Cyber Investigation – Syllabus

Text/Materials

Incident Response & Computer Forensics, Third Edition Luttgens, Pepe and Mandia McGraw-Hill Education 2014 ISBN 978-0-07-179869-3

Course Description

This course is an introduction to cyber investigation. It focuses digital forensic incident response (DFIR) as well as traditional cyber-crime investigation.. The course will examine investigative techniques for cyber investigators, case studies of representative cyber crimes, cyber crime/crime scene assessment, cyber investigation tools, incident response and analysis, and expert witnessing. There is significant lab work, on-line discussions and a final lab that consists of analysis of a cyber incident. This is a course that incorporates very heavy reading.

Prerequisite

None

COURSE CALENDAR

SESSION	TOPIC	LAB	ASSIGNMENT
1	Defining incident response and building IOCs	Building IOCs	Text chapters 2, 4, 5, 6, 7
2	Data Collection	Data collection	Text chapter 9, 10, 11
3	Network Evidence	Network Analysis	Text chapters 12, 13, 1
4	Platform Evidence	O/S and Apps	Text chapter 16
5	Report Writing		Report Exercise Text chapter 15 and Supplementary Readings
6	Malware Introduction	Malware Lab #1	Supplementary Readings

7	Malware Continued	Malware Lab #2	Supplementary Reading
8	Cyber Crime Assessment (CCA) and Social Media	CCA analysis of Social Media Evidence	Supplementary Readings
9	On-line Predators and Deviants	On-Line Tracing	Supplementary Readings
10	The Dark Web	Dark Web Tracing	Preparation for Incident Exercise #1
11	Start of 2-Week Incident Lab #1		
12	Complete 2-Week Incident Lab #1 and Report		Supplementary Readings
13	Crimeware Tracing	Prep. For Incident Lab #2	
14	Start of Final Incident Lab		
15	Complete Final Incident Lab and Report		