98-212

"Forensics" & Steganography

Administrivia

- Check your email

What *is* computer forensics?

- Collecting "evidence" from a computer
    - usually: image disks, hash & verify
    - Look for photos, *passwords*, web history, etc
- Incident response
    - Once a machine is attacked, reconstructing what happened

So, just looking around in a file browser?

No!

What makes forensics hard

- What if things are encrypted?
  - If encryption is done correctly, there is *no way* to get the data
  - A lot (a *lot*) of people don't encrypt correctly
    - or don't encrypt at all
- What if things are hidden?

CTF Forensics

- "Real-world" forensics is mostly concerned with legalities
  - How to extract data while still being able to prove you haven't tampered with it - otherwise inadmissible in court
- Legal stuff involves a lot of paperwork
- We don't like paperwork

CTF Forensics

- CTF forensics is more of the form:
  - Here is a file (or a bunch of files)
  - There is something here you are supposed to find
- Almost like a scavenger hunt, but with files and crypto instead of parks and fences
- The techniques, however, are often *exactly the same*
  - Well, once you have the data off the physical disk anyway

CTF Forensics

- Forensics also has the dubious honor of containing an infamous sub-category...

Steganography

Wikipedia:

"The art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message."

Steganography

- Basic premise:
  - Encrypted data is *suspicious* and attracts attention
    - People don't usually send each other completely random bytes
  - Use seemingly innocuous data to hide what you are really sending
- This is a form of security by obscurity!

Stego: "Common" Implementation

- Pictures are completely normal things to send each other, right?
    - How are pictures encoded?
    - Are there bits we can "hijack?"

Let's do an example! (or two)

Does anyone actually do this?

- Supposedly, yes
  - Al-Qaeda
  - Allegedly, Russia's SVR (a.k.a. Russian CIA)
- But real-world stego is hard to detect
  - Hidden data is usually encrypted
  - They are usually more clever than what we just showed you

Other Simple Forensics

- Given a copy of a file system, find "suspicious" web history
  - Where do browsers keep their data?
    - Does this vary by system?
- Given a copy of a file system, find a certain user's password
  - How do operating systems protect user passwords?
- Given some keylogger output, find a given password

A "simple" example

Hard Drive Data

- What happens when you delete a file?
- ... well....
- that depends on what you mean by delete!
  - Windows: move to recycle bin? "hard-delete"?
  - Linux: rm -f? dd -if /dev/null -of file?
  - OSX: any of the above?

Hard Drive Data

- Do any of these actually get rid of your data?
  - For all but one, no!
- Why would the hard drive waste precious I/O time deleting data when your filesystem can just forget that it assigned meaning to those bytes?

Hard Drive Data

- If I overwrite a file, I'm clear though, right?
  - Not necessarily!
  - Anyone ever heard the word "defragment?"

Hard Drive Data

- Wait, but if the metadata's gone, how do we know which data is with?
    - *File carving*
        - *"the process of reassembling computer files in the absence of filesystem metadata"* -- Wikipedia
        - Most filesystems fragment in a consistent and known way
        - File carving is a target of a lot of research!
            - "Forensically important" files (e.g. word documents, email logs, browser history) fragment often

Hard Drive Data

- If the system crashes while I'm writing stuff to the disk, is *that* recoverable?
    - maybe
        - Many filesystems now are *journaling*

Hard Drive Data

- So... how do we actually *do* the recovery?
    - General forensics tools
        - Autopsy/SleuthKit
    - File carvers
        - eg `scalpel`
    - Semi-manually
        - hex editors (eg 010)
        - programs that understand a lot of formats (eg `hachoir`)

Autopsy

- Tyler promised me he would have autopsy working by today...