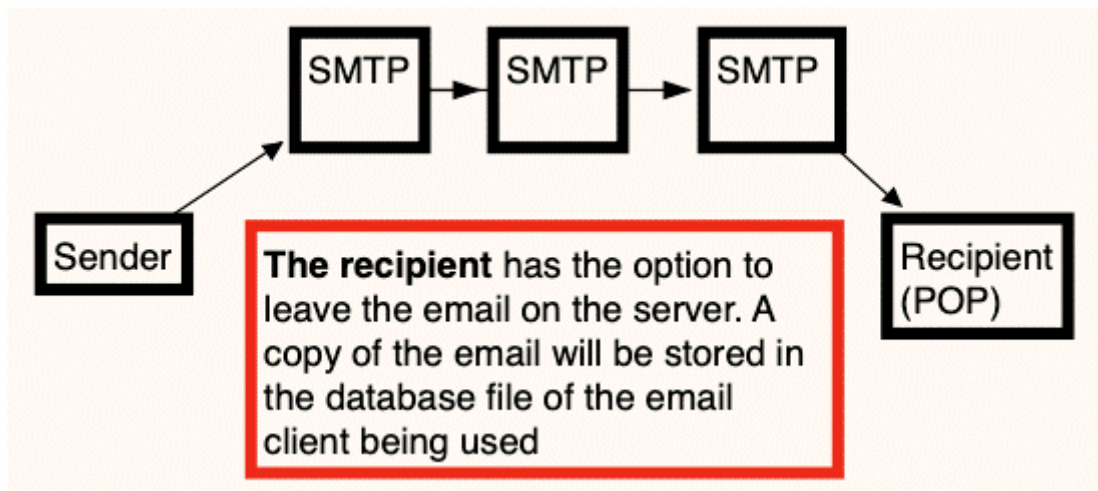
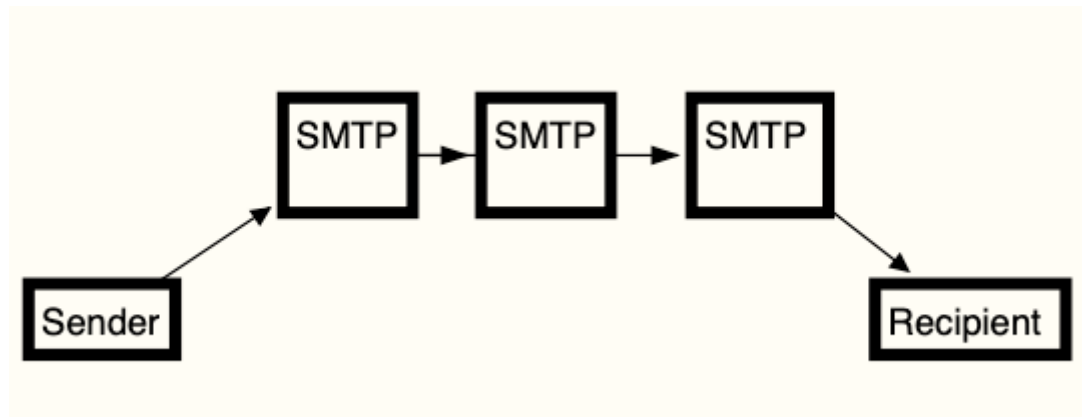
alerts.txt	Processing errors recorded in a text file.
ccn.txt	Processes Credit card numbers recorded in a text file.
ccn_track2.txt	Processes Credit card "track 2" information, which has been found in some bank card fraud cases recorded in a text file.
domain.txt	Processes Internet domains found on the 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.
rfe822.txt	Processes Email message headers including 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_*.txt	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.







Chapter 8: Email Forensics - Investigation Techniques



Chapter 9: Internet Artifacts

```
"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/"
},
,
```

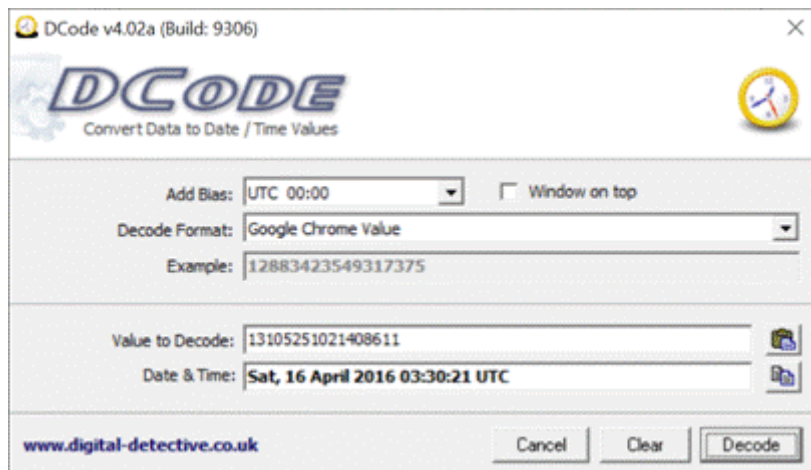
```
JSON
- checksum : d5686c72fcf309b5fa2e90a0bebc96ed
- roots
  - bookmark_bar
    - children
      - date_added : 13181512829205642
      - date_modified : 13210451812960795
      - id : 1
      - name : Bookmarks bar
      - type : folder
    - other
      - sync_transaction_version : 604
    - synced
  - version : 1
```

```
JSON
- checksum : d5686c72fcf309b5fa2e90a0bebc96ed
- roots
  - bookmark_bar
    - children
      - 0
      - 1
        - children
          - date_added : 13181512915741695
          - date_modified : 13211478457727677
          - id : 40
          - name : News
          - sync_transaction_version : 1
          - type : folder
```



```

JSON
- checksum : d5686c72fcf309b5fa2e90a0bebc96ed
- roots
  - bookmark_bar
    - children
      - 0
      - 1
        - children
          - 0
            - date_added : 13105251021405925
            - id : 110
            - meta_info
              - name : BBC News
              - sync_transaction_version : 592
            - type : url
            - url : http://news.bbc.co.uk/
  
```



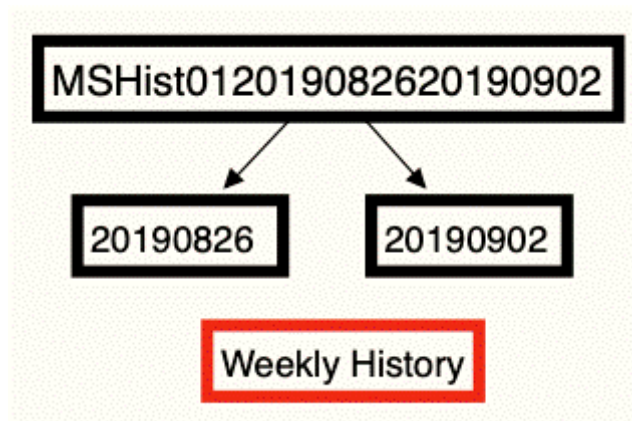
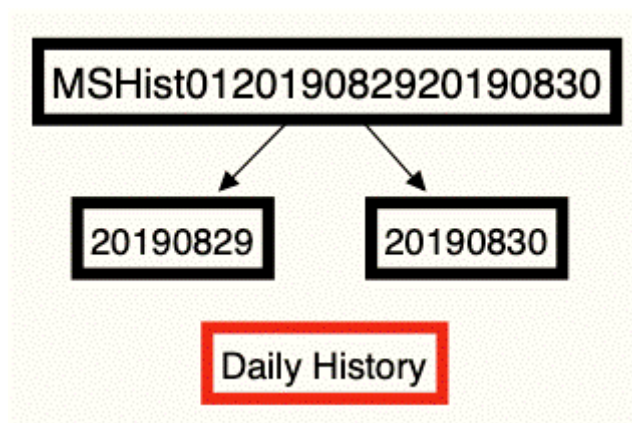
creation_utc	host_key	name	value	path	expires_utc	is_secure	is_httponly	last_access_utc	has_expires	is_pe
13211504229653934	.google.com	_ga		/gmail/about	13274576231000000	0	0	13211504229653934	1	1
13211504229654926	.google.com	_gid		/gmail/about	13211590631000000	0	0	13211504229654926	1	1
13211504361869670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

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	8/27/2021 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

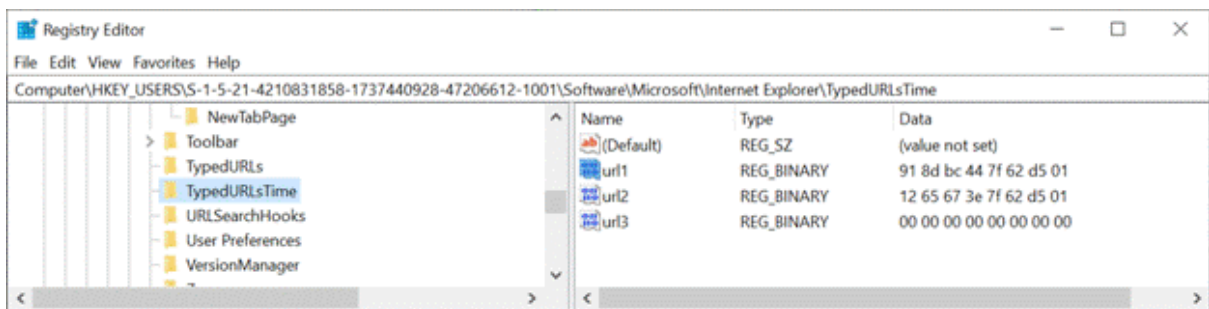
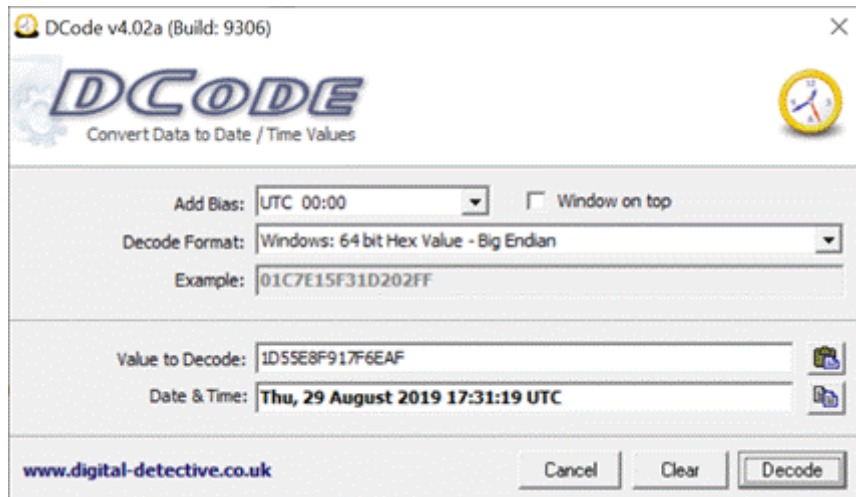
Icon	Host Name	Path	Name	Value	Expires	Secure	HTTP Only	Last Access...	Created On	Expires
gmail.html	https://www.google...	text/html	0	8/28/2019 15:17	8/28/2019 15:17		HTTP/1.1 302		private	172.217.14.100
s2	https://www.google...	text/javascript	14,685	8/28/2019 15:17	8/27/2019 14:47	8/27/2019 14:27	8/28/2020 14:47	8/28/2019 15:17	public, max-age=31536000	172.217.14.100
about.html	https://mail.google...	text/html	0	8/28/2019 15:17	8/27/2019 21:40	8/28/2019 21:40	8/28/2019 21:40	8/28/2019 15:17	public, max-age=86400	172.217.11.165
about.html	https://www.google...	text/html	0	8/28/2019 15:17	8/28/2019 04:21	8/28/2019 04:21	8/28/2019 15:17	8/28/2019 15:17	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	8/28/2019 15:17	private, max-age=3000	172.217.14.100

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

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\History\History.IE5\
4	132119207924265464	History	C:\Users\IEUser\AppData\Local\Microsoft\Windows\History\History.IE5\
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.IE5\MSHist012019082820190829\
13	132115041147334574	iedownload	C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\
14	132119207959762526	MSHist012019082920190830	C:\Users\IEUser\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012019082920190830\
15	132119207959762526	MSHist012019082620190902	C:\Users\IEUser\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012019082620190902\
16	132119207959954922	MSHist012019090220190903	C:\Users\IEUser\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012019090220190903\



EntryId	SyncTime	ExpiryTime	ModifiedTime	AccessedTime	Url
1	132115734791679663	132138198789360361	132115482789355131	132115734791679663	:2019082920190830: IEUser@file:///C:/Program%20Files/Windows%20Mail/MSOERES.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



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	http://static-global-s-msn-com.akamaized.net/...	9/2/2019 11:23	9/2/2019 04:57	9/7/2019 04:56
AAesHLQ[1].png	image/png	http://static-global-s-msn-com.akamaized.net/...	9/2/2019 11:23	8/30/2019 00:28	9/4/2019 00:28
AAGHCg4[1].jpg	image/jpeg	http://static-global-s-msn-com.akamaized.net/...	9/2/2019 11:23	9/2/2019 10:27	9/7/2019 10:27

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\

EntryId	AccessCount	SyncTime	CreationTime	ExpiryTime	ModifiedTime	AccessedTime	Url	Filename
36	18	132119208683123513	132119208683098265	132435432680000000	132119208683098265	132119208683123513	Cookieieuser@yahoo.com/	IF0DA7EK.txt
41	2	132115040834588257	132115040834204478	132452000840000000	132115040834204478	132119208375537727	Cookieieuser/www2.bing.com/	QZVGRJVN.txt
21	17	132119208820850307	132119208820850307	132460487960000000	132119208820850307	132119222099087060	Cookieieuser/www.msn.com/	Q01C9WT2.txt
47	3	132115044434921485	132115044434921485	132115908430000000	132115044434921485	132115044436696825	Cookieieuser/www.mozilla.org/	YP2ZL4QD.txt
45	4	132115040938396120	132115040938396120	132192800940000000	132115040938396120	132119208561572465	Cookieieuser/www.google.com/	U095J589.txt
88	1	132119208810386393	132119208810378061	132750792850000000	132119208810378061	132119208810386393	Cookieieuser/www.bing.com/images	6MC65DME.txt
38	6	132115040768554247	132115040768554247	132452000760000000	132115040768554247	132119222095615988	Cookieieuser/www.bing.com/	IT9CA013.txt
60	20	132119208680379897	132119208680379897	133696008670000000	132119208680379897	132119208686590905	Cookieieuser/www.aks.org/	OW6YLVUJ.txt
24	8	132119208661351321	132119208661342905	132461352650000000	132119208661342905	132119208661351321	Cookieieuser/w55c.net/	XTF8XNVC.txt
50	1	132119208020635033	132119208020550601	132434568060000000	132119208020550601	132119208020635033	Cookieieuser/tpixel.com/	QLCX0XOB.txt

MZHistoryView - C:\RAID Storage\VMUE11.Win7.VirtualBox\Windows 7 VM\MSEdge - Win10-disk001_27, PTUsers\UEUser\AppData\Roaming\Microsoft\Edge\History

URL	First Visit Date	Last Visit Date	Visit Count	Referrer
https://www.google.com/search?client=firefox-b-d&ei=3-FuQZyHh5S-w5...	N / A	9/3/2019 14:54	1	https://www.google.co...
https://www.google.com/search?client=firefox-b-d&ei=L-FuXY7i96Z-g5...	N / A	9/3/2019 14:54	1	https://www.google.co...
https://www.google.com/search?client=firefox-b-d&q=bad+guy+loving	N / A	9/3/2019 14:53	1	
https://www.mozilla.org/en-US/privacy/firefox/	N / A	9/3/2019 14:53	1	https://www.mozilla.org...
https://www.mozilla.org/privacy/firefox/	N / A	9/3/2019 14:53	1	

5 item(s) NirSoft Freeware, http://www.nirsoft.net

Properties

URL:

First Visit Date:

Last Visit Date:

Visit Count:

Referrer:

Host Name:

Title:

Record Index:

Visit Type:

Frequency:

URL Length:

OK

PasswordFox - C:\RAID Storage\VMUE11.Win7.VirtualBox\Windows 7 VM\MSEdge - Win10-disk001_29, PTUsers\UEUser\AppData\Roaming\Mozilla\Firefox\Profile\...\passwords

Record	Web Site	User Name	Password	User Name Field	Password Field	Signons File
1	https://accounts.google.com	badguyneedslove@gma...	[REDACTED]	identifier	password	logins.json

1 item(s), 1 Selected NirSoft Freeware, http://www.nirsoft.net

Properties

Record Index: 1

Web Site: https://accounts.google.com

User Name: badguyneedslove@gmail.com

Password: b[REDACTED]

User Name Field: identifier

Password Field: password

Signons File: logins.json

HTTP Realm:

Password Strength: Strong

Firefox Version: 32+

Created Time: 9/4/2019 10:23

Last Time Used: 9/4/2019 10:23

Password Change Time: 9/4/2019 10:23

Password Use Count: 1

OK

Favorite/New Mozilla - C:\AAD Storage\VM\1186\1\VirtualBox\Windows 7 VM\86756af-4506-4b74-a864-8b761209d31_P1\user@User...

File Edit View Help







Title	URL	Created Date	Modified Date	Last Visited	Folder Name
☐ About Us	https://www.mozilla.org/en-US/about/	8/28/2019 22:21	8/28/2019 22:21	N/A	Mozilla Firefox
☐ Customize Firefox	https://support.mozilla.org/en-US/kb/customize-firefox	8/28/2019 22:21	8/28/2019 22:21	N/A	Mozilla Firefox
☐ Get Involved	https://www.mozilla.org/en-US/contribute/	8/28/2019 22:21	8/28/2019 22:21	N/A	Mozilla Firefox
☐ Help and Tutorials	https://support.mozilla.org/en-US/products/firefox	8/28/2019 22:21	8/28/2019 22:21	N/A	Mozilla Firefox
☐ Getting Started	https://www.mozilla.org/en-US/firefox/central/	8/28/2019 22:21	8/28/2019 22:21	N/A	toolbar
☐ bad boys - Google Search	https://www.google.com/search?client=firefox-b-d...	8/31/2019 03:05	8/31/2019 03:05	N/A	unfiled
☐ Will Smith & Martin Lawrence Conf...	https://www.youtube.com/watch?v=bad-boys-for-life...	8/31/2019 03:05	8/31/2019 03:05	N/A	unfiled
☐ Inner Circle: Bad Boys - YouTube	https://www.youtube.com/watch?v=onT009Vyk...	8/31/2019 03:06	8/31/2019 03:06	N/A	unfiled





8 items

https://www.facebook.com/badguy27



Bulk Extractor	Histogram File	url_facebook-id.txt
• alerts.txt	n=12	1398069580413568
• ccn.txt	n=12	1819946191667827
• ccn_histogram.txt	n=7	296280873867140
• domain.txt	n=5	990491837629352
• domain_histogram.txt	n=2	1243316582352556
• elf.txt	n=1	1661729067442897
• email.txt	n=1	1835684153362700
• email_domain_histogram.txt	n=1	282409338764678
• email_histogram.txt	n=1	307729452976042
• ether.txt	n=1	382649952068500
• ether_histogram.txt	n=1	520255291469580
• exif.txt	n=1	658500157678938
• hex.txt		
• jpeg_carved.txt		
• json.txt		
• rfc822.txt		
• sqlite_carved.txt		

 CollectionPath	REG_SZ	C:\Users\IEUser\AppData\Roaming\Shareaza\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

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