ASU
Arizona State University

CSE 469: Computer and Network Forensics

Topic 0: Course Overview

Dr. Mike Mabey | Spring 2019

Instructor

Dr. Mike Mabey

- Alumnus of ASU (MS & PhD)
- Adjunct / Faculty Associate
  - Full time job: US Army
- Office: N/A
- Office Hours: Tuesdays 4:15 - 5:15 PM
- mmabey@asu.edu

TAs

Adam Oest

- PhD Student
- aoest@asu.edu
- Office:
  - BYENG 469 AC
- Office Hours:
  - Thursdays 12-1 PM
    BYENG 423

Sukwha Kyung

- PhD Student
- skyung1@asu.edu
- Office:
  - BYENG 469 AB
- Office Hours:
  - Wednesdays 1-2 PM
    BYENG 423

INFOSEC at ASU

Programs:

- Two undergraduate IA concentration programs
  - BS in computer science
  - BSE in computer systems engineering
- Three graduate IA concentration programs
  - MS
  - MCS
  - PhD

INFOSEC at ASU

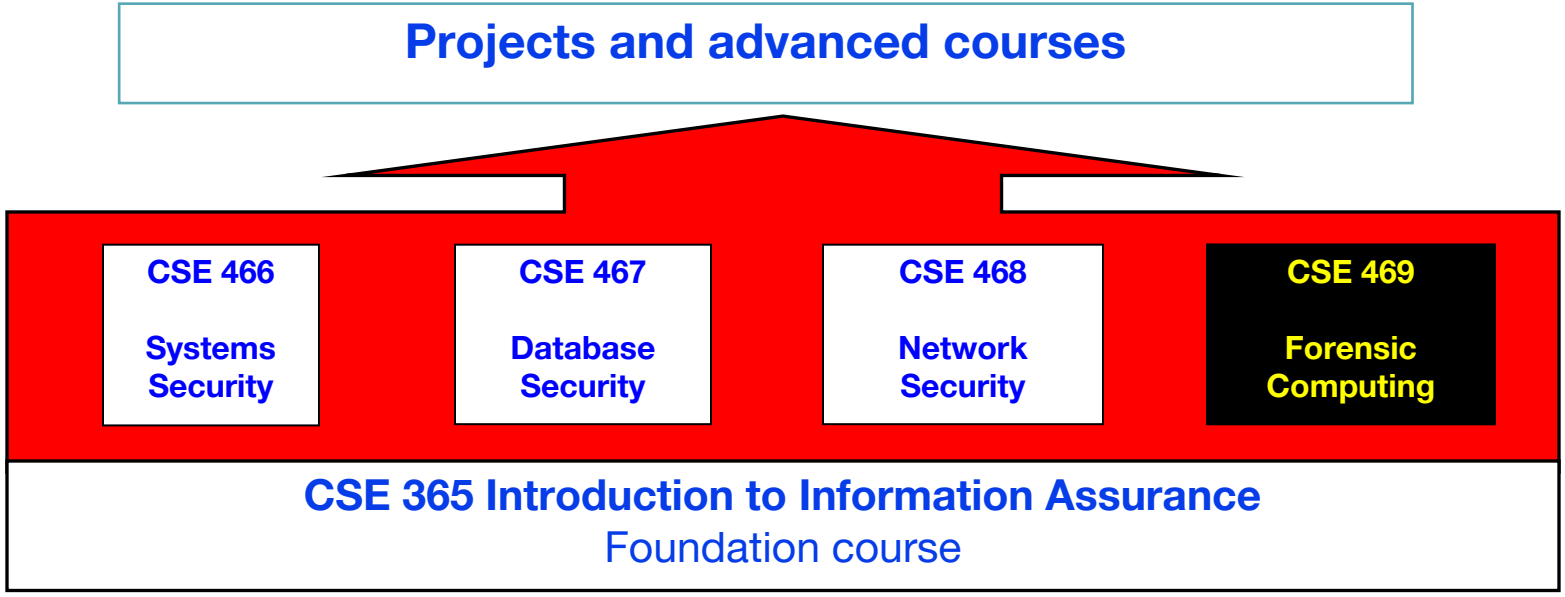
Concentration in BS (Computer Science):

- Minimum of 15 credits in IA and related areas as technical electives
- Courses:
  - CSE 465 Introduction to Information Assurance
  - CSE 466 Computer System Security
  - CSE 467 Data and Information Security
  - CSE 468 Network Security
  - CSE 469 Computer and Network Forensics

Graduate Level Security Classes

- CSE 539 Applied Cryptography
- CSE 543 Information Assurance and Security
- CSE 545 Software Security
- CSE 548 Advanced Computer Network Security
- Seminar: Computer Security: Techniques and Tactics

INFOSEC at ASU



NSA and DHS designated ASU as a National Center of Academic Excellence in Information Assurance Education

Computer Security? Computer Forensics?

Arizona State University launches

the Center for Cybersecurity and Digital Forensics

within the ASU Global Security Initiative

Goals of Computer Security (CIA Triad)

- **Confidentiality**: Prevent/detect/deter improper *disclosure* of information
- **Integrity**: Prevent/detect/deter improper *modification* of information
- **Availability**: Prevent/detect/deter improper *denial of access to services* provided by the system

Examples

- Confidentiality: You should not come to know the scores of your classmates in this class
- Integrity: You should not be able to change your or others' scores in this class
- Availability: You should always be able to view the assignments on the course web site

In Addition to CIA Triad

- **Authenticity**: The assurance that a message, transaction, or other exchange of information is from the *source* it claims to be from.

- **Non-repudiation**: The assurance that someone cannot deny something, such as the receipt of a message or the authenticity of a statement or contract.

Examples

- Authenticity: You should not pretend, as the TA, to send an email to your classmates

- Non-repudiation: The TA can not pretend he did not send out the message

Goals of Computer Forensics

- Forensics is defined as “relating to the use of scientific knowledge or methods in solving crimes.”
- Postmortem: Forensic analysis *after* a computer or network is compromised
- Acquire data even if the original owner does not want to leak that data (e.g. deleted from hard disk)
  - Breach the security goal **confidentiality**

Course Objectives

- Get hands-on experiences with lots of lab exercises and programming assignments
- Introduce you to reading research papers
- Introduce you to real-world security and forensics by inviting external speakers from government, industry, and academia

Two Elements of Digital Forensics

- Process
  - Distinguishes forensics from data recovery, bug hunting
  - How to acquire, handle, and analyze evidence properly
  - What precautions to take, pitfalls to be aware of
  - Difference between evidence being admissible in court!
  - Can apply to any type of digital forensic evidence (if the process is good)
- Technical Knowledge
  - Deep understanding of the specific technology you need to extract information from
    - How is the data stored at the binary level?
  - Technical side is where most forensic research is done

Digital forensics is the application of technical knowledge to extract information from evidence while adhering to a lawful process.

Course Prerequisites

- Knowledge of information systems, computer networks, and their operations:
  - CSE 310 Data Structures and Algorithms
    - Must understand relationship between a data structure and its binary representation

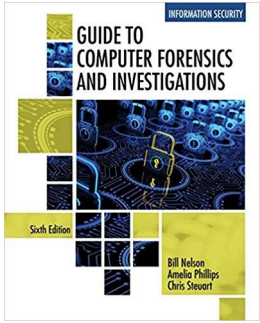
For example:
If I give you this data structure and tell you that a `short` is 2 bytes, an `int` is 2 bytes, and a `double` is 4 bytes, you should be able to tell me which hex values represent the person's age in this memory sample:

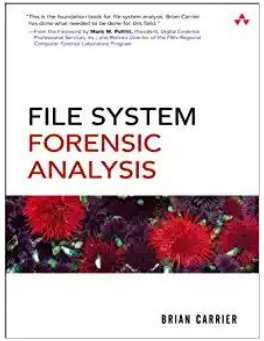
```
struct Employee {
    short id;
    int age;
    double wage;
};
```

0xc5	0x01	0x32	0x00	0x50	0x34	0x03	0x00

Textbook/Readings

- No required textbook
- Highly recommended books:
  - Guide To Computer Forensics and Investigations
  - File System Forensic Analysis
- Slides and important reading material will be posted to the course website





NOTE: Please see the syllabus for more information!

Course Communication

1. Class website: mikemabey.com/cse469s19
   a. Syllabus, assignments, schedule, notes, lecture recordings, important links, etc.
2. Exam grades: Gradescope
   a. Detailed, consistent grading
3. Mailing list: Piazza
   a. Collaborative discussion board
   b. Be careful not to violate academic integrity! (see course website for examples)

Note: Federal law prevents me from spending time on outside employment (this class) while I'm on the clock for the Army. Please be understanding of this!

NOTE: Please see the syllabus for more information!

Course Topics

- Principles of digital forensics (Process)
  - Acquisition
  - Authentication
  - Analysis
  - Presentation
  - Rules of evidence
- Computing basics
  - File systems
  - How computers store data
  - How computers communicate
- Forensic tools and technologies
  - Open-source tools
  - Commercial tools
  - How to write your own tools
- Cybercrime investigation
  - What constitutes cyber crime
  - Law and policies on cyber crime
  - Trends in cyber crime
- Other cool topics:
  - Mobile and car forensics
  - Cloud and web forensics

Grading Policy

- Homework: 60%
  - Assignments: 35%
  - Course Project: 20%
  - Paper Report/Presentation: 5%
- Exams: 40%
  - Midterm: 15%
  - Final: 25%
- Attendance:
  - Will affect your grade

NOTE: Please see the syllabus for more information!

Grading Policy

- Homework: To be done individually
  - Unless otherwise noted in the assignment description
- Project: To be done in groups of 2
- Paper Report: Individual report on a research paper from list on the course website
  - Grad and Honors students will *also* give a 20 minute presentation on their paper in class
- Late work: 20% deduction each day late
- Attendance: Will affect your grade

NOTE: Please see the syllabus for more information!

Academic Integrity

- Regular rules apply
  - See the ASU Student Code of Conduct and ASU Student Academic Integrity Policy.
- Use of code snippets is allowed as long as:
  - Proper credit for the source is given in a comment AND
  - The snippet doesn't constitute a significant portion of your code AND
  - The source is not another past or present student of the course
- Posting assignment code online is not allowed

NOTE: Please see the syllabus for more information!

Class Format

- Lecturing
  - Lecture notes will be posted to the class website
  - Videos of lectures will be posted to YouTube
  - Links to videos will be on the website
- In-class exercises
  - Two students form a group, but each one has to do the exercise
  - Students MUST attend all classes
  - There will be an attendance sheet for every class

Homework

- Done individually
- Several programming assignments:
  - Reinforce principles from class by forcing you to think through the details
  - Goal is to give you the skills to be forensic computer scientists, not just tool users
- Some lab exercises:
  - More hands-on practice with forensic tools
  - Extension/continuation of in-class exercises
  - Necessary software will be provided

Course Project

- Group project
  - Same groups of 2 for doing in-class labs
- Write a program for tracking actions taken with evidence items while in custody
- Command-line, Linux-compatible
  - Programming language is your choice

Group Formation Due: January 16

Instructions to be sent out via Piazza