Day Four

Assignments

Readings

Source	Assignment
Mandia and Prosise	Data Analysis Techniques (Ch 11) Analyzing Network Traffic (Ch 14) Investigating Hacker Tools (Ch 15) Writing Computer Forensic Reports (Ch 17)
Smith	Pros and Cons of using Linux and Windows Live CDs in Incident Handling and Forensics [1]
Carrier	Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. [2]

Class Project
Prepare a brief written plan that describes your goals and your processes for creating your custom IR Kit. You should come to the next class prepared to discuss your plan.

Where appropriate, you may use this assignment to update your project abstract. Post and link both your updated project abstract and your project plan to our Google Group.

Journal Assignment
Read today's class outside reading assignment concerning Live CDs (or Live USBs). Find a current online news article that deals with Live CDs. Articles that deal with Live CDs in a security context are preferred. Write a brief blog entry that explains how that article is relevant to class.

[1]
http://www.sans.org/reading_room/whitepapers/incident/pros_and_cons_of_using_linux_and_windows_live_cds_in_incident_handling_and_forensics_1706

[2]
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.14.9813&rep=rep1&type=pdf