CEIC® 2015

Improving Windows External Device Investigations

David Dym, G-C Partners

My Background

- Forensic investigator for G-C Partners
- 8 years in Forensics
- Contributor for Hacking Exposed Computer Forensics 2nd and 3rd editions and Computer Forensics InfoSec Pro Guide

Top Artifacts

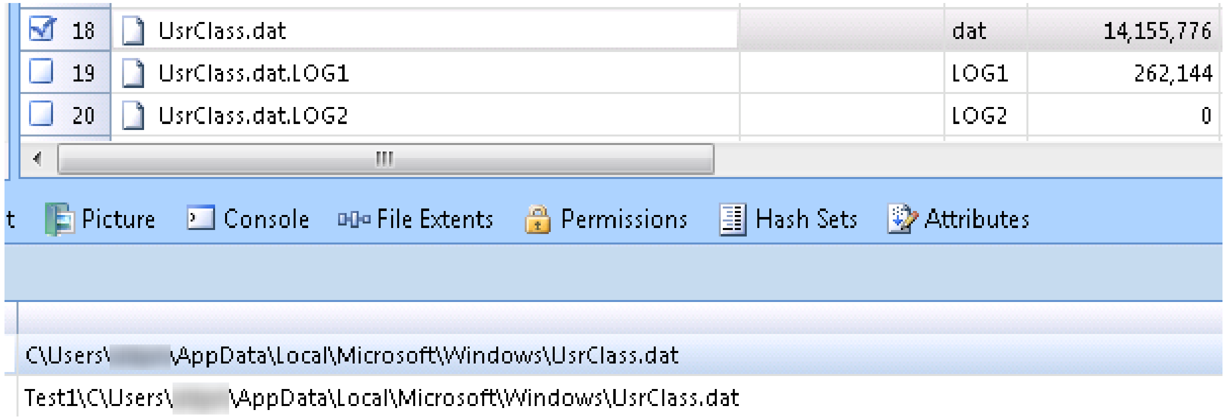
- Activity – ShellBags, LNK’s and Jumplists
- Device Plugins - USBStor, EMDMgmt, Device Classes and System Event Log, etc..
- Shadow Copies

Activity

You think I won’t know?

Activity: ShellBags

- What they are
- Why you should care
- Common mistakes

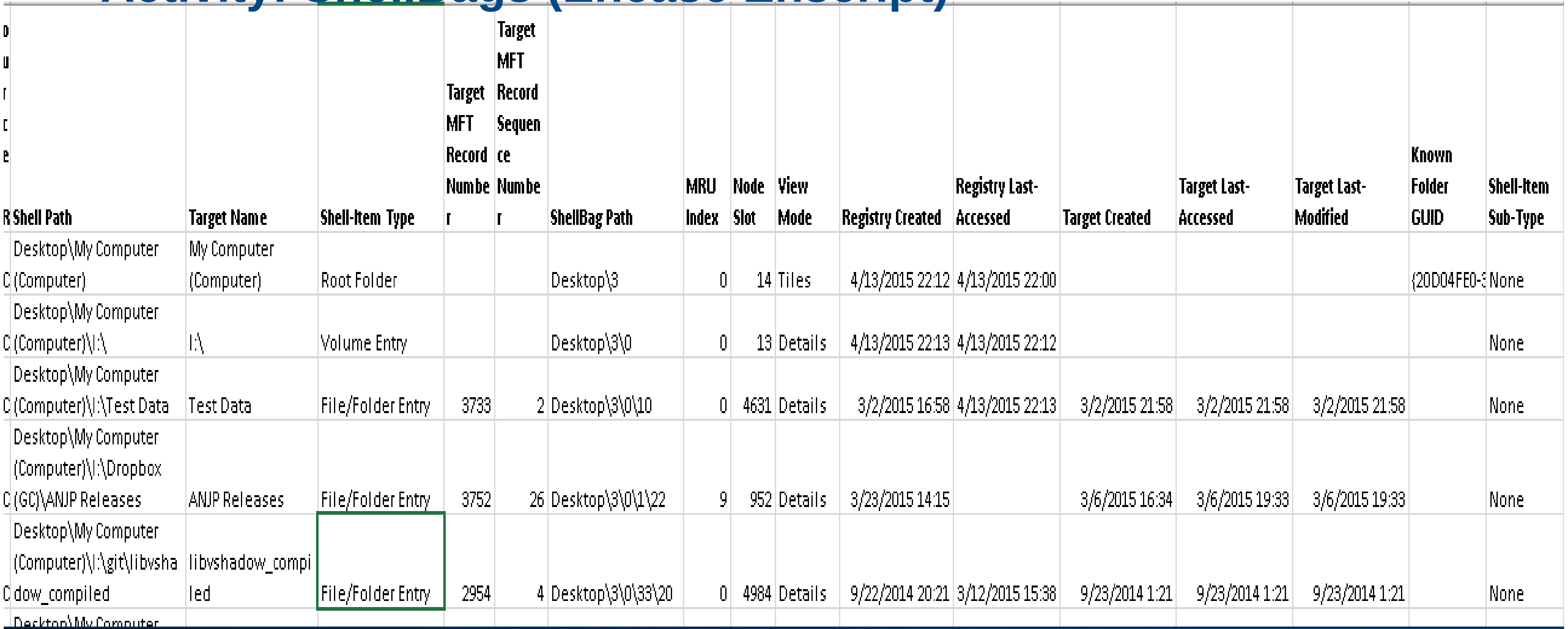


☑	18	UsrClass.dat		dat	14,155,776
□	19	UsrClass.dat.LOG1		LOG1	262,144
□	20	UsrClass.dat.LOG2		LOG2	0

C\Users\[redacted]\AppData\Local\Microsoft\Windows\UsrClass.dat

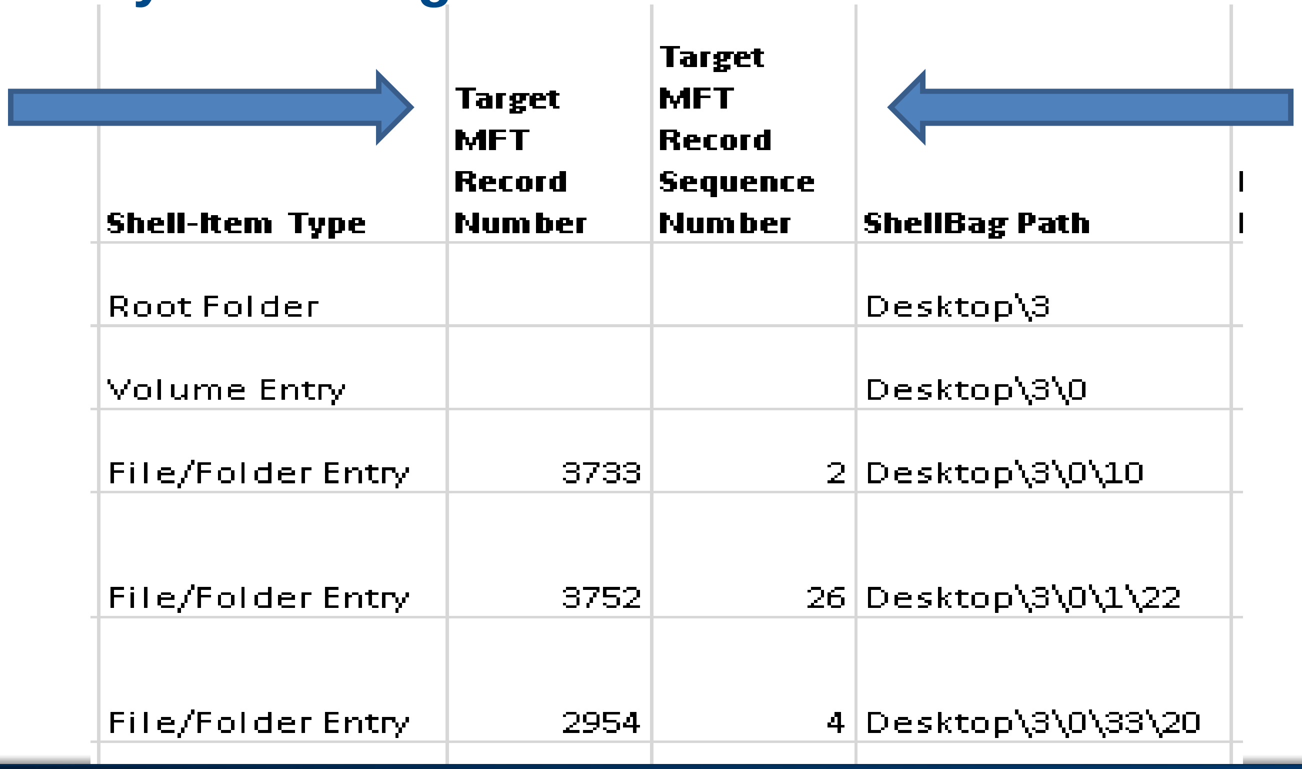
Test1\C\Users\[redacted]\AppData\Local\Microsoft\Windows\UsrClass.dat

Activity: ShellBags (Encase Enscript)



D u r c e R	Shell Path	Target Name	Shell-Item Type	Target MFT Record Number	Target MFT Record Sequence Number	ShellBag Path	MRU Index	Node Slot	View Mode	Registry Created	Registry Last-Accessed	Target Created	Target Last-Accessed	Target Last-Modified	Known Folder GUID	Shell-Item Sub-Type
C	Desktop\My Computer (Computer)	My Computer (Computer)	Root Folder			Desktop\3	0	14	Tiles	4/13/2015 22:12	4/13/2015 22:00				{20D04FE0-3	None
C	Desktop\My Computer (Computer)\I:\	I:\	Volume Entry			Desktop\3\0	0	13	Details	4/13/2015 22:13	4/13/2015 22:12					None
C	Desktop\My Computer (Computer)\I:\Test Data	Test Data	File/Folder Entry	3733	2	Desktop\3\0\10	0	4631	Details	3/2/2015 16:58	4/13/2015 22:13	3/2/2015 21:58	3/2/2015 21:58	3/2/2015 21:58		None
C	Desktop\My Computer (Computer)\I:\Dropbox (GC)\ANJP Releases	ANJP Releases	File/Folder Entry	3752	26	Desktop\3\0\1\22	9	952	Details	3/23/2015 14:15		3/6/2015 16:34	3/6/2015 19:33	3/6/2015 19:33		None
C	Desktop\My Computer (Computer)\I:\git\libvshadow_compiled	libvshadow_compiled	File/Folder Entry	2954	4	Desktop\3\0\33\20	0	4984	Details	9/22/2014 20:21	3/12/2015 15:38	9/23/2014 1:21	9/23/2014 1:21	9/23/2014 1:21		None
	Desktop\My Computer															

Activity: ShellBags



Shell-Item Type	Target MFT Record Number	Target MFT Record Sequence Number	ShellBag Path	I I
Root Folder			Desktop\3	
Volume Entry			Desktop\3\0	
File/Folder Entry	3733	2	Desktop\3\0\10	
File/Folder Entry	3752	26	Desktop\3\0\1\22	
File/Folder Entry	2954	4	Desktop\3\0\33\20	

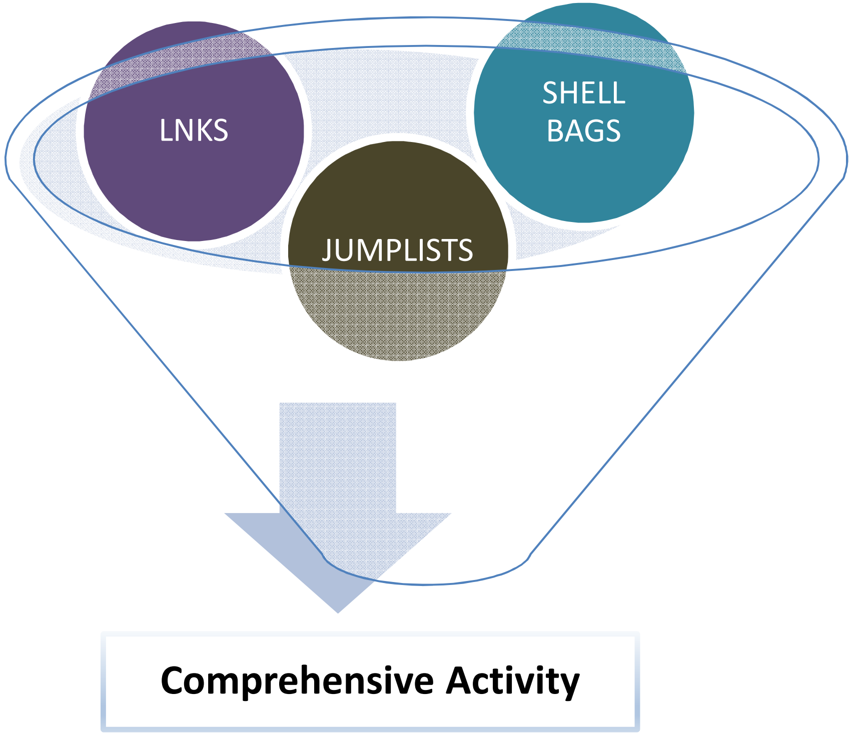
Activity: LNKs & Jumplists

- Always pull LNKs and Jumplists
- Don’t forget Jumplists!

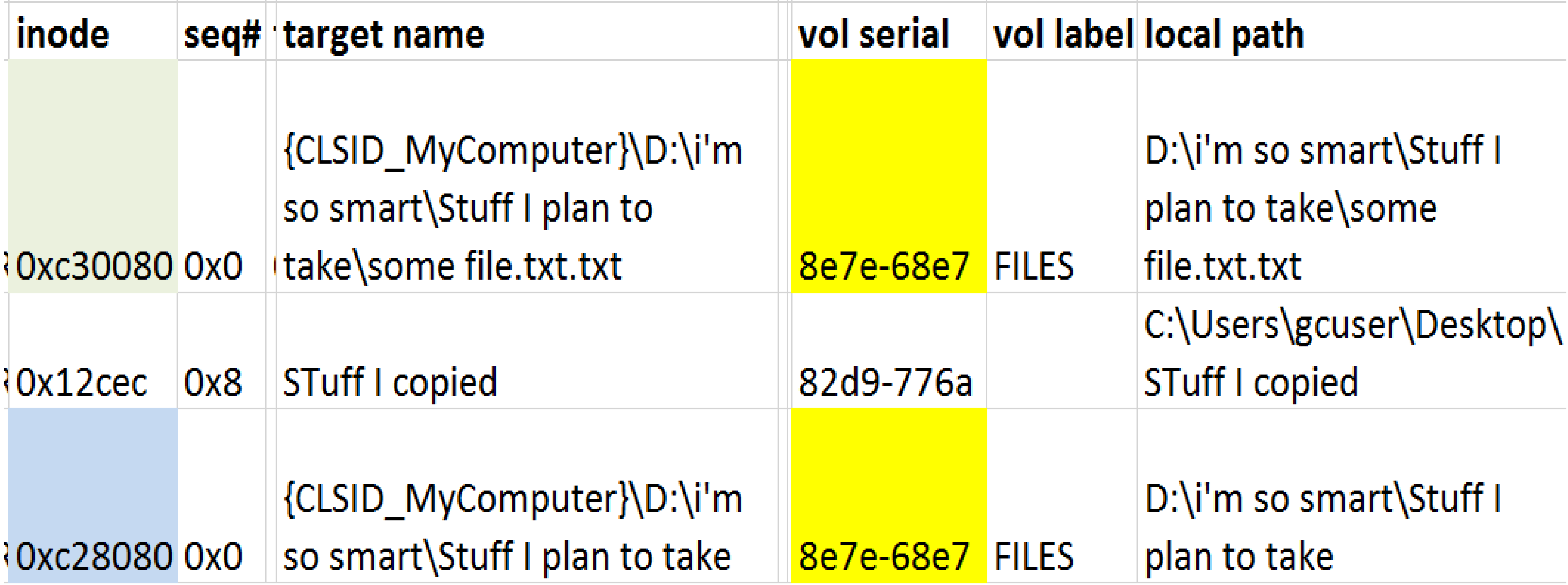
This sounds familiar…

Activity: Commonality

- Artifacts can be correlated

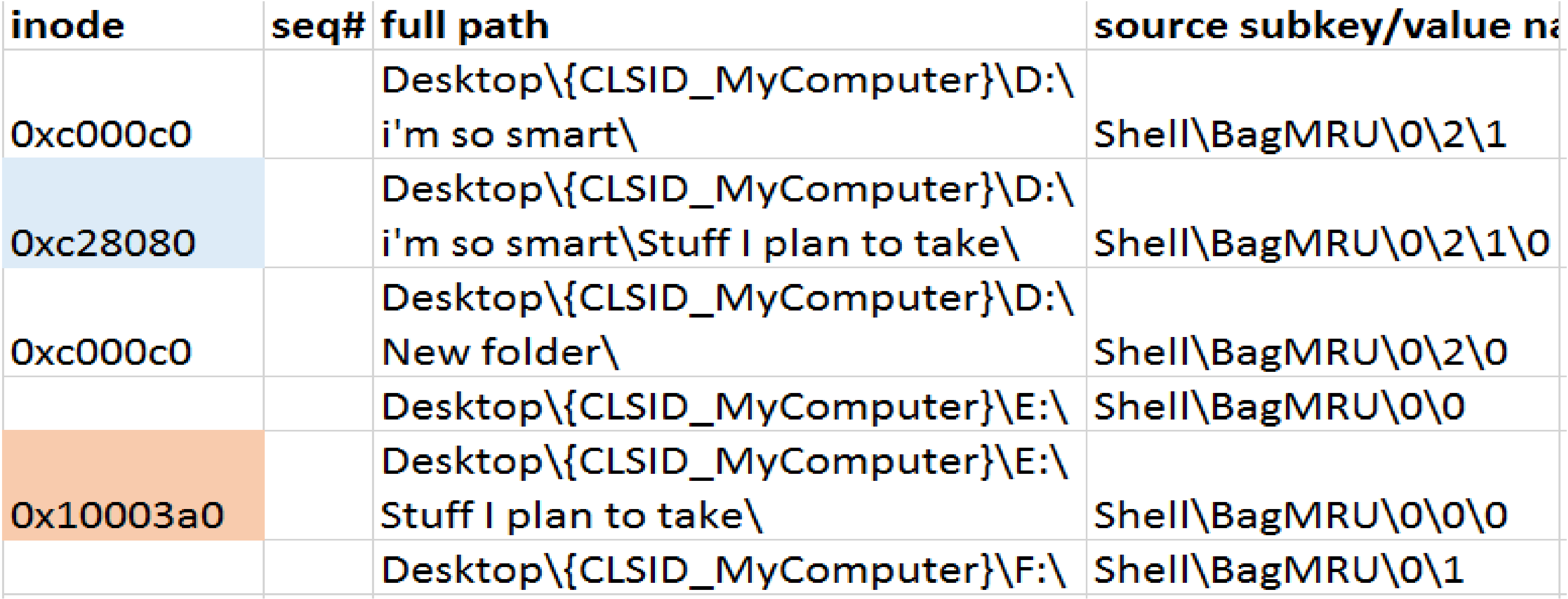


Activity: LNK Shortcuts



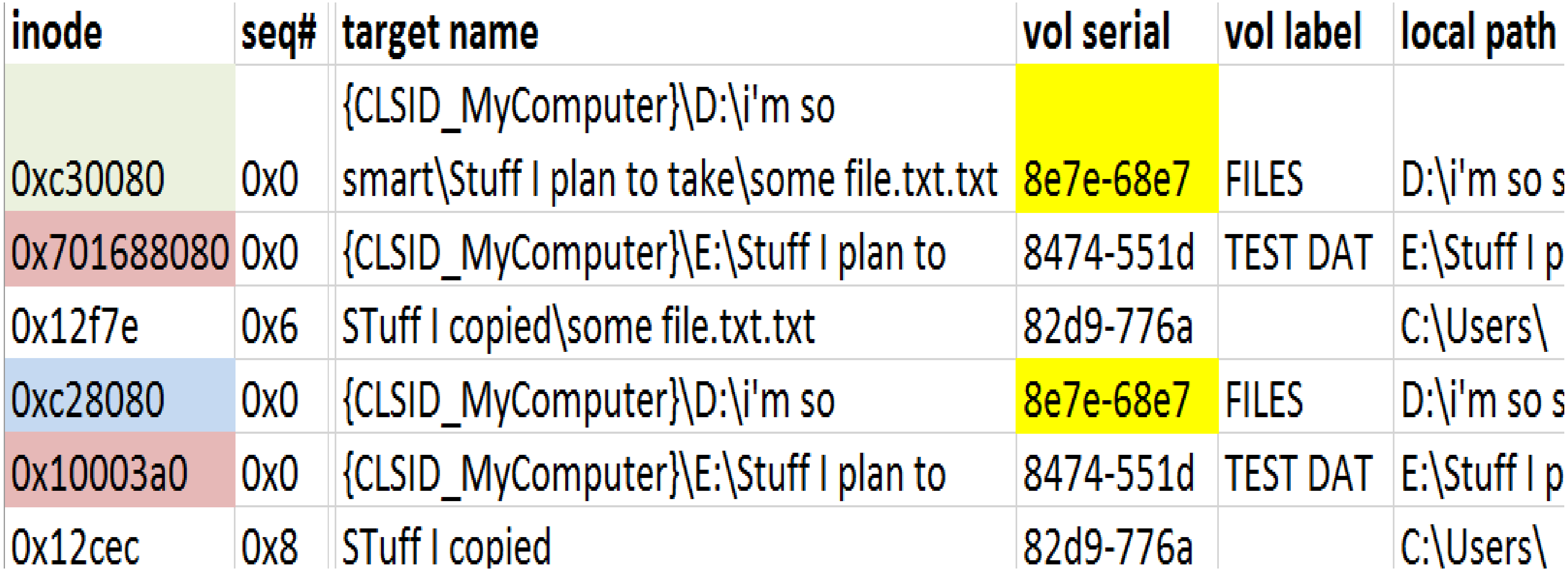
inode	seq#	target name	vol serial	vol label	local path
0xc30080	0x0	{CLSID_MyComputer}\D:\i'm so smart\Stuff I plan to take\some file.txt.txt	8e7e-68e7	FILES	D:\i'm so smart\Stuff I plan to take\some file.txt.txt
0x12cec	0x8	STuff I copied	82d9-776a		C:\Users\gcuser\Desktop\STuff I copied
0xc28080	0x0	{CLSID_MyComputer}\D:\i'm so smart\Stuff I plan to take	8e7e-68e7	FILES	D:\i'm so smart\Stuff I plan to take

Activity: Shellbags



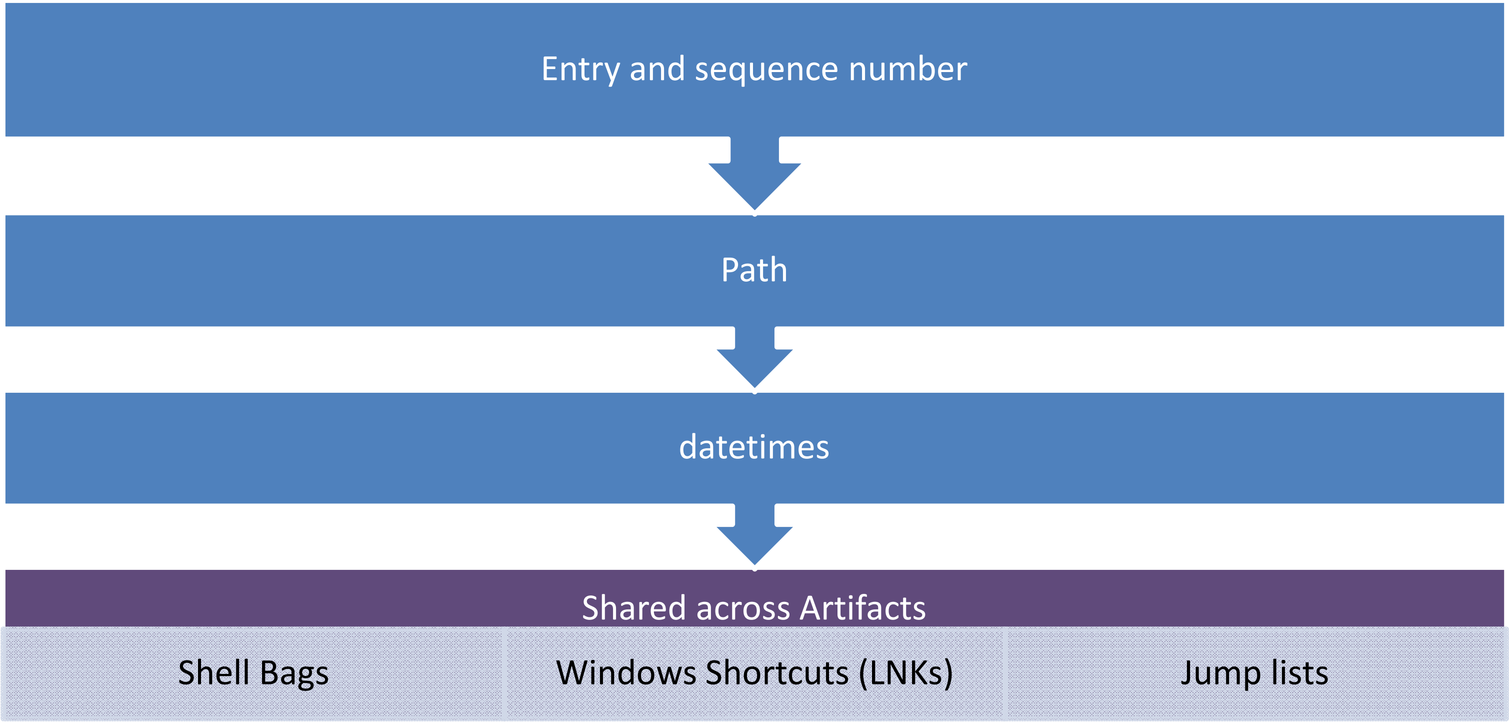
inode	seq#	full path	source subkey/value na
0xc000c0		Desktop\{CLSID_MyComputer}\D:\i'm so smart\	Shell\BagMRU\0\2\1
0xc28080		Desktop\{CLSID_MyComputer}\D:\i'm so smart\Stuff I plan to take\	Shell\BagMRU\0\2\1\0
0xc000c0		Desktop\{CLSID_MyComputer}\D:\New folder\	Shell\BagMRU\0\2\0
		Desktop\{CLSID_MyComputer}\E:\	Shell\BagMRU\0\0
0x10003a0		Desktop\{CLSID_MyComputer}\E:\Stuff I plan to take\	Shell\BagMRU\0\0\0
		Desktop\{CLSID_MyComputer}\F:\	Shell\BagMRU\0\1

Activity: Jumplist



inode	seq#	target name	vol serial	vol label	local path
0xc30080	0x0	{CLSID_MyComputer}\D:\i'm so smart\Stuff I plan to take\some file.txt.txt	8e7e-68e7	FILES	D:\i'm so s
0x701688080	0x0	{CLSID_MyComputer}\E:\Stuff I plan to	8474-551d	TEST DAT	E:\Stuff I p
0x12f7e	0x6	STuff I copied\some file.txt.txt	82d9-776a		C:\Users\
0xc28080	0x0	{CLSID_MyComputer}\D:\i'm so	8e7e-68e7	FILES	D:\i'm so s
0x10003a0	0x0	{CLSID_MyComputer}\E:\Stuff I plan to	8474-551d	TEST DAT	E:\Stuff I p
0x12cec	0x8	STuff I copied	82d9-776a		C:\Users\

Activity: Commonality



Entry and sequence number

Path

datetimes

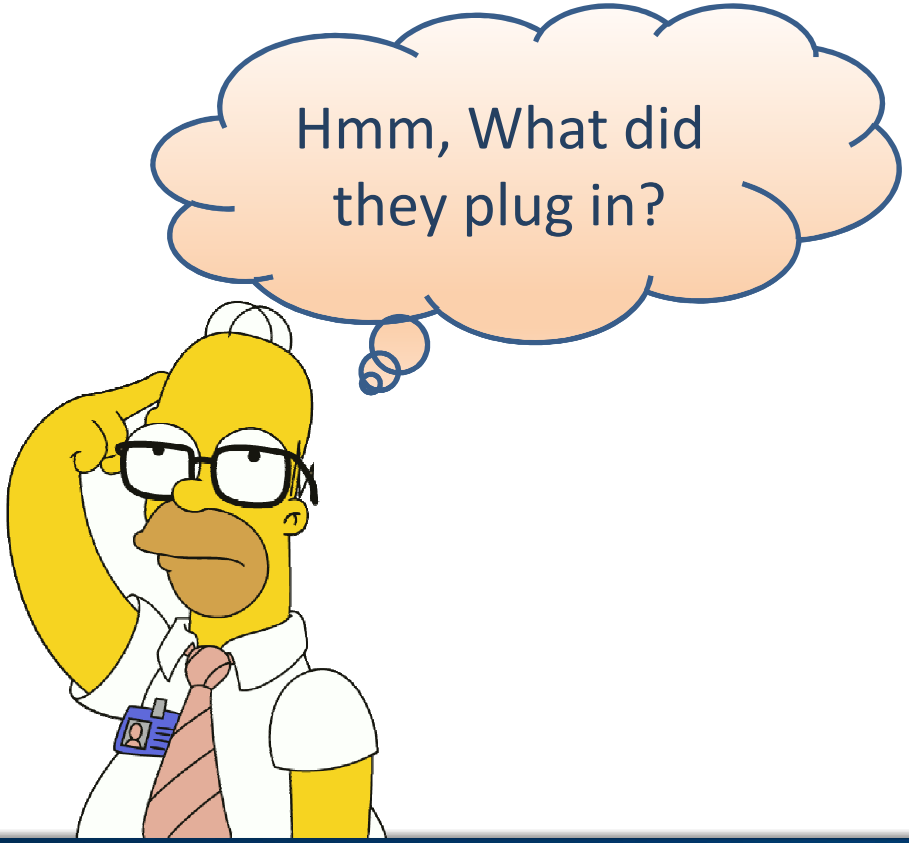
Shared across Artifacts

Shell Bags

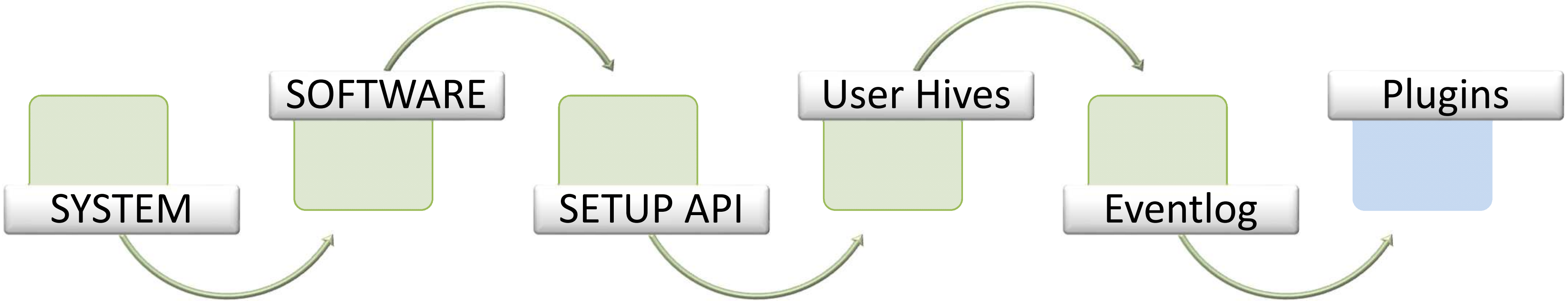
Windows Shortcuts (LNKs)

Jump lists

Plugins

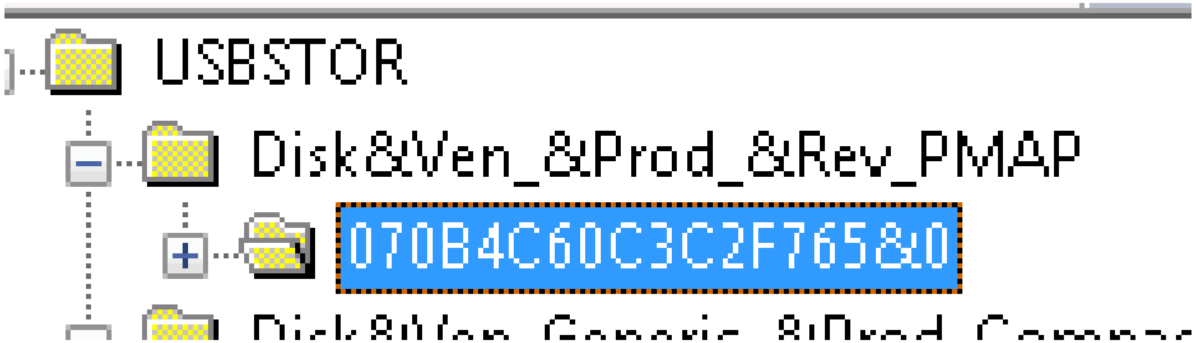


Plugins: Getting a full view



Plugins: USBStor

- Serial Number
- Hardware Info
- Friendly Name
- Device Class GUID

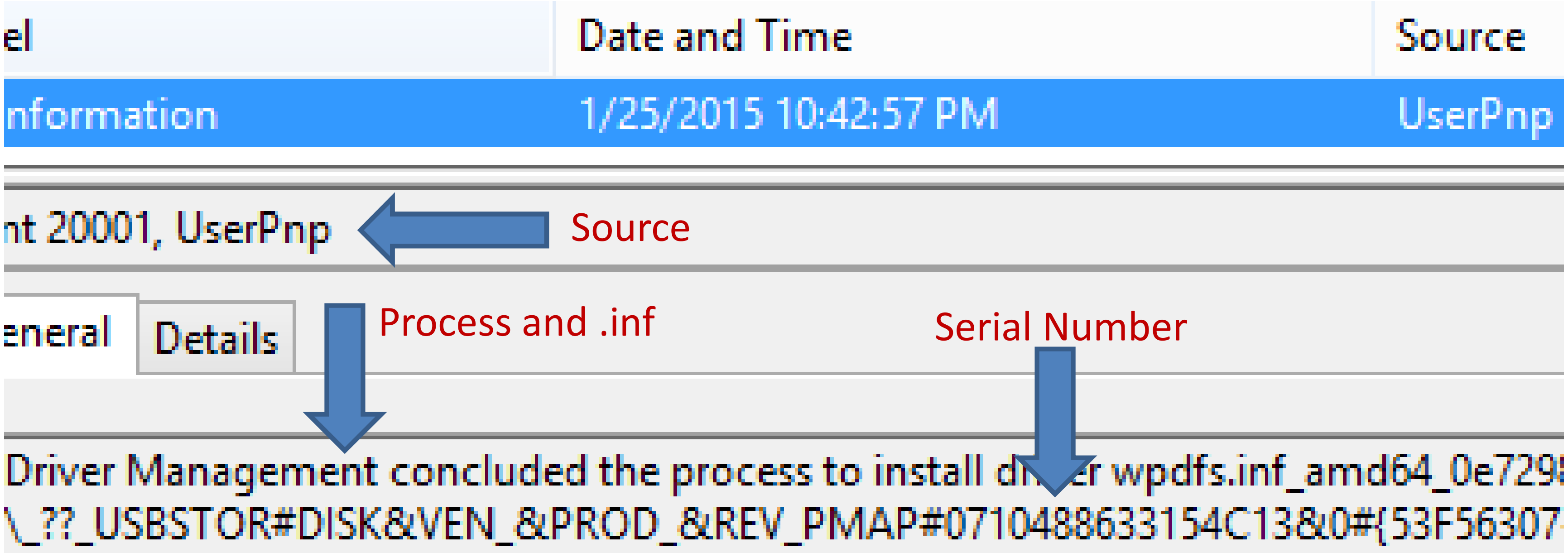


USBSTOR

Disk&Ven_&Prod_&Rev_PMAP

070B4C60C3C2F765&0

Plugins: System Eventlog



el	Date and Time	Source
nformation	1/25/2015 10:42:57 PM	UserPnp

nt 20001, UserPnp

Source

Process and .inf

Serial Number

```
Driver Management concluded the process to install dr  er wpdfs.inf_amd64_0e729
\_??_USBSTOR#DISK&VEN_&PROD_&REV_PMAP#0710488633154C13&0#{53F56307
```

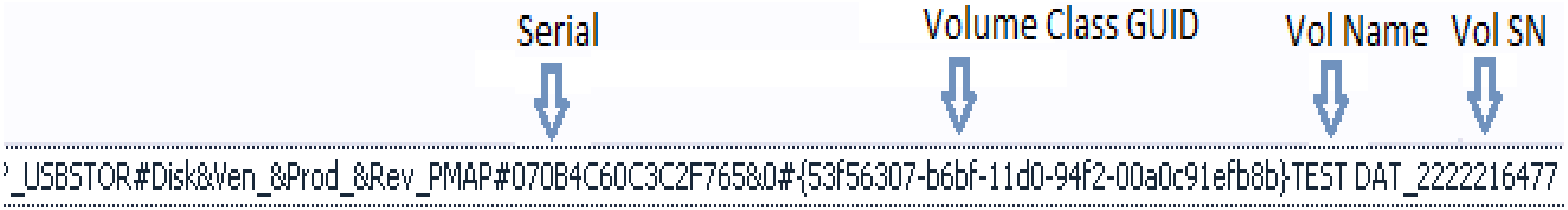
Plugins: Device Classes & MountPoint

- Device Classes (SYSTEM\CurrentControlSet\Control\DeviceClasses\)
  - First Plugin
  - Last Plugin
- Mounted Devices (SYSTEM\MountedDevices)
  - Drive Letter mapping
- MountPoints2 (NTUSER\..\Windows\CurrentVersion\Explorer\MountPoints2)
  - User plugin

```
DeviceClasses (53f56307-b6bf-11d0-94f2-00a0c91efb8b): Saturday,
April 04, 2015 21:43:50 Z (UTC)
```

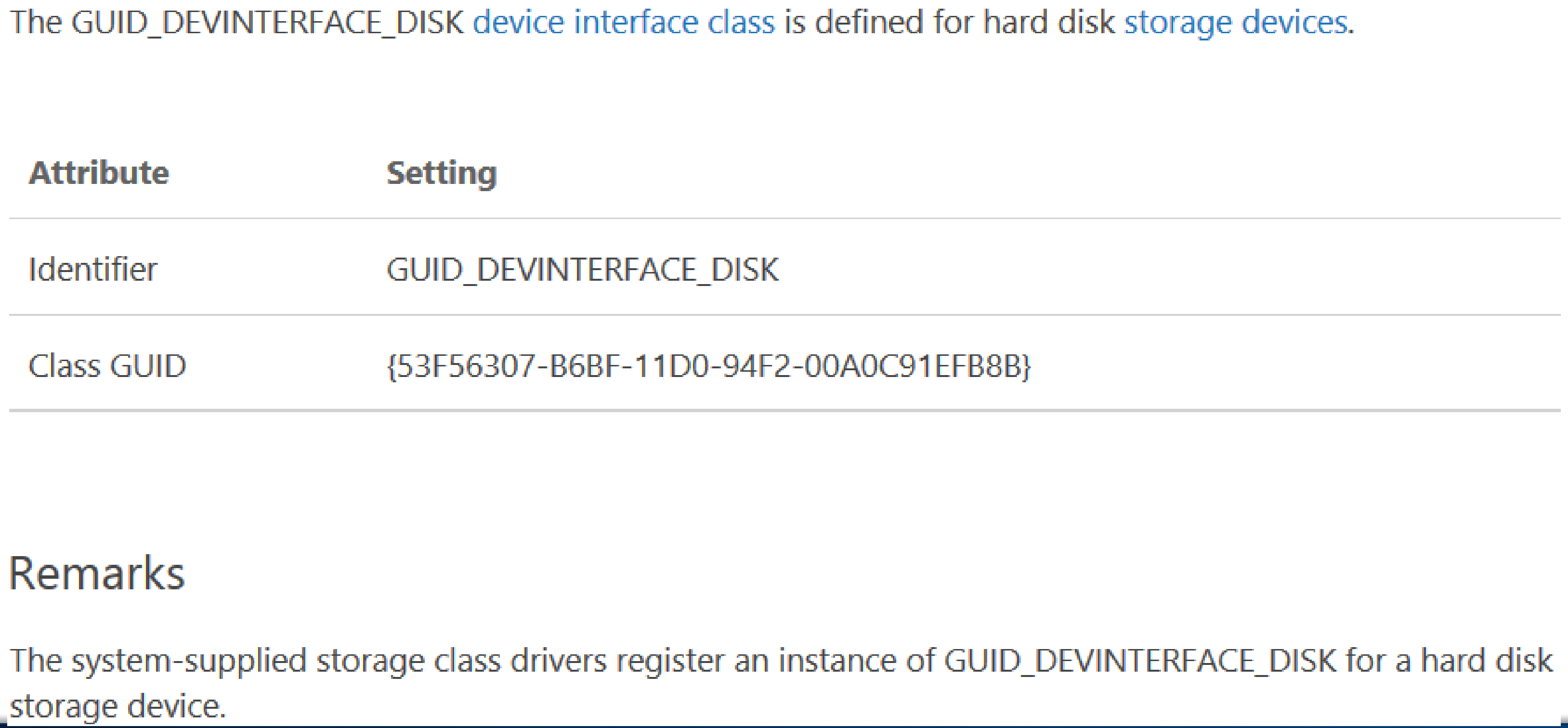
Plugins: EMDMgmt

- ReadyBoost (External Memory Device) artifact
- SOFTWARE\Microsoft\WindowsNT\CurrentVersion\EmdMgmt
- Not just USB devices
- Disabled on SSD’s



```
?_USBSTOR#Disk&Ven_&Prod_&Rev_PMAP#070B4C60C3C2F765&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}TEST DAT_2222216477
```

Plugins: EMDMgmt (Class GUID)



The GUID_DEVINTERFACE_DISK device interface class is defined for hard disk storage devices.

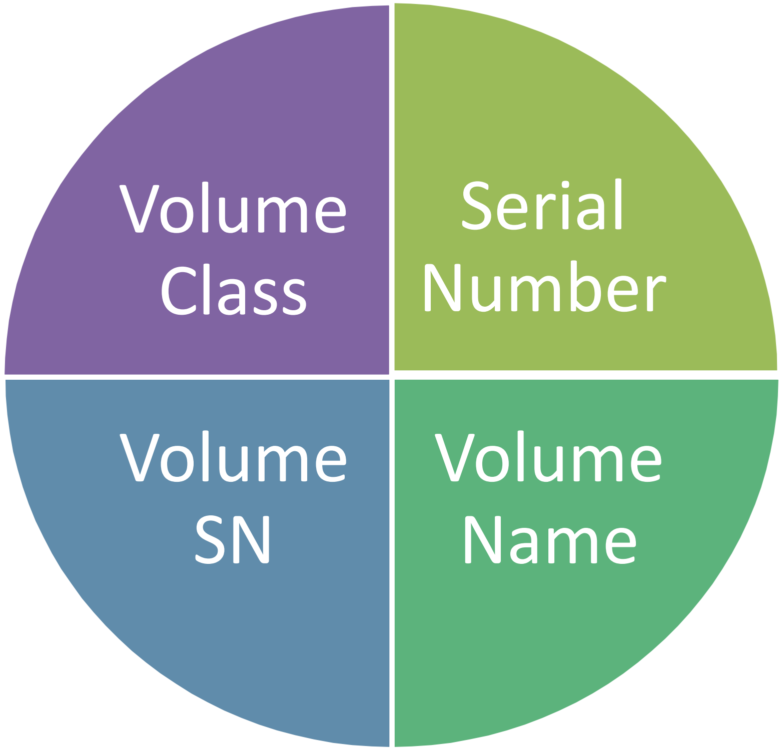
Attribute	Setting
Identifier	GUID_DEVINTERFACE_DISK
Class GUID	{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}

Remarks

The system-supplied storage class drivers register an instance of GUID_DEVINTERFACE_DISK for a hard disk storage device.

Plugins: EMDMgmt

- ➢ Not just USB!



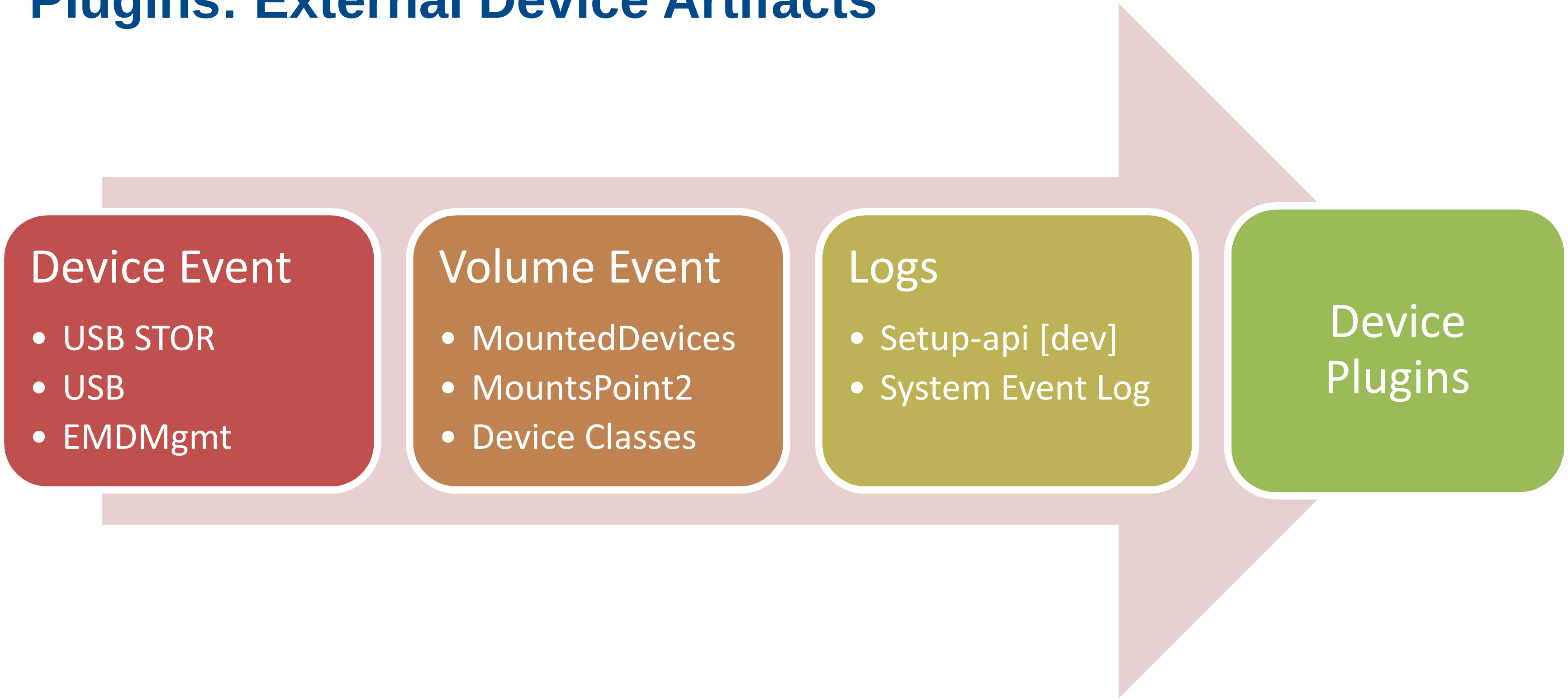
Volume Class

Serial Number

Volume SN

Volume Name

Plugins: External Device Artifacts



Device Event

- USB STOR
- USB
- EMDMgmt

Volume Event

- MountedDevices
- MountsPoint2
- Device Classes

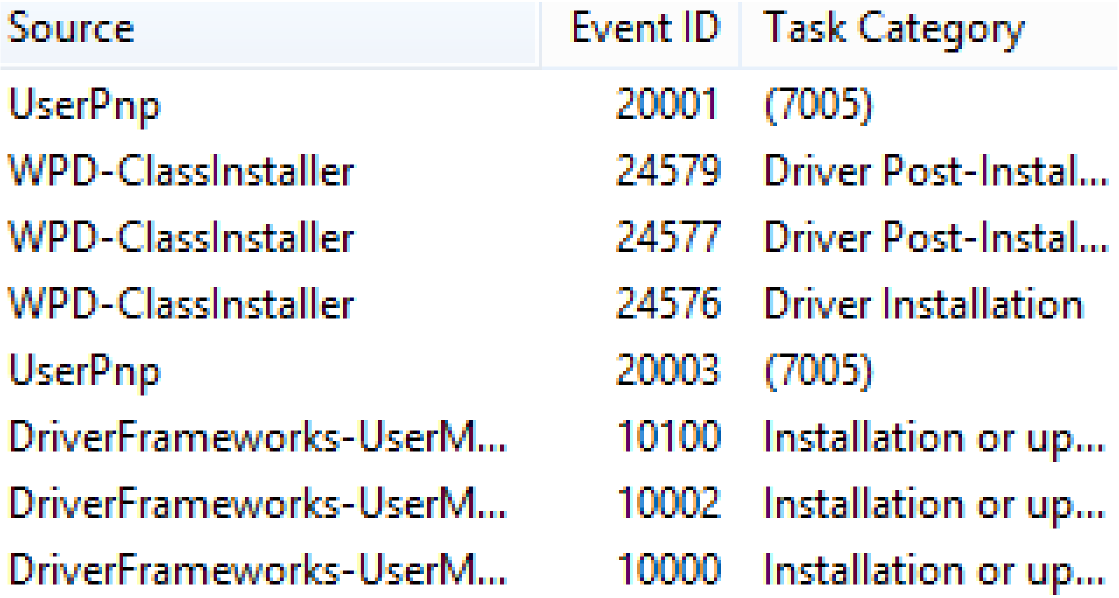
Logs

- Setup-api [dev]
- System Event Log

Device Plugins

Plugins: What you may be missing

- Group policy
  - USBStor not enough
- Phones an exception?
  - Event logs
  - Setup-api-dev.log



Source	Event ID	Task Category
UserPnp	20001	(7005)
WPD-ClassInstaller	24579	Driver Post-Instal...
WPD-ClassInstaller	24577	Driver Post-Instal...
WPD-ClassInstaller	24576	Driver Installation
UserPnp	20003	(7005)
DriverFrameworks-UserM...	10100	Installation or up...
DriverFrameworks-UserM...	10002	Installation or up...
DriverFrameworks-UserM...	10000	Installation or up...

Shadow Copies

Shadow Copies: Why are they important?

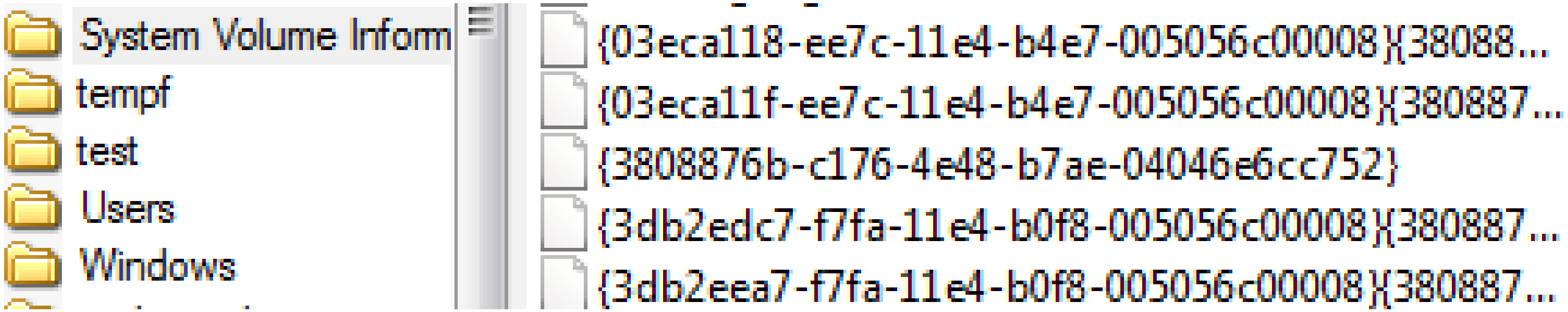
Block level changes

Previous versions

It’s history!

Shadow Copies: Why are they important?

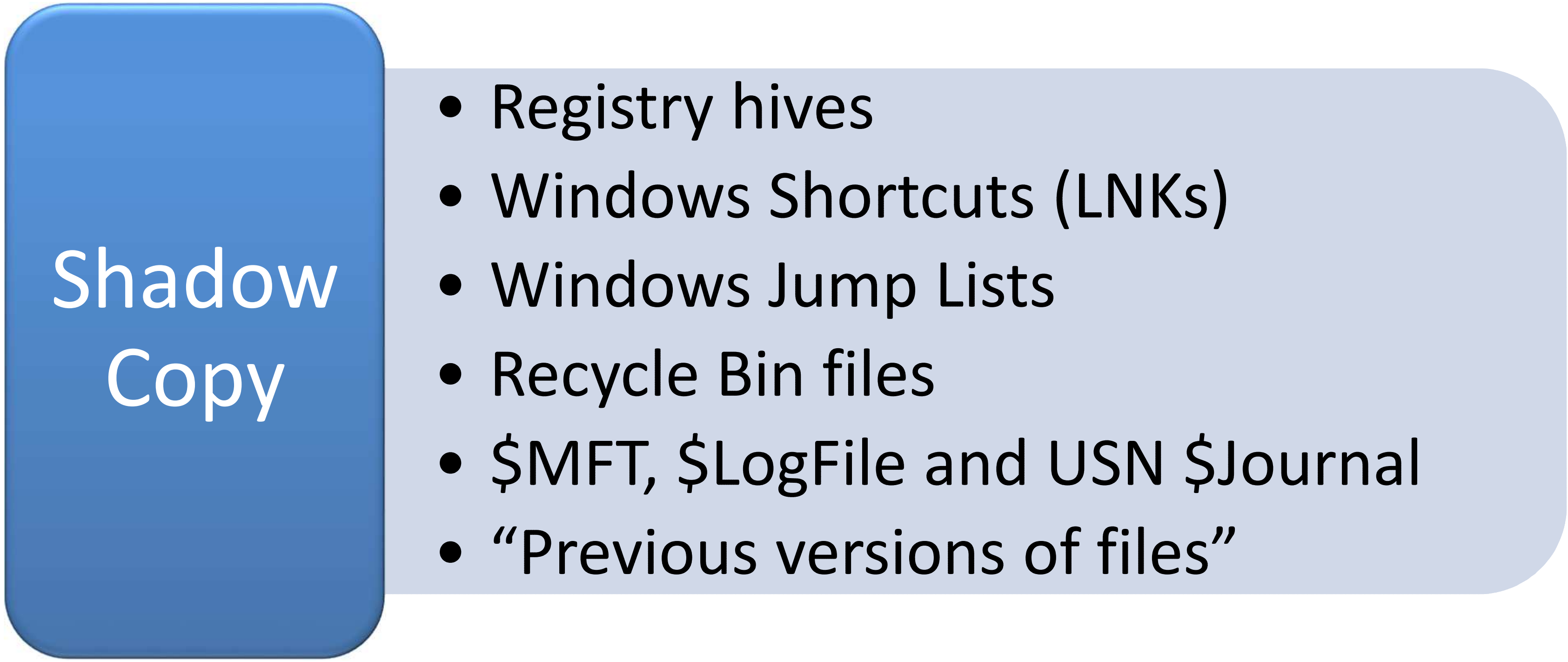
- Where to look for Shadows



System Volume Inform
tempf
test
Users
Windows

{03eca118-ee7c-11e4-b4e7-005056c00008}{38088...
{03eca11f-ee7c-11e4-b4e7-005056c00008}{380887...
{3808876b-c176-4e48-b7ae-04046e6cc752}
{3db2edc7-f7fa-11e4-b0f8-005056c00008}{380887...
{3db2eea7-f7fa-11e4-b0f8-005056c00008}{380887...

Shadow Copies: Why are they important?

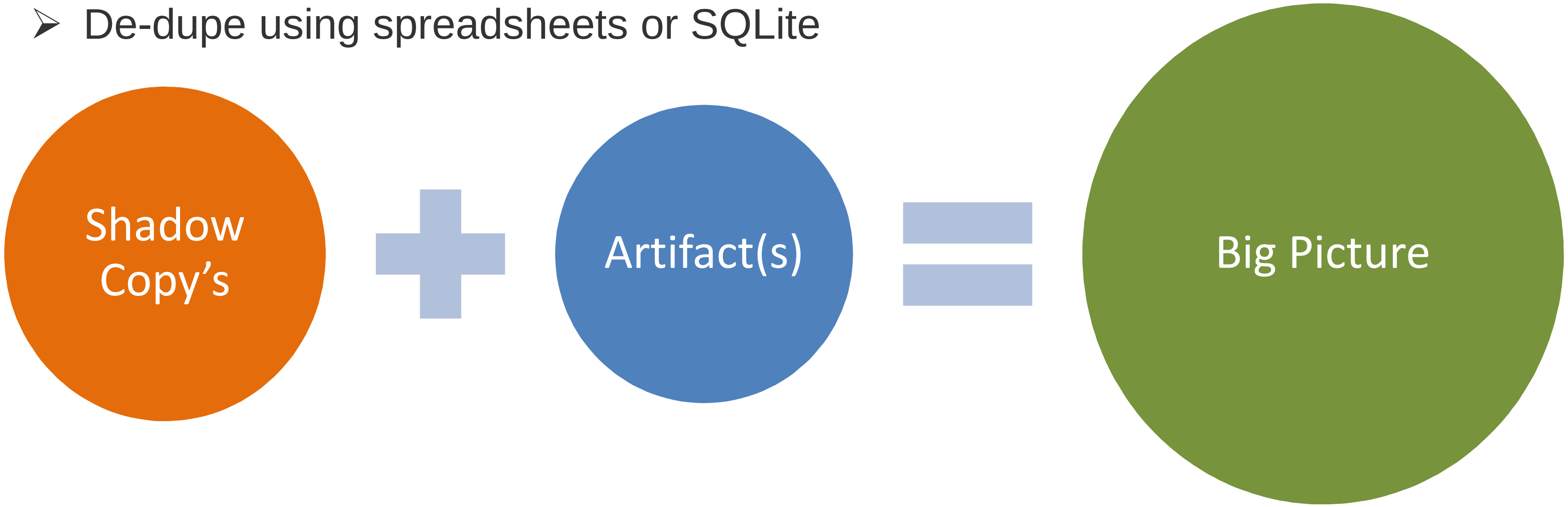


Shadow Copy

- Registry hives
- Windows Shortcuts (LNKs)
- Windows Jump Lists
- Recycle Bin files
- $MFT, $LogFile and USN $Journal
- “Previous versions of files”

Shadow Copies: Don't leave stuff out

- Repeat for each Shadow Copy
- De-dupe using spreadsheets or SQLite



Artifacts: Can’t cover everything

System Activity

HIVEs

HKLM\SYSTEM

-USB Stor

-MountedDevices

-IDE

-Firewire

-Device Class

-Application Compatibility Cache

HKLM\SOFTWARE

-EMDMgmt

Logs/vent Logs

-\System (UserPnP, WPD, DriverFramework)

-\Plug n Play

-\Driverframework-usermode

-\Microsoft-Windows-WPD-MTPClassDriver

-\Microsoft Office Alerts

-\ntfs operational

-Setup-api-dev.log

File System

-Master File Table

-Logfile

-USN Journal

-Shadow Copy’s

User Activity

HIVEs

HKCU\NTUSER.DAT

-Shell Bags

-MRU

-Recent Docs

HKCU\UsrClass.DAT

-Shell Bags

File System

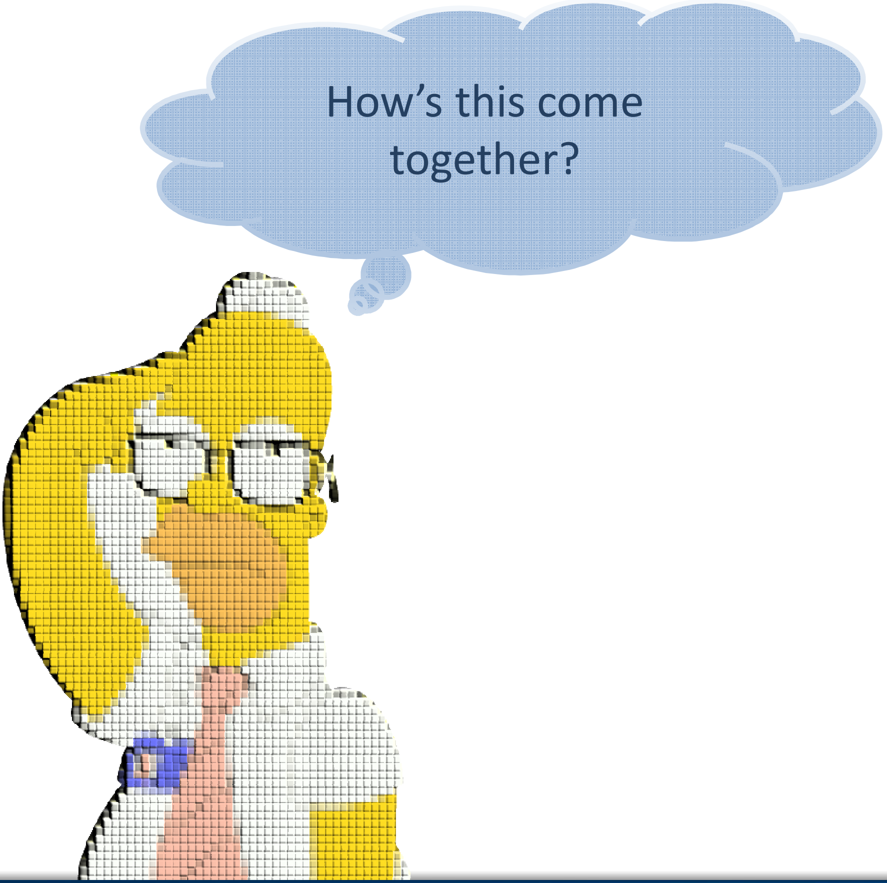
-Windows Shortcuts (LNKs)

-Jumplists

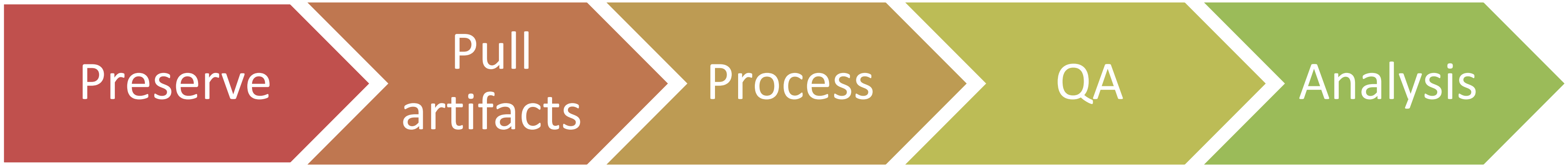
-Temp files

-Shadow Copy’s

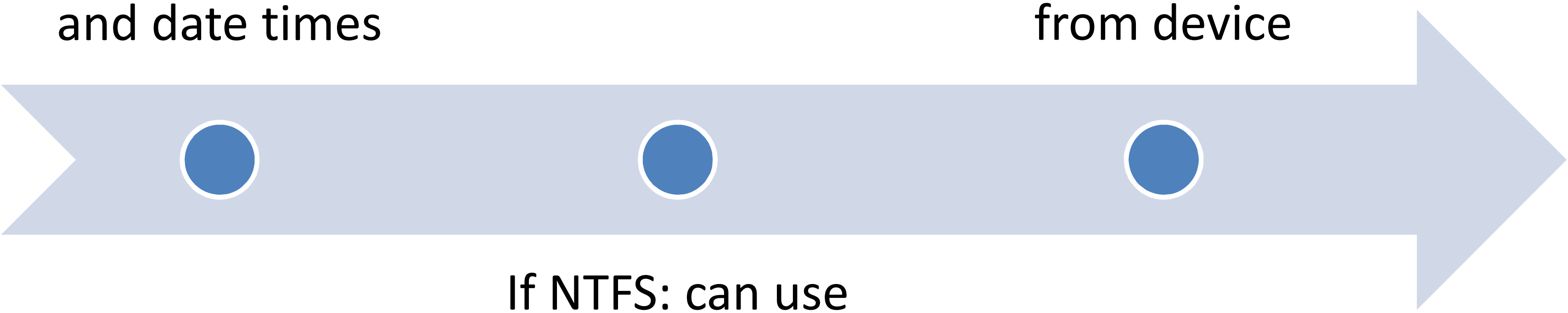
Pulling it together



Process



Process: Correlating to device



Drive letter, path and date times

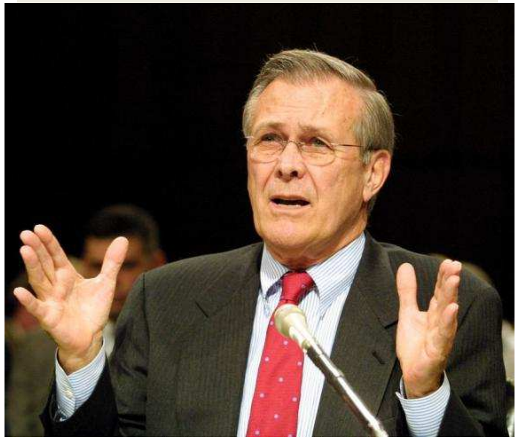
If NTFS: can use MFT record and Sequence numbers

If USN Journal: review USN activity from device

External Device: Direct Correlation

- Serial Number
- Volume Serial
- MFT Record and Sequence Numbers
- *Then use path including drive letter

Use known knowns



External Device: Indirect Correlation

- Timelining activity based on datetimes
- Drive Letter, filename, path
- MRUs
- Easy to make mistakes

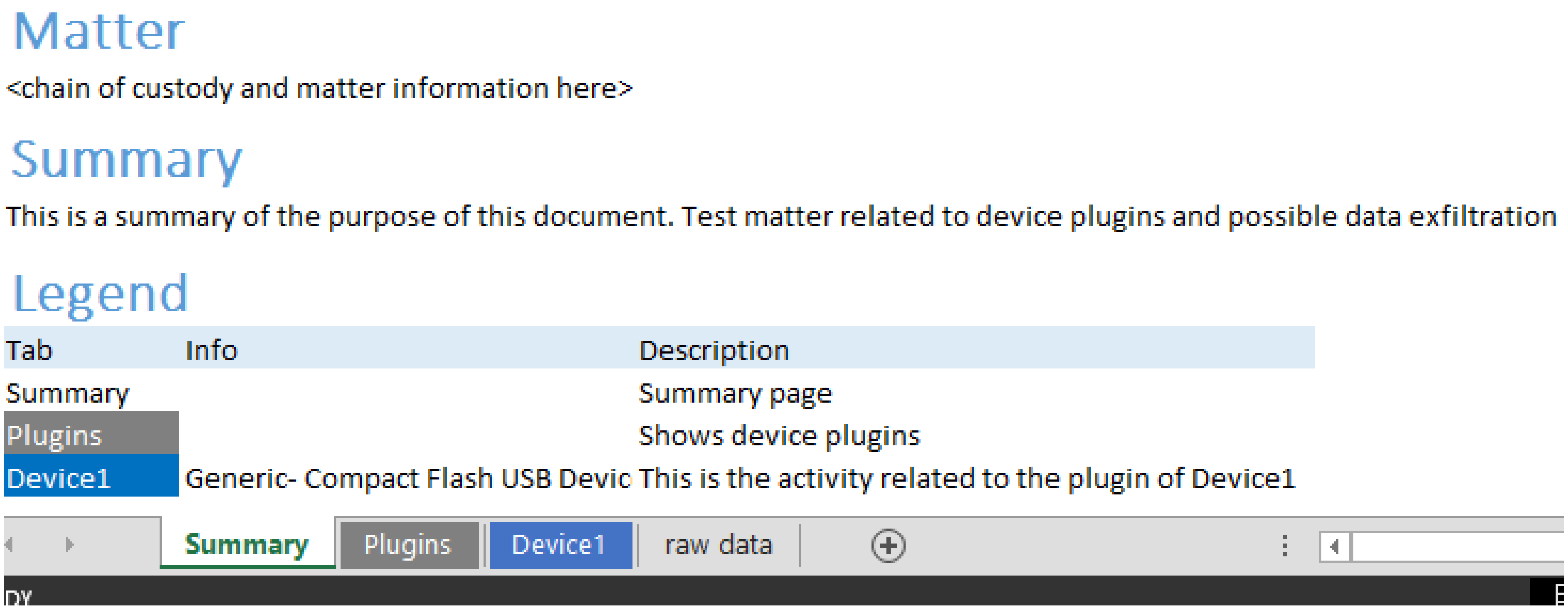
Make it presentable: Concepts

- Simple and detailed
- Easy to review
- Stick to what you can prove

Make it presentable: Content

- Capturing via a Workbook
- Summary page
- Legend on summary page
- Device plugins tab
- Color coded tab per device
- Correlated artifacts per device tab

Make it presentable: Summary Tab



Matter

<chain of custody and matter information here>

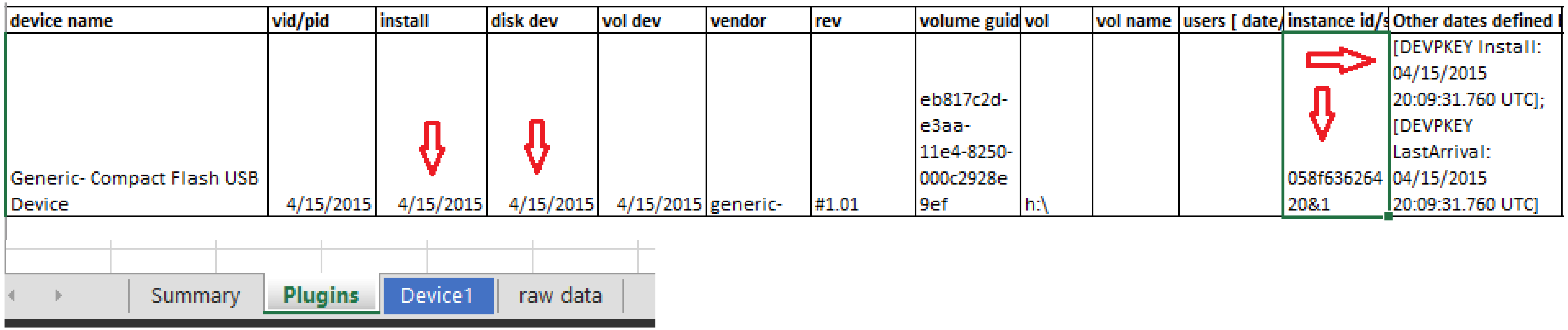
Summary

This is a summary of the purpose of this document. Test matter related to device plugins and possible data exfiltration

Legend

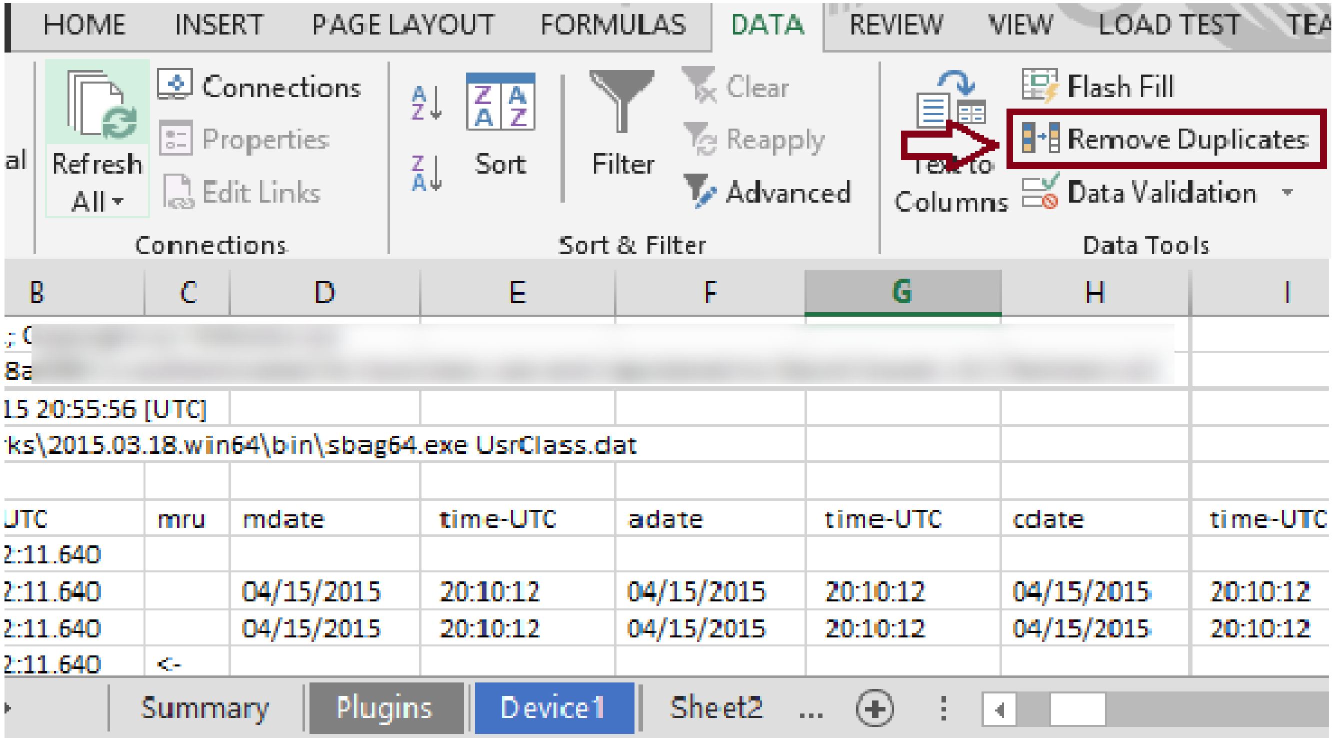
Tab	Info	Description
Summary		Summary page
Plugins		Shows device plugins
Device1	Generic- Compact Flash USB Devic	This is the activity related to the plugin of Device1

Make it presentable: Plugins Sheet



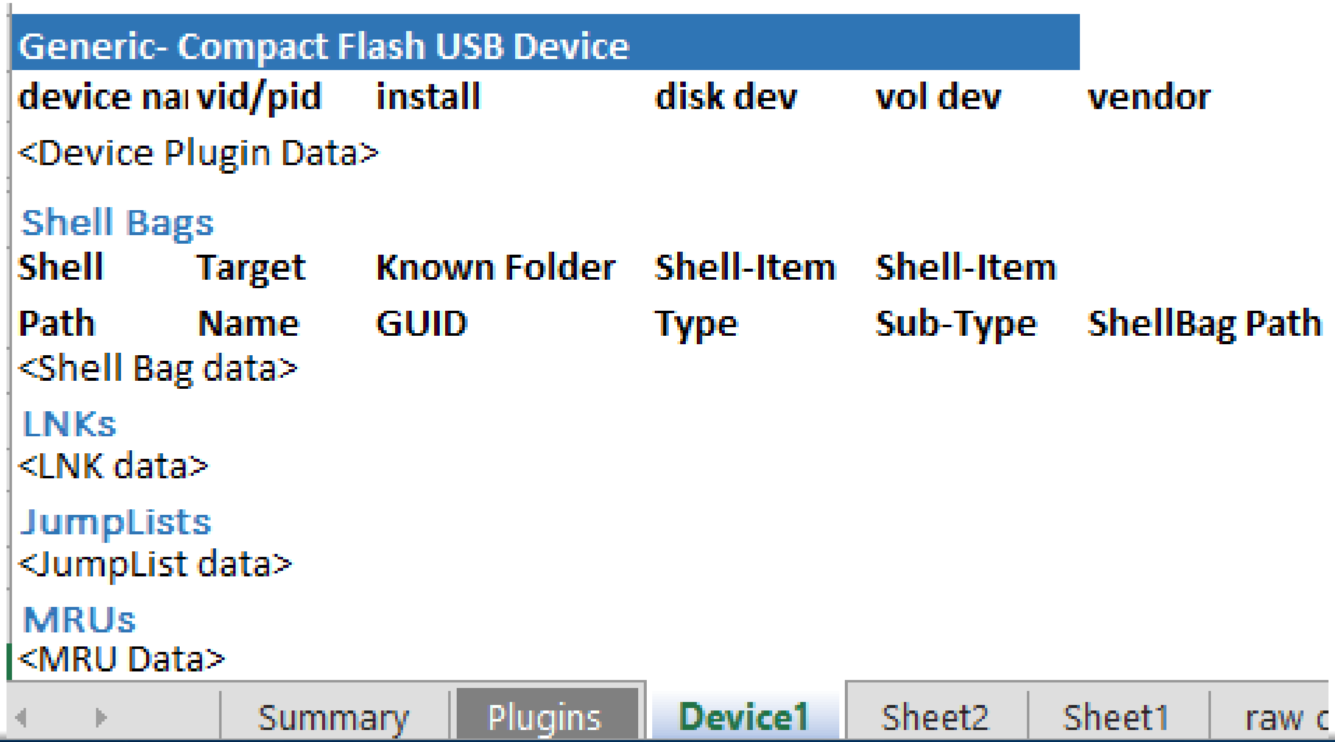
device name	vid/pid	install	disk dev	vol dev	vendor	rev	volume guid	vol	vol name	users [date/	instance id/s	Other dates defined l
Generic- Compact Flash USB Device	4/15/2015	4/15/2015	4/15/2015	4/15/2015	generic-	#1.01	eb817c2d-e3aa-11e4-8250-000c2928e9ef	h:\			058f63626420&1	[DEVPKEY Install: 04/15/2015 20:09:31.760 UTC]; [DEVPKEY LastArrival: 04/15/2015 20:09:31.760 UTC]

Make it presentable: Dupes aren't fun



B	C	D	E	F	G	H	I
; (							
8a							
15 20:55:56 [UTC]							
ks\2015.03.18.win64\bin\sbag64.exe UsrClass.dat							
UTC	mru	mdate	time-UTC	adate	time-UTC	cdate	time-UTC
2:11.640							
2:11.640		04/15/2015	20:10:12	04/15/2015	20:10:12	04/15/2015	20:10:12
2:11.640		04/15/2015	20:10:12	04/15/2015	20:10:12	04/15/2015	20:10:12
2:11.640	<-						

Make it presentable: Device Sheet



Generic- Compact Flash USB Device

device na	vid/pid	install	disk dev	vol dev	vendor

<Device Plugin Data>

Shell Bags

Shell Path	Target Name	Known Folder GUID	Shell-Item Type	Shell-Item Sub-Type	ShellBag Path

<Shell Bag data>

LNKs

<LNK data>

JumpLists

<JumpList data>

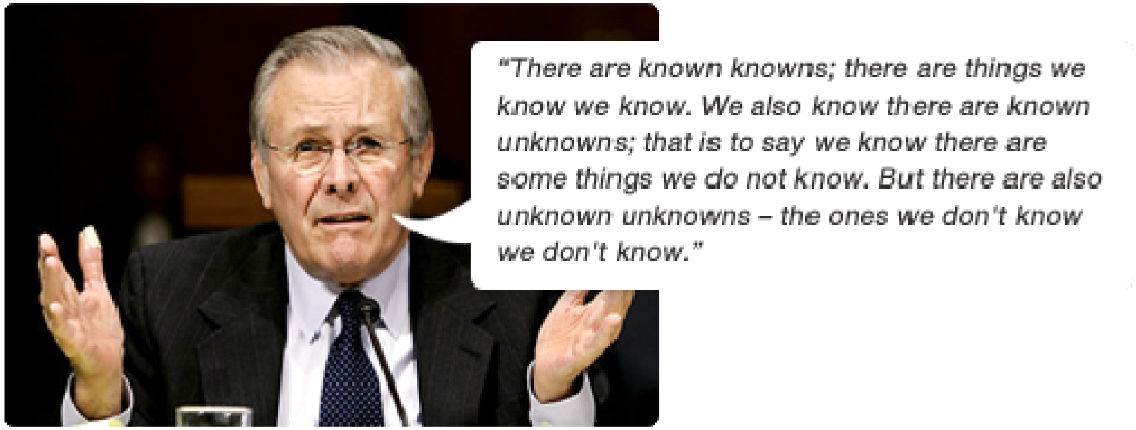
MRUs

<MRU Data>

Make it presentable: Hands on

- Hands-on: Building a spreadsheet

Dealing with Destruction


“There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know.”

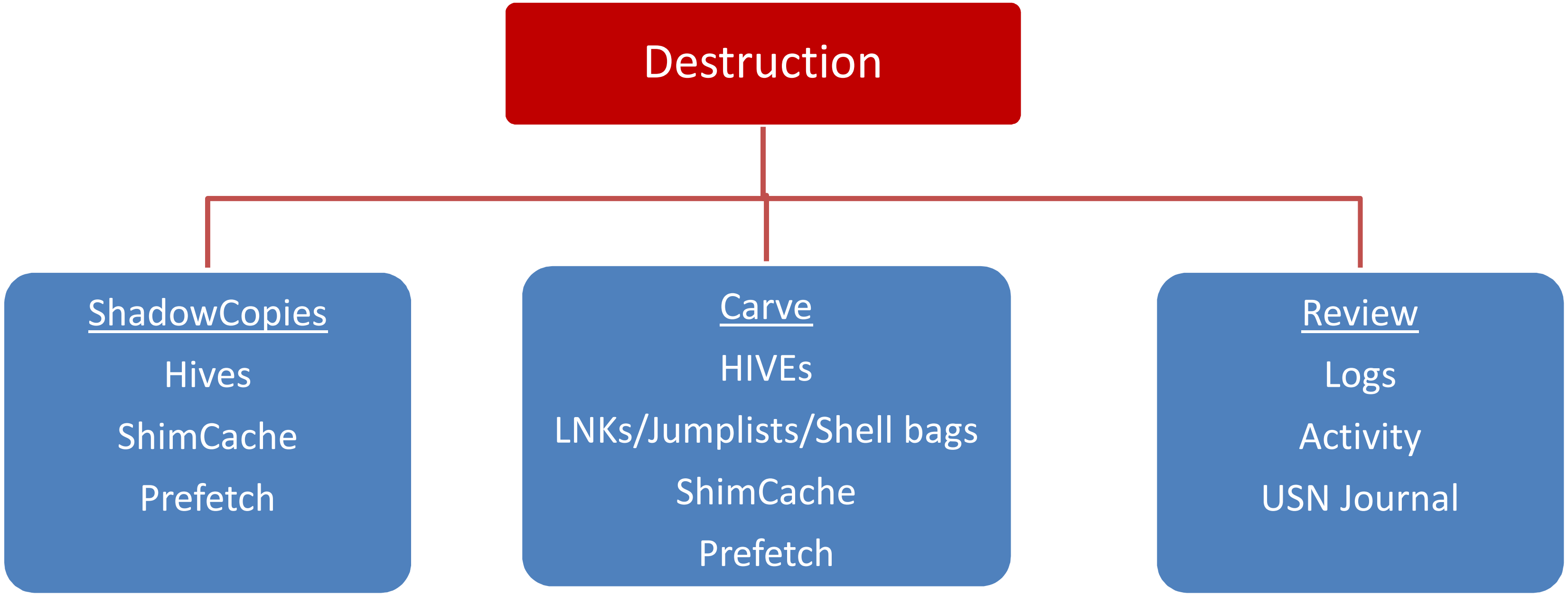
Destruction: Getting started

- Not wiped? Not a dead end!
- Act fast to preserve!
- Carving tools exists but are limited!

Destruction: Indicators

- User hive/folder dates
- OS Install Date
- USN Journal activity
- Original file activity may be carved (unless wiped)

Destruction: Where to look



Destruction

ShadowCopies
Hives
ShimCache
Prefetch

Carve
HIVEs
LNKs/Jumplists/Shell bags
ShimCache
Prefetch

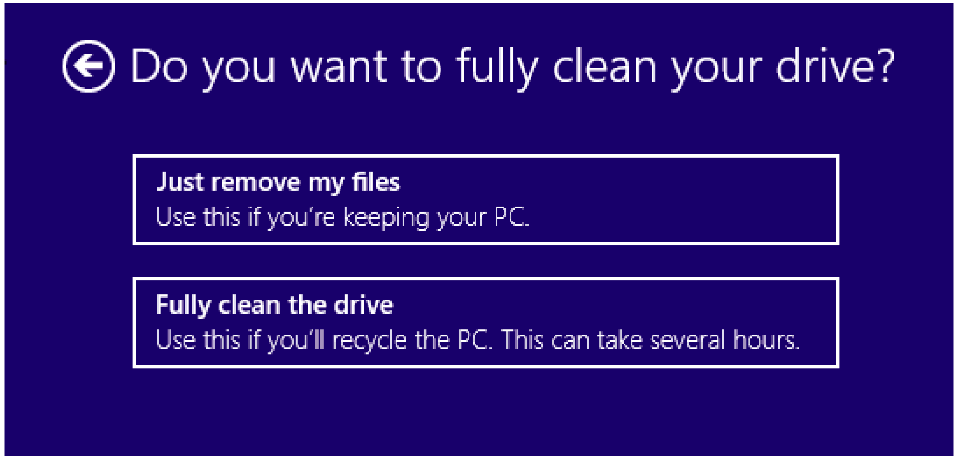
Review
Logs
Activity
USN Journal

Destruction Scenario: Windows 8 was “refreshed”

- Original files including hives moved to \Windows.old
  - Review create dates
- \Recovery – review create dates on log files
- Check the USN $Journal

Destruction Scenario: Windows 8 was “Reset”

- Indicators
  - \$SysReset\Logs\dism.log
    - Review file dates
  - \Recovery\Logs\Reload.xml
    - Review file dates
  - OS Install Date
  - Folder create dates
- Original file activity may be carveable (unless CLEANED)



Do you want to fully clean your drive?

Just remove my files
Use this if you’re keeping your PC.

Fully clean the drive
Use this if you’ll recycle the PC. This can take several hours.

Destruction: Recovering data

- Want to know what occurred?
  - Harness Shadow Copies
  - Carve for hives
  - Carve for event logs
  - Carve for Windows Shortcuts
  - Carve for USN journal fragments
  - Carve for known file signatures

Tools: Getting the job done

Destruction: Tools to Carve for device plugins

Hives

- Reg Recon by Arsenal Recon
- X-Ways Forensics
- Scalpel using recover.py (Andrew Case)

Logs

- X-Ways Forensics
- FTK Toolkit
- TZWorks
- Blade
- Encase

Destruction: Tools to Carve for user activity

- General carving
  - Encase
  - FTK
  - X-Ways Forensics
  - Blade
  - Scalpel
  - Bulk Extractor
- USN
  - Triforce ANJP
  - X-Ways Forensics

Tools: External device activity

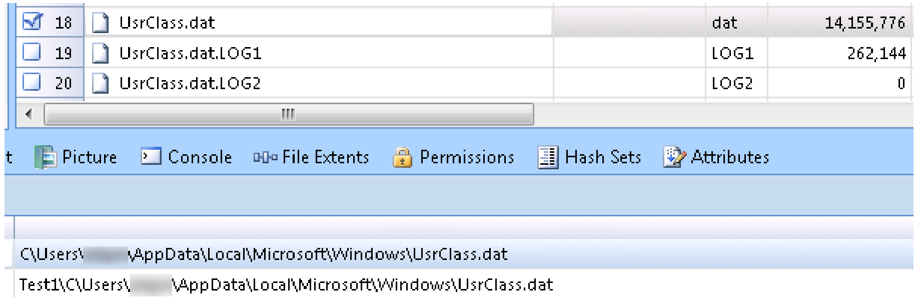
- Sbags,Jmp,lp,cafae by TZWorks
- Encase – ShellBags_Parser Enscript
- ShellBag Explorer – Command line and GUI (free)
- Reg Ripper (free)

Tools: External device plugins

- Usp by TZWorks
- USBDeviceForensics by WoanWare
- Registry viewers
  - FTK Registry Viewer
  - Registry Explorer
  - Encase

Tools: ShellBags with Encase

- (1) Find the UsrClass.dat and NTUSER.dat



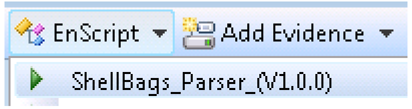
☑	18	UsrClass.dat	dat	14,155,776
□	19	UsrClass.dat.LOG1	LOG1	262,144
□	20	UsrClass.dat.LOG2	LOG2	0

t Picture Console File Extents Permissions Hash Sets Attributes

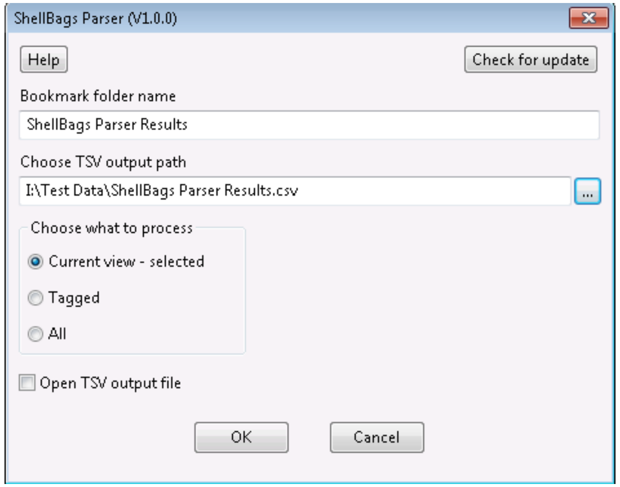
C\Users\[redacted]\AppData\Local\Microsoft\Windows\UsrClass.dat

Test1\C\Users\[redacted]\AppData\Local\Microsoft\Windows\UsrClass.dat

- (2) Run the ShellBags_Parser Enscript



- (3) Choose output options



ShellBags Parser (V1.0.0)

Bookmark folder name: ShellBags Parser Results

Choose TSV output path: I:\Test Data\ShellBags Parser Results.csv

Choose what to process

● Current view - selected

○ Tagged

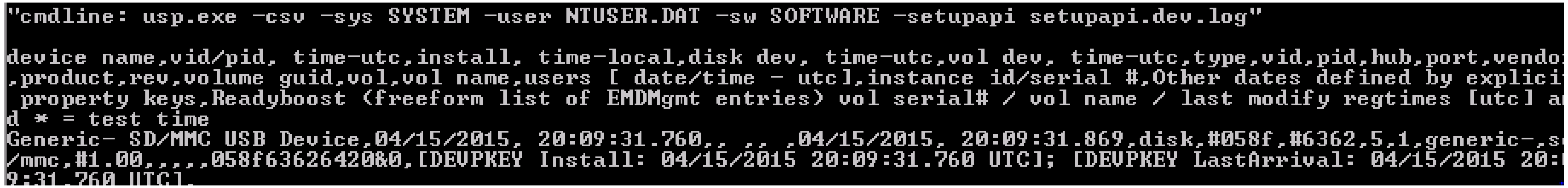
○ All

□ Open TSV output file

Tools: Pull USB Activity

- USB Device plugins using TZWorks

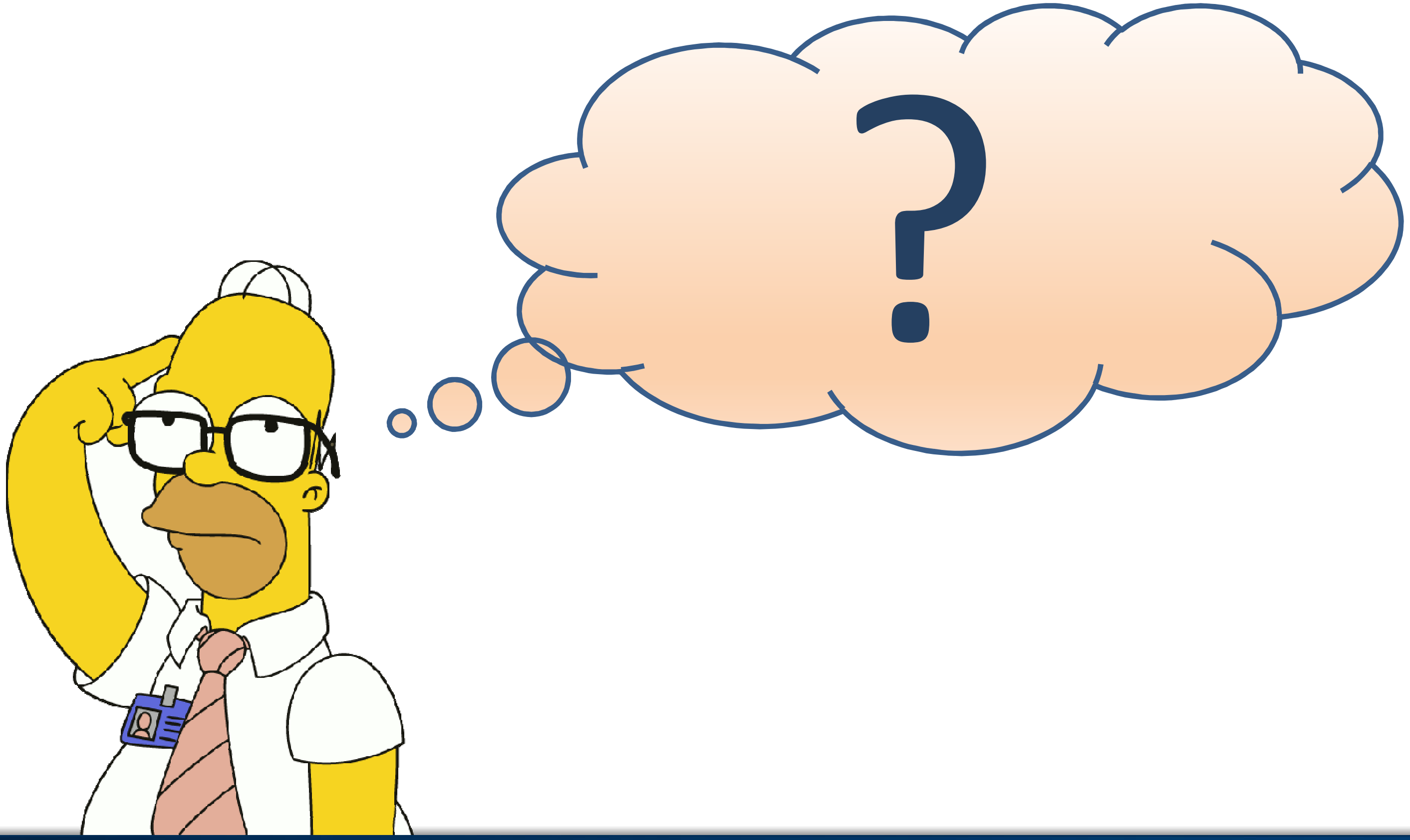
usp64.exe -csv -sys SYSTEM -user “NTUSER.DAT | NTUSERDAT[2].DAT” -sw SOFTWARE -setupapi setupapi.dev.log



```
"cmdline: usp.exe -csv -sys SYSTEM -user NTUSER.DAT -sw SOFTWARE -setupapi setupapi.dev.log"

device name,vid/pid, time-utc,install, time-local,disk dev, time-utc,vol dev, time-utc,type,vid,pid,hub,port,vendo
,product,rev,volume guid,vol,vol name,users [ date/time - utc],instance id/serial #,Other dates defined by explici
 property keys,Readyboost (freeform list of EMDMgmt entries) vol serial# / vol name / last modify regtimes [utc] a
d * = test time
Generic- SD/MMC USB Device,04/15/2015, 20:09:31.760,, ,, ,04/15/2015, 20:09:31.869,disk,#058f,#6362,5,1,generic-,s
/mmc,#1.00,,,,,058f63626420&0,[DEVPKEY Install: 04/15/2015 20:09:31.760 UTC]; [DEVPKEY LastArrival: 04/15/2015 20:
9:31.760 UTC].
```

Questions



Contact Information

David Dym

Email: ddym@g-cpartners.com

Twitter: @dave873

My Blog: www.easymetadata.com/news

Presentation and examples: www.easymetadata.com/Downloads/CEIC/2015/