COMP 4430: DIGITAL FORENSICS Spring 2018

Instructor: Denise Ferebee **Room: FIT 107** **Class Time: 5:30-6:55pm (TuTh)**

Contact Information:

E-mail: dferebee@memphis.edu

Office Hours:

Monday	Tuesday	Wednesday	Thursday	Friday
By Appointment and ***participation in ecourseware discussion board (https://www.elearn.memphis.edu)***				

Course Description:

COMP 4430. Societal and legal impact of computer activity: computer crime, intellectual property, privacy issues, legal codes; risks, vulnerabilities, and countermeasures; methods and standards for extraction, preservation, and deposition of legal evidence in a court of law. PREREQUISITE: COMP 3825 and COMP 4270 or equivalent, or permission of instructor.

Motivation & Objectives:

Digital forensic is a hybrid science which offers professionals a systematic approach to perform comprehensive investigation in order to solve computer crimes. The needs for digital forensic experts are growing in corporations, law firms, insurance agencies, and law enforcement. Organizations are now realizing that evidence retrieved from computers and other digital media are becoming more relevant to convicting hackers and criminals. Though this digital evidence can be powerful, but if it is not retrieved through proper investigative procedure, it can be easily damaged and ruled inadmissible in a court of law.

The course covers both the principles and practice of digital forensics. Societal and legal impact of computer activity: computer crime, intellectual property, privacy issues, legal codes; risks, vulnerabilities, and countermeasures; methods and standards for extraction, preservation, and deposition of legal evidence in a court of law. This course provides hands-on experience in different computer forensics situations that are applicable to the real world. Students will learn different aspects of digital evidence: ways to uncover illegal or illicit activities left on disk and recovering files from intentionally damaged media with computer forensics tools and techniques.

Course Syllabus (Topics will be covered subject to availability of time):

- Introduction to Digital Forensics: computer crimes, evidence, extraction, preservation, etc.
- Overview of hardware and operating systems: structure of storage media/devices; windows/Macintosh/ Linux -- registry, boot process, file systems, file metadata.
- Data recovery: identifying hidden data, Encryption/Decryption, Steganography, recovering deleted files.
- Digital evidence controls: uncovering attacks that evade detection by Event Viewer, Task Manager, and other Windows GUI tools, data acquisition, disk imaging, recovering swap files, temporary &cache files
- Computer Forensic tools: Encase, Helix, FTK, Autopsy, Sleuth kit Forensic Browser, FIRE, Found stone Forensic ToolKit, WinHex, Linux dd , Volatility and other open source tools
- Memory Forensic: Image acquisition, Memory Image Analysis using Volatility, Detecting code injection etc.

- Network Forensic: PCAP file analysis, Collecting and analyzing network-based evidence, reconstructing web browsing, e-mail activity, and windows registry changes, intrusion detection, tracking offenders, etc.
- Reverse Engineering of Software Applications: defend against software targets for viruses, worms and other malware, improving third-party software library, identifying hostile codes-buffer overflow, provision of unexpected inputs, etc.
- Computer crime and Legal issues: Intellectual property, privacy issues, Criminal Justice system for forensic, audit/investigative situations and digital crime scene, investigative procedure/standards for extraction, preservation, and deposition of legal evidence in a court of law.

Suggested Textbook:

1. ***Guide to Computer Forensics and Investigations*** (4th edition). By B. Nelson, A. Phillips, F. Enfinger, C. Steuart. ISBN 0-619-21706-5, Thomson, 2009.
2. ***The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*** (1st Edition). By Michael Hale Ligh, Andrew Case, Aaron Walters.
3. *Computer Forensics and Cyber Crime: An Introduction (3rd Edition)* by Marjie T. Britz, 2013.

Reference Books:

- ***Computer Forensics: Hard Disk and Operating Systems,*** EC Council, September 17, 2009
- ***Computer Forensics Investigation Procedures and response,*** EC-Council Press, 2010
- ***Computer Forensics: Principles and Practices*** by Linda Volonino, Reynaldo Anzaldua, and Jana Godwin (Paperback - Aug 31, 2006)
- ***EnCase Computer Forensics***., 2016
- ***File System Forensic Analysis***. By Brian Carrier. Addison-Wesley Professional, March 27, 2005.
- NIST ***Computer Forensic*** Tool Testing Program (www.cftt.nist.gov/)
- ***Computer Forensics: Investigating Data and Image Files (Ec-Council Press Series: Computer Forensics) by EC-Council (Paperback - Sep 16, 2009)***
- ***Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet by Eoghan Casey, 2011***

Other Resources:

- Computer Forensic Training Center Online http://www.cftco.com/
- https://www.memoryanalysis.net/amf
- Computer Forensics World http://www.computerforensicsworld.com/
- Computer Forensic Services http://www.computer-forensic.com/
- Digital Forensic Magazine http://www.digitalforensicsmagazine.com/
- The Journal of Digital Forensics, Security and Law **http://www.jdfsl.org/**
- Journal of Digital Forensic Practice **http://www.tandf.co.uk/15567281**
- DOJ Computer Crime and Intellectual Property Section - http://www.usdoj.gov/criminal/cybercrime/searching.html
- Electronic Crime Scene Investigation: A Guide for First Responders - http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm and related publications at http://nij.ncjrs.org/publications/pubs_db.asp
- CERIAS Forensics Research (http://www.cerias.purdue.edu/research/forensics/)
- Scientific Working Group on Digital Evidence (http://ncfs.org/swgde/index.html)
- DoD Cyber Crime Center (http://www.dc3.mil)
- National Criminal Justice Reference Service - http://www.ncjrs.gov/app/publications/alphalist.aspx
- Digital Forensics Research Workshop (http://www.dfrws.org/)
- National White Collar Crime Center (http://www.nw3c.org/)
- Website relating to DOS commands, batch files, autoexec.bat/config.sys, and boot disks http://www.computerhope.com/
- The IACIS® Forensic Examination procedures -

http://www.iacis.info/iacisv2/pages/forensicprocedures.php

- Computer Security-related organizations : CERT, SANS, CIS, CASPR, CSI, CIAO, DRII, ISSA, IATFF, I2SF, NIAP, CSRC, OWASP

Evaluation:

Students are expected to participate in class discussions. In-class participation will be viewed as a continuous two-sided feedback process, which (a) allow students to assess themselves on their progress in learning the material/understanding the computer forensic issues; and (b) allows the instructor to assess how well he is fostering the communication process with and among students. Good evaluations will thus reflect not only your grasp of the material, but also how well you take advantage of class time and how well you end up communicating with other people (class participants) about the course material. The evaluation process will include paper presentations, assignments, software testing, class tests (or quizzes), and a term project to make sure that you have integrated the material into your general practice of computer forensics. You should read all material available in the textbook, lecture notes and other assigned papers to gather knowledge.

Your final grade for the course will be based on the following course-related activities (given in percentages):

Grading:

Class Participation	15%
Quizzes	20%
Experiments/Assignments/Lab exercises	25%
Midterm Exam	20%
Final Exam	20%

Grading Scale:

A+	95.1-100	**B+**	85.1 - 88	**C+**	76.1 – 79	**D+**	60.1-66
A	90.1 - 95	**B**	82.1- 85	**C**	70.1 – 76	**D**	50 - 60
A-	88.1 - 90	**B-**	79.1 – 82	**C-**	66.1 – 70	**F**	< 50

Plagiarism/Cheating Policy:

Plagiarism or cheating behavior in any form is unethical and detrimental to proper education and ***will not be tolerated.*** All work submitted by a student (projects, programming assignments, lab assignments, quizzes, tests, etc.) is expected to be a student's own work. The plagiarism is incurred when any part of anybody else's work is passed as your own (no proper credit is listed to the sources in your own work) so the reader is led to believe it is therefore your own effort. Students are allowed and encouraged to discuss with each other and look up resources in the literature (including the internet) on their assignments, but ***appropriate references must be***

included for the materials consulted, and appropriate citations made when the material is taken verbatim.

If plagiarism or cheating occurs, the student will receive a failing grade on the assignment and (at the instructor's discretion) a failing grade in the course. The course instructor may also decide to forward the incident to the University Judicial Affairs Office for further disciplinary action. For further information on U of M code of student conduct and academic discipline procedures, please refer to: **http://www.people.memphis.edu/~jaffairs/**

"Your written work may be submitted to Turnitin.com, or a similar electronic detection method, for an evaluation of the originality of your ideas and proper use and attribution of sources. As part of this process, you may be required to submit electronic as well as hard copies of your written work, or be given other instructions to follow. By taking this course, you agree that all assignments may undergo this review process and that the assignment may be included as a source document in Turnitin.com restricted access database solely for the purpose of detecting plagiarism in such documents. Any assignment not submitted according to the procedures given by the instructor may be penalized or may not be accepted at all." (Office of Legal Counsel, October 17, 2005).

Detailed Course Syllabus (Topics will be covered subject to availability of time):

Week	Starting	**Lecture Topics**
1		Course Overview, Scope and Agenda, Introduction to Computer Forensics
1		Introduction to computer crimes, évidence, extraction, préservation, etc.
2		Overview of hardware and operating systems: structure of storage media/devices Overview of hardware and operating systems: windows/Macintosh/ Linux -- registry, boot process, file systems, file metadata.
2		Data recovery: identifying hidden data, Encryption/Decryption, Hash functions, Message Authentication Code etc.
3		Steganography, recovering deleted files, identifying forged images, etc
3		Digital evidence controls: uncovering attacks that evade detection by Event Viewer, Task Manager, and other Windows GUI tools.
4		Digital evidence controls (continued): data acquisition, disk imaging, recovering swap files, temporary &cache files, memory forensic. *Computer Forensic tools: TBD*
4		Data Erasers, File & Disk Lockers Demonstration of Various Computer Forensic tools by students
5		Network forensic: Collecting and analyzing network-based evidence in windows and Unix environments, reconstructing web browsing, cyber forensics
5		Network and Mobile Network forensic: e-mail activity, and windows registry changes, intrusion detection, tracking offenders, mobile network architecture etc. *Lab session on Encase*
6		Software reverse engineering: defend against software targets for viruses, worms, hostile codes and other malware, improving third-party software library. *Lab session on Encase*
6		Software reverse engineering: identifying hostile codes-buffer overflow, provision of unexpected inputs, etc. *Lab session on Encase*
7		Computer crime and Legal issues: Intellectual property, privacy issues, Criminal Justice system for forensic, audit/investigative situations and digital crime scene, investigative procedure/standards for extraction, preservation, and deposition of legal evidence in a court of law.
7		Mobile Device Forensics, Cloud Forensics
8		Fundamental of Computer Network: OSI-reference model. TCP/IP model review. Tools: **netstat**, **lsof**,

8		Protocol Architecture, Protocol Layers, Encapsulation, and Network Abstractions.
9		DNS Protocol and SSL/TLS Protocol: Analyzing Encrypted traffic using Wireshark, Digital Certificate, Public and private key.
9		Network Forensic: Analyzing PCAP file using **Scapy framework**. **TCPDUMP**.
10		Memory Forensic: Preserving the Digital Artifacts, Software Tools, Memory Dump Formats. Tools: **/dev/mem**, **/dev/kmem**, **ptrace**.
10		Modern Memory Acquisition: fmem, Linux Memory Extractor (LiME), /proc/kcore.
11		Memory Forensic using Volatility: Introduction, Process and Process Memory, **task_struct** structure, Process Control Block (PCB), Kernel Symbol Table: /boot/System.map.
11		Analyzing Process Activity: **pslist**, **pstree**, **psscan**, **psxview**. Process Hollowing/Hollow Process to detect malware: using the PEB and the VAD structure.
12		Memory Forensic to collect Network Artifacts: Hidden Connections, Internet History, Raw Sockets, and Sniffers.
12		Internet Digital Artifacts: Introduction, Browser Artifacts: Firefox, Chrome. Mail Artifacts.
13		Application Forensics: Installing forensic framework: **Sleuthkit** and **Autopsy** using source code. **Exiftool** to find hidden information.
13		Windows Registry: Windows Registry Analysis, Volatility's Registry API, Dumping Password Hashes, Obtaining LSA Secrets. Tools: **regedit**, **regini**, **winreg** or **_winreg**.
14		Course Review
15		Exam

NOTE:

- *There will quizzes, a midterm, and final exam. Students should come prepared (on previous lectures and topics covered) in each class for quizzes.*

- *There will be a number of Lab sessions on forensic tools; in case Lab set ups cannot be done in time, alternative arrangements (lectures/assignments) will be made.*

- *All course-related information will be available from elearn.memphis.edu. Check the course Web page at http://elearn.memphis.edu for class notes and updated information. This schedule will be updated regularly during the semester to reflect class activity changes.*

- *If I need to communicate with the class as a group, I'll be using elearn email. You may need to check your email regularly.*