CS 695 Host Forensics Syllabus

The syllabus below describes a recent offering of the course, but it may not be completely up to date. For current details about this course, please contact the course coordinator. Course coordinators are listed on the course listing for undergraduate courses and graduate courses.

Text Books

Required
, , None

Recommended
Keith J. Jones, Richard Bejtlich, Curtis W. Rose, Dan Farmer, Wietse Venema, Brian Carrier , *Computer Forensics Library Boxed Set (contains Forensic Discovery, Real Digital Forensics, and File System Forensic Analysis)* , Addison-Wesley Professional, 2007, ISBN 0321525647
, *The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler* , No Starch Press, 2008, ISBN 1593271786

Week-by-Week Schedule

Week	Topics Covered	Reading	Assignments
1	Introduction. Basics. Incidents, scene reconstruction. Data collection.	Forensic Discovery, Chapter 1	
2	Capturing volatile and non-volatile information. Understanding file systems. Simple and extended attributes, erased data, file reassembly.	Knoppix CD Forensic discovery, Chapters 3, 4, 7. Real digital forensics, Chapter 4	Submit selection of topics for midterm project (e.g. HoneyNet challenge, instructor supplied challenge disk images, etc.), as well as topics for final project.
3	The importance of time. File header magic. Cached information. Meta-data.	Forensic discovery, Chapter 2	Midterm project proposals due
4	Memory forensics. Process tables (Unix, Windows, MacOS) and threads. Libraries.	Forensic discovery, Chapter 8	
5	Rootkits and realizing that not everything is as it seems: files, processes, and entire operating systems.	SubVirt paper	
6	Malware analysis basics. Function call hooking, control flow analysis, dynamic binary instrumentation.	OllyDbg manual	
7	Midterm project presentations		Midterm project due. Final project revised proposal due.
8	Collecting data with and from honeypots.	The Honeynet project page	
9	Advanced malware analysis: bypassing packing, obfuscation, and other obstructions	IDA Pro Book, Parts I and II	
10	Advanced malware analysis, part 2: stego, encryption, and virtual machines issues.	IDA Pro Book, Part IV	

Week	Topics Covered	Reading	Assignments
11	Connecting the dots: relating to the network	Real digital forensics, Chapter 2	
12	Finding data on small devices (PDAs, phones, USB sticks, etc.)	Real digital forensics, Chapter 6	
13	Special topics - papers from a recent conference	Recent papers from a relevant conference (e.g. Usenix Security or LEET)	Draft presentations/papers due
14	Final Project presentations		Final Project due