

Course Number	CS 415	Course Title	Network Forensics				
Semester Hours	3	Course Coordinator	Henry Hexmoor				
Catalog Description	With the proliferation of wireless networks, security is at odds with privacy and integrity. The course provides a broad overview of security strategies for wireless networks. Topics will range from intrusion detection and network security protocols to collaborative computing. Contemporary tools and techniques for wireless network security are reviewed. A hands on project will be an integral part of this course.						
Textbooks							
Messier, R., 2017. Network Forensics, Wiley press.							
References							
<ul style="list-style-type: none"> • Campbell, R., et al., 2014-2016, Introduction to Digital Forensics, UIUC. • Buttyan, L. and Hubaux, J.P., 2007. Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing, Cambridge University Press. • Northcutt, S. and Novak, A., 2002. Network Intrusion Detection, Sams Publishing. 							
Course Learning Outcomes							
<ul style="list-style-type: none"> • Obtain the state-of-the-art knowledge on network forensic methods including legal concerns • Obtain basic skills in wired and wireless digital data transfer and analysis of digital media 							
Assessment of the Contribution to Student Outcomes							
Outcome →	1	2	3	4	5	6	
Assessed →	X	X	X	X	X	X	
Prerequisites by Topic							
CS 410 or Graduate Standing							

CS 415	Network Forensics	Page 2
Major Topics Covered in the Course		
1. Security of Existing Wireless Networks <ul style="list-style-type: none"> ○ Basics of Wireless networking Vulnerabilities ○ Basics of forensic investigation process 	(10 Lectures) (5 Lectures) (5 Lectures)	
2. Network Intrusion Detection and Analysis and attacks	(6 Lectures)	
3. Analyzing Network Traffic	(4 Lectures)	
4. Packet Dissection Using TCPdump	(4 Lectures)	
5. Mitnick Attack	(2 Lectures)	
6. Cryptographic Algorithms	(2 Lectures)	
7. Game Theory for Wireless Networks	(2 Lectures)	
8. Neighbor Discovery	(4 Lectures)	
9. Shared Spectrum and Secure Protocols	(6 Lectures)	