Proposed Topics for FCM 745
Fall 2009

Standard Topics (by week)[1]

1. Network Forensics: definitions and process

2. Legal Considerations for network forensic investigations

3. Internet addressing: IP address, TCP and UDP port numbers, DNS registrations, NAT and DHCP, Traceback Techniques.

4. Capturing network traffic (taps, switches, routers and firewalls)

5. Analysis of logs of network devices

6. Recognizing network traffic associated with malicious activity

7. Intrusion detection

8. Case studies of network forensic investigations: criminal versus those done for security concerns.

Research issues in Network Forensics (by week)

9. ForNet – a distributed network forensics system.

10. Anomaly versus signature based detection systems (e.g., SPAM filters)

11. Web 2.0 vulnerabilities and novel attack vectors (Why everything you learned about network forensics and security now is obsolete).

12. System designs for forensic discovery

13. Floating lecture[2]

14. Floating Lecture

[1] Lectures are based on monographs, papers and web sites that will be available on the course home page.

[2] Floating lectures will be used when needed to discuss projects and assignments.