CO4	This course on mobile and digital forensics will provide a better understanding for these course participants on different forms of evidences in many digital devices,collections and interpretation of the same.

S. NO	Contents	Hours

UNIT 1	Overview of wireless technologies and Security: Personal Area networks,Wireless Local Area Networks, Metropolitan Area Networks,Wide Area Networks.	**4**
UNIT 2	Wireless threats, Vulnerabilities and Security: Wireless LANs,War Driving,War Chalking,War Flying,Common Wi-fi security recommendations,PDA Security,Cell phones and Security,Wireless DoS attacks,GPS Jamming, Identity theft.	**8**
UNIT 3	CIA triad in mobile phones-Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Netmonitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues	**10**
UNIT 4	Mobile phone forensics: crime and mobile phones, evidences, forensic procedures, files present in SIM card, device data, external memory dump, evidences in memory card, operators systems- Android forensics: Procedures for handling an android device, imaging android USB mass storage devices, logical and physical techniques10	**10**
UNIT 5	Digital forensics: Introduction – Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential- Device handling: seizure	**10**
	TOTAL	**42**