CS593: Digital Forensics

Lecture 1: Introduction

D. Kevin McGrath

Sunday, June 25, 2023

Why Digital Forensics?

- A very new field.
- Ad hoc knowledge base.
- Standards for digital forensics are just starting to be formed.
- We have a rare opportunity to shape the future of digital forensics.

Instructor

- D. Kevin McGrath
- Spent 4 years at McAfee/Trellix as vulnerability researcher
  - Reverse engineering
  - Hardware/firmware/software/RF hacking
- Teach a variety of security courses
  - Network Security
  - Intro to Security
  - DevSecOps
- Programs in C using any language

Introduction to the Course and Digital Forensics Concepts

First Lectures

- Course overview.
- Digital forensics concepts.
  - What is forensics?
  - Branches and applications of digital forensics.
  - Overview of forensics principles: scientific method, evidence principles, documentation, reporting & testimony.

Sociological Aspects of Digital Forensics

Law in Action

- Structure of legal system:
  - Disputes/adversarial.
  - Civil vs. criminal justice systems.
  - Courtroom workgroup.

Elements of Trials

- Evidence:
  - Standards for scientific evidence.
  - Forensic sciences.
- Decision-makers:
  - Judges.
  - Juries.

Legal Aspects of Digital Forensics

Forensics and Digital Forensics

- *Forēnsis*: In Latin, “of or before the forum,” as in the Roman Forum.
- Investigate events after the fact and establish what happened, based on the evidence that is collected.
- In our case, from digital devices…
- Necessarily raises issues about lawfully collecting the evidence; the veracity/authenticity of the evidence; and the conclusions that can be drawn.
- The adversarial process and its mechanisms to arrive at the “truth” in civil or criminal cases.

Legal Aspects of Digital Forensics 1

- The Fourth Amendment in the Bill of Rights:
  - "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
- The warrant requirement.
- Reasonable expectation of privacy.
- Exceptions to the warrant requirement: consent, plain view, exigent circumstances, etc…

Legal Aspects of Digital Forensics 2

- Evidence (rules that govern proof of facts) and the Federal Rules of Evidence.
- Chain of custody.
- Best evidence rule.
- Non-hearsay: admissions, prior statements.
- Hearsay exceptions: business records exception, declarations against interest, prior inconsistent statements, etc…
- Scientific evidence and Rule 702.
- Expert witness testimony and expert reports.

Legal Aspects of Digital Forensics 3

- Privacy laws:
  - HIPAA (Health Insurance Portability and Accountability Act).
  - FERPA (Family Educational Rights and Privacy Act).
- ECPA (Electronic Communications Privacy Act); Stored Communications Act; Wiretap Act.
- Cyber Crimes: CFAA (Computer Fraud and Abuse Act) with examples: hacking, cyber stalking, etc…

Computer Forensics

What Is Computer Forensics?

- Searching for and analyzing digital evidence in computers.
- Often supports investigation of “conventional” crimes like robbery.
- Cornerstone of digital forensics.

Computer Forensics Topics

- Computer hardware fundamentals.
- File systems analysis.
- Deleted file recovery.
- Analysis of Windows systems.

Network Forensics

Network Forensics

- Recovery and analysis of digital evidence from network sources.
- You will learn about:
  - Various sources of network-based evidence, including on the wire, in the air, switches, routers, servers, firewalls, and intrusion detection systems.
  - Evidence acquisition techniques.
  - Protocol/packet/flow analysis.
  - Network intrusion detection and analysis.

Network Intrusion Detection/Protection

- Will give an overview of network intrusion detection/prevention (NIDS/NIPS) systems.
  - Their functionality.
  - Modes of detection.
  - Types of NIDS/NIPS.
- NIDS/NIPS evidence acquisition.
- Provide examples of detecting network anomalies using NIDS.

Mobile Forensics and Malware

Mobile Device Forensics

- Searching for and analyzing digital evidence on mobile phones and GPS devices.
- Like computer forensics, usually supports investigations of “conventional” crimes.
- Can provide valuable location information.

Digital Archives

Outside the Juridical Context: Maintaining Historical Records

- How and why the practice of maintaining archives originated in the ancient world and evolved over time.
- The age-old problems of forgery and corruption, and the development of approaches to detecting and fighting them.
- How advances in technology have created both opportunities and challenges as archives work to meet the same fundamental social needs.

Digital Data in Libraries & Archives

- Archives have the special challenge of needing to preserve records over the very long term.
  - The challenge of diverse, obscure, obsolete, or undocumented hardware, software, and file formats.
- Difficulty of handling the massive amounts of data associated with modern people's lives.
  - Privacy, security, ease of use.
- Trends in digital forensics hardware and software used for archival purposes.

Questions?