Data Recovery

By Aya the Awesome

DISCLAIMER

I'm going to be talking about how to recover data. This does ***NOT*** mean I think you should never back up your data anymore! Please please please please ***pleeeeaase*** keep back ups because when you accidentally encrypt your entire hard drive instead of your flash drive, there will be no forensic tool on Earth that can help you.

Why Need Recover Data?

- Common reasons
  - human oopsies (accidentally delete/modify data)
  - malware
  - power loss during write to disk
- Built-in OS tools
  - fsck for Unix-like system
  - CHKDSK for Windows
- May get more advanced if doing forensic analysis

Let's talk about deleting

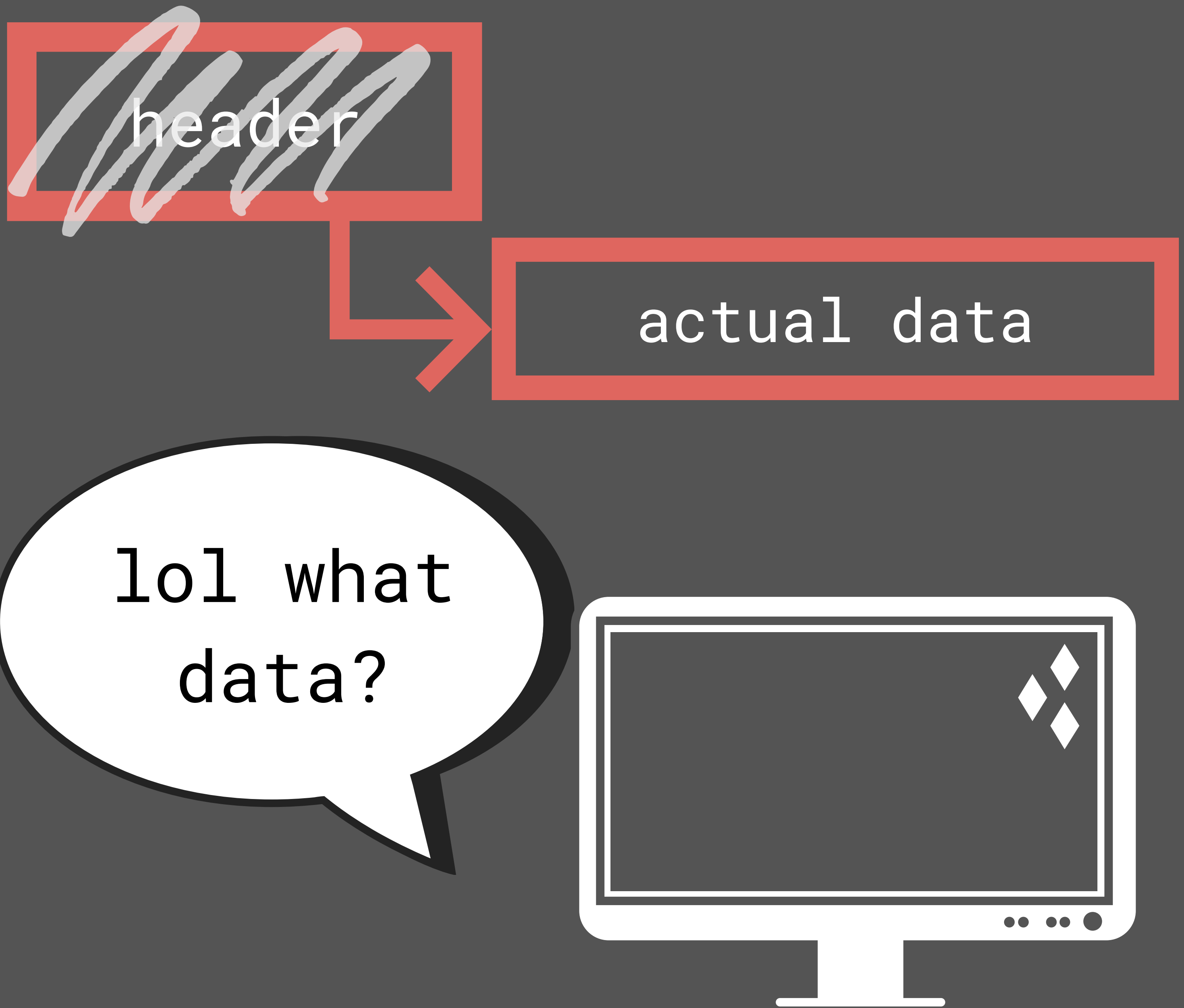
So before we talk about recovery, let's go over deleting a bit...

- It's easy to *say* data has been deleted
  - Just remove a reference to the data
- Much harder to delete a way that's not recoverable
  - With enough analysis, you can guess what used to/should be there

Typical Deletion

What you see

What actually happens



header

actual data

lol what data?

So, that was unimpressive....

Gotta up our game

- Clearing: prevent recovery w/ software
- Purging: prevent recovery w/ lab equipment
- Could just physically destroy the drive
  - low key extra dough
  - Google does this, not normies
- Nomies' approach: data sanitation
  - overwriting data
  - clears and purges (if you do it right)

Old Hard Drive

- Let's overwrite whole thing with 0x00!
- Is this enough?
    - Maybe
- General consensus is 1-3 passes is enough

Old Phone

- Let's try the same thing!
- Is this enough?
    - Uhh...maybe
    - Harder to do it right
- Cuz solid state drive
    - Harder to physically destroy
    - Need special commands to erase *all* of disk
    - Multiple passes wear down and reduce lifetime

So...what?

- It's hard to *really* delete data
- Means that data recovery is usually possible
- Again, *pleeeaaaasseeee* don't take this to mean you don't need backups!

How to Recover Data

Tools + Strategies

- General strategy (🕵️‍♀️ = probs not need do in ctf)
  - 🕵️‍♀️ Reduce search space
  - You figure out what the problem is
    - (you = general-purpose tool)
  - Find appropriate tool to fix it
  - Undelete, then uncorrupt
  - 🕵️‍♀️ Remove any bad/corrupted data couldn't fix

- For proper tool, wanna consider
  - Extent of deletion/corruption
  - Size of data and extent of recovery
  - File system

Some Free & Open-Sourced Tools

THE SLEUTH KIT (TSK)

Uses: generally very versatile library for disk analysis and data recovery. Even if you can't recover the data fully using this, great tool to get started and do general analysis.

AUTOPSY

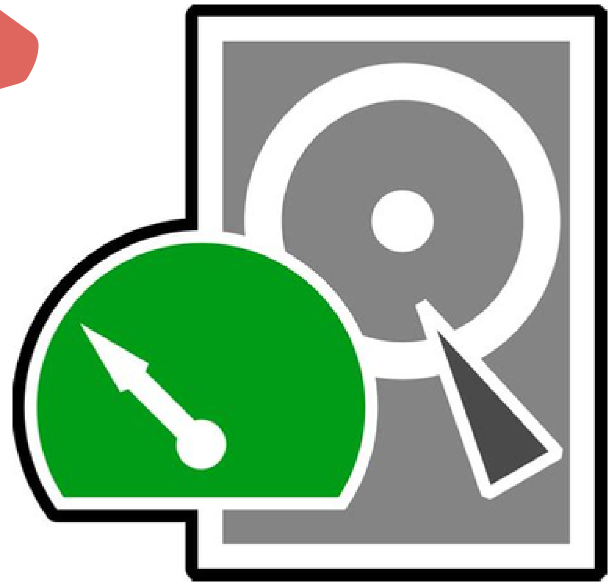
Uses: GUI-program that uses TSK in the backend

GENERAL PURPOSE ONES

I'd recommend starting off with these to get a preliminary idea of what needs to be done

TESTDISK

Uses: heavy emphasis on partition tables (recover lost/corrupted partition, fix partition table), rebuild boot sector, some file recovery (extent of recovery it can do will depend on file system)



EXTUNDELETE

Uses: recovering deleted file on ext3 and ext4 file systems

BINWALK

Uses: searches for embedded files. May not recover file content, but it will tell you what files used to be there/are hidden there

MORE SPECIALIZED TOOLS

Usually your more general-purpose tools will be enough for a CTF problem, but if you do run into the limitations of a tool, you may need to look for something more niche.

Pop Quiz!

Keeping back ups of data is only for noobs who don't know about data recovery.

True

or

False?

Psssst! Here's a hint: the answer is FALSE!

Questions?