Digital Forensic Investigation

한림대학교 조슈아 제임스 교수

This course gives an introduction into computer basics, computer security and digital forensic investigation. After learning basic computer concepts, we will focus on conducting digital forensic investigations in computer systems and mobile devices. We will also discuss other potential sources of digital evidence.

차시 (Week)	목차(Major topic)	세부목차(Details)	학습활동 (Learning Activity)
1	Introduction	Introduction to the course	
		Cybercrime and Networks	Quiz
		Cyber Security and Cybercrime	Quiz
2	Security	Cyber Security	Quiz
		How hackers hack	
		How to secure a Windows computer	
		How to secure a Linux computer	
3	Computer Basics	Intro to computer	Quiz
		Introduction to network analysis	
		Password attacks practice	Assignment
4	Cybercrime Investigation	Basics of Cybercrime Investigation	Quiz
		Investigation Methods	Quiz
		Electronic Evidence	Quiz
		Documentation and reporting	Quiz
5	Digital Forensic Science	Forensic investigation Definition	Quiz
		Scientific Method	Quiz
		Procedure	Quiz
6	Forensic Acquisition of Data	Data Storage	Quiz
		Data Structures	Quiz
		Acquire	Quiz
		Hardware Write Blockers	
		Forensic Acquisition in Windows (Forensic Acquisition in Windows using FTK Imager)	
		Forensic Acquisition in Linux	
		Forensic Acquisition in Linux Command Line	
7	Data Recovery	Data Recovery Overview	Quiz
		Data Recovery with Photorec	
		Data Recovery using tsk_recover	
		Data Recovery using The Sleuth Kit	

차시 (Week)	목차(Major topic)	세부목차(Details)	학습활동 (Learning Activity)
8	Relating Data to the Case	Location and Meaning of Data	Quiz
		Starting a case in Autopsy4	
		Processing and Analysis of Disk Image with Autopsy 4 default modules	
		How to use hfind from the command line	
		How to add a hash database to Autopsy 4	
9	Cyber Attack Techniques	Hacking	Quiz
		Malware	Quiz
		Social Engineering	Quiz
10	Random Access Memory Acquisition and Analysis	RAM Acquisition and Analysis	Quiz
		Forensic Memory Acquisition in Windows – FTK Imager	
		Forensic Memory Acquisition in Linux – LiME	
		Digital Forensic Memory Analysis – strings, grep and photorec	
		Digital Forensic Memory Analysis – Volatility	
11	Mobile Device Investigation	Mobile Device Investigations	Quiz
		Mobile Device Acquisition	
12	International Cooperation in Cybercrime	International Nature of Cybercrime	Quiz
		Current State of International Cooperation	Quiz
13	Cybercrime and Digital Forensics Research	Research and the Future of Cybercrime Investigation	Quiz
		Keeping up to date with Digital Forensics	
14	Final Exam	Final Exam	

*** 강좌에 대한 세부 진행은 K-MOOC 사이트에서 확인하시기 바랍니다.**