CO's-PO's & PSO's MAPPING

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3	3	3	3	1	-	-	-	2	1	1	2	2	1
2	1	3	2	1	2	-	-	-	3	2	2	2	2	1
3	1	1	2	3	2	-	-	-	1	1	1	3	1	1
4	3	1	2	1	3	-	-	-	3	2	1	2	3	2
5	2	3	3	3	3	-	-	-	3	1	1	1	2	1
AVg.	2	2.2	2.4	2.2	2.2	-	-	-	2.4	1.4	1.2	2	2	1.2

1 - low, 2 - medium, 3 - high, '-' - no correlation

CCS343 DIGITAL AND MOBILE FORENSICS L T P C
2 0 2 3

COURSE OBJECTIVES:

- To understand basic digital forensics and techniques.
- To understand digital crime and investigation.
- To understand how to be prepared for digital forensic readiness.
- To understand and use forensics tools for iOS devices.
- To understand and use forensics tools for Android devices.

UNIT I INTRODUCTION TO DIGITAL FORENSICS 6

Forensic Science – Digital Forensics – Digital Evidence – The Digital Forensics Process – Introduction – The Identification Phase – The Collection Phase – The Examination Phase – The Analysis Phase – The Presentation Phase

UNIT II DIGITAL CRIME AND INVESTIGATION 6

Digital Crime – Substantive Criminal Law – General Conditions – Offenses – Investigation Methods for Collecting Digital Evidence – International Cooperation to Collect Digital Evidence

UNIT III DIGITAL FORENSIC READINESS 6

Introduction – Law Enforcement versus Enterprise Digital Forensic Readiness – Rationale for Digital Forensic Readiness – Frameworks, Standards and Methodologies – Enterprise Digital Forensic Readiness – Challenges in Digital Forensics

UNIT IV iOS FORENSICS 6

Mobile Hardware and Operating Systems - iOS Fundamentals – Jailbreaking – File System – Hardware – iPhone Security – iOS Forensics – Procedures and Processes – Tools – Oxygen Forensics – MobilEdit – iCloud

UNIT V ANDROID FORENSICS 6

Android basics – Key Codes – ADB – Rooting Android – Boot Process – File Systems – Security – Tools – Android Forensics – Forensic Procedures – ADB – Android Only Tools – Dual Use Tools – Oxygen Forensics – MobilEdit – Android App Decompiling

COURSE OUTCOMES:

On completion of the course, the students will be able to:

CO1: Have knowledge on digital forensics.

CO2: Know about digital crime and investigations.

CO3: Be forensic ready.

CO4: Investigate, identify and extract digital evidence from iOS devices.

CO5: Investigate, identify and extract digital evidence from Android devices.

30 PERIODS

LAB EXPERIMENTS: 30 PERIODS

1. Installation of Sleuth Kit on Linux. List all data blocks. Analyze allocated as well as unallocated blocks of a disk image.
2. Data extraction from call logs using Sleuth Kit.
3. Data extraction from SMS and contacts using Sleuth Kit.
4. Install Mobile Verification Toolkit or MVT and decrypt encrypted iOS backups.
5. Process and parse records from the iOS system.
6. Extract installed applications from Android devices.
7. Extract diagnostic information from Android devices through the adb protocol.
8. Generate a unified chronological timeline of extracted records,

TOTAL:60 PERIODS

TEXT BOOK:

1. Andre Arnes, “Digital Forensics”, Wiley, 2018.
2. Chuck Easttom, “An In-depth Guide to Mobile Device Forensics”, First Edition, CRC Press, 2022.

REFERENCES

1. Vacca, J, Computer Forensics, Computer Crime Scene Investigation, 2nd Ed, Charles River Media, 2005, ISBN: 1-58450-389.

CO’s-PO’s & PSO’s MAPPING

CO’s	PO’s												PSO’s	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3	1	3	2	1	-	-	-	1	1	3	3	1	3
2	3	3	3	3	3	-	-	-	2	2	1	2	1	3
3	3	3	2	3	1	-	-	-	3	2	1	1	3	2
4	3	1	2	2	3	-	-	-	1	3	3	2	1	3
5	1	3	2	3	2	-	-	-	2	3	2	3	1	2
AVg.	3	2	2	3	2	-	-	-	2	2	2	2	1	3

1 - low, 2 - medium, 3 - high, ‘-' - no correlation

CCS339 CRYPTOCURRENCY AND BLOCKCHAIN TECHNOLOGIES L T P C

2 0 2 3

COURSE OBJECTIVES:

- To understand the basics of Blockchain
- To learn Different protocols and consensus algorithms in Blockchain
- To learn the Blockchain implementation frameworks
- To understand the Blockchain Applications
- To experiment the Hyperledger Fabric, Ethereum networks