Lesson Plan of Mrinal Kanti Bhowmik

Name of the Subject: Digital Forensics

Subject Code: CSE 1001 E1

	Topic	Contact Hours	Contact Occurred on	Remarks
Class 1:	**Introduction to Digital Forensics** − Definition of digital forensics and computer forensics and its principles − Cyber-crime and computer based crime − Evolution of computer forensics − Stages of computer forensics process − Benefits of computer forensics − Uses of computer forensics − Objectives of computer forensics − Role of forensics investigator − Forensics readiness its goals, benefits and steps for effective Forensic Readiness Planning − Understanding the legal and ethical considerations in digital forensics. Reference Books/ e-books/ Research Articles: 1. Digital evidence and computer crime Forensic science, computers, and the internet. Third edition: E. Casey, 2011. 2. Digital image forensics: HT Sencar, N Memon, 2013. 3. Multimedia forensics: H. T. Sencar, L. Verdoliva, & N. Memon, 2022.	**04:00**		
Class 2:	**Computer Crime Investigation & Different types of Acquiring Evidence or Crime Scene Management and Forensic Evidence** − Introduction to digital evidence − Techniques for acquiring digital evidence from various sources (hard drives, USB drives, mobile devices, cloud storage) − Initial decision making system − Chain of custody and preserving evidence integrity. − Crime Scene Management: • Introduction to the crime scene, Types of Crime Scene, Evaluation and processing of crime scene of crime, Documenting the crime scene (Note making, sketching, photography, videography of crime scene), role of the first arriving officer at the crime scene. • Searching techniques of crime scene, processing of physical evidence-discovering, recognizing and examination of physical evidence. • Preservation, packaging, sealing, labelling and forwarding of physical evidence, maintaining the chain of custody, probative value of physical evidence, reconstruction of scene of crime.	**04:00**		

	• Introduction to physical evidences, Types of physical evidences, classification and role of physical evidences in criminal investigations & Trails. Reference Books/ e-books/ Research Articles: 1. Digital evidence and computer crime Forensic science, computers, and the internet. Third edition: E. Casey, 2011. 2. An introduction to criminalistics: C. E. O'hara, & J. W. Osterburg, (1952). 3. Dahiya M S, Crime scene management: a scientific approach; Shanti SarvarPrakashan 4. R. Saferstein; Forensic Science Handbook, Vols. I, 11; (Ed); Prentice Hall, Eaglewood Cliffs,NJ; 5. F.W. Sears, M.W Zernansky, and H. D. Young; University Physics, Sixth Ed.,Narosa; 6. D. Shaw, Physics in the prevention and detection of crime. Contemporary Physics, 17(4), 307-330, 1976.			
Class 3:	**File Systems** − Understanding different file systems (NTFS, FAT, ext4, HFS+) − File system analysis techniques for digital forensics Reference Books/ e-books/ Research Articles: 1. Operating systems internals and design principles: W. Stallings, 1998. 2. File system forensic analysis: B. Carrier, Addison-Wesley Professional, 2005. 3. Guide to computer forensics and investigations: B. Nelson, A. Phillips, & C. Steuart, 2010. 4. Digital forensics and incident response: G. Johansen, 2017.	**03:00**		
Class 4:	**Open-Source Forensic Tools** − Introduction to popular open-source forensic tools (Autopsy, Sleuth Kit, Volatility, Wireshark, Photo forensics) − Hands-on exercises with open-source tools for evidence analysis Reference Books/ e-books/ Research Articles: 1. Practical digital forensics: R. Boddington, 2016. 2. Performing File Forensics on Windows 10 FAT 32 and NTFS File Systems using The Sleuth Kit (Autopsy Wrapper): U. Salter, 2023.	**03:00**		
Class 5:	**Windows / Mac / Linux Forensics** − Platform-specific forensic analysis techniques for Windows, Mac, and Linux operating systems − Identifying artifacts and conducting investigations on each platform Reference Books/ e-books/ Research Articles: 1. Digital forensics with open source tools: H. Carvey, & C. Altheide, 2011.	**03:00**		

	2. Practical forensic imaging: securing digital evidence with Linux tools: B. Nikkel, 2016.			
Class 6:	**Advanced Windows Forensics** − Registry analysis − Link file analysis − Event log analysis Reference Books/ e-books/ Research Articles: 1. The Art of memory forensics: detecting malware and threats in windows, linux, and Mac memory: M. H. Ligh, A. Case, J. Levy, & A. Walters, 2014. 2. Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices: R. Tamma, O. Skulkin, H. Mahalik, & S. Bommisetty, 2020.	**03:00**		
Class 7:	**Programming for Digital Forensics** − Introduction to scripting languages (Python, PowerShell) for digital forensics − Writing scripts to automate forensic tasks and data analysis Reference Books/ e-books/ Research Articles: 1. Integrating python with leading computer forensics platforms: C. Hosmer, 2016. 2. Learning Python for Forensics: Leverage the power of Python in forensic investigations: P. Miller, & C. Bryce, 2019.	**04:00**		
Class 8:	**Application & Database Forensics** − Database designing Protocol for Forensics analysis − Creation of Forge data for Forensics analysis − Recovering and analyzing data from various applications and databases Reference Books/ e-books/ Research Articles: 1. File system forensic analysis: B. Carrier, 2005. 2. Guimaraes, M. A., Austin, R., & Said, H. (2010, October). Database forensics. In 2010 Information Security Curriculum Development Conference (pp. 62-65).	**04:00**		
Class 9:	**Network Forensics** − Understanding network protocols and traffic analysis − Investigating network-based attacks and intrusions Reference Books/ e-books/ Research Articles: 1. Network forensics: tracking hackers through cyberspace: S. Davidoff, & J. Ham, 2012. 2. The practice of network security monitoring: understanding incident detection and response: R. Bejtlich, 2013. 3. Practical packet analysis: Using Wireshark to solve real-world network problems: C. Sanders, 2017.	**03:00**		
Class 10:	**Volatile Memory Analysis**			

	− Techniques for analyzing volatile memory (RAM) for forensic evidence − Extracting volatile data and analyzing it for indicators of compromise <u>Reference Books/ e-books/ Research Articles:</u> 1. Windows forensic analysis toolkit: advanced analysis techniques for Windows 8: H. Carvey, 2014. 2. The Art of memory forensics: detecting malware and threats in windows, linux, and Mac memory: M. H. Ligh, A. Case, J. Levy, & A. Walters, 2014. 3. Practical forensic imaging: securing digital evidence with Linux tools: B. Nikkel 2016.	**03:00**		
Class 11:	**Malware Analysis** − Understanding malware behavior and characteristics − Analyzing malware samples to determine their functionality and impact <u>Reference Books/ e-books/ Research Articles:</u> 1. Malware analyst's cookbook and DVD: tools and techniques for fighting malicious code: M. Ligh, S. Adair, B. Hartstein, & M. Richard, 2010. 2. Practical malware analysis: the hands-on guide to dissecting malicious software: M. Sikorski & A. Honig, 2012.	**03:00**		
Class 12:	**Threat Hunting & Incident Response** − Proactive threat hunting methodologies − Incident response strategies and best practices <u>Reference Books/ e-books/ Research Articles:</u> 1. The practice of network security monitoring: understanding incident detection and response: R. Bejtlich, 2013. 2. Hunting cyber criminals: a hacker's guide to online intelligence gathering tools and techniques: V. Troia, 2020.	**04:00**		
Class 13:	**Audio Recognition and Video Analysis** − Introduction to voice identification/speaker recognition, speech enhancement. − Speaker Profiling: Segregation of speech samples, auditory analysis/listener's approach, spectographic approach or voiceprint analysis, Automatic speaker recognition technique. − Video processing and enhancement, video auhenticition, hash value generation. − Video Analysis: Frame Extraction, frame by frame analysis, shot by shot analysis. − Technical aspacts of the video, collection, handling and prservation of video files. <u>Reference Books/ e-books/ Research Articles:</u> 1. Beigi, H., & Beigi, H. (2011). Speaker recognition (pp. 543-559). Springer US. 2. S. Singh, Forensic and Automatic Speaker Recognition System. International Journal of	**04:00**		

Electrical & Computer Engineering (2088-8708), 8(5), 2018. 3. Robustness-related issues in speaker recognition: T. F. Zheng, & L. Li, 2017. 4. Digital video processing: A. M. Tekalp, 2015. 5. Handbook of video databases: design and applications: B. Furht, & O. Marques 2003.			
Class 14: Image and Video Forensics/ Multimedia Forensics - I − Introduction to digital forgery − Taxonomy for digital forgery. − Different challenges for forgery detection − Basic steps of the image/ video forensic investigation process − Challenges faced during forged content creation. − Tools used by the research community for creation of forged media content. − Encoder-decoder frameworks for forged object localization in images/ videos − Classification models for forged and authentic image classification. − Performance evaluation metrics used for measuring the robustness of forgery detection methods. Reference Books/ e-books/ Research Articles: 1. Digital evidence and computer crime Forensic science, computers, and the internet. Third edition: E. Casey, 2011. 2. Digital image forensics: HT Sencar, N Memon, 2013. 3. Multimedia forensics: H. T. Sencar, L. Verdoliva, &amp; N. Memon, 2022. 4. Schuld, Maria, Ilya Sinayskiy, and Francesco Petruccione. "The quest for a quantum neural network." Quantum Information Processing 13 (2014): 2567-2586. 5. Jia, Z. A., Yi, B., Zhai, R., Wu, Y. C., Guo, G. C., & Guo, G. P. (2019). Quantum neural network states: A brief review of methods and applications. Advanced Quantum Technologies, 2(7-8), 1800077. 6. Beer, K., Bondarenko, D., Farrelly, T., Osborne, T. J., Salzmann, R., Scheiermann, D., & Wolf, R. (2020). Training deep quantum neural networks. Nature communications, 11(1), 808. 7. Verdoliva, L. (2020). Media forensics and deepfakes: an overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 910-932.	**04:00**		
Class 15: Image and Video Forensics/ Multimedia Forensics - II − Deep Fake, its Types, and Challenges − Conventional blind methods for forgery detection − Parameters used for analysis of the quality of the forged datasets − Concept and need of metadata information for forgery detection in images/ videos.	**04:00**		

– Photo-response non-uniformity (PRNU) based forgery localization – Long short-term memory (LSTM) networks for forgery detection – Domain adaptation models in context of forgery detection tasks. – Quantum Neural Network in context of forgery detection tasks. <u>Reference Books/ e-books/ Research Articles:</u> 1. Digital evidence and computer crime Forensic science, computers, and the internet. Third edition: E. Casey, 2011. 2. Digital image forensics: HT Sencar, N Memon, 2013. 3. Multimedia forensics: H. T. Sencar, L. Verdoliva, &amp; N. Memon, 2022. 4. Schuld, Maria, Ilya Sinayskiy, and Francesco Petruccione. "The quest for a quantum neural network." Quantum Information Processing 13 (2014): 2567-2586. 5. Jia, Z. A., Yi, B., Zhai, R., Wu, Y. C., Guo, G. C., & Guo, G. P. (2019). Quantum neural network states: A brief review of methods and applications. Advanced Quantum Technologies, 2(7-8), 1800077. 6. Beer, K., Bondarenko, D., Farrelly, T., Osborne, T. J., Salzmann, R., Scheiermann, D., & Wolf, R. (2020). Training deep quantum neural networks. Nature communications, 11(1), 808. 7. Verdoliva, L. (2020). Media forensics and deepfakes: an overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 910-932.			