MCA532D– DIGITAL FORENSICS

Total Teaching Hours for Semester: 30 Max Marks: 50 Credits: 2

Course Objectives

To provide extensive knowledge about computer forensic and recognize diverse aspects of forensics science. It is also used to covering the fundamental principles, methodologies, and tools used to collect, preserve, analyze, and present digital evidence in legal proceedings.

Course Outcomes

Upon successful completion of the course, the student will be able to

CO1: Apply various tools and techniques for acquiring and analysing digital evidence and interpret and document digital evidence findings.

CO2: Analyse best practices for handling and preserving digital evidence.

Unit-1 Teaching Hours: 6

FUNDAMENTALS OF DIGITAL FORENSICS

Definition and scope of digital forensics - History of digital forensics -Digital Evidence-Increasing awareness of Digital Evidence-Types of digital evidence -Challenging aspects of digital Evidence- **Legal and ethical considerations** – Laws and regulations- Rules of evidence-Chain of custody -Standards and best practices.

Unit-2 Teaching Hours: 6

DIGITAL EVIDENCE ACQUISITION

Data acquisition methods -Incident response and first responders- **Imaging techniques** – Bitstream Imaging-Logical Imaging-Live and Memory Imaging-Volatility and live response -**Network forensics** – Packet capture -Log Analysis-Timeline Analysis-Malware Analysis-**Cloud forensics** – Data collection and preservation- Legal and Jurisdictional considerations -Cloud Service Models-Meta data Analysis- Mobile forensics

Unit-3 Teaching Hours: 6

DIGITAL EVIDENCE ANALYSIS

File system analysis -File System identification and Acquisition- File Carving- File system journal and logs- Registry analysis -**Memory forensics** -Memory Imaging and Analysis-Artifact extraction- Timeline Analysis-Malware analysis -**Data carving and steganography** – Definition- Process- Use Cases- Tools and techniques

Unit-4 Teaching Hours: 6

DIGITAL EVIDENCE INTERPRETATION & REPORTING

Analysing and interpreting evidence - **Documenting findings** – Incident tracking- Written reports- **Reporting procedures** – Evidence collection- Analysis Methodology- Findings and Observations- Interpretation of Evidence- **Expert witness testimony** – Qualification as an expert- Expert opinion and report- Cross examination- Redirect examination

Unit-5 Teaching Hours: 6

EMERGING TRENDS IN DIGITAL FORENSICS

Big data and forensics – Challenges of data volume and variety, data acquisition and collection-real time forensics - Internet of Things (IoT) forensics - **Social media forensics** – User Profiling-Content and Sentiment Analysis- Geolocation and Network Analysis- **Blockchain forensics** – Understanding Blockchain Technology-Address and Wallet Analysis-Cryptocurrency Mixers and Tumblers

Text Books and Reference Books

[1] Digital Forensics & Incident Response by Chuck Easttom , Jones and Bartlett Publishers, Inc, 4th Edition, 2021

[2] Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation" by Lee Reiber, McGraw-Hill Education, 2nd Edition, 2019

[3] Digital Forensics and Incident Response: A Practical Guide to Deploying Forensic Techniques in Response to Cyber Security Incidents, Gerard Johansen, Apress, 3rd Edition,2017

[4] Digital Forensics with Kali Linux: Perform data acquisition, digital investigation, and threat analysis using Kali Linux tools, Shiva V. N Parasram, Packt Publishing, 2020

[5] Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Eoghan Casey, Brent E. Turvey, and James M. O. E. Bernard, Academic Press, 5th Edition, 2019

[6] Emerging Trends in ICT Security: Big Data Analytics, Cloud Computing, Internet of Things Forensics,Babak Akhgar, David Waddington, and Hamid Jahankhani ,Elsevier Science, 2013

Essential Reading / Recommended Reading

[1] Photo Forensics, Hany Farid, The MIT Press, 1st Edition, 2019.

[2] Fake Photos, Hany Farid, The MIT Press, 1st Edition, 2019.

[3] The Practice of Crime Scene Investigation, John Horswell, CRC Press, 2016.

Web Resources:

1. https://www.udemy.com/topic/digital-forensics/
2. www.forensicscience.ufl.edu
3. www.handbook.uts.edu.a

CO – PO Mapping

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	2	3	3	1	2	2	3	1	2	2
CO2	1	1	1	2	2	3	1	1	1	2	1	2