M Square Consulting, LLC

Michael De La Cruz

Marielen Montalvo

Internal Training Notes
Computer Forensics

20191030

MFT Collection from a Live System

https://github.com/jschicht/RawCopy

```
C:\Users\mdelacruz\Desktop\Collections\RawCopy-master>RawCopy.exe /FileNamePath:C:0 /OutputName:MFT_C.bin
```

```
C:\Users\mdelacruz\Desktop\Collections\RawCopy-master\RawCopy.exe
RawCopy v1.0.0.21

Writing: MFT_C.bin
```

MFT_C.bin 12/4/2018 4:54 PM BIN File 765,952 KB

Parsing the MFT file

https://binaryforay.blogspot.com/2018/06/introducing-mftecmd.html

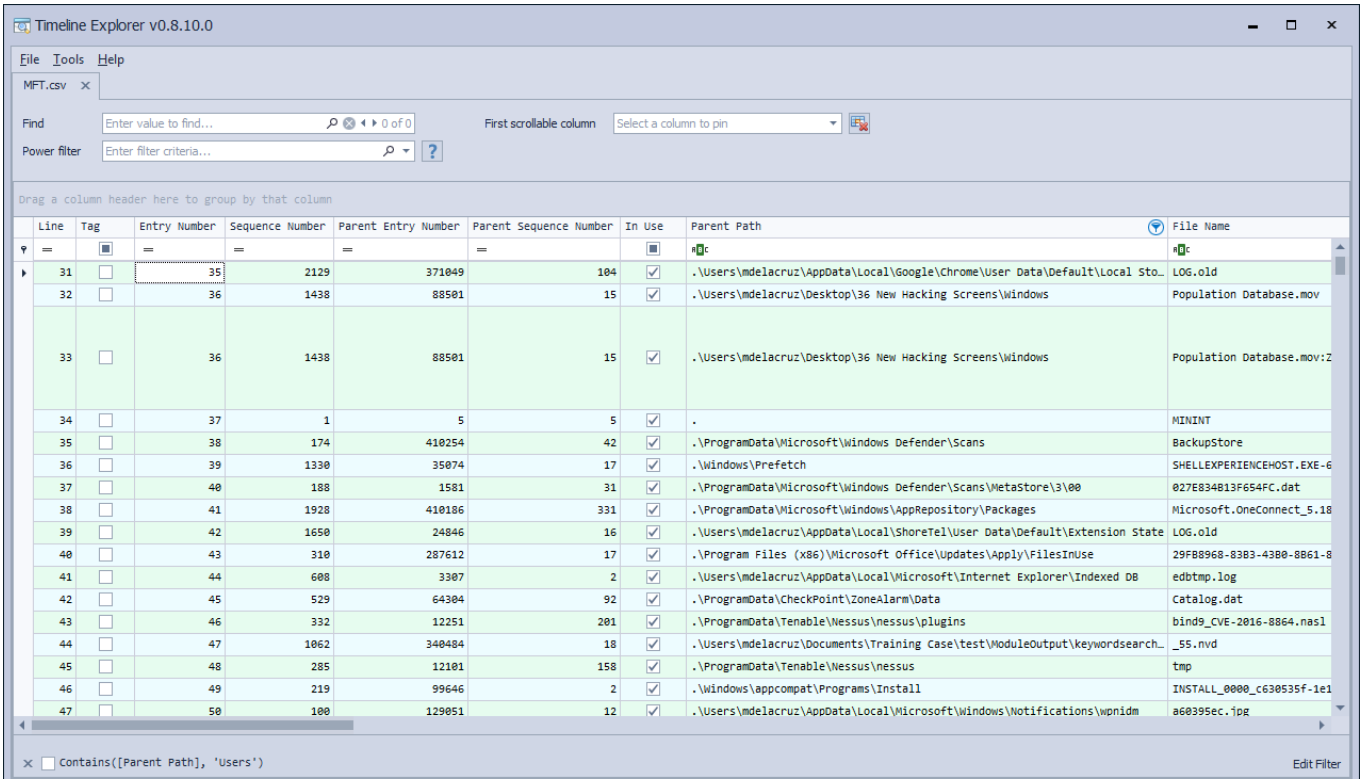
MFTECmd.exe -f "C:\Users\mdelacruz\Desktop\Collections\MFT_C.bin" --csv "C:\Users\mdelacruz\Desktop\Collections" --bn MFT.csv

```
C:\Users\mdelacruz\Desktop\Collections>MFTECmd.exe -f "C:\Users\mdelacruz\Desktop\Collections\MFT_C.bin" --csv "C:\Users\mdelacruz\Desktop\Collections" --bn MFT.csv
MFTECmd version 0.3.3.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f C:\Users\mdelacruz\Desktop\Collections\MFT_C.bin --csv C:\Users\mdelacruz\Desktop\Collections --bn MFT.csv


Processed 'C:\Users\mdelacruz\Desktop\Collections\MFT_C.bin' in 38.7406 seconds

CSV output will be saved to 'C:\Users\mdelacruz\Desktop\Collections\MFT.csv'
```

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD
1	EntryNumber	Sequenc	InUse	ParentEr	ParentSe	ParentPath	FileName	Extensior	FileSize	Referenc	Reparse	IsDirecto	HasAds	IsAds	SI<FN	uSecZer	Copied	SiFlags	NameTyp	CreatedC	CreatedC	LastModi	LastModi	LastRecc	LastRecc	LastAcce	LastAcce	UpdateS	LogfileSe	Securityl
2	0	1	TRUE	5	5	.	$MFT		8E+08	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	5E+10	256
3	1	1	TRUE	5	5	.	$MFTMir		4096	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	3E+07	256
4	2	2	TRUE	5	5	.	$LogFile		7E+07	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	3E+07	256
5	3	3	TRUE	5	5	.	$Volume		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	3E+07	257
6	4	4	TRUE	5	5	.	$AttrDef		2560	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	4E+10	0
7	5	5	TRUE	5	5	.	.		0	1		TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	Hidden\S	DosWind	04:24.6	03:28.0	25:18.6	03:28.0	25:18.6	03:28.0	25:18.6	03:28.0	2E+10	5E+10	7252
8	6	6	TRUE	5	5	.	$Bitmap		3E+07	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	2E+09	256
9	7	7	TRUE	5	5	.	$Boot		8192	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	0	0
10	8	8	TRUE	5	5	.	$BadClus		0	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	1E+09	256
11	8	8	TRUE	5	5	.	$BadClus:$Bad		5E+11	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	1E+09	256
12	9	9	TRUE	5	5	.	$Secure		2E+07	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	4E+10	257
13	9	9	TRUE	5	5	.	$Secure:$SDS		2E+07	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	4E+10	257
14	10	10	TRUE	5	5	.	$UpCase		131072	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	4E+10	256
15	10	10	TRUE	5	5	.	$UpCase:$Info		32	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	4E+10	256
16	11	11	TRUE	5	5	.	$Extend		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	DosWind	03:28.0		03:28.0		03:28.0		03:28.0		0	2E+08	257
17	24	1	TRUE	11	11	.\$Extend	$Quota		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	Posix	03:32.3		03:32.3		03:32.3		03:32.3		0	3E+07	257
18	25	1	TRUE	11	11	.\$Extend	$ObjId		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	Posix	03:32.3		03:32.3		03:32.3		03:32.3		0	5E+10	257
19	26	1	TRUE	11	11	.\$Extend	$Reparse		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	Posix	03:32.3		03:32.3		03:32.3		27:06.1	03:32.3	0	5E+10	257
20	27	1	TRUE	11	11	.\$Extend	$RmMetadata		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	Posix	03:32.3		03:32.3		03:32.3		03:32.3		0	3E+07	258
21	28	1	TRUE	27	1	.\$Extend\$RmMetadata	$Repair		0	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden\S	Posix	03:32.3		03:32.3		03:32.3		03:32.3		0	3E+09	257
22	28	1	TRUE	27	1	.\$Extend\$RmMetadata	$Repair:$Config		8	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden\S	Posix	03:32.3		03:32.3		03:32.3		03:32.3		0	3E+09	257
23	28	1	TRUE	27	1	.\$Extend\$RmMetadata	$Repair:$Corrupt		8E+07	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden\S	Posix	03:32.3		03:32.3		03:32.3		03:32.3		0	3E+09	257
24	28	1	TRUE	27	1	.\$Extend\$RmMetadata	$Repair:$Verify		1E+07	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden\S	Posix	03:32.3		03:32.3		03:32.3		03:32.3		0	3E+09	257
25	29	1	TRUE	27	1	.\$Extend\$RmMetadata	$TxfLog		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden\S	Posix	03:32.3		53:56.0	03:32.3	53:56.0	03:32.3	53:56.0	03:32.3	0	4E+10	258
26	30	1	TRUE	27	1	.\$Extend\$RmMetadata	$Txf		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	-2E+09	Posix	03:32.3		12:23.8	03:32.3	12:23.8	03:32.3	12:23.8	03:32.3	0	5E+10	258
27	31	1	TRUE	29	1	.\$Extend\$RmMetadata\$TxfLog	$Tops		100	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden\S	Posix	03:32.3		03:32.3		03:32.3		03:32.3		0	5E+10	258
28	31	1	TRUE	29	1	.\$Extend\$RmMetadata\$TxfLog	$Tops:$T		1E+06	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden\S	Posix	03:32.3		03:32.3		03:32.3		03:32.3		0	5E+10	258
29	32	1	TRUE	29	1	.\$Extend\$RmMetadata\$TxfLog	$TxfLog:$I		65536	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	Posix	03:32.3		11:44.4	03:32.3	11:44.4	03:32.3	27:15.5	03:32.3	2E+10	5E+10	259
30	33	1	TRUE	29	1	.\$Extend\$RmMetadata\$TxfLog	$TxfLogContainer(		1E+07	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	Posix	03:32.3		42:55.9	03:32.3	42:55.9	03:32.3	03:32.3		0	4E+10	260
31	34	576	TRUE	16024	67	.\ProgramData\Tenable\Nessus\nessus\backups	global-2(.db		319464	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive\H	Windows	15:24.8		55:33.8	55:33.8	55:33.8	55:33.8	55:33.8		2E+10	4E+10	6986
32	35	2129	TRUE	371049	104	.\Users\mdelacruz\AppData\Local\Google\Chrome\User Data\De	LOG.old	.old	187	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	DosWind	04:08.2		02:31.8		13:55.6	13:55.6	02:24.5		2E+10	5E+10	3182
33	36	1438	TRUE	88501	15	.\Users\mdelacruz\Desktop\36 New Hacking Screens\Windows	Populatic	.mov	6E+07	1		FALSE	TRUE	FALSE	TRUE	TRUE	TRUE	Archive	Windows	35:00.0	59:10.7	59:12.6	59:10.7	54:32.6	59:10.7	35:00.0	59:10.7	1E+10	5E+09	3988
34	36	1438	TRUE	88501	15	.\Users\mdelacruz\Desktop\36 New Hacking Screens\Windows	Populatic	Identifier	114	1		FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	Archive	Windows	35:00.0	59:10.7	59:12.6	59:10.7	54:32.6	59:10.7	35:00.0	59:10.7	1E+10	5E+09	3988
35	37	1	TRUE	5	5	.	MINNT		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	0	Posix	03:34.0		55:13.5	03:34.0	22:04.5	03:34.0	47:27.8	03:34.0	7E+09	3E+10	7240

MFT Timeline Explorer

https://ericzimmerman.github.io/Software/TimelineExplorer.zip



Extracting the SAM file from a live system

Locate the MFT Entry number for the SAM file

455331	5	TRUE	414678	66	.\Windows\System32\config	SAM{8ebe .regtrans-
455332	5	TRUE	415852	10	.\Windows\System32\SMI\Store\Machine	SCHEMA.D .regtrans-
455333	5	TRUE	414678	66	.\Windows\System32\config	SECURITY{ .regtrans-
455334	5	TRUE	414678	66	.\Windows\System32\config	SOFTWAR .regtrans-
455335	5	TRUE	414678	66	.\Windows\System32\config	SYSTEM{a .regtrans-
455336	5	TRUE	414678	66	.\Windows\System32\config	SAM
455337	5	TRUE	414678	66	.\Windows\System32\config	SECURITY
455338	5	TRUE	414678	66	.\Windows\System32\config	SOFTWARE
455339	5	TRUE	414678	66	.\Windows\System32\config	SYSTEM

RawCopy.exe /FileNamePath:C:455336 /OutputName:SAM

```
C:\Users\mdelacruz\Desktop\Collections\RawCopy-master>RawCopy.exe /FileNamePath:C:455336 /OutputName:SAM
```

SAM 12/4/2018 5:11 PM File 72 KB

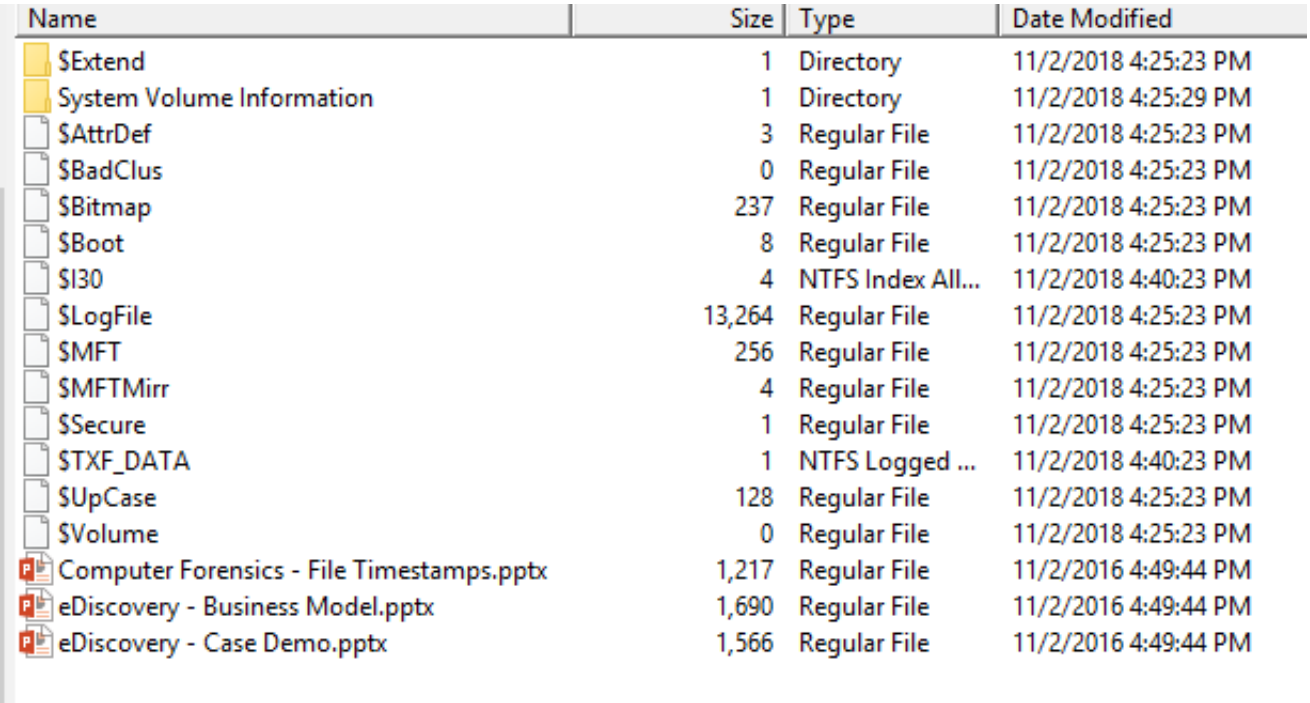
Hard disk 1 | SAM

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	72	65	67	66	4A	00	00	00	4A	00	00	00	9A	43	0F	0A	regfJ J šC
00000016	83	F7	D3	01	01	00	00	00	05	00	00	00	00	00	00	00	ƒ÷Ó
00000032	01	00	00	00	20	00	00	00	00	C0	00	00	01	00	00	00	À
00000048	5C	00	53	00	79	00	73	00	74	00	65	00	6D	00	52	00	\ S y s t e m R
00000064	6F	00	6F	00	74	00	5C	00	53	00	79	00	73	00	74	00	o o t \ S y s t
00000080	65	00	6D	00	33	00	32	00	5C	00	43	00	6F	00	6E	00	e m 3 2 \ C o n
00000096	66	00	69	00	67	00	5C	00	53	00	41	00	4D	00	00	00	f i g \ S A M
00000112	3B	4F	85	43	76	63	E8	11	8A	63	C2	7E	94	1C	1A	1A	;O…Cvcè ŠcÂ~”
00000128	3B	4F	85	43	76	63	E8	11	8A	63	C2	7E	94	1C	1A	1A	;O…Cvcè ŠcÂ~”
00000144	00	00	00	00	3C	4F	85	43	76	63	E8	11	8A	63	C2	7E	<O…Cvcè ŠcÂ~
00000160	94	1C	1A	1A	72	6D	74	6D	22	44	FF	51	70	86	D4	01	” rmtm"DÿQp†Ô
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Your client suspects important files were downloaded to a USB drive in 2016.

On 11/1 you request the forensic image of that USB drive.

You receive the following forensic image on 11/3 and begin to review it in FTK.



Name	Size	Type	Date Modified
$Extend	1	Directory	11/2/2018 4:25:23 PM
System Volume Information	1	Directory	11/2/2018 4:25:29 PM
$AttrDef	3	Regular File	11/2/2018 4:25:23 PM
$BadClus	0	Regular File	11/2/2018 4:25:23 PM
$Bitmap	237	Regular File	11/2/2018 4:25:23 PM
$Boot	8	Regular File	11/2/2018 4:25:23 PM
$I30	4	NTFS Index All...	11/2/2018 4:40:23 PM
$LogFile	13,264	Regular File	11/2/2018 4:25:23 PM
$MFT	256	Regular File	11/2/2018 4:25:23 PM
$MFTMirr	4	Regular File	11/2/2018 4:25:23 PM
$Secure	1	Regular File	11/2/2018 4:25:23 PM
$TXF_DATA	1	NTFS Logged ...	11/2/2018 4:40:23 PM
$UpCase	128	Regular File	11/2/2018 4:25:23 PM
$Volume	0	Regular File	11/2/2018 4:25:23 PM
Computer Forensics - File Timestamps.pptx	1,217	Regular File	11/2/2016 4:49:44 PM
eDiscovery - Business Model.pptx	1,690	Regular File	11/2/2016 4:49:44 PM
eDiscovery - Case Demo.pptx	1,566	Regular File	11/2/2016 4:49:44 PM

Did you receive a forensic image of the USB drive?

Does anything look suspicious?

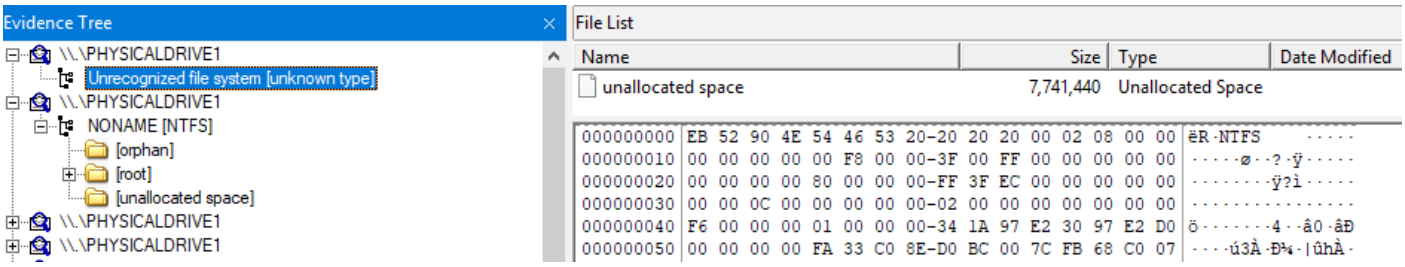
How could the PPTX files have a date prior to the MFT last modified date?

What are some questions to ask opposing counsel about the image you received?

Your client suspects important files were downloaded to a USB drive in 2016.

On 11/1 you request the forensic image of that USB drive.

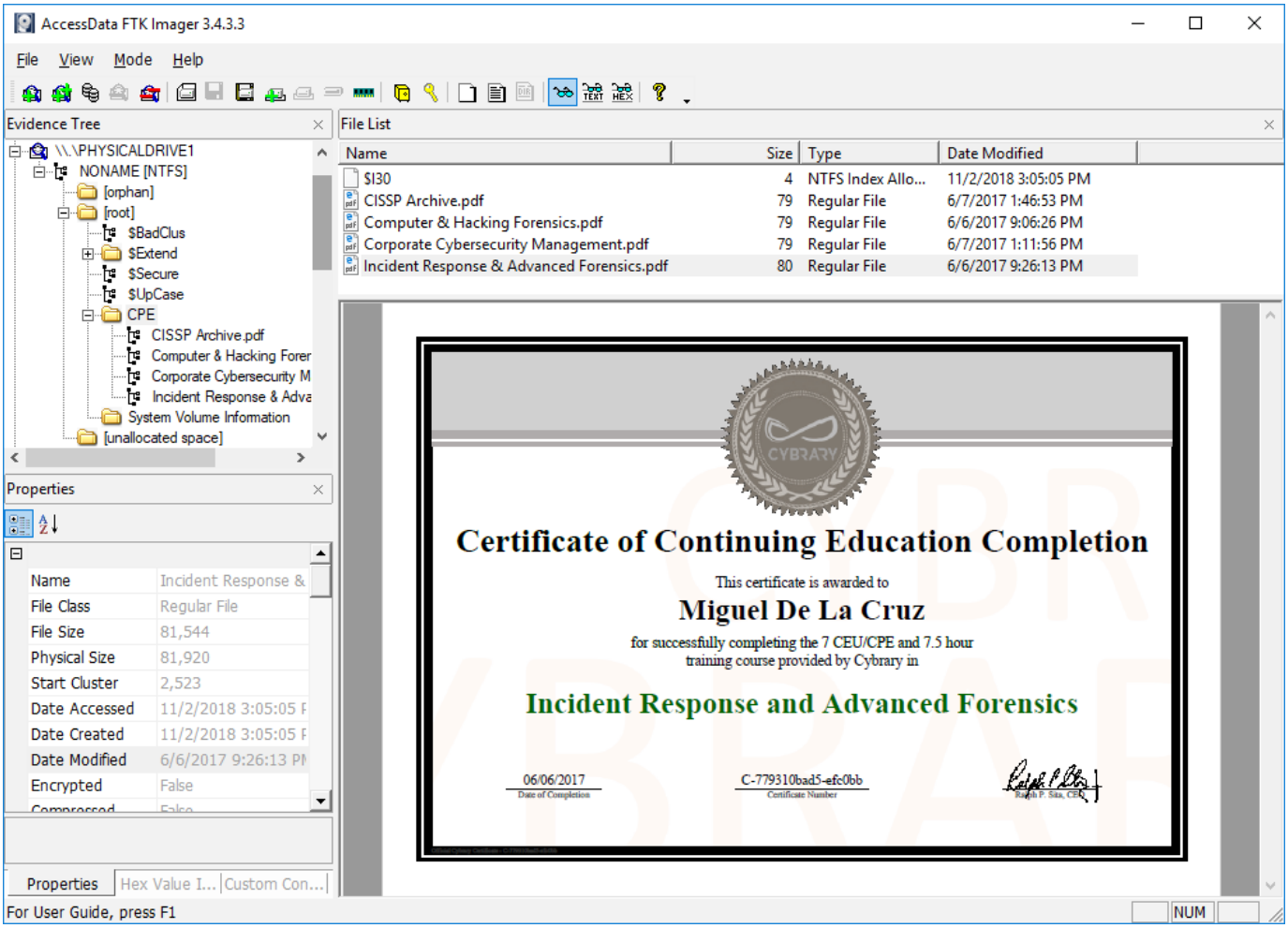
You receive the following image on 11/3 and begin to review it in FTK.



Why is the partition unrecognized?

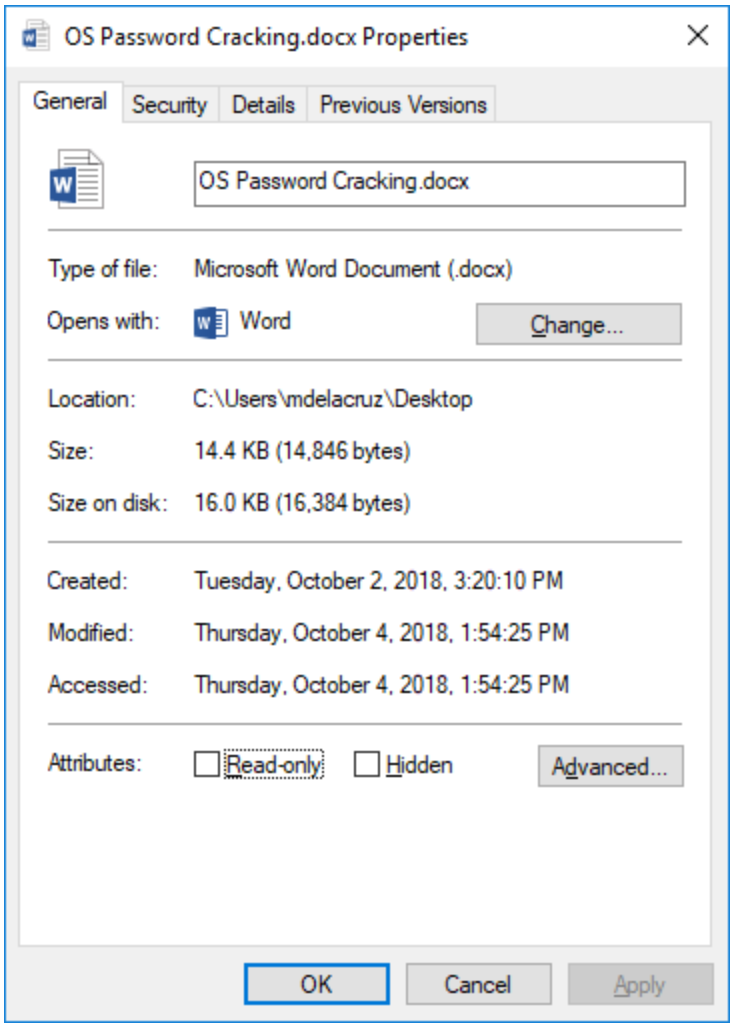
How can you verify there is data on the image?

How can you recover the data structures?



File Timestamps

What are the 3 timestamps recorded in a file? Created, Accessed, and Modified

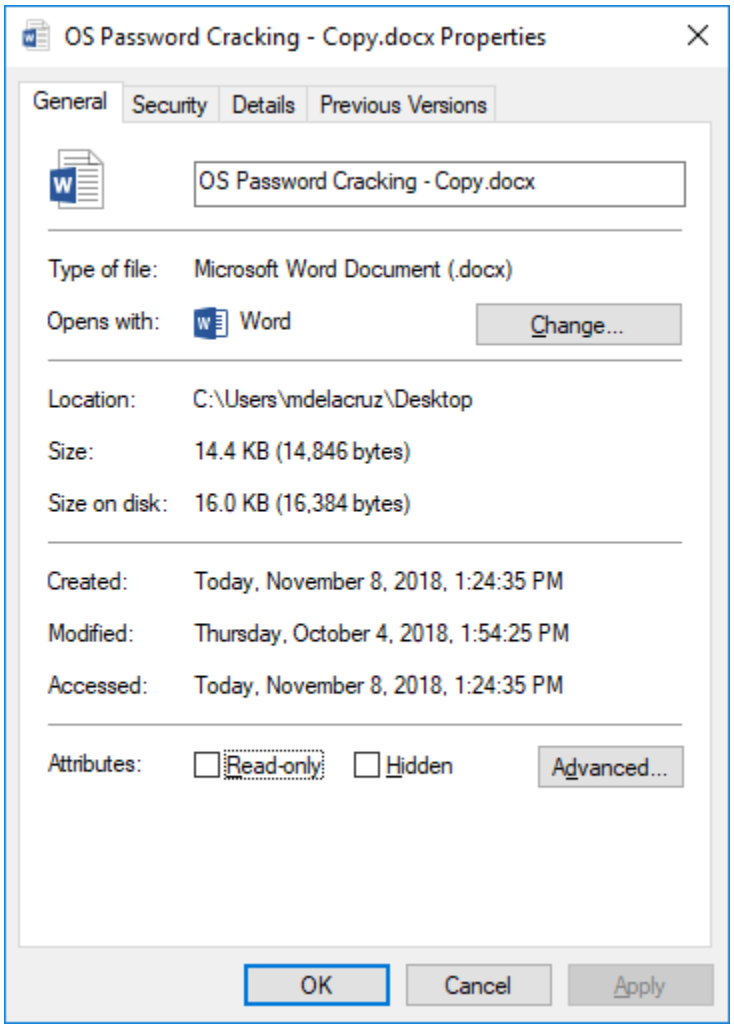

OS Password Cracking.docx Properties
General
Security
Details
Previous Versions
OS Password Cracking.docx
Type of file:
Microsoft Word Document (.docx)
Opens with:
Word
Change...
Location:
C:\Users\mdelacruz\Desktop
Size:
14.4 KB (14,846 bytes)
Size on disk:
16.0 KB (16,384 bytes)
Created:
Tuesday, October 2, 2018, 3:20:10 PM
Modified:
Thursday, October 4, 2018, 1:54:25 PM
Accessed:
Thursday, October 4, 2018, 1:54:25 PM
Attributes:
Read-only
Hidden
Advanced...
OK
Cancel
Apply

Analyzing Timestamps

Copying a File

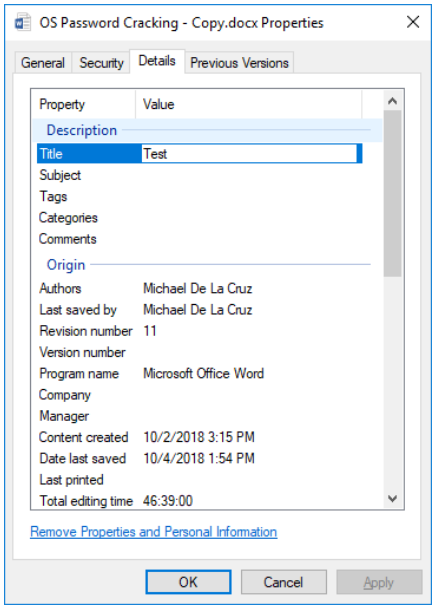
Which timestamps changed?

Which timestamp was inherited from the original file?

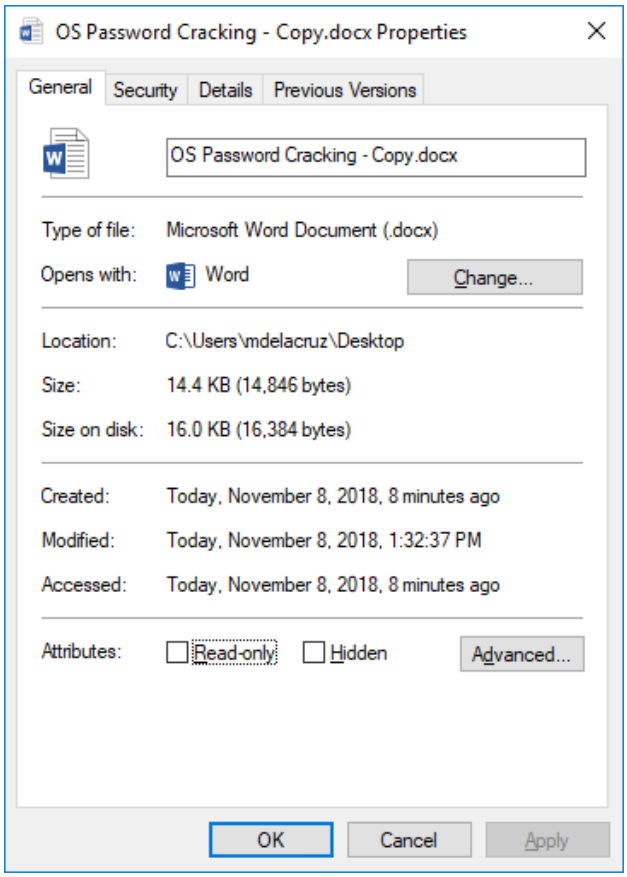


The Modified Timestamp

Editing the Title value



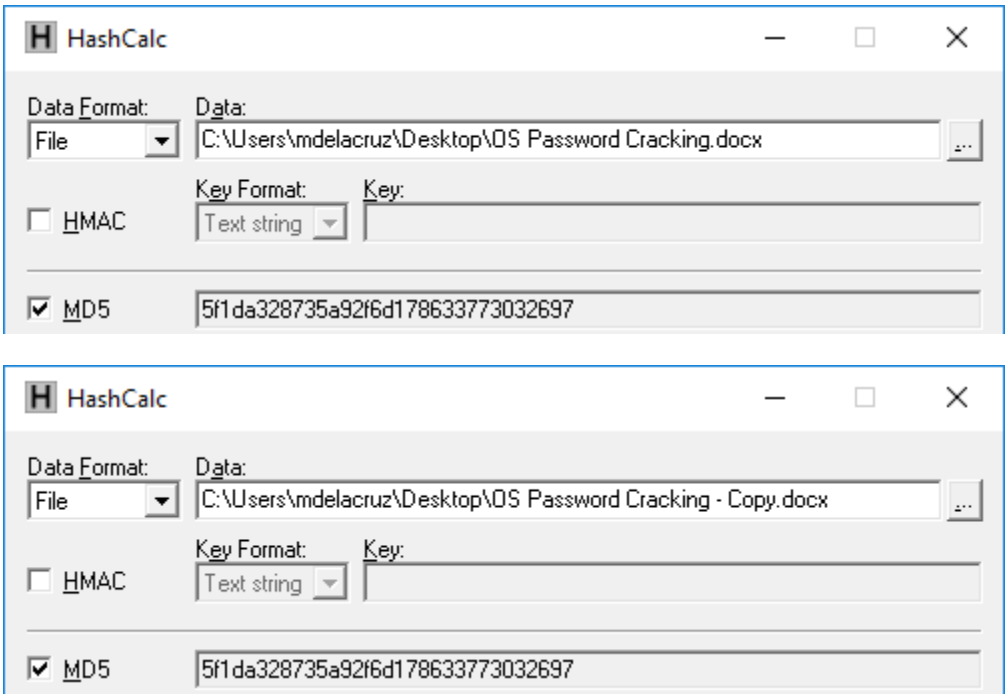
Which timestamp changed? Which timestamps stayed the same?


OS Password Cracking - Copy.docx Properties
General
Security
Details
Previous Versions
OS Password Cracking - Copy.docx
Type of file:
Microsoft Word Document (.docx)
Opens with:
Word
Change...
Location:
C:\Users\mdelacruz\Desktop
Size:
14.4 KB (14,846 bytes)
Size on disk:
16.0 KB (16,384 bytes)
Created:
Today, November 8, 2018, 8 minutes ago
Modified:
Today, November 8, 2018, 1:32:37 PM
Accessed:
Today, November 8, 2018, 8 minutes ago
Attributes:
Read-only
Hidden
Advanced...
OK
Cancel
Apply

File Hashing

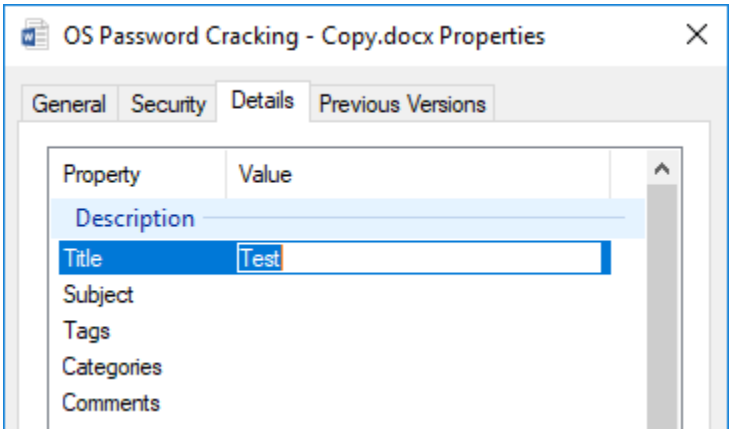
Hashing is an algorithm that calculates a fixed-size bit string value from a file.

Two files with different file names

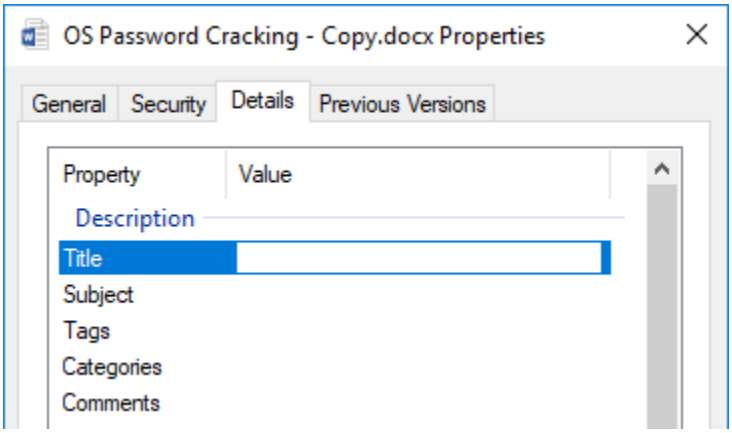


File hashes match.

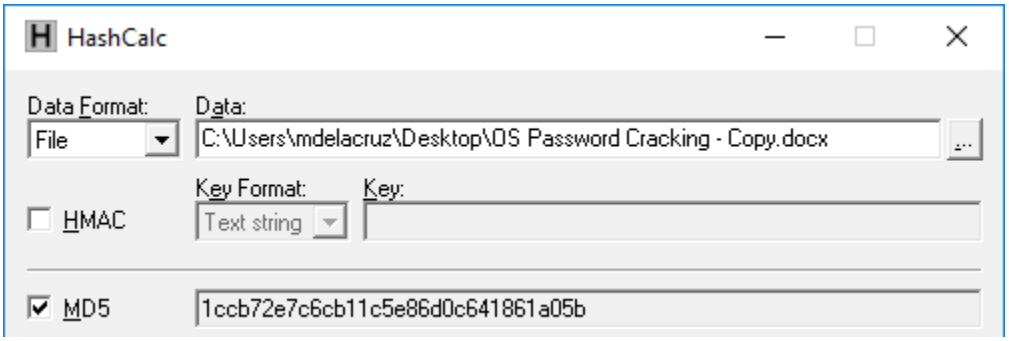
What happens if we modify one metadata field for one file?



Delete “Test” from the Title field.



Re-hash the file. Our MD5 value has changed.

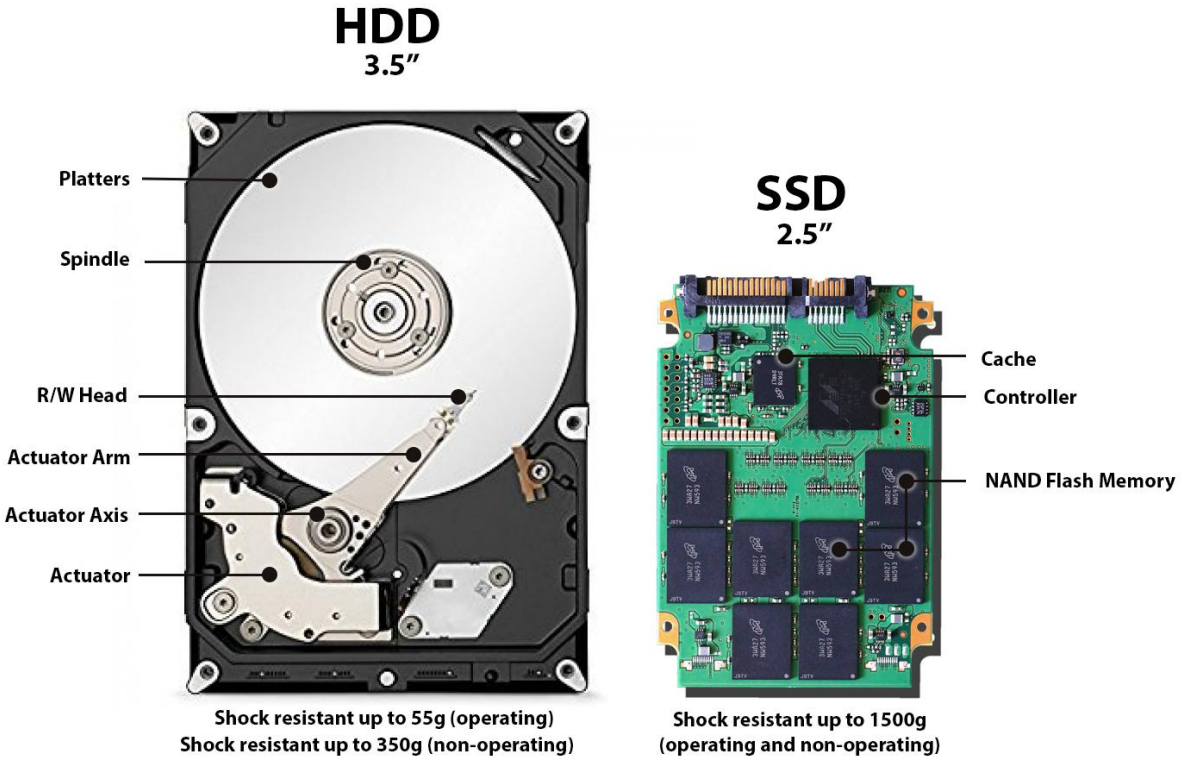


File hash mismatch

What changes need to occur to a file to cause a file hash mismatch? Changes to data area of the file.

Do changes to the filename or timestamps cause a file hash mismatch?

HDD vs Solid-State Hard Drives



What happens when you delete a file on a traditional HDD? The operating system marks the data as unallocated and the space the delete file takes up is available for new data. The old data remains untouched and recoverable until it has been overwritten with new data.

What happens when you delete a file on a Solid-State Hard Drive? TRIM immediately purges the areas of the SSD where the deleted data resided.

How can you determine if TRIM is enabled on your SSD?

Zero (0) = TRIM enabled

```
C:\WINDOWS\system32>fsutil behavior query DisableDeleteNotify
NTFS DisableDeleteNotify = 0  (Disabled)
ReFS DisableDeleteNotify = 0  (Disabled)
```

How can you disable TRIM?

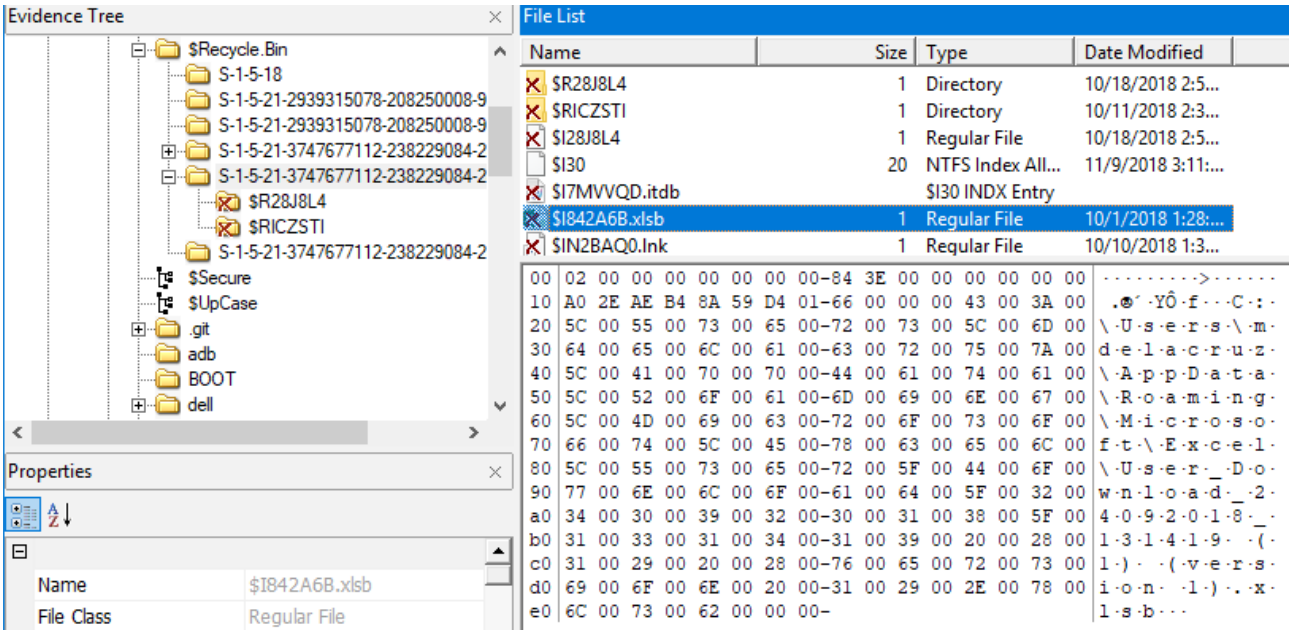
One (1) = TRIM disabled

```
C:\WINDOWS\system32>fsutil behavior set DisableDeleteNotify 1
NTFS DisableDeleteNotify = 1  (Enabled)
```

If TRIM is enabled, can you recover deleted files from the SSD?

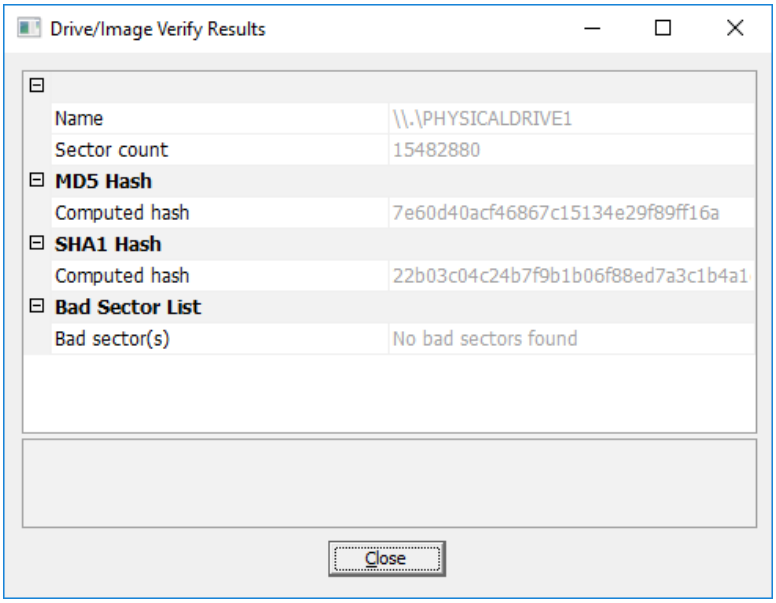
TRIM disabled – Recycle Bin emptied out

How can you identify if the files are recoverable?



What steps should be taken by any forensic analyst prior to reviewing forensic images? Chain of custody review, MD5 hash verification, Set Case Time Zone, view MFT timestamp, and identify the last timestamp recorded by the system.

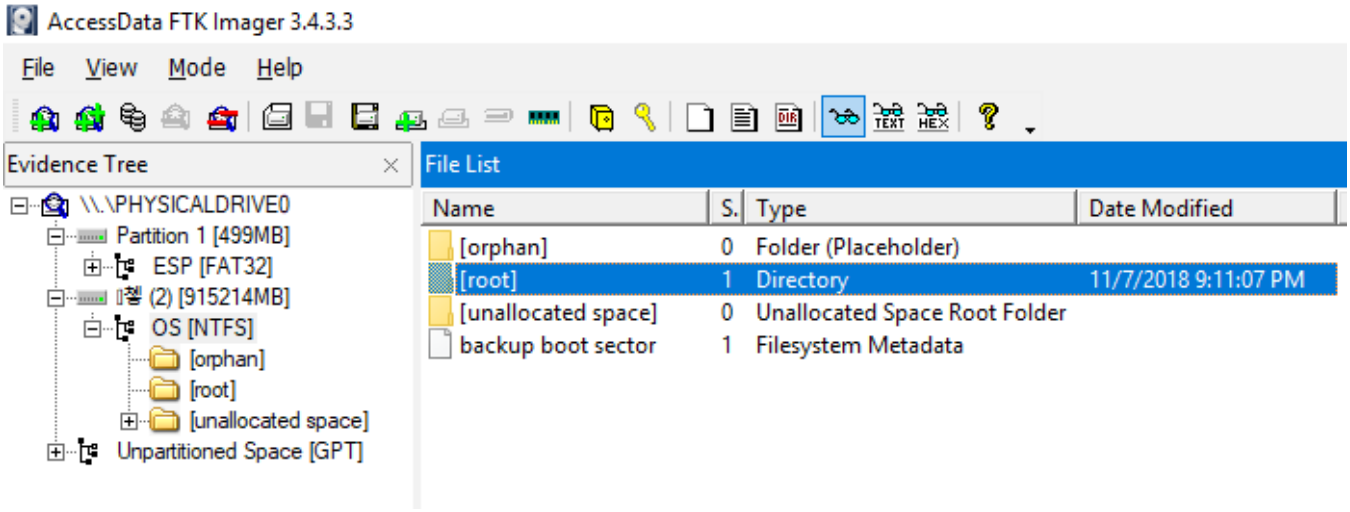
How can you verify a proper forensic image has been acquired? Acquisition hash verification must be done prior to signing the chain of custody form. This ensures the integrity of the data collected.



What if the hash verification doesn't match the hash on the chain of custody form?

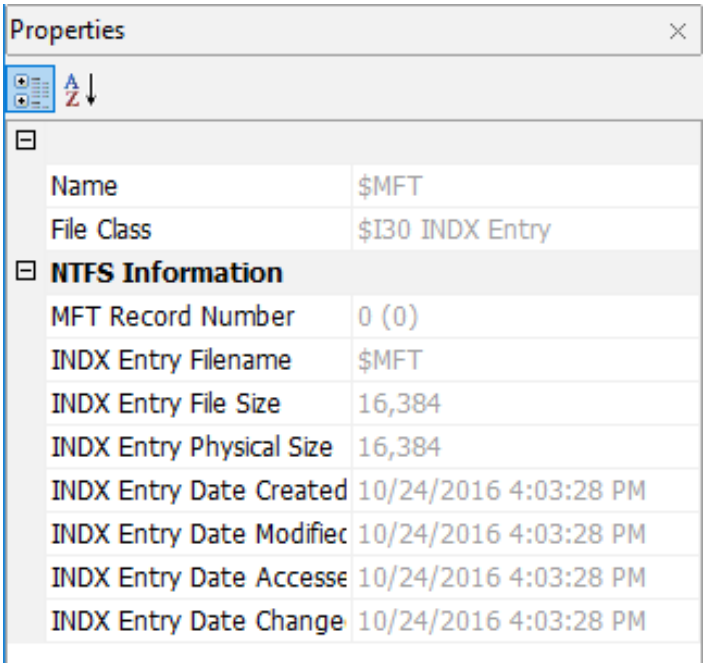
Should any timestamps exist after the forensic collection date?

According to the chain of custody sheet, the following forensic image was created on 11/1/2018.

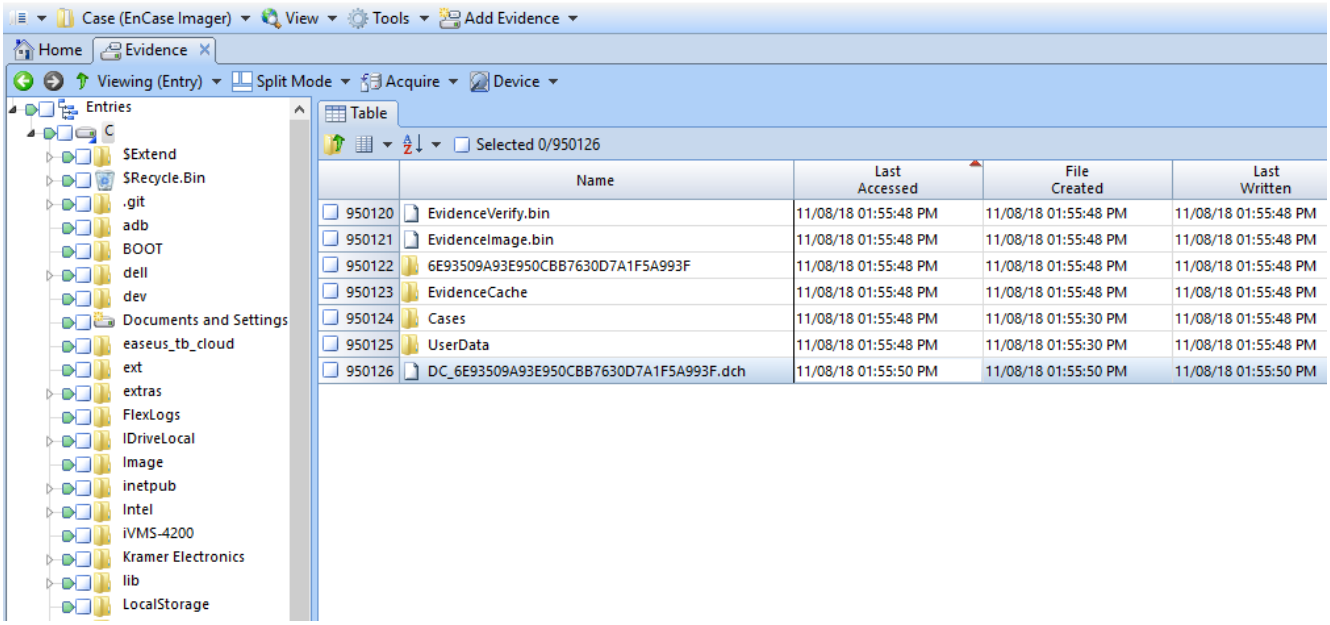


View the MFT timestamp

Why is the MFT timestamp an important artifact?



Identify the last timestamp recorded by the system



Should you proceed with analyzing this image if the chain of custody sheet indicates it was collected on 11/1/2018?

What questions should you have about how this image was collected?

Why is a chain of custody crucial to verifying the integrity of digital evidence?

File Type Categories

What are the four most common file type categories found on a Windows PC? Active, deleted, slack, & unallocated space.

What are active files? Files that are accessible by the operating system.

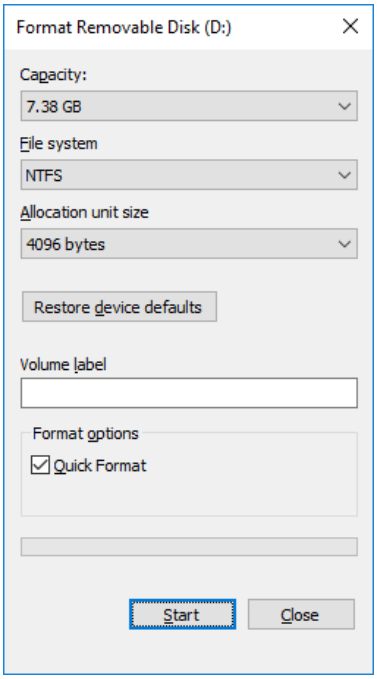
What are deleted files? Files that have been hard deleted or emptied out of the Recycle Bin.

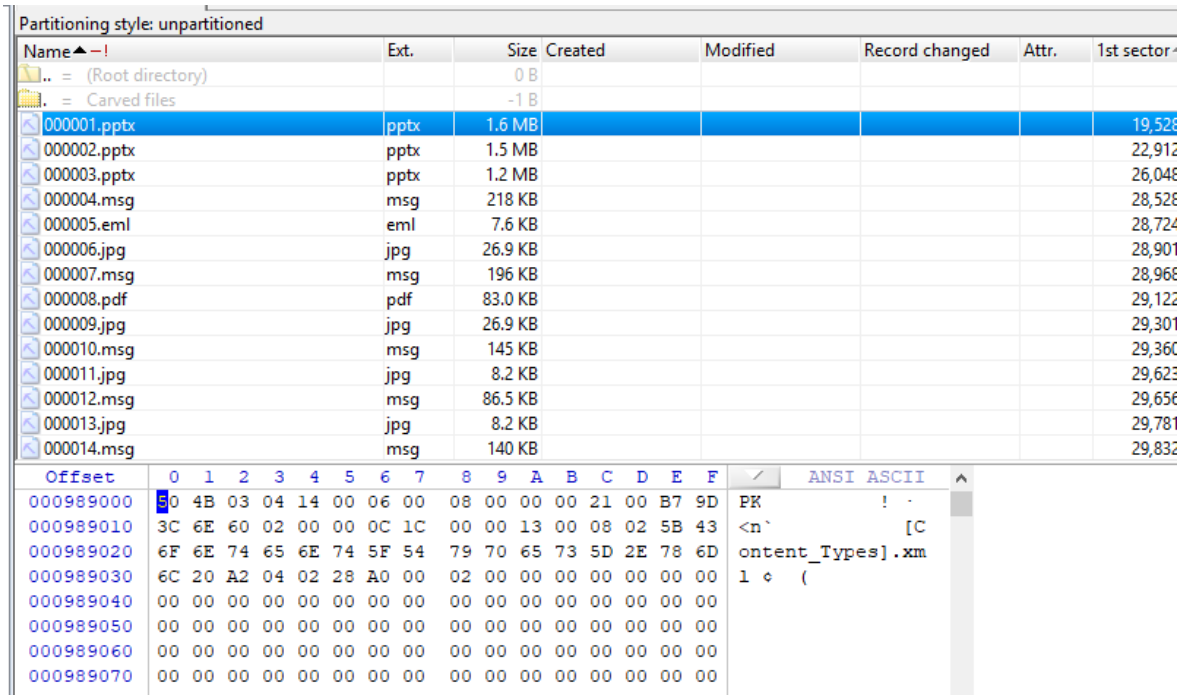
What are slack files? Remnants of deleted files that exists at the end of a file's allocated data sector/cluster.

What is unallocated space? Any space that is available for use within a logical partition.

What is unused space? The unused sectors outside of a logical partition.

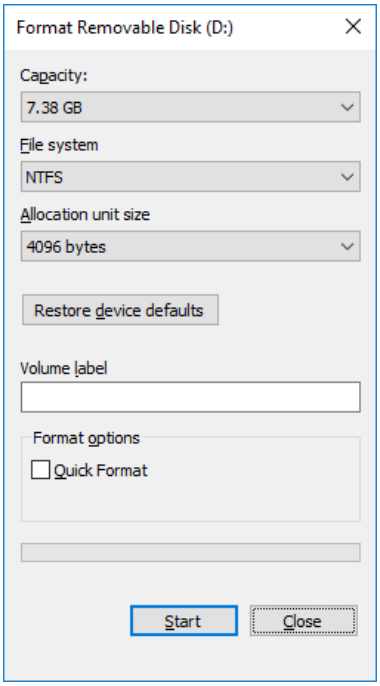
Quick Format

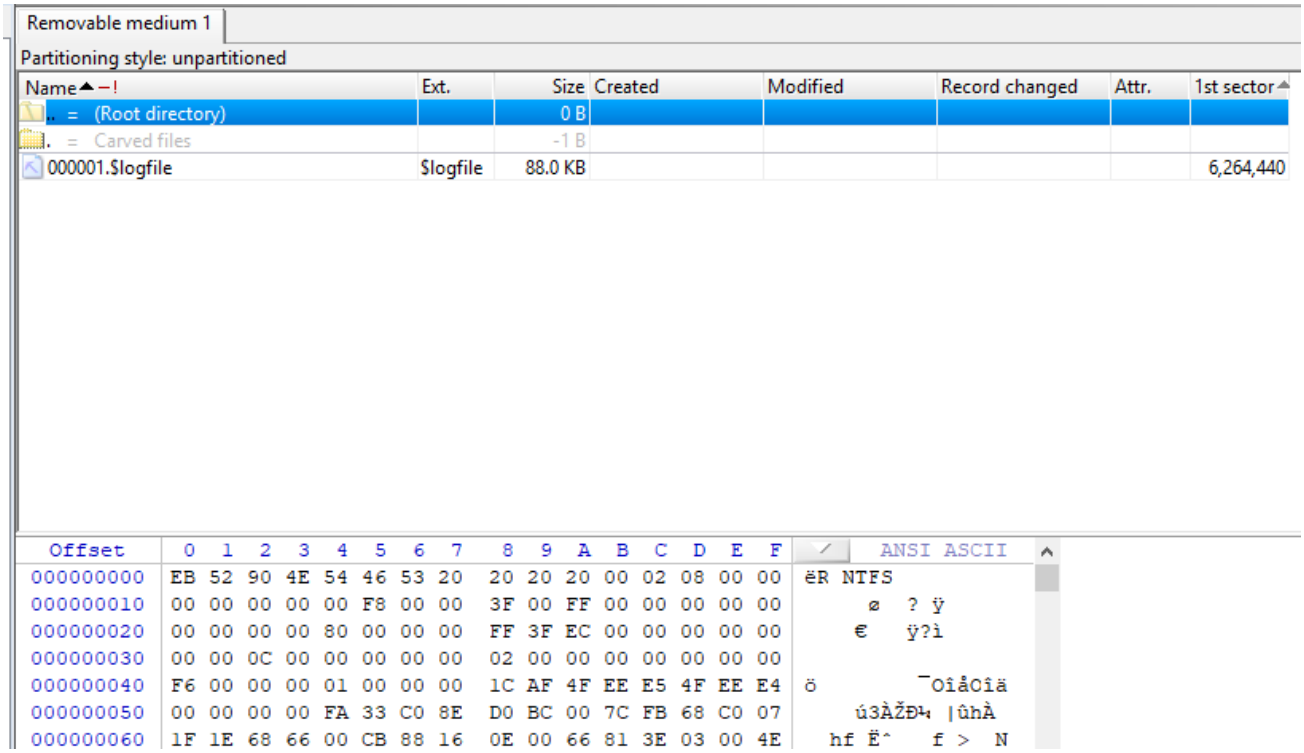




Recoverable user data

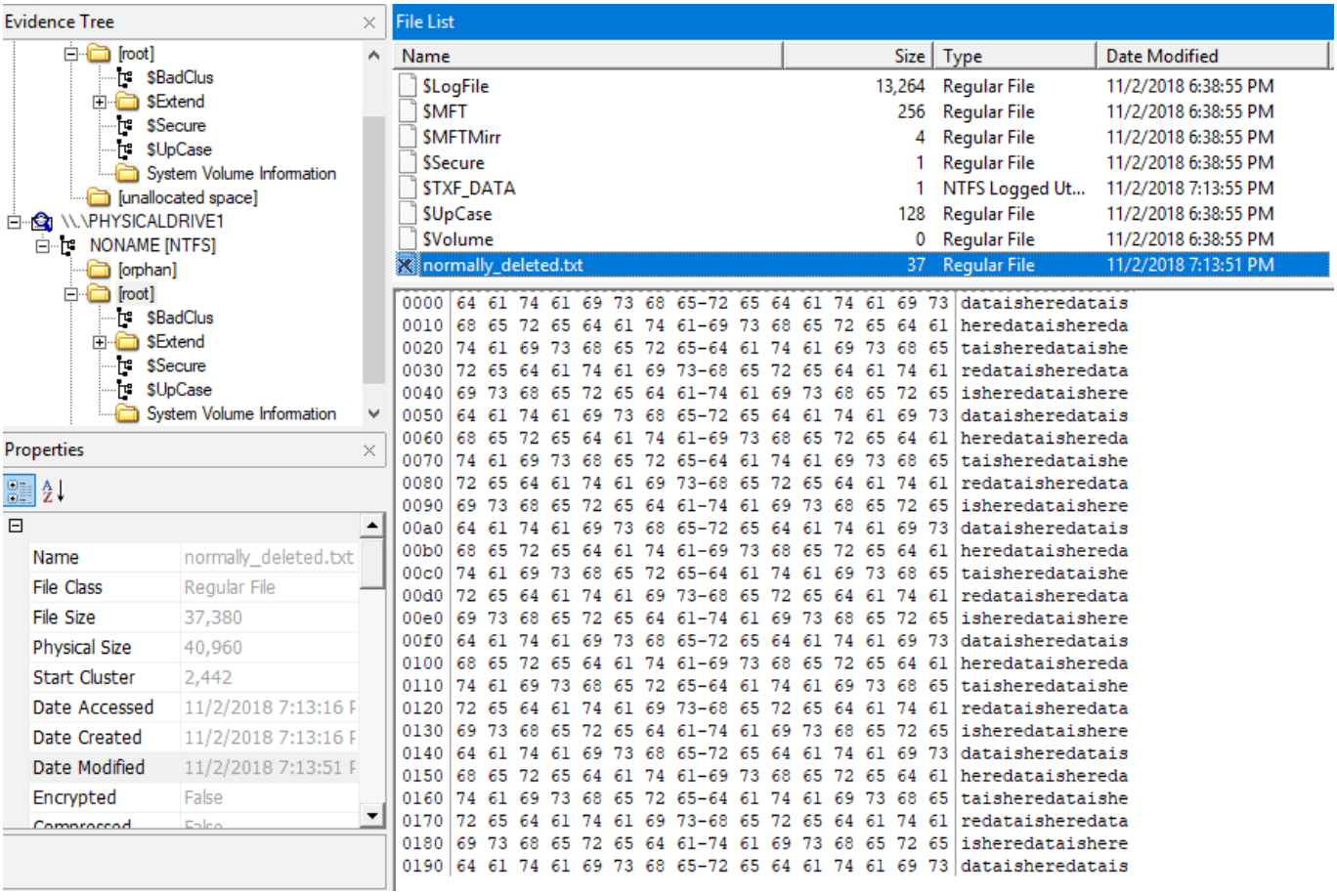
Full Format



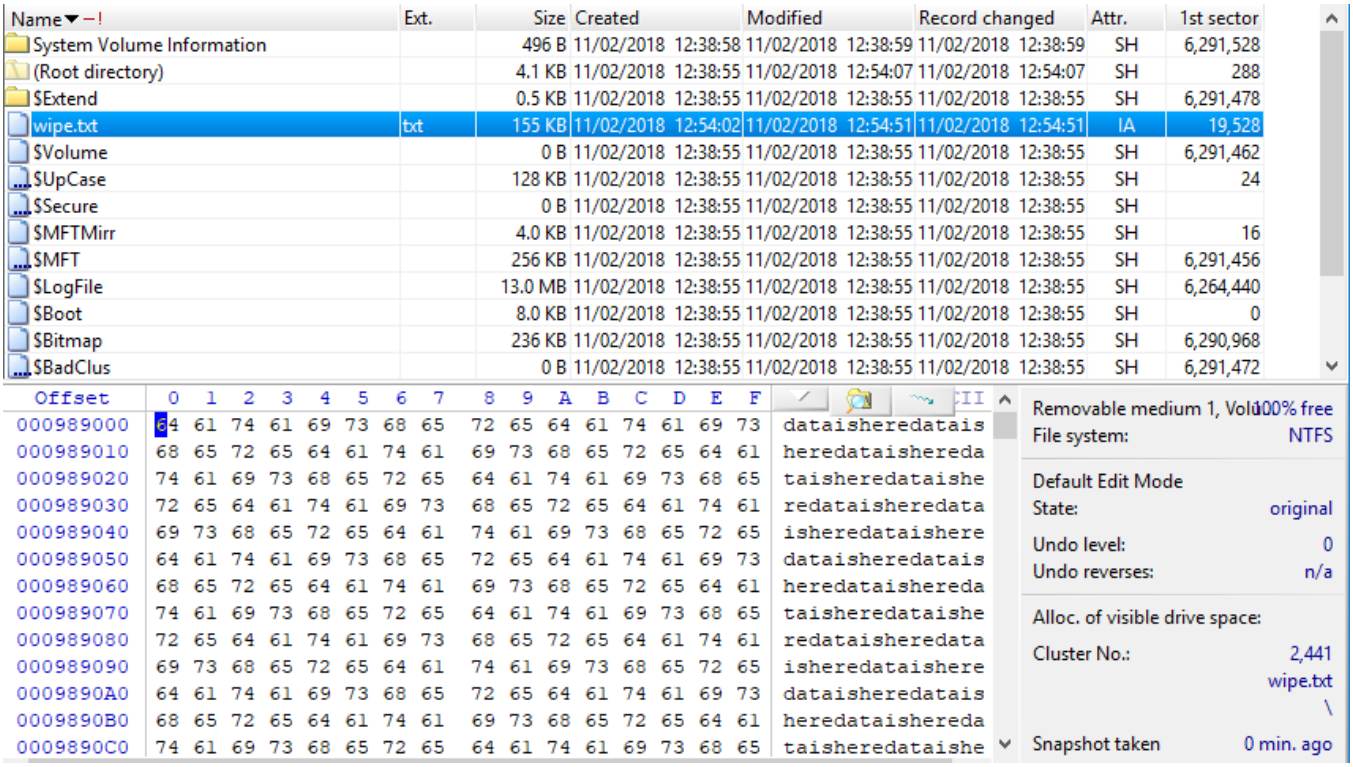


No recoverable user data. Evidence of system data.

Normally deleted file.



File Wiping with data patterns



Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
System Volume Information		496 B	11/02/2018 12:38:58	11/02/2018 12:38:59	11/02/2018 12:38:59	SH	6,291,528
(Root directory)		4.1 KB	11/02/2018 12:38:55	11/02/2018 12:54:07	11/02/2018 12:54:07	SH	288
$Extend		0.5 KB	11/02/2018 12:38:55	11/02/2018 12:38:55	11/02/2018 12:38:55	SH	6,291,478
wipe.txt	txt	155 KB	11/02/2018 12:54:02	11/02/2018 12:54:51	11/02/2018 12:54:51	IA	19,528
$Volume		0 B	11/02/2018 12:38:55	11/02/2018 12:38:55	11/02/2018 12:38:55	SH	6,291,462
$UpCase		128 KB	11/02/2018 12:38:55	11/02/2018 12:38:55	11/02/2018 12:38:55	SH	24
$Secure		0 B	11/02/2018 12:38:55	11/02/2018 12:38:55	11/02/2018 12:38:55	SH	
$MFTMirr		4.0 KB	11/02/2018 12:38:55	11/02/2018 12:38:55	11/02/2018 12:38:55	SH	16
$MFT		256 KB	11/02/2018 12:38:55	11/02/2018 12:38:55	11/02/2018 12:38:55	SH	6,291,456
$LogFile		13.0 MB	11/02/2018 12:38:55	11/02/2018 12:38:55	11/02/2018 12:38:55	SH	6,264,440
$Boot		8.0 KB	11/02/2018 12:38:55	11/02/2018 12:38:55	11/02/2018 12:38:55	SH	0
$Bitmap		236 KB	11/02/2018 12:38:55	11/02/2018 12:38:55	11/02/2018 12:38:55	SH	6,290,968
$BadClus		0 B	11/02/2018 12:38:55	11/02/2018 12:38:55	11/02/2018 12:38:55	SH	6,291,472

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000989000	64	61	74	61	69	73	68	65	72	65	64	61	74	61	69	73	datasheredatais
000989010	68	65	72	65	64	61	74	61	69	73	68	65	72	65	64	61	heredataishereda
000989020	74	61	69	73	68	65	72	65	64	61	74	61	69	73	68	65	taisheredataishe
000989030	72	65	64	61	74	61	69	73	68	65	72	65	64	61	74	61	redataisheredata
000989040	69	73	68	65	72	65	64	61	74	61	69	73	68	65	72	65	isheredataishere
000989050	64	61	74	61	69	73	68	65	72	65	64	61	74	61	69	73	datasheredatais
000989060	68	65	72	65	64	61	74	61	69	73	68	65	72	65	64	61	heredataishereda
000989070	74	61	69	73	68	65	72	65	64	61	74	61	69	73	68	65	taisheredataishe
000989080	72	65	64	61	74	61	69	73	68	65	72	65	64	61	74	61	redataisheredata
000989090	69	73	68	65	72	65	64	61	74	61	69	73	68	65	72	65	isheredataishere
0009890A0	64	61	74	61	69	73	68	65	72	65	64	61	74	61	69	73	datasheredatais
0009890B0	68	65	72	65	64	61	74	61	69	73	68	65	72	65	64	61	heredataishereda
0009890C0	74	61	69	73	68	65	72	65	64	61	74	61	69	73	68	65	taisheredataishe

Removable medium 1, Volu 100% free
File system: NTFS

Default Edit Mode
State: original

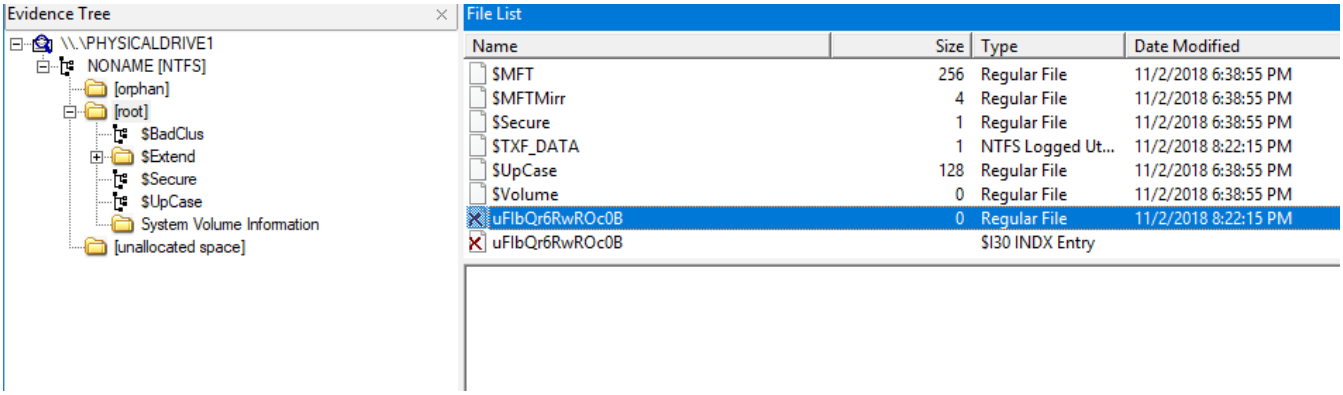
Undo level: 0
Undo reverses: n/a

Alloc. of visible drive space:

Cluster No.: 2,441
wipe.txt
\

Snapshot taken 0 min. ago

File Wiping with Zeros



Evidence Tree

- \\.\PHYSICALDRIVE1
  - NONAME [NTFS]
    - [orphan]
    - [root]
      - $BadClus
      - $Extend
      - $Secure
      - $UpCase
      - System Volume Information
    - [unallocated space]

File List

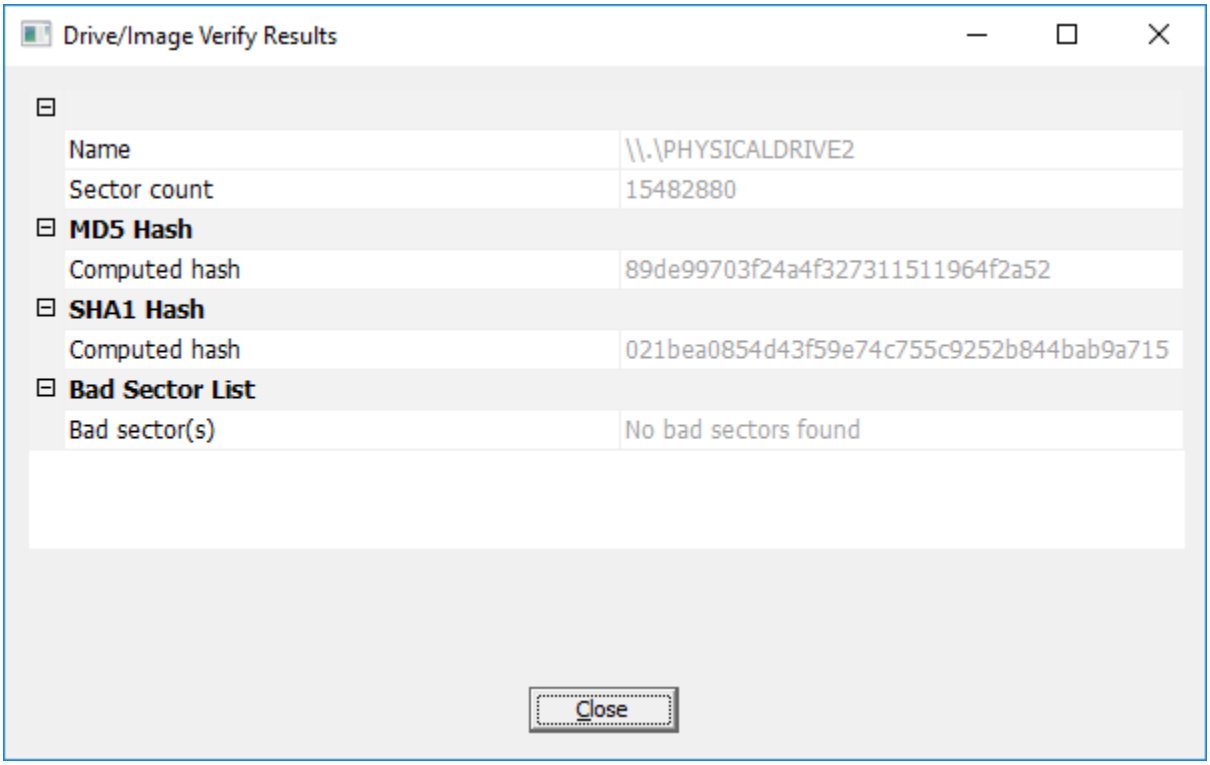
Name	Size	Type	Date Modified
$MFT	256	Regular File	11/2/2018 6:38:55 PM
$MFTMirr	4	Regular File	11/2/2018 6:38:55 PM
$Secure	1	Regular File	11/2/2018 6:38:55 PM
$TXF_DATA	1	NTFS Logged Ut...	11/2/2018 8:22:15 PM
$UpCase	128	Regular File	11/2/2018 6:38:55 PM
$Volume	0	Regular File	11/2/2018 6:38:55 PM
uFlbQr6RwROc0B	0	Regular File	11/2/2018 8:22:15 PM
uFlbQr6RwROc0B		$I30 INDX Entry	

What key indicators can we look at to determine if a file has been shredded/wiped?

Can you determine when a file was wiped?

Can you determine which tool was used to wipe the file?

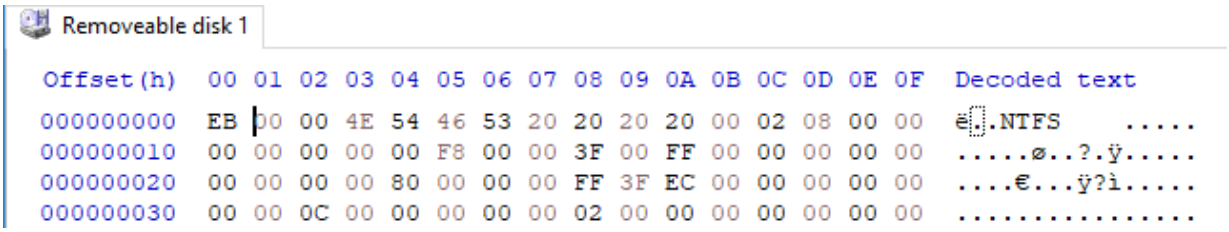
Hashing a drive/image



Why are MD5 hash verifications of forensic images important?

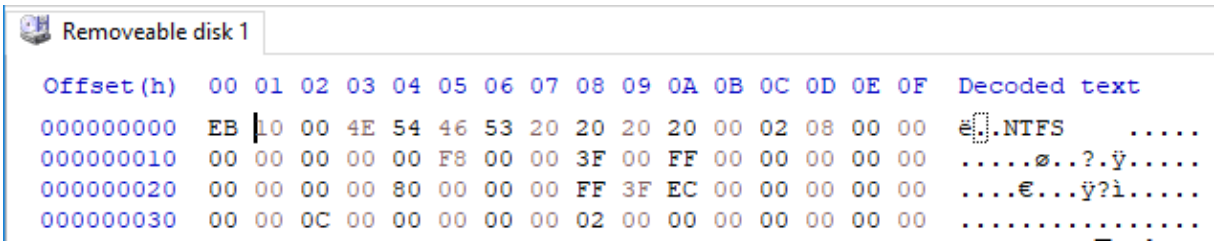
How much data needs to change to have a hash mismatch?

MD5 Hash: **89de99703f24a4f327311511964f2a52**



Changed one bit from “0” to “1”

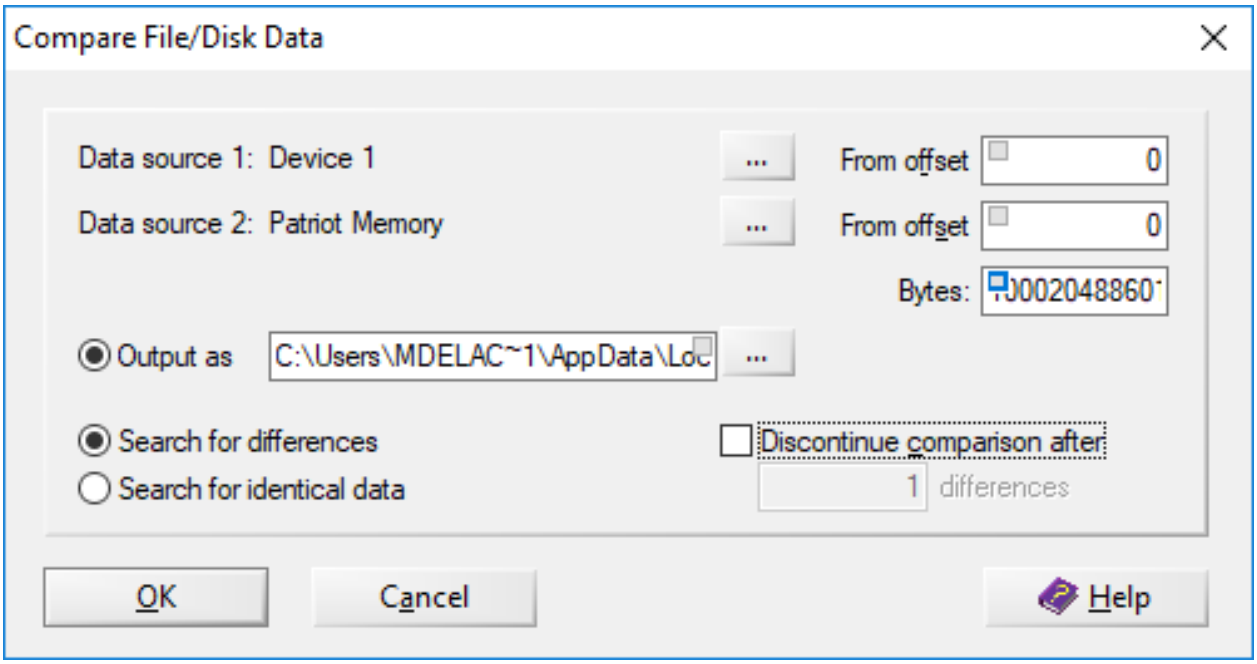
MD5 Hash: **89e1110ef65d95e5e320d869dab738c6**


Removeable disk 1
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
000000000 EB 10 00 4E 54 46 53 20 20 20 20 00 02 08 00 00 ë..NTFS .....
000000010 00 00 00 00 00 F8 00 00 3F 00 FF 00 00 00 00 00 .....ø..?.ÿ.....
000000020 00 00 00 00 80 00 00 00 FF 3F EC 00 00 00 00 00 ....€...ÿ?ì.....
000000030 00 00 0C 00 00 00 00 00 02 00 00 00 00 00 00 00 ....

Chain of Custody should have number of sectors imaged and MD5 hash value generated.

How do bad sectors affect the MD5 hash value creation? Validation?

How can you identify the differences in two images that have different MD5 hashes?



When would this comparison be useful?

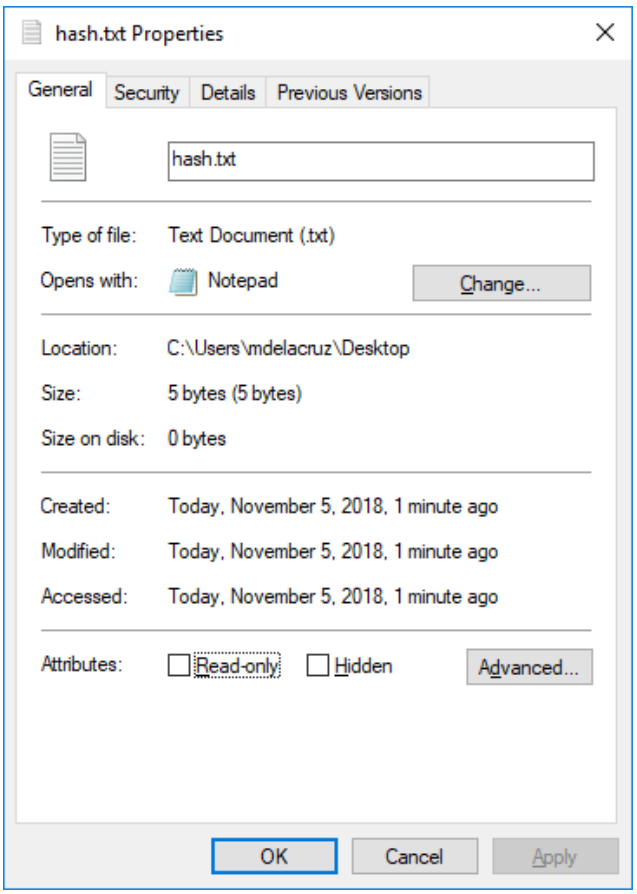
File Hashing (Checksum)

What part of a file is hashed?

Why would you conduct a file hash verification before reviewing them?

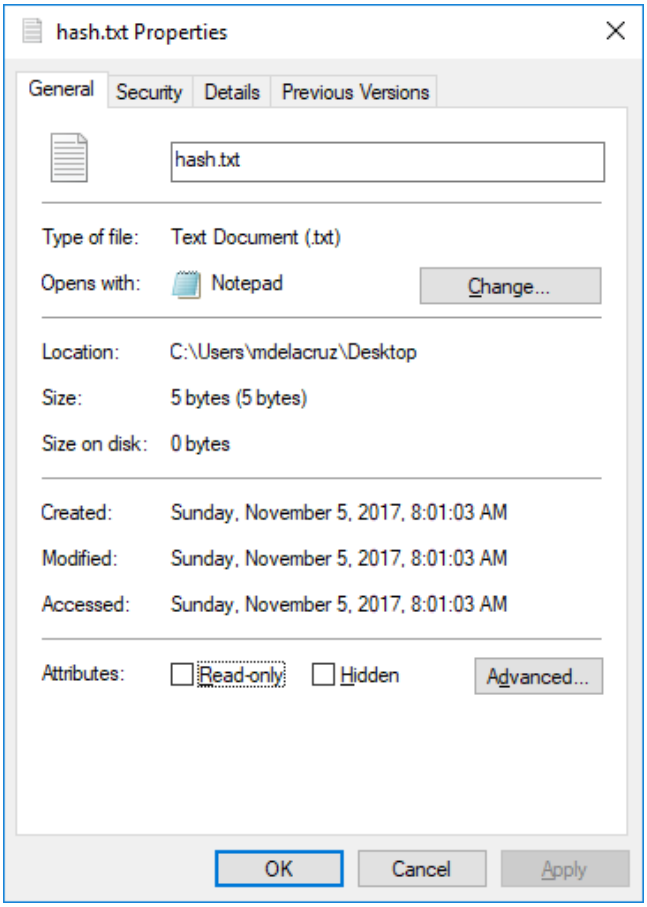
What areas of the file can change without affecting the file hash value?

Hash.txt – MD5: 827ccb0eea8a706c4c34a16891f84e7b



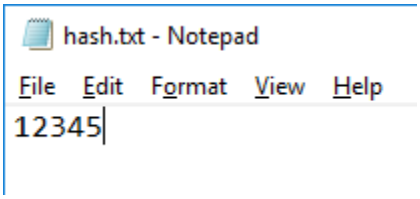
Program used to change the Created/Accessed/Modified timestamps.

Hash.txt – MD5: 827ccb0eea8a706c4c34a16891f84e7b



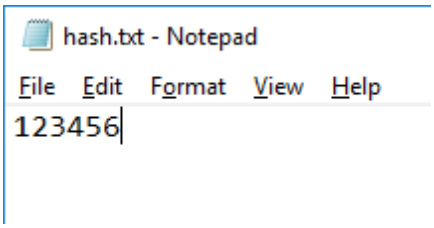
Original hash.txt file

MD5: 827ccb0eea8a706c4c34a16891f84e7b



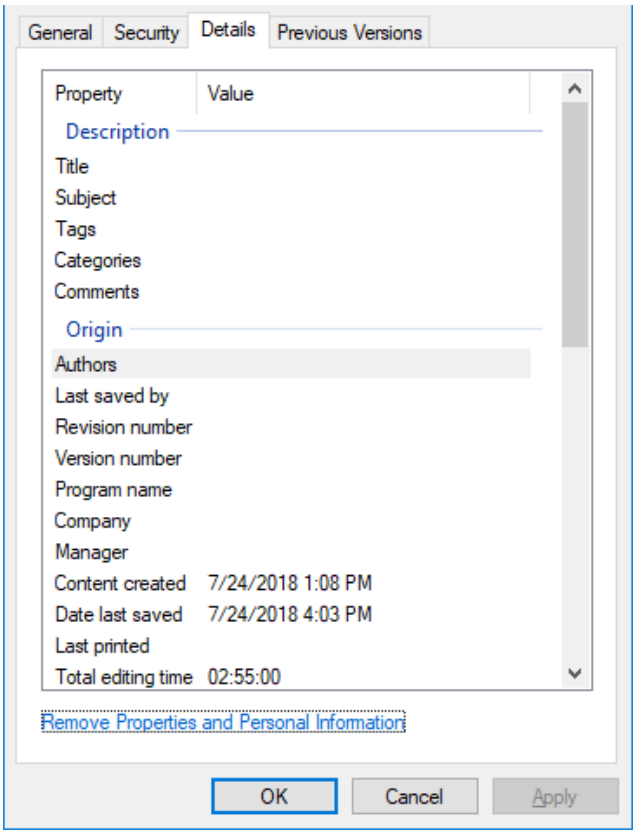
Edited hash.txt file

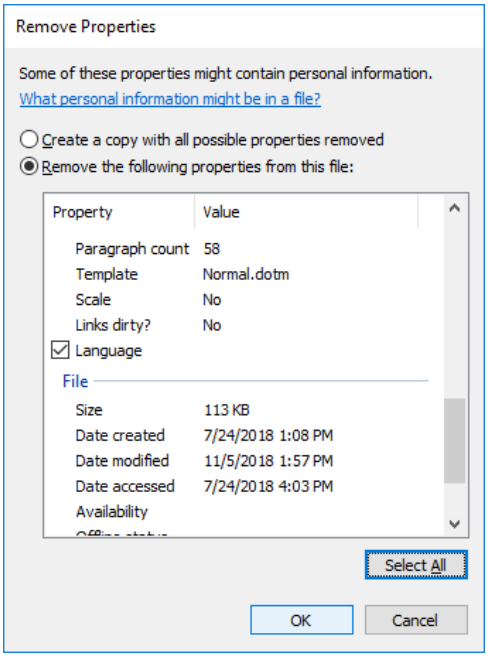
MD5: e10adc3949ba59abbe56e057f20f883e



Does changing the filename change the file's hash value?

Will removing metadata from a document change its hash value?


General
Security
Details
Previous Versions
Property
Value
Description
Title
Subject
Tags
Categories
Comments
Origin
Authors
Last saved by
Revision number
Version number
Program name
Company
Manager
Content created 7/24/2018 1:08 PM
Date last saved 7/24/2018 4:03 PM
Last printed
Total editing time 02:55:00
Remove Properties and Personal Information
OK
Cancel
Apply


Remove Properties
Some of these properties might contain personal information.
What personal information might be in a file?
Create a copy with all possible properties removed
Remove the following properties from this file:
Property
Value
Paragraph count 58
Template Normal.dotm
Scale No
Links dirty? No
Language
File
Size 113 KB
Date created 7/24/2018 1:08 PM
Date modified 11/5/2018 1:57 PM
Date accessed 7/24/2018 4:03 PM
Availability
Select All
OK
Cancel

Metadata Analysis

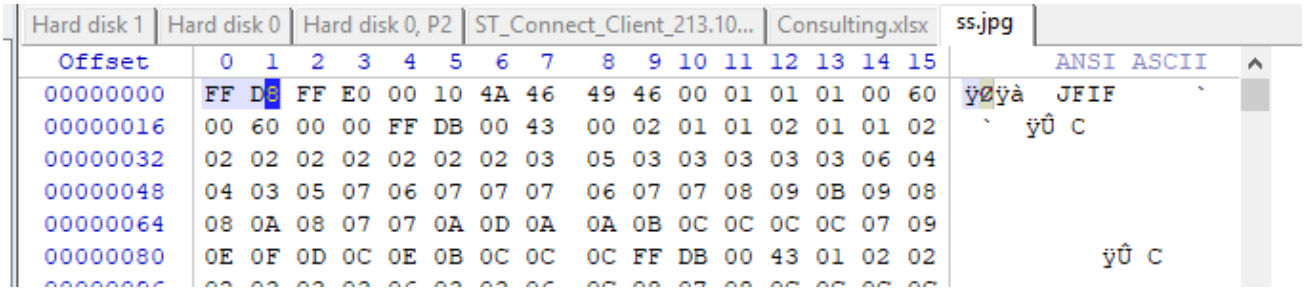
What are compound files?

Why is it important to analyze timestamps recorded in the MFT and within compound files?

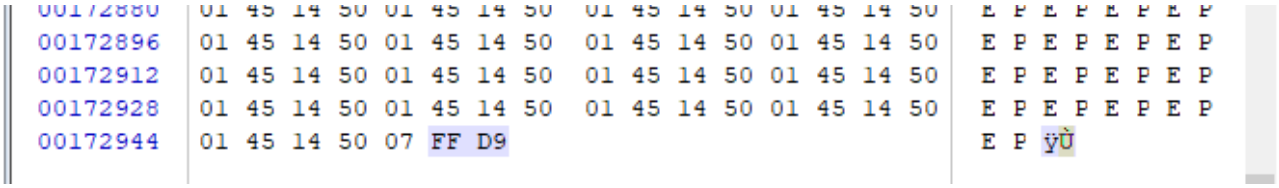
What are file signatures?

How are file signatures used to identify deleted files?

JPG header signature



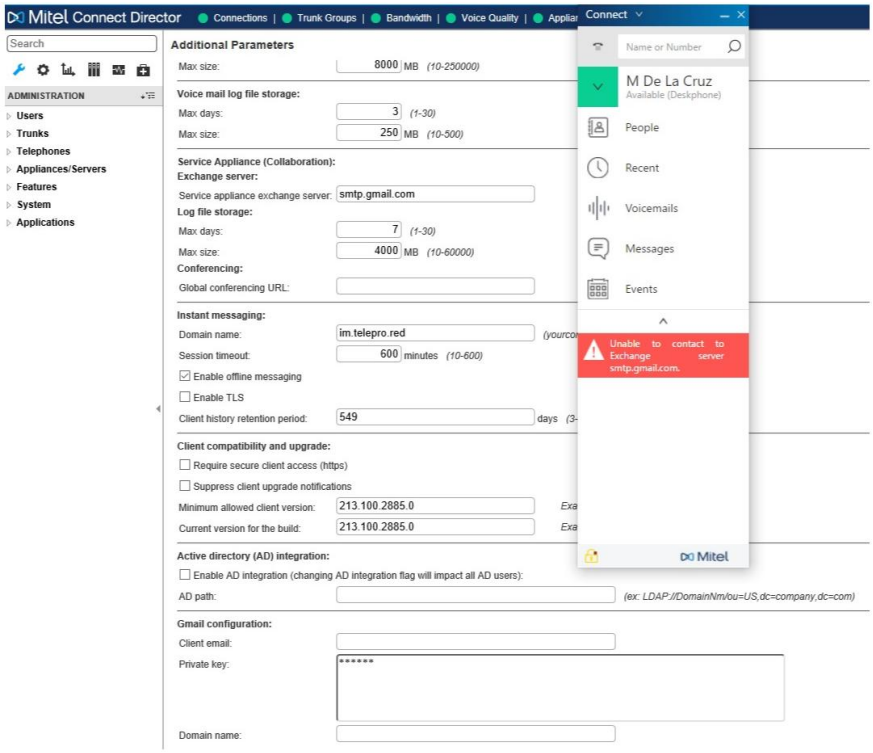
JPG footer signature (End of File)



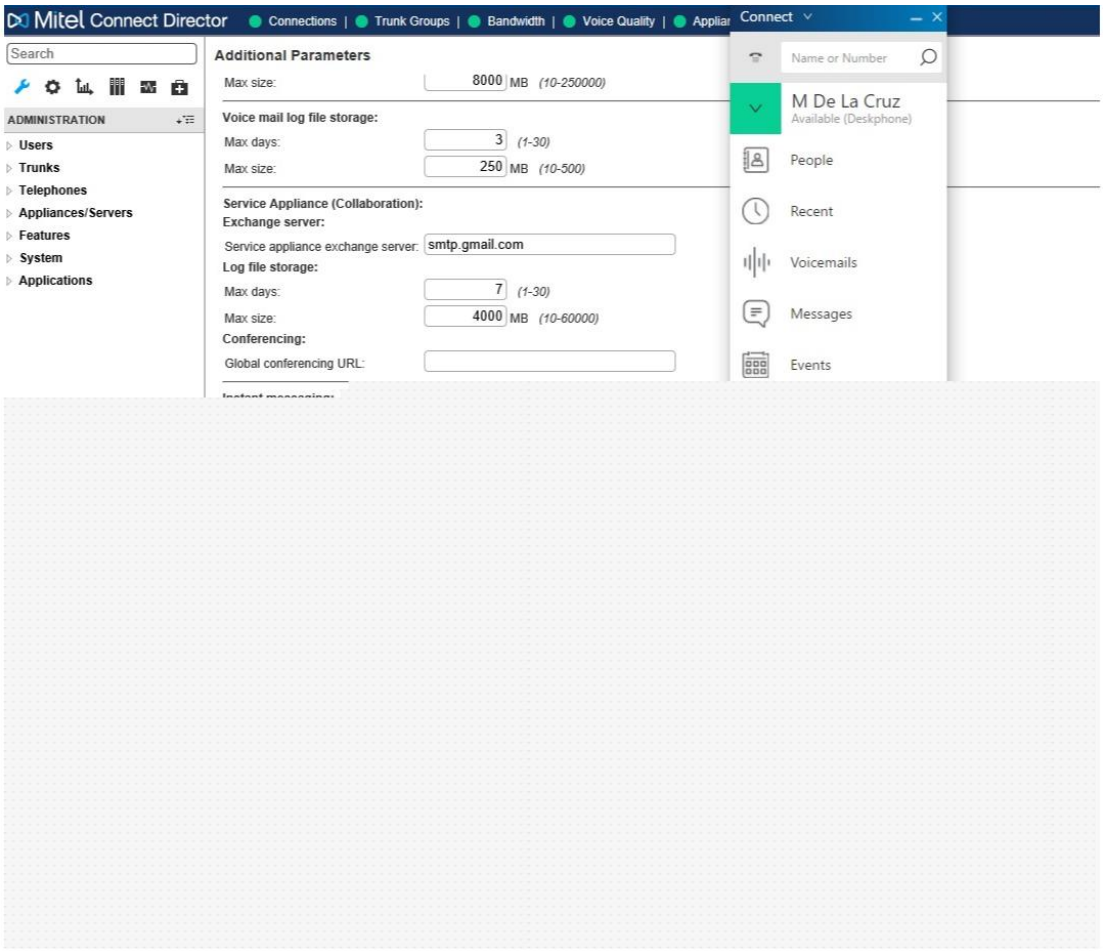
Locate the header and footer signatures and copy out everything in between.

What if the footer signature was been overwritten?

Fully recovered JPG with header and footer signature intact.



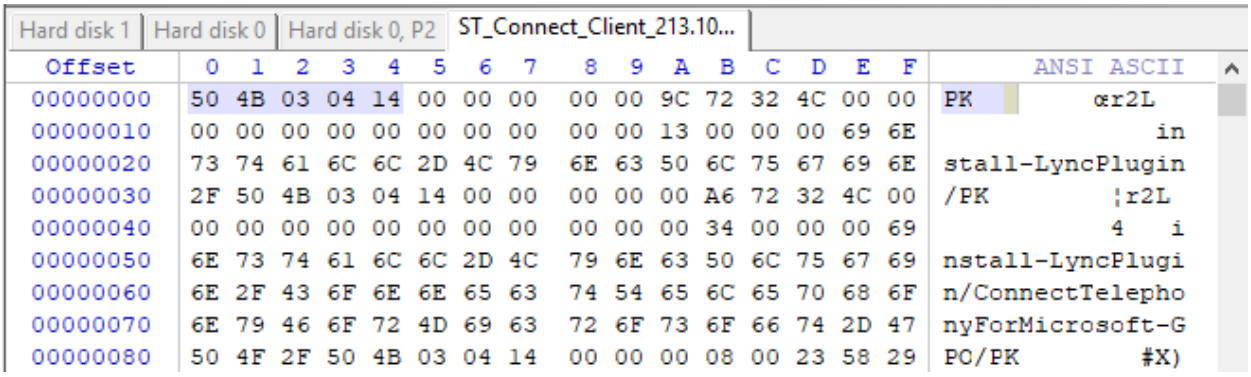
Partially recovered JPG. Header intact, but half of the file and footer have been overwritten.


Mitel Connect Director
Connections | Trunk Groups | Bandwidth | Voice Quality | Appliar
Connect
Search
ADMINISTRATION
Users
Trunks
Telephones
Appliances/Servers
Features
System
Applications
Additional Parameters
Max size: 8000 MB (10-250000)
Voice mail log file storage:
Max days: 3 (1-30)
Max size: 250 MB (10-500)
Service Appliance (Collaboration):
Exchange server:
Service appliance exchange server: smtp.gmail.com
Log file storage:
Max days: 7 (1-30)
Max size: 4000 MB (10-60000)
Conferencing:
Global conferencing URL:
Name or Number
M De La Cruz
Available (Deskphone)
People
Recent
Voicemails
Messages
Events

File Carving Embedded Files

Description	Extensions	Header	Offset	Footer	Default size	Flags
Zip Archive	zip;jar;xps;apk;pages	PK\x03\x04|PK00|PK\x05\x06	0	~14	4194304/536870912	gGE

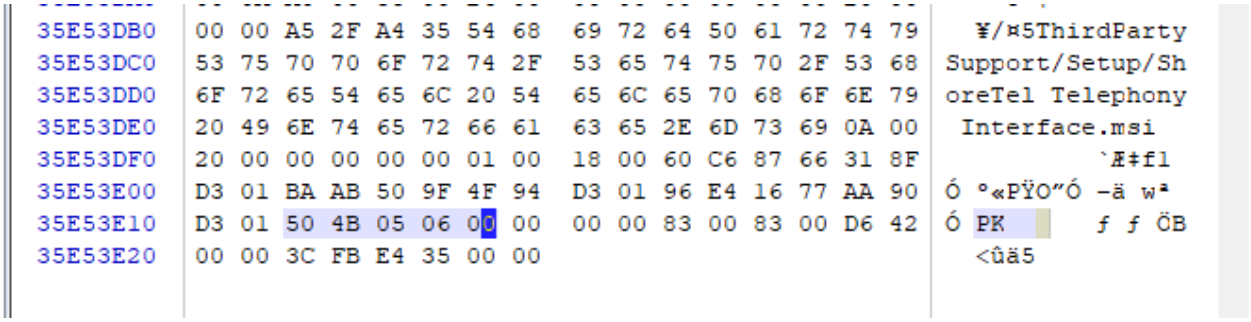
ZIP File Header: \x50 \x4B \x03 \x04 at Offset 0



Hard disk 1 | Hard disk 0 | Hard disk 0, P2 | ST_Connect_Client_213.10...

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	50	4B	03	04	14	00	00	00	00	00	9C	72	32	4C	00	00	PK œr2L
00000010	00	00	00	00	00	00	00	00	00	00	13	00	00	00	69	6E	in
00000020	73	74	61	6C	6C	2D	4C	79	6E	63	50	6C	75	67	69	6E	stall-LyncPlugin
00000030	2F	50	4B	03	04	14	00	00	00	00	00	A6	72	32	4C	00	/PK ¦r2L
00000040	00	00	00	00	00	00	00	00	00	00	00	34	00	00	00	69	4 i
00000050	6E	73	74	61	6C	6C	2D	4C	79	6E	63	50	6C	75	67	69	nstall-LyncPlugi
00000060	6E	2F	43	6F	6E	6E	65	63	74	54	65	6C	65	70	68	6F	n/ConnectTelepho
00000070	6E	79	46	6F	72	4D	69	63	72	6F	73	6F	66	74	2D	47	nyForMicrosoft-G
00000080	50	4F	2F	50	4B	03	04	14	00	00	00	08	00	23	58	29	PO/PK #X)

ZIP File Footer: \x50 \x4B \x05 \x06 + 18 trailing bytes before the end of file.



35E53DB0	00	00	A5	2F	A4	35	54	68	69	72	64	50	61	72	74	79	¥/¤5ThirdParty
35E53DC0	53	75	70	70	6F	72	74	2F	53	65	74	75	70	2F	53	68	Support/Setup/Sh
35E53DD0	6F	72	65	54	65	6C	20	54	65	6C	65	70	68	6F	6E	79	oreTel Telephony
35E53DE0	20	49	6E	74	65	72	66	61	63	65	2E	6D	73	69	0A	00	Interface.msi
35E53DF0	20	00	00	00	00	00	01	00	18	00	60	C6	87	66	31	8F	`Æ‡f1
35E53E00	D3	01	BA	AB	50	9F	4F	94	D3	01	96	E4	16	77	AA	90	Ó º«PŸO"Ó –ä wª
35E53E10	D3	01	50	4B	05	06	00	00	00	00	83	00	83	00	D6	42	Ó PK ƒ ƒ ÖB
35E53E20	00	00	3C	FB	E4	35	00	00									<ûä5

Does renaming a file extension change the files signature?

File Carving Embedded Files 2

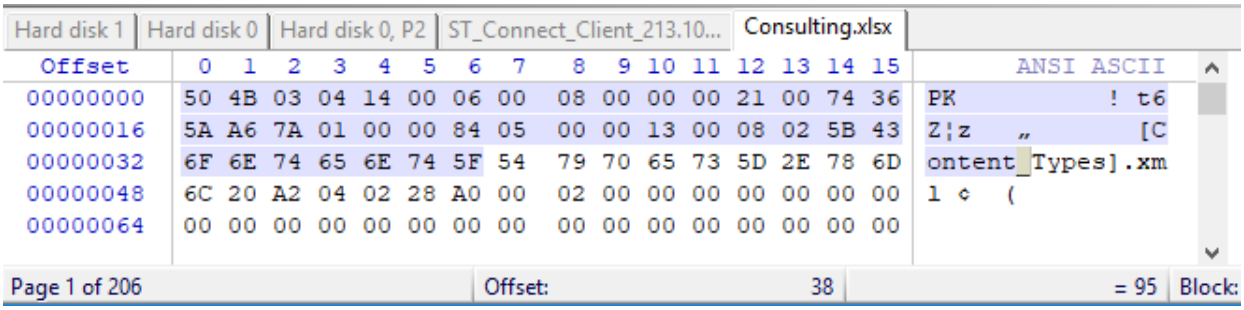
File Type Signatures Search.txt - Notepad

File Edit Format View Help

Description	Extensions	Header	Offset	Footer	Default size	Flags
MS Office 2007+	docx;xlsx;pptx	_Types\]\.xml	38	~14		g

Search for "_Types].xml".

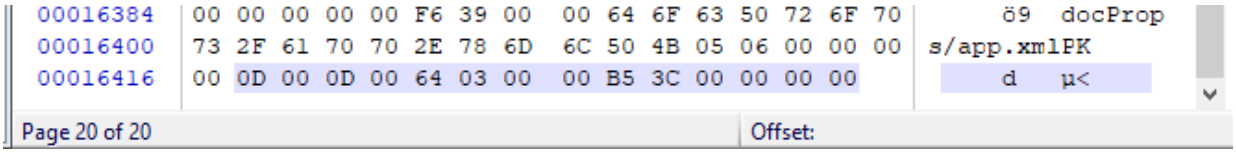
Jump back 38 bytes to find the start of the file. (ZIP header \x50 \x4B \x03 \x04)



Search for the file signature footer data for a ZIP \x50 \x4B \x05 \x06\x00\x00\x00\x00

Jump forward 14 bytes to find the end of the file.

Copy out everything between the start of file and end of file.



Searching Compound Files

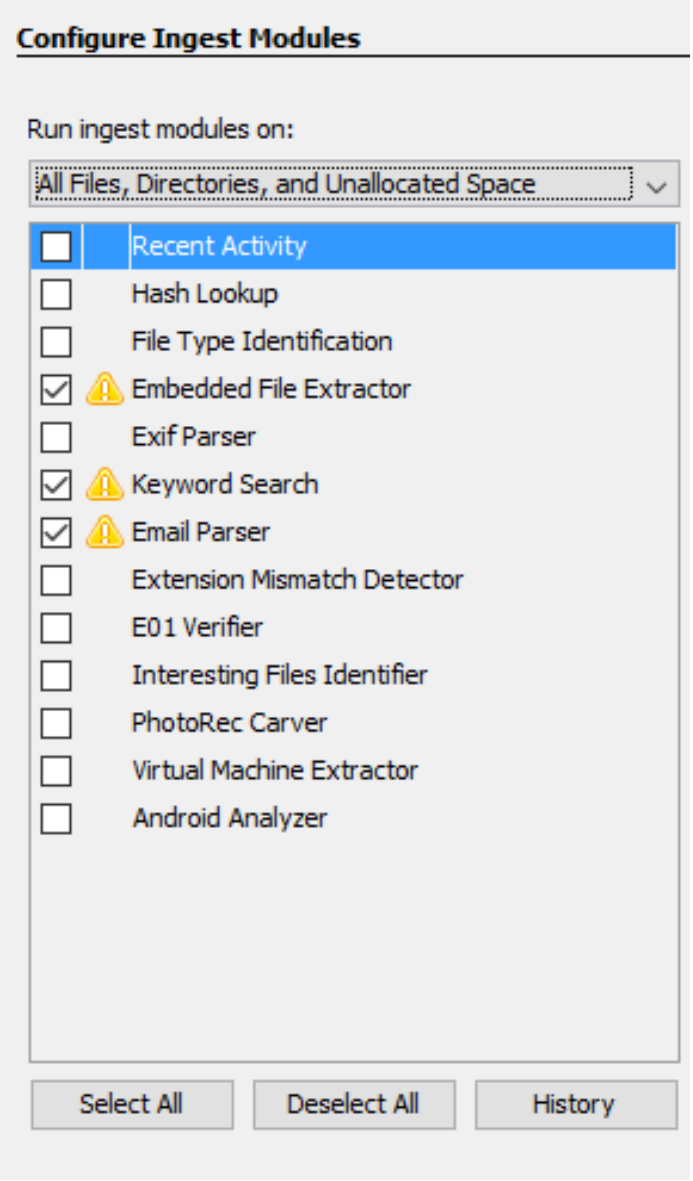
What is a PST file? ZIP file? RAR file?

How can you ensure you're searching all possible emails in a PST file? PST recovery

What isn't searched when using non-forensic search tools? Non-text attachments

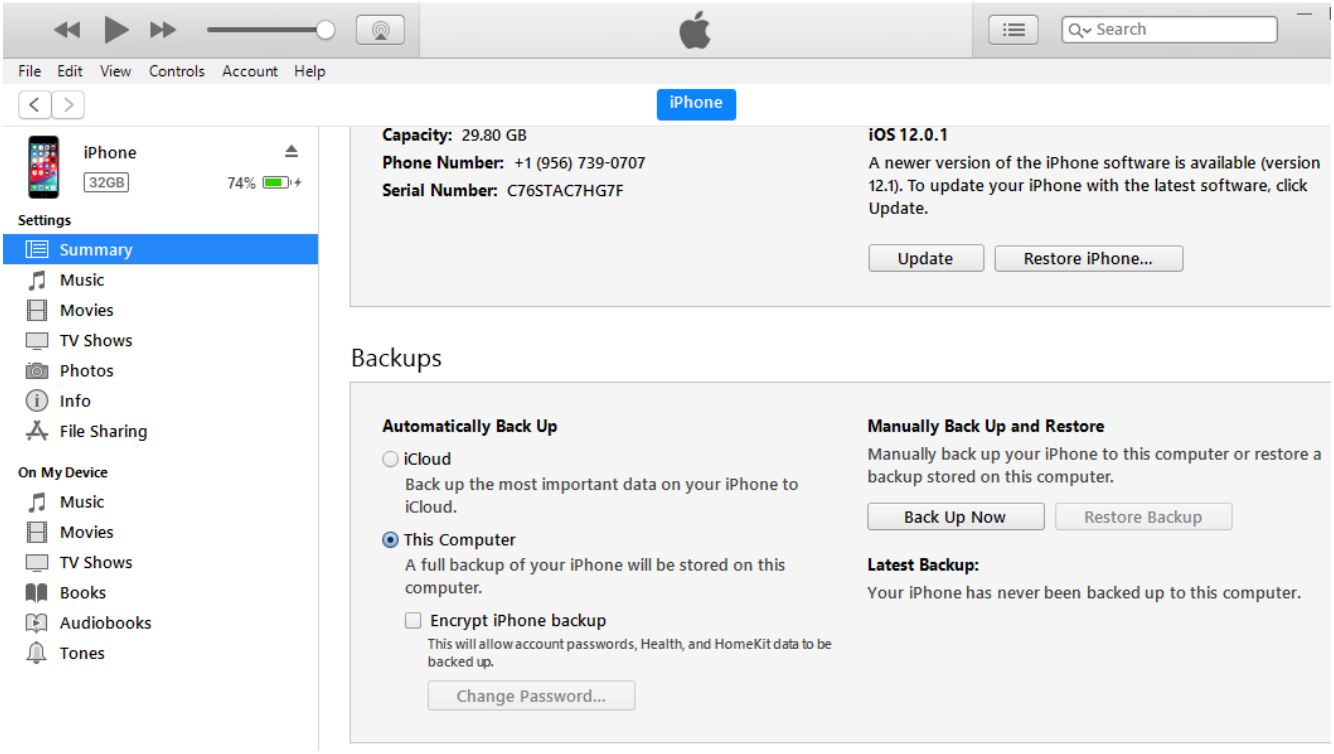
How can you search for text in scanned documents/PDF's? OCR all scanned files.

How can you ensure you're searching all possible data containers in a PST file? Parse email files, extract all embedded files, then run your keyword search. (Scanned files with no embedded text will not be included in the search. In order to include scanned image files in the search, you would need to OCR them prior to searching them.)


Configure Ingest Modules
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Embedded File Extractor
Exif Parser
Keyword Search
Email Parser
Extension Mismatch Detector
E01 Verifier
Interesting Files Identifier
PhotoRec Carver
Virtual Machine Extractor
Android Analyzer
Select All
Deselect All
History

iPhone Backups on a computer

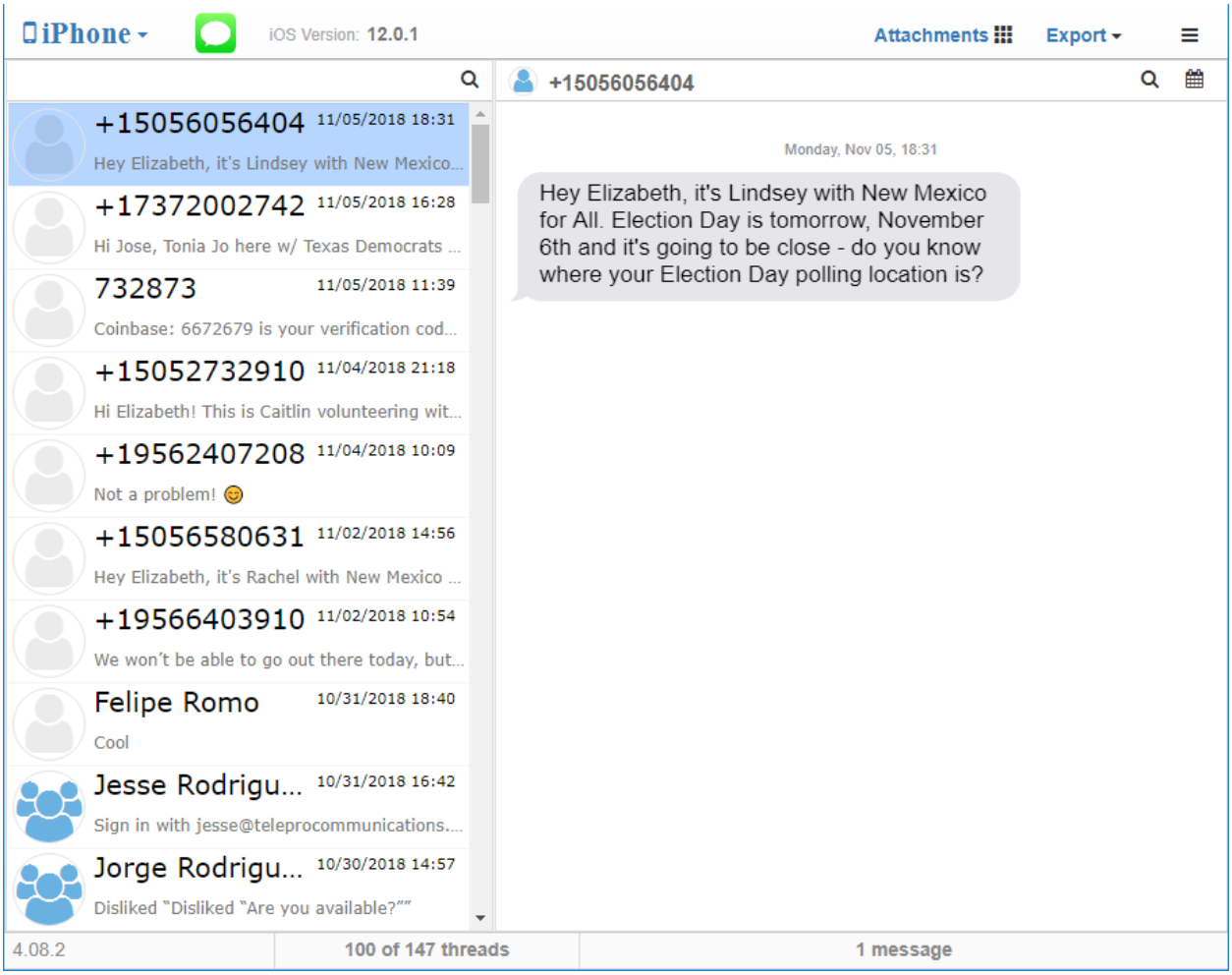
C:\Users\username\AppData\Roaming\Apple Computer\MobileSync\Backup\



What type of information can you extract from an iPhone backup?

Contacts, Call History, Text Messages, WhatsApp Messages, Calendar Items, Notes, Voicemail, Voice Memos, Safari History, Photos, Apps, Raw Files

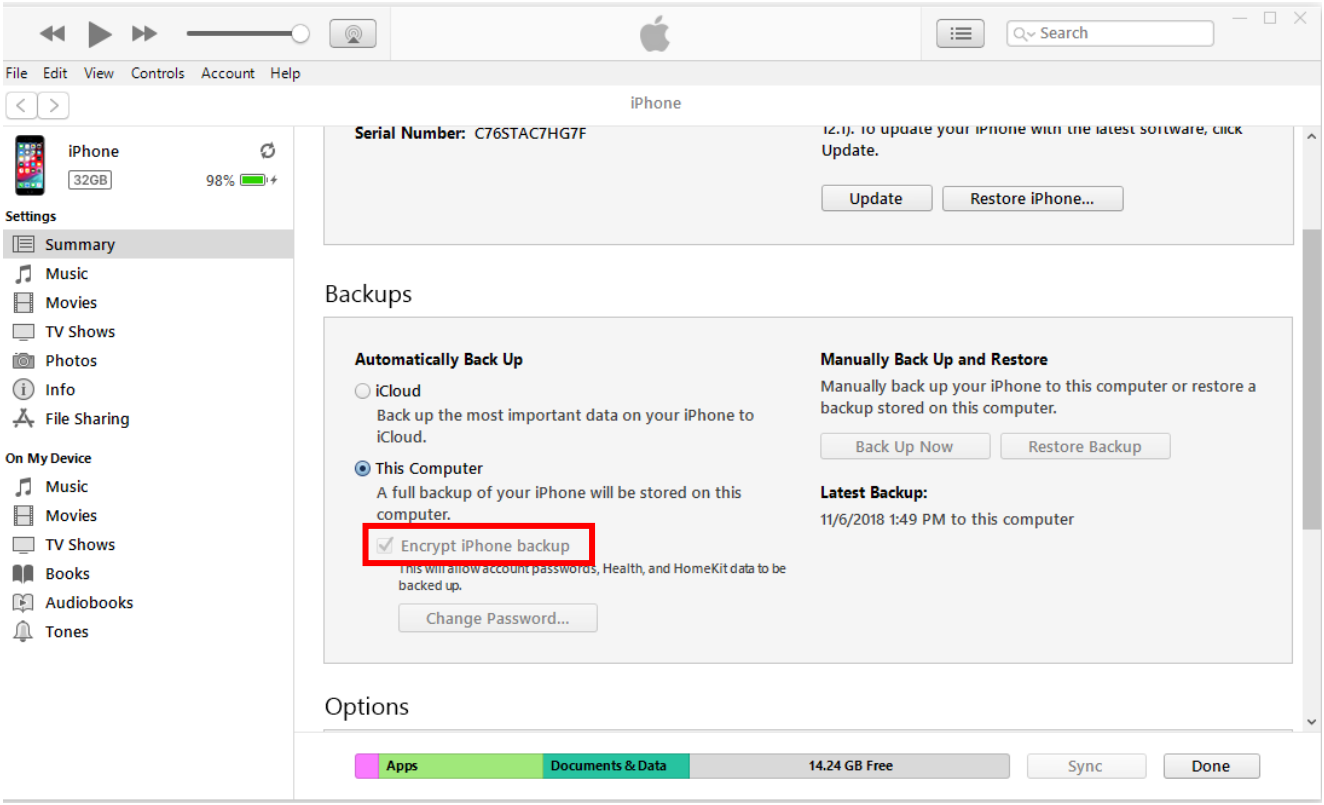
Text messages



What if the iPhone backup is encrypted?

Cracking iPhone Backup Encryption

From iTunes, verify the local iPhone backup is encrypted,



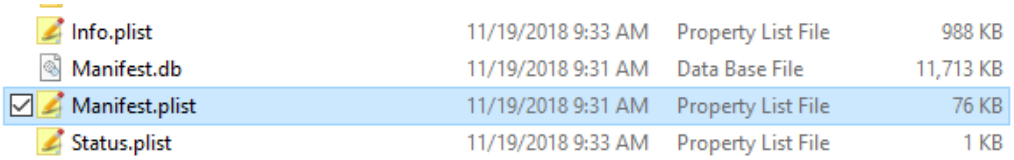
Go the iPhone backup location and locate the manifest.plist file

Manifest.plist location in Windows and Mac

The iPhone Backup location is slightly different depending on your **Windows** version:

- For Windows XP: C:\Documents and Settings\{user_name}\Application Data\Apple Computer\MobileSync\Backup\
- For Windows 10/8/7/Vista: C:\Users\{user_name}\AppData\Roaming\Apple Computer\MobileSync\Backup\
- To browse to see the iPhone backup files, you have to enable Windows Explorer to show hidden files.

No matter what version of **Mac OS X** you are running, iTunes stores your iPhone backup in the same directory:
~/Library/Application Support/MobileSync/Backup/


Info.plist 11/19/2018 9:33 AM Property List File 988 KB
Manifest.db 11/19/2018 9:31 AM Data Base File 11,713 KB
Manifest.plist 11/19/2018 9:31 AM Property List File 76 KB
Status.plist 11/19/2018 9:33 AM Property List File 1 KB

Upload the manifest.plist file and submit

iPhone information extracted from the manifest.plist file

Filename	Version	Current Wordlist	Status	Password	Actions
Manifest.plist	>= 10.0	Basic search	IN PROGRESS	-	

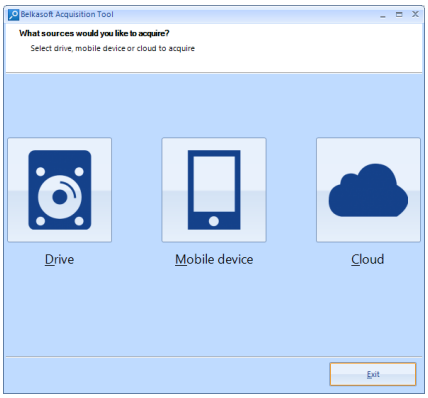
Added date	2018-11-19 16:33:51	Hash	$itunes_backup$*10*ab2dadabab73b26bbb66d16344126236b71f6b354bb4b1...
Deletion date	2019-01-19 *(+2 months)*	File SHA1	ebdbb0980c7d5af5cf702121bf79d3c5d6c3005c
User Note	N/A	File size	77720 bytes
Download original file	Manifest.plist		
Device Name	iPhone	Product Version	12.0.1
Product Type	iPhone9,3	Build Version	16A404
Serial Number	C76STAC7HG7F	Device ID	9e2826e7e071dfe8b8e9dde4b53704877f408f55
Type	application/x-plist	File(s)	
Backup Version	>= 10.0	Salt	a320355f42b8f5358f8b2482cf24ff7af7b58224
Iterations	10000	WPKY	ab2dadabab73b26bbb66d16344126236b71f6b354bb4b13a0e81d680279cbdb5e...
DPIC	10000000	DPSL	4a8b34fef759ddc7466c88ab62989a8a6cbf3dea

What is the benefit of analyzing a backup versus the actual iPhone?

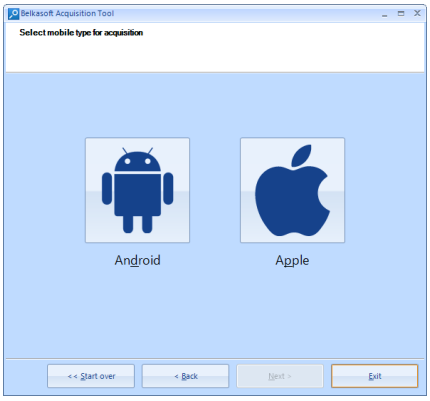
Logical acquisition of an iPhone device

Belkasoft Acquisition Tool - https://belkasoft.com/get

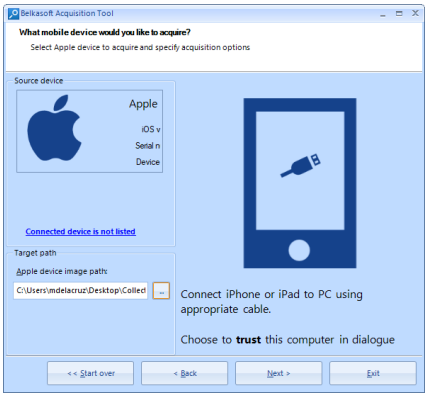
Select Mobile Device



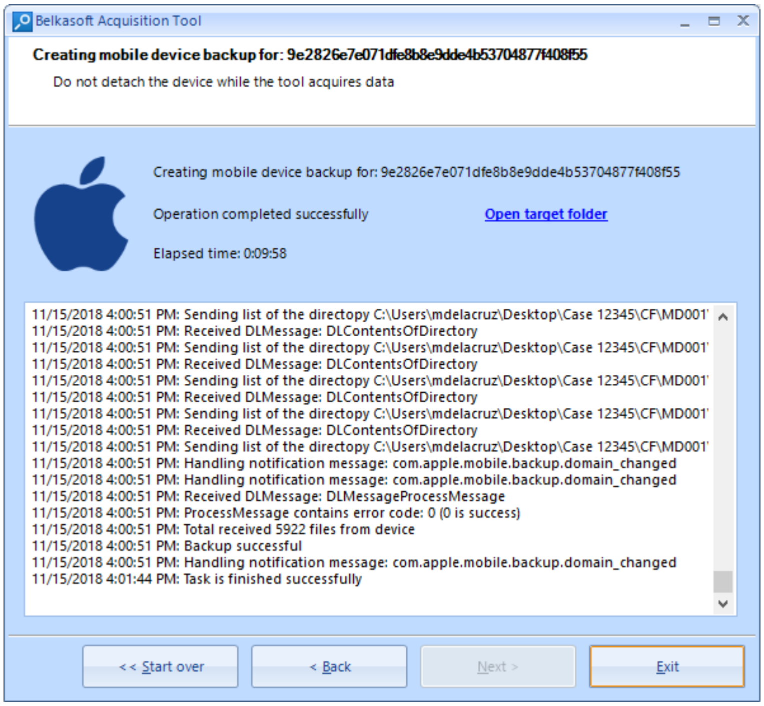
Select Apple



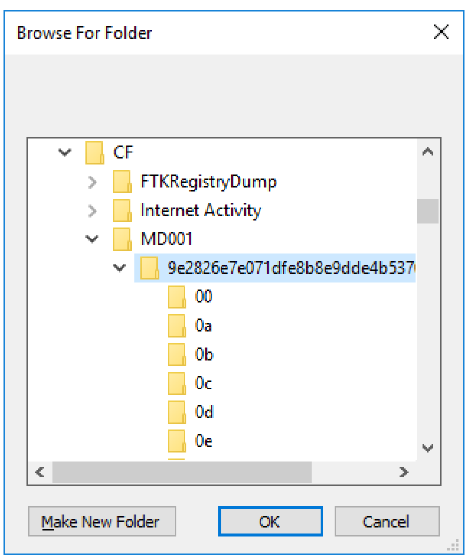
Enter Target Path

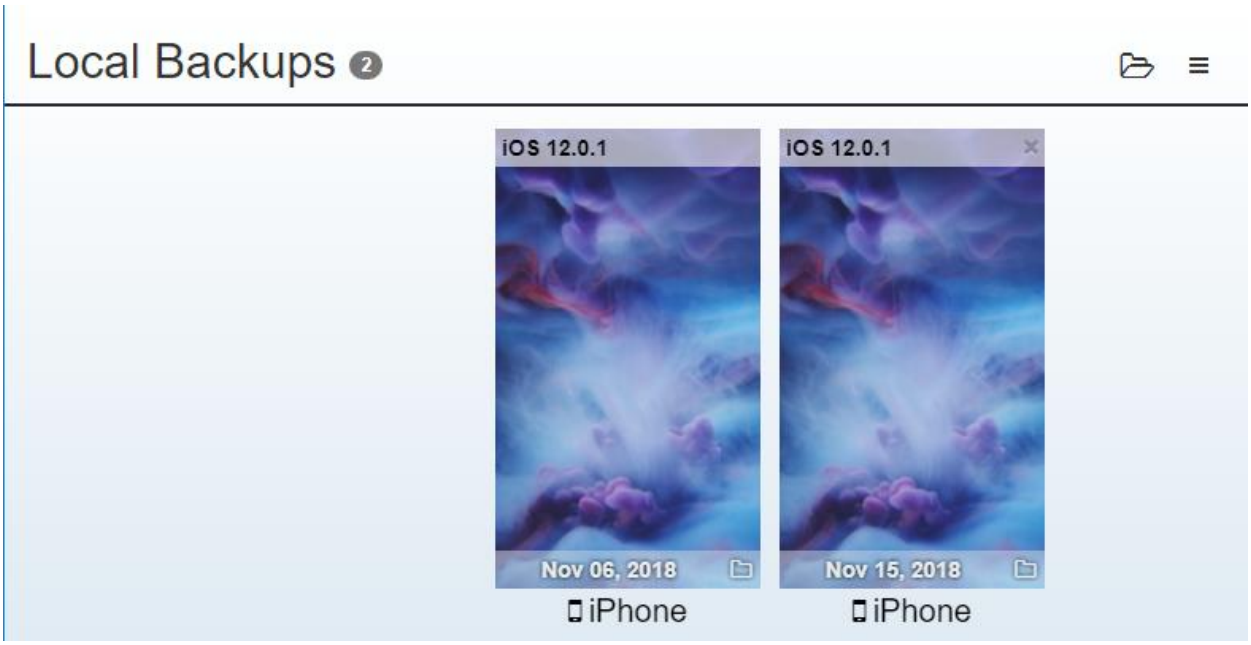


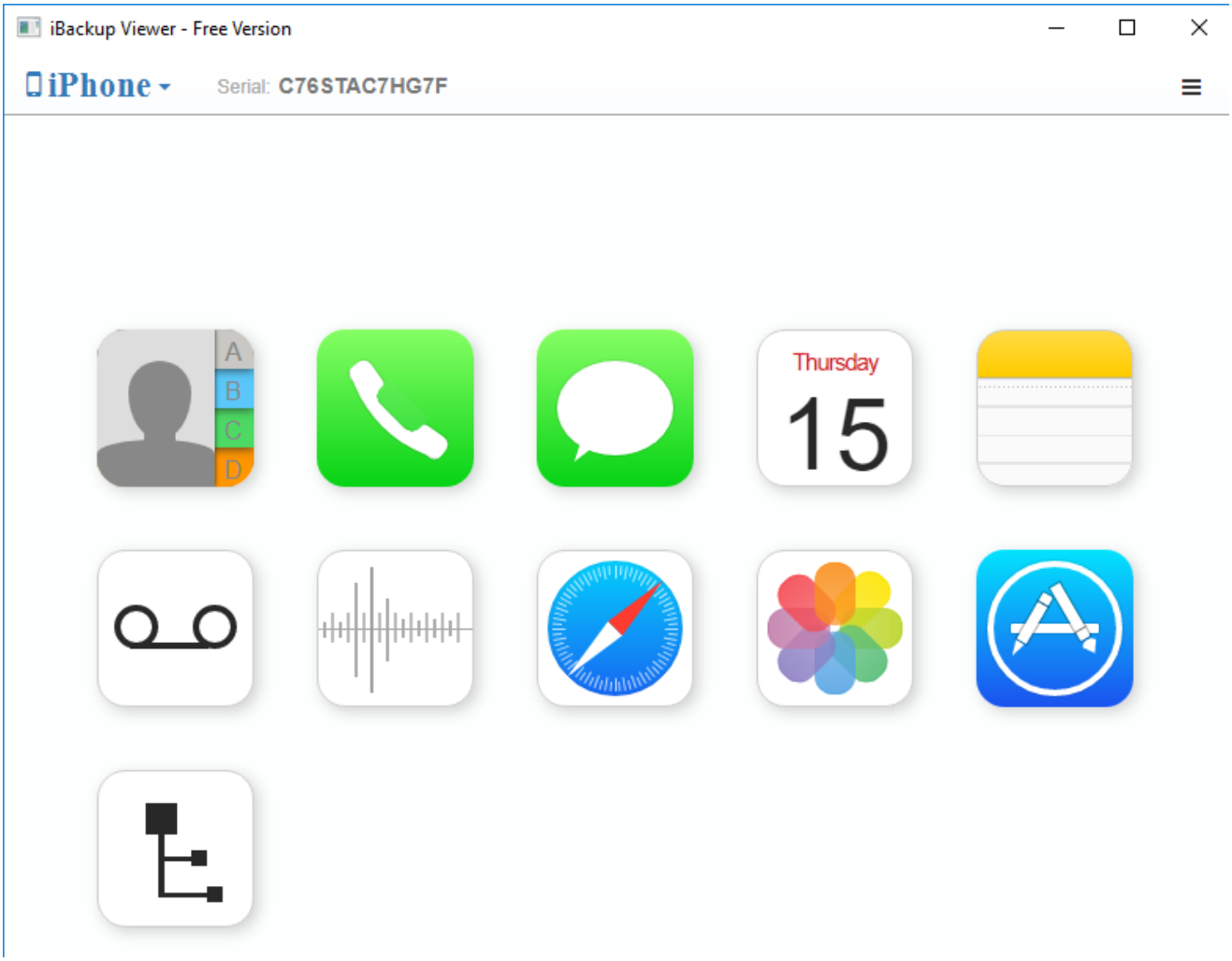
Verify iPhone backup completed successfully



Open iBackup Viewer to parse the iPhone backup created

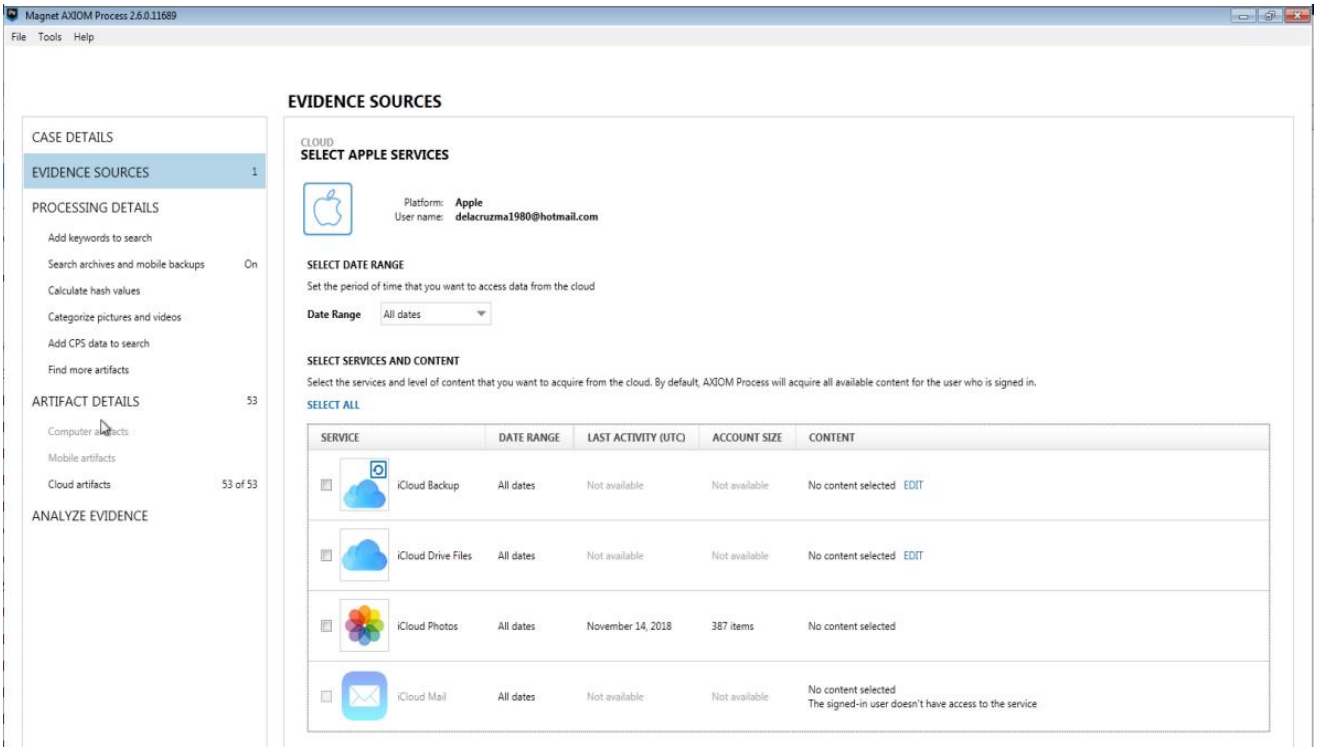



Local Backups 2
iOS 12.0.1
Nov 06, 2018
iPhone
iOS 12.0.1
Nov 15, 2018
iPhone

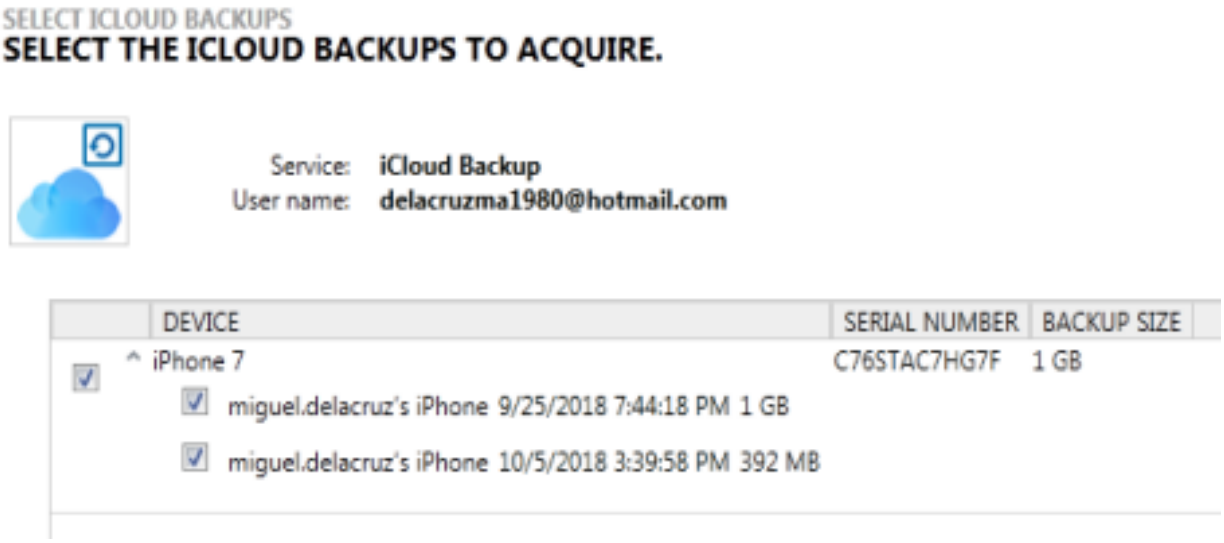

iBackup Viewer - Free Version
iPhone
Serial: C76STAC7HG7F
Thursday
15

What if the iPhone backup is on iCloud?

iCloud Acquisitions with AXIOM



Select the iCloud Backup to acquire

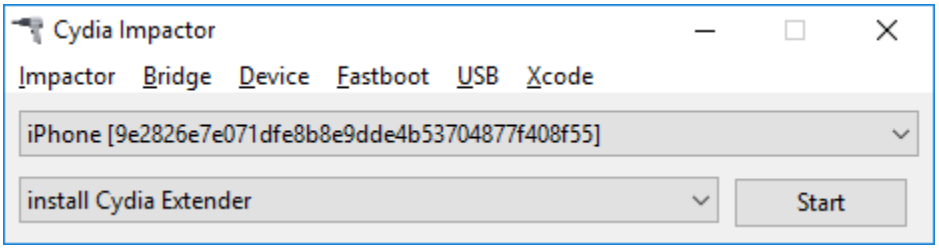


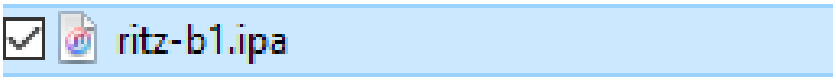
Jailbreaking an iPhone to Collect a Physical Image

Create a backup your iPhone and identify your iOS version.

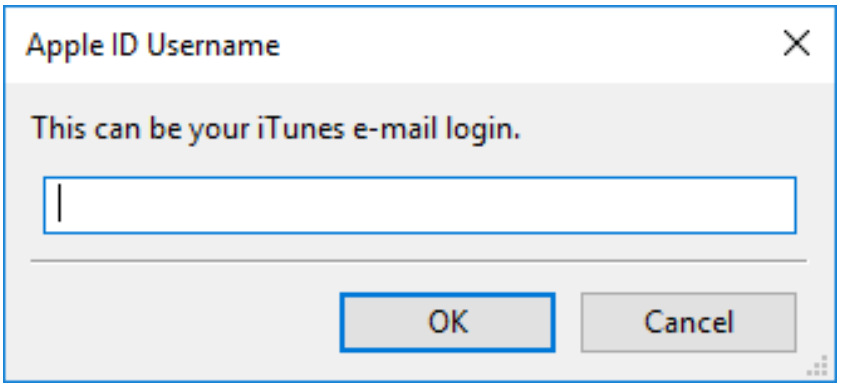
Download Cydia Impactor (http://www.cydiaimpactor.com/) and Ritz IPA (http://pangu8.com/jailbreak/12/ritz-b1.ipa)

Launch Cydia Impactor





Drag Ritz IPA into Cydia Impactor and sign in with iTunes e-mail account

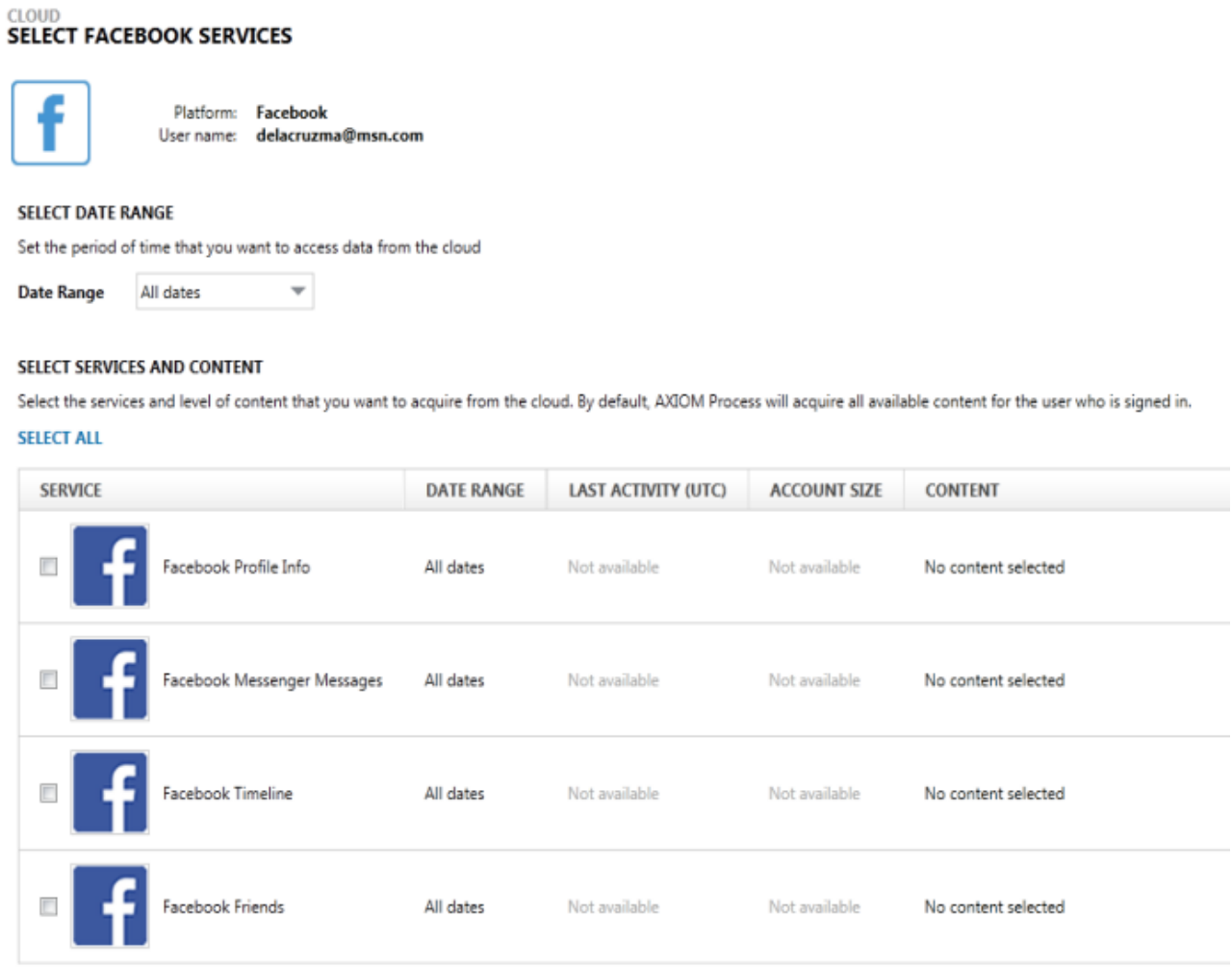


Go to Profiles & Device Management on the iPhone and select the entry in the Develop App section, and Trust the app.

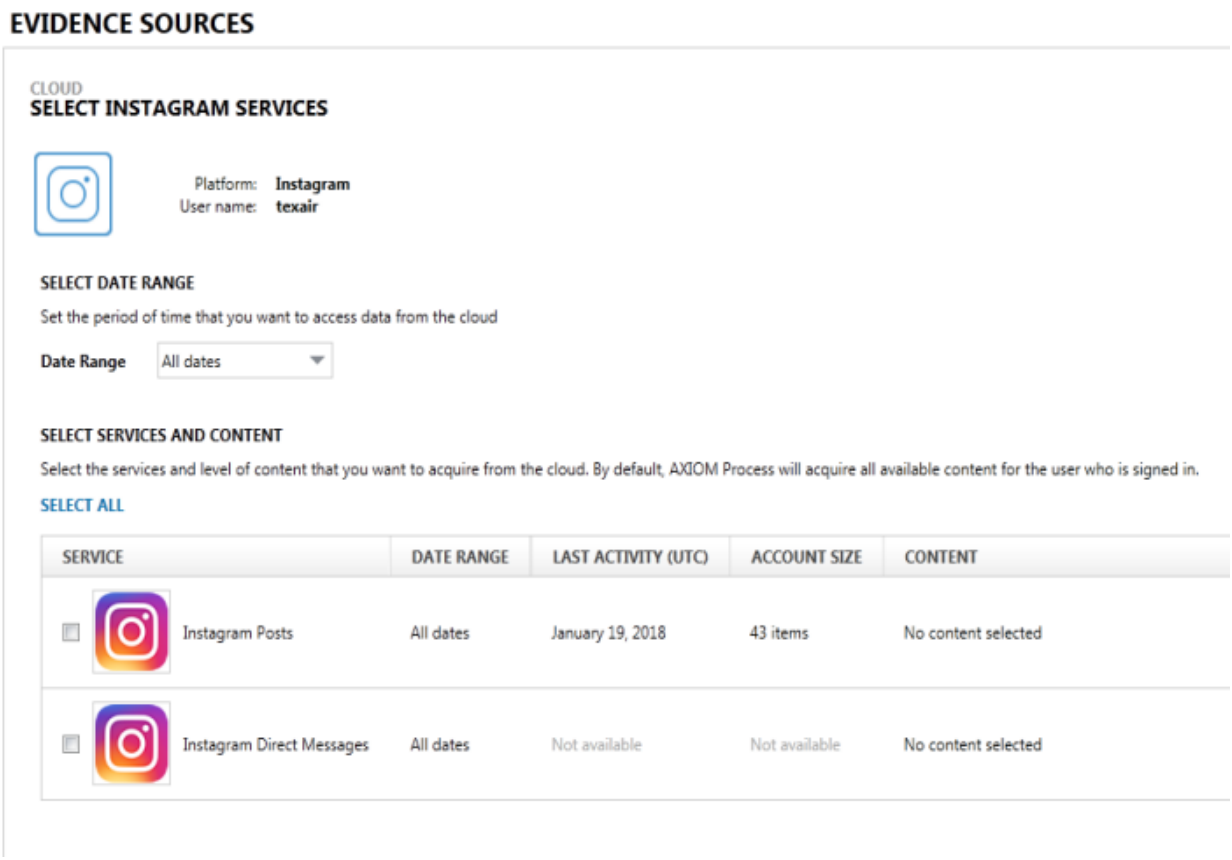
Social Media Acquisitions

Facebook

EVIDENCE SOURCES



Instagram Acquisition



Link Files

What information can you gather from a link file?

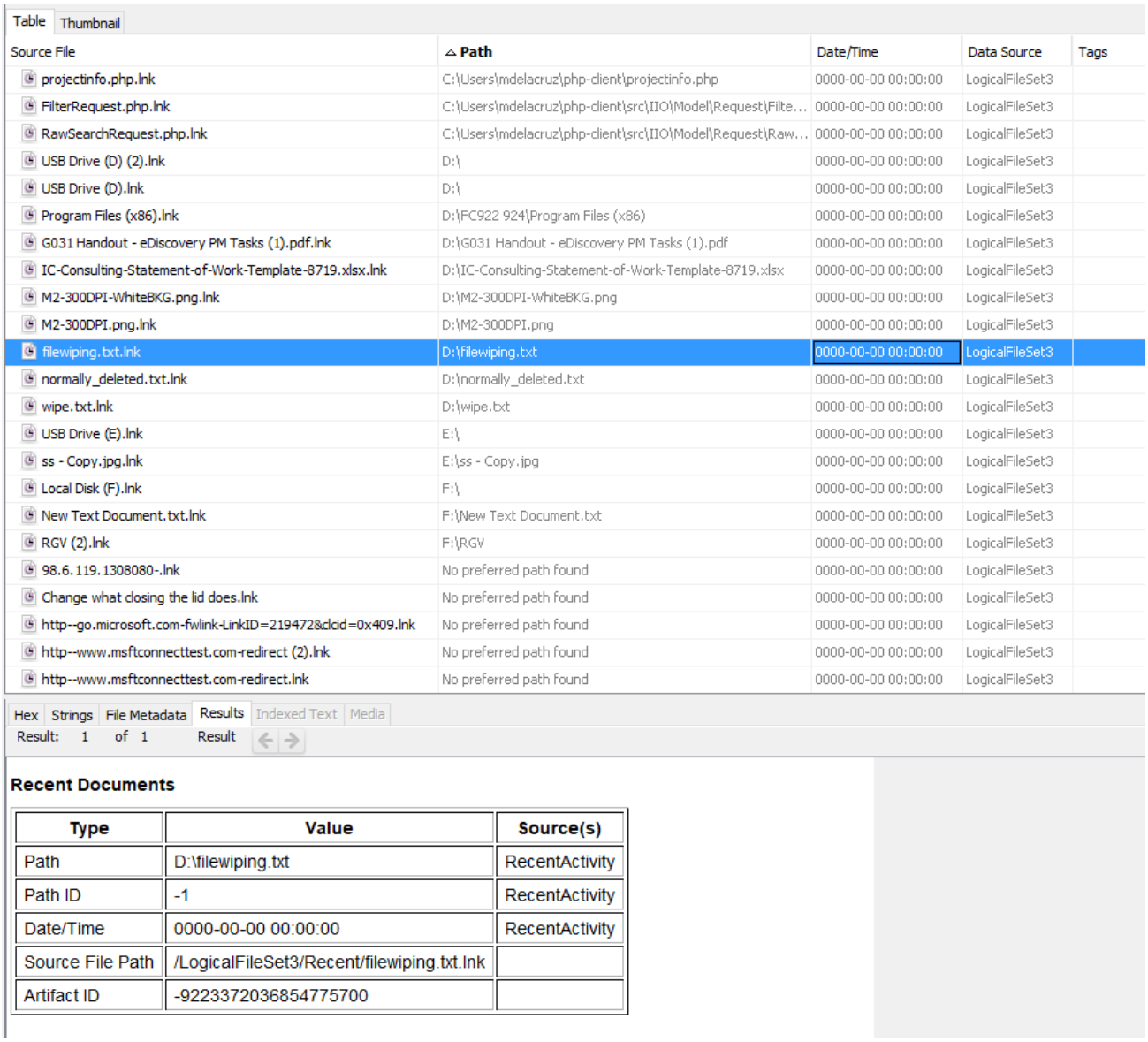


Table | Thumbnail

Source File	Path	Date/Time	Data Source	Tags
projectinfo.php.lnk	C:\Users\mdelacruz\php-client\projectinfo.php	0000-00-00 00:00:00	LogicalFileSet3	
FilterRequest.php.lnk	C:\Users\mdelacruz\php-client\src\IIO\Model\Request\Filte...	0000-00-00 00:00:00	LogicalFileSet3	
RawSearchRequest.php.lnk	C:\Users\mdelacruz\php-client\src\IIO\Model\Request\Raw...	0000-00-00 00:00:00	LogicalFileSet3	
USB Drive (D) (2).lnk	D:\	0000-00-00 00:00:00	LogicalFileSet3	
USB Drive (D).lnk	D:\	0000-00-00 00:00:00	LogicalFileSet3	
Program Files (x86).lnk	D:\FC922 924\Program Files (x86)	0000-00-00 00:00:00	LogicalFileSet3	
G031 Handout - eDiscovery PM Tasks (1).pdf.lnk	D:\G031 Handout - eDiscovery PM Tasks (1).pdf	0000-00-00 00:00:00	LogicalFileSet3	
IC-Consulting-Statement-of-Work-Template-8719.xlsx.lnk	D:\IC-Consulting-Statement-of-Work-Template-8719.xlsx	0000-00-00 00:00:00	LogicalFileSet3	
M2-300DPI-WhiteBKG.png.lnk	D:\M2-300DPI-WhiteBKG.png	0000-00-00 00:00:00	LogicalFileSet3	
M2-300DPI.png.lnk	D:\M2-300DPI.png	0000-00-00 00:00:00	LogicalFileSet3	
filewiping.txt.lnk	D:\filewiping.txt	0000-00-00 00:00:00	LogicalFileSet3	
normally_deleted.txt.lnk	D:\normally_deleted.txt	0000-00-00 00:00:00	LogicalFileSet3	
wipe.txt.lnk	D:\wipe.txt	0000-00-00 00:00:00	LogicalFileSet3	
USB Drive (E).lnk	E:\	0000-00-00 00:00:00	LogicalFileSet3	
ss - Copy.jpg.lnk	E:\ss - Copy.jpg	0000-00-00 00:00:00	LogicalFileSet3	
Local Disk (F).lnk	F:\	0000-00-00 00:00:00	LogicalFileSet3	
New Text Document.txt.lnk	F:\New Text Document.txt	0000-00-00 00:00:00	LogicalFileSet3	
RGV (2).lnk	F:\RGV	0000-00-00 00:00:00	LogicalFileSet3	
98.6.119.1308080-.lnk	No preferred path found	0000-00-00 00:00:00	LogicalFileSet3	
Change what closing the lid does.lnk	No preferred path found	0000-00-00 00:00:00	LogicalFileSet3	
http--go.microsoft.com-fwlink-LinkID=219472&clcid=0x409.lnk	No preferred path found	0000-00-00 00:00:00	LogicalFileSet3	
http--www.msftconnecttest.com-redirect (2).lnk	No preferred path found	0000-00-00 00:00:00	LogicalFileSet3	
http--www.msftconnecttest.com-redirect.lnk	No preferred path found	0000-00-00 00:00:00	LogicalFileSet3	

Hex | Strings | File Metadata | Results | Indexed Text | Media

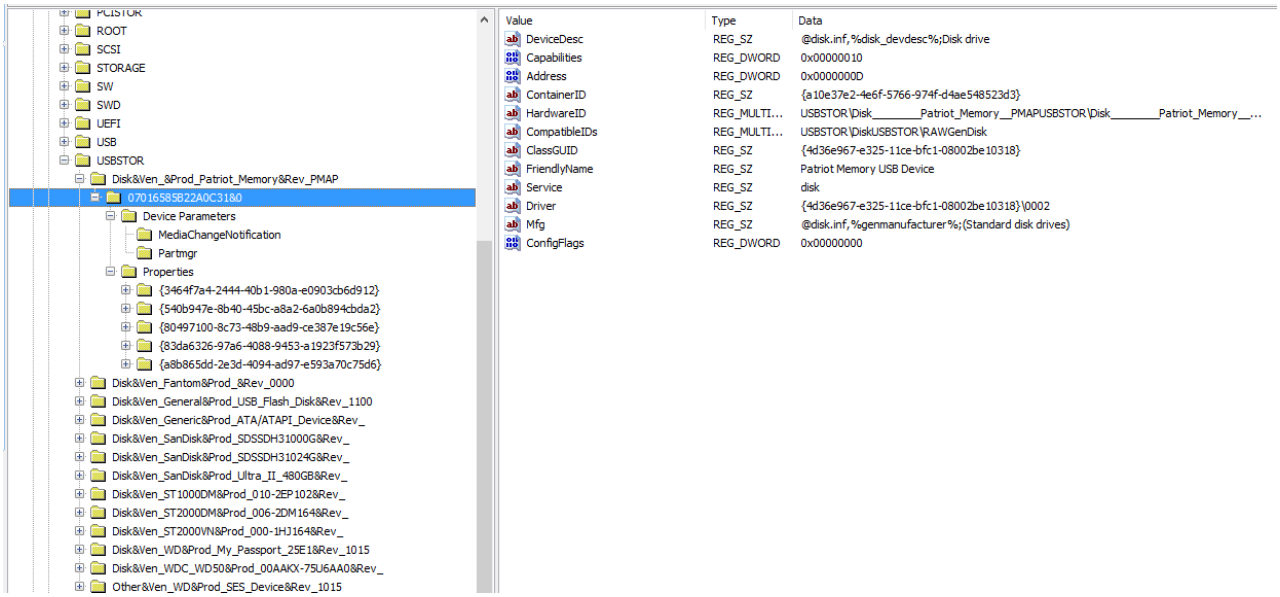
Result: 1 of 1 Result

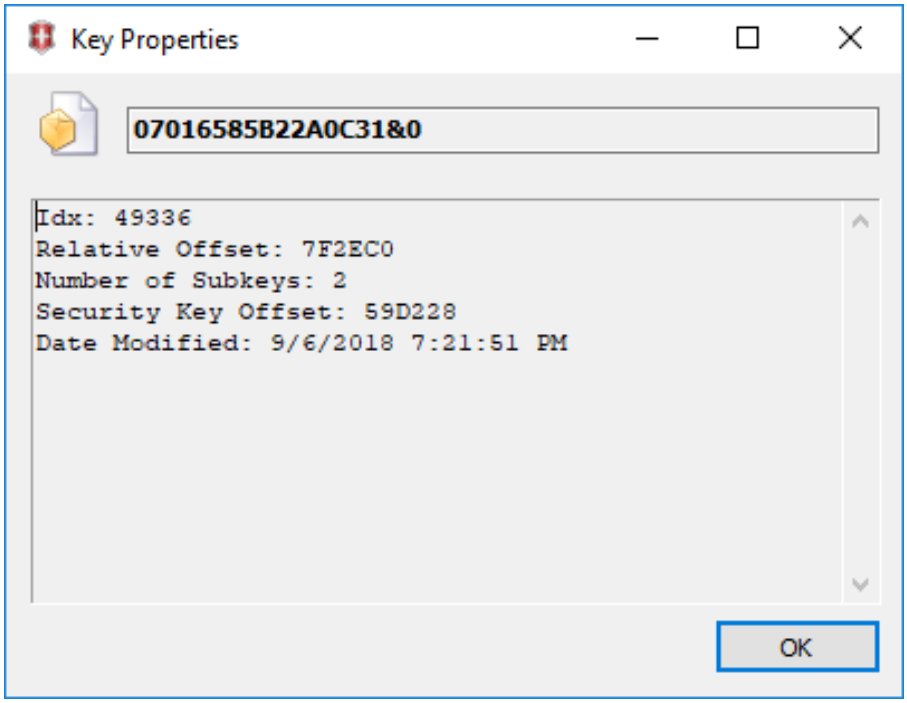
Recent Documents

Type	Value	Source(s)
Path	D:\filewiping.txt	RecentActivity
Path ID	-1	RecentActivity
Date/Time	0000-00-00 00:00:00	RecentActivity
Source File Path	/LogicalFileSet3/Recent/filewiping.txt.lnk	
Artifact ID	-9223372036854775700	

Can you identify how many USB storage devices were attached to a computer?

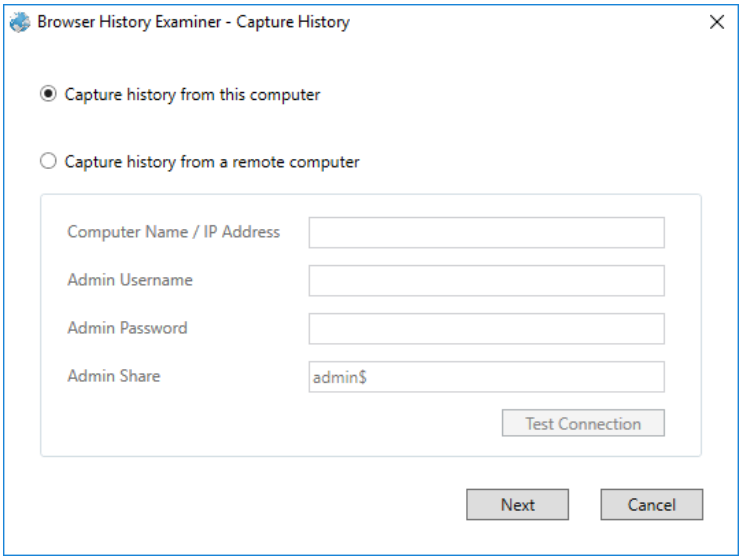
What information is stored in the registry about a USB storage device?

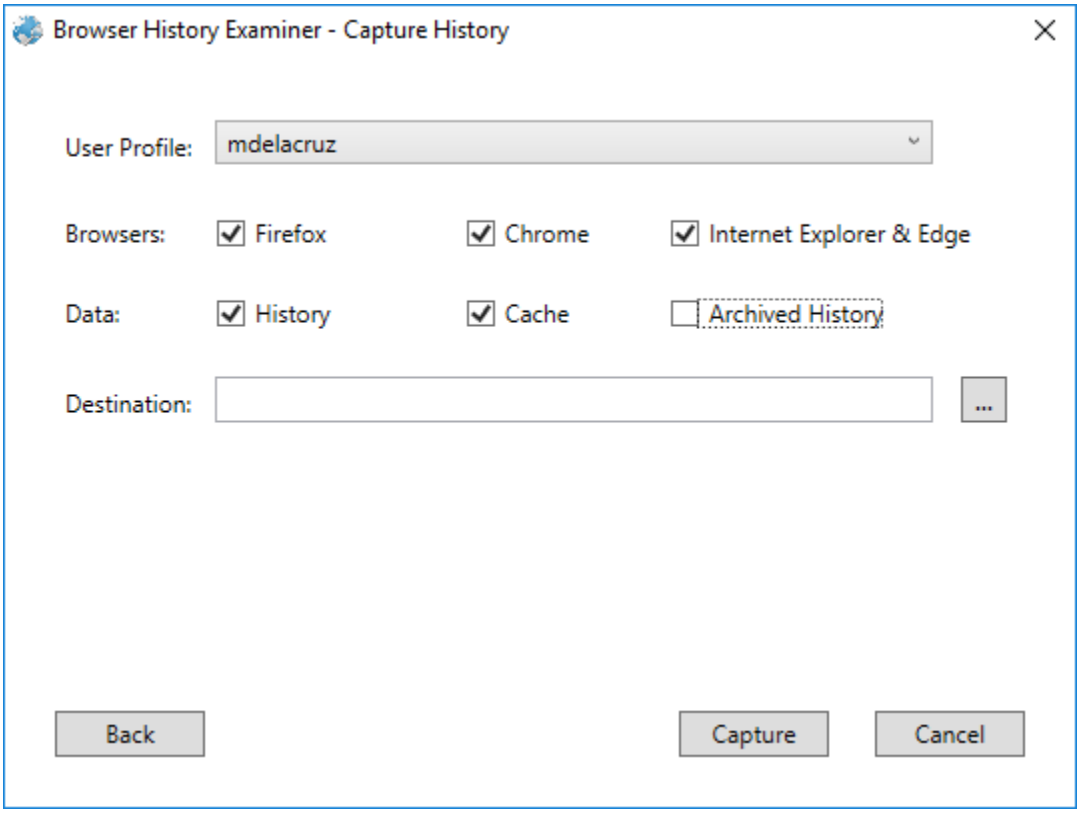




Internet Activity - Browser History Examiner

Capture history from local or remote PC.





Identify login information

Hostname	Origin URL	Submit URL	Username	Date Created	Last Used	Password Changed	Times Used	Web Browser
https://accounts.zoho.com/	https://accounts.zoho.com/signin	https://accounts.zoho.com/signin/a		10/26/2018 19:05:58			0	Chrome
https://m2rgv.indexed.io/	https://m2rgv.indexed.io/	https://m2rgv.indexed.io/		10/17/2018 14:52:00			0	Chrome
https://admin.microsoft.com/	https://admin.microsoft.com/Admi	https://admin.microsoft.com/Admi		10/11/2018 20:21:45			0	Chrome
https://app.indexed.io/	https://app.indexed.io/	https://app.indexed.io/		10/10/2018 17:51:09			0	Chrome
https://www.idrive.com/	https://www.idrive.com/idrive/partr	https://www.idrive.com/idrive/partr		10/05/2018 14:55:41			0	Chrome
https://login.microsoftonline.com/	https://login.microsoftonline.com/c	https://login.microsoftonline.com/c		10/03/2018 17:25:21			0	Chrome
https://accounts.google.com/	https://accounts.google.com/Servic	https://accounts.google.com/signir	jacklyn@teleprocommunications.cc	09/10/2018 20:43:39			0	Chrome
https://sso.godaddy.com/	https://sso.godaddy.com/	https://account.godaddy.com/secu	45308765	08/30/2018 21:22:28			1	Chrome
https://sso.godaddy.com/	https://sso.godaddy.com/	https://sso.godaddy.com/	45308765	08/30/2018 21:22:28			1	Chrome
https://on.spiceworks.com/	https://on.spiceworks.com/sign_in	https://on.spiceworks.com/sessions	michael@safeguardrgv.com	08/28/2018 22:22:54			9	Chrome
https://on.spiceworks.com/	https://on.spiceworks.com/sign_in	https://on.spiceworks.com/sessions	mich 45308765 gv.com	08/27/2018 16:20:52			14	Chrome
https://login.microsoftonline.com/	https://login.microsoftonline.com/c	https://login.microsoftonline.com/c	telepro@texaircompany.com	08/13/2018 14:25:37			13	Chrome
https://accounts.google.com/	https://accounts.google.com/signir	https://accounts.google.com/signir	michael@teleprocommunications.c	04/06/2018 15:01:23			0	Chrome
https://www.tradingview.com/	https://www.tradingview.com/	https://www.tradingview.com/accou	delacruzma	03/07/2018 14:20:52			0	Chrome
https://myturbotax.intuit.com/	https://myturbotax.intuit.com/	https://myturbotax.intuit.com/hom	delacruzma	03/06/2018 18:03:57			3	Chrome
https://on.spiceworks.com/	https://on.spiceworks.com/sessions	https://on.spiceworks.com/sessions	michael@teleprocommunications.c	03/06/2018 17:56:27			1	Chrome
https://login.microsoftonline.com/	https://login.microsoftonline.com/c	https://login.microsoftonline.com/c	rolando@longoriaselectric.com	02/19/2018 17:18:51			2	Chrome
https://login.microsoftonline.com/	https://login.microsoftonline.com/c	https://login.microsoftonline.com/c	texair@texaircompany.com	08/10/2017 15:50:20			3	Chrome
https://login.shoretel.com/	https://login.shoretel.com/ShoreTel	https://login.shoretel.com/ShoreTel		06/27/2017 18:34:50			0	Chrome

Identify email addresses

Last Used	Email Address	Domain	Source	Web Browser
11/08/2018 17:31:18	michael@teleprocommunications.com	charteruc.webex.com	Website Visit	Edge
11/07/2018 21:08:54	michael@teleprocommunications.com	demo.passware.com	Website Visit	Edge
11/06/2018 21:17:13	michael@teleprocommunications.com	outlook.office.com	Website Visit	Chrome
11/06/2018 20:49:30	michael@teleprocommunications.com	login.microsoftonline.com	Website Visit	Edge
11/06/2018 15:53:40	admin@teleprocommunications.com	outlook.office.com	Session Tab	Chrome
11/06/2018 15:50:29	admin@teleprocommunications.com	accounts.google.com	Form History	Chrome
11/05/2018 15:11:15	michael@teleprocommunications.com	portal.office.com	Website Visit	Edge
11/05/2018 15:11:02	michael@teleprocommunications.com	outlook.office365.com	Website Visit	Edge
11/01/2018 19:06:49	telepro@texaircompany.com	login.microsoftonline.com	Website Visit	Edge
11/01/2018 15:40:52	telepro@texaircompany.com	outlook.office365.com	Website Visit	Edge
11/01/2018 14:52:49	telepro@texaircompany.com	login.microsoftonline.com	Website Visit	Chrome
10/30/2018 16:57:44	marketing@safeguardrgv.com	outlook.office.com	Website Visit	Chrome
10/26/2018 22:26:58	michael@m2rgv.com	mail.zoho.com	Website Visit	Chrome
10/26/2018 05:39:28	michael@teleprocommunications.com	login.microsoftonline.com	Website Visit	Chrome
10/25/2018 15:45:34	telepro@texaircompany.com	portal.office.com	Website Visit	Edge
10/25/2018 15:25:51	telepro@texaircompany.com.pst		Website Visit	Internet Explorer
10/24/2018 16:57:57	jesse@teleprocommunications.com	login.microsoftonline.com	Website Visit	Edge
10/24/2018 16:55:17	jesse@teleprocommunications.com	office.com	Website Visit	Edge
10/24/2018 16:33:51	jesse@carnesirgv.com	login.microsoftonline.com	Website Visit	Edge
10/24/2018 16:15:45	jesse@safeguardrgv.com	login.microsoftonline.com	Website Visit	Edge
10/23/2018 21:25:43	Raymundo@valdezmonarrez.onmicrosoft.com	portal.office.com	Website Visit	Edge
10/23/2018 21:25:42	Raymundo@valdezmonarrez.onmicrosoft.com	outlook.office365.com	Website Visit	Edge
10/23/2018 21:24:38	Raymundo@valdezmonarrez.onmicrosoft.com	login.microsoftonline.com	Website Visit	Edge
10/23/2018 21:15:35	raymundo@valdezmonarrez.com	login.live.com	Website Visit	Edge
10/23/2018 17:40:31	michael@teleprocommunications.com	accounts.google.com	Form History	Chrome

Identify web searches conducted

11/09/2018 14:32:26	file hashing	Google	https://www.google.com/search?ei=5_zhW8PICZLUtQW_q4_gAQ&q=file+hashing&	Website Visit	Edge
11/08/2018 22:25:20	255.255.255.x 16	Google	https://www.google.com/search?ei=f7bkW7ScD4uwjwShlImACw&q=255.255.255.x·	Website Visit	Edge
11/08/2018 22:25:20	255.255.255.x 16	Google	https://www.google.com/search?ei=f7bkW7ScD4uwjwShlImACw&q=255.255.255.x·	Website Visit	Edge
11/08/2018 22:25:07	255.255.255.x	Google	https://www.google.com/search?ei=zrTkW56-O5DvjwSX15uIAQ&q=255.255.255.x&	Website Visit	Edge
11/08/2018 22:25:07	255.255.255.x	Google	https://www.google.com/search?ei=zrTkW56-O5DvjwSX15uIAQ&q=255.255.255.x&	Website Visit	Edge
11/08/2018 22:21:41	spacex brownsville	Google	https://www.google.com/search?ei=U6nkW8C7JezcjwSExI64CQ&q=spacex+brown:	Website Visit	Edge

Identify downloaded files

URL	Local Path	State	Start Time	End Time	Bytes Downloaded	Total Bytes	Web
blob:https://portal.azure.com/59512b65-326c-43de-bb6f-4	C:\Users\mdelacruz\Downloads\SignIns_2018-10-29_2018-11-05.csv	Complete	11/05/2018 14:15:26	11/05/2018 14:15:27	288695	288695	Chro
https://protection.office.com/api/UnifiedAuditLog/Export	C:\Users\mdelacruz\Downloads\AuditLog_2018-09-01_2018-09-05.csv	Complete	11/01/2018 15:39:16	11/01/2018 15:39:30	701919	701919	Chro
blob:https://protection.office.com/1290a514-b8ea-44c1-85	C:\Users\mdelacruz\Downloads\UnifiedAuditLog (4).csv	Complete	10/31/2018 21:51:35	10/31/2018 21:51:35	42140	42140	Chro
blob:https://protection.office.com/95e793a7-4711-41bd-8	C:\Users\mdelacruz\Downloads\UnifiedAuditLog (3).csv	Complete	10/31/2018 21:39:23	10/31/2018 21:39:23	45250	45250	Chro
blob:https://protection.office.com/fb263b93-ba84-4c94-94	C:\Users\mdelacruz\Downloads\UnifiedAuditLog (2).csv	Complete	10/31/2018 15:45:43	10/31/2018 15:45:44	42273	42273	Chro
blob:https://protection.office.com/85b750e0-8ec5-4872-8	C:\Users\mdelacruz\Downloads\UnifiedAuditLog (1).csv	Complete	10/30/2018 15:28:50	10/30/2018 15:28:51	17246	17246	Chro
blob:https://protection.office.com/72	blob:https://protection.office.com/fb263b93-ba84-4c94-9496-dfae0d65dda4	Complete	10/30/2018 15:28:03	10/30/2018 15:28:04	4806	4806	Chro
blob:https://portal.azure.com/21b45723-6527-4ca1-a657-	C:\Users\mdelacruz\Downloads\SignIns_2018-10-22_2018-10-29.csv	Complete	10/29/2018 13:18:40	10/29/2018 13:18:40	669995	669995	Chro
blob:https://portal.azure.com/b67fc4d6-00f2-4564-bbd5-0	C:\Users\mdelacruz\Downloads\SignIns_2018-10-15_2018-10-22.csv	Complete	10/22/2018 15:36:17	10/22/2018 15:36:31	764019	764019	Chro
blob:https://portal.azure.com/0c96a4f1-4102-4d57-b292-f	C:\Users\mdelacruz\Downloads\SignIns_2018-10-15_2018-10-22.csv	Complete	10/22/2018 15:24:03	10/22/2018 15:24:04	760587	760587	Chro
https://iio-projects.s3.amazonaws.com/project-5bbb8149e	C:\Users\mdelacruz\Downloads\Resource_Report_10_16_2018_@_14_8_12.csv	Complete	10/16/2018 20:09:43	10/16/2018 20:09:44	197789	197789	Chro
https://iio-projects.s3.amazonaws.com/project-5bbb8149e	C:\Users\mdelacruz\Downloads\Tag_Report_10_16_2018_@_12_47_36.zip	Complete	10/16/2018 18:47:55	10/16/2018 18:47:56	529	529	Chro
file:///C:/Users/mdelacruz/Desktop/Custodian/ZIP/ZIP(Pass	C:\Users\mdelacruz\Downloads\ZIP(Password).zip	Complete	10/10/2018 22:11:59	10/10/2018 22:12:01	221217	221217	Chro
http://www.idrive.com/downloads/IDriveWinSetup.exe	C:\Users\mdelacruz\Downloads\IDriveWinSetup.exe	Complete	10/05/2018 15:08:06	10/05/2018 15:08:19	24818160	24818160	Chro
http://www.idrive.com/reseller/marketing_kit/application_s	C:\Users\mdelacruz\Downloads\application_screenshots.zip	Complete	10/05/2018 14:45:42	10/05/2018 14:45:45	2679821	2679821	Chro
https://statics.teams.microsoft.com/production-windows-x	C:\Users\mdelacruz\Downloads\Teams_windows_x64.exe	Complete	10/04/2018 17:20:50	10/04/2018 17:21:37	93214256	93214256	Chro
https://msproduct.download.microsoft.com/pr/SW_DVD9_	C:\Users\mdelacruz\Downloads\SW_DVD9_Win_Server_STD_CORE_2016_64Bit	Complete	09/06/2018 19:18:36	09/06/2018 21:33:52	6003804160	6003804160	Chro
https://www.microsoft.com/Licensing/servicecenter/Assets		Cancelled	09/06/2018 19:17:43		0	1558	Chro
https://on.spiceworks.com/api/attachments/eyJfcmFpbHM	C:\Users\mdelacruz\Downloads\Customer_Signoff_Form use on all navco ticke	Complete	09/04/2018 16:44:17	09/04/2018 16:44:20	103581	103581	Chro
https://on.spiceworks.com/api/attachments/eyJfcmFpbHM	C:\Users\mdelacruz\Downloads\Customer Signoff Form (1).pdf	Complete	09/04/2018 16:43:48	09/04/2018 16:43:52	36420	36420	Chro
https://on.spiceworks.com/api/attachments/eyJfcmFpbHM	C:\Users\mdelacruz\Downloads\TELEPRO WO 9974 - ALAMO.pdf	Complete	09/04/2018 16:43:06	09/04/2018 16:43:11	343383	343383	Chro
https://on.spiceworks.com/api/attachments/eyJfcmFpbHM	C:\Users\mdelacruz\Downloads\TELEPRO WO 9974.pdf	Complete	09/04/2018 16:42:35	09/04/2018 16:42:43	306272	306272	Chro
https://on.spiceworks.com/api/attachments/eyJfcmFpbHM	C:\Users\mdelacruz\Downloads\TELEPRO WO 9974.pdf	Other	09/04/2018 16:42:13		0	306272	Chro
file:///C:/Users/mdelacruz/Downloads/NAVCO%20SIGN%2	P:\Consulting\NAVCO SIGN OFF SHEET CHEDDARS WO 9966.pdf	Complete	08/31/2018 19:04:48	08/31/2018 19:05:04	368254	368254	Chro
https://on.spiceworks.com/api/attachments/eyJfcmFpbHM	C:\Users\mdelacruz\Downloads\City of Donna-WO9963 - Copy (1).pdf	Complete	08/31/2018 17:54:59	08/31/2018 17:55:05	528633	528633	Chro

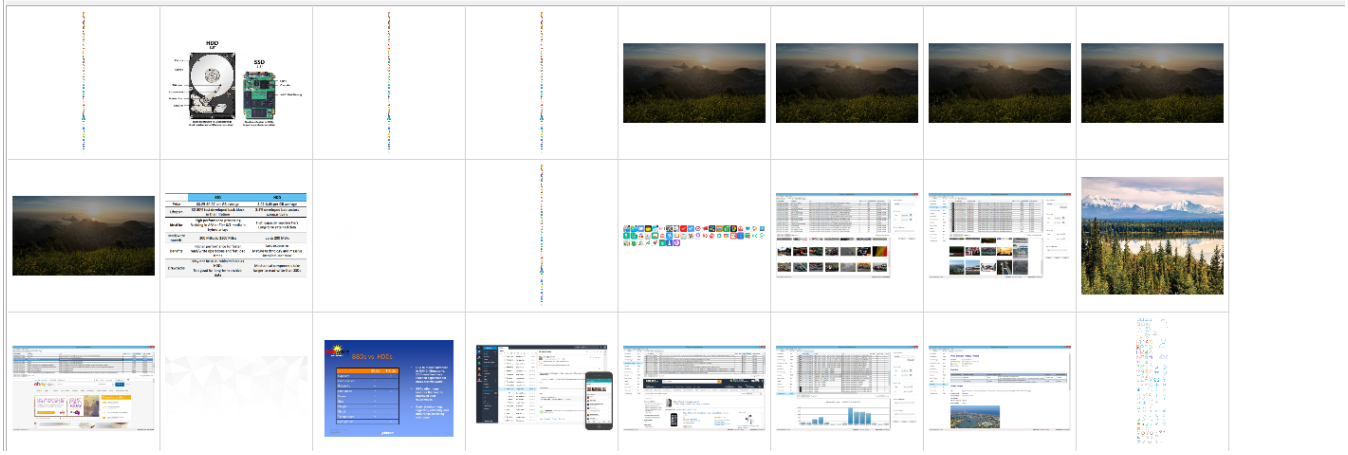
Identify Form History data

Field Name	Value	First Used	Calculated Domain (First Used)
identifier	admin@teleprocommunications.com	11/06/2018 15:50:29	accounts.google.com
query	68.201.174.232	10/29/2018 13:37:10	
query	172.58.109.214	10/29/2018 13:36:53	iplocation.net
query	2607:fb90:5cb1:93de:7d10:ec6b:23c7:ef6f	10/29/2018 13:32:27	iplocation.net
query	25.169.19.142	10/29/2018 13:32:00	iplocation.net
query	172.58.27.67	10/29/2018 13:30:28	iplocation.net
identifier	michael@teleprocommunications.com	10/23/2018 17:40:31	accounts.google.com
query	indexed	10/23/2018 17:16:19	
name	Resource Report 10/16/2018 @ 14:8:12	10/16/2018 20:08:21	
name	Tag Report 10/16/2018 @ 12:47:36	10/16/2018 18:47:51	
password	Ten[redacted]	10/10/2018 22:24:44	
name	Custodian4	10/10/2018 17:55:39	
last_name	De La Cruz	10/05/2018 15:05:41	
llcType	S	10/05/2018 14:43:13	idrive.com
ssn1	[redacted]	10/05/2018 14:43:13	idrive.com
ein1	83	10/05/2018 14:43:13	idrive.com
ein2	1954120	10/05/2018 14:43:13	idrive.com
signature	Miguel De La Cruz	10/05/2018 14:43:13	idrive.com
paddressW9	723 S J St	10/05/2018 14:58:20	idrive.com
email	michael@m2rgv.com	10/05/2018 14:42:12	idrive.com
pCompanyName	M2 Consulting Services, LLC	10/05/2018 14:42:12	idrive.com
city	McAllen	10/05/2018 14:42:12	idrive.com
others_info	Google	10/05/2018 14:42:12	idrive.com
paddress	723 S J St	10/05/2018 14:57:56	idrive.com
identifier	xerox@teleprocommunications.com	09/18/2018 18:14:27	accounts.google.com

Identify cached images from websites

	Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
		image/png	https://css.zohostatic.com/zohoone/20180910_1787408/zhome/images/product-logos/product-icons-128.png		763353	Chrome
		image/png	https://www.backblaze.com/blog/wp-content/uploads/2018/03/hdd_vs_ssd_bz.png	1	671511	Internet Explorer
		image/png	https://css.zohostatic.com/zohoone/20180910_1787408/zhome/images/product-logos/product-icons-96.png		522745	Chrome
		image/png	https://css.zohostatic.com/zohoone/20180910_1787408/zhome/images/product-logos/product-icons-64.png		299145	Chrome
		image/jpeg	https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8233.22/content/images/backgrounds/0.jpg?x=a5dbd4393ff6a725c7e62b61df7e72f0		283351	Chrome
		image/jpeg	https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8233.21/content/images/backgrounds/0.jpg?x=a5dbd4393ff6a725c7e62b61df7e72f0		283351	Chrome
		image/jpeg	https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8233.23/content/images/backgrounds/0.jpg?x=a5dbd4393ff6a725c7e62b61df7e72f0		283351	Chrome
		image/jpeg	https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8283.10/content/images/backgrounds/0.jpg?x=a5dbd4393ff6a725c7e62b61df7e72f0		283351	Chrome
		image/jpeg	https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8255.6/content/images/backgrounds/0.jpg?x=a5dbd4393ff6a725c7e62b61df7e72f0		283351	Chrome
		image/jpeg	http://www.enterprisestorageforum.com/imagesvr_ce/6746/ssd-hdd.jpg	1	256895	Edge
		image/svg+xml	https://abm-website-assets.s3.amazonaws.com/sites/all/themes/abm_channel_for/logo.svg	1	247121	Edge
		image/png	https://css.zohostatic.com/zohoone/20180910_1787408/zh		201395	Chrome
		image/png	https://www.zoho.com/images/mobile-apps-icons-sprite@2x.png		185805	Chrome
		image/png	https://www.foxtonforensics.com/Screenshots/s_bhv_2.png	1	167031	Edge
		image/png	https://www.foxtonforensics.com/Screenshots/s_bhe_2.png	2	165665	Edge
		image/jpeg	https://cdn.flashtalking.com/feeds/celebrity/images/ALCAN_Impression_1_300x250.jpg		135930	Chrome
		image/png	https://www.foxtonforensics.com/Screenshots/s_bhv_3.png	1	133797	Edge
		image/png	https://css.zohostatic.com/zohoone/20180910_1787408/zhome/images/bg.png		120676	Chrome
		image/jpeg	https://image.slidesharecdn.com/SSDvsHDD-123294206412-phpapp03/95/ssd-vs-hdd-a-shift-in-data-storage-by-todd-dinkelman-6-728.jpg?cb=1232920	1	120393	Edge
		image/png	https://iz.zohostatic.com/sites/default/files/mail-home-screen.png		111897	Chrome
		image/png	https://www.foxtonforensics.com/Screenshots/s_bhe_3.png	2	103776	Edge

Viewing 25/25 records << < 1 of 1 pages > >> Page size 50



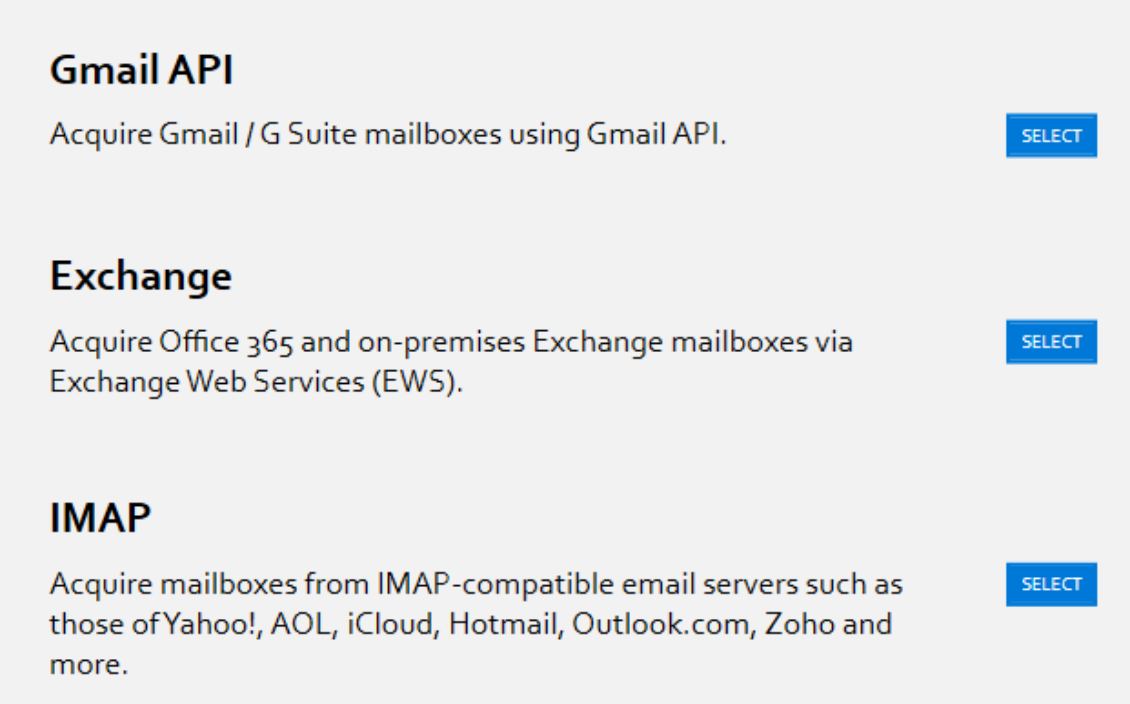
Website Visit Count

	Date Visited	Title	URL	Visit Type	Visit Count	URL Record Count	Visited From	Web Browser
	11/09/2018 15:52:21		file:///C:/Users/mdelacruz/Desktop/Collections/Forensics.docx			1		Internet Explorer
	11/09/2018 15:52:09		https://www.foxtonforensics.com/browser-history-examiner/download			2		Edge
	11/09/2018 15:52:07		https://www.foxtonforensics.com/browser-history-examiner/download			2		Edge
	11/09/2018 15:52:03		https://www.foxtonforensics.com/browser-history-examiner/			2		Edge
	11/09/2018 15:52:00		https://www.foxtonforensics.com/browser-history-examiner/purchase			2		Edge
	11/09/2018 15:52:00		https://www.foxtonforensics.com/browser-history-examiner/purchase			2		Edge
	11/09/2018 15:51:52		https://www.foxtonforensics.com/browser-history-examiner/			2		Edge
	11/09/2018 15:51:52		https://www.foxtonforensics.com/browser-history-examiner			1		Edge
	11/09/2018 15:51:35		https://www.foxtonforensics.com/browser-history-viewer/download			2		Edge
	11/09/2018 15:51:35		https://www.foxtonforensics.com/browser-history-viewer/download			2		Edge
	11/09/2018 15:51:32		https://www.foxtonforensics.com/browser-history-viewer/			2		Edge
	11/09/2018 15:51:30		https://www.foxtonforensics.com/			1		Edge
	11/09/2018 15:51:30		https://www.foxtonforensics.com/browser-history-viewer/			2		Edge
	11/09/2018 15:51:29		about:blank			1		Edge
	11/09/2018 15:51:29		https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwjhg7			1		Edge
	11/09/2018 15:51:23		https://www.google.com/search?source=hp&ei=savlW4D-OsLbzgKWmpmQCg&q=internet+h			2		Edge
	11/09/2018 15:51:22		https://www.google.com/search?source=hp&ei=savlW4D-OsLbzgKWmpmQCg&q=internet+h			2		Edge
	11/09/2018 15:51:18		https://www.google.com/			1		Edge
	11/09/2018 15:51:16		https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1541778353&rver=6.7.6631.0&v			1		Edge
	11/09/2018 15:51:15		https://www.bing.com/msa/sso			1		Edge
	11/09/2018 15:49:16		https://tpc.googlesyndication.com/sodar/6uQTKQJz.html			1		Edge
	11/09/2018 15:49:16		https://ad.doubleclick.net/ddm/adi/N418801.130396SPICEWORKS/B21268213.223209499;dc_v			1		Edge
	11/09/2018 15:49:15		https://ad.doubleclick.net/ddm/adi/N487001.130396SPICEWORKS/B20614218.232106421;dc_v			1		Edge
	11/09/2018 15:49:14		https://tpc.googlesyndication.com/safeframe/1-0-30/html/container.html			1		Edge
	11/09/2018 15:49:12		https://gekko.spiceworks.com/taylor.html?_chd=1&u=5524340&CHD=1314c942&b=gekko&e			1		Edge

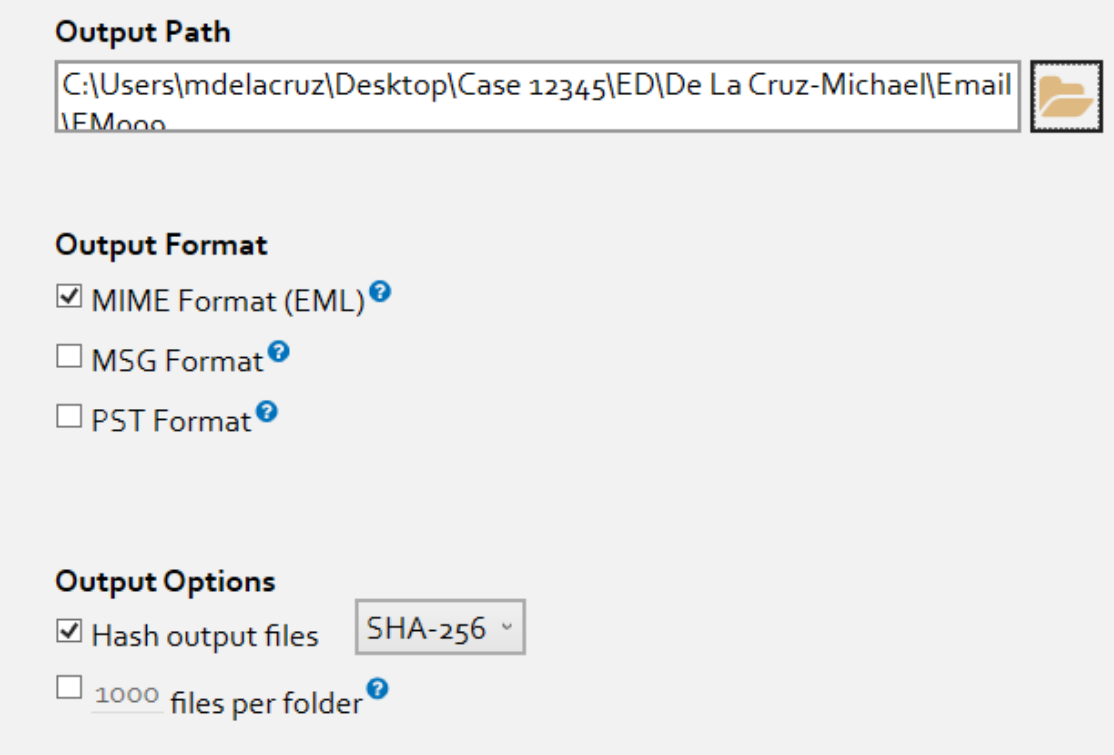
Recover Stored Web Passwords

Email Collections

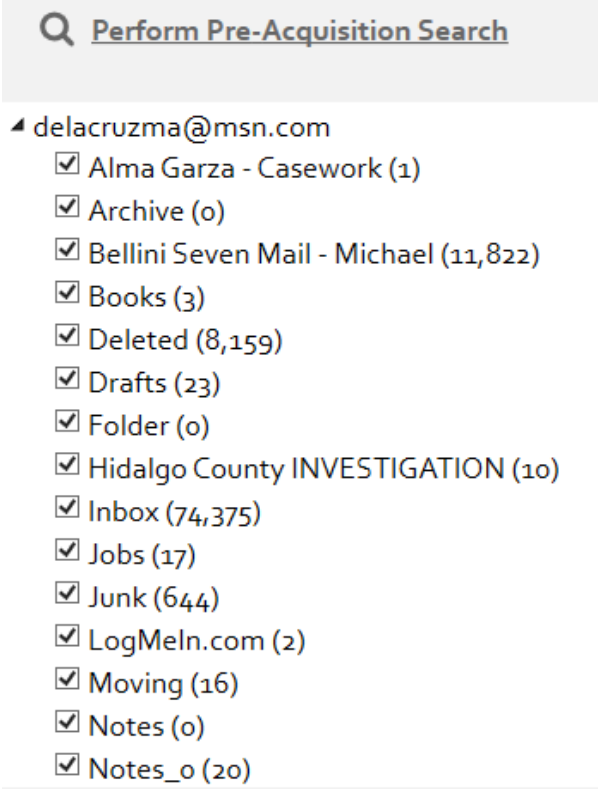
What are the most common types of email collections? POP, IMAP, Gmail, Exchange



Collection to EML, MSG, or PST file format. Files are hashed for verification purposes.

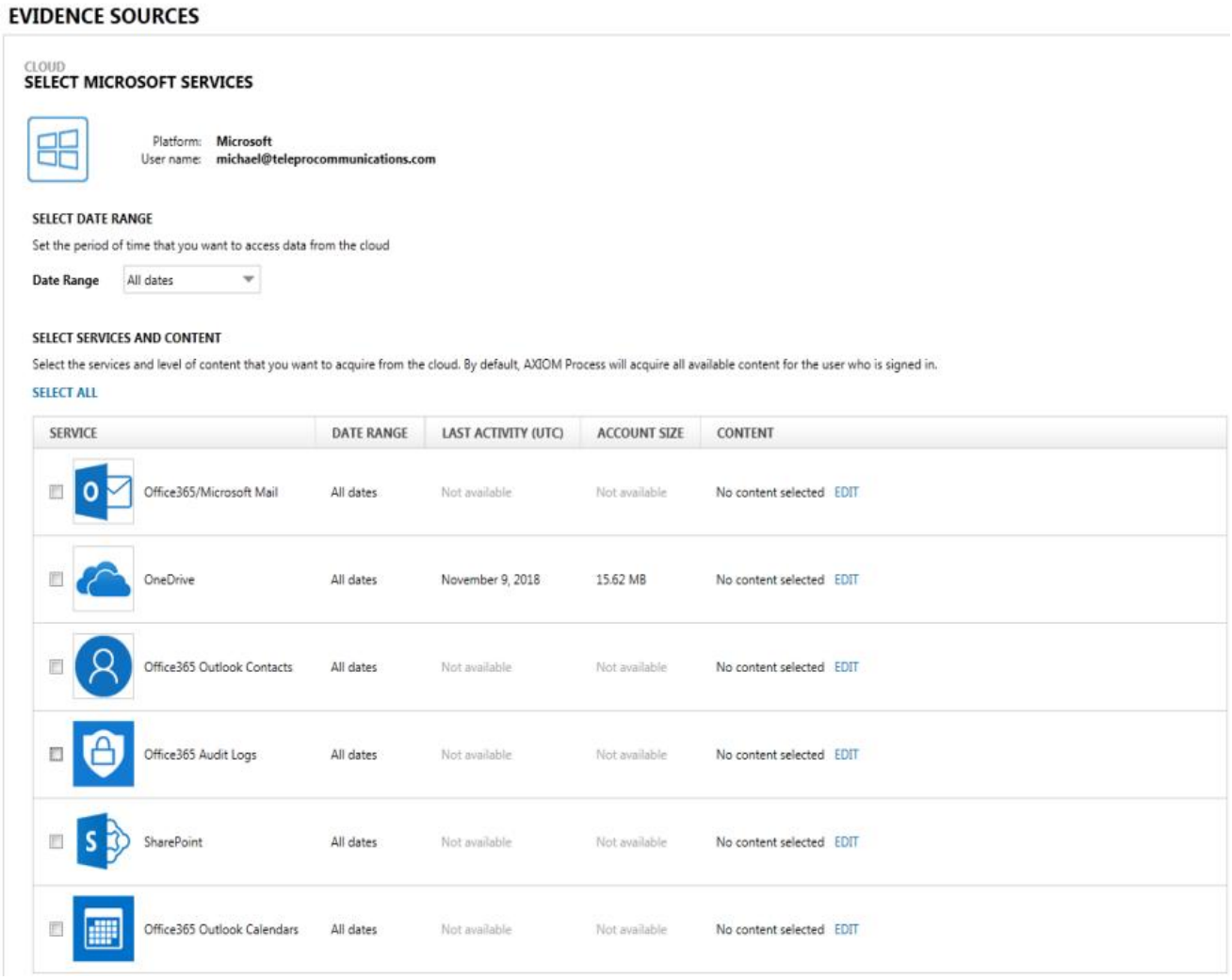


Select ALL, only select folders, or perform a pre-acquisition search.


Perform Pre-Acquisition Search
delacruzma@msn.com
Alma Garza - Casework (1)
Archive (0)
Bellini Seven Mail - Michael (11,822)
Books (3)
Deleted (8,159)
Drafts (23)
Folder (0)
Hidalgo County INVESTIGATION (10)
Inbox (74,375)
Jobs (17)
Junk (644)
LogMeIn.com (2)
Moving (16)
Notes (0)
Notes_0 (20)

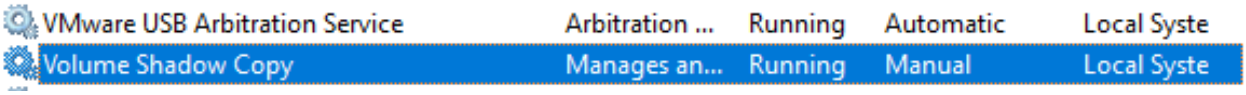
Email Collections

Magnet AXIOM

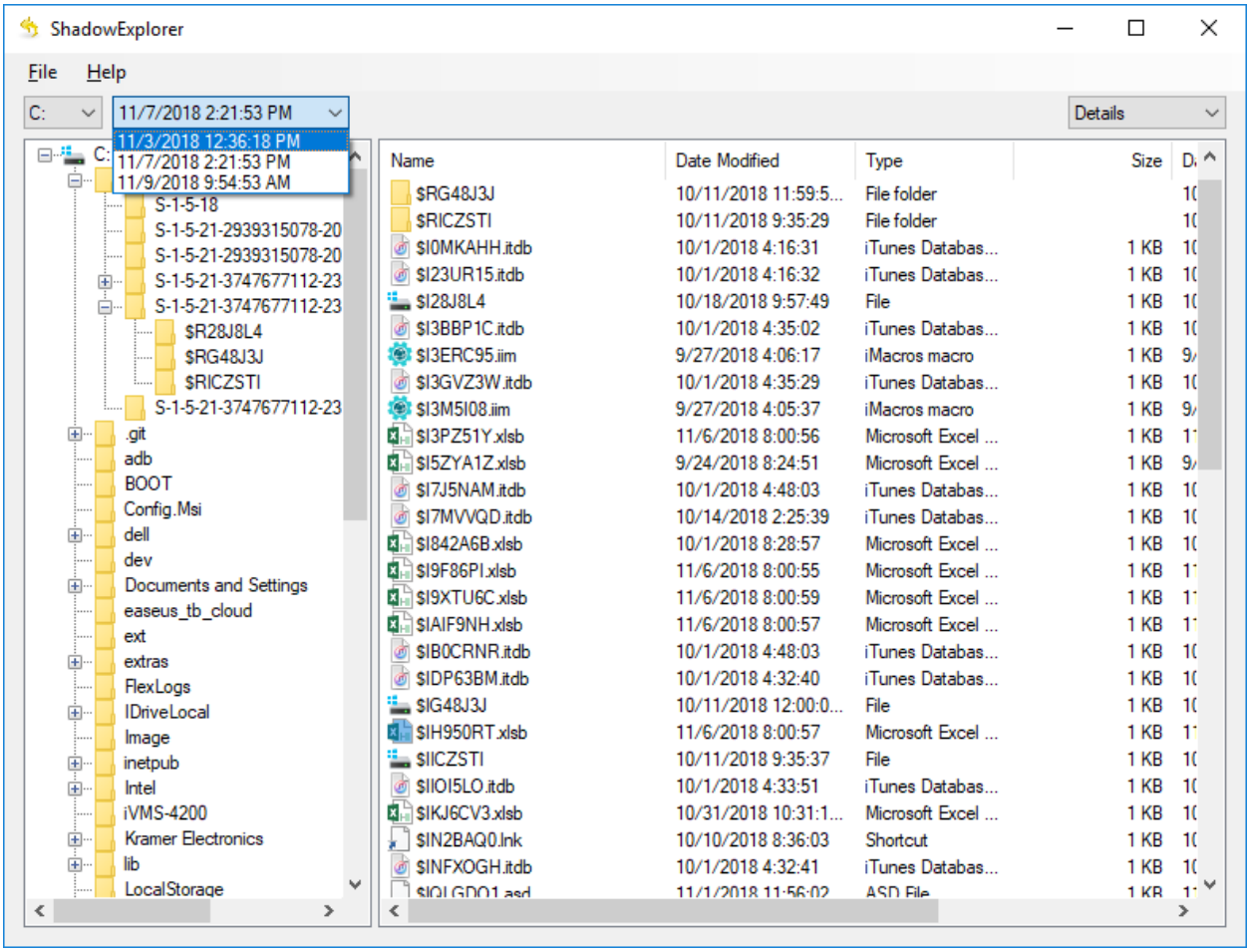


Volume Shadow Copy (VSS)

Windows service that takes a snapshot of files/volumes while in use.



Shadow Explorer will parse all available snapshots.



Accessing VSS snapshot as a volume

Why is it useful to be able to access the MFT of different VSS snapshots?

Install Dokan - https://github.com/dokan-dev/dokany/releases/tag/v0.7.4

Run vshadowmount with byte offset ([Sector Offset] x 512) = byte offset

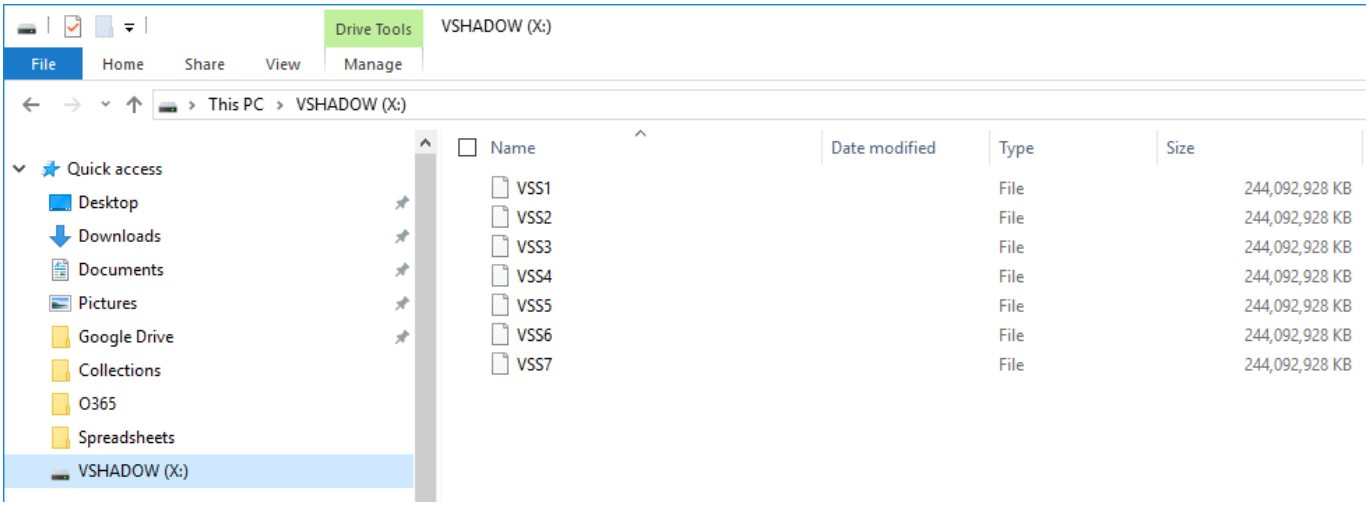
vshadowmount -o 105906176 -X allow_other D:\Collection\WS_002\WS_002.001 x:

```
vshadowmount -o [byte offset] -X allow_other z:\disk.img x:
```

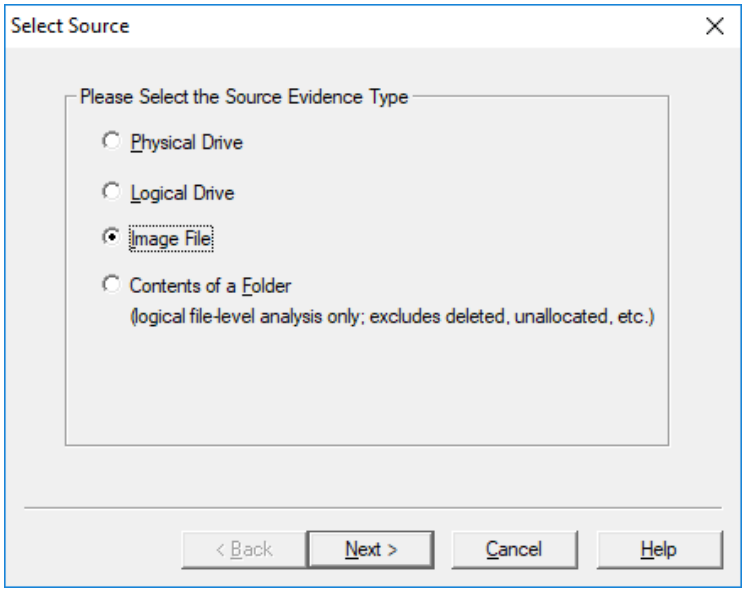
If you get the following error message, reinstall Dokan.

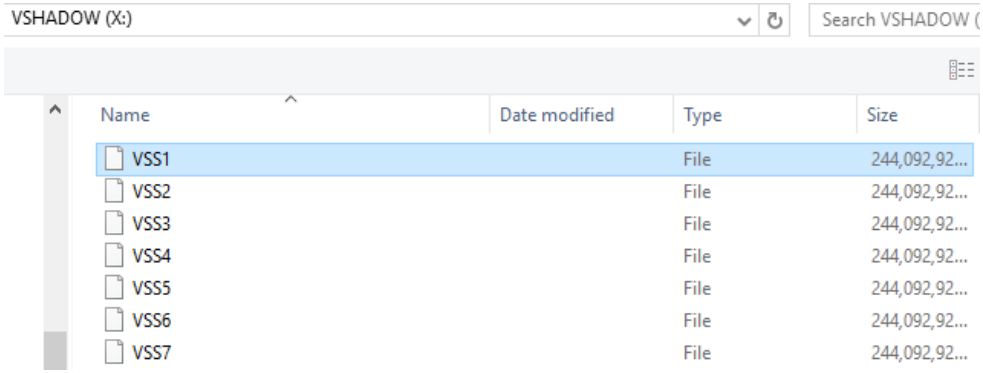
```
C:\Users\mdelacruz\Desktop\Collections\vshadowmount>vshadowmount -o 105906176 -X allow_other D:\Collection\WS_002\WS_002.001 x:
vshadowmount 20130509

Unable to run dokan main: unable to load driver
```

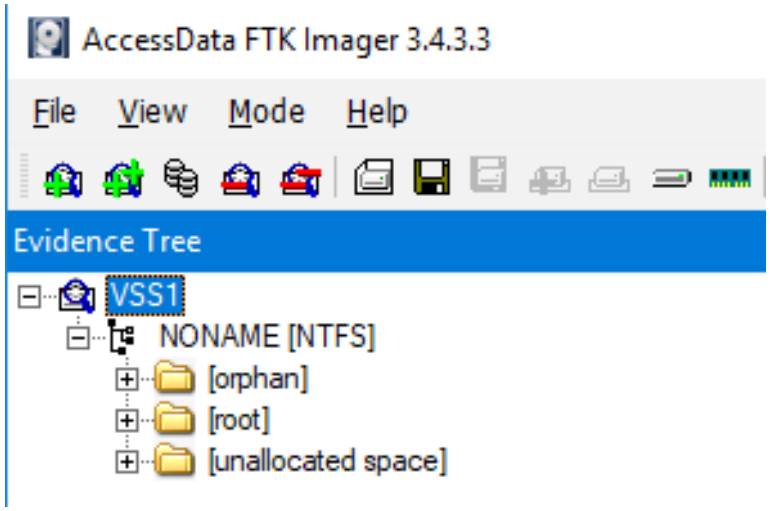
If successful, you will see all available VSS snapshots on the X drive.



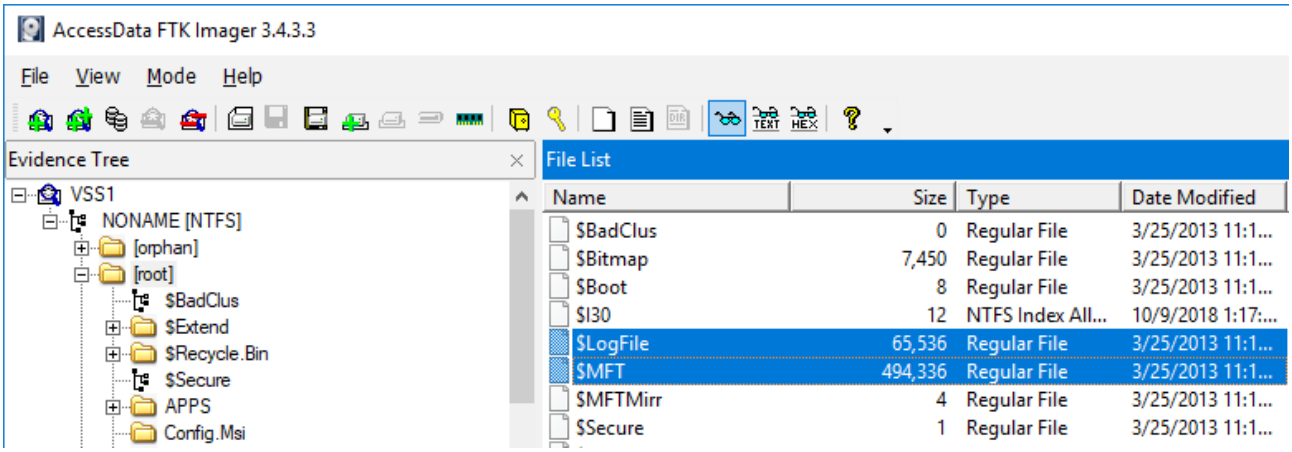
Access X:\ volume using FTK Imager and import each VSS snapshot at an image file



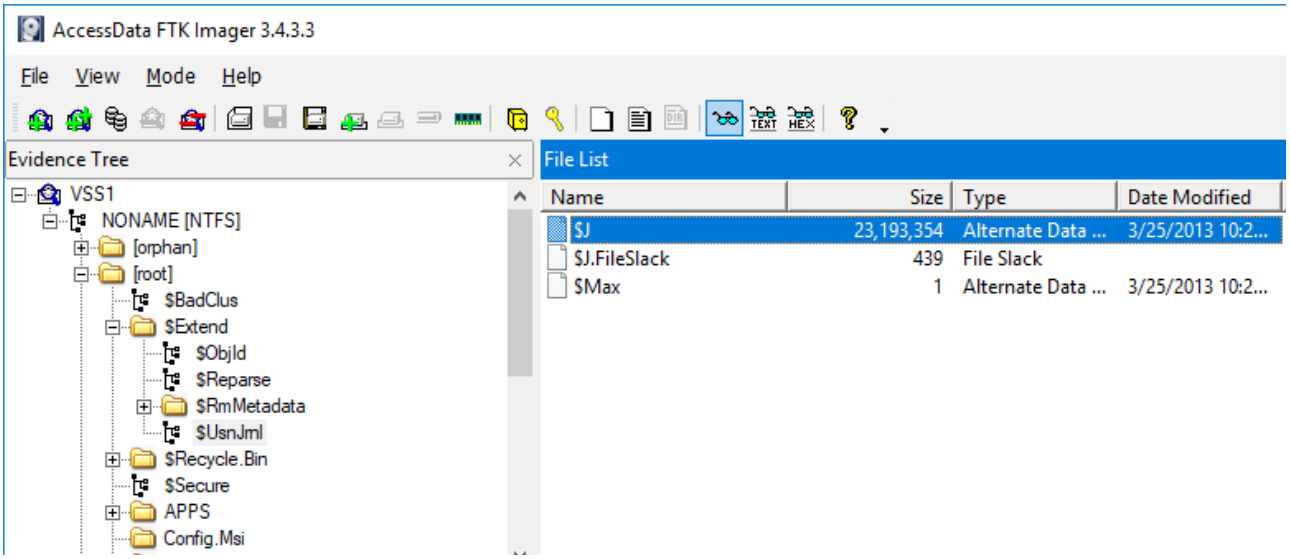




For each VSS snapshot, extract $MFT and $LogFile



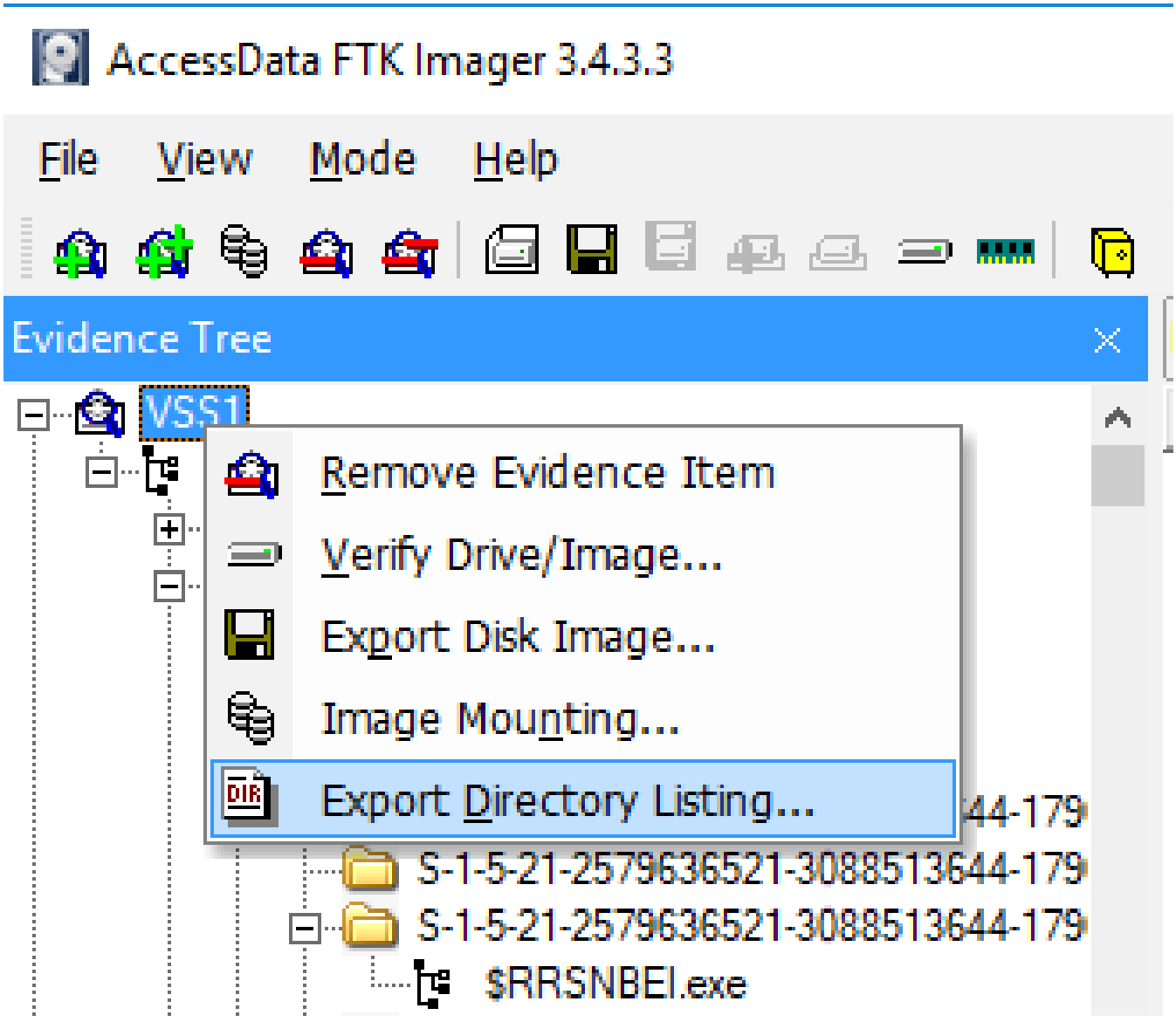
And extract the $USnJrnl\$J file



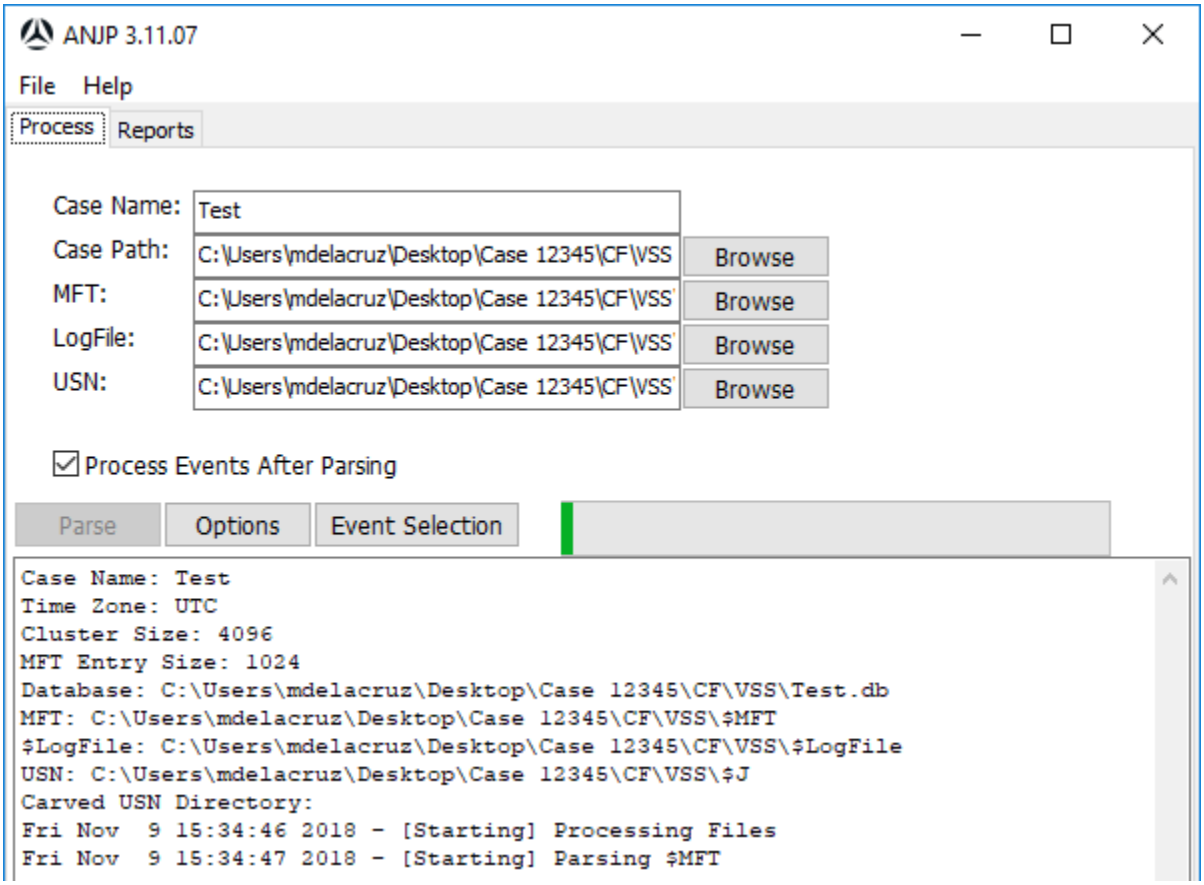
Additional files to extract from the VSS snapshot for additional data extraction

- C:\pagefile.sys
- C:\hiberfil.sys
- C:\Windows\system32\config\SAM
- C:\Windows\system32\config\SYSTEM
- C:\Windows\inf\setupapi.app.log

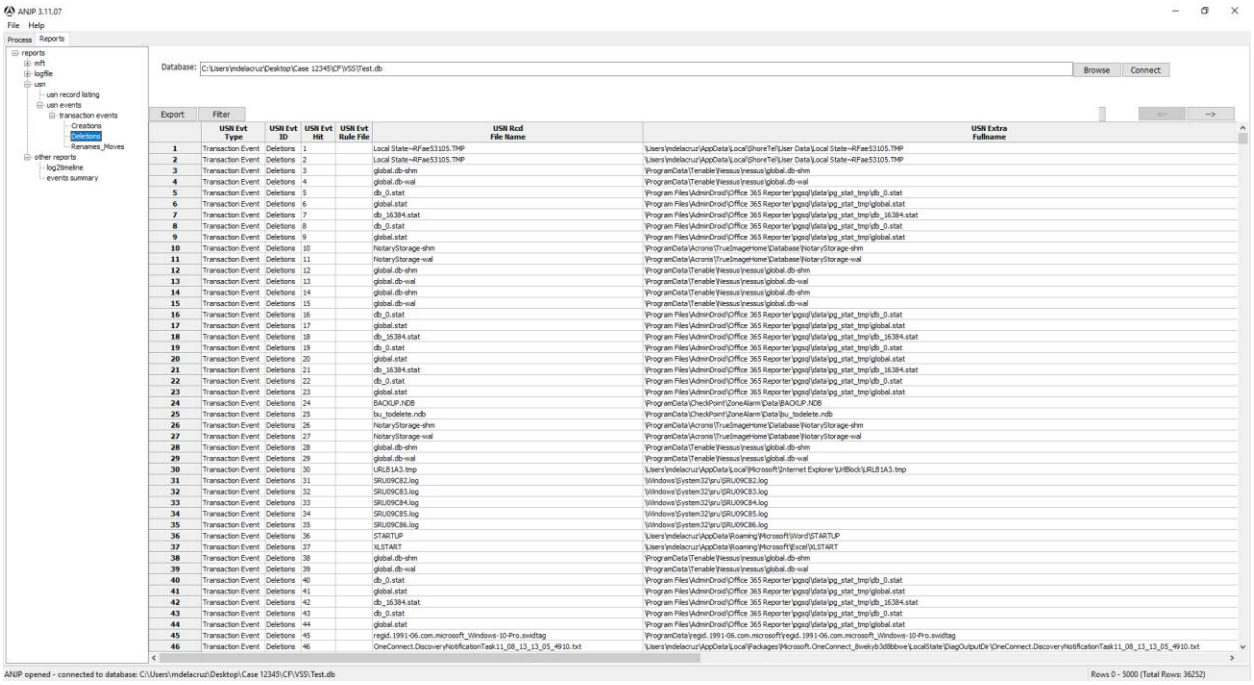
Generating a file listing report for each VSS snapshot is also recommended.



Parse the $MFT, $LogFile, and $J files for each of the VSS snapshots



Export the Creation, Deletions, and Renames/Moves reports



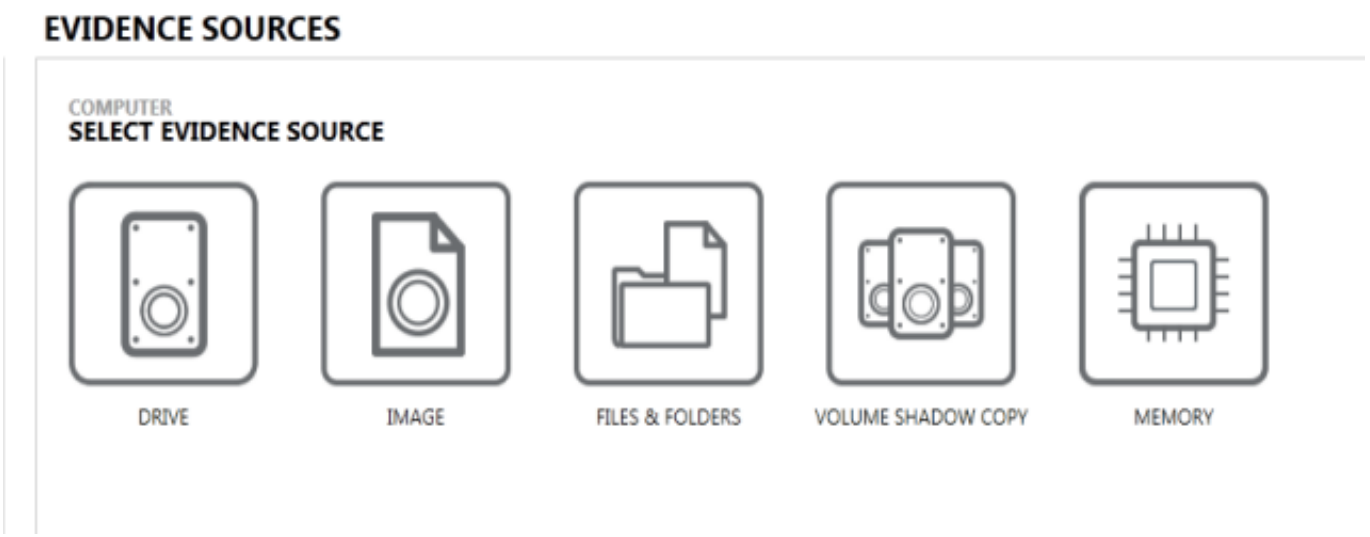
	USN Evt Type	USN Evt ID	USN Evt Hit	USN Evt Rule File	USN Rcd File Name	USN Extra Fullname
1	Transaction Event	Deletions	1		Local State~RFae53105.TMP	\Users\mdelacruz\AppData\Local\ShoreTel\User Data\Local State~RFae53105.TMP
2	Transaction Event	Deletions	2		Local State~RFae53105.TMP	\Users\mdelacruz\AppData\Local\ShoreTel\User Data\Local State~RFae53105.TMP
3	Transaction Event	Deletions	3		global.db-shm	\ProgramData\Tenable\Nessus\nessus\global.db-shm
4	Transaction Event	Deletions	4		global.db-wal	\ProgramData\Tenable\Nessus\nessus\global.db-wal
5	Transaction Event	Deletions	5		db_0.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\db_0.stat
6	Transaction Event	Deletions	6		global.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\global.stat
7	Transaction Event	Deletions	7		db_16384.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\db_16384.stat
8	Transaction Event	Deletions	8		db_0.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\db_0.stat
9	Transaction Event	Deletions	9		global.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\global.stat
10	Transaction Event	Deletions	10		NotaryStorage-shm	\ProgramData\Acronis\TrueImageHome\Database\NotaryStorage-shm
11	Transaction Event	Deletions	11		NotaryStorage-wal	\ProgramData\Acronis\TrueImageHome\Database\NotaryStorage-wal
12	Transaction Event	Deletions	12		global.db-shm	\ProgramData\Tenable\Nessus\nessus\global.db-shm
13	Transaction Event	Deletions	13		global.db-wal	\ProgramData\Tenable\Nessus\nessus\global.db-wal
14	Transaction Event	Deletions	14		global.db-shm	\ProgramData\Tenable\Nessus\nessus\global.db-shm
15	Transaction Event	Deletions	15		global.db-wal	\ProgramData\Tenable\Nessus\nessus\global.db-wal
16	Transaction Event	Deletions	16		db_0.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\db_0.stat
17	Transaction Event	Deletions	17		global.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\global.stat
18	Transaction Event	Deletions	18		db_16384.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\db_16384.stat
19	Transaction Event	Deletions	19		db_0.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\db_0.stat
20	Transaction Event	Deletions	20		global.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\global.stat
21	Transaction Event	Deletions	21		db_16384.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\db_16384.stat
22	Transaction Event	Deletions	22		db_0.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\db_0.stat
23	Transaction Event	Deletions	23		global.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\global.stat
24	Transaction Event	Deletions	24		BACKUP.NDB	\ProgramData\CheckPoint\ZoneAlarm\Data\BACKUP.NDB
25	Transaction Event	Deletions	25		bu_todelete.ndb	\ProgramData\CheckPoint\ZoneAlarm\Data\bu_todelete.ndb
26	Transaction Event	Deletions	26		NotaryStorage-shm	\ProgramData\Acronis\TrueImageHome\Database\NotaryStorage-shm
27	Transaction Event	Deletions	27		NotaryStorage-wal	\ProgramData\Acronis\TrueImageHome\Database\NotaryStorage-wal
28	Transaction Event	Deletions	28		global.db-shm	\ProgramData\Tenable\Nessus\nessus\global.db-shm
29	Transaction Event	Deletions	29		global.db-wal	\ProgramData\Tenable\Nessus\nessus\global.db-wal
30	Transaction Event	Deletions	30		URLB1A3.tmp	\Users\mdelacruz\AppData\Local\Microsoft\Internet Explorer\UrlBlock\URLB1A3.tmp
31	Transaction Event	Deletions	31		SRU09C82.log	\Windows\System32\sru\SRU09C82.log
32	Transaction Event	Deletions	32		SRU09C83.log	\Windows\System32\sru\SRU09C83.log
33	Transaction Event	Deletions	33		SRU09C84.log	\Windows\System32\sru\SRU09C84.log
34	Transaction Event	Deletions	34		SRU09C85.log	\Windows\System32\sru\SRU09C85.log
35	Transaction Event	Deletions	35		SRU09C86.log	\Windows\System32\sru\SRU09C86.log
36	Transaction Event	Deletions	36		STARTUP	\Users\mdelacruz\AppData\Roaming\Microsoft\Word\STARTUP
37	Transaction Event	Deletions	37		XLSTART	\Users\mdelacruz\AppData\Roaming\Microsoft\Excel\XLSTART
38	Transaction Event	Deletions	38		global.db-shm	\ProgramData\Tenable\Nessus\nessus\global.db-shm
39	Transaction Event	Deletions	39		global.db-wal	\ProgramData\Tenable\Nessus\nessus\global.db-wal
40	Transaction Event	Deletions	40		db_0.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\db_0.stat
41	Transaction Event	Deletions	41		global.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\global.stat
42	Transaction Event	Deletions	42		db_16384.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\db_16384.stat
43	Transaction Event	Deletions	43		db_0.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\db_0.stat
44	Transaction Event	Deletions	44		global.stat	\Program Files\AdminDroid\Office 365 Reporter\pgsql\data\pg_stat_tmp\global.stat
45	Transaction Event	Deletions	45		regid.1991-06.com.microsoft_Windows-10-Pro.swidtag	\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft_Windows-10-Pro.swidtag
46	Transaction Event	Deletions	46		OneConnect.DiscoveryNotificationTask11_08_13_13_05_4910.txt	\Users\mdelacruz\AppData\Local\Packages\Microsoft.OneConnect_8vekyb3d8bbwe\LocalState\DiagOutputDir\OneConnect.DiscoveryNotificationTask11_08_13_13_05_4910.txt

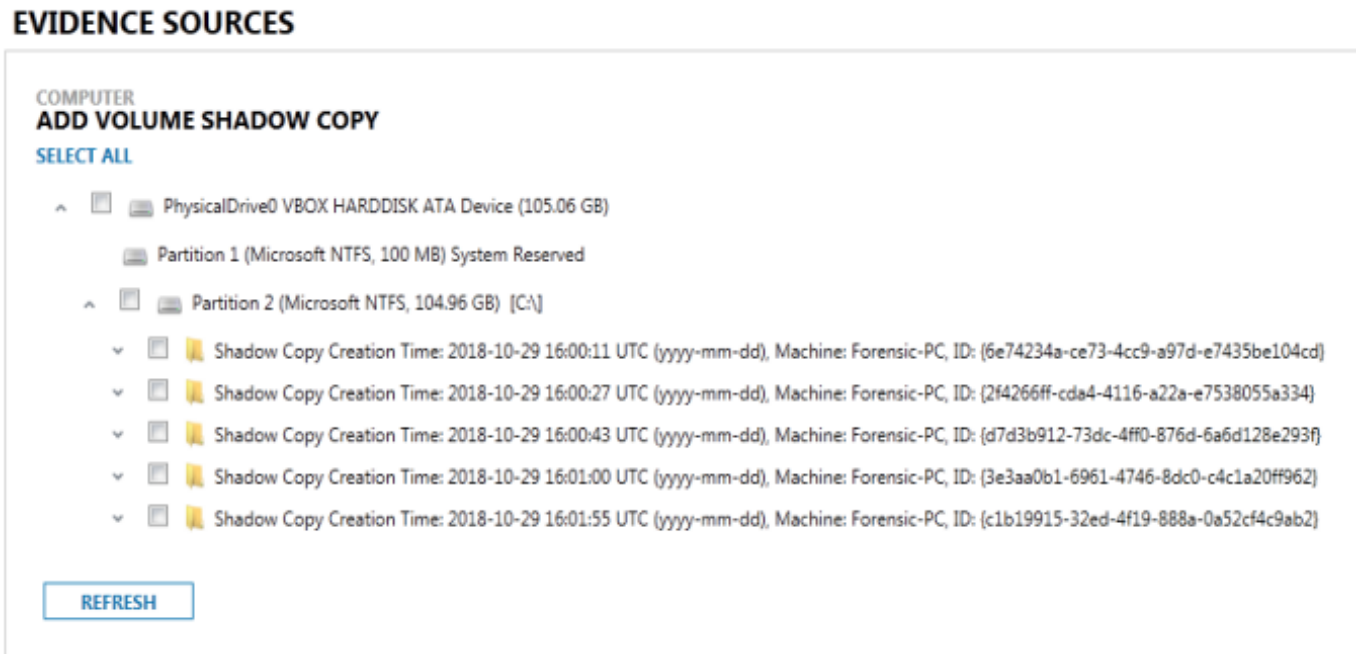
Concatenate the log files

type system_DELETED_EVENTS.txt vss_01_DELETED_EVENTS.txt vss_02_DELETED_EVENTS.txt vss_03_DELETED_EVENTS.txt vss_04_DELETED_EVENTS.txt > master_DELETED_EVENTS.txt

USN Evt Type	USN Evt ID	USN Rcd Time	USN Extra Fullname
Transaction Event	Deletions	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Creations	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Deletions	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Creations	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Deletions	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Windows\Recent\Forensics.docx.lnk
Transaction Event	Creations	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Windows\Recent\Forensics.docx.lnk
Transaction Event	Deletions	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Windows\Recent\Collections (2).lnk
Transaction Event	Creations	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Windows\Recent\Collections (2).lnk
Transaction Event	Deletions	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Creations	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Deletions	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Creations	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Creations	11/8/18 10:45 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Word\Forensics307014923360982237\Forensics.docx.lnk
Transaction Event	Deletions	11/8/18 11:02 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Creations	11/8/18 11:02 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Deletions	11/8/18 11:02 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Creations	11/8/18 11:02 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Deletions	11/8/18 11:02 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Creations	11/8/18 11:02 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Deletions	11/8/18 11:02 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Creations	11/8/18 11:02 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Office\Recent\Forensics.docx.LNK
Transaction Event	Deletions	11/8/18 11:02 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Windows\Recent\Forensics.docx.lnk
Transaction Event	Creations	11/8/18 11:02 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Windows\Recent\Forensics.docx.lnk
Transaction Event	Deletions	11/8/18 11:02 PM	\Users\mdelacruz\AppData\Roaming\Microsoft\Windows\Recent\Collections (2).lnk

VSS in AXIOM


EVIDENCE SOURCES
COMPUTER
SELECT EVIDENCE SOURCE
DRIVE
IMAGE
FILES & FOLDERS
VOLUME SHADOW COPY
MEMORY

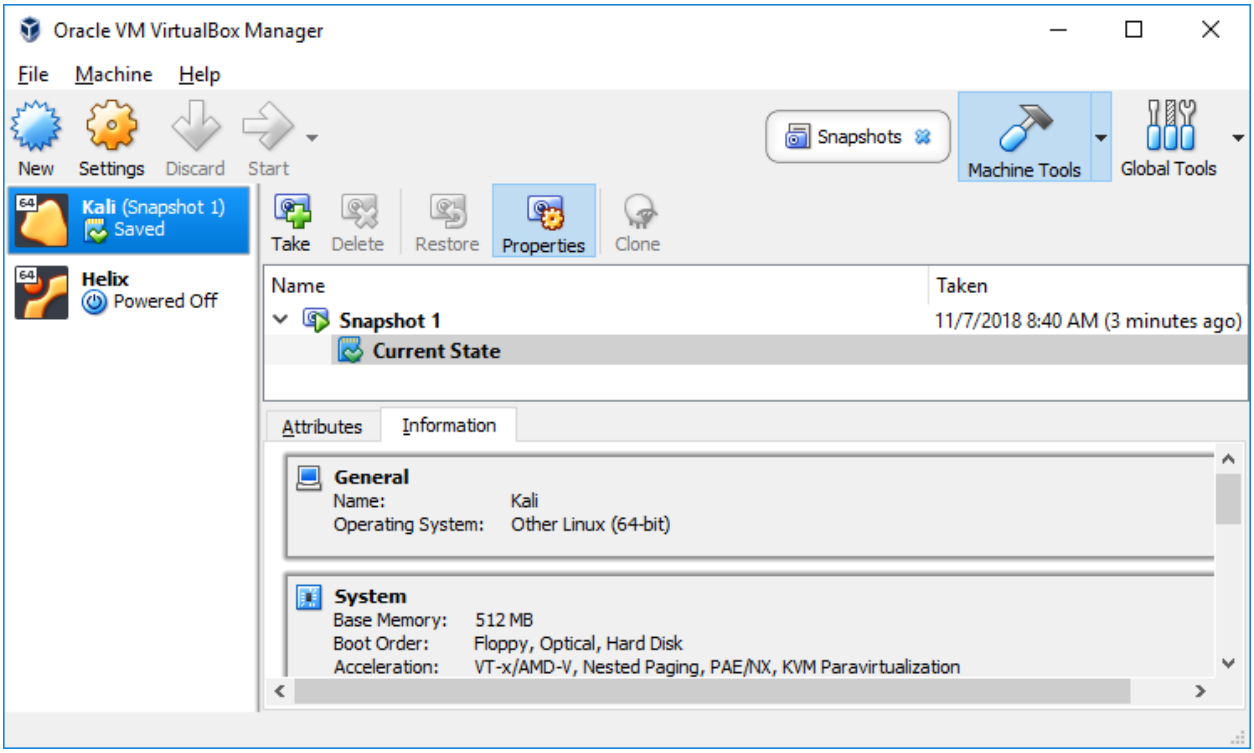

EVIDENCE SOURCES
COMPUTER
ADD VOLUME SHADOW COPY
SELECT ALL
PhysicalDrive0 VBOX HARDDISK ATA Device (105.06 GB)
Partition 1 (Microsoft NTFS, 100 MB) System Reserved
Partition 2 (Microsoft NTFS, 104.96 GB) [C:\]
Shadow Copy Creation Time: 2018-10-29 16:00:11 UTC (yyyy-mm-dd), Machine: Forensic-PC, ID: {6e74234a-ce73-4cc9-a97d-e7435be104cd}
Shadow Copy Creation Time: 2018-10-29 16:00:27 UTC (yyyy-mm-dd), Machine: Forensic-PC, ID: {2f4266ff-cda4-4116-a22a-e7538055a334}
Shadow Copy Creation Time: 2018-10-29 16:00:43 UTC (yyyy-mm-dd), Machine: Forensic-PC, ID: {d7d3b912-73dc-4ff0-876d-6a6d128e293f}
Shadow Copy Creation Time: 2018-10-29 16:01:00 UTC (yyyy-mm-dd), Machine: Forensic-PC, ID: {3e3aa0b1-6961-4746-8dc0-c4c1a20ff962}
Shadow Copy Creation Time: 2018-10-29 16:01:55 UTC (yyyy-mm-dd), Machine: Forensic-PC, ID: {c1b19915-32ed-4f19-888a-0a52cf4c9ab2}
REFRESH

Virtual Machines

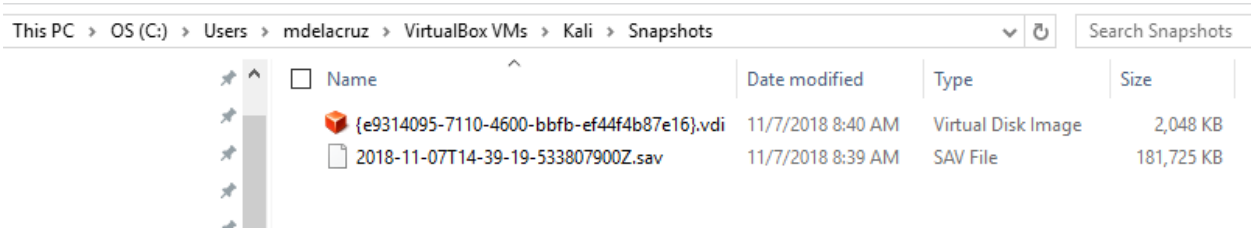
What are virtual machines?

What is the best way to acquire the contents of a live virtual hard disk?

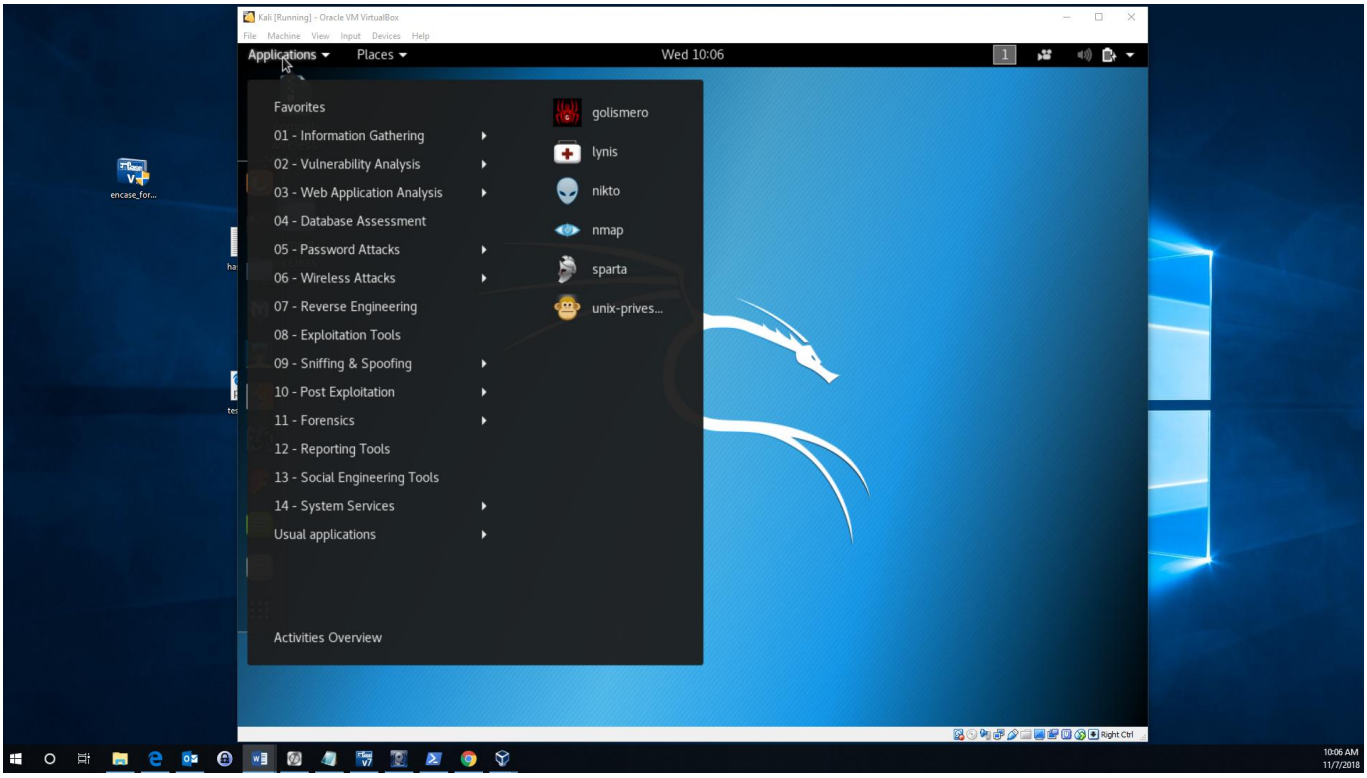
What are snapshots?



Where are snapshots located and what information can I get from them?

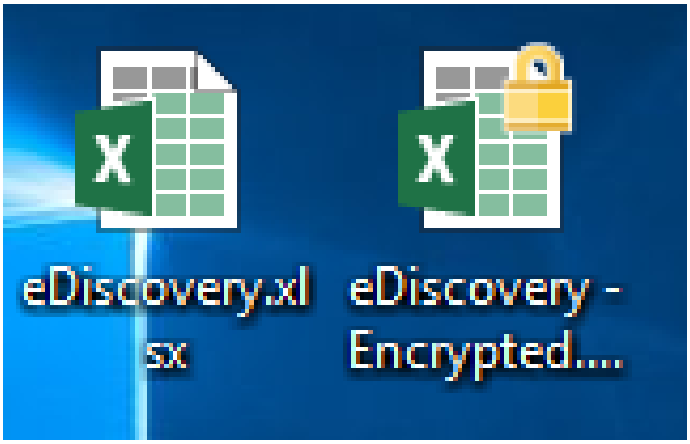


Why do virtual machines need to be mounted to be properly analyzed?

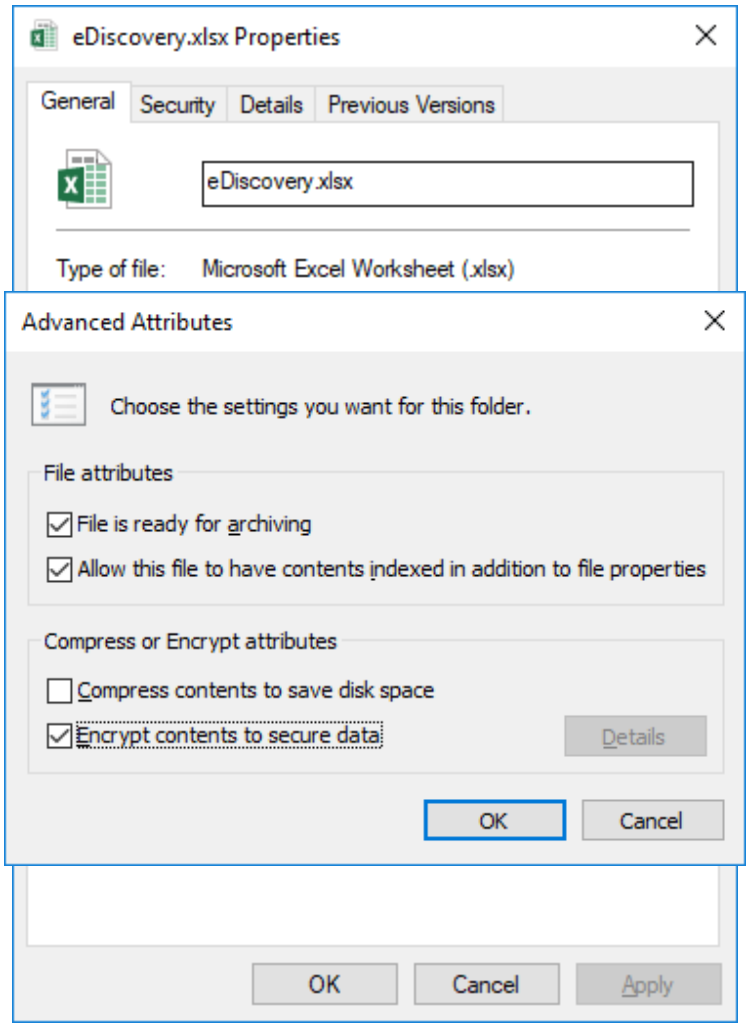


Encrypted Files on Windows (EFS)

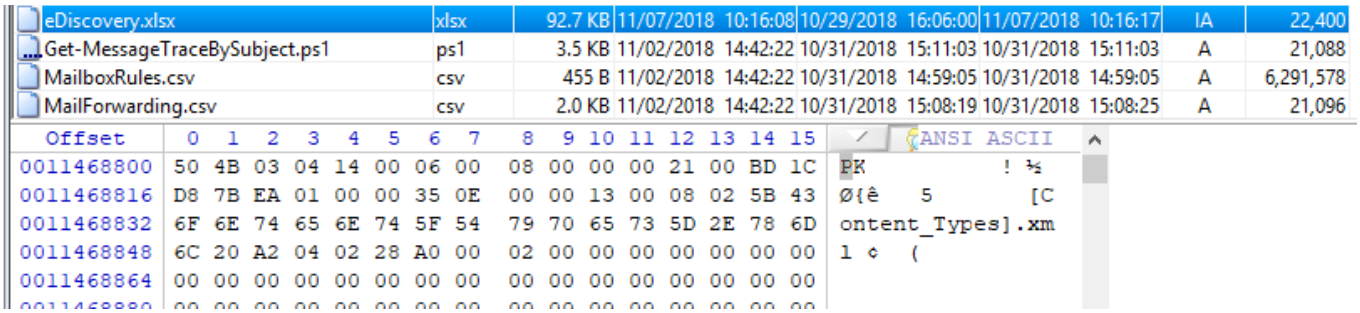
What are encrypted files?



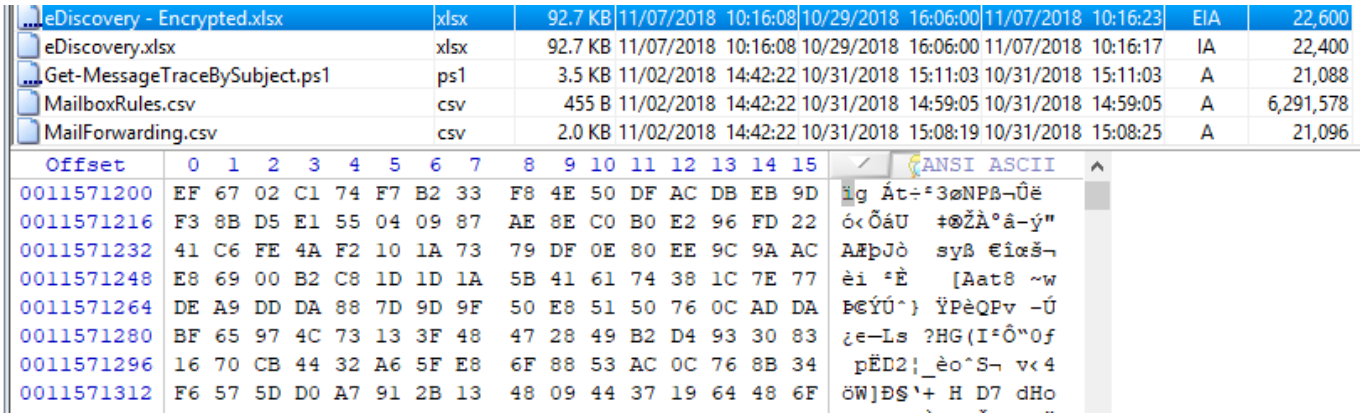
How can forensic tools identify encrypted files?



Hex view of unencrypted XLSX file



Hex view of encrypted XLSX file

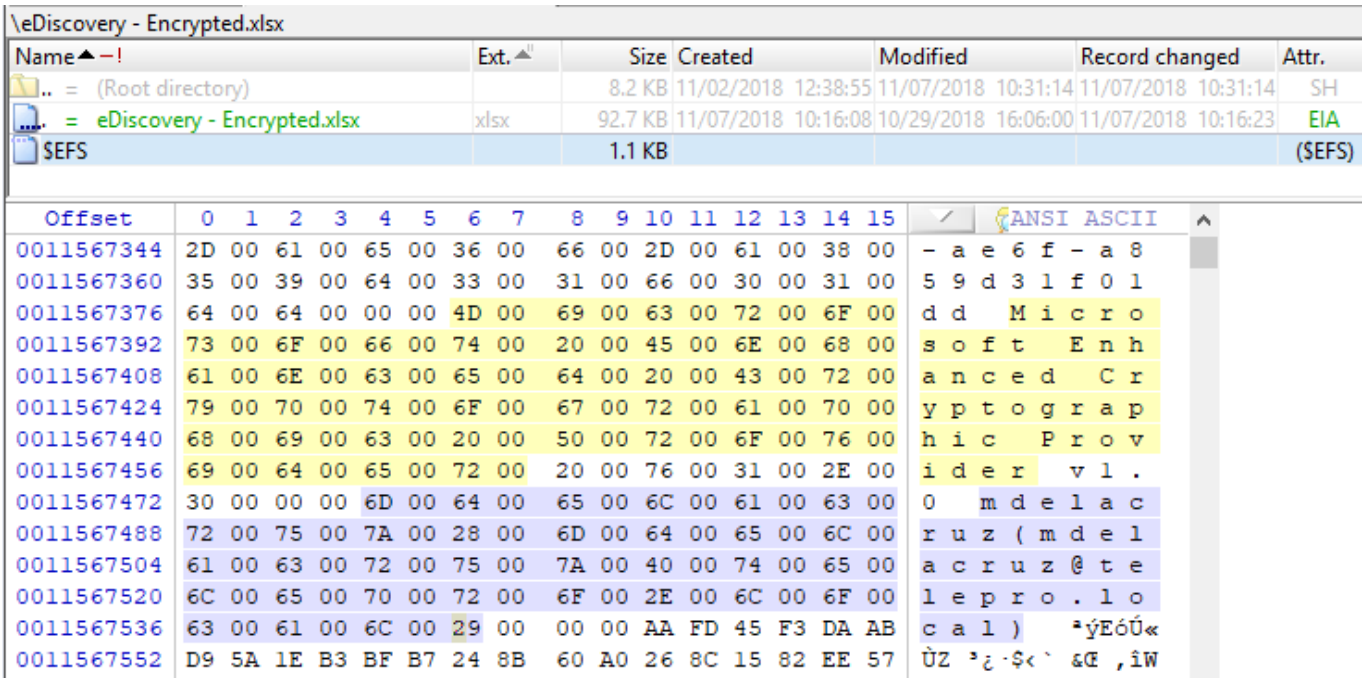


eDiscovery - Encrypted.xlsx	xlsx	92.7 KB	11/07/2018 10:16:08	10/29/2018 16:06:00	11/07/2018 10:16:23	EIA	22,600
eDiscovery.xlsx	xlsx	92.7 KB	11/07/2018 10:16:08	10/29/2018 16:06:00	11/07/2018 10:16:17	IA	22,400
Get-MessageTraceBySubject.ps1	ps1	3.5 KB	11/02/2018 14:42:22	10/31/2018 15:11:03	10/31/2018 15:11:03	A	21,088
MailboxRules.csv	csv	455 B	11/02/2018 14:42:22	10/31/2018 14:59:05	10/31/2018 14:59:05	A	6,291,578
MailForwarding.csv	csv	2.0 KB	11/02/2018 14:42:22	10/31/2018 15:08:19	10/31/2018 15:08:25	A	21,096

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
0011571200	EF	67	02	C1	74	F7	B2	33	F8	4E	50	DF	AC	DB	EB	9D	ïg Át÷²3øNPß¬Ûë
0011571216	F3	8B	D5	E1	55	04	09	87	AE	8E	C0	B0	E2	96	FD	22	ó‹ÕáU ‡®ŽÀ°â–ý"
0011571232	41	C6	FE	4A	F2	10	1A	73	79	DF	0E	80	EE	9C	9A	AC	AÆþJò syß €îœš¬
0011571248	E8	69	00	B2	C8	1D	1D	1A	5B	41	61	74	38	1C	7E	77	èi ²È [Aat8 ~w
0011571264	DE	A9	DD	DA	88	7D	9D	9F	50	E8	51	50	76	0C	AD	DA	Þ©ÝÚˆ} ŸPèQPv -Ú
0011571280	BF	65	97	4C	73	13	3F	48	47	28	49	B2	D4	93	30	83	¿e—Ls ?HG(I²Ô"0ƒ
0011571296	16	70	CB	44	32	A6	5F	E8	6F	88	53	AC	0C	76	8B	34	pËD2¦_èoˆS¬ v‹4
0011571312	F6	57	5D	D0	A7	91	2B	13	48	09	44	37	19	64	48	6F	öW]Ð§'+ H D7 dHo

Encryption Information

How can we identify who is able to open an encrypted file?

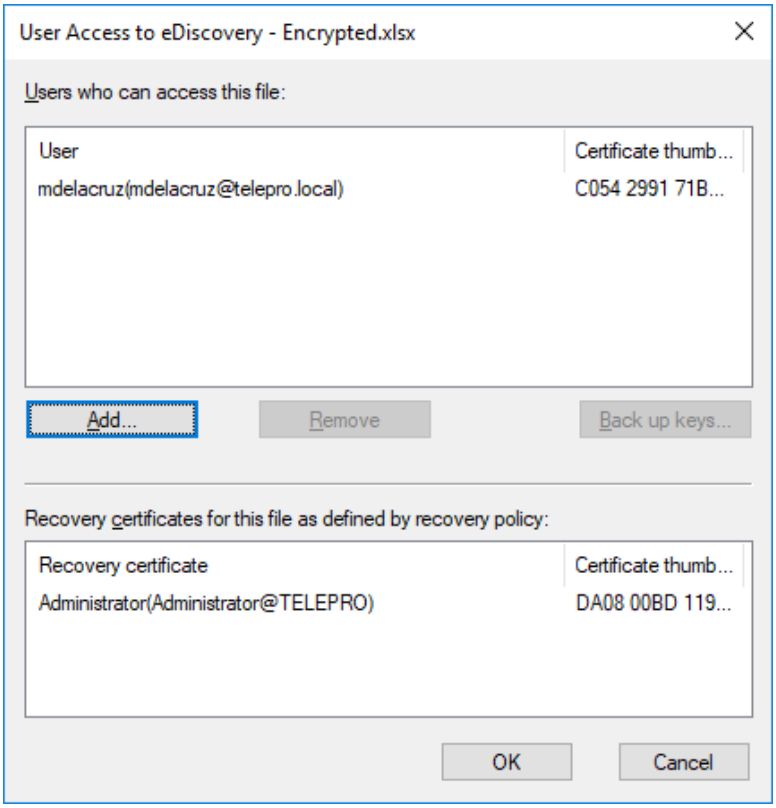


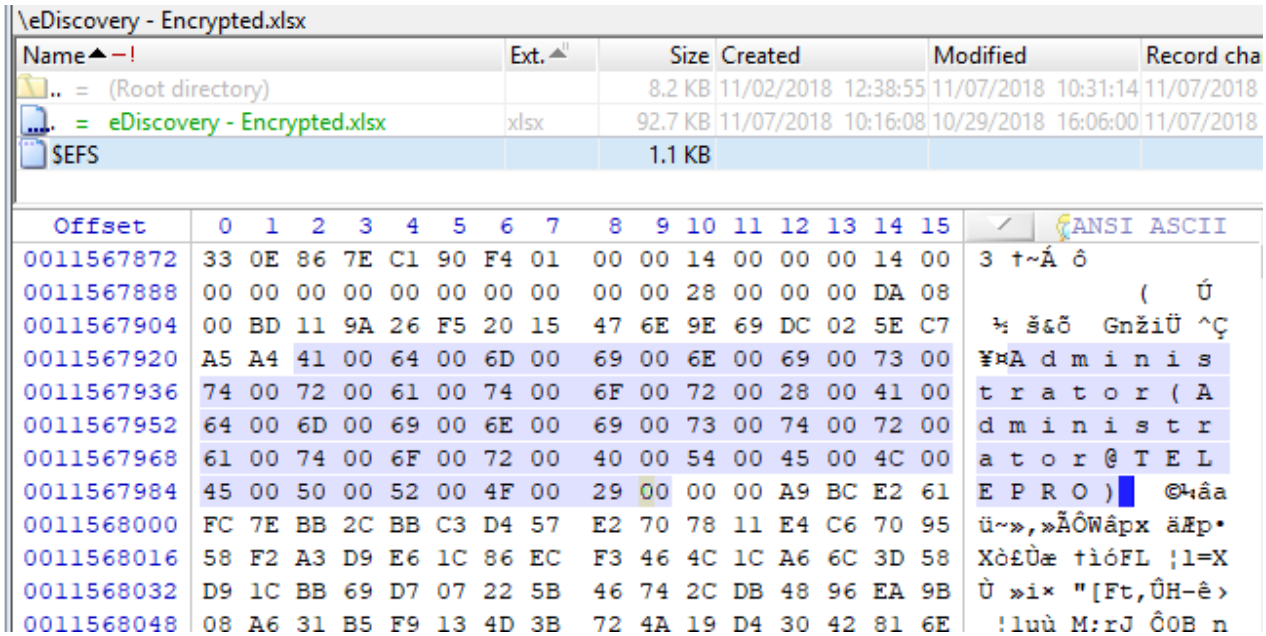
\eDiscovery - Encrypted.xlsx

Name	Ext.	Size	Created	Modified	Record changed	Attr.
.. = (Root directory)		8.2 KB	11/02/2018 12:38:55	11/07/2018 10:31:14	11/07/2018 10:31:14	SH
. = eDiscovery - Encrypted.xlsx	xlsx	92.7 KB	11/07/2018 10:16:08	10/29/2018 16:06:00	11/07/2018 10:16:23	EIA
$EFS		1.1 KB				($EFS)

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
0011567344	2D	00	61	00	65	00	36	00	66	00	2D	00	61	00	38	00	- a e 6 f - a 8
0011567360	35	00	39	00	64	00	33	00	31	00	66	00	30	00	31	00	5 9 d 3 1 f 0 1
0011567376	64	00	64	00	00	00	4D	00	69	00	63	00	72	00	6F	00	d d M i c r o
0011567392	73	00	6F	00	66	00	74	00	20	00	45	00	6E	00	68	00	s o f t E n h
0011567408	61	00	6E	00	63	00	65	00	64	00	20	00	43	00	72	00	a n c e d C r
0011567424	79	00	70	00	74	00	6F	00	67	00	72	00	61	00	70	00	y p t o g r a p
0011567440	68	00	69	00	63	00	20	00	50	00	72	00	6F	00	76	00	h i c P r o v
0011567456	69	00	64	00	65	00	72	00	20	00	76	00	31	00	2E	00	i d e r v 1 .
0011567472	30	00	00	00	6D	00	64	00	65	00	6C	00	61	00	63	00	0 m d e l a c
0011567488	72	00	75	00	7A	00	28	00	6D	00	64	00	65	00	6C	00	r u z (m d e l
0011567504	61	00	63	00	72	00	75	00	7A	00	40	00	74	00	65	00	a c r u z @ t e
0011567520	6C	00	65	00	70	00	72	00	6F	00	2E	00	6C	00	6F	00	l e p r o . l o
0011567536	63	00	61	00	6C	00	29	00	00	00	AA	FD	45	F3	DA	AB	c a l) ªýEóÚ«
0011567552	D9	5A	1E	B3	BF	B7	24	8B	60	A0	26	8C	15	82	EE	57	ÙZ ³¿·$‹` &Œ ‚îW

How can we identify the recovery account?

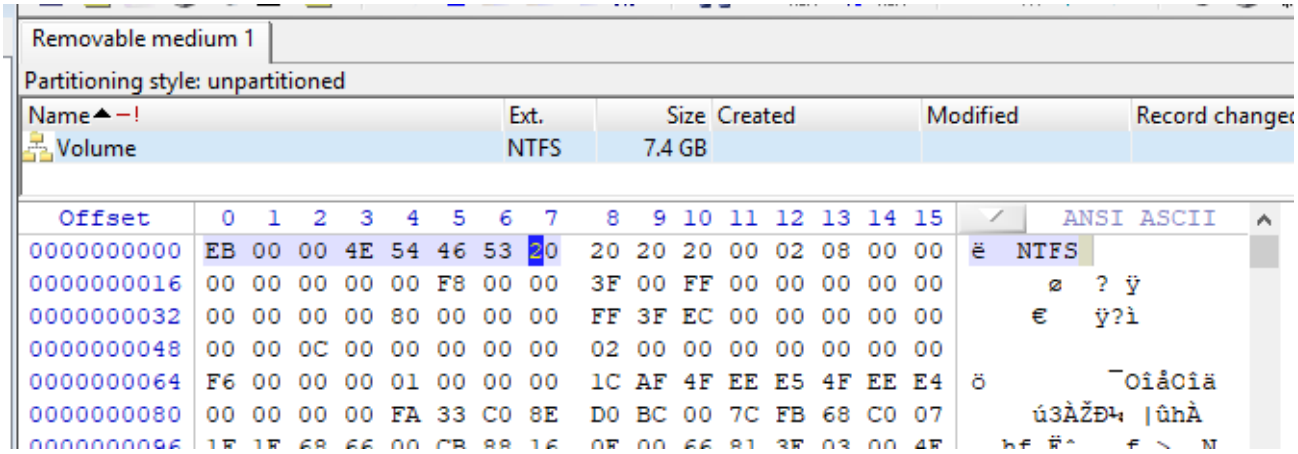

User Access to eDiscovery - Encrypted.xlsx
Users who can access this file:
User
Certificate thumb...
mdelacruz(mdelacruz@telepro.local)
C054 2991 71B...
Add...
Remove
Back up keys...
Recovery certificates for this file as defined by recovery policy:
Recovery certificate
Certificate thumb...
Administrator(Administrator@TELEPRO)
DA08 00BD 119...
OK
Cancel


\eDiscovery - Encrypted.xlsx
Name
Ext.
Size
Created
Modified
Record cha
.. = (Root directory)
8.2 KB 11/02/2018 12:38:55 11/07/2018 10:31:14 11/07/2018
. = eDiscovery - Encrypted.xlsx
xlsx
92.7 KB 11/07/2018 10:16:08 10/29/2018 16:06:00 11/07/2018
$EFS
1.1 KB
Offset 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ANSI ASCII
0011567872 33 0E 86 7E C1 90 F4 01 00 00 14 00 00 00 14 00
0011567888 00 00 00 00 00 00 00 00 00 00 28 00 00 00 DA 08
0011567904 00 BD 11 9A 26 F5 20 15 47 6E 9E 69 DC 02 5E C7
0011567920 A5 A4 41 00 64 00 6D 00 69 00 6E 00 69 00 73 00
0011567936 74 00 72 00 61 00 74 00 6F 00 72 00 28 00 41 00
0011567952 64 00 6D 00 69 00 6E 00 69 00 73 00 74 00 72 00
0011567968 61 00 74 00 6F 00 72 00 40 00 54 00 45 00 4C 00
0011567984 45 00 50 00 52 00 4F 00 29 00 00 00 A9 BC E2 61
0011568000 FC 7E BB 2C BB C3 D4 57 E2 70 78 11 E4 C6 70 95
0011568016 58 F2 A3 D9 E6 1C 86 EC F3 46 4C 1C A6 6C 3D 58
0011568032 D9 1C BB 69 D7 07 22 5B 46 74 2C DB 48 96 EA 9B
0011568048 08 A6 31 B5 F9 13 4D 3B 72 4A 19 D4 30 42 81 6E

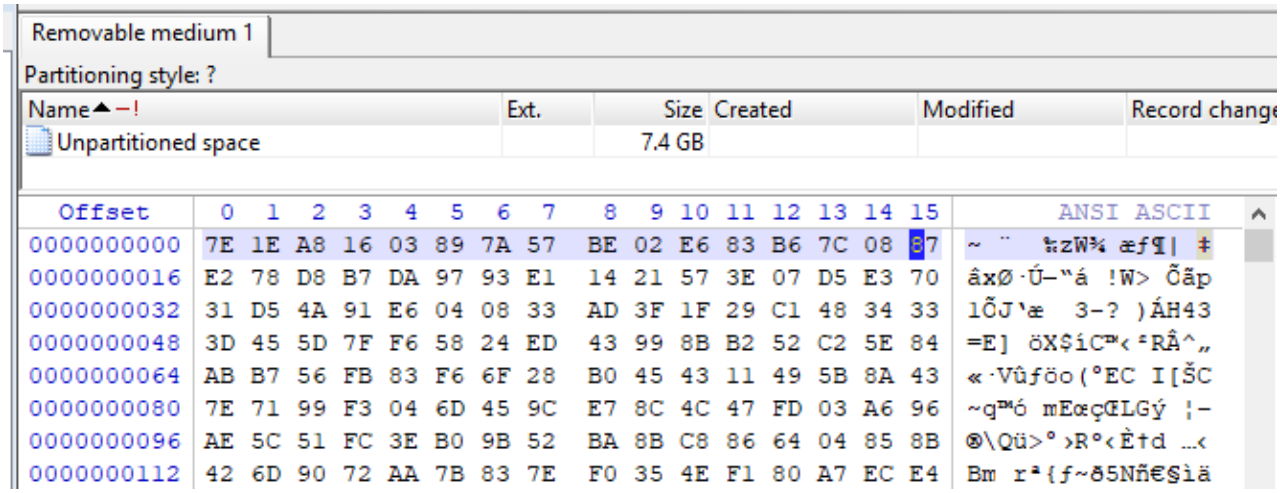
Encrypted Volumes

What are encrypted volumes?

Hex view of an unencrypted partition entry



Hex view of a VeraCrypt encrypted partition file

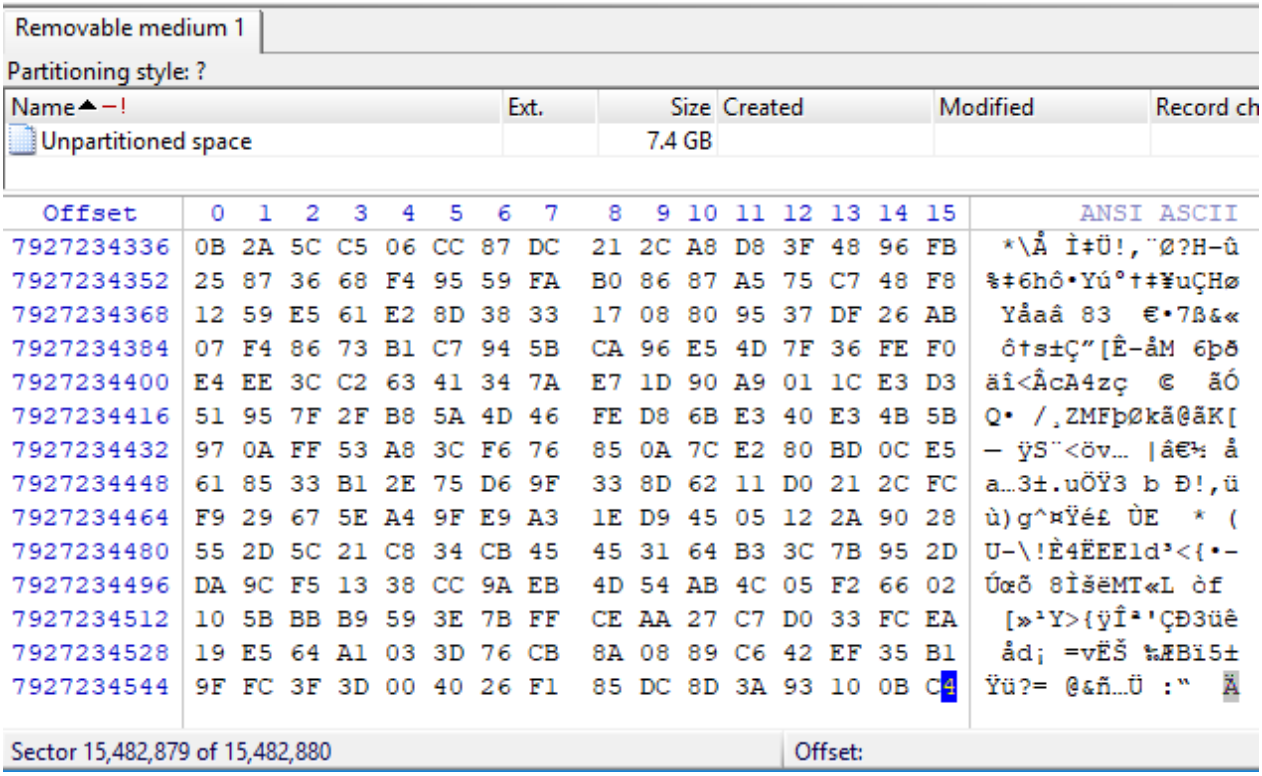


Are there file signatures associated with encrypted volumes?

What methods can we use to identify possible encrypted volumes? Size, signature, entropy

Encrypted Volumes – File Size

Encrypted volume containers will always be divisible by 512.



Removable medium 1

Partitioning style: ?

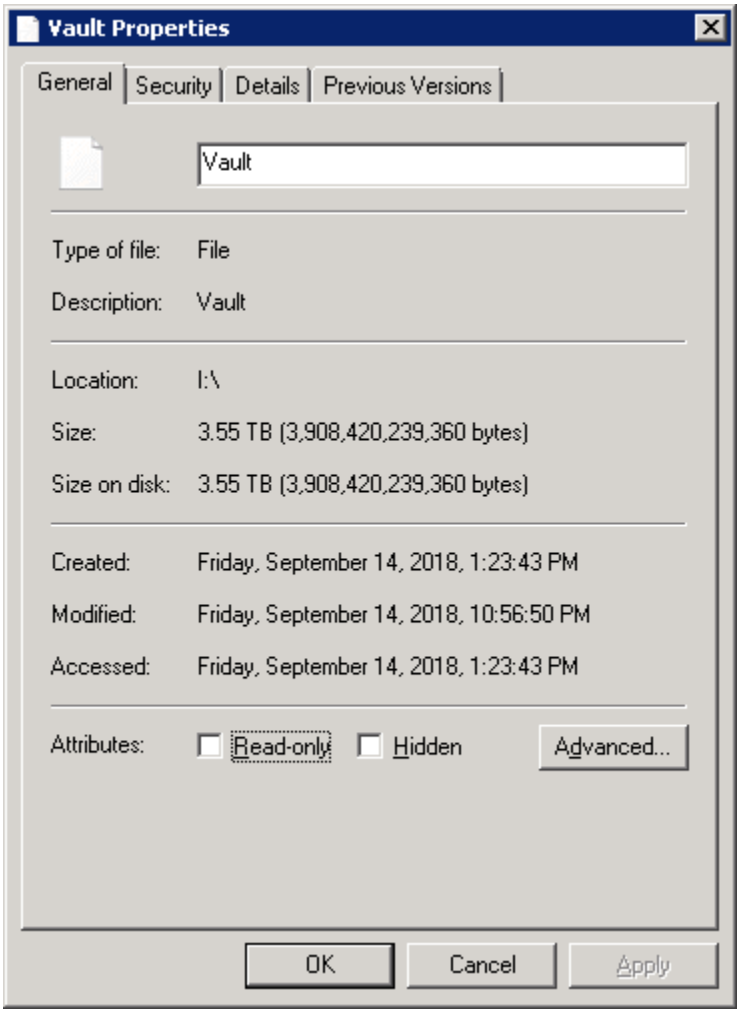
Name	Ext.	Size	Created	Modified	Record ch
Unpartitioned space		7.4 GB			

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
7927234336	0B	2A	5C	C5	06	CC	87	DC	21	2C	A8	D8	3F	48	96	FB	*\Å Ì‡Ü!,¨Ø?H–û
7927234352	25	87	36	68	F4	95	59	FA	B0	86	87	A5	75	C7	48	F8	%‡6hô•Yú°†‡¥uÇHø
7927234368	12	59	E5	61	E2	8D	38	33	17	08	80	95	37	DF	26	AB	Yåaâ 83 €•7ß&«
7927234384	07	F4	86	73	B1	C7	94	5B	CA	96	E5	4D	7F	36	FE	F0	ô†s±Ç”[Ê–åM 6þð
7927234400	E4	EE	3C	C2	63	41	34	7A	E7	1D	90	A9	01	1C	E3	D3	äî<ÂcA4zç © ãÓ
7927234416	51	95	7F	2F	B8	5A	4D	46	FE	D8	6B	E3	40	E3	4B	5B	Q• /¸ZMFþØkã@ãK[
7927234432	97	0A	FF	53	A8	3C	F6	76	85	0A	7C	E2	80	BD	0C	E5	— ÿS¨<öv… \â€½ å
7927234448	61	85	33	B1	2E	75	D6	9F	33	8D	62	11	D0	21	2C	FC	a…3±.uÖŸ3 b Ð!,ü
7927234464	F9	29	67	5E	A4	9F	E9	A3	1E	D9	45	05	12	2A	90	28	ù)g^¤Ÿé£ ÙE * (
7927234480	55	2D	5C	21	C8	34	CB	45	45	31	64	B3	3C	7B	95	2D	U-\!È4ËEEld³<{•-
7927234496	DA	9C	F5	13	38	CC	9A	EB	4D	54	AB	4C	05	F2	66	02	Úœõ 8ÌšëMT«L òf
7927234512	10	5B	BB	B9	59	3E	7B	FF	CE	AA	27	C7	D0	33	FC	EA	[»¹Y>{ÿÎª'ÇÐ3üê
7927234528	19	E5	64	A1	03	3D	76	CB	8A	08	89	C6	42	EF	35	B1	åd¡ =vËŠ ‰ÆBï5±
7927234544	9F	FC	3F	3D	00	40	26	F1	85	DC	8D	3A	93	10	0B	C4	Ÿü?= @&ñ…Ü :“ Ä

Sector 15,482,879 of 15,482,880 Offset:

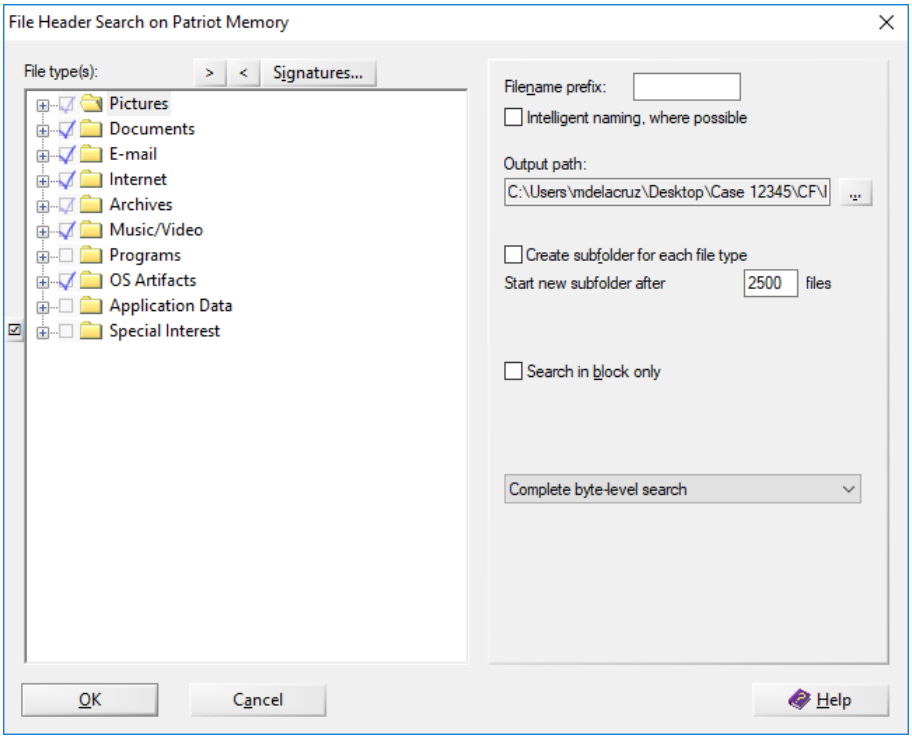
15,482,880 / 512 = 30,240

3,908,420,239,360 / 512 = 7,633,633,280



Encrypted Volumes – File Signature Technique

How can a file signature search be used to identify a possible encrypted volume container?



What would be an unusual number of recovered files for an 8GB file/disk?

```
Removable medium 1
Scope: 0000000000 - 7927234559
Complete byte-level search

0405586214 - 0405848357: 000001.mpx FAILED
0493027533 - 0493627532: 000002.cwk FAILED
0887648503 - 0987648502: 000003.rm FAILED
1372793340 - 1373055483: 000004.mpx FAILED
1644081951 - 1744081950: 000005.rm FAILED
1815542059 - 1815804202: 000006.mpx FAILED
2703763100 - 2712151707: 000007.qdf FAILED
4062527000 - 4062789143: 000008.mpx FAILED
4734810853 - 4735072996: 000009.mpx FAILED
5118321110 - 5118621109: 000010.mid FAILED
7696227194 - 7696231289: 000011.pwl

11/07/2018, 13:58:16
484,440 file headers were found. 1 files were retrieved.
```

Encrypted Volumes – File Entropy

What is an entropy test? Measures the predictability of any specific character in the file.

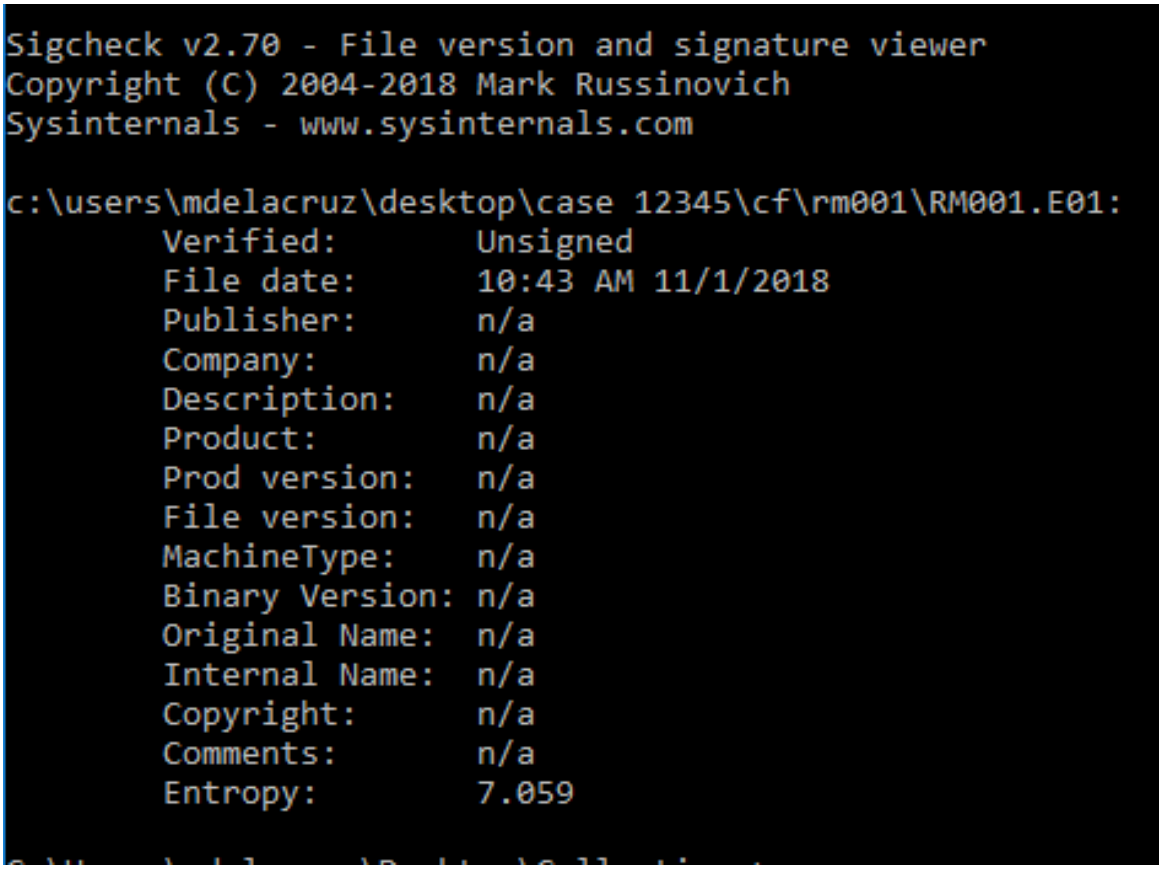
A high entropy score indicates a random or chaotic series.

A low entropy score indicates a high degree of regularity.

Encrypted volumes will always get high entropy scores.

```
Sigcheck v2.70 - File version and signature viewer
Copyright (C) 2004-2018 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\users\mdelacruz\desktop\case 12345\cf\Encrypted.001:
        Verified:       Unsigned
        File date:      2:07 PM 11/7/2018
        Publisher:      n/a
        Company:        n/a
        Description:    n/a
        Product:        n/a
        Prod version:   n/a
        File version:   n/a
        MachineType:    n/a
        Binary Version: n/a
        Original Name:  n/a
        Internal Name:  n/a
        Copyright:      n/a
        Comments:       n/a
        Entropy:        8
```

Entropy test on an unencrypted disk image.



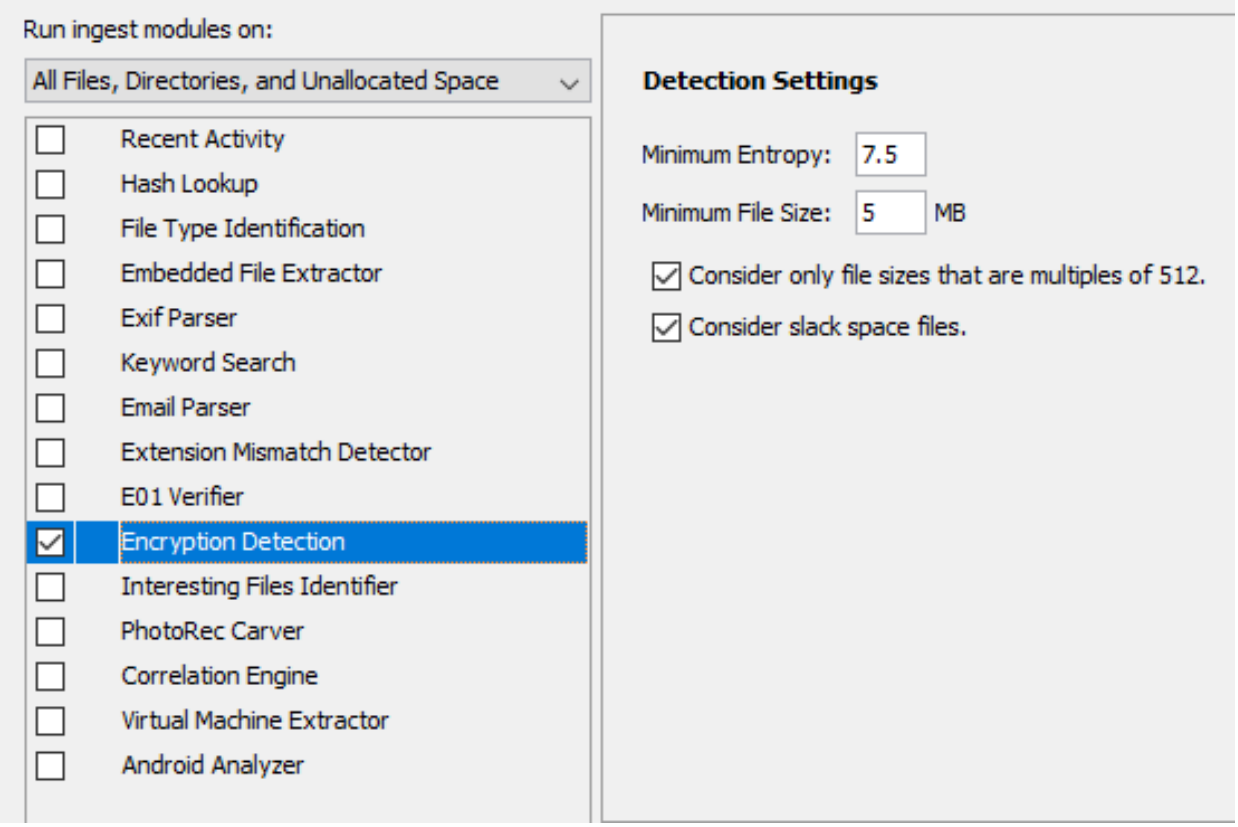
Entropy test on an executable.

```
c:\users\mdelacruz\desktop\collections\ODIN.exe:
        Verified:       Unsigned
        Link date:      9:52 AM 10/9/2011
        Publisher:      n/a
        Company:        n/a
        Description:    ODIN Executable Module
        Product:        ODIN
        Prod version:   0, 3, 4, 308
        File version:   0, 3, 4, 308
        MachineType:    32-bit
        Binary Version: 0.3.4.308
        Original Name:  ODIN.exe
        Internal Name:  ODIN
        Copyright:      Copyright 2011 Licensed under the GNU
        Comments:       n/a
        Entropy:        6.299
```

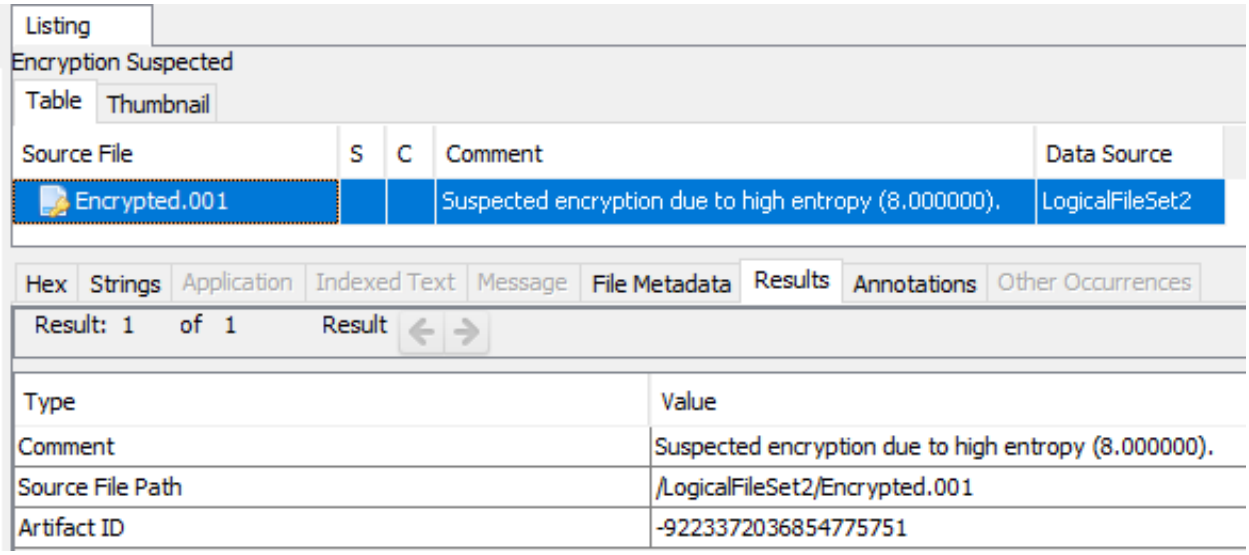
Entropy test on a Powershell script.

```
c:\users\mdelacruz\desktop\collections\touch.ps1:
        Verified:       Unsigned
        File date:      10:42 AM 11/2/2018
        Publisher:      n/a
        Company:        n/a
        Description:    n/a
        Product:        n/a
        Prod version:   n/a
        File version:   n/a
        MachineType:    n/a
        Binary Version: n/a
        Original Name:  n/a
        Internal Name:  n/a
        Copyright:      n/a
        Comments:       n/a
        Entropy:        4.349
```

Automating an Entropy Test Scan

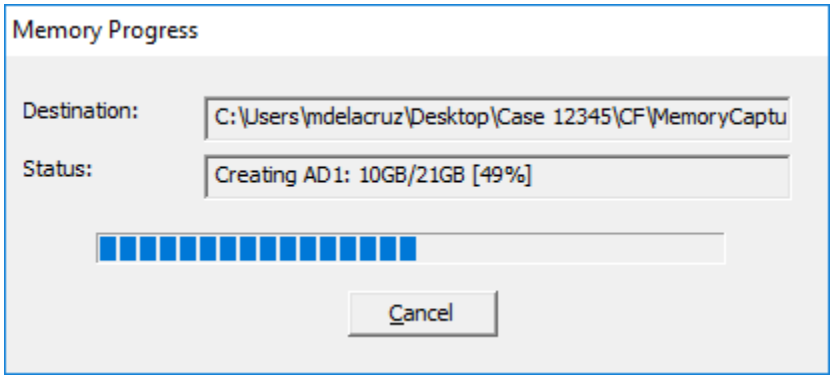


Reviewing the Entropy Scan results

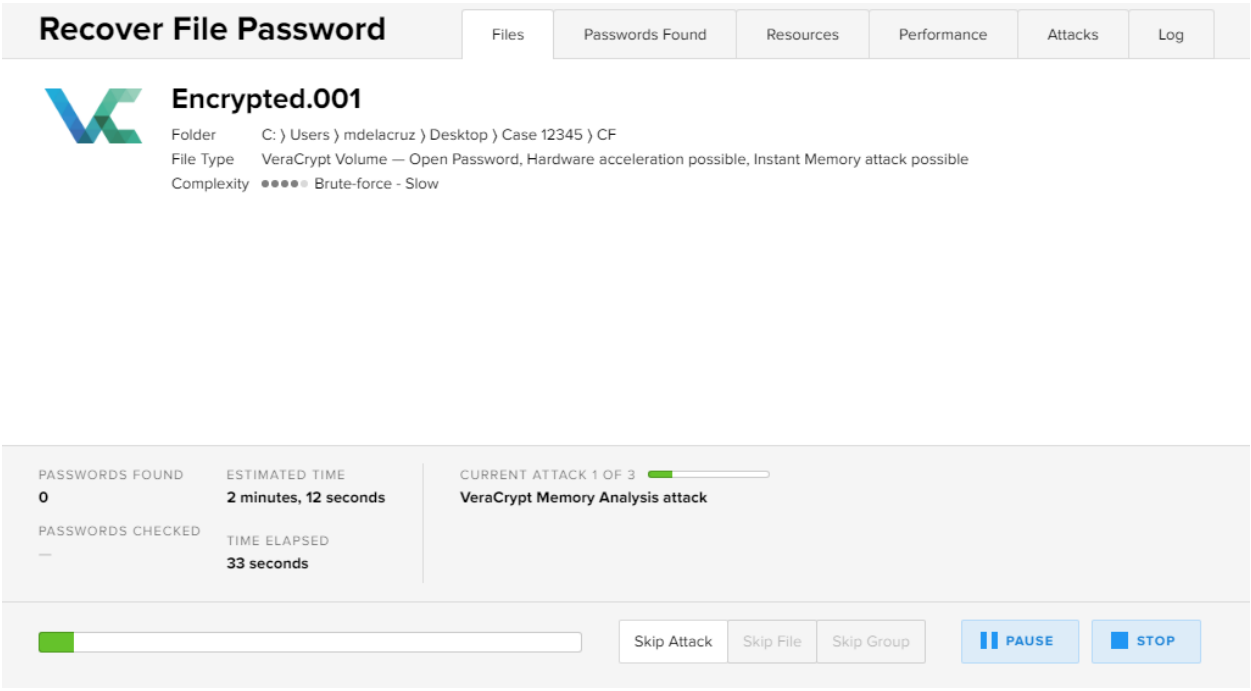


Decrypting a Veracrypt container

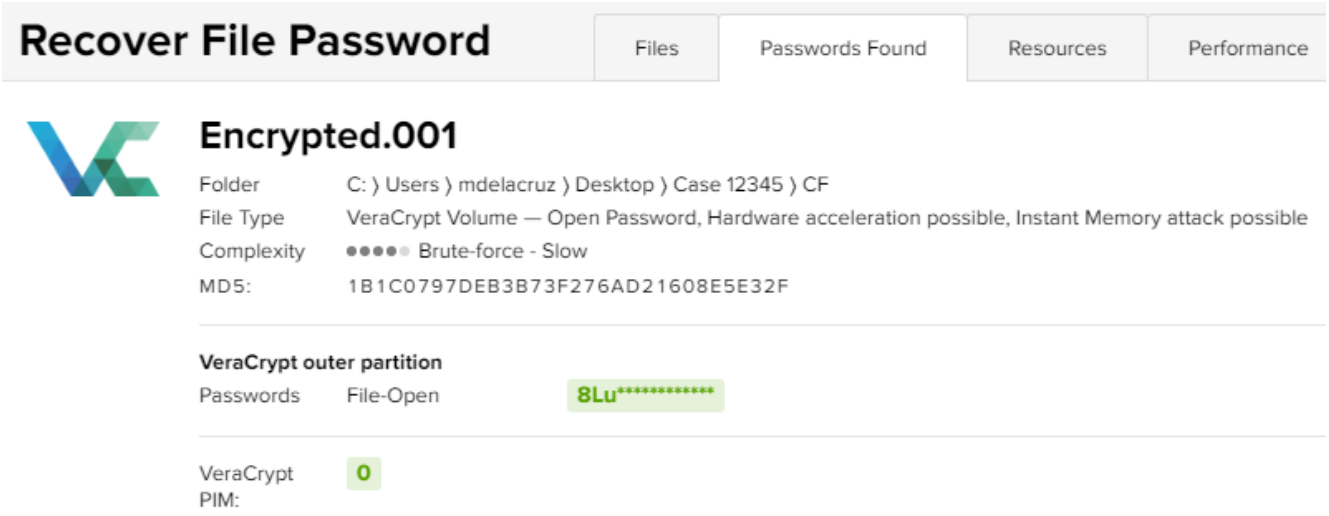
Why is a memory capture important to obtain on a live system?



Using a memory dump to decrypt a Veracrypt container.

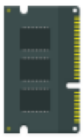


Using a brute-force attack to decrypt a Veracrypt container.



Password recovery from a memory dump.

Recover File Password



memdump.mem

Folder	C: ⟩ Users ⟩ mdelacruz ⟩ Desktop ⟩ Case 12345 ⟩ CF ⟩ MemoryCapture
File Type	Websites from a memory image
Complexity	●○○○○ Instant Unprotection
Memory image file:	C: ⟩ Users ⟩ mdelacruz ⟩ Desktop ⟩ Case 12345 ⟩ CF ⟩ MemoryCapture ⟩ memdump.mem
MD5:	4FFE9E445EEEE02631783E21BF4353A9

Websites Passwords

Site: an		
Accounts' passwords		PD
Site: http://aS1.		
Accounts' passwords		Set**********
Site: secure.comodo.com		
Accounts' passwords	michael@m2rgv.com	Ful**********
Site: www.anyA		
Accounts' passwords		Par**********
Site: www.anyd		
Accounts' passwords		L
Site: www.anyde		
Accounts' passwords		hes**********
Site: Unknown Websites		
Accounts' passwords	michael	b81**********
		Has
		Hes**********
		K
		Kod**********
		P
		Pa
		Pas**********
		Sal**********
		Wa
		o
		pwd

Memory Forensics

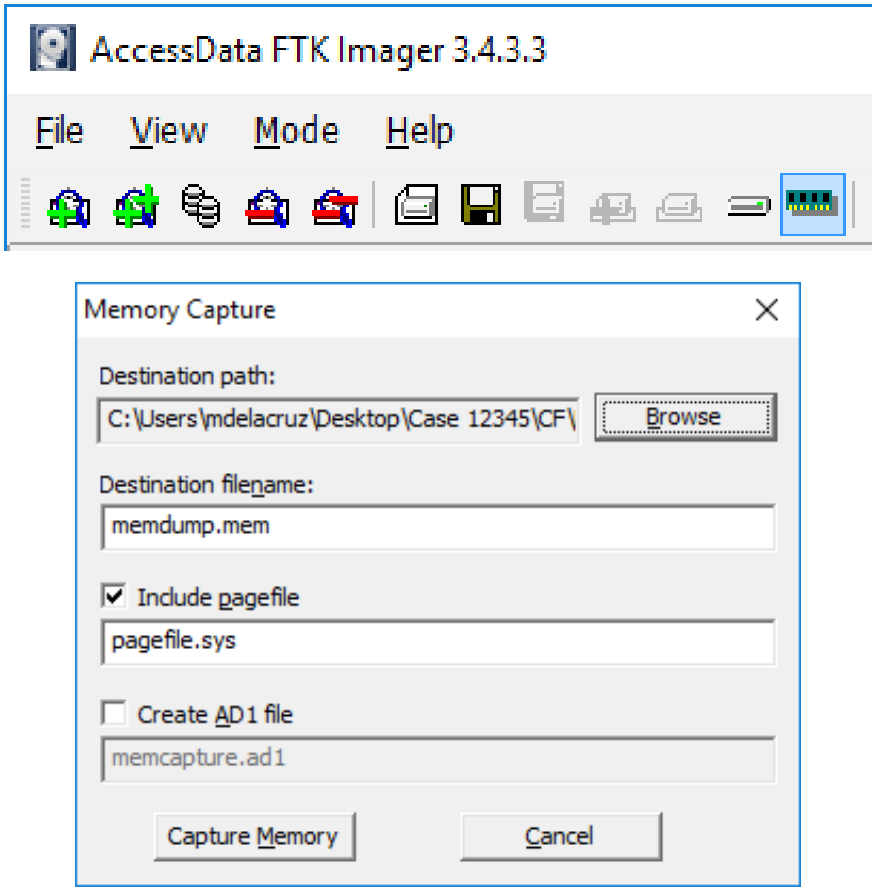
What is memory forensics? The analysis of volatile data in a computer's memory dump.

What information can be extracted from a memory image? Running programs, OS info, passwords.

What is the pagefile.sys file? A reserved portion of a hard disk used as an extension of memory.

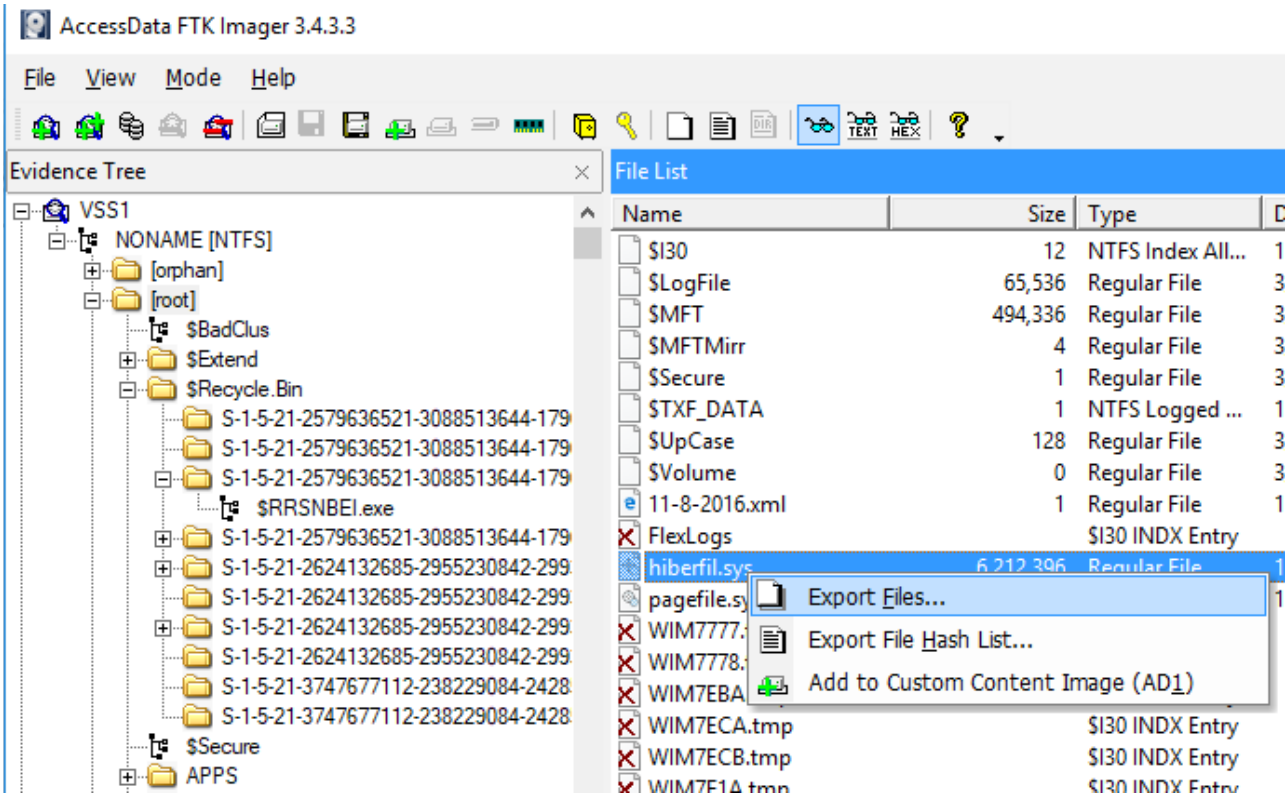
Analyzing the pagefile with AXIOM

Memory Capture with FTK



What is the hiberfil.sys file? A compressed copy of memory that Windows creates when the computer goes into hibernation mode.

Copying out the hiberfil.sys file with FTK



How do you convert the hiberfil.sys file into a format that can be parsed by Volatility? Use Volatility to convert the compressed file into a raw memory dump that can then be processed by Volatility.

volatility_2.6_win64_standalone.exe -f "C:\Users\mdelacruz\Desktop\Case 12345\CF\VSS\VSS1\hiberfil.sys" --profile=Win7SP0x64 imagecopy -O "C:\Users\mdelacruz\Desktop\Case 12345\CF\VSS\VSS1\hiberfil.raw"

```
C:\Users\mdelacruz\Desktop\Case 12345\CF\MemoryCapture>volatility_2.6_win64_standalone.exe -f "C:\Users\mdelacruz\Desktop\Case 12
345\CF\VSS\VSS7\hiberfil.sys" --profile=Win7SP0x64 imagecopy -O "C:\Users\mdelacruz\Desktop\Case 12345\CF\VSS\VSS7\hiberfil.raw"
Volatility Foundation Volatility Framework 2.6
Writing data (5.00 MB chunks): |.....................................................................................................
.....................................................................
```

Hash the hiberfil RAW files with HashCalc to verify they are unique

Identify the memory profile from the RAW hiberfil file

volatility_2.6_win64_standalone.exe imageinfo -f "C:\Users\mdelacruz\Desktop\Case 12345\CF\VSS\VSS1\hiberfil.raw"

```
C:\Users\mdelacruz\Desktop\Case 12345\CF\MemoryCapture>volatility_2.6_win64_standalone.exe imageinfo -f "C:\Users\mdelacruz\Deskt
op\Case 12345\CF\VSS\VSS1\hiberfil.raw"
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_2341
8
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\mdelacruz\Desktop\Case 12345\CF\VSS\VSS1\hiberfil.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80003055110L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80003056d00L
                KPCR for CPU 1 : 0xfffff880009ec000L
                KPCR for CPU 2 : 0xfffff88002f65000L
                KPCR for CPU 3 : 0xfffff88002fd7000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2017-04-24 23:38:32 UTC+0000
     Image local date and time : 2017-04-24 18:38:32 -0500
```

List the registry hive

volatility_2.6_win64_standalone.exe -f "C:\Users\mdelacruz\Desktop\Case 12345\CF\VSS\VSS1\hiberfil.raw" hivelist --profile=Win7SP0x64

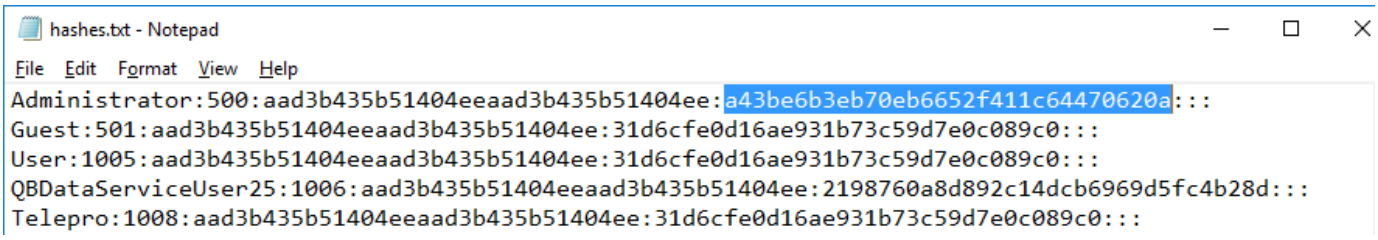
```
C:\Users\mdelacruz\Desktop\Case 12345\CF\MemoryCapture>volatility_2.6_win64_standalone.exe -f "C:\Users\mdelacruz\Desktop\Case 12
345\CF\VSS\VSS1\hiberfil.raw" hivelist --profile=Win7SP0x64
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a000152010 0x00000000002f2010 \??\C:\Users\User\ntuser.dat
0xfffff8a0023f9010 0x00000001de7ce010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a0023fa410 0x00000001de7cf410 \SystemRoot\System32\Config\SAM
0xfffff8a0023fd010 0x00000001de812010 \SystemRoot\System32\Config\SECURITY
0xfffff8a0023ff010 0x00000001e0d20010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a002fb4010 0x00000001bf74f010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a002ffa010 0x00000001bbd49010 \??\C:\Users\User\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a003008010 0x00000001c10f3010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a004355010 0x00000001681f6010 \??\C:\Users\QBDataServiceUser25\ntuser.dat
0xfffff8a004391410 0x00000001680c6410 \??\C:\Users\QBDataServiceUser25\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a004b05010 0x000000019e9aa010 \??\C:\Windows\AppCompat\Programs\Amcache.hve
0xfffff8a014d92010 0x00000001316e0010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a00000e010 0x00000001e3f80010 [no name]
0xfffff8a000024010 0x00000000002a8010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000063010 0x00000000002e8010 \REGISTRY\MACHINE\HARDWARE
```

Extract the hashes using the Virtual addresses for the SYSTEM (-y) and SAM (-s) files

volatility_2.6_win64_standalone.exe -f "C:\Users\mdelacruz\Desktop\Case 12345\CF\VSS\VSS1\hiberfil.raw" --profile=Win7SP0x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a0023fa410 > "C:\Users\mdelacruz\Desktop\Case 12345\CF\VSS\VSS1\hashes.txt"

```
C:\Users\mdelacruz\Desktop\Case 12345\CF\MemoryCapture>volatility_2.6_win64_standalone.exe -f "C:\Users\mdelacruz\Desktop\Case 12
345\CF\VSS\VSS1\hiberfil.raw" --profile=Win7SP0x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a0023fa410 > "C:\Users\mdelacruz\Des
ktop\Case 12345\CF\VSS\VSS1\hashes.txt"
Volatility Foundation Volatility Framework 2.6
```

Viewing the exported hashes.txt file



Identify the memory profile from the MemDump

volatility_2.6_win64_standalone.exe imageinfo -f memdump.bin

```
C:\Users\mdelacruz\Desktop\Case 12345\CF\MemoryCapture>volatility_2.6_win64_standalone.exe imageinfo -f memdump.bin
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win2003SP0x86, Win2003SP1x86, Win2003SP2x86 (Instantiated with Win2003SP0x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\mdelacruz\Desktop\Case 12345\CF\MemoryCapture\memdump.bin)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x805583d0L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2012-11-27 02:01:57 UTC+0000
     Image local date and time : 2012-11-26 20:01:57 -0600
```

List the registry hive

volatility_2.6_win64_standalone.exe -f memdump.mem hivelist –profile=Win2003SP0x86

```
C:\Users\mdelacruz\Desktop\Case 12345\CF\MemoryCapture>volatility_2.6_win64_standalone.exe -f memdump.bin hivelist --profile=Win2003SP0x86
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe142fa90 0x05df8a90 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1241008 0x06024008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe142d958 0x05df6958 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe1417938 0x0486b938 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe1230008 0x02d17008 [no name]
0xe10192a8 0x02adf2a8 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe1013008 0x02afa008 [no name]
0xe10a4008 0x1e96b008 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe10273d0 0x1f74e3d0 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
0xe15f7a90 0x009b6a90 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe15eba90 0x001dca90 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe15e1760 0x00109760 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe15da8e8 0x009708e8 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
```

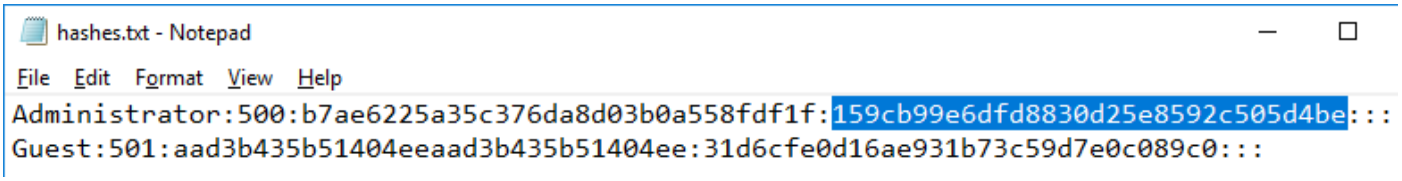
Extract the hashes

volatility_2.6_win64_standalone.exe -f memdump.bin --profile=Win2003SP0x86 hashdump -y 0xe10192a8 -s 0xe1417938 > hashes.txt

```
C:\Users\mdelacruz\Desktop\Case 12345\CF\MemoryCapture>volatility_2.6_win64_standalone.exe -f memdump.bin --profile=Win2003SP0x86 hashdump -y 0xe10192a
8 -s 0xe1417938 > hashes.txt
Volatility Foundation Volatility Framework 2.6
```

Crack the hashes

Open the output file



Run it through an NTLM hash crack tool

Date	Hash	Algorithm	Priority	Status	Size
2018-11-09	31D6CFE0D16AE931B73C59D7E0C089C0	NTLM	Normal	FOUND !	0
2018-11-09	159CB99E6DFD8830D25E8592C505D4BE	NTLM	Normal	FOUND !	13

NTLM hash crack completed in under 5 minutes.

Password Recovery

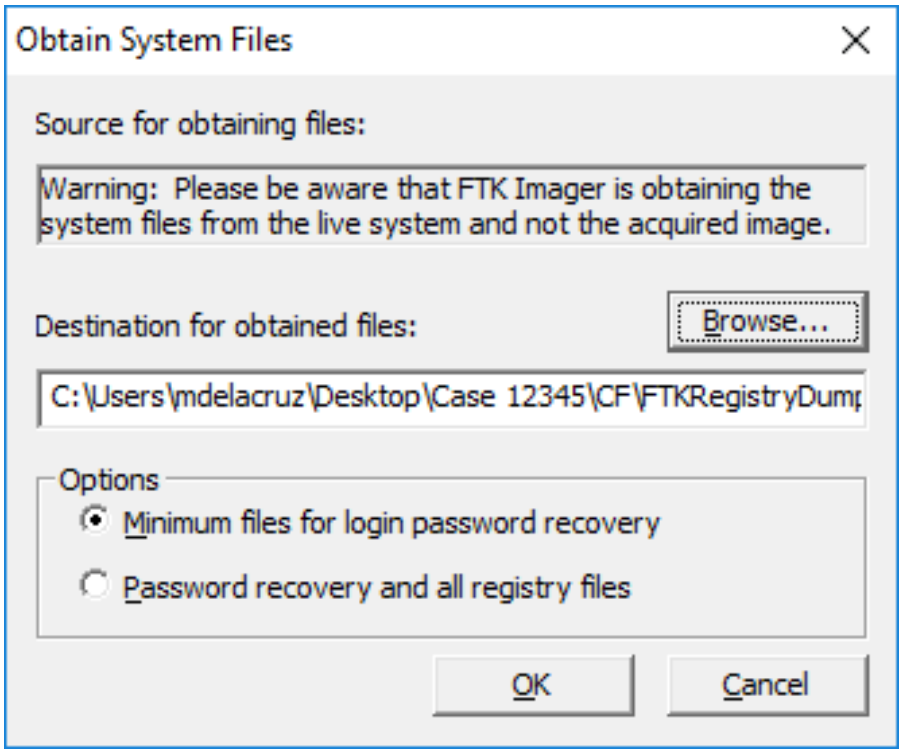
Why would I need to crack a local password?

What files are needed to crack local passwords?

What is a SAM file?

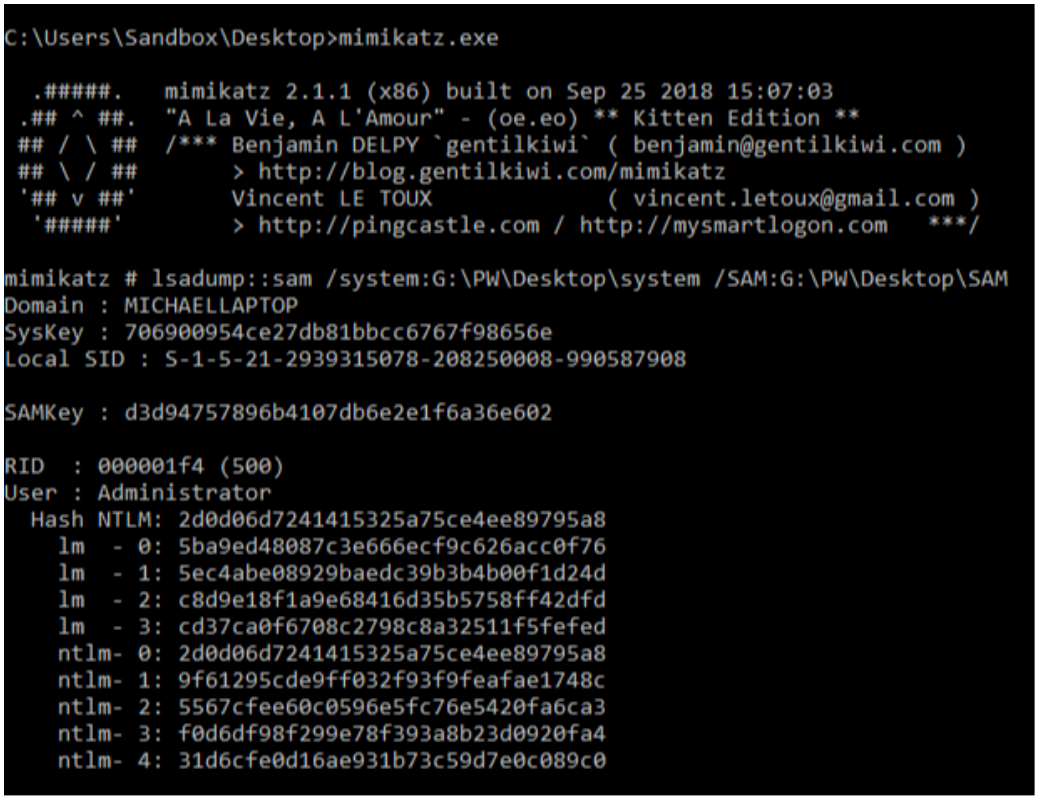
How do you obtain the files needed for a password recovery?

How long does it take to crack once an NTLM hash has been extracted? Up to 3 days, but usually under 24 hours.



Extract the NTLM hashes from the SAM database. (Run as Administrator)

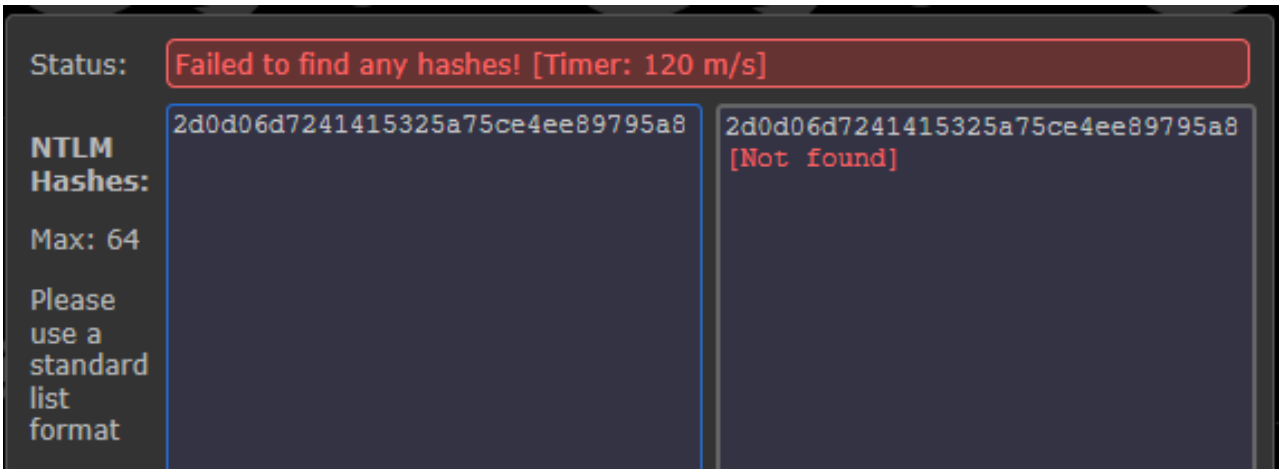
NTLM Hash: 2d0d06d7241415325a75ce4ee89795a8



Crack the extracted NTLM hash

What is Hashcat? A CPU & GPU-based password recovery tool.

What is Hashkiller? Free online searchable database of over 312 Billion unique decrypted NTLM hashes since August 2007. https://hashkiller.co.uk/



What are rainbow tables? Pre-computed tables for cracking password hashes.

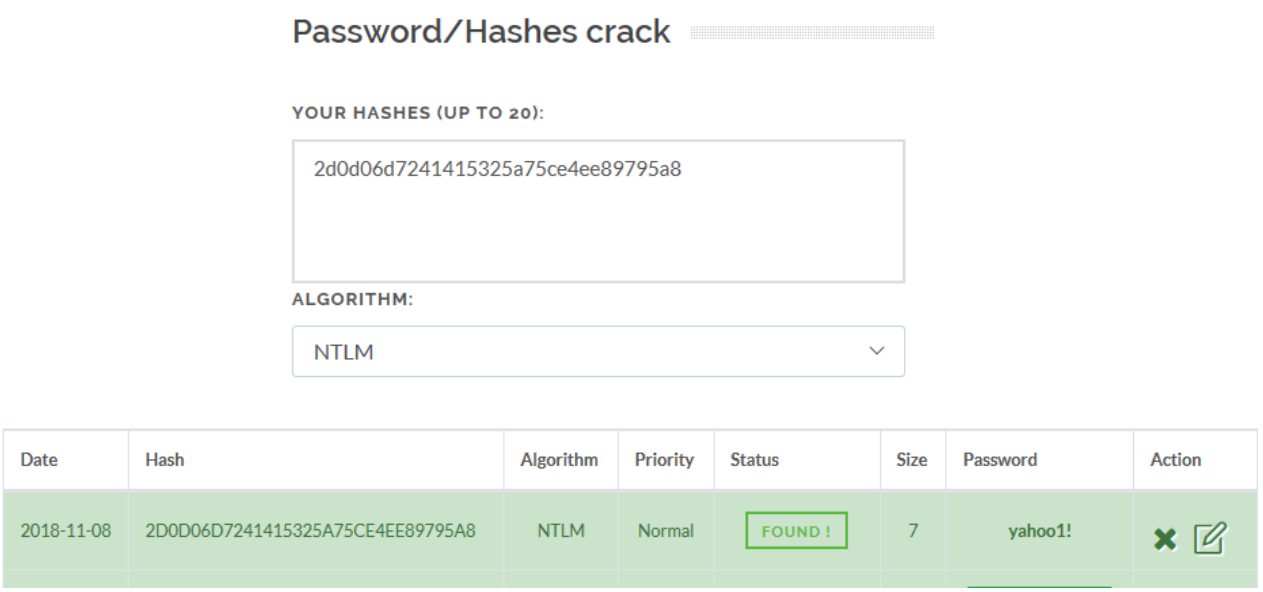
NTLM, MD5 and SHA1 Perfect Rainbow Tables (USD 2400)

Includes:

- Perfect Rainbow Tables

Table ID	Charset	Plaintext Length	Success Rate	Table Size
lm_ascii-32-65-123-4#1-7	All 95 characters on standard keyboard	1 to 14	99.9 %	27 GB
ntlm_ascii-32-95#1-7	All 95 characters on standard keyboard	1 to 7	99.9 %	52 GB
ntlm_ascii-32-95#1-8	All 95 characters on standard keyboard	1 to 8	96.8 %	460 GB
ntlm_mixalpha-numeric#1-8	a-z, A-Z, 0-9	1 to 8	99.9 %	127 GB
ntlm_mixalpha-numeric#1-9	a-z, A-Z, 0-9	1 to 9	96.8 %	690 GB
ntlm_loweralpha-numeric#1-9	a-z, 0-9	1 to 9	99.9 %	65 GB
ntlm_loweralpha-numeric#1-10	a-z, 0-9	1 to 10	96.8 %	316 GB
md5_ascii-32-95#1-7	All 95 characters on standard keyboard	1 to 7	99.9 %	52 GB
md5_ascii-32-95#1-8	All 95 characters on standard keyboard	1 to 8	96.8 %	460 GB
md5_mixalpha-numeric#1-8	a-z, A-Z, 0-9	1 to 8	99.9 %	127 GB
md5_mixalpha-numeric#1-9	a-z, A-Z, 0-9	1 to 9	96.8 %	690 GB
md5_loweralpha-numeric#1-9	a-z, 0-9	1 to 9	99.9 %	65 GB
md5_loweralpha-numeric#1-10	a-z, 0-9	1 to 10	96.8 %	316 GB
sha1_ascii-32-95#1-7	All 95 characters on standard keyboard	1 to 7	99.9 %	52 GB
sha1_ascii-32-95#1-8	All 95 characters on standard keyboard	1 to 8	96.8 %	460 GB
sha1_mixalpha-numeric#1-8	a-z, A-Z, 0-9	1 to 8	99.9 %	127 GB
sha1_mixalpha-numeric#1-9	a-z, A-Z, 0-9	1 to 9	96.8 %	690 GB
sha1_loweralpha-numeric#1-9	a-z, 0-9	1 to 9	99.9 %	65 GB
sha1_loweralpha-numeric#1-10	a-z, 0-9	1 to 10	96.8 %	316 GB

Online Hash Crack - https://www.onlinehashcrack.com/

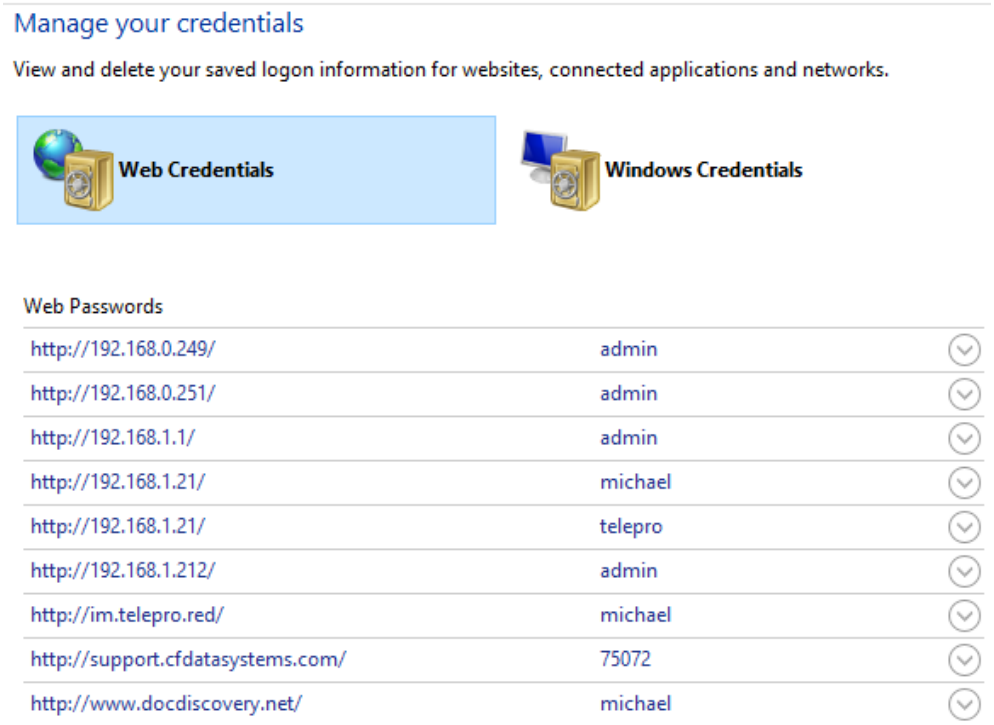


Why is it beneficial to have the local administrator password?

What other hashes can be cracked online?

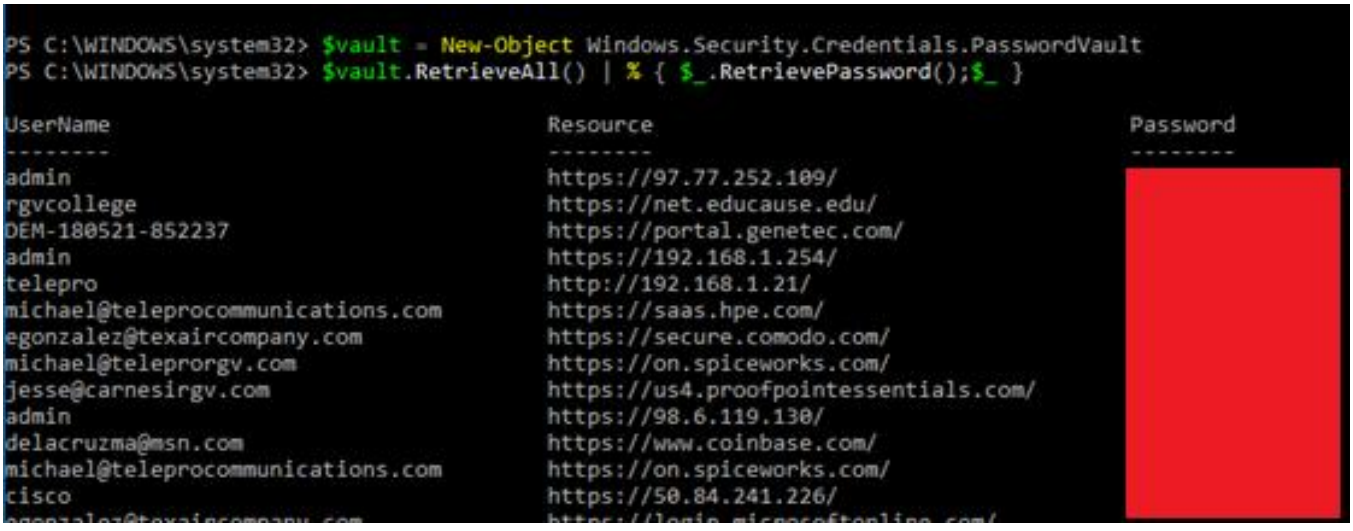
Password Extraction

Windows Credential Manager



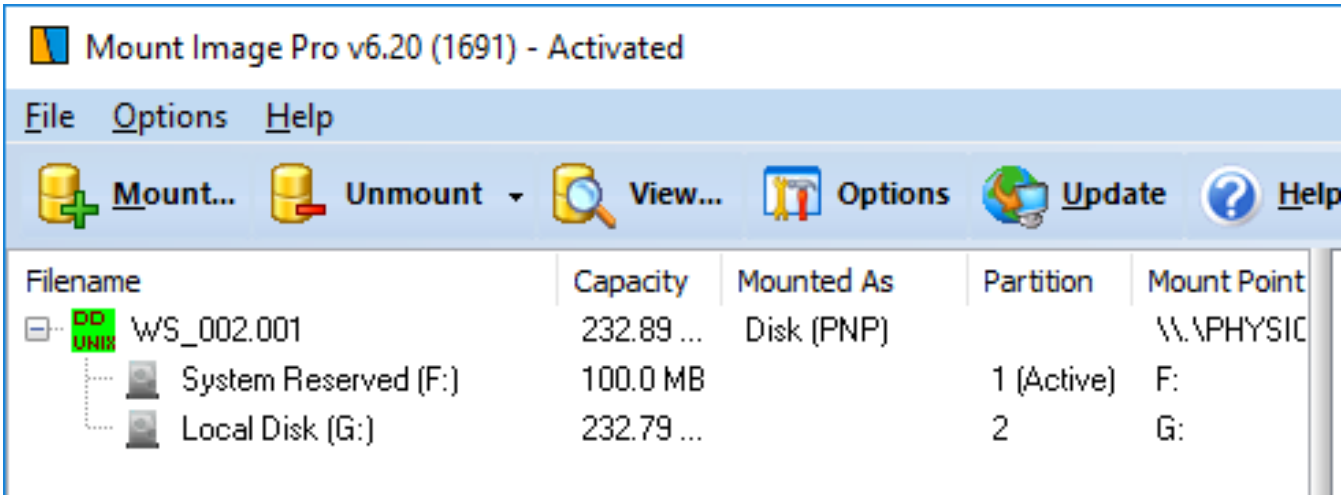
Powershell script to extract passwords from currently logged on user's password vault

$vault = New-Object Windows.Security.Credentials.PasswordVault
$vault.RetrieveAll() | % { $_.RetrievePassword();$_ }



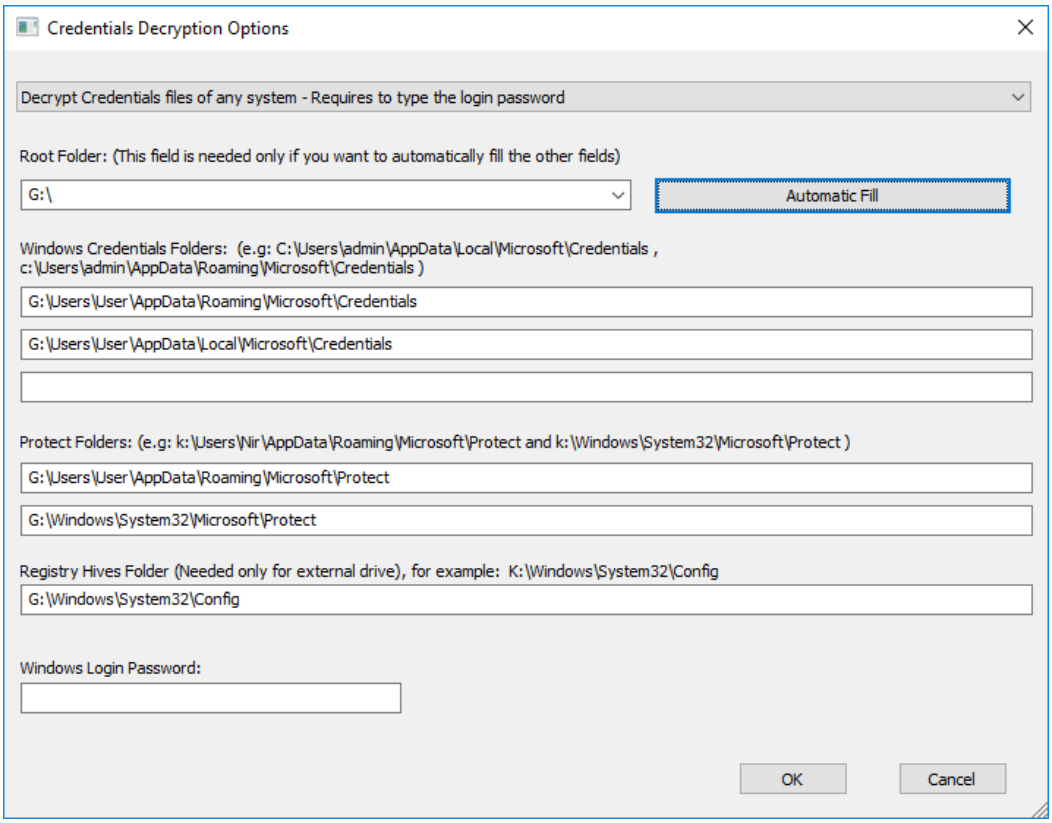
Password Extraction from a Forensic Image

Mount the forensic image with Mount Image Pro

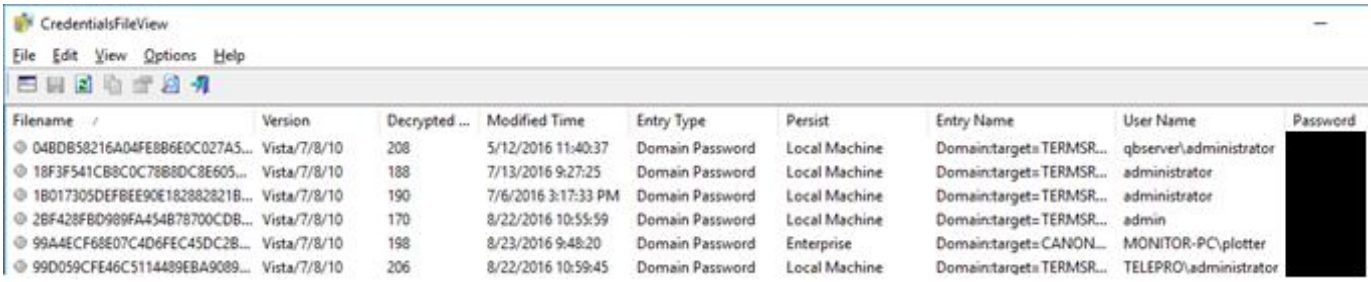


Download Credential File View - https://www.nirsoft.net/utils/credentials_file_view.html

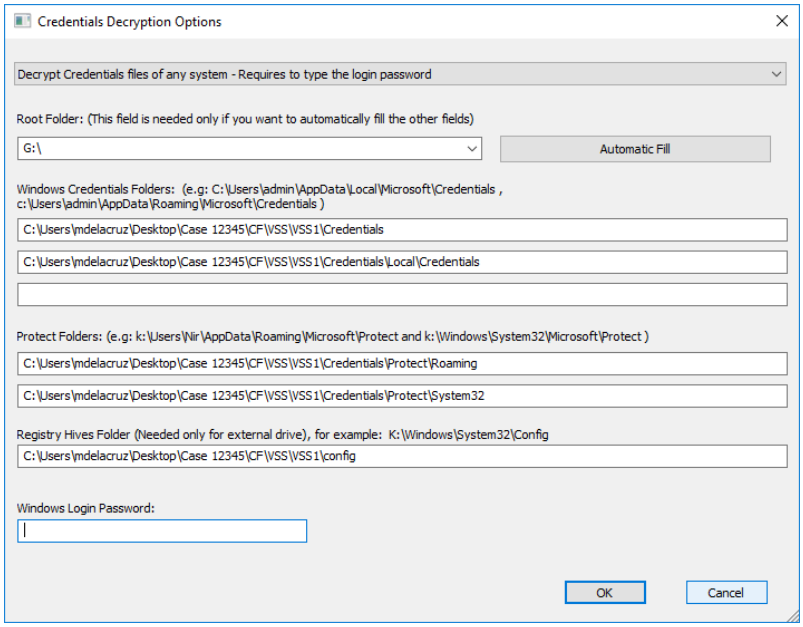
Select the drive letter the image was mounted on, and click Automatic Fill

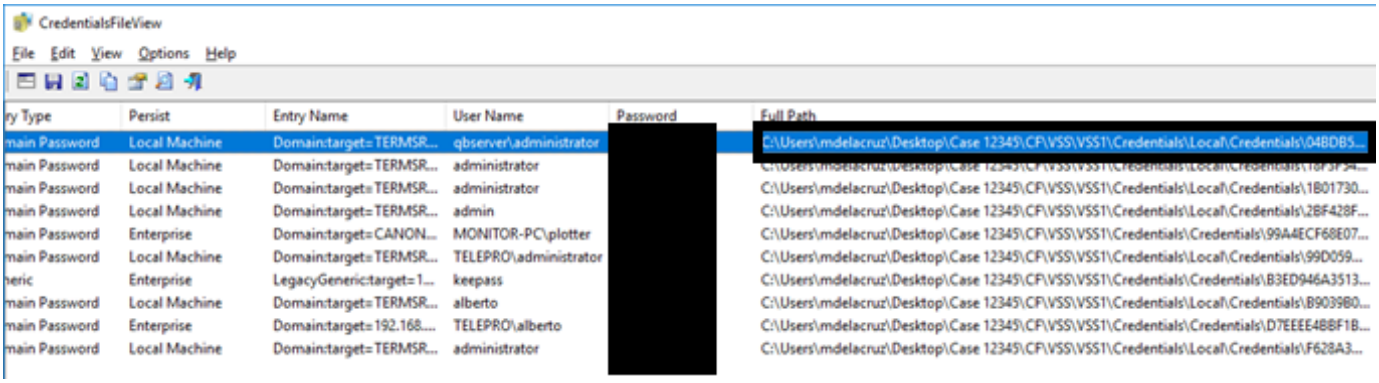

Credentials Decryption Options
Decrypt Credentials files of any system - Requires to type the login password
Root Folder: (This field is needed only if you want to automatically fill the other fields)
G:\
Automatic Fill
Windows Credentials Folders: (e.g: C:\Users\admin\AppData\Local\Microsoft\Credentials , c:\Users\admin\AppData\Roaming\Microsoft\Credentials)
G:\Users\User\AppData\Roaming\Microsoft\Credentials
G:\Users\User\AppData\Local\Microsoft\Credentials
Protect Folders: (e.g: k:\Users\Nir\AppData\Roaming\Microsoft\Protect and k:\Windows\System32\Microsoft\Protect)
G:\Users\User\AppData\Roaming\Microsoft\Protect
G:\Windows\System32\Microsoft\Protect
Registry Hives Folder (Needed only for external drive), for example: K:\Windows\System32\Config
G:\Windows\System32\Config
Windows Login Password:
OK
Cancel

Usernames and decrypted passwords are displayed



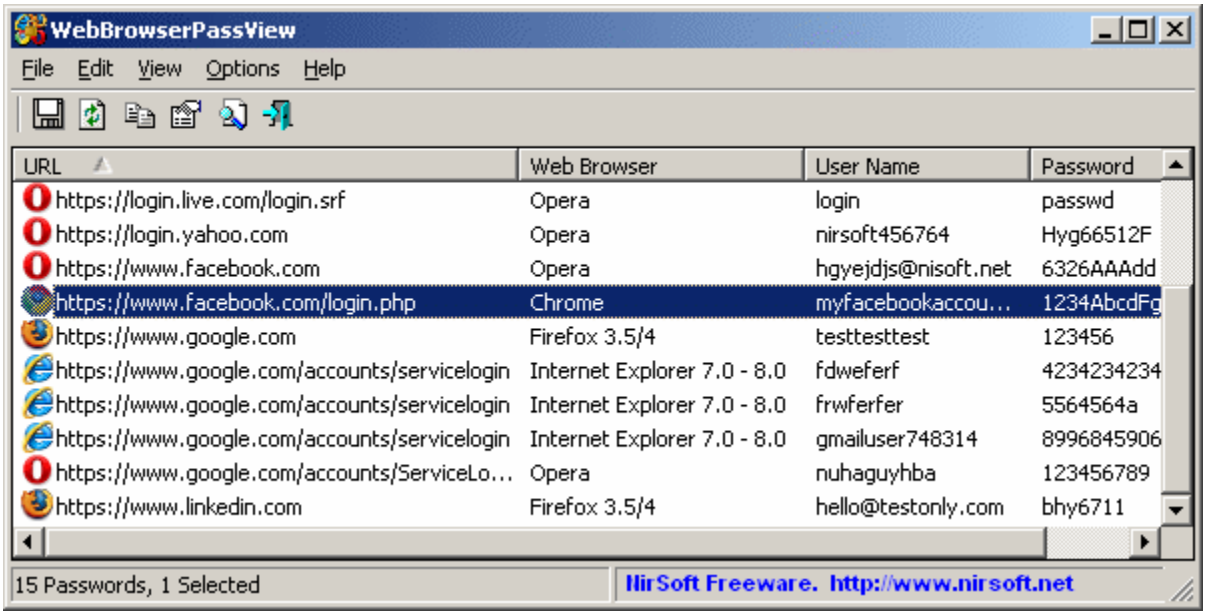
Password Vault's can also be extracted from each of the VSS snapshots and decrypted with Credential File View. Do not use the autofill option. Path locations will need to be manually entered to point to the VSS export folders.





Recovering Stored Web Passwords

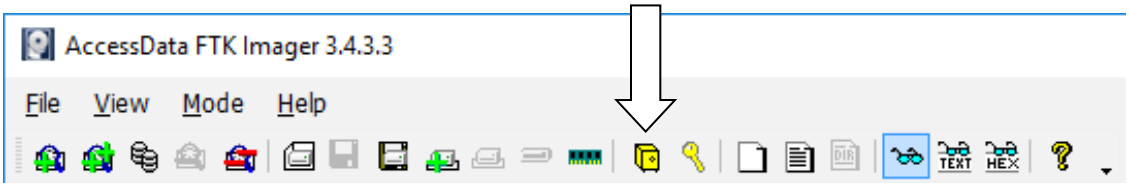
WebBrowserPassView - http://www.nirsoft.net/utils/web_browser_password.html



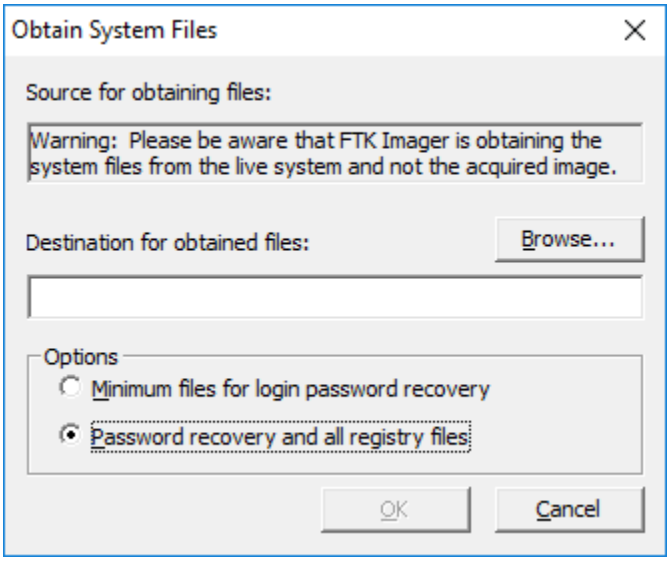
Identifying Attached USB Devices

Extracting the SYSTEM file and setupapi.app.log files from a live system

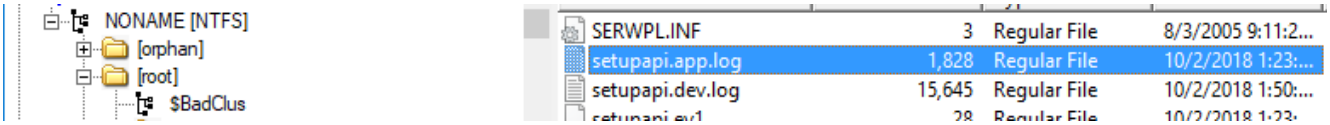
Obtain Protected Files with FTK



Select Password recovery and all registry files

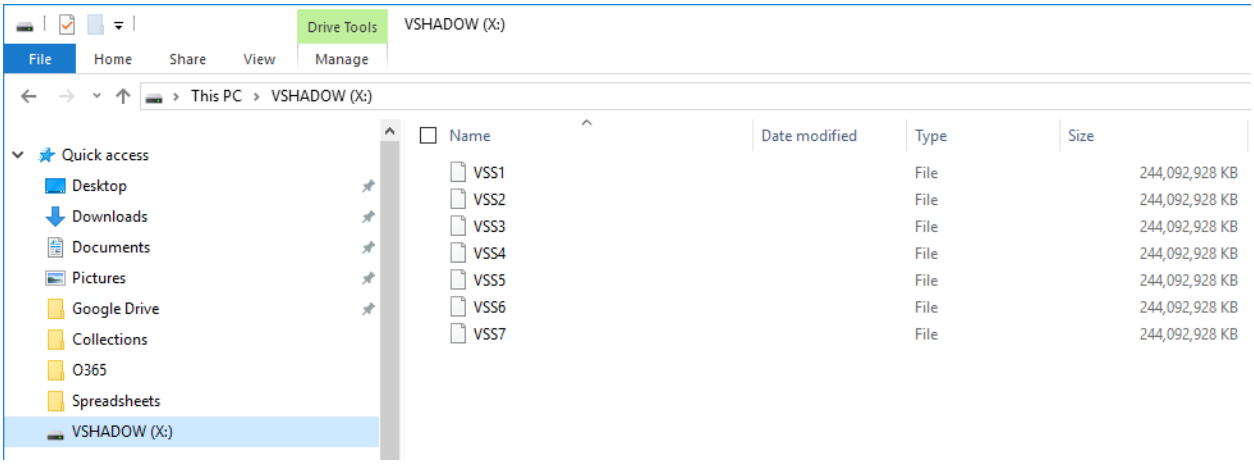


Extract the C:\Windows\inf\setupapi.app.log file

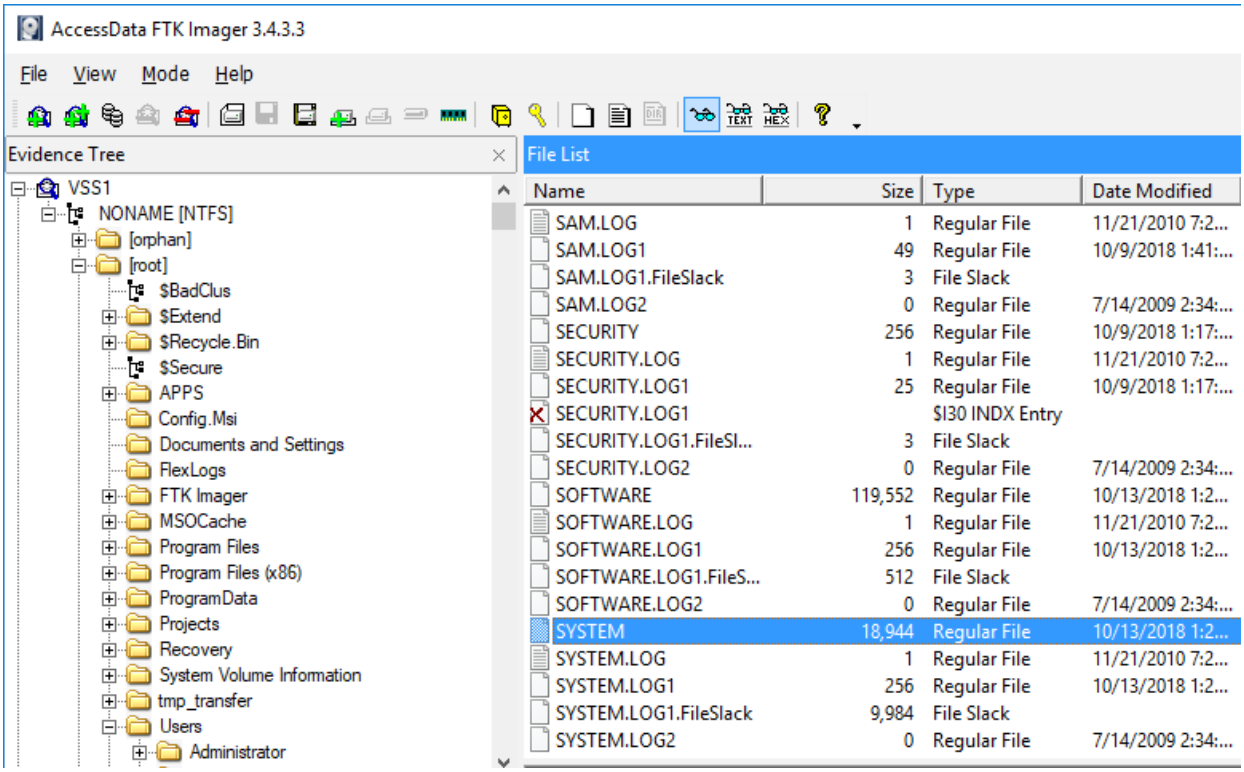


Extracting the SYSTEM file and setupapi.app.log files from a VSS snapshot

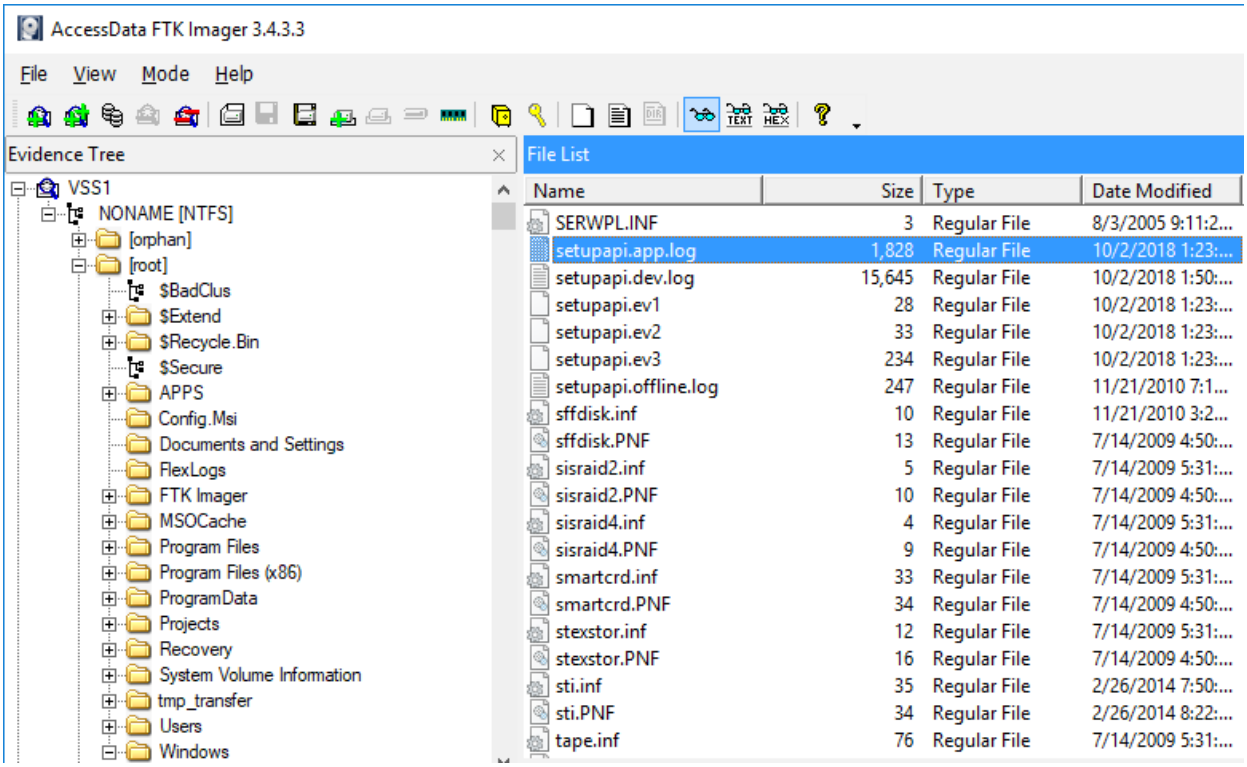
Assuming the VSS snapshots are still mounted with vshadowmount



For each VSS snapshot, extract the SYSTEM file

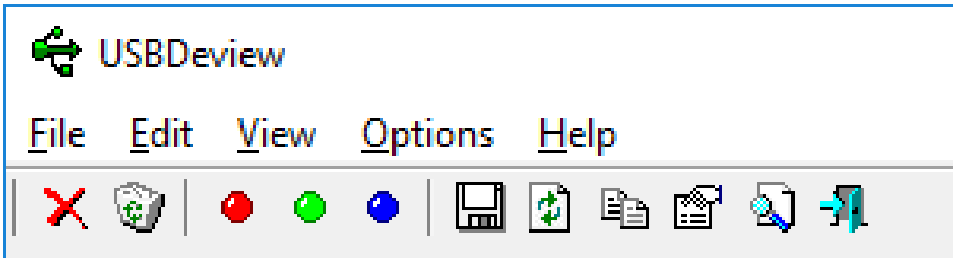


For each VSS snapshot, extract the C:\Windows\inf\setupapi.app.log file

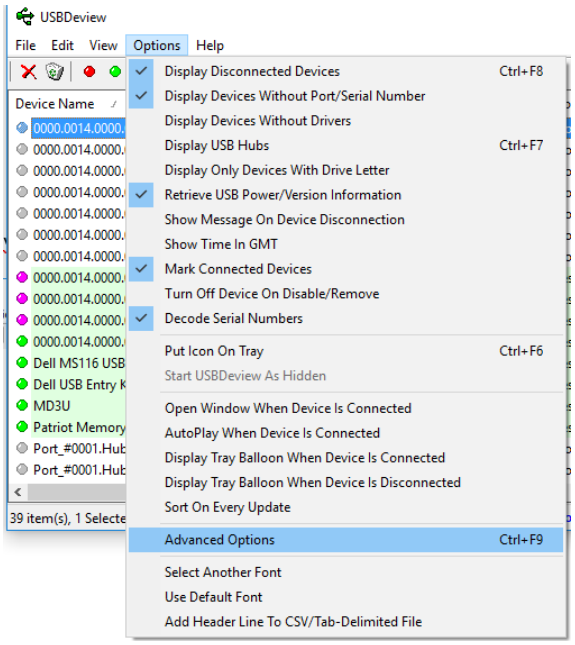


Creating the USB Devices Report

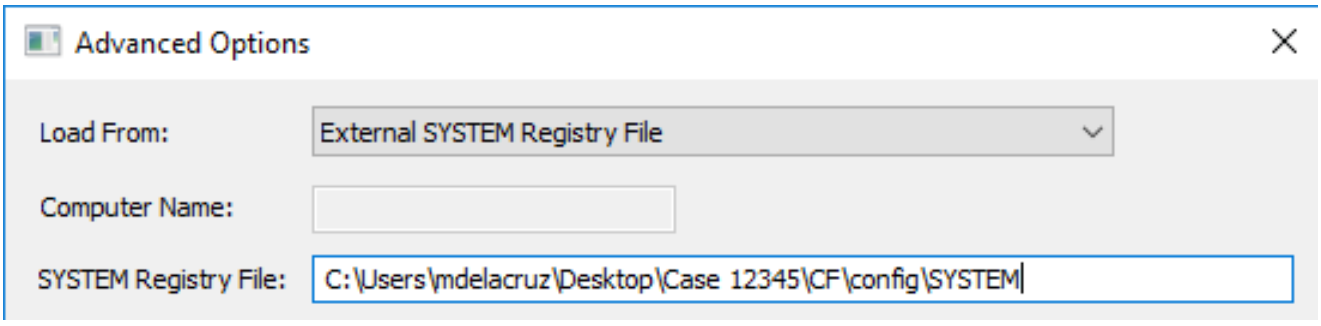
Open USBDeview (Run as Administrator)



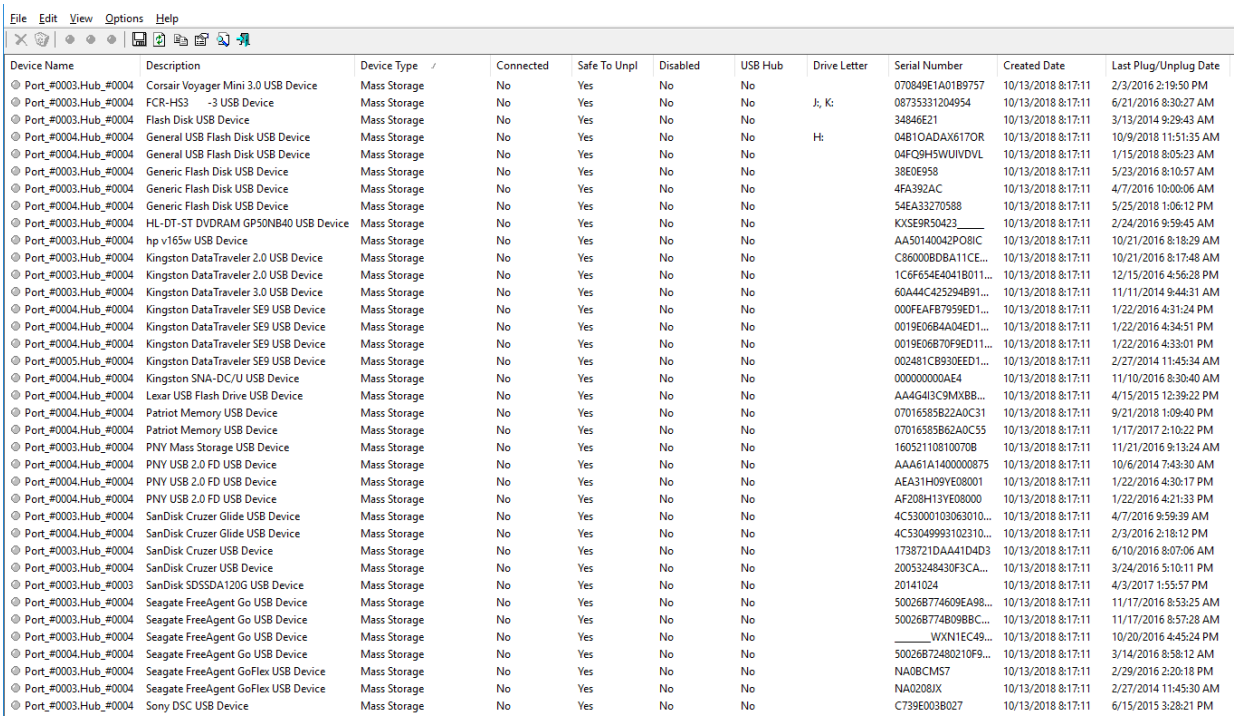
Options-Advanced Options



Change Load From to External SYSTEM Registry File and enter the path of the exported SYSTEM file



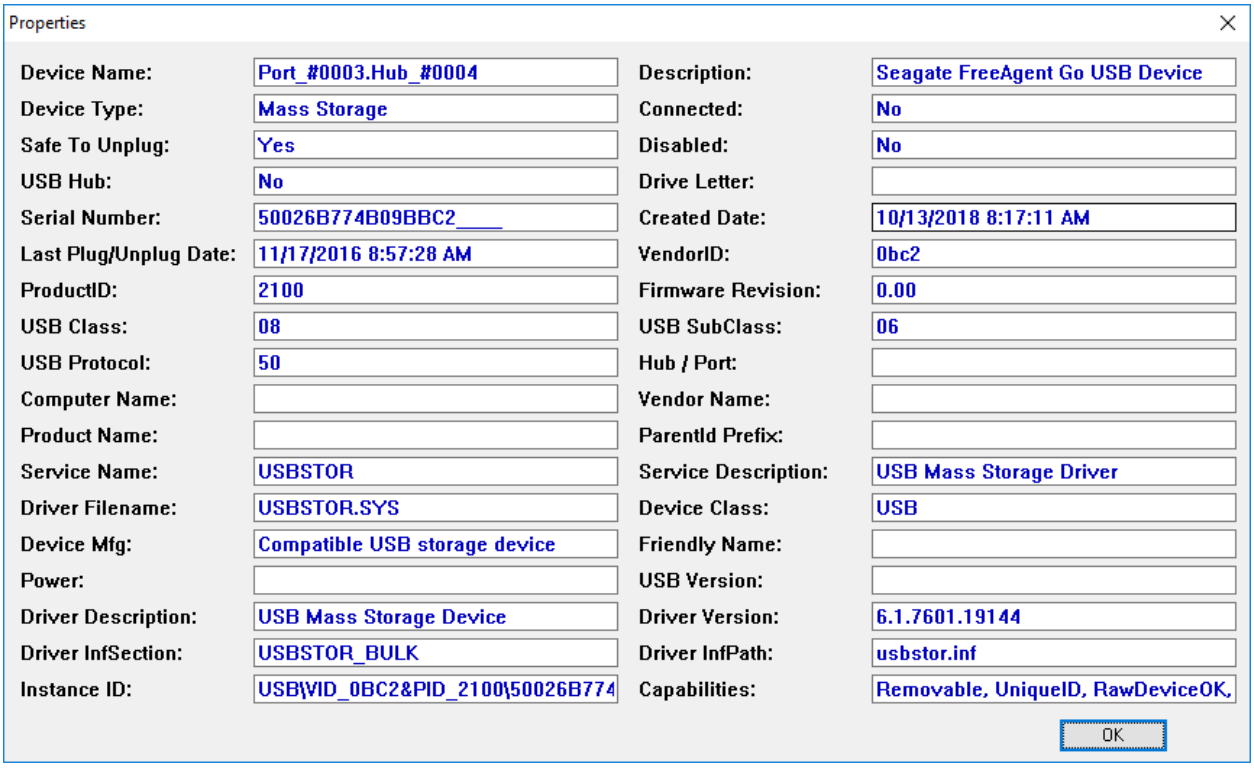
Sort by Device Type and look for Mass Storage entries



File Edit View Options Help

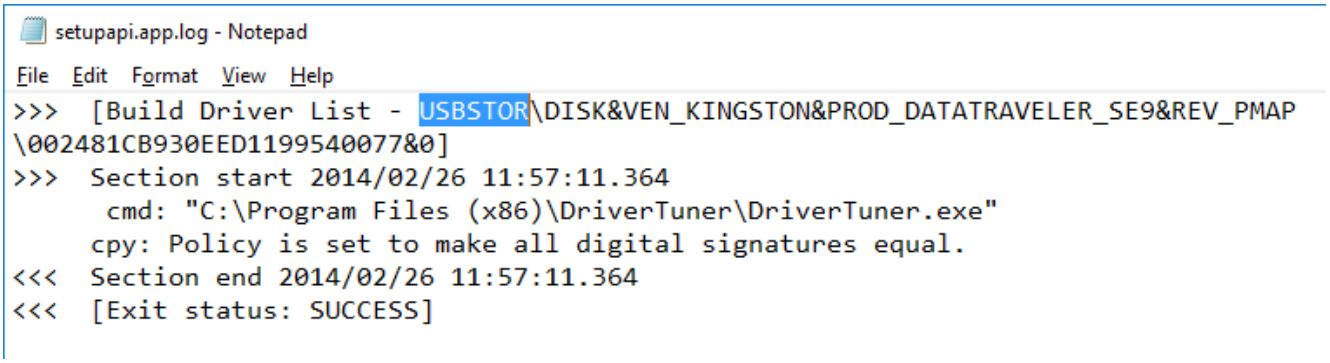
Device Name	Description	Device Type	Connected	Safe To Unpl	Disabled	USB Hub	Drive Letter	Serial Number	Created Date	Last Plug/Unplug Date
Port_#0003.Hub_#0004	Corsair Voyager Mini 3.0 USB Device	Mass Storage	No	Yes	No	No		070849E1A01B9757	10/13/2018 8:17:11	2/3/2016 2:19:50 PM
Port_#0003.Hub_#0004	FCR-HS3 -3 USB Device	Mass Storage	No	Yes	No	No	J:, K:	08735331204954	10/13/2018 8:17:11	6/21/2016 8:30:27 AM
Port_#0003.Hub_#0004	Flash Disk USB Device	Mass Storage	No	Yes	No	No		34846E21	10/13/2018 8:17:11	3/13/2014 9:29:43 AM
Port_#0004.Hub_#0004	General USB Flash Disk USB Device	Mass Storage	No	Yes	No	No	H:	04B1OADAX617OR	10/13/2018 8:17:11	10/9/2018 11:51:35 AM
Port_#0004.Hub_#0004	General USB Flash Disk USB Device	Mass Storage	No	Yes	No	No		04FQ9H5WUIVDVL	10/13/2018 8:17:11	1/15/2018 8:05:23 AM
Port_#0003.Hub_#0004	Generic Flash Disk USB Device	Mass Storage	No	Yes	No	No		38E0E958	10/13/2018 8:17:11	5/23/2016 8:10:57 AM
Port_#0003.Hub_#0004	Generic Flash Disk USB Device	Mass Storage	No	Yes	No	No		4FA392AC	10/13/2018 8:17:11	4/7/2016 10:00:06 AM
Port_#0004.Hub_#0004	Generic Flash Disk USB Device	Mass Storage	No	Yes	No	No		54EA33270588	10/13/2018 8:17:11	5/25/2018 1:06:12 PM
Port_#0003.Hub_#0004	HL-DT-ST DVDRAM GP50NB40 USB Device	Mass Storage	No	Yes	No	No		KXSE9R50423_____	10/13/2018 8:17:11	2/24/2016 9:59:45 AM
Port_#0003.Hub_#0004	hp v165w USB Device	Mass Storage	No	Yes	No	No		AA50140042PO8IC	10/13/2018 8:17:11	10/21/2016 8:18:29 AM
Port_#0003.Hub_#0004	Kingston DataTraveler 2.0 USB Device	Mass Storage	No	Yes	No	No		C86000BDBA11CE...	10/13/2018 8:17:11	10/21/2016 8:17:48 AM
Port_#0003.Hub_#0004	Kingston DataTraveler 2.0 USB Device	Mass Storage	No	Yes	No	No		1C6F654E4041B011...	10/13/2018 8:17:11	12/15/2016 4:56:28 PM
Port_#0003.Hub_#0004	Kingston DataTraveler 3.0 USB Device	Mass Storage	No	Yes	No	No		60A44C425294B91...	10/13/2018 8:17:11	11/11/2014 9:44:31 AM
Port_#0004.Hub_#0004	Kingston DataTraveler SE9 USB Device	Mass Storage	No	Yes	No	No		000FEAFB7959ED1...	10/13/2018 8:17:11	1/22/2016 4:31:24 PM
Port_#0004.Hub_#0004	Kingston DataTraveler SE9 USB Device	Mass Storage	No	Yes	No	No		0019E06B4A04ED1...	10/13/2018 8:17:11	1/22/2016 4:34:51 PM
Port_#0004.Hub_#0004	Kingston DataTraveler SE9 USB Device	Mass Storage	No	Yes	No	No		0019E06B70F9ED11...	10/13/2018 8:17:11	1/22/2016 4:33:01 PM
Port_#0005.Hub_#0004	Kingston DataTraveler SE9 USB Device	Mass Storage	No	Yes	No	No		002481CB930EED1...	10/13/2018 8:17:11	2/27/2014 11:45:34 AM
Port_#0004.Hub_#0004	Kingston SNA-DC/U USB Device	Mass Storage	No	Yes	No	No		000000000AE4	10/13/2018 8:17:11	11/10/2016 8:30:40 AM
Port_#0004.Hub_#0004	Lexar USB Flash Drive USB Device	Mass Storage	No	Yes	No	No		AA4G4I3C9MXBB...	10/13/2018 8:17:11	4/15/2015 12:39:22 PM
Port_#0004.Hub_#0004	Patriot Memory USB Device	Mass Storage	No	Yes	No	No		07016585B22A0C31	10/13/2018 8:17:11	9/21/2018 1:09:40 PM
Port_#0004.Hub_#0004	Patriot Memory USB Device	Mass Storage	No	Yes	No	No		07016585B62A0C55	10/13/2018 8:17:11	1/17/2017 2:10:22 PM
Port_#0003.Hub_#0004	PNY Mass Storage USB Device	Mass Storage	No	Yes	No	No		16052110810070B	10/13/2018 8:17:11	11/21/2016 9:13:24 AM
Port_#0004.Hub_#0004	PNY USB 2.0 FD USB Device	Mass Storage	No	Yes	No	No		AAA61A1400000875	10/13/2018 8:17:11	10/6/2014 7:43:30 AM
Port_#0004.Hub_#0004	PNY USB 2.0 FD USB Device	Mass Storage	No	Yes	No	No		AEA31H09YE08001	10/13/2018 8:17:11	1/22/2016 4:30:17 PM
Port_#0004.Hub_#0004	PNY USB 2.0 FD USB Device	Mass Storage	No	Yes	No	No		AF208H13YE08000	10/13/2018 8:17:11	1/22/2016 4:21:33 PM
Port_#0003.Hub_#0004	SanDisk Cruzer Glide USB Device	Mass Storage	No	Yes	No	No		4C53000103063010...	10/13/2018 8:17:11	4/7/2016 9:59:39 AM
Port_#0004.Hub_#0004	SanDisk Cruzer Glide USB Device	Mass Storage	No	Yes	No	No		4C53049993102310...	10/13/2018 8:17:11	2/3/2016 2:18:12 PM
Port_#0003.Hub_#0004	SanDisk Cruzer USB Device	Mass Storage	No	Yes	No	No		1738721DAA41D4D3	10/13/2018 8:17:11	6/10/2016 8:07:06 AM
Port_#0003.Hub_#0004	SanDisk Cruzer USB Device	Mass Storage	No	Yes	No	No		20053248430F3CA...	10/13/2018 8:17:11	3/24/2016 5:10:11 PM
Port_#0003.Hub_#0003	SanDisk SDSSDA120G USB Device	Mass Storage	No	Yes	No	No		20141024	10/13/2018 8:17:11	4/3/2017 1:55:57 PM
Port_#0003.Hub_#0004	Seagate FreeAgent Go USB Device	Mass Storage	No	Yes	No	No		50026B774609EA98...	10/13/2018 8:17:11	11/17/2016 8:53:25 AM
Port_#0003.Hub_#0004	Seagate FreeAgent Go USB Device	Mass Storage	No	Yes	No	No		50026B774B09BBC...	10/13/2018 8:17:11	11/17/2016 8:57:28 AM
Port_#0003.Hub_#0004	Seagate FreeAgent Go USB Device	Mass Storage	No	Yes	No	No		_____WXN1EC49...	10/13/2018 8:17:11	10/20/2016 4:45:24 PM
Port_#0004.Hub_#0004	Seagate FreeAgent Go USB Device	Mass Storage	No	Yes	No	No		50026B72480210F9...	10/13/2018 8:17:11	3/14/2016 8:58:12 AM
Port_#0003.Hub_#0004	Seagate FreeAgent GoFlex USB Device	Mass Storage	No	Yes	No	No		NA0BCMS7	10/13/2018 8:17:11	2/29/2016 2:20:18 PM
Port_#0003.Hub_#0004	Seagate FreeAgent GoFlex USB Device	Mass Storage	No	Yes	No	No		NA0208JX	10/13/2018 8:17:11	2/27/2014 11:45:30 AM
Port_#0003.Hub_#0004	Sony DSC USB Device	Mass Storage	No	Yes	No	No		C739E003B027	10/13/2018 8:17:11	6/15/2015 3:28:21 PM

Detailed view for each entry



All or select entries can be exported out to HTML or pasted into Excel.

Export all USBSTOR entries from the setupapi.app.log files



Use the setupapi.app.log files to identify when USB storage devices were first attached to the PC.

Putting it all together

Was the collection done in a certifiable manner?

Can the collected data be verified by a second party?

Can the results of your analysis be duplicated from the original data set?

Can the analysis results be achieved/explained without using automated tools?

Did the analysis accurately identify all PC activity from available snapshots?

How does the analysis of the data affect my case?

Each case will require a unique strategy to analyze. Understanding which strategy to take is key in every computer forensic case.