Adventures with FTK (and other forensics tales)

Daniel Schwalbe

NWACC Security Workshop 2015

Computer Forensics

- The application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

- The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Why Forensics?

- What happened?
- When did it happen?
- Who did it?
- What did they do?
- Where else did they go?

Criminal vs. Civil vs. Internal

- The reason for doing forensics will often determine the technique
- Chain of custody
- Evidence integrity
- Reporting

Forensics on what?

- Hard Drive
- Thumb Drive
- Mobile Phone
- Any electronic media
- Logs
- Emails
- Digital Files

Software Options

- EnCase
- FTK
- Sleuth Kit / Autopsy
- Volatility
- ‘dd’
- Various Live CDs

DEMO TIME

QUESTIONS ?

Thank You !

dfs@uw.edu

http://ciso.washington.edu