CEIC® 2014

Advanced Digital Forensic's

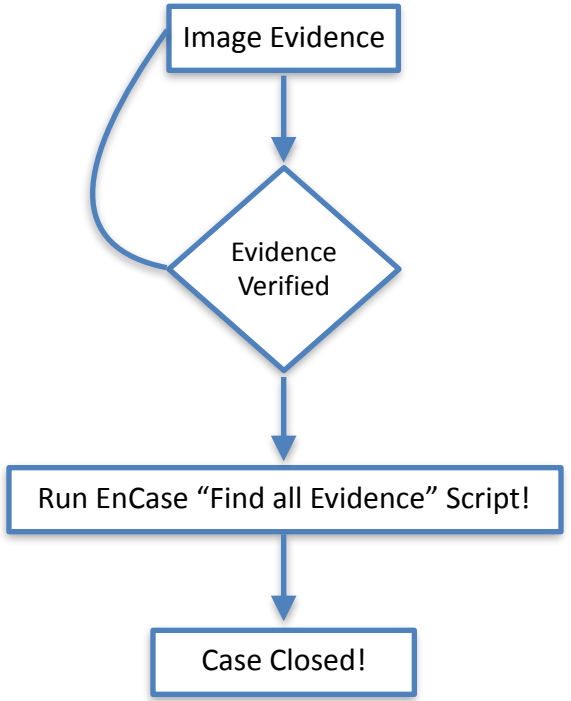
Presented by: Brian Coleman
Senior Manager
Pfizer
Business Technology - Computer Forensics
May 20, 2014

Disclaimer: *This presentation outlines a general technology direction. Pfizer Inc has no obligation to pursue any approaches outlined in this presentation or to develop or use any functionality mentioned in this presentation. The technology strategy and possible future developments are subject to change and may be changed at any time for any reason without notice.*

The views and opinions expressed in this presentation and any related discussion(s) are solely those of the individual presenter(s) and may not express the views of and opinions of Pfizer Inc.

Outline for Today

- About Me / My Forensic Background
- What are “Shellbags”?
- How do you find them?
- What do they look like?
- What value do they hold?
- What does it mean?
- Discussion / Questions?



My Background

- Sacred Heart University
  Bachelor of Science in Computer Science
- Lead Dog Digital
  Web Developer
- Baltimore City Police Department
  Police Officer
- PA Attorney Generals Office Computer Forensics Unit (PA OAG - CFU)
  Special Agent/Supervisory Special Agent
- Defense Cyber Crime Center (General Dynamics Contractor)
  Senior Forensic Examiner
- Federal Bureau of Investigation Computer Analysis Response Team
  Forensic Examiner (FBI - CART)
- Pfizer Inc., Computer Forensics (BT Forensics)
  Senior Manager

My Forensic Background

Certifications:

- FBI CART Forensic Examiner (Windows / MAC Basic)
- DCFL Forensic Examiner
- Certified Digital Media Collector (DCFL and FBI)
- Certified Digital Camera Examiner

- 850+ hours of Training (NW3C, Guidance, FBI, DCFL, AccessData, Sumuri, Blacklight)
- Examined WIN, MAC, Mobile Devices, Game Consoles, GPS Devices, Digital Cameras
- Offered Expert Testimony in State, Federal Grand Jury and Military Court
- Examinations on the following types of cases: child exploitation, fraud, death investigations, bank robbery, espionage, counter intelligence, political corruption, rape, intellectual property……

Presentations for:

Del. Valley HTCIA

Philadelphia Area ECTF

Disclaimer

1. I do not claim to know everything or be a “Forensic God”. I learn new techniques and methods everyday.

2. Information provided is based on a real case, but some information has been redacted so not to identify any individuals.

3. Some Filenames may be offensive and these are not filenames generated by myself but are actual filenames on a suspects evidence.

4. This presentation is meant to be informative and show artifacts that are POSSIBLE to recover. It is up to you to research, test and document for your own purposes. Your results may vary and these types of artifacts may not exist depending on many environmental variables.

SHELLBAGS?

Microsoft Windows uses a Registry key called “Shellbags” to track user settings related to window size, icon and position of folder via Windows Explorer.

Shellbags hold information about directories even after they have been removed/deleted.

Shellbags can be found within the NTUser.dat within Windows XP and the UsrClass.dat within Windows Vista/7.

NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags
NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoamBagMRU
NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\Bags

UsrClass.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
UsrClass.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
UsrClass.DAT\Local Settings\Software\Microsoft\Windows\ShellNoRoam\BagMRU
UsrClass.DAT\Local Settings\Software\Microsoft\Windows\ShellNoRoam\Bags

How do you find them?

Finding “Shellbag” entries that may be of use is just like any other part of your examination, you have to know what you are looking for! If you don’t know what you are looking for, it could be a long day so get a big cup of coffee.

Finding the data in “Shellbags” is the easy part....understanding is not so bad.....testifying about it in detail to a Judge, Jury or Legal Experts you better know what you are talking about.

Lets look at some initial “CLUES” to when a “Shellbag” may be useful.

How do you find them?

1. Understand your case, form “GOOD” keywords
2. Note any keyword hits in UsrClass.dat or NTUser.dat
3. Compare ShellBag data to MOUNTED/USB devices
4. Look at link (.lnk) files to external devices
5. Look at Log files to specific software
6. Look at Internet history with external devices being accessed
7. Mount Volume Shadow Copies and examine thoroughly

Case Review

Foreign Law Enforcement began an investigation into a US Military officer, decided they didn't have enough evidence to proceed -> US Military Investigators

Suspect is being investigated for Rape of a foreign citizen (former girlfriend) and possession of CP (to include pictures of his former underage girlfriend and her friend).

ALL CP (mostly Thumbnails) is in Thumbcache or Unallocated, Suspect had used WIPING software numerous times and uses Encryption.

Pictures of former girlfriend found, but all in UNALLOCATED.

Former girlfriend had some Computer background, so DEFENSE took the approach that it was girlfriend who hacked into and planted this information on computer.

Understand the CASE - Form KEYWORDS

Since most evidence was in UNALLOCATED, took a CHANCE and mounted 17 Volume Shadow Copies (Looking for ANYTHING)

Hash Analysis provided hit within 1 VSC for 2 NCMEC video files.

Performed typical CP Keyword search. In addition, decided to do a keyword search on the 2 unique NCMEC file hits (0013.mpg and 0108.mpg).

POP QUIZ: What is this?

HarddiskVolumeShadowCopy10\Users\<USER>\AppData\Local\Temp\Rar$DR00.689

Many hits within UsrClass.dat within VSC10. (What is this?)

ASK QUESTIONS!!!! IF you don't know someone else might.

MOUNTED DEVICES / USB

Notice Anything Interesting?

	Name	Last Written	Serial	Vendor
1	IronKey Secure Drive USB Device	04/25/08 18:18:01	7A0C01065a6947150f07&0	IronKey
2	CENTON DS PRO 2GB USB Device	04/25/08 18:18:01	0000000000007D&0	__CENTON
3	Apple iPod USB Device	04/25/08 18:18:01	000A270014FAD113&0	Apple
4	CASIO DIGITAL_CAMERA USB Device	04/25/08 18:18:01	6&1c377cf4&0	CASIO
5	CASIO DIGITAL_CAMERA USB Device	04/25/08 18:18:01	6&1fa5350c&0	CASIO
6	CASIO DIGITAL_CAMERA USB Device	04/25/08 18:18:01	7&2c1a74818&0	CASIO
7	CASIO DIGITAL_CAMERA USB Device	04/25/08 18:18:01	7&332d353a&0	CASIO
8	CASIO DIGITAL_CAMERA USB Device	04/25/08 18:18:01	7&fe8c9ee&0	CASIO
9	Hama CF Card Reader USB Device	04/25/08 18:18:01	000000000036&0	Hama
10	Hama FlashPen USB Device	04/25/08 18:18:01	0B20F16080D2F889&0	Hama
11	Hama MS Card Reader USB Device	04/25/08 18:18:01	000000000036&3	Hama
12	Hama SD Card Reader USB Device	04/25/08 18:18:01	000000000036&2	Hama
13	Hama SM Card Reader USB Device	04/25/08 18:18:01	000000000036&1	Hama
14	IronKey Secure Drive USB Device	04/25/08 18:18:01	7A0C01065a6947150f07&1	IronKey
15	Maxtor OneTouch II USB Device	04/25/08 18:18:01	L60B7LPH____&0	Maxtor
16	ST340810 A USB Device	04/25/08 18:18:01	11100E00004F0583	ST340810

MOUNTED DEVICES / USB

IronKey Secure Drive USB Device

VOLUME I:

Name	Device
\DosDevices\I:	?? USBSTOR#Disk&Ven_IronKey&Prod_Secure_Drive&Rev_1.00#7A0C01065a6947150f0

Link (.lnk) file Analysis and Playlists showed many files being accessed on I:

[playlist]
NumberOfEntries=1
file1=H:\Secret Shit
\Webcam_10Yo_Daugther_With_Dad.avi
Version=2
————————————————————
————————————

[playlist]
NumberOfEntries=1
file1=I:\Secret Shit
_28_28Hussyfan_29_29PthcLittleNadyaAnd
Dad.mpg
Version=2

MPCPLAYLIST
1,type,0
1,filename,C:\Users\Patrick\AppData\Local
\Temp\Rar$DR14.922\1 (2).MPG

Log Files/ Link files / Internet History

```
***  Installation Started 03/26/2008 2:23  ***
Title: Kremlin Installation
Source: I:\Secret Shit\KremlinInstaller.exe
```

Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified
Kremlin Wipe.lnk	lnk	3/26/2008 2:23:20 AM	3/26/2008 2:23:20 AM	3/26/2008 2:23:20 AM	4/22/2008 12:21:21 PM

Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified
Kremlin Encrypt.lnk	lnk	3/26/2008 2:23:19 AM	3/26/2008 2:23:19 AM	3/26/2008 2:23:19 AM	4/22/2008 12:25:28 PM

Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified
Lorna.lnk	lnk	5/5/2007 6:39:40 PM	4/21/2007 9:27:24 PM	5/5/2007 6:39:40 PM	4/22/2008 12:25:27 PM

Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified
Hannah.lnk	lnk	4/17/2007 9:19:31 PM	4/17/2007 9:19:31 PM	4/17/2007 9:19:31 PM	4/22/2008 12:25:27 PM

Type	URL
http	http://www.google.co.uk/search?num=100&hl=en&safe=off&sa=X&oi=spell&resnum=0&ct=result&cd=1&q=command+prompt+hard+drive+free+space+wipe&spell=1

What about Shellbags?

Examined Shellbag data within the USRClass.dat

UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\

bag	Regkey modtime [UTC]	folder name	createdate	ctime	modifydate	mtime	accessdate	atime	full path
307	03/09/08 15:42:22.623	Secret Shit	02/10/2008	16:49:48	02/10/2008	16:49:48	02/13/2008	00:00:00	Desktop\{CLSID_MyComputer}\I:\Secret Shit\

BAG 307 - FOLDER NAME = SECRET SHIT

(maybe a clue)

and it is on a VOLUME I:

(IronKey Encrypted USB Drive)

What about Shellbags?

"UsrClass.dat" file reveals a file with the same exact filename, modified date and file size existed on a "IronKey USB Device" within a folder labeled "Secret Shit".

ShellBag results for hive: K:\Users\Patrick\AppData\Local\Microsoft\Windows\usrclass.dat

bag	Regkey modtime [UTC]	folder name
307	03/09/08 15:42:22.623	Secret Shit

createdate	ctime	modifydate	mtime	full path
02/10/2008	16:49:48	02/10/2008	16:49:48	Desktop\{CLSID_MyComputer}\I:\Secret Shit\

bag	Regkey modtime [UTC]	file name
307	04/25/08 01:14:34.764	0108.mpg

A bag id number of "307" which has a folder name of "Secret Shit" along with the associated created time, modified time and the path to the "Secret Shit" folder on the IronKey USB device (I:) has been recorded by the Windows registry.

bag	Regkey modtime [UTC]	file name
307	04/25/08 01:14:34.764	0013.mpg

file size	createdate	ctime	modifydate	mtime
0x000785a0	03/06/2008	12:00:36	10/17/2006	03:28:04

"0013.mpg"

Is Deleted	Last Accessed	File Created	Last Written	Entry Modified	Physical Size
No	04/13/08 14:23:53	04/13/08 14:23:53	10/17/06 03:28:04	04/13/08 14:23:53	492,960

Shellbag file size in HEX: 785A0

Converted to Decimal: 492960

File size matches, Last Written date MATCHES SBag modify date....More than likely the same video!

We Never had the Iron Key!

	Regkey modtime [UTC]	file name
)7	04/25/08 01:14:34.764	Links
)7	04/25/08 01:14:34.764	Temp Download Folder
)7	04/25/08 01:14:34.764	Pix
)7	04/25/08 01:14:34.764	Previews
)7	04/25/08 01:14:34.764	UU34.mpg
)7	04/25/08 01:14:34.764	nelia 11 yo.avi
)7	04/25/08 01:14:34.764	_28pthc_29_21_21_21NEWanyanew2.r
)7	04/25/08 01:14:34.764	_28pthc_29Mes4_6yrgirlwith17yrboy_
)7	04/25/08 01:14:34.764	babyj-face.avi
)7	04/25/08 01:14:34.764	Cbaby.mpeg
)7	04/25/08 01:14:34.764	cbabynoon3.wmv
)7	04/25/08 01:14:34.764	K14&K13.AVI
)7	04/25/08 01:14:34.764	Lada 9Yr.avi
)7	04/25/08 01:14:34.764	Lada 9yr undress.avi
)7	04/25/08 01:14:34.764	Lada In Bathtub.avi
)7	04/25/08 01:14:34.764	Lada Kinky Cat.mpg
)7	04/25/08 01:14:34.764	madisonsarah001.avi
)7	04/25/08 01:14:34.764	Mary Belize (14m10s).mpg
)7	04/25/08 01:14:34.764	MFPD Wednesday.avi
)7	04/25/08 01:14:34.764	O_Dvd007PreteenBoyAndGirlFuck_Pt

Victim testified that she found pictures of herself and a friend on Suspects computer within folders that contained their first name. After she DELETED them, somehow they kept coming back.

Suspect was storing Volume Shadow Copies on this Device. It was suspected that he was restoring the pictures from Shadow Copies which Shellbags showed were on this device also.

What does it all mean?

1. IronKey USB was used but never found/seized
2. IronKey was mounted as H and I
3. IronKey contains CP
4. IronKey contains common CP terms/filenames
5. IronKey contains a folder “Secret Shit”
6. IronKey contains files that are “NCMEC” hits
7. IronKey contained copies of Volume Shadow Copy
8. IronKey contained “Kremlin” software
9. Kremlin wipe was used on machine

Why its Important

The ability to state facts about files on devices which were never seized..... (Criminal Inv., Employee theft, Unauthorized Copying to/from system)

The digital evidence proved beyond a reasonable doubt the victim was telling the TRUTH!

Just because you don't have the device, doesn't mean you can't state anything about what was on it.

If you don't ask QUESTIONS, you will miss things.

Be CURIOUS! Be THOROUGH!
Compare Dates/Times, File Paths, USB Devices, Link files, Internet history .....

Lesson's Learned

Don't cut corners to save time. If you do, you will overlook some evidence that may prove guilt or innocence.

As the examiner, YOU are the one who will be held responsible. Your lab manager/ director will not be the one testifying or liable…..Do your job.

Document, Document, Document……..Keep detailed notes
(Imaging and Examination)

Ask Questions, Ask more Questions, Test and Understand

Help legal council understand the technical results

EXCELLENT RESOURCES

- 4N6K BLOG - Shellbag Forensics: Addressing a Misconception
  Dan Pullega (Twitter @4n6k)
  http://www.4n6k.com/2013/12/shellbags-forensics-addressing.html

- SANS Digital Forensic BLOG (Computer Forensic Artifacts: Windows 7 Shellbags)
  http://digital-forensics.sans.org/blog/2011/07/05/shellbags

- Windows Shellbag Forensics
  http://www.williballenthin.com/forensics/shellbags/

- Using Shellbag information to reconstruct user activities (DFRW 2009 Research Paper)
  http://www.dfrws.org/2009/proceedings/p69-zhu.pdf

- MoVP 3.2 Shellbags in Memory, SetRegTime, and TrueCrypt Volumes
  http://volatility-labs.blogspot.com/2012/09/movp-32-shellbags-in-memory-setregtime.html

- Harlen Carvey Blogs on Shellbag Artifacts and Testing
  http://windowsir.blogspot.com/2013/10/shell-item-artifacts-reloaded.html
  http://windowsir.blogspot.com/2012/10/shellbag-analysis-revisitedsome-testing.html

What QUESTIONS do you have?