# Network Forensics Syllabus

## Text/Materials

Network Forensics, Davidoff and Ham, Prentice Hall, ISBN: 0-13-256471-8

## Course Description

This course is an introduction to network forensics. In this course the student will be introduced to digital forensic concepts and practices on local area networks, wide area networks and large scale networks such as the Internet. Use of tools such as packet monitors, security information and event managers (SIEMs), network forensic tools, tracing tools and other tools useful for analyzing events on a network will make up a large part of the course. Material be covered through lecture, demonstration and student hands-on labs. However, this is a "thinking" course where students are required to perform outside research, experiment and draw conclusions. In many lab exercises students will create the attack, run it and then analyze it forensically

## Prerequisite

None

**Where no assignment is shown supplementary readings pertinent to the current environment will be assigned.**

| SESSION | TOPIC | ASSIGNMENT |
|---|---|---|
| 1 | Intro to digital investigation | |
| 2 | Crime assessment | Text Chapter 2 |
| 3 | Technical Fundamentals | Text Chapter 3 |
| 4 | Evidence management | Text Chapter 4 |
| 5 | Packet analysis | |
| 6 | Packet analysis | Text Chapter 5 |
| 6 | Statistical flow analysis | Text Chapter 6 |
| 7 | Wireless networks | Text Chapter 7 |
| 8 | Intrusion detection – Snort lab | Snort configuration |
| 9 | Snort lab | Text Chapter 8 |
| 10 | Using logs – Log lab | |
| 11 | Log lab – ***FINAL PROJECT PROPOSAL DUE!!!*** | Text Chapter 9 |
| 12 | Internetworking devices | Text Chapter 10 |

| | | |
|---|---|---|
| 13 | Internetworking devices | |
| 14 | Web | |
| 15 | Web log lab | Text Chapter 11 |
| 16 | Network tunneling | |
| 17 | Network tunneling | Text Chapter 12 |
| 18 | Malware forensics | |
| 19 | Malware forensics lab | |
| 20 | Following the cybertrail | |
| 21 | Web – Maltego Lab | |
| 22 | Conducting an investigation | |
| 23 | Conducting an investigation | |
| 27 | Work on final projects | |
| 28 | Work on final projects | |
| 29 | Final lab | |
| 30 | Final lab | |
| 31 | Project presentations | |
| 32 | Project presentations | |