Talking to the Tech

Asking the Right Questions

Eric R. Zimmerman
Senior director, Kroll Cyber Security
eric.zimmerman@kroll.com
501-313-3778
@EricRZimmerman
https://binaryforay.blogspot.com/

Why are we here?

- Learn some lingo
- Explore some forensic artifacts
- Search concepts
- Discover a framework to effectively ask for what you need

Lingo and you: a guide

- Forensic images
- Data recovery
- Searching

Forensic image

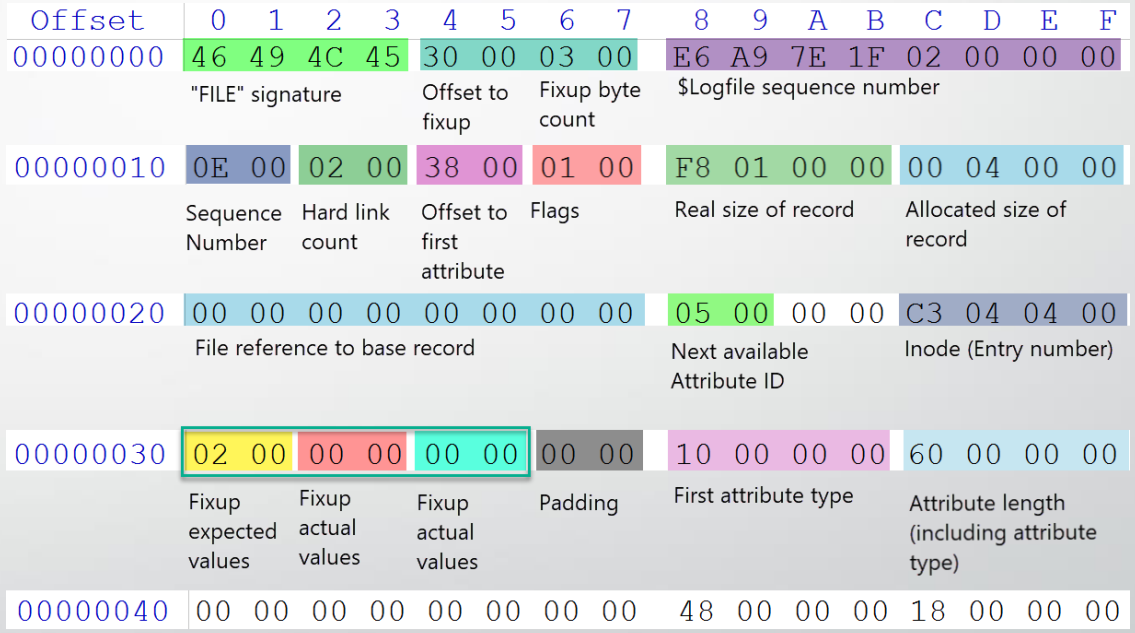
- Do not work on original evidence
  - The forensic image solves this
- Common image formats
  - DD
  - E01
- Physical vs logical vs targeted collection

Data recovery

- What happens when a file is deleted?
- Recovery scenarios
  - Via the file system
  - Carving

Data recovery: file deletion

- For any given file on a computer, a record tracks details about the file
  - Location, size, timestamps, filename
- When a file is deleted, the details are not really gone
  - The record tracking the file is just marked as not being in use any more
- In addition to the record being marked as free, the storage space used to hold a file's contents is also marked as free



Data recovery: scenarios

- Via the file system
  - By using metadata about the file, it is possible to recover information about deleted files by looking for free records.
  - In some cases, if the storage that was originally assigned to a file has not been reused by other files, content can also be recovered
- Carving
  - If metadata is not available to aid in recovery, looking for signatures for different file types can be used to recover data.
  - This involves looking at free space on a hard drive for specific patterns that identify things like photographs, Word documents, archives, etc.

Data recovery: compare and contrast

File system	Carving
Recover original file name and location	Filename and location not available
Fragmentation less of an issue	Fragmentation more of an issue
Data located quickly	Data located more slowly
File system metadata available (timestamps)	No file system metadata available (but internal metadata may be present
May not be able to recover original data (clusters in use)	Data can usually be recovered (unless fragmented)

Searching

- Traditional vs index
- Concerns and pitfalls
  - Compression
  - Fragmentation
  - Compound file types
- Building effective search term lists

Searching: Traditional vs index

- Traditional
  - For a given set of search terms, look at the data inside files for one or more of the terms. Each search requires iterating over the data in a case looking for strings
  - Can be faster than waiting for an index if you already know what you want to look for and it won't change
- Index
  - Involves looking for all unique instances of words based on minimum and maximum lengths.
  - Can take a long time to build the index, but very fast to search
  - More useful if search terms are unknown or dynamic

- Certain forensic tools require BOTH to be done in order to not miss data. Examiners should know the capabilities and limitations of their tool of choice

Searching: Concerns and pitfalls

- Compression: Changes how the data is represented on disk. Search tools have to decompress data before searching
- Fragmentation: If files are not stored contiguously, data can be missed across these boundaries
- Compound file types: Searching plain text vs encoded documents like PDFs, Word documents, Excel, etc. This can also involve issues with compression depending on the file type

Searching: term lists

- Keep it simple
  - Do not try to look for every variation of a word
    - cannot, can't, cant
  - Take the common base, or avoid all together. Context can be searched for around other keyword hits as needed
- Focus on less common words
  - Depends on the type of case
- Avoid compound terms
  - 'Eric Zimmerman' vs searching for 'Eric' and 'Zimmerman' separately
  - Why? What if the actual term was 'Eric R Zimmerman'?
- By following these principles, more accurate hits can be composed by combining simpler terms into more complex criteria
  - 'Eric' AND 'Zimmerman' within 5 characters

Navigating a sea of forensic artifacts

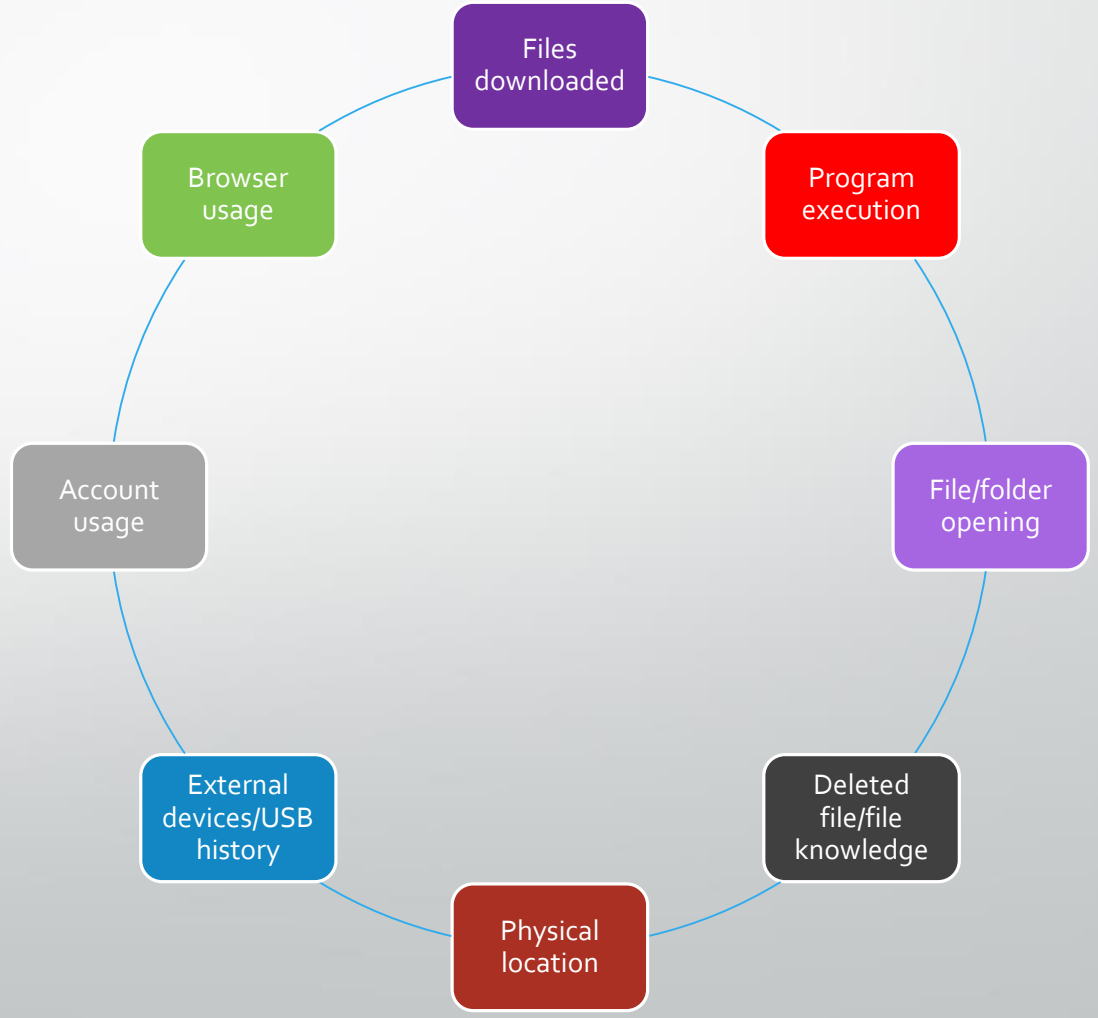
- Think categorically
- Focus on the questions you want answered
- Map these questions to one or more categories

Think categorically

- Rather than get lost in the minutia of seemingly countless forensic artifacts, we need a framework that allows us to provide guidance to forensic examiners
- By thinking about WHAT you need from a computer, it allows you to stay on target with the questions you need answers to vs getting lost in the weeds.

Focus on the questions you want answered

- What do you need to prove or disprove?
- Who, what, where, when
  - **Who** was using a system?
  - **What** where they doing?
  - **Where** was the computer?
  - **When** did it happen?



Program execution: Prefetch

- Keeps track of
  - Program executed
  - How many times
  - Up to the last eight execution times
  - Files and directories a program interacted with

- Why do we care?
  - Tracking program execution intersects essentially every investigation

```
PS C:\Tools> .\PECmd.exe -f D:\Temp\POWERPNT.EXE-40AAC806.pf
PECmd version 1.0.0.0

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

Command line: -f D:\Temp\POWERPNT.EXE-40AAC806.pf

Warning: Administrator privileges not found!

Keywords: temp, tmp

Processing 'D:\Temp\POWERPNT.EXE-40AAC806.pf'

Created on: 2018-07-07 15:09:44
Modified on: 2018-08-07 13:10:44
Last accessed on: 2018-07-07 15:09:44

Executable name: POWERPNT.EXE
Hash: 40AAC806
File size (bytes): 444,596
Version: Windows 10

Run count: 11
Last run: 2018-08-07 13:10:34
Other run times: 2018-08-06 22:32:37, 2018-08-06 22:28:23, 2018-08-06 13:19:16, 2018-07-25 18:17:36,
2018-07-25 18:11:36, 2018-07-25 18:05:08, 2018-07-18 13:28:32
```

Program execution: Jump lists

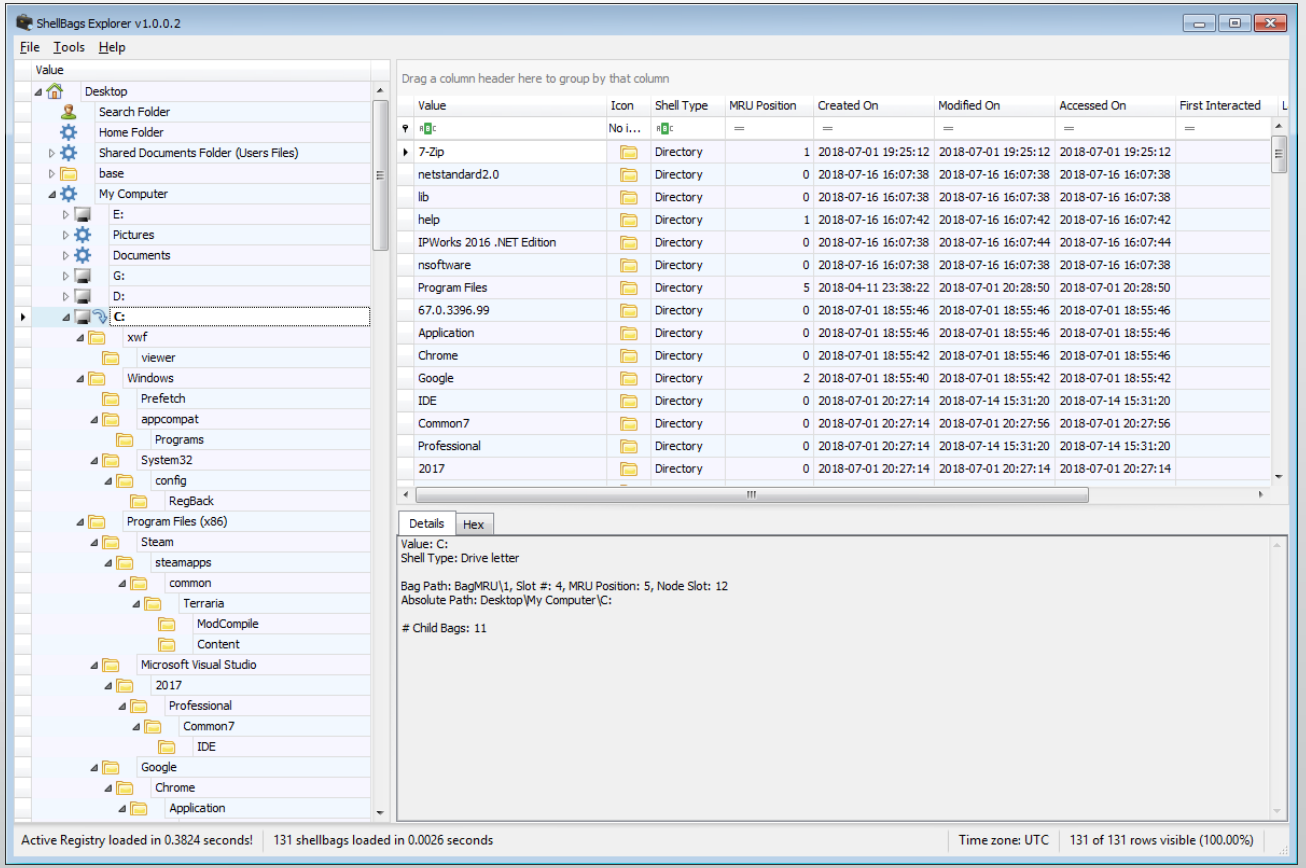
- Keeps track of
  - Program executed
  - Files and directories opened by a program
  - Timestamps
- Why do we care?
  - Track around 2,000 unique files or directories per jump list
  - Specific to a single application means the data stays around for a long time
  - Stored on a per user basis, so allows for attributing actions to a given user

```
PS C:\Tools> .\JLECmd.exe -f C:\Users\eric\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinati
ons\f01b4d95cf55d32a.automaticDestinations-ms
JLECmd version 1.0.0.0

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

Command line: -f C:\Users\eric\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f01b4d95
cf55d32a.automaticDestinations-ms

Warning: Administrator privileges not found!

Processing 'C:\Users\eric\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f01b4d95cf55d
32a.automaticDestinations-ms'

Source file: C:\Users\eric\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f01b4d95cf55
d32a.automaticDestinations-ms

--- AppId information ---
  AppID: f01b4d95cf55d32a
  Description: Windows Explorer Windows 8.1.

--- DestList information ---
  Expected DestList entries:  101
  Actual DestList entries: 101
  DestList version: 4

--- DestList entries ---
Entry #: 18
  MRU: 0
  Path: D:\Egnyte\Private\ezimmerman\!!SANS WORK\Expenses\53985 Augusta GA
  Pinned: False
  Created on: 2018-06-12 12:08:47
  Last modified: 2018-08-07 17:52:31
  Hostname: ez-w
  Mac Address: b0:6e:bf:ba:73:80

--- Lnk information ---

  Absolute path: My Computer\D:\Egnyte\Private\ezimmerman\!!SANS WORK\Expenses\53985 Augusta GA
```

File/folder opening: Shellbags

- Keeps track of
  - Directories accessed
  - Network resources
  - Timestamps

- Why do we care?
  - Acts like a GPS for a user's file system in that it shows you exactly where (and usually when) a user went on their computer
  - Quickly lets you hone in on suspicious behavior



File/folder opening: Lnk files

- Keeps track of
  - Files, programs, and directories accessed
  - Timestamps
    - First and last opened

- Why do we care?
  - Like jump lists, stored on a per user basis
  - Contains device serial numbers (USB, hard drives, etc.)
  - Contains data that allows examiners to link shell bag data to lnk files which allows examiners to show access on specific devices

```
PS C:\Tools> .\LECmd.exe -f 'C:\Users\eric\Desktop\X-Ways Forensics 32-bit.lnk'
LECmd version 1.0.0.0

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

Command line: -f C:\Users\eric\Desktop\X-Ways Forensics 32-bit.lnk

Warning: Administrator privileges not found!

Processing 'C:\Users\eric\Desktop\X-Ways Forensics 32-bit.lnk'

Source file: C:\Users\eric\Desktop\X-Ways Forensics 32-bit.lnk
  Source created:  2018-07-14 15:32:58
  Source modified: 2018-07-25 23:06:07
  Source accessed: 2018-07-14 15:32:58

--- Header ---
  Target created:  2018-07-14 15:32:53
  Target modified: 2018-07-11 23:06:02
  Target accessed: 2018-07-14 15:32:53

  File size: 4,133,544
  Flags: HasTargetIdList, HasLinkInfo, HasName, HasRelativePath, IsUnicode, RunAsUser
  File attributes: FileAttributeArchive
  Icon index: 0
  Show window: SwNormal (Activates and displays the window. The window is restored to its original siz
e and position if the window is minimized or maximized.)

Name: X-Ways Forensics 32-bit
Relative Path: ..\..\..\xwf\xwforensics.exe

--- Link information ---
Flags: VolumeIdAndLocalBasePath

>>Volume information
  Drive type: Fixed storage media (Hard drive)
  Serial number: 1ED165D7
  Label: CDrive_512GBM2)
  Local path: C:\xwf\xwforensics.exe

--- Target ID information (Format: Type ==> Value) ---

  Absolute path: My Computer\C:\xwf\xwforensics.exe

  -Root folder: GUID ==> My Computer

  -Drive letter ==> C:
```

The map!

- Rather than concern yourself with lists of things like the following:
  - Open/save MRU, email attachments, ADS Zone.Identifer, UserAssist, Last Visited MRU, AppCompatCache, Amcache.hve, BAM/DAM, RecentDocs, WordWheelQuery, thumbs.db, Thumbscache, recyclebin, file://, Network history, timezone, cookies, browser search terms, first and last insertion times, volume serial numbers, PnP events, last login, login types, service events, scheduled tasks, browser cache, flash cookies…..
- Focus on a higher level story that provides what you need to prove your case…

The map: some examples

- I need account usage history showing any external devices that were used in conjunction with files and folders that were opened that shows which accounts accessed the intellectual property in question.
- What evidence of execution artifacts are there that show files being downloaded and browser usage between September and December of last year?
- Does proof exist that the user 'Steve' accessed files or folders and subsequently deleted any files that were accessed?
- What user was signed into a laptop on the night of January first and where was it located at the time? What programs were used?

Why take this approach?

- Computer forensics is a vastly complex and technical discipline and forensic examiners have a wide range of experience and skills
- By focusing on the category vs a specific artifact in the category, it allows freedom to an examiner to look for a wider range of artifacts in a given category vs. only the one you specified
- Different artifacts yield different information. By combining the information available in several artifacts from a given category, a more complete and accurate understanding of the facts is possible
- It makes both your life AND the forensic examiner's much easier!


Questions