STARK STATE COLLEGE

GENERAL SYLLABUS

Course Information

Course Name: Network Forensics
Course Number: CFS287

Required Materials

1. Wireshark 101 Essential Skills for Network Analysis, 2nd Edition, Chappell, 2017, Chappell University., ISBN-987-1-893939-75-2
2. Hands-On Network Forensics, Jaswal, 2019, Packt Publishing., ISBN 978-1-78934-452-3

Required Readings: None

Additional Materials:
1. Windows 10 Operating System (Physical PC, Virtual Machine or Windows to Go)
2. Other materials are available from LMS or furnished by the instructor.

Course Outline/Calendar

The date of coverage and order of coverage may be modified based on the faculty member and events beyond the control of faculty members that interfere with class times and teaching.

Week	Chapter/Topic/Lab
Week 1	• Introduction, Practical Investigative Strategies, User Agent & Network Privacy • Academic Honesty Prerequisite, User Agent Lab
Week 2	• Chapter 0 Skills: Explore Key Wireshark Elements & Traffic Flows • Chapter 1: Introducing Network Forensics • Wireshark Installation Lab
Week 3	• Continue Chapter 0: Skills • Chapter 1 Continued • Wireshark Labs 1-3
Week 4	• Chapter 1 Skills: Customize Wireshark Views & Settings • Chapter 2: Technical Concepts & Acquiring Evidence • Wireshark Labs 4 & 5
Week 5	• Continue with Chapter 1 Skills • Chapter 2: Continued • Wireshark Labs 6-8, • Exam I • Solar Winds Hack Discussion
Week 6	• Nmap, Ethics & Hacking, Chapter 2 Skills: Apply Capture Filters • Chapter 3: Deep Packet Inspection • Wireshark Labs 9-11, • Ethics Lab

Week	Chapter/Topic/Lab
Week 7	• Network Miner, Continue Chapter 2 Skills: • Chapter 3: Continued • Wireshark Labs 12 & 13 • Exercise 1 p. 29-40
Week 8	• Chapter 3 Skills: Apply Display Filters to Focus on Specific Traffic • Chapter 4: Statistical Flow Analysis • Wireshark Labs 14-17 • Exercise 2 p. 40-41 • Open-Source Tool Discussion
Week 9	• Continue Chapter 3 Skills • Chapter 5: Combatting Tunneling & Encryption • Wireshark Labs 18-21, OS Tool Discussion Due
Week 10	• Complete Chapter 3 Skills: • Chapter 6: Investigating Good, Known, & Ugly Malware • Wireshark Labs 22-24, • Exam 2
Week 11	• Chapter 4 Skills: Colors and Export Interesting Packets • Chapter 6: Continued • Wireshark Labs 25-30
Week 12	• Chapter 5 Skills: Build & Interpret Charts & Graphs • Chapter 7: Investigating C2 Servers • Wireshark Labs 31-36
Week 13	• Chapter 6 Skills: Reassemble Traffic for Faster Analysis • Chapter 8: Investigating & Analyzing Logs • Wireshark Labs 37-39 • OWASP Discussion
Week 14	• WEP Encryption, Using Aircrack, Chapter 7 Skills: Add Comments to Your Trace Files & Packets • Chapter 9: WLAN Forensics • Wireshark Labs 40-41
Week 15	• Chapter 8 Skills: Use Command-Line Tools to Capture, Split & Merge Traffic • Chapter 10: Automated Evidence Aggregation & Analysis • Wireshark Labs 42-46 • SANS Poster Discussion
Week 16	• Final Exam