CIS 283F : PRACTICAL DIGITAL FORENSICS

Transcript title
Practical Digital Forensics

Credits
4

Grading mode
Standard letter grades

Total contact hours
50

Lecture hours
30

Other hours
20

Course Description
Presents digital forensics instruction from a systems security perspective. Students participating in this intermediate-level class will use a variety of digital forensics tools and software; and are exposed to drive image making, investigations of files and documents, and working with various PC and mobile device hardware. Investigative techniques practiced in this class are performed in a secure environment.

Course learning outcomes
1. Analyze various cases to determine digital actions of a user.
2. Compare and contrast analysis differences between common computer operating systems.
3. Demonstrate analysis techniques to open SAM, SYSTEM and SECURITY files.
4. Demonstrate the creation of a digital image of a physical storage device.
5. Describe appropriate evidence handling process.
6. Describe how analysis of computer logs demonstrate attribution.
7. Describe various laws affecting the pursuance of a forensic analysis.
8. Explain how deleted digital information can be recovered.
9. Using an existing report template, write a report of an analysis of digital evidence for a case.
10. Using common digital forensics tools, demonstrate the technique for locating a variety of file types.

Content outline
1. User actions:
   a. Evidential
   b. Non-evidential
2. Operating Systems differences for forensic analysis Windows, MacOS, Linux
3. File Types:
   a. SAM file types
   b. SYSTEM files and
   c. SECURITY files including logs
4. Different digital images on physical storage devices:
   a. jpg
   b. png
   c. gnu
   d. mov
5. Evidence handling processes
   a. Digital evidence
   b. Physical evidence
6. Computer logging techniques - various access methods - evidence
7. Attribution from evidence - OS analysis, logs, physical files, images
8. Extracting evidence from a digital file
   a. Image
   b. Text
   c. Video
   d. Binary or Hex
9. Legal implications of digital evidence versus physical evidence.
10. Recovery of deleted or damaged information from physical devices.
11. Recovery of deleted or damaged information from Internet sources
12. Recovery of deleted or damaged information from Operating System or Dark Web sources.
13. Location of hidden files and images
14. Forensic Analysis reporting methods - tools and templates
15. Legal requirements for Forensic Analysis reports

Required materials
None.