ITMS 438 SYLLABUS

ITMS 438 Cyber Forensics

Hours: 3 credit hours / 45 contact hours

Instructor: William Lidinsky

Textbook, title, author, and year:

Guide to Computer Forensics and Investigations, B. Nelson, A. Phillips, C. Steuart, 2019

File System Forensic Analysis, B. Carrier,2005

Specific course information

a. **Catalog description:** This course will address methods to properly conduct a computer and/or network forensics investigation including digital evidence collection and evaluation and legal issues involved in network forensics. Technical issues in acquiring court admissible chains-of-evidence using various forensic tools that reconstruct criminally liable actions at the physical and logical levels are also addressed. Technical topics covered include detailed analysis of hard disks, files systems (including FAT, NTFS and EXT) and removable storage media; mechanisms for hiding and detecting hidden information; and the hands-on use of powerful forensic analysis tools.

b. **Prerequisites:** ITMS 448 and ITMO 356

c. **Required for Applied Cybersecurity and Information Technology.**

Specific goals for the course

a. Course Outcomes:

- Demonstrate knowledge of cyber forensic analysis at levels ranging from professional to executive levels including applicable legal issues.
- Apply this knowledge to planning and executing specific cyber forensic analyses. This includes the use of cyber forensic tools.
- Demonstrate knowledge of steganography and steganalysis and apply it to determination of existence of covert information.

b. Course student outcomes:

At the conclusion of this course, each student should be able to:

- Demonstrate knowledge of cyber forensic procedures, planning of analyses and the use of common tools for analysis
- Describe several file systems including FAT, EXT, YAFFS and NTFS.
- Describe several common booting procedures.
- Describe how to find file system objects that have been deleted or obfuscated.
- Describe how to track past computer and Internet activity and to establish time lines for this activity.
- Describe techniques for inserting covert information in various text, document and image carrier files.
- Demonstrate the ability to use tools such as WinHex, EnCase, SleuthKit and Autopsy. Also, several forensic imaging, carving and discovery tools.

Topics to be covered

a. Course Introduction. ForSec Lab Discussion. Introduction to Network & Computer Forensics.
b. Computer Investigations. Forensic Tools and Tool systems
c. Certification: Investigators and Laboratories.
d. Data Acquisition & Image Creation. Proc. Crimes & Incidents.
e. Mass storage. Solid state (flash) and rotating magnetic drives.
f. Volumes & Partitions.
g. MBR Partitions. GPT Partitions.
h. FAT File system. NTFS File system.
i. Linux Boot & Disk & Partition. EXT File Systems. Sleuthkit
j. File Carving. File carving analysis & lab
k. ADS. ADS lab.
l. Memory (RAM) forensics.
m. Virtual machine forensics.