

IS406A Digital Investigation

Spring 2008 SYLLABUS

Hybrid - Tuesdays and Thursdays 18:30 - 20:00 Dewey 106 and NUoodle

Professor Peter R. Stephenson, PhD, CISSP, CISM, FICAF

Office Hours - On Campus (Basement of Dewey): Monday 1400-1600, Wednesday 1400-1600 - Off Campus: AIM as Available

Office: 248-373-2813 - Mobile: 248-760-1152 pstephen@norwich.edu - AIM: NUCISO

Week	Date	Lecture #	Quizes	TOPICS	Readings			Projects
					Stephenson	NUoodle	Additional	
1	15-Jan-07	1		Introduction to Cyber Crime	Ch 1, 2 & 4 BEFORE Class			
	17-Jan-07	2		Introduction to TCP/IP as an Investigative tool			"Introduction to TCP/IP" "Under the Hood of the Internet" "Common UDP and TCP Port Scans and their Meanings"	
2	22-Jan-07	3		Technical Aspects of Cyber Crime - Network Intrusions	Ch 3	Lecture and Discussion questions	The "Script Kiddie Papers" (Know Your Enemy) "Know Your Enemy - Forensics"	
	24-Jan-07	4		Search & Seizure and Human Factors	CH 6			
3	29-Jan-07	5		End-to-End Digital Investigation	CH 5	Lecture and Discussion questions	"Getting the Whole Picture - vol 1"	
	31-Jan-07	6		Investigation Issues	CH 7, 8, 9,10			

4	5-Feb-07	7		Evidence Management		Lecture and Discussion questions	"Electronic Crime Scene Investigation - DoJ"	
	7-Feb-07	8		Incident Post Mortem			"A Comprehensive Approach to Digital Incident Investigation" "Conducting Incident Post Mortems"	
5	12-Feb-07	9		Review Weeks 2-4 and Adore Exercise				
	14-Feb-07	10	Adore Analysis	Specialized tools Lab 1: Link Analysis				
6	19-Feb-07	11		Using Link Analysis to Analyze hacker group		Lecture and Discussion Questions		Hacker Analysis
	21-Feb-07	12		Case Study 1: U.S. v. Parson			"Minnesota Man Sentenced to 18 Months in Prison for Creating and Unleashing a Variant of the MS Blaster Computer Worm"	
7	26-Feb-07	13		Case Study 2: U.S. v Shan		Lecture and Discussion Questions	"China Citizen Pleads Guilty to Unauthorized Access of a Software Company with Intent to Defraud"	U.S. v Shan Analysis
	28-Feb-07	14		Administrative Issues	CH 11, 12, 13			
8	4-Mar-07	15		Intro to Characterizing Incidents with DIPL		Lecture and Discussion Questions	"DIPL Language Manual"	

	6-Mar-07	16		Using DIPL			"DIPL Language Manual"	Analyze U.S. v Parson using DIPL
	8-Mar-07			SPRING BREAK				
	17-Mar-07			SPRING BREAK				
9	18-Mar-07	17	DIPL - Open Book Quiz	U.S. v Parson Analysis Review				
	20-Mar-07	18		ADORE Review			"Expert Qualification and Testimony" to be Read BEFORE Class	
10	26-Mar-07	19		Expert Witnessing Link Analysis Review				
	27-Mar-07	20		Case Preparation Case Study 3: Shadow Crew - Preliminary Analysis			"Six Defendants Plead Guilty in Internet Identity Theft and Credit Card Fraud Conspiracy"	
11	1-Apr-07	21		Case Study 3: Shadow Crew - Advanced Analysis		Lecture and Discussion Questions	"Six Defendants Plead Guilty in Internet Identity Theft and Credit Card Fraud Conspiracy"	
	3-Apr-07	22		Moot Court Case Pre-Analysis Tasks Using EEDI				Pre-Analysis of Moot Court Case
12	8-Apr-07	23		Moot Court Preliminary Correlation, Normalization, Deconfliction				Preliminary Correlation of Moot Court Case
	10-Apr-07	24		Moot Court Second Level Correlation Moot Court Timeline Analysis				Second Level Correlation of Moot Court Case

