Projected Readings

Wk	Mandia, Prosise, and Pepe	Project Reading	Outside Reading
1 27 Mar	Real World Incidents (Ch 1) Incident Response Process (Ch 2) Preparing for Incident Response (Ch 3)	NIST SP 800-61, Scarfone Grance, andy Masone, Computer Security Incident Handling Guide [1]	Crowley, Corporate Forensics Class Design with Open Source Tools and Live CDs [5]
2 3 Apr	Incident Detection (Ch 4) Live Data Collection Windows Systems (Ch 5) Live Data Collection Unix Systems (Ch 6)	NIST SP 800-86, Kent, Chevalier, Grance, Dang, Guide to Integrating Forensic Techniques into Incident Response [2]	Ciardhuain, An Extended Model of Cybercrime Investigations [6]
3 10 Apr	Forensics Duplication (Ch 7) Collecting Network Based Evidence (Ch 8) Evidence Handling (Ch 9) Computer System Storage Fundamentals (Ch 10)	Garfinkel and Sellat, Remembrance of Data Passed, IEEE Security & Privacy, Jan/Feb 03.	Manson, Is the Open Way a Better Way? [7]
4 17 Apr	Data Analysis Techniques (Ch 11) Analyzing Network Traffic (Ch 14)	Smith, Pros and Cons of using Linux and Windows Live CDs in Incident Handling and Forensics [3]	Carrier, Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers [8]

	Investigating Hacker Tools (Ch 15) Writing Computer Forensic Reports (Ch 17)		
5 24 Apr	Forensic Toolkits	Knopper, Build your own Distro Intro, Linux-Magazine, 2008. [4]	NSA, The Manageable Network Plan [9]
7 1 May	Poster/Portfolio Day	Final Prep	
8 8 May	Final Presentation	Final Presentation	

[1] http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
[2]
http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
[3]
http://www.sans.org/reading_room/whitepapers/incident/pros_and_cons_of_using_linux_and_windows_live_cds_in_incident_handling_and_forensics_1706
[4]
http://www.linux-magazine.com/w3/issue/88/Build_Your_Own_Distro_Intro.pdf
[5]
http://www.tech.uh.edu/cae-dc/documents/CORPORATEForensicsCrowley.pdf
[6
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.80.1289&rep=rep1&type=pdf
[7]
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.1684&rep=rep1&type=pdf
[8]
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.14.9813&rep=rep1&type=pdf
[9]
http://www.nsa.gov/ia/_files/vtechrep/ManageableNetworkPlan.pdf