DFIR

FILE SYSTEM FORENSICS

DEV DUA (@dev0x01)

>> whois Dev.Dua

```
# Star Wars fan, clearly.
# M.Eng. Cybersecurity
# JOATMON –
      Full Stack Developer,
      Security Engineer,
      Scripting/Automation,
      Researcher
# Twitter: dev0x01
# Web: code.devdua.me
```

Famous case - BTK Killer

“BTK” Serial Killer – Denis Rader, on the run for more than 30 years,

Last victim – Kansas, U.S.A.

Downfall –

- He sent a floppy disk to the police with a letter on it.
- Upon forensic investigation, the investigators found a deleted Microsoft Word file.
- The metadata recovered showed that the last person to edit the file was authored by “Dennis”
- The disk had been used to take printouts at a church

Ironically, Rader had sent a floppy disk to the police because the police had previously told him that letters on floppy disks could not be traced.

Locard's Exchange Principle

"A criminal is always going to bring something to and leave something from a crime scene."

What will be covered

Static!

+DFIR Process
+Forensic Data Acquisition & Imaging
+Analysis of Forensic Images
+File Carving

What's DFIR?

DF | IR

The process of digital forensics can be broken down into three categories of activity: *acquisition*, *analysis*, and *presentation*.

Evidence data acquired must be preserved in a way to be presented in a court of law.

Tools should preserve this data as well as attached metadata

No one should be able to challenge the data collected

DFIR Process

Acquisition

- collection of digital media to be examined.
- Depending on the type of examination, media could be physical or digital.
- Media to be examined should be treated delicately. At a minimum the acquisition process should consist of
  - creating a duplicate of the original media (more on this later)
  - maintaining good records of all actions taken with any original media.


ONE DOES NOT
SIMPLY
PUSH THE "FIND EVIDENCE"
BUTTON

DFIR Process

Analysis

- Examination of the acquired media examination - “identification, analysis, and interpretation”
- Identification consists of locating items or items present in the media in question and then further reducing this set to items or artifacts of interest.
- These items are then subjected to the appropriate analysis
- Finally, the examiner interprets results of this analysis


ONE DOES NOT
SIMPLY
PUSH THE "FIND EVIDENCE"
BUTTON

DFIR Process

Presentation

refers to the process by which the examiner shares results of the analysis phase with the interested party or parties.

This consists of generating a report of

- actions taken by the examiner,
- artifacts uncovered,
- meaning of those artifacts.

The presentation phase can also include the examiner defending these findings under challenge (in court)

Data Acquisition & Imaging

Media types

Typical media collected during an investigation-

+ Hard drives (internal and external)
+ Optical discs (DVDs, CDs, etc)
+ Removable media (USB keys, SD cards, Compact Flash, etc)
+ Mobile devices (phones, tablets)

Forensic Investigation 101

Forensics should NOT be performed on the actual copy of the data – puts evidence at risk.

A bit-for-bit copy of the media must be created and used for the investigation.

Why?

- Digital evidence is very volatile, accidents can lead to permanent data loss.
- By performing forensic analysis on a clone, you give yourself an option to start over if things go awry.

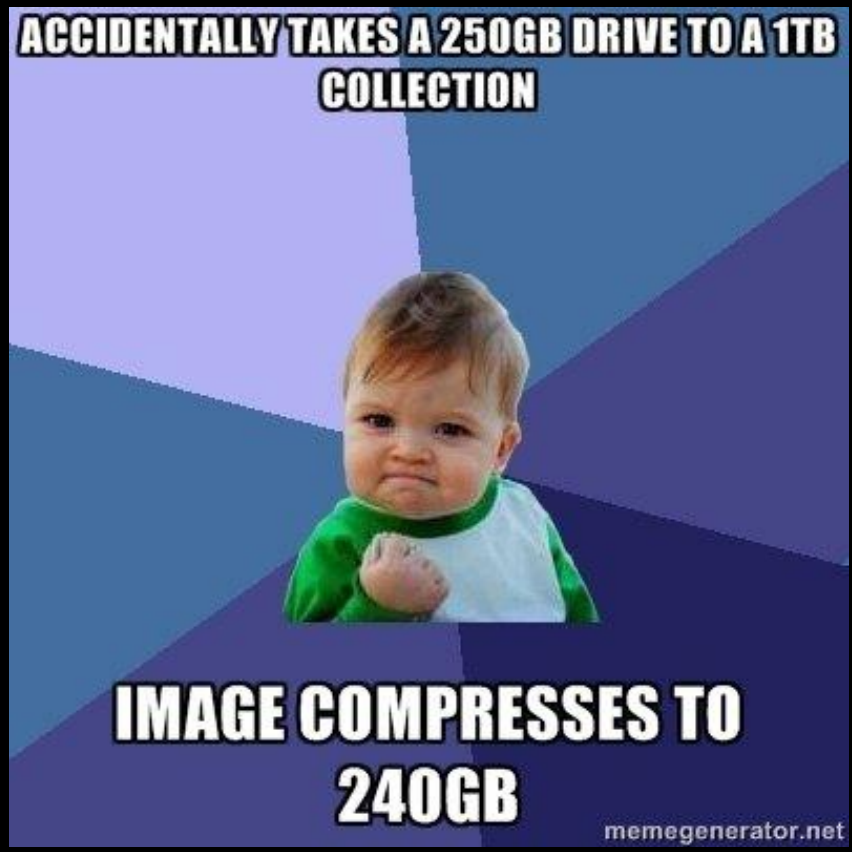
Cloning Process

Copy from the source drive (drive you want to make a copy of) to a destination drive/space.

Destination drive needs to be at least as large as the source drive

Typically the drive to be cloned is removed from the system and attached to a hardware cloning device or another computer

Some kind of write-blocking device must be put into place before cloning! (Often built into most hardware cloners)



Forensic Duplication

- The tool must create a forensic duplicate or mirror image of the original storage medium.
- The tool must handle read errors in a robust and graceful manner. The tool must not make any changes to the source medium.
- The tool must have the ability to be held up to scientific and peer review. Results must be repeatable and verifiable by a third party, if necessary.

Imaging tools

- dd - linux imaging tool
- dc3dd - dd with features: on-the-fly hashing, progress meter, split output files
- dcfldd – similar to dc3dd but developed as a fork of dd
- Guymager -Linux-based tool with GUI interface
- Helix3 – Bootable image, commercial
- FTK Imager – commercial

Imaging tool: dd

```
dd if=IFILE of=OFILE [options]
```

options:

- bs = block size - set block size
- count=NUM - copy only NUM blocks from IFILE
- skip=NUM - skip ahead NUM blocks in input IFILE
- conv=noerror, sync - skip unreadable sections (very important for forensic imaging)

Imaging tool: dd

```
dd if=/dev/sda1 of=/mnt/usb/sda.img bs=1M count=700
conv=noerror,sync
```

- Input file = /dev/sda1 (first partition on the sda device)
- Output file = /mnt/usb/sda.img (sda.img file on the mounted USB drive)
- bs = 1M block size
- count = only copy the first 700 Blocks (700MB here)
- noerror = continue on errors
- sync= use synchronized I/O for data and metadata

Example -

```
dd if=/dev/sdb of=sdb_image.img bs=65536 conv=noerror,sync
```

Imaging tool: dcfldd

```
dcfldd
\     if=/dev/zero of=zero.img
\     hash=md5,sha256 hashwindow=256M
\     md5log=md5.txt sha256log=sha256.txt
\     bs=8k conv=noerror,sync
\     split=256M
```

Imaging tool: dc3dd

REMOTE ACQUISITION

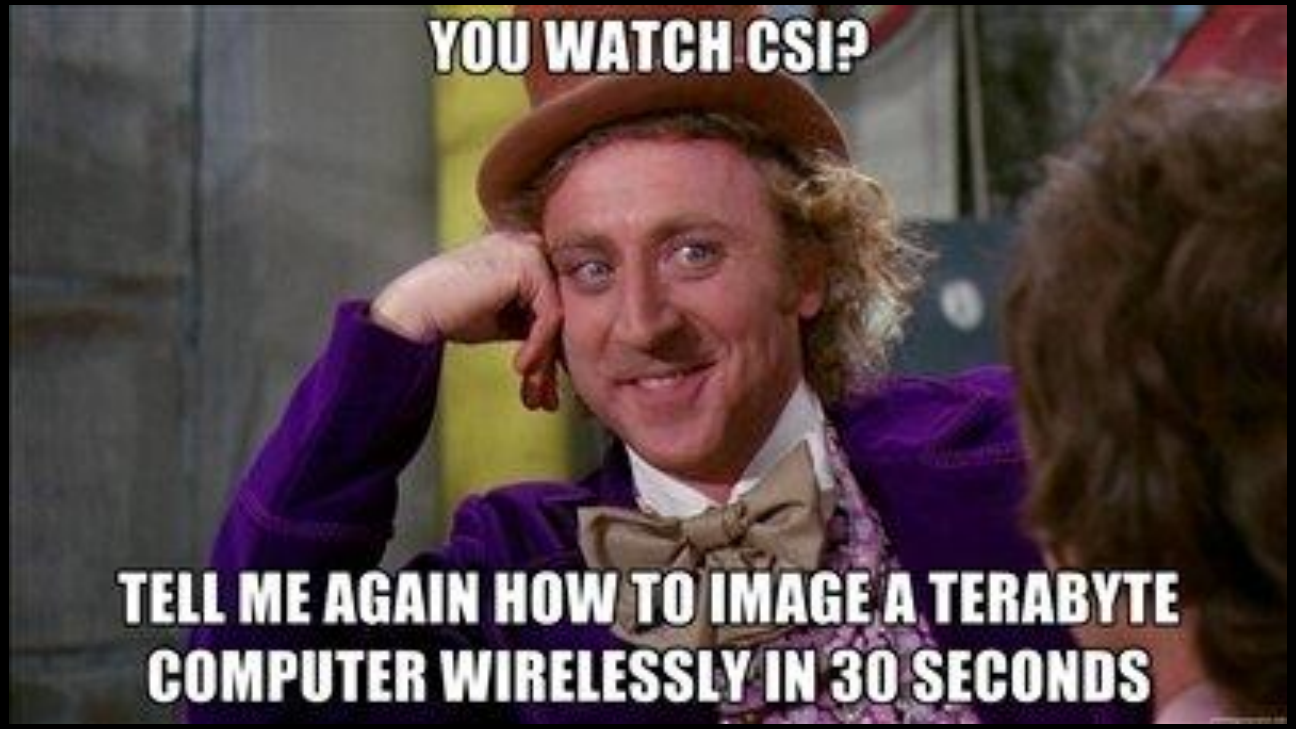
```
dc3dd if=/dev/sda1 hash=md5 progress=on | ./nc
192.168.1.3 12345 -w 3
```

```
nc –l –p 12345
```

```
ssh dev@192.168.72.142 "dd if=~/remote_test.img " |
dc3dd hofs=secPG/remote_test_copy.img.0 ofsz=256M
hash=md5 hash=sha1 verb=on hlog=secPG/remote-acq-
hash.log
```

Remote Acquisition

It’s better to image over wire compared to the remote method.



DEMO

Analysis of Forensic Images

DEV DUA (@dev0x01)

Analysis

Probably the longest step – The analyst must use their skills, experience, and tools to local and interpret artifacts found on the images they analyze.

During this phase they should take copious notes of every so you/someone else can repeat those steps and find the same results.

Verifiability.

How to Analyze?

- Linking activity to a specific person/user, Identify relationships between people
- Establish a timeline of events
- Recovering deleted files
- Determining if a system was compromised
- Identifying websites visited/search engine queries
- Determining if/when files were accessed or modified
- Check for
  - hidden or unusual files
  - unusual processes and open sockets
  - unusual application requests
  - suspicious accounts

Types of Data

- Active – Data we use every day, typical file can be viewed on the computer. Easy to acquire forensically.
- Latent – Data that has been deleted or partially overwritten. Needs to be acquired with forensic tools.
- Archival – Backups of data that was active at some point. Acquisition can be easy to near impossible.

File Systems

The File System keeps track of the files and directories on a computer, their location (physically and logically), as well as the free space (unallocated space)

Most common:

- FAT
- NTFS
- HFS+
- ext2/3/4

Sleuth Kit

File System Forensics framework

20+ command line utilities

Includes tools that operate on –

- volumes (aka “media management”),
- file system structures,
- data unit (or “block”) layer,
- metadata (or “inode”) layer,
- file name layer

…

[SK] - Volume Layer Tools

mmstat command will display the type of volume system in use on the target image file or disk

mmls - parses and displays the media management structures on the image file or disk (i.e., the partition table)

```
>> mmls 10-ntfs-autodetect/10-ntfs-disk.dd
```

mmcat streams the content of the specified volume to STDOUT (usually the console).

[SK] - File System Layer Tools

fsstat command displays file system information - volume names, data unit sizes, and statistical information about the state of the file system.

```
>> fsstat ubnist1.casper-rw.gen3.E01
```

Note that this tool provides the block size used on the file system. This is important information when carving data from unallocated space.

[SK] - Data Unit Layer Tools

blkstat command displays information about a specific data unit (allocation status)

```
>> blkstat ubnist1.casper-rw.gen3.E01 521
```

blkls command lists details about data units. Blkls can also be used to extract all unallocated space of the file system.

```
>> blkls ubnist1.casper-rw.gen3.E01 > ubnist1.
casper-rw.gen3.unalloc
```

[SK] - Data Unit Layer Tools

blkcat command will stream the content of a given data unit to STDOUT. This is similar in effect to using dd to read and write a specific block.

```
>> blkcat ubnist1.casper-rw.gen3.E01 521 | xxd | head
```

[SK] - File Name Layer Tools

fls command lists file names (deleted and allocated).

```
>> fls ubnist1.casper-rw.gen3.E01
```

The **ffind** command finds file names that reference the provided metadata number (inode).

```
>> ffind ubnist1.casper-rw.gen3.E01 19
```

Autopsy

Digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools.

Autopsy was designed to be an end-to-end platform with modules that come with it out of the box.

Features → Timeline Analysis, Hash Filtering, Keyword Search, Web Artifacts, Data Carving, Multimedia, Indicators of Compromise

DEMO

File Carving

Carving

Involves searching a data stream for

- file headers and magic values
- determining (or guessing) the file end point
- saving this sub-stream out into a carved file

Popular tools – foremost, scalpel, bulk_extractor

foremost/scalpel

Foremost is a Linux based program data for recovering deleted files and served as the basis for the more modern Scalpel.

The program uses a configuration file to specify headers and footers to search for.

foremost can search through most any kind of data without worrying about the format.

Scalpel can also extract pcap files.

bulk_extractor

Swiss Knife!

Bulk Extractor is a forensics tool that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures

By default it doesn’t carve files, carving mode needs to be specifically mentioned in the command line arguments.

Comparison of tools

- Scalpel returns more files than Foremost
- Unfortunately, the filenames returned by both tools are not the original filenames
- There may be duplicates of carved files as many files may be fragmented and appear to be separate files.
- bulk_extractor is a handy tool for analysis of an image, but scalpel is more useful for carving.

DEMO

Thanks!

Sources –

SANS, Infosec Institute, Forensics Wiki, Usage documentation of tools discussed

Memes courtesy @DFIRmemes