CIS 522/422
Computer Forensics and Incidence Response

Text Computer Forensics: Principles and Practices
Volonino, Anzaldua, and Godwin
ISBN 0131547275
Lecture notes posted on Blackboard

Course Objective and Overview:

This course is designed to give students an understanding of basic computer forensics and the handling of evidence. The course is rigorous. You are advised to pay careful attention to the class lectures and especially sample problems and lab exercises. Exam questions are based primarily on the material covered in class and are designed to test your *understanding of the underlying concepts of computer forensics and evidence handling.* Note the course will cover the technical and legal aspects of evidence collection. I urge you to ask questions if you don't understand. You can come during my office hours, email me or (better yet, since everyone will benefit) ask in class. *There are not any dumb questions in this course.* You have to make sure there are no vague areas in your knowledge *before* exams. You will have to work hard to get an A in the class. On the other hand, many people do get an A in my class so hard work does pay off.

Course Objectives:

Module 1
Understand what constitutes a crime and identify categories of crime.
Understand law enforcement's authority to investigate information warfare and terrorist threats to national security.
Explain the different types of evidence.
Identify what affects the admissibility of evidence.
Identify how electronic evidence differs from physical evidence.
Identify what computer forensics tools and techniques can reveal and recover.
Explain the process of discovery and electronic discovery.

Module 2
Recognize the role e-evidence plays in physical, or violent, and computer crimes.
Describe the basic steps in a computer forensics investigation.
Identify the legal and ethical issues affecting evidence search and seizure.
Identify the types of challenges to the admissibility of e-evidence.
Understand how criminals' motives can help in crime detection and investigation.
Explain chain of custody.
Explain why acceptable methods for computer forensics investigations and e-discovery are still emerging.

Module 3
Explain how to manage e-evidence throughout the life-cycle of a case.
Identify the requirements for acquiring and authenticating evidence.

Describe acceptable methods for searching and analyzing evidence.
Explain investigative environments and analysis modes.
Explain the functions and features of forensics tools and toolkits.
Describe the types of equipment a forensics lab should have available.
Describe types of certification programs and credentials available for a computer forensics investigator.

Module 4
Explain the reasons for policies and procedures.
Formulate policies and procedures.
Identify the steps in a forensic examination.
Conduct an investigation.
Report the results of an investigation.

Module 5
Recognize and identify types of drives and media storage devices.
Describe PDA and cellular phone technologies.
Explain techniques for acquiring and analyzing data from hard drives and other storage media.
Describe techniques for acquiring and analyzing data from PDAs and cellular phones.
List and describe tools that can be used to analyze disk images, PDA data, and cellular phone data.

Module 6
Define and recognize an operating system.
Identify the different types of operating system interfaces.
Identify the different components of an operating system.
Understand and identify the different file systems.
Understand the OSI and TCP models.
Understand the basics of how data is transmitted on networks.

Module 7
Conduct efficient and effective investigations of Windows systems.
Find user data and profiles in Windows folders.
Locate system artifacts in Windows systems.
Examine the contents of Linux folders.
Identify graphic files by file extensions and file signatures.
Identify what computer forensics graphic tools and techniques can reveal and recover.

Module 8
Understand the flow of electronic mail across a network.
Explain the difference between resident e-mail client programs and webmail.
Understand the difference between typical desktop data storage and server data storage.
Identify the components of e-mail headers.
Understand the flow of instant messaging across the network.

Module 9
Explain the operation of intrusion detection systems (IDSs).
Discuss the value of using a network forensic analysis toolkit (NFAT).
Identify the components of an NFAT.
List the different areas from which data can be extracted.
Understand how to use an NFAT to capture physical and logical network data.
Identify the most common NFAT systems.

Module 10
Identify tactics and digital media used in the preparation and planning of devastating crimes or large-scale attacks and the cybertrails they leave.
Understand how the Internet is used as a tool for terrorism or virtual warfare.
Explain the objectives of hackers and those involved in criminal commerce.
Explain the process of collecting e-evidence in computer hacking cases.

Module 11
Understand the challenges of fraud investigations.
Describe the common types of fraud committed against and on behalf of companies and organizations.
Explain the characteristics and symptoms of fraud.
Identify the role of computer forensics in fraud detection and deterrence.
Understand the purposes of forensic accounting investigations and how to participate in them.

Module 12
Identify federal rules of evidence and other principles of due process of the law.
Explain the legal foundation and reasons for pretrial motions regarding evidence.
Identify the limitations on expectations of privacy.
Explain the major anticrime laws and amendments impacting discovery and use of e-evidence.

In Class Labs – We will conduct a series of class labs using Encase Software. These labs will be conducted in groups of three. Again, you will be asked to answer a series of questions concerning your findings in the lab. Participation in these labs is essential to the learning experience and will contribute to the Participation Portion of the Grade.

Paper – Students in CIS 522 will have to write a paper (5-10) concerning some aspect of computer forensics. This could be a case or a topic. This will be due on the last day of class, however, the topic must be approved by the Christmas Break.

Evaluation

The final course grade will be computed from the following inputs:

Exam 1		**30.00%**	
Final Exam		**30.00%**	**2 Tests = 60%**
Class Participation	**(Labs)**	**20.00%**	
Paper		**20.00%**	

TOTAL		**100%**	

The final course grade will be determined as follows:

90 or above	A
80-89.99	B
70-79.99	C
60-69.99	D
Less than 60%	F

Tentative Course Schedule

W1 Forensic Evidence and Crime Investigation Module 1
- 1.1 Cyber Crimes
- 1.2 Crime Categories
- 1.3 Cyber Crime Categories and Statutes
- 1.4 Criminal Prosectutions
- 1.4 Civil vs. Criminal
- 1.5 Information Warfare and CyberTerrorism
- 1.6 Computer Forensics Skills
- 1.7 Evidence Collection
- 1.8 Types of Evidence
- 1.9 Rules of Evidence – Search Warrants
- 1.10 Electronic Evidence
- 1.11 Fourth Amendment Rights
- 1.12 Investigative Authorities
- 1.13 Discovery Process
- 1.14 Electronic Discovery
- 1.15 Categories of Stored Data

W2 Computer Forensics and Digital Detective Module 2
- 2.1 E-Evidence and Hidden Trails
- 2.2 Technical Forensic Knowledge
- 2.3 Five W's (Who, What, Where, When and Why)
- 2.4 Preserving Evidence
- 2.5 Computer Forensic Science
- 2.6 Admissibility of Evidence

2.7 Digital Signatures and Profiling
2.8 Forensic Investigation Methods
2.9 Unallocated Space and File Slack
2.10 Challenges to Evidence
2.11 Search Warrants
2.12 Cybercrime Motives
2.13 Attribution
2.13 Chain of Custody Procedures
2.14 Forensic Investigator Responsibilities

W3 Tools and Equipment Module 3
3.1 Case Life Cycle
3.2 Criminal Tools
3.3 Chain of Custody Practices
3.4 Documentation
3.5 Data Collection
3.6 Power Down or Unplug
3.7 The Copy Rule
3.8 Write Blocking
3.9 Image Drive
3.10 Residual Data
3.11 Acquiring a Forensic Copy
3.12 Data Searches
3.13 Data Types
3.14 Investigative Environments
3.14a Trusted
3.14b Not Trusted
3.15 Forensic Tools
3.16 Forensic Equipment
3.17 Certification and Training Programs
Lab 1 Imaging and Using Write Blocks

W4 Policies and Procedures Module 4
4.1 Forensic Policies and Procedures
4.2 Forensic Personnel Hiring/Skill Set
4.3 Forensic Personnel Training
4.4 Data Exposed in Forensic Investigations
4.5 Documenting First Steps in a Case
4.6 Steps in a Forensic Case
4.6a Verify Legal Authority
4.6b Collect Preliminary Data
4.6c Determine the Environment for the Investigation
4.6d Secure and Transport Evidence
4.6e Acquire the Evidence
4.6f Examine the Evidence
4.7 Layers of Evidence

	4.8 Analyzing the Data 4.9 Reporting on the Investigation Lab 2 Encase #1
W5	PDA and Cell Data Module 5 5.1 Hard Drive Technologies 5.2 Storage Devices 5.21 Floppy Drives 5.22 Tape Drives 5.23 Zip Drives 5.24 Flash Drives 5.25 Optical Drives 5.3 PDAs 5.31 PDA Operating Systems 5.4 Drive and Media Analysis 5.41 Acquiring Data 5.5 PDA Chain of Custody 5.6 Cell Phone Analysis
W6	Operating Systems Module 6 6.1 Operating Systems 6.1a Operating System Functions 6.2 Types of Interfaces 6.3 Categories of Use 6.3a Single User Systems 6.3b Multiple User Systems 6.4 File and Memory Management 6.5 Job and Device Management 6.6 Security 6.7 Common Operating Systems 6.7a DOS 6.7b Windows 6.7c Linux 6.7d UNIX 6.7e MAC 6.8 Common File System Types 6.8a FAT 6.8b FAT 16 6.8c FAT 32 6.8d NTFS 6.8e UNIX/Linux Lab Encase #2 Midterm Exam
W7	Investigating Windows and Linux Module 7 7.1 Windows Systems User Activities User Data

7.2 System Artifact Data Generated by Operating System
7.3 Hidden Files
7.4 User Authentication for FAT and NTFS
7.5 Finding User Data and Profiles
7.6 User Root Folders
7.7 Investigating System Artifacts
7.7a Registry and Event Logs
7.7b Swap Files
7.7c Printer Spool
7.7d Recycle Bin
7.8 Shredding Data
7.9 Linux File System and Types
7.10 Linux System Categories
7.11 Linux Deleted and Compressed Files
7.12 File Signatures
7.13 Graphic File Forensics
7.14 Steganography

W8 Email and Webmail Forensics Module 8
8.1 E-Mail as Evidence
8.2 E-Mail Data Flow
8.3 Resident E-Mail Files
8.4 E-Mail Clients
8.5 Webmail
8.6 Webmail Data Flow
8.7 Webmail Files
8.8 Mail Servers
8.9 RAID
8.9a Acquiring Data from RAID Servers
8.10 E-Mail Headers
8.11 IP Address Registries
8.12 E-Mail Attachments
8.13 Anonymous Remailers
8.14 Instant Messaging
Lab Encase #3

W9 Network Forensics and IDS Module 9
9.1 Technical Surveillance Methods
9.2 Monitoring (Data and Line)
9.3 Intrusion Detection Systems
9.3a Anomaly Based
9.3b Signature Based
9.4 Reactive and Active Systems
9.5 Real Time NFAT Analysis
9.6 Threats
9.7 Major Categories of Threats

9.8 Threat Impact Areas
9.8 Network Forensics Abuse
9.9 Investigation of Security Breaches
9.10 Data Sources on a Network
9.10a Host Computers
9.10b Firewalls
9.10c DHCP Servers
9.10d NFAT/IDS Agents
9.10e IDS/Network Monitoring Software
9.10f Packet Sniffers
9.11 Capturing Data
9.11a Physical Aspects
9.11b Logical Aspects (Agents, Logs, Network Data)
9.12 Examining Data
9.12a Data Integrity
9.12b Pattern Analysis
9.12c Content Analysis
9.12d Playback Analysis
Lab Encase #4

W10 Countermeasures Module 10
10.1 Assessments (e.g., surveys, inspections)
10.2 Cover and Deception
10.3 Education, Training and Awareness
10.4 Humint
10.5 Conducting Security Reviews
10.6 Effectiveness of Security Programs
Large Scale Investigations Module 10
11.1 Terrorism and Cyber Warfare
11.2 Identity Theft
11.3 Phishing
11.4 Tracking Criminal Trails

W11 Fraud Module 12
12.1 Fraud, Waste and Abuse
12.2 Scope of Fraud
12.3 Fraud Investigations
12.4 Special Protections
12.4a Privacy
12.4b Privilege
12.5 Fraud Legal Elements
12.6 Investigator Independence
12.7 Types of Fraud
12.8 Characteristics and Symptoms of Fraud
12.9 Review of Accountability Controls
12.10 Review of Audit Trails and Logs

	12.11 Monitoring Systems for Accuracy and Abnormalities Lab Encase #5
W12	Criminal Codes Module 13 13.1 Federal Rules of Evidence 13.2 Exclusionary Rules 13.3 Anti Crime Laws 13.4 U. S. Patriot Act Lab Encase #6 Final Exam Paper Due