CS 47207/57207  DIGITAL FORENSICS  3 credit hours

Instructor’s Name: Kambiz Ghazinour


Course Content:
(Slashed with CS 57207) This course addresses the need for digital forensics, best practices for general incidence response, legal aspects of forensics, tools and techniques to perform a full computer forensic investigation.

Prerequisites or co-requisites: Minimum C grade or better in CS 23001.

Required, elective, or selected elective

Topics to be Covered (45 hours):

1. Introduction of digital forensics? (4 hours)
2. Key technical concepts (4 hours)
3. Labs and tools (4 hours)
4. Collecting evidence (4 hours)
5. Windows system artifacts (4 hours)
6. Anti-forensics (4 hours)
7. Legal (The fourth amendment, Searching with a warrant, etc.) (4 hours)
8. Internet and e-mail (4 hours)
9. Network forensics (4 hours)
10. Mobile device forensics (4 hours)
11. Looking ahead: challenges and concerns (5 hours)

Learning Outcomes:

1- Describe what is a Digital Investigation is, the sources of digital evidence, and the limitations of forensics.
2- Explain how to design software to support forensics.
3- Describe the legal requirements for use of seized data.
4- Describe the process of evidence seizure from the time when the requirement was identified to the disposition of the data.
5- Describe how data collection is accomplished and the proper storage of the original and forensics copy.
6- Conduct data collection on a hard drive.
7- Describe a person’s responsibility and liability while testifying as a forensics examiner.
8- Recover data based on a given search term from an imaged system.
9- Reconstruct application history from application artifacts.
10- Reconstruct web browsing history from web artifacts.
11- Capture and interpret network traffic.
12- Discuss the challenges associated with mobile device forensics.
13- Inspect a system (network, computer, or application) for the presence of malware or malicious activity.
14- Apply forensics tools to investigate security breaches.
15- Identify anti-forensic methods.

Learning Outcomes Assessment:
1- Four assignments during the semester
2- Midterm exam
3- Final exam
4- Class discussion