How to collect evidence?

- If the system is up:
  - Should we turn the compromised system off?
  - What if we gracefully shutdown the system?
    - Intruders may rig systems
      - Delete some / all files on system on graceful shutdown

- Shutdown flushes buffers, ensures all info is written to disk, users are notified, services are cleanly shutdown, etc.

Turn the compromised system off and take out the hard drive?

- To prevent damage from "rigging", often best to yank the power cord.
  - NOTE: You'll lose data !

- With time, smarter hard drives will be available:

- At least one hard drive product available today is marketed with a capability to wipe itself if removed from its native location and connected elsewhere, such as to a write-blocking device.
- This means the hard drive should remain connected inside the compromised system.
- This makes live incident response and evidence collection very important.

Loss of volatile data when system is turned off

- System date and time
- A list of the users who are currently logged on
- Open files
- A list of currently running processes
- A list of currently open sockets
- The applications listening on open sockets
- A list of the systems that have current or had recent connections to the system

Volatile Evidence

- most volatile -> least volatile
  - Memory
    - Kernel / user
  - Swap Space or Pagefile
  - Network status and Connections
  - Processes running
  - File opening
  - Hard Drive media
  - Removable Media (Floppy, Zip)