CprE 536: Computer and Network Forensics

Fall 2024

Instructor: Yong Guan
Office: 309 Durham Hall, ECE Dept.
Iowa State University
Ames, Iowa 50011

Tel: (515) 294-8378(o)
Fax: (515) 294-8432
E-mail: yguan@iastate.edu
http://www.eng.iastate.edu/∼guan/

Course Description:

The knowledge of digital forensics has become essential in securing today's network-centric computing environment. This course will give the students both the fundamental knowledge and hands-on practice on digital forensics. The added exposure to forensics will enhance the marketability of our students and serve the students who carry the skills and knowledge forward into their future careers.

Digital forensics studies cyber-attack prevention, detection, response, and investigation with the goals of counteracting cybercrimes, and making the responsible persons/groups accountable. Computer crime investigation incorporates multiple areas of concern, including computer science/engineering, information security, incident response, cryptography, information hiding, law, business, and even psychology. The topics covered in this course include fundamentals of digital forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anonymity and pseudonymity, anti-forensics techniques, cyber law and privacy, computer security policies and guidelines, court report writing and presentation, and case studies. Course projects will be done using the licensed toolkits and equipments in the NSF-funded Digital Forensics Lab in Coover Hall, Room 3223.

The course will consist of two investigative course projects (i.e., machine problems) based on licensed forensic toolkits, one programming project (develop/test a forensic tool), two exams, and one term paper. We will have a small number of quizzes/homework assignments, demonstrations (Zoom, on your course projects), and presentations. The students will define a research problem and finish a term paper:

- Write a 6-pages (double column and single space) term paper: including defining a specific problem, surveying existing work, developing a (better) solution, and evaluating your results. A list of selected topics/problems will be provided. You are also welcome to propose your own one.
- Learn to use and evaluate digital forensic software tools and write reports on them.
- Give demos and/or presentations on projects, and term papers.

For each topic covered in the class, we will provide a suggested reading list including a number of selected classical papers and some new papers published on the top security and forensics conferences/journals in recent years.

Prerequisite:

Familiarity with basic concepts in operating systems and networking.

Course Materials:

There will be no textbooks. Most readings are from papers published on top security/forensics conferences or journals, reference books, and related Internet web sites. Two reading lists will be given: The required readings are 30-35 papers and a suggested reading list includes a selected set of 150+ papers published within the last 15 years.

The following are a list of reference books:

- Bruce Middleton, *Cyber Crime Investigator's Field Guide*, Boca Raton, Florida:Auerbach Publications, 2001, ISBN 0-8493-1192-6.
- Brian Carrier, *File System Forensic Analysis*, Addison-Wesley, 2005, ISBN 0-321-26817-2.
- Chris Prosise and Kevin Mandia, *Incident Response: Investigating Computer Crime*, Berkeley, California: Osborne/McGraw-Hill, 2001, ISBN 0-07-213182-9.

- Warren Kruse and Jay Heiser, *Computer Forensics: Incident Response Essentials*, Addition-Wesley, 2002, ISBN 0-201-70719-5.
- Rebecca Gurley Bace, *Intrusion Detection*, Indianapolis, Indiana: Macmillan Technical, 2000, ISBN 1578701856.
- Stephen Northcutt, Mark Cooper, Matt Fearnow, and Karen Frederick, *Intrusion Signatures and Analysis*, Indianapolis, Indiana: New Riders, 2001, ISBN 0-7357-1063-5.
- R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, 2001, ISBN: 0471389226.
- Alberto Leon-Garcia and Indra Widjaja, *Communication Networks: Fundamental Concepts and Key Architectures*, First Edition, McGraw-Hill Companies, Inc., 2000, ISBN 0-07-022839-6.

Course Outline:

In this course, we will tentatively discuss the following issues.

- Module I: Digital Forensics: An Overview
- Module II: Forensics Basics and Criminalistics
- Module III: Basics of OS and Networking: A Review
- Module IV: Advanced Topics in Digital Forensics
  - Forensic Modeling and Principles
  - Forensic Duplication
  - Forensics Analytics
  - File Carving
  - Mobile Device Forensics
  - Cyber Forensics Tools and the Testing Thereof (Encase, FTK, OnlineDFS, etc.)
  - Network Surveillance and Forensics
    - Internet Accountability and Traceback
    - Stepping Stone Attack Attribution
    - Botnets Investigative Analysis
    - Tracing Anonymous VoIP Calls
    - Multicast Fingerprinting
    - Online Community Structure and Linkage Analysis (Social Network Websites)
  - Multimedia Forensics
- Module V: Online Frauds Detection and Response
- Module VI: Cryptocurrency and Blockchain
- Module VII: Steganography & Steganalysis
- Module VIII: Anonymity/Pseudonymity/P3P
- Module IX: Cyber Law, Privacy, Security Policies and Guidelines
- Module X: Cases Studies, Ethical issues
- Module XI: Court Report Writing and Testimony Skills

Grading:

Grading will be on the absolute scale. The cutoff for an 'A' will be at most 90% of total score, 80% for a 'B', 70% for a 'C', and 60% for a 'D'. However, these cutoffs might be lowered at the end of the semester to accommodate the actual distribution of grades.

1. Mid-term & Final Take-home Exam: 35%
2. Course Projects: 30%
3. Presentations and demos: 5%
4. Online quizzes and/or short surveys on selected DF topics: 10%
5. Term Papers: 20%
   (a) Vision and Related Work: Give your view of the big picture and compare and relate your work to others
   (b) Critiques: Identify holes, research questions, and potential improvements of the work
   (c) Depth and breadth of the knowledge in the materials

Academic Policy:

1. All incidents of academic dishonesty will be dealt with according to the university policy. No exceptions. Anyone suspected of academic dishonesty will be reported to the Dean of Students Office.
   (a) All references must be properly cited, including internet web pages (URL must be provided). If plagiarism is detected, i.e. without proper citation and quotation, you will automatically receive an F. When in doubt, please ask the instructor if it is reasonable to include other's work in your assignments.
2. We welcome active participation and discussions from both on- and off-campus students.
3. Due date for term papers and course projects is hard (no late hand-in will be accepted.) except that you have reasonable reasons. However, for the whole semester, you may have at most one time no-reason three-day extension. But the final term paper due and other due dates in the dead week are hard.

Time: Tuesday & Thursday 9:00 am - 10:45 am

Location: HOWE 1242.

Office Hours: Thursday 2-3pm. Zoom Link:

https://iastate.zoom.us/j/92372099753?pwd=cXdGME92THVFTlZDMlZLK3cwUDc3Zz09.

You are welcome to email me a time to schedule a meeting, if the time does not work for you.