Evidence Analysis

Digital Forensics

Typical Investigation Sequence

- Record case info, document evidence custody
- Identify partitions and filesystems of interest
- Import filesystem images into forensic software
- Locate files and folders which may be of interest and tag them
- Identify deleted files and folders which may be recoverable and interesting and recover them

Locating Interesting Files

- Use signature analysis to identify files that do not open properly
- Find encrypted files and attempt to decrypt
- Perform keyword searches for names, addresses, phone numbers, email addresses, social media handles, investigation-specific words or phrases (requires topic knowledge)
- Identify unusual files which may require carving (files that are bigger than they should be, files that are mis-named, binary files that match keyword searches, etc.)

https://xkcd.com/208/

Direct Evidence

- Files which contain evidence can be produced by any application
- Common data files with direct evidence:
  - Photos or other images
  - Videos
  - Other multimedia such as audio
  - Documents
  - Emails or social media records
  - Cracked software or installed malware

Supporting Evidence

- It can be very helpful for investigators trying to connect evidence to persons if you can build a more complete picture of the use of the computer around the time of the situation being investigated
- Files which are useful for building context:
  - Social media records and logs
  - Email and web history
  - Contact lists
  - Bookmarks and shortcuts both in apps such as browsers, and in the filesystem as links
  - Recycle bin contents or history
  - Breadcrumbs like thumbnails, indexes
  - Installed software and custom scripts and programs

Digging Deeper

- A file may not always contain what it appears to contain
- It may be misnamed to make it harder to find or notice (e.g. BirthdayPartyInvite.docx might be the name of a file that contains a document having nothing to do with birthday parties)
- It may have extra information beyond the obvious that turns out to be useful (e.g. BirthdayPartyInvite.docx might describe an uninteresting event, but may show that John Badguy knew Sally Succubus and contain her contact information)
- It may be useful for building a timeline of events involving people (e.g. a log file showing Mike Miscreant logging on with his password at 3:05AM, with no-one else logged on, shortly before the company sales forecast was exfiltrated interactively by email, despite the email account belonging to someone other than Mike)
- It may also be that BirthdayPartyInvite.docx isn't even a word document, see Corrupt File Forensics for a real-life example

Signature Analysis

- Signature Analysis means looking at file content to determine what kind of file you have
- A bad signature is when a filename looks recognizable, but file header is not any known file type, sometimes this is called a bad tag
- Files whose name does not match their file header are sometimes called aliases, terrible name, they are simply misnamed, sometimes on purpose
- Use Open with… or rename the file to open a file with a correct and valid signature using the intended application
- Unknown files without a recognized name or signature can be investigated with a binary file viewer and a resource like filesignatures.net to try to identify files, beware of header offsets or padding being used to prevent automatic file identification
- The Linux file command does signature-based analysis of files, most forensic analysis programs take signatures into account when identifying files
- See UCF File Carving video series part 1 for a detailed discussion with examples of signature analysis

Encrypted Files

- Encrypted files present extra challenges
- Some applications can encrypt their data files
- Encryption utilities which can be used to encrypt files no matter where they came from
- A filesystem may be encrypted in full
- Encryption can be done using hardware devices embedded in drives, such as USB sticks and external drives

Recognizing Encrypted Files

- Encryption is often encountered in both corporate and criminal investigations
- Encrypted files can have a signature if they are written by an application that does uses its own builtin encryption such as zip, rar, vi, gpg, ssl, cryptfs, veracrypt, office productivity programs, and malware (Methods for detecting ransomware activity article on netfort.com has a list of known extensions for ransomware encryption programs)
- A file with an invalid signature may be an indication that you have an encrypted file
- Encrypted whole filesystems can sometimes be recognized (e.g. with Encrypted disk detector tool from Magnet Forensics)
- You can use the cipher /u /n DOS command to find files Windows recognizes as encrypted
- Otherwise, you won't know a file is encrypted unless opening it causes it to request a password, entropy analysis isn't conclusive

Accessing Encrypted Data

- In corporate investigations, IT can often provide the necessary recovery keys for encrypted company devices
- Users tend to use a small number of passwords with very little variation in them repeatedly, so trying common (e.g. first name, last name, birthdate, family/pet names, etc.) or known passwords (from other apps or sites) for users can sometimes work
- Many users use password managers which are increasingly backed up to the cloud especially with mobile device apps, and password databases can sometimes be obtained through those channels
- Messaging app caches and logs may contain passwords a suspect sent to others, these can be gathered from other devices belonging to the suspect
- Various password cracking programs can be tried, depending on what you are trying to decrypt
- There are public databases of stolen/cracked passwords
- You can always try the $5 wrench (metaphorically of course)

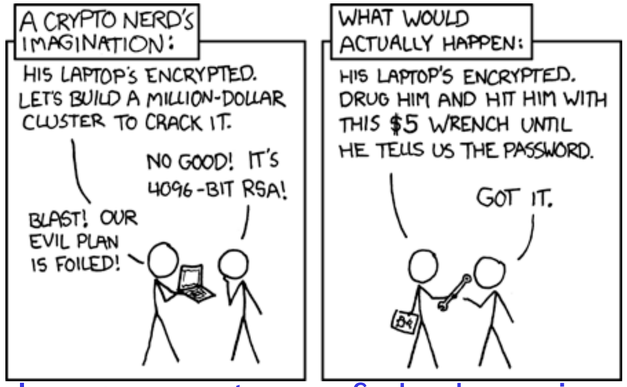

Image courtesy of xkcd comics

Keyword Searching

- All forensic software provides a way to search for keywords in allocated files, as well as unallocated files
- Not all forensic software properly finds unallocated files, so some can be missed, see Paper comparing some popular graphical forensic analysis tools for examples of the differences in results from otherwise respected programs
- To make definitive statements about whether keywords are present as unencrypted clear text in an image, directly search the image file using a tool like grep at the command line
- The hardest part of keyword searching isn't the search commands, it is knowing what to search for, which requires domain knowledge

Obfuscated Files

- Similar to encryption, files can have their contents obfuscated to make it harder to search, view, and use them
- There are many ways to transform a file's contents to make them difficult to use, ciphers do not have to be complex to be effective
- Consider swapping every four bits in a file, the resulting bytes will not look anything like the original when viewed in the original application
- winhex and tools like it can be used to transform file data using methods like rotate file bits, swap them, shift them, add offsets, etc.
- See UCF File Carving video series part 2 and UCF File Carving video series part 3 for examples

Hiding Places

- In addition to files having their names changed, their contents transformed or obfuscated or encrypted, and files deleted or media formatted, there are places where serious bad guys can put the files to try to escape your notice - this is very uncommon
- Raw disk - partitions with no filesystem, or unmounted filesystems - use fdisk or lsblk to find them and mount to see if any of their partitions are currently mounted, don't forget they may be metadisk components (RAID or LVM or ZFS, etc.)
- HPA - use hdparm to access this space
- File-based filesystems - search for these with file and other similar tools
- Inode 1 - the bad blocks list - view with dumpe2fs -b or filesystem analyzer

Hiding Places

- File slack - space from logical end of file and actual end of file on disk - examine using grep or winhex
- Unallocated filesystem blocks - space which may or may not have been used since filesystem creation - examine using foremost
- Commercial forensic applications with graphical interfaces are great tools for searching unallocated space but remember they vary in effectiveness and you cannot know if they did not find something due to it not being there or due to shortcomings in the software
- Sometimes hardware implementations do the hiding unintentionally, see Digital forensics truths that turn out to be wrong on youtube for a very interesting video on how data can sometimes be recovered even when the hardware device is trying to not let you get at it

Report Creation

- The summary report for an investigation describes what was searched, what was found, and documents how these things were done for credibility
- It should describe what equipment was seized and imaged, and the complete chain of custody for those items (i.e. a full description of how every item was acquired, handled, stored, and verified at every step of the process)
- It should describe what was on that equipment, both in general terms, and as a specific list of items of relevance to the investigation you are doing or supporting
- It should describe any steps which were taken to recover information that did not simply involve use of programs, such as obtaining passwords or using online resources
- Forensics Report Writing on youtube has an explanation of a formal report writing method employed by the FBI, Reporting for Digital Forensics has an overview of elements to consider when writing reports for use in court (USA-specific)