Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science
B.Sc. Hons. Digital & Cyber Forensics- Batch (2023-26)
SEMESTER-III

BDCF301-Fundamentals of Online Social Network Forensics

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL		L	T	P	CREDITS
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*				
BDCF301	Major I	Fundamentals of Online Social Network Forensics	60	20	20	60	40	4	0	4	6

Legends: **L** - Lecture; **T** - Tutorial/Teacher Guided Student Activity; **P** – Practical: **C** - Credit; Th. - Theory
*__Teacher Assessment__ shall be based on following components: Quiz/Assignment/ Project/Participation in Class, given that no component shall exceed more than 10 marks.

COURSE OBJECTIVES

The student will have ability:

1. Understand the fundamentals of social media networks
2. Understand dynamics and evolution of social networks.
3. Acquainted to protect personal data, securing simple computer networks, and safe Internet Usage

COURSE OUTCOMES:

Upon completion of the subject, students will be able to:
1. Secure both clean and corrupted systems, protecting personal data, securing simple computer networks, and safe Internet usage.
2. Understand dynamics and evolution of social networks.
3. Understand the framework of network analysis.
4. Understand how various social media networks are working and using SNA in their infrastructure.

UNIT I Cyber Laws:

Introduction to the Legal Perspectives of Cybercrimes and Cyber security, Cybercrime and the Legal Landscape around the World, Why Do We Need Cyber laws, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act, Digital Signatures and the Indian IT Act, Cybercrime and Punishment, Cyber law, Technology and Students: Indian Scenario.

UNIT II Cyber Ethics:

Ethics, Legal Developments, Cyber security in Society, Security in cyber laws case studies, General Law and Cyber Law-a Swift Analysis. Private ordering solutions, Regulation and Jurisdiction for global Cyber security, Copy Right source of risks, Pirates, Internet Infringement, Fair Use, Postings, and Criminal Liability.

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science
B.Sc. Hons. Digital & Cyber Forensics- Batch (2023-26)
SEMESTER-III

UNIT III Social Media and Network Analysis: Phenomenology of Social Media, Network Analysis Types of Networks: General Random Networks, Small World Networks, Scale-Free Networks; Examples of Information Networks; Network Centrality Measures; Strong and Weak ties. Influence and Centrality in Social Networks. Basic of Sentiment Analysis.

UNIT IV Social Media Behaviour: Social Ties and Information Diffusion. Social Ties and Link Prediction, Social Network Analysis and Online Social Networks -Concepts: How Services such as Facebook, LinkedIn, Twitter, Couch Surfing, etc. are using SNA to understand their users and improve their functionality.

UNIT V Security and Privacy in Social Network: Privacy in a Networked World, Social Spam and Malicious Behaviour, Sybil attack, distributed denial of service attack, Leakage and Linkage of user information and content, predicting the future with social media, Friendship paradox and detection of contagions.

List of Practical:

1. Case study of current IT act related cases.
2. Case study of Cyber Crimes.
3. Case study of IT law related real life examples.
4. Practical analysis of Social Networking sites.
5. Practical analysis of Networks.
6. Finding out the vulnerable data on Social Networking sites.
7. Find out attacks on Social networking sites.
8. Practical analysis of Malwares in Social Networking sites.
9. Case study of Social Networking related crimes

References

1. Sunit Belapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd, 2011.
2. John Scott, Social Network Analysis, 3rd Edition, SAGE, 2012.
3. Wouter de Nooy, Andrej Mrvar, Vladimir Batagelj, Exploratory Social Network Analysis with Pajek, 2nd Revised Edition, Cambridge University Press, 2011
4. Patrick Doreian, Frans Stokman, Evolution of Social Networks, Routledge, 2013.

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science
B.Sc. Hons. Digital & Cyber Forensics- Batch (2023-26)
SEMESTER-III

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL		L	T	P	CREDITS
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*				
BDCF502	Minor 1	Memory Forensics	60	20	20	60	40	4	0	4	6

Legends: **L** - Lecture; **T** - Tutorial/Teacher Guided Student Activity; **P** – Practical: **C** - Credit; Th. - Theory
*__Teacher Assessment__ shall be based on following components: Quiz/Assignment/ Project/Participation in Class, given that no component shall exceed more than 10 marks.

Learning Objectives:

1. Memory Analysis in Incident Handling
2. Network Connection Analysis
3. Understanding Memory Artifacts
4. Live Response of Memory Analysis using various Tools

Learning Outcomes: upon completion of the subject student will be able to know the

1. Integration with Incident Handling
2. Memory Imaging Skills
3. Malware Identification
4. Incident response proficiency

UNIT-I: Introduction to Memory Forensics

Memory Forensics Examinations, Tools for memory acquisition, Identify Rogue Processes, Analyze Process DLLs and Handles, Review Network Artefacts, Looking for Evidence of Code Injection, Checking for Signs of a Rootkit, Acquire Suspicious Processes and Drivers, Advanced Memory Analysis with Volatility, Code Injection, Malware, and Rootkit Hunting in Memory

UNIT-II Memory Extraction Techniques

Perform In-Memory Windows Registry Examinations, Extract Typed Adversary Command Lines, Investigate Windows Services, Hunting Malware Using Comparison Baseline Systems, Dumping Hashes and Credentials from Memory, Prefetch and Shimcache Extraction via Memory

UNIT-III Memory Analysis Techniques

Memory Analysis Techniques with Redline and Rekall Framework, identifying malware infection from memory using volatility workbench

UNIT-IV Collecting Live responses using various distribution and Volatile data

Live response using Linux distributions, use of Kali Linux, D.E.F.T., SANS SIFT work station, collecting volatile data – kernel version, login history, network connections, running processes, loaded kernel modules, system logs, Dumping RAM, use of LiME, volatility profiles

UNIT-V:SmartPhoneForensics

Smartphone forensics – Introduction to a smartphone, smartphone components, and identifiers, the forensic impact of flash memory, preserving smartphone evidence, forensic acquisition process, logical, file system, and physical acquisition, introduction to forensic tools for smartphone, android memory capturing, introduction to JTAG technology, introduction to a cellular network, different cellular networks – GSM, GPRS, EDGE, UMTS, LTE, VOLTE Generations and evolution of a cellular network, the structure of mobile phone cellular network, cell site (base transceiver station)

Practicals

1. Analyze the malicious process from various memory samples
2. Identify malicious network activities from given memory samples
3. Analyze the memory sample and extract the User ID, password, and Name of the computer, and use other volatility plugins
4. Acquire the physical memory of the system using various tools
5. Identify the user mode rootkit from the memory sample
6. Identify kernel-mode rootkit from memory sample
7. Analyze the memory sample using a redline
8. Memory acquisition and creating volatility profile of Linux distro
9. Acquire data from a mobile phone

References

1. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware by Monnappa K. A.
2. Linux Forensics - With Python and Shell coding by Philip Polstra
3. Computer Forensics: Computer Crime Scene Investigation by John R. Vacca
4. Malware Forensic Field Guide for Unix Systems: Digital Forensics Field Guides by Cameron Malin
5. Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices, 4th Edition by Rohit Tamma

J