COMP3731 Computer Forensics

Finals Study Guide

Internet Artifacts:

- Artifacts of importance and what information can they provide (no need to memorize location paths)
- Formats used by different browsers to store the artifacts

Analysis & Validation:

- Basic steps for all computer forensics investigations
- Data hiding techniques: file manipulation (methods and detection), hiding partitions and clusters, bit shifting, steganography, rootkits (what they do and how to detect them)
- How to recover encrypted files and passwords

Data Carving/Steganography/Image Forensics:

- Data carving
  - impact of file fragmentation, what are false positives, magic numbers
  - types of data carving: basic and advanced
  - header-footer, header-maximum length and header-embedded length carving
  - file structure types, what is file structure based carving, performing it on jpeg and zip files
  - how to carve file fragments, carving bi-fragmented files, carving using matching metrics
- Steganography
  - what is it and general idea of how its done using data insertion and data substitution
  - what is LSB substitution and how can it be done on images and audio files
  - steganalysis on images: basic idea behind enhanced LSB and chi-square method
- Image format types (no need to memorize offsets), lossy and lossless compression, idea of how Huffman codes work

Network Forensics:

- Layered network defense strategy
- How does network forensics differ from typical computer forensics?
- TCP/IP layers, what is a packet, different headers (no need to memorize entire structure), handshaking process, identifying parts from a packet dump
- Port scanning, how is it done, regular scanning/stealth scanning/banner grabbing/other types of scanning
- Analyzing packet traces, sequence and acknowledgment numbers, make sure you did the exercises from class (*ConnectGoogle.pcap, Captures.zip*)

Email Investigations:

- Client/Server architecture of email, different components in this architecture, what is SMTP, POP, IMAP
- Analyzing email headers, tracking a message using them (see how spam messages are generated and can be detected - open relay and direct-to-MX)
- What are email logs, what different kinds may be generated