SY110
Forensics

Major Brian Hawkins, USMC

U.S. Naval Academy

Fall AY 2018

Outline

Review

Admin

- Tomorrow/Tuesday: Lecture at 1200 in Alumni Hall
- Friday: no Class

Modern Day Crypto Tools

- AES - Strong (& Fast) Symmetric Encryption (128-bit key)
- Use a Hash algorithm to produce key for AES
- RSA - Assymetric encryption is SLOW!
  - So, sign the hash(file) instead of the entire file.
  - Use Assymetric encyption initially to exchange a 128-bit key and then switch to AES.

Forensics

Regular-old forensics

Analyzing a crime scene for traces of hair, fingerprints, *etc*.

Computer Forensics

Applying the scientific method to reconstruct a sequence of events involving computers and data. Figuring out *after the fact* what has occurred on an information system.

Forensics

Regular-old forensics

Analyzing a crime scene for traces of hair, fingerprints, *etc*.

Computer Forensics

Applying the scientific method to reconstruct a sequence of events involving computers and data. Figuring out *after the fact* what has occurred on an information system.

Locard's Exchange Principle

Fancy-pants name for how perpetrators of a crime:

- *leave* evidence of their presence at the scene
- *take* something from the scene with them

This is true in computing, even when we're not committing a crime

Examples

What traces do we leave? What do we take with us?

- Visiting a website?
- Our message board injection attack?
- Man-in-the-middle demonstration?
- Login attempts?
- Shell command histories?

Demos

Demos

- Web Cache - Open ChromeCacheView.exe
- Meta Data - unimportant.docx
- File Access & Registry - regedit

Questions

Questions?