Forgotten But Not Gone: Gathering NTFS Artifacts of Deletion

MARI DEGRAZIA AND SCOTT HANSON

About Us

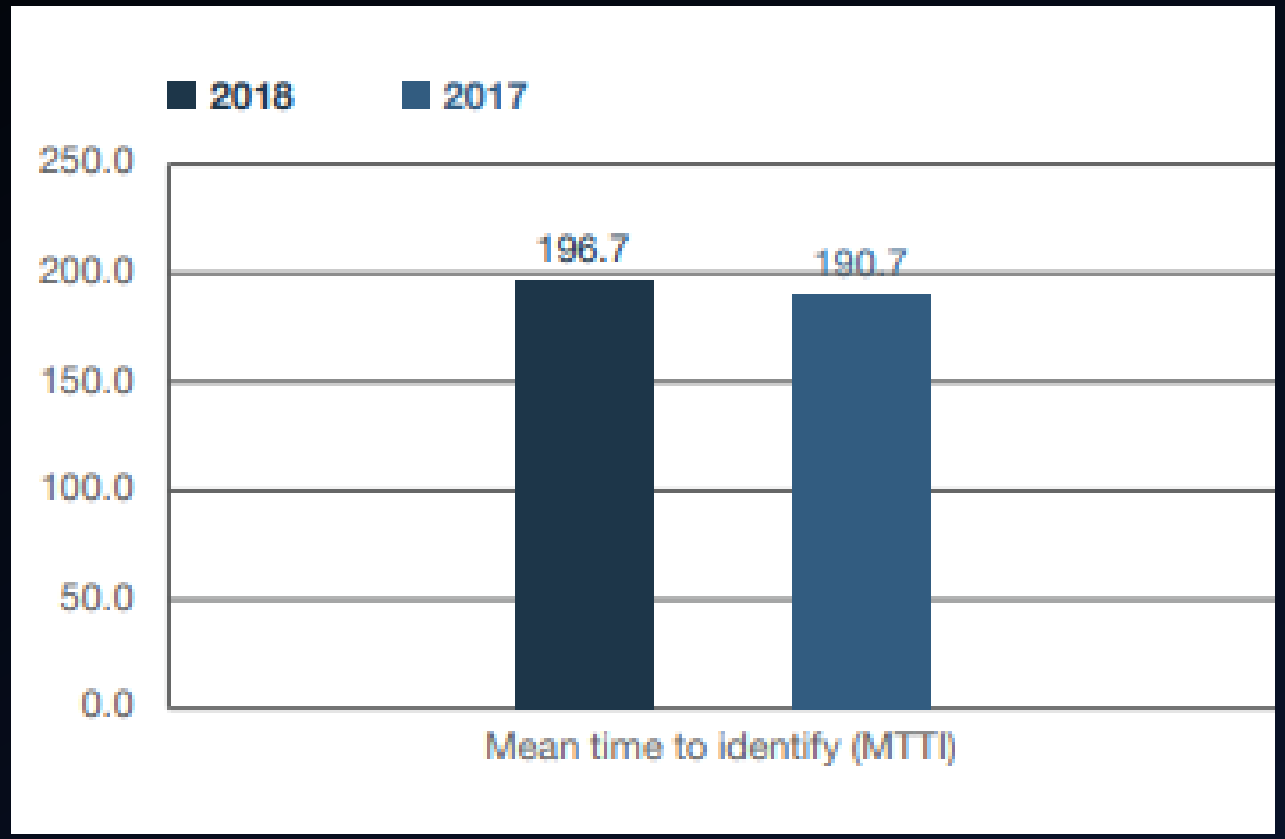
Mari

- Senior Director, Kroll Cyber Risk
- az4n6.blogspot.com
- github.com/mdegrazia
- @MariDeGrazia
- mari.degrazia@kroll.com

Scott

- Senior Director, Kroll Cyber Risk
- www.linkedin.com/in/shanson
- scott.hanson@kroll.com

PWNED



Source: 2018 Cost of a Data Breach Study, IBM

Case Study

Injected Process

Scrapes Credit Card Data

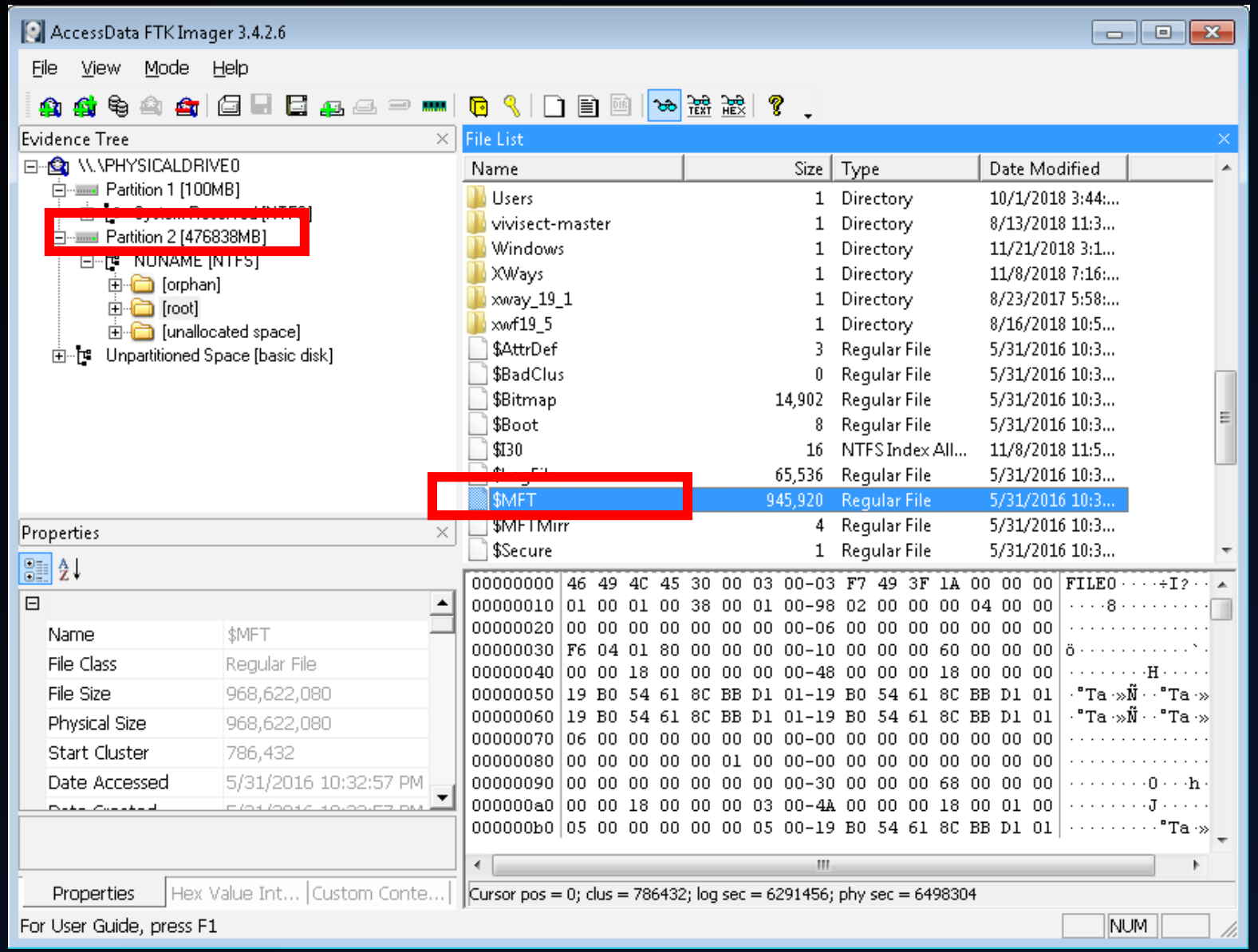
Encrypted Output File: C:\Windows\temp\wmsetup.tmp

Attacker Deletes

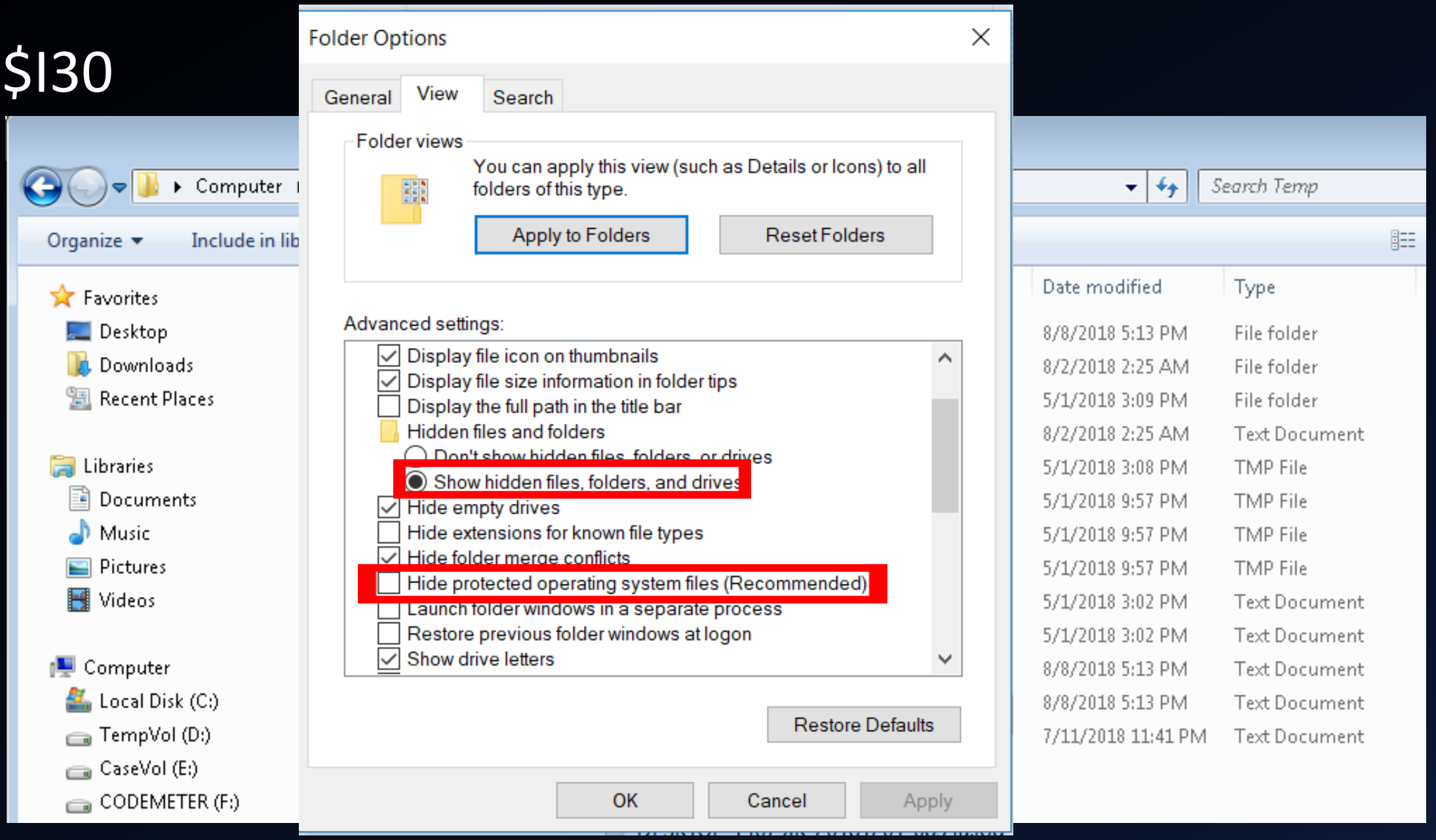
File Recreated (maybe)

Numerous Locations

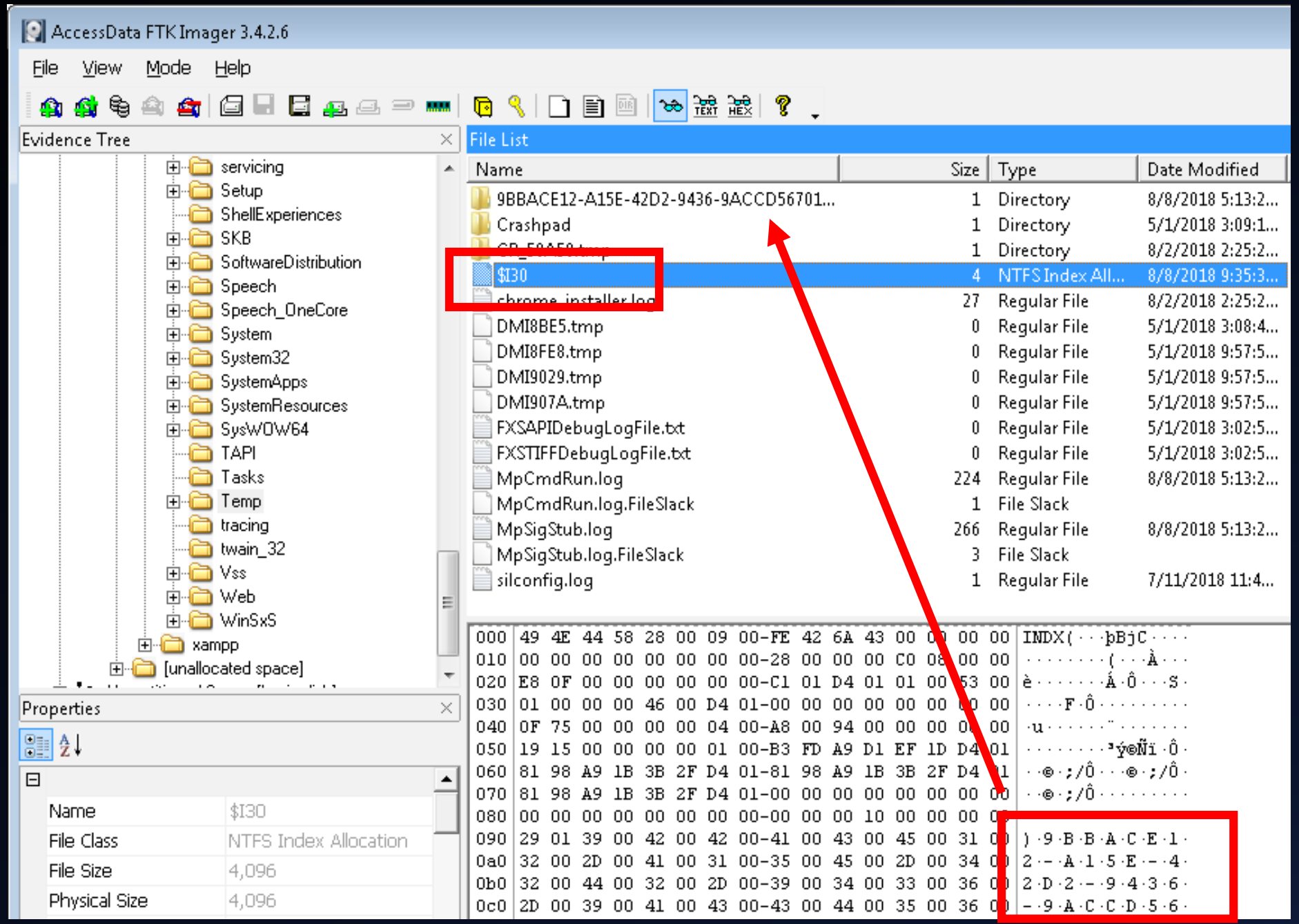
Master File Table



$130

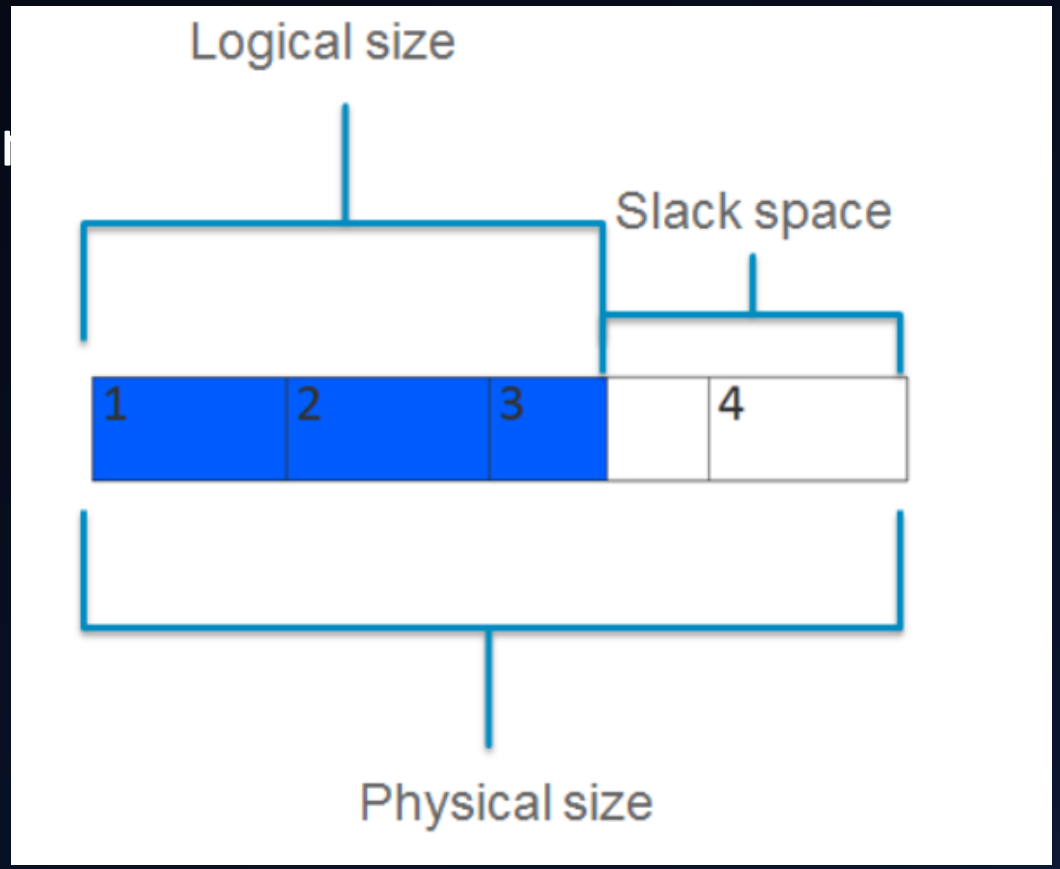

Folder Options
General
View
Search
Folder views
You can apply this view (such as Details or Icons) to all folders of this type.
Apply to Folders
Reset Folders
Advanced settings:
Display file icon on thumbnails
Display file size information in folder tips
Display the full path in the title bar
Hidden files and folders
Don't show hidden files, folders, or drives
Show hidden files, folders, and drives
Hide empty drives
Hide extensions for known file types
Hide folder merge conflicts
Hide protected operating system files (Recommended)
Launch folder windows in a separate process
Restore previous folder windows at logon
Show drive letters
Restore Defaults
OK
Cancel
Apply
Computer
Organize
Include in lib
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
TempVol (D:)
CaseVol (E:)
CODEMETER (F:)
Search Temp
Date modified
Type
8/8/2018 5:13 PM
File folder
8/2/2018 2:25 AM
File folder
5/1/2018 3:09 PM
File folder
8/2/2018 2:25 AM
Text Document
5/1/2018 3:08 PM
TMP File
5/1/2018 9:57 PM
TMP File
5/1/2018 9:57 PM
TMP File
5/1/2018 9:57 PM
TMP File
5/1/2018 3:02 PM
Text Document
5/1/2018 3:02 PM
Text Document
8/8/2018 5:13 PM
Text Document
8/8/2018 5:13 PM
Text Document
7/11/2018 11:41 PM
Text Document

$I30


AccessData FTK Imager 3.4.2.6
File View Mode Help
Evidence Tree
servicing
Setup
ShellExperiences
SKB
SoftwareDistribution
Speech
Speech_OneCore
System
System32
SystemApps
SystemResources
SysWOW64
TAPI
Tasks
Temp
tracing
twain_32
Vss
Web
WinSxS
xampp
[unallocated space]
Properties
Name $I30
File Class NTFS Index Allocation
File Size 4,096
Physical Size 4,096
File List
Name Size Type Date Modified
9BBACE12-A15E-42D2-9436-9ACCD56701... 1 Directory 8/8/2018 5:13:2...
Crashpad 1 Directory 5/1/2018 3:09:1...
1 Directory 8/2/2018 2:25:2...
$I30 4 NTFS Index All... 8/8/2018 9:35:3...
27 Regular File 8/2/2018 2:25:2...
DMI8BE5.tmp 0 Regular File 5/1/2018 3:08:4...
DMI8FE8.tmp 0 Regular File 5/1/2018 9:57:5...
DMI9029.tmp 0 Regular File 5/1/2018 9:57:5...
DMI907A.tmp 0 Regular File 5/1/2018 9:57:5...
FXSAPIDebugLogFile.txt 0 Regular File 5/1/2018 3:02:5...
FXSTIFFDebugLogFile.txt 0 Regular File 5/1/2018 3:02:5...
MpCmdRun.log 224 Regular File 8/8/2018 5:13:2...
MpCmdRun.log.FileSlack 1 File Slack
MpSigStub.log 266 Regular File 8/8/2018 5:13:2...
MpSigStub.log.FileSlack 3 File Slack
silconfig.log 1 Regular File 7/11/2018 11:4...
000 49 4E 44 58 28 00 09 00-FE 42 6A 43 00 00 00 00 INDX(···þBjC····
010 00 00 00 00 00 00 00 00-28 00 00 00 C0 08 00 00 ········(···À···
020 E8 0F 00 00 00 00 00 00-C1 01 D4 01 01 00 53 00 è·····Á·Ô···S·
030 01 00 00 00 46 00 D4 01-00 00 00 00 00 00 00 00 ····F·Ô·····
040 0F 75 00 00 00 00 04 00-A8 00 94 00 00 00 00 00 ·u·····¨·····
050 19 15 00 00 00 00 01 00-B3 FD A9 D1 EF 1D D4 01 ·····³ý©Ñï·Ô·
060 81 98 A9 1B 3B 2F D4 01-81 98 A9 1B 3B 2F D4 01 ··©·;/Ô···©·;/Ô·
070 81 98 A9 1B 3B 2F D4 01-00 00 00 00 00 00 00 00 ··©·;/Ô·····
080 00 00 00 00 00 00 00 00-00 00 00 10 00 00 00 00
090 29 01 39 00 42 00 42 00-41 00 43 00 45 00 31 00)·9·B·B·A·C·E·1·
0a0 32 00 2D 00 41 00 31 00-35 00 45 00 2D 00 34 00 2·-·A·1·5·E·-·4·
0b0 32 00 44 00 32 00 2D 00-39 00 34 00 33 00 36 00 2·D·2·-·9·4·3·6·
0c0 2D 00 39 00 41 00 43 00-43 00 44 00 35 00 36 00 -·9·A·C·C·D·5·6·

NTFS Index Attributes AKA $I30

- Tracks the contents of the directory for efficiency
- Can contain slack space
- Can contain deleted file information
- $FILE_NAME attributes
  - Full filename
  - Parent directory
  - File Size
  - Timestamps
  - MFT Record number



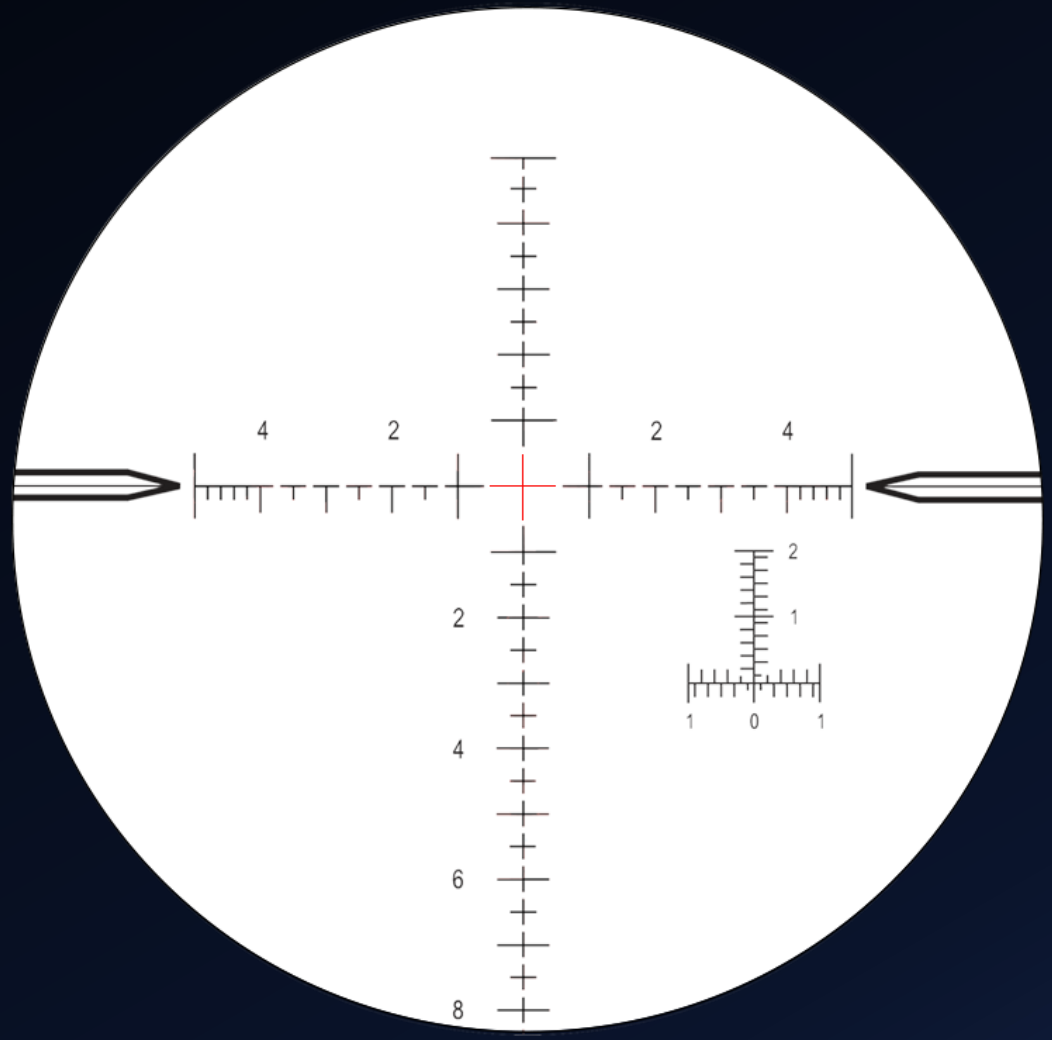
https://digital-forensics.sans.org/blog/2011/09/20/ntfs-i30-index-attributes-evidence-of-deleted-and-overwritten-files

Case Study

- Gap with current tools
- Need to identify locations with output files
- Numerous locations and systems
- Need to get the $I30 file
- Don’t want to grab images
- Leverage hunting tools

$I30 Targeted Approach

- Pull specific data with EDR
- Reduce images collected
- Low footprint
- Reduce “wait” time
- Scales easily
- Defeat anti-forensics



EDR Methodology

$MFT

- RawCopy , ntfscopy or TZ Works Dup tool
  - ntfscopy64.exe C:\$MFT D:\System1\$MFT
- Parse $MFT with MFTECmd
  - MFTECmd.exe –f C:\Documents\$MFT –csv C:\Output\mft
- Find $MFT sequence number

A	F	G	L	T	V
EntryNumber	ParentPath	FileName	IsDirectory	Created0x10	LastModified0x10
5396	.\Windows\SysWOW64	zh-CN	TRUE	2016-07-16 13:23:22	2016-07-16 13:23:32
5397	.\Windows\SysWOW64	zh-HK	TRUE	2016-07-16 13:23:22	2016-07-16 13:23:32
5398	.\Windows\SysWOW64	zh-TW	TRUE	2016-07-16 13:23:22	2016-07-16 13:23:32
5399	.\Windows	TAPI	TRUE	2016-07-16 13:23:22	2016-07-16 13:23:22
5400	.\Windows	Tasks	TRUE	2016-07-16 13:23:22	2018-02-02 19:39:18
5401	.\Windows	Temp	TRUE	2016-07-16 13:23:22	2018-08-08 21:35:31
5402	.\Windows	tracing	TRUE	2016-07-16 13:23:22	2016-07-16 13:23:22
5403	.\Windows	twain_32	TRUE	2016-07-16 13:23:22	2016-07-16 13:23:32
5404	.\Windows	Vss	TRUE	2016-07-16 13:23:22	2016-07-16 13:23:22
5405	.\Windows\Vss	Writers	TRUE	2016-07-16 13:23:22	2016-07-16 13:23:22
5406	.\Windows\Vss\Writers	Application	TRUE	2016-07-16 13:23:22	2016-07-16 13:23:22
5407	.\Windows\Vss\Writers	System	TRUE	2016-07-16 13:23:22	2016-07-16 13:23:32

Copy out $I30

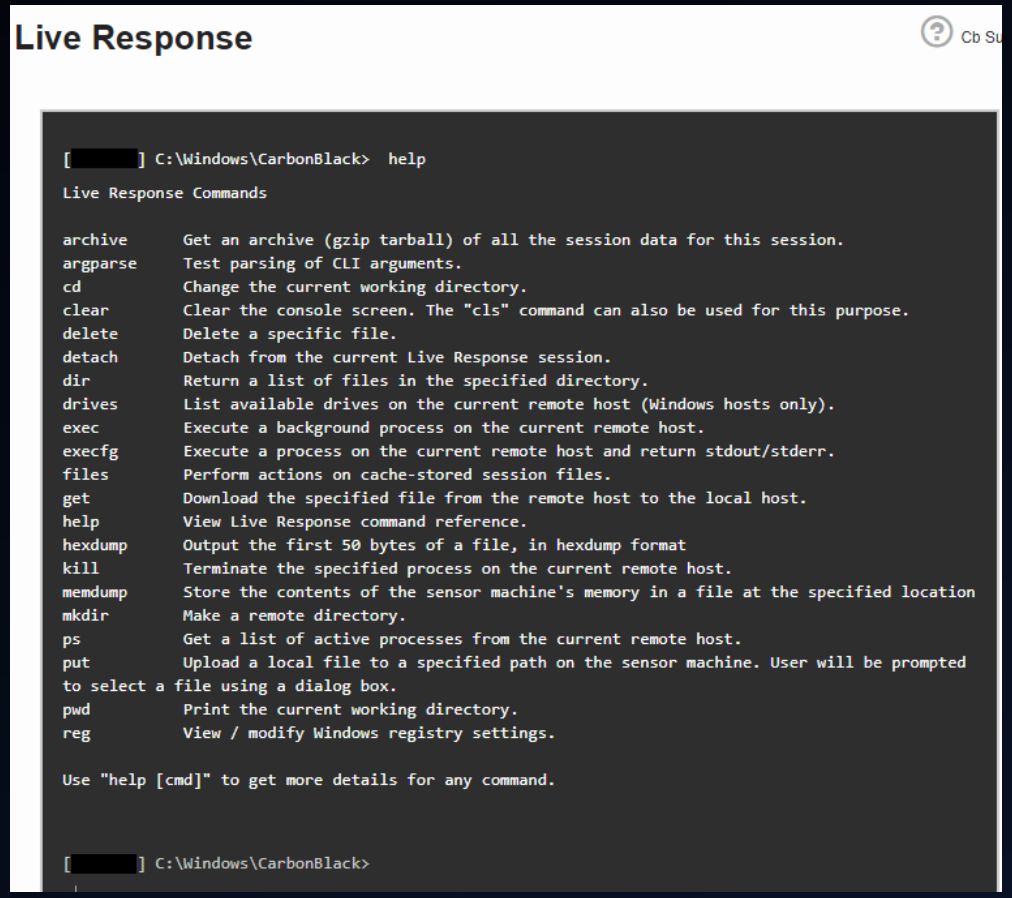
- RawCopy64.exe /FilenamePath:C:359308 /OutputPath:C:\Users\<user>\preso\output /OutputName:System1 /AllAttr:1

```
C:\tools\RawCopy>RawCopy64.exe /FileNamePath:C:359308 /OutputPath:C:\Users\
rnj\Documents\preso\output  /OutputName:System1 /AllAttr:1
RawCopy v1.0.0.21

Writing: System1_359308_$STANDARD_INFORMATION.bin
Writing: System1_359308_$FILE_NAME.bin
Writing: System1_359308_$OBJECT_ID.bin
Writing: System1_359308_$INDEX_ROOT_$I30.bin
Writing: System1_359308_$INDEX_ALLOCATION_$I30.bin
Writing: System1_359308_$BITMAP_$I30.bin

Job took 3.43 seconds

C:\tools\RawCopy>_
```

https://github.com/jschicht/RawCopy

Carbon Black Live Response

Interactive

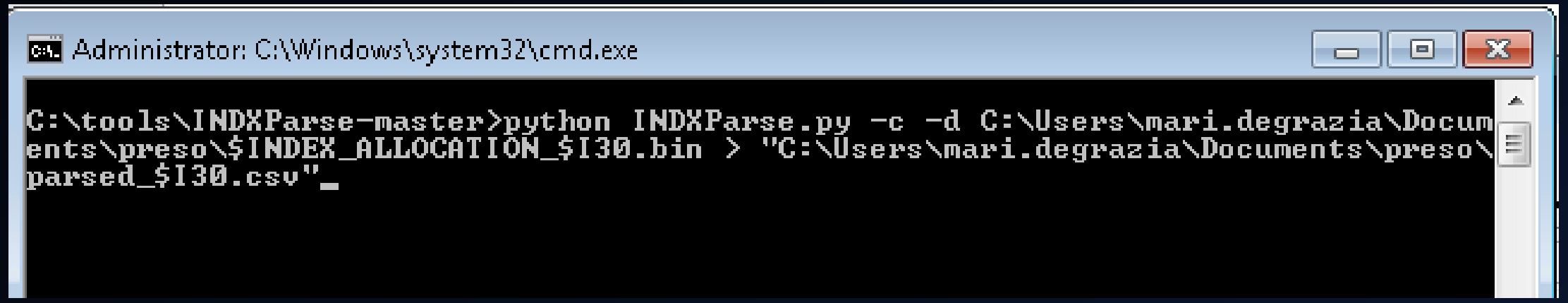


API-driven

```
class RetrieveI30(object):

path = "I30"

command = r'cmd /c "rawcopy
/filenamepath:c:72
/outputpath:c:\windows\carbonblack
/outputname:mft /allattr:1"’

binary = r'rawcopy.exe'
ext = "bin"
```

Parse $I30

- INDXParse.py –c –d $INDEX_ALLOCATION_$I30.bin > parsed_$I30.csv
  - -c = csv
  - -d = slack space



https://github.com/williballenthin/INDXParse

Not in $MFT, Not in Logfile, $I30 slack space only

A	B	C	D	E	F	G
FILENAME	**PHYSICAL SIZE**	**LOGICAL SIZE**	**MODIFIED TIME**	**ACCESSED TIME**	**CHANGED TIME**	**CREATED TIME**
SOPHOS~1.TXT	4096	554	2014-01-01 11:13:24.701468	2014-01-01 11:13:24.701468	2014-01-01 11:13:24.701468	2014-01-01 11:13:23.842093
SOPHOS~2.LOG	172032	170122	2014-01-01 11:14:19.826468	2014-01-01 11:14:19.826468	2014-01-01 11:14:19.826468	2014-01-01 11:14:17.404591
SOPHOS~2.TXT	585728	583460	2017-08-01 12:11:34.917309	2017-08-01 12:11:34.917309	2017-08-01 12:11:34.917309	2014-01-01 11:13:24.701468
SOPHOS~3.LOG	176128	175096	2015-02-25 01:30:23.137005	2015-02-25 01:30:23.137005	2015-02-25 01:30:23.137005	2015-02-25 01:30:12.793322
SOPHOS~3.TXT	4194304	4192312	2017-12-04 12:25:37.748161	2017-12-04 12:25:37.748161	2017-12-04 12:25:37.748161	2017-12-04 12:24:34.202101
SOPHOS~4.LOG	184320	181792	2015-04-14 17:17:59.179375	2015-04-14 17:17:59.179375	2015-04-14 17:17:59.179375	2015-04-14 17:17:31.195181
SOPHOS~4.TXT	6127616	6127526	2016-04-07 19:03:16.716339	2016-04-07 19:03:16.716339	2016-04-07 19:03:16.716339	2015-02-25 01:27:48.434870
wmsetup.tmp (slack at 0x68f0)	800	678	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901
wmsetup.tmp (slack at 0x6960)	800	678	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901
wmsetup.tmp (slack at 0x69d0)	800	678	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901
wmsetup.tmp (slack at 0x6a40)	800	678	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901
wmsetup.tmp (slack at 0x6aa8)	800	678	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901
wmsetup.tmp (slack at 0x6b18)	800	678	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901
wmsetup.tmp (slack at 0x6b80)	800	678	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901	2018-10-31 13:05:17.162901
Sophos Anti-Virus CustomActions Log_18	4096	1584	2018-05-16 13:45:38.047722	2018-05-16 13:45:38.047722	2018-05-16 13:45:38.047722	2018-05-16 13:45:34.422768

Automate for the Win

- EDR: Collect $MFT records
- grep outputs for MFT record number
- EDR: kick off script to collect $I30
- Use script to parse bin files
  - dir_index_parse.py C:\index_files
- grep for file(s) of interest

$I30 goodness

- Recover deleted entries
- Check staging folders
- Attackers “favorite” folders
- Fill out gaps in timeline
- Identify additional compromised systems

Gotchas

- Targeted
- Need existing IOCs
- EDR Deployment
- *Absence of evidence is **not** evidence of absence*

Resources

- MFTECmd: https://ericzimmerman.github.io/
- RawCopy: https://github.com/jschicht/RawCopy
- tzworks tools: https://tzworks.net/
- INDEXParse: https://github.com/williballenthin/INDXParse
- CB Live Response Triage: https://github.com/krollcyber/cblr_triage

Questions