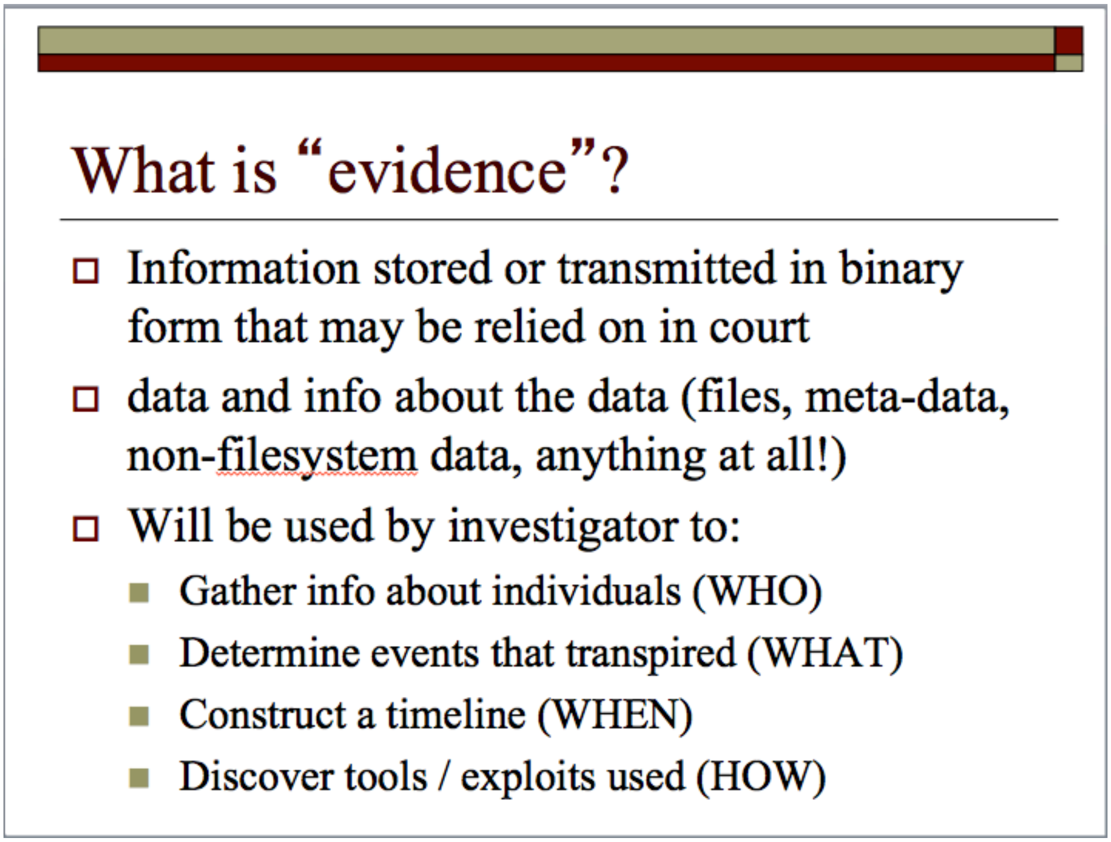
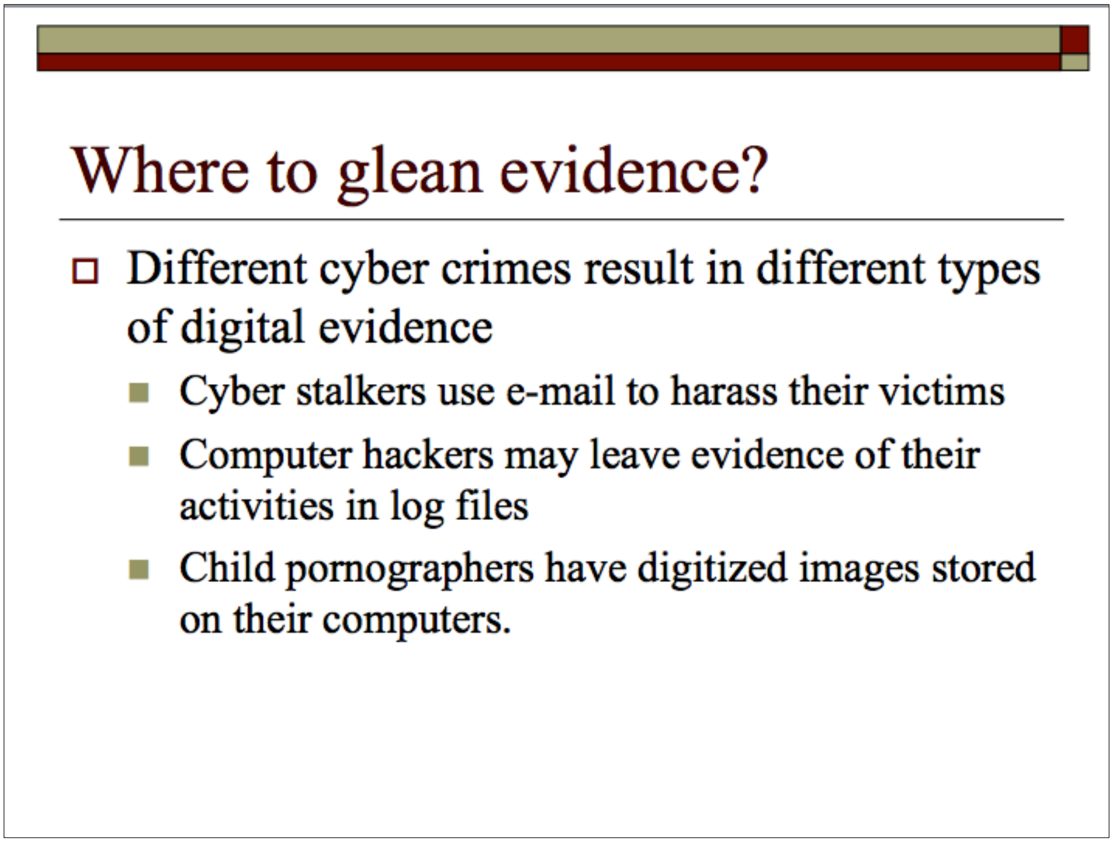


What is "evidence"?

- Information stored or transmitted in binary form that may be relied on in court
- data and info about the data (files, meta-data, non-filesystem data, anything at all!)
- Will be used by investigator to:
  - Gather info about individuals (WHO)
  - Determine events that transpired (WHAT)
  - Construct a timeline (WHEN)
  - Discover tools / exploits used (HOW)



Where to glean evidence?

- Different cyber crimes result in different types of digital evidence
  - Cyber stalkers use e-mail to harass their victims
  - Computer hackers may leave evidence of their activities in log files
  - Child pornographers have digitized images stored on their computers.

Where to glean evidence? (Con’ t)

- Network based information
- Internet and cloud forensics
  - Bruce Nikkel's *Domain Name Forensics: A Systematic Approach to Investigating an Internet Presence*
  - Cloud Computing: Another Digital forensics challenge
- Host based information
  - Volatile data and Nonvolatile data
  - RAM, Hard drive, compact disks, floppy disks, magnetic tapes, zip and jazz disks, log files,…, etc
- Others
  - Removable devices, Interview people, etc