

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	Mobile Security and Forensics
Course Code:	2ET2070106T
Pre-requisite Course:	Mobile Security Fundamental Knowledge

Course Objectives: After successful completion of the course, student will be able to

1. Describe basic principles of digital forensics and identify the unique challenges involved in mobile forensics.
2. Describe mobile ecosystem security mechanisms and risks
3. Explain and apply the procedures of the validation, preservation, acquisition, examination, analysis and reporting of digital information from a mobile device. Explain and compare the internals of iphone and android platforms such as hardware, OS architectures and file systems. Explain and compare the jailbreaking process for iphone and rooting process for android phones
4. Explain and compare various data acquisition and analysis techniques used in mobile forensics.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)									Total (Marks)
					Theory (Marks)				Practical (Marks)					
	L	T	P	Total	SEE		CCA		SEE		CCA			
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.		
3	3	-	-	3	24	60	16	40	-	-	-	-	100	

Course Contents:

Unit No	Topics	Total Hours	Weight age (%)
1	Introduction to mobile forensics: Statistics, Feature phones vs. smartphones, challenges, policies and guidelines, mobile forensics tools (5 levels), Process (identification, preparation, isolation, acquisition, authentication, analysis, presentation, archiving)	07	10
2	Introduction to Mobile Ecosystem Systems: hardware components, SIM card UICC, cellular network (CDMA vs. GSM vs TDMA vs iDEN vs. LTE) & Mobile IP (wifimax) , Mobile Operating Systems Overview(Android, IOS, Windows Phone, Blackberry), App Stores, Forensics & Security	06	10
3	Internals of Android Devices: Android Device Hardware, Android OS (history, architecture, booting process, Fragmentation), File System and Data Storage, Android application Android Security: rooting, malware Forensics Environment Setup and Tools: Android SDK, Android Debug Bridge, Forensics CE, Linux VM, commercial tools Acquisition from Android Devices: bypass passcode, Imaging specification, Memory & Sim acquisition, Physical acquisition: acquire all data including deleted one, logical acquisition: acquire allocated data, acquisition from backup files, verification of acquisition Android Forensic Analysis and reporting: Evidence sources (ids, contact, sms, phone logs, audio/video/image etc), Timeline analysis, File System analysis, Application analysis, Data recovery	16	40

4	IOS Security Issues: jailbreak, malware IOS Forensics Environment setup and Tools: Encase? Iphone analyzer, VM setup? Preservation & Acquisition from iOS Devices: bypass the passcode, Physical acquisition, logical acquisition: acquire allocated data, acquisition from iTunes/iCloud backup IOS Forensic Analysis & Reporting: Timeline analysis , File System analysis, Application analysis, Database analysis Windows Phone & Blackberry: windows phone security mechanism, acquisition & analysis Blackberry phone security mechanism, acquisition & analysis Mobile Network Related Issues: (cellular network, wifi, cloud ...)	16	40
---	---	----	----

Text Books:

1. Practical Mobile Forensic by Satish Bommisetty, Rohit Tamma and Heather Mahalikunder Packet Publishing
2. Learning Android Forensics, Tamma & Tindall, ISBN-13: 978-1782174578

Reference Books:

1. <https://www.nist.gov/system/files/documents/forensics/5-Punja-nist-2014-bbforensics- FULL.pdf>
2. https://en.wikipedia.org/wiki/List_of_Android_smartphones
3. subscription.packtpub.com/book/application_development/9781783288311/10
4. <https://study.com/academy/lesson/data-extraction-techniques-for-androiddevices-logicalphysical.html#:~:text=Gaining%20root%20access%20to%20the,%2Doff%2C%20micro%20read.> manual-20and%

List of Open-Source Software/learning website:

1. <http://sourceforge.net/projects/iphoneanalyzer/>
2. <https://www.nowsecure.com/forensics/community/>
3. <http://www.zdziarski.com/blog/?p=2287>
4. http://www.cftt.nist.gov/mobile_devices.htm
5. <http://appleExaminer.com>
6. <https://www.nowsecure.com/blog/>

Course Learning Outcomes (CLO):

Course Outcomes	Description	Bloom's Taxonomy Level
COL1	Understand what data is able to be acquire from mobile devices and be able to acquire and investigate data from mobile devices using forensically sound and industry standard tools	Understanding (2) Applying (3)
COL2	Understand the relationship between mobile and desktop devices in relationship to a criminal and corporate investigations	Applying (3)
COL3	Be able to analyze mobile devices, their backup files, and artifacts for forensic evidence	Applying (3)
COL4	Different forensic tools that are used for various mobile platforms	Applying (3)

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	H	M	M		M											
CLO2	H	M			M							L				
CLO3	H	M	M		M											
CLO4	M	M	M		M							L				
CLO5	M	M										L				

H: High, M: Medium, L: Low