Department of Electrical Engineering & Computer Science
CGS 5131 0R01/0V61/0084 – Digital Forensics I: Seizure and Examination of Computer Systems
Fall 2021

Lecturer: Rick Leinecker
Email: Richard.Leinecker@ucf.edu

Lecture Meetings: Tuesday/Thursday 7:30 PM – 8:45 PM in BA1 in 216

Office Hours: Monday/Wednesday 1:30 PM – 2:15 PM in HEC 357

Prerequisites: Permission

TA/Grader: Seema Reddy -- seemareddy18@knights.ucf.edu

Credit Hours: 3

Required classroom tools
WinHex: Specialist Version

CGC 5131 Learning Objectives and Outcomes

Legal issues regarding seizure and chain of custody. Technical issues in acquiring computer evidence. Popular file systems are examined. Reporting issues in the legal system.

Learning Objectives

- Use the dd command and the FTK Imager program to produce "forensically sound" disk images, using a Windows platform (XP or Visa).
- Learn DOS partitions using various tools (commands) available on Helix CD from Carrier's Sleuthkit, applied to a 1 GB thumb drive image file in dd format.
- Learn about Windows FAT systems particularly FAT12, using Norton's Diskedit tool as the main examination tool in a DOS environment under Microsoft Virtual PC.
- Learn Windows NTFS file system data structures (particularly, the date/time stamps and data clusters) using WinHex, and string searching based on grep expressions using AccessData's FTK.
- Perform forensic examination of a Windows XP disk image using FTK and associated tools, and write a forensic report.

Learning Outcomes

- conduct digital investigations that conform to accepted professional standards and are based on the investigative process: identification, preservation, examination, analysis and reporting;
- cite and adhere to the highest professional and ethical standards of conduct, including impartiality and the protection of personal privacy;
- identify and document potential security breaches of computer data that suggest violations of legal, ethical, moral, policy and/or societal standards;

- apply a solid foundational grounding in computer networks, operating systems, file systems, hardware and mobile devices to digital investigations and to the protection of computer network resources from unauthorized activity;
- work collaboratively with clients, management and/or law enforcement to advance digital investigations or protect the security of digital resources;
- access and critically evaluate relevant technical and legal information and emerging industry trends; and
- communicate effectively the results of a computer, network and/or data forensic analysis verbally, in writing, and in presentations to both technical and lay audiences.

Proposed Schedule:

Topic
What is Digital Forensics
Imaging
WinHex
NTFS/FAT
Data Hiding and Data Carving
Anti-Forensics
SysInternals
Registry
Reports
Network Forensics
Memory Forensics
TBD
Live Analysis
TBD
Case Analysis

Grading will be as follows: Assignments – 42% total
Discussions – 16% total
Quizzes – 42% total

Attendance: Attendance is not required but is highly recommended.

Grading Scale:

94-100	A
90-93.99	A-
87-89.99	B+
84-86.99	B
80-83.99	B-
77-79.99	C+
74-76.99	C
70-73.99	C-
67-69.99	D+
64-66.99	D
60-63.99	D-
0-59.99	F

Academic Dishonesty: UCF's Golden Rule http://goldenrule.sdes.ucf.edu/ will be strictly applied.

Important Dates:
Classes Begin: August 23

Thursday Football Game:	September 2
Veterans Day Holiday:	November 11
Thanksgiving Holiday:	November 24-28
Last Day of Class:	December 1

Makeups:
Discussions, assignments, and quizzes are not accepted late since you have them in advance.