Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

Choice Based Credit System (CBCS) in Light of NEP-2020
M.Sc. Cyber Forensics - IV SEMESTER
Batch- 2021-2023

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*				
MSCFN401		Malware Analysis	60	20	20	30	20	4	0	2	5

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P - Practical; C - Credit;
*Teacher Assessment shall be based 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. To understand malware analysis concept
2. To understand advanced malware analysis

Course Outcomes:
After studying this course, the students will :

1. To know to analysis of malware using tools
2. To get overviews of malware analysis

UNIT IBasic Static Malware Analysis-I
Introduction to Malware, Types of malware – Virus, Worm, Trojan, Backdoor,Ransomware, The Goals of Malware Analysis, Malware Analysis Techniques,

UNIT IIBasic Static Malware Analysis- II
Basic Static Techniques: Hashing, Finding Strings, Packed and ObfuscatedMalware, PortableExecutable File Format, Linked Libraries and Functions, PEFile Header and Sections,Virtual Machines for Malware Analysis

UNIT III Advanced Static Malware Analysis
Introduction to x86 Disassembly: Architecture, Main Memory, Instructions,Opcodes and Endianness, Operands, Registers, Simple Instructions, Stack,Conditionals, Branching,Analyzing Malicious Windows Programs: WindowsAPI, Windows Registry, Networking APIs, Kernel vs User Mode, Native API.

UNIT IV: Advanced Dynamic Malware Analysis
Debugging: Source Level vs Assembly Level Debuggers, Kernel vs User modeDebugging, Using Debugger – OllyDbg/IDA Pro, Exceptions, Modifyingexecution with Debugger, Malware Behavior: Reverse Shell, RAT, Botnet,Process Injection, Hook Injection, APC Injection

UNIT VDynamic Malware Analysis

Basic Dynamic Analysis: Executing Malware Analysis in safe environment,Monitoring with Process Monitor, Viewing Processes with Process Explorer,Comparing Registry Snapshots with Regshot, Faking a Network, Packet Sniffingwith Wireshark

Experiments

1. Assembling a toolkit for effective malware analysis
2. Examining static properties of suspicious programs
3. Understanding core x86 assembly concepts for malicious code analysis
4. Recognizing common malware characteristics at the Windows API level
5. Malicious PDF file analysis, including the analysis of suspicious websites; VBA macros in Microsoft Office documents
6. Using debuggers for dumping packed malware from memory; Analyzing multi-technology and "fileless" malware
7. Code injection and API hooking
8. How malware detects debuggers and protects embedded data
9. Unpacking malicious software that employs process hollowing
10. Bypassing the attempts by malware to detect and evade analysis tools
11. Handling code misdirection techniques, including SEH and TLS callbacks
12. Unpacking malicious executables by anticipating the packer's actions

Reference Books-:

1. Michael Sikorski, Andrew Honig : Practical Malware Analysis - The Hands-On Guide toDissecting Malicious Software, 1st Edition
2. Eldad Eilam : Reversing – Secrets of Reverse Engineering, Wiley Publishing

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

Choice Based Credit System (CBCS) in Light of NEP-2020
M.Sc. Cyber Forensics - IV SEMESTER
Batch- 2021-2023

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*				
MSCFN402		Social Network Analysis & Open Source Intelligence	60	20	20	30	20	4	0	2	5

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P - Practical; C - Credit;
*Teacher Assessment shall be based 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. To learn about structure and evolution of networks, to build a framework of network analysis that covers measures.
2. To learn cyber ethics
3. To learn social media and network analysis

Course Outcomes:
After studying this course, the students will :
1. Be able to secure both clean and corrupted systems, protecting personal data, securing simple computer networks, and safe Internet usage.
2. Be able to understand dynamics and evolution of social networks.
3. Be able to understand the framework of network analysis.
4. Be able to understand how various social media networks are working and using SNA in their infrastructure.

UNIT 1Introduction to Social Network
What is Online Social Networks, data collection from social networks, challenges, opportunities, and pitfalls in online social network, Cybercrimes related to social media and its awareness, scrapping of data from social media API's.
.
UNIT 2 Privacy in Social Network Analysis
Information privacy disclosure, revelation, and its effects in OSM and online social networks, Privacy issues related to location based services on OSM.

UNIT 3 Social Media Analysis

Tracking social footprint / identities across different social network, Identifying fraudulent entities in online social networks, Effective and usable privacy setting and policies on OSM, Policing & OSM

UNIT 4 Social Media Behaviour:
Social Media Forensics: Case Studies Open Source tools or social media analytics, Safety on social media, Legal Issues in world social media, Information Technology (Intermediary Guidelinesand Digital Media Ethics Code) Rules, 2021

UNIT 5 Social Network Behaviour Analysis
Detection and characterization of spam, phishing, frauds, hate crime, abuse and extremism via online social media, Data Collection & Analysis, Fake News & content on social media

Experiment-:

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

Text Books -:

2) Sunit Belapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd, 2011.
3) John Scott, Social Network Analysis, 3rd Edition, SAGE, 2012.

Reference Books-:

1) Wouter de Nooy, Andrej Mrvar, Vladimir Batagelj, Exploratory Social Network Analysis with Pajek, 2nd Revised Edition, Cambridge University Press, 2011
2) Patrick Doreian, Frans Stokman, Evolution of Social Networks, Routledge, 2013
3) Social Media Analytics: Effective Tools for Building, Interpreting, and Using Metrics
4) Social Network Analysis: Methods and Application by Katherine Faust and Stanley Wasserman.
5) Understanding Social Networks: Theories, Concepts by Charles Kadushin
6. Social Media Data Extraction and Content Analysis by Shalin Hai-Jew

.

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

Choice Based Credit System (CBCS) in Light of NEP-2020
M.Sc. Cyber Forensics - IV SEMESTER
Batch- 2021-2023

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*				
MSCFN403		Multimedia Forensics	60	20	20	30	20	4	0	2	5

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P - Practical; C - Credit;
*Teacher Assessment shall be based 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. To learn about phonetics and speech and synthesis of sounds.
2. To learn about forensic speaker identification
3. To learn audio & video authentication importance in forensic science

Course Outcomes:

After studying this course, the students will :

1. Be able understand audio and video authentication using forensic tools..
2. Be able to understand speech synthesis of collection of voice sample.
3. Be able to understand CCTV and DVR analysis.

Unit-I Physics of Sound & Waves

Physics Of Sound: Waves And Sound, Analysis And Synthesis Of Complex Waves, Human And Non-Human Utterances, Anatomy Of Vocal Tract, Speech And Noise Characteristics, Audio Clarification Principles, Difference Between Language And Speech, Collection Of Voice Sample

Unit-II Forensic Speaker Identification

Various Approaches In Forensic Speaker Identification, Instrumental Analysis Of Speech Sample, Interpretation Of Result, Speech Recognition And Speaker Identification, Voice Authentication, Tools And Software Used In Audio Analysis, Noise Reduction Tools, Authenticity Of Audio Evidence In Courtroom, Basics of VoIP technology.

Unit-III Video Technology

Introduction to video technology, different video formats, video recording devices, Legal concepts regarding Digital Multi-Media Evidence, Scientific methodology of forensic video analysis: Best practices of collection, recovery, enhancement, analysis and interpretation of video evidence, Authentication of video as an evidence

Unit-IV CCTV & DVR Analysis
Basics of CCTV and DVR, best practices of CCTV evidence retrieval and storage at scene of crime and laboratory, challenges and precaution at the scene of crime, evidence handling procedure, Analysis of CCTV recordings, legal issues

Unit-V Collection and Authentication of Video Sample
Collecting voice sample for analysis, Analysis of voice sample for authentication, Speaker identification from sample, Video recording of crime scene, Video analysis and authentication, Metadata analysis of Audio / Video/image file, evidence handling, Case studies.

Experiment-:
1. Collection of Voice Sample
2. To retrieve data from CCTV
3. To perform metadata analysis of video file
4. To perform metadataanalysis of image file
5. To perform metadata analysis of audio file
6. To perform video authentication using forensics tools.
7. To perform audio authenticationusing forensics tools.
8. Case studies related video and audio morphing and its admissibility in court of law.

Reference Books –

1. Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools, Syngressimprint of Elsevier.
2. Bill Nelson, Amelia Phillips, Christopher Steuart, "Guide to Computer Forensics andInvestigations", Fourth Edition, Course Technology.
3. Angus M.Marshall, "Digital forensics: Digital evidence in criminal investigation", John –Wiley and Sons, 2008.

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

Choice Based Credit System (CBCS) in Light of NEP-2020
M.Sc. Cyber Forensics - IV SEMESTER
Batch- 2021-2023

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*				
MSCFN403		**Internship**	0	0	0	90	60	0	0	18	9

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

Every student will carry out Internship in Organization/Private Lab/Govt. Lab of one month under the supervision of Supervisor/(s) (Internal/External). Every student will be required to present seminar talktowards the end of the semester and should submit a report of the same presenting the workcarried out by him/her in the semester.

Chairperson	Chairperson	Controller of Examination	Joint Registrar
Board of Studies Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore	Faculty of Studies Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore	Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore	Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

Choice Based Credit System (CBCS) in Light of NEP-2020
M.Sc. Cyber Forensics - IV SEMESTER
Batch- 2021-2023

Chairperson	Chairperson	Controller of Examination	Joint Registrar
Board of Studies	Faculty of Studies	Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth
Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth	Vishwavidyalaya, Indore	Vishwavidyalaya, Indore
Vishwavidyalaya, Indore	Vishwavidyalaya, Indore		