COMP 2555 Principles of Computer Forensics

Lecture 10

Ramki Thurimella, PhD

University of Denver

Overview

- Project 2 discussion
- Review commands from pp. 142—153, the rest of Module 3 of CERT Book
- Midterm review

Before the test

- Make sure you have an account on our UNIX lab
- Two parts:
  - First part: 30 short questions, each worth ½ point (closed book)
  - Second part: 5 exercises (use the lab machines to answer), each worth 2 points
- Become familiar with ls, grep, diff on Linux and dir, netstat on

Announcements

- May 6th—forensics practitioner from Lucidata
- Submit questions for Jeremy
  - Physical damage
  - Most interesting case (typical cases)
  - Technology that you come across
  - Flash drives, solid state drives
  - Toolset
  - Live system forensic analysis
  - Business model for forensic companies
  - As part of investigation, what happens if
    - See pirated software, music
    - Illegal activity taking using the machine
    - Where are your loyalties?
    - Do you sign consent not to disclose
- CANVAS (again) on May 4th