COMP 597 – Computer Forensics
Study Guide for the Final Exam
Spring 2017

Introduction:

- Digital Evidence:
  - Definition
  - usage
- Three phases of investigation process of a digital crime
- message digest algorithm
- Data Analysis (last slide)

Computer Foundation:

- *big-endian* architecture
- little-*endian* architecture
- bit flags
- Boot Process

Data Acquisition:

- Acquisition Type
- Acquisition Level
- Know how to use dd
- Windows Registry

Volume Analysis:

- Definition of volume analysis & partition system
- Everything about DOS partitions
- Recovering Deleted Partitions
- Everything about BSD partitions

File System Analysis:

- Everything we discussed is included

Steganography:

- Everything we discussed is included

Document Analysis:

- Everything we discussed is included

The style of questions is similar to the first exam and will include questions from:

- Labs
- Assignments