COMPUTER FORENSICS

(NON CSE & IT)

CourseCode:20CS11Q1

L	T	P	C
3	0	0	3

Course Outcomes: At the end of the course a student will be able to:

CO1: Outline the types of forensics technologies and services (L2)

CO2: Examine forensic evidence and preservation of digital evidence (L3)

CO3: Illustrate about networks and reconstructing past events (L3)

CO4: Demonstrate about the surveillance tools for information warfare in future (L3)

CO5: Examine advanced computer forensics (L3)

UNIT-I: (10 Lectures)

Computer Forensics Fundamentals: Use of forensics in Law enforcement, Employment proceedings, Services, Benefits of professional forensics methodology, Steps taken by computer forensics specialists

Types of Forensics Technology: Types of military forensics technology, Types of law enforcement in forensics technology, Types of business forensics technology.

Types of forensics services: Risk-management techniques, Forensics investigative services, Forensic process improvement

Learning Outcomes: At the end of the unit, student will be able to

1. Discuss about benefits of forensics technology (L2)
2. Demonstrate different types of forensics technologies (L3)
3. Discuss about forensic services (L2)

UNIT-II: (10 Lectures)

Computer Forensics Evidence: Data backup and recovery, Data recovery solution, Evidence collection and obstacles, Types and rules of evidence, Methods of collection, Artifacts and collection steps.

Preservation of Digital Evidence: Preserving digital crime scene, computer evidence processing steps, Legal aspects of collecting and preserving evidence

Learning Outcomes: At the end of the unit, student will be able to

1. Explain about the data backup and recovery process (L2)
2. Discuss about the methods of collecting evidence (L2)
3. Explain about the process of evidence processing (L2)

UNIT-III: (10 Lectures)

Identifying data and Reconstructing past events: Forensics identification and analysis of technical surveillance devices, Useable file formats, unusable file formats, converting files.

Networks: A technical approach, Destruction of email, Damaging computer evidence, Documenting the intrusion of destruction of data, system testing.

Learning Outcomes: At the end of the unit, student will be able to

1. Discuss about the analysis of surveillance devices (L2)
2. Explain the usable and un usable file formats (L2)
3. Discuss about the destruction of email (L2)

UNIT-IV: (10 Lectures)

Information Warfare: E-bombs, Emp effect, Snoop, sniff and snuff tools, Email wiretaps, spy dust balls and mechanical dragonflies, Nanotechnology

Surveillance tools for Information warfare in future: Cyber surveillance, Cyber footprint and criminal tracking, Implications of cookies and integrated platforms, Data mining for what? The wireless internet.

Learning Outcomes: At the end of the unit, student will be able to

1. Discuss about E-bombs, Snoop, Sniff and snuff tools (L2)
2. Explain about nanotechnology (L2)
3. Demonstrate the surveillance tools for information warfare (L3)

UNIT-V: (10 Lectures)

Advanced Computer Forensics: Advanced Encryption, Advanced hacking, Source addresses, the problem of present, The outlook for future, Summary, Conclusions, Recommendations, Computer Forensics needs and challenges.

Learning Outcomes: At the end of the unit, student will be able to

1. Explain about Advanced Encryption (L3)
2. Discuss Conclusions and recommendations of advanced computer forensics (L2)
3. Explain the needs and challenges of advanced computer forensics (L2)

TEXT BOOKS:

1. John R.Vacca, Computer Forensics: Computer crime scene investigation.

REFERENCE BOOKS:

A Practical Guide to Computer Forensics Investigations Dr. Darren R. Hayes, 2014

WEB REFERENCES:

https://in.coursera.org/specializations/computerforensics