Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science
B.Sc. Hons. Digital & Cyber Forensics- Batch (2021-24)
SEMESTER-V

BSDFN501 CYBER SECURITY AND RELATED LAWS

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL					
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*	L	T	P	CREDITS
BSDFN501	Compulsory	Cyber Security and Related Laws	60	20	20	30	20	4	0	2	5

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 to:
1. Basics of Cyber Security
2. To know status of cybercrimes.
3. Introduction to Cyber Laws.
4. Various types of Intellectual property Rights.

COURSE OUTCOMES
Upon completion of the subject, students will be able to:
1. Basics of Cyber Security.
2. To understand cyber security risks in India.
3. Understand local and global level cybercrimes.
4. Understand Cyber Law of India.
5. Various types of cybercrimes and their effect.

COURSE CONTENT

Unit I:
Introduction to cybercrime and information security, classification of cybercrimes. Computer security concepts, Security services, OSI security, Security mechanism, Security attacks and their types, Fundamental security design principle, Model for security network security.

Unit II:
Modus operandi of cybercrime, proxy server and anonymizers, identity theft, password cracking, virus, and worms; types, manner of attack- trojan horse, backdoors, logic bombs etc., steganography, DoS and DDoS attacks, SQL injection, buffer overflow, attacks on wireless networks.

Chairperson	**Chairperson**	**Controller of Examinations**	**Joint Registrar**
Board of Studies- Forensic Science	Faculty of Studies- Sciences	Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth
Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth	Vishwavidyalaya, Indore	Vishwavidyalaya, Indore
Vishwavidyalaya, Indore	Vishwavidyalaya, Indore		

Unit III:

Information Technology (Amendment) Act 2008 –Objective, Applicability and Jurisdiction; Various cyber-crimes under Sections 43 (a) to (j), 43A, 65, 66, 66A to 66F, 67, 67A, 67B, 70,70A, 70B, 80 etc. along with respective penalties, punishment and fines, Penal Provisions for Phishing, Spam, Virus, Worms, Malware, Hacking, Trespass and Stalking; Human rights in cyberspace, International Co-operation in investigating cybercrimes.

Unit IV:

Introduction to Intellectual Property Rights, Concept and Theories. Kinds of Intellectual Property Rights. Need for Private Rights versus Public Interests Advantages and Disadvantages of Intellectual Property Rights.

Unit V:

Cybercrime status in India. Need of cyber law in India. Digital signature and the Information Technology Act. Overview of digital evidence related to cybercrimes. Admissibility of digital evidence in Indian courts.

List of Practical:

1. Case study related to cybercrime in India.
2. Review a case in which punishment was given for infringement of copyright.
3. Review cyber security protocols.
4. Search and collect evidence related to digital and cybercrime from a dummy crime scene.
5. Pack, seal and label evidence related to digital and cybercrime from a dummy crime scene.
6. Write a review on process of submission of digital evidence in court.
7. Any other practical/ visit may be conducted based on the syllabus.

Suggested readings:

1. Nina Godbole and Sunit Belapore; "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publications, 2011.
2. Karnika Seth;"Computers, Internet and New Technology Laws", Lexis Nexis Buttersworth Wadhwa, 2012.
3. Bill Nelson, Amelia Phillips and Christopher Steuart; "Guide to Computer Forensics and Investigations" –3rdEdition, Cengage, 2010 BBS.
4. William Stallings; "Cryptography and Network Security: Principles and Practices", Fifth Edition, Prentice Hall Publication Inc., 2007.
5. Atul Jain; "Cyber Crime: Issues, Threats and Management", 2004.
6. Majid Yar; "Cybercrime and Society", Sage Publications, 2006.
7. Pavan Duggal; "Cyber Law –The Indian Perspective", Saakshar Law Publications

Chairperson	Chairperson	Controller of Examinations	Joint Registrar
Board of Studies- Forensic Science	Faculty of Studies- Sciences	Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth
Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth	Vishwavidyalaya, Indore	Vishwavidyalaya, Indore
Vishwavidyalaya, Indore	Vishwavidyalaya, Indore		

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science
B.Sc. Hons. Digital & Cyber Forensics- Batch (2021-24)
SEMESTER-V

BSDFN502 FUNDAMENTALS OF MOBILE 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*				
BSDFN502	Compulsory	Fundamentals of Mobile Forensics	60	20	20	30	20	4	0	2	5

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 to:
1. Understand wireless and mobile network security and its relation to the new security-based protocols.
2. Apply proactive and defensive measures to counter potential threats, attacks and intrusions.
3. Design secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks.

COURSE OUTCOMES
Upon completion of the subject, students will be able to:
1. Know security and privacy problems in the realm of wireless networks and mobile computing.
2. Understand wireless and mobile network security and its relation to the new security-based protocols.
3. Apply proactive and defensive measures to counter potential threats, attacks and intrusions.
4. Learn to design secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks.

COURSE CONTENT
Unit I:
Wireless threats, vulnerabilities, and security: Wireless LANs, War Driving, War Chalking, War Flying, Common Wi-fi security recommendations, PDA Security, Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft.

Unit II:
CIA triad in mobile phones-Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Netmonitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues.

Unit III:
Mobile phone forensics: crime and mobile phones, evidence, forensic procedures, files present in SIM card, device data, external memory dump, evidence in memory card, operators systems- Android forensics: Procedures for handling an android device, imaging android USB mass storage devices, logical and physical techniques.

Unit IV:
Introduction To Mobile Network Techs, Vulnerabilities Threats, and Attack Entry Points. Categorization Of Attacks in Mobile Networks, Signaling Attacks.

Unit V:
Threats And Attacks In 4g Networks- Attacks Against Security and Confidentiality, Ip-Based Attacks, Gtp-Based Attacks, Volte Sip-Based Attacks, Diameter-Based Attacks.

List of Practical:
1. Mobile Phone Acquisition.
2. SIM Analysis.
3. To acquire mobile cache memory image using forensic tool.
4. To perform mobile memory forensics practical using Magnet Forensics Tool.
5. Any other practical/ visit may be conducted based on the syllabus.

Suggested Reading:
1. Andrew Hoog, " Android Forensics: Investigation, Analysis and Mobile Security for Google Android", Elsevier publications, 2011
2. Angus M.Marshall, " Digital forensics: Digital evidence in criminal investigation", John – Wiley and Sons, 2008
3. Kia Makki, Peter Reiher, "Mobile and Wireless Network Security and Privacy ", Springer, ISBN 978-0-387-71057-0, 2007.
4. Siva Ram Murthy.C, Manoj B.S, "Adhoc Wireless Networks Architectures and By Yulong Zou, Senior Member IEEE, Jia Zhu, Xianbin Wang, Senior Member IEEE, and Lajos Hanzo, Fellow IEEE
5. "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends" Zou et al.: A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends

Chairperson	Chairperson	Controller of Examinations	Joint Registrar
Board of Studies- Forensic Science	Faculty of Studies- Sciences	Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth
Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth	Vishwavidyalaya, Indore	Vishwavidyalaya, Indore
Vishwavidyalaya, Indore	Vishwavidyalaya, Indore		

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science
B.Sc. Hons. Digital & Cyber Forensics- Batch (2021-24)
SEMESTER-V

BSDFN503 DIGITAL FORENSICS

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL					
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*	L	T	P	CREDITS
BSDFN503	Compulsory	Digital Forensics	60	20	20	30	20	4	0	2	5

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 to:
1. Know about fundamentals of digital forensics.
2. Understand rules of digital forensics.
3. Learn various evidence related to digital forensics.
4. Learn Various software used in digital forensics.

COURSE OUTCOMES
Upon completion of the subject, students will be able to:
1. Know about fundamentals of digital forensics.
2. Understand rules of digital forensics.
3. Learn various evidence related to digital forensics.
4. Learn the procedure of handling digital evidence.
5. Learn various software used in digital forensics.

COURSE CONTENT
Unit I:
Digital Forensics- Introduction, Objective and Methodology, Rules of Digital Forensics, Good
Forensic Practices, Daubert‟s Standards, Principles of Digital Evidence. Overview of types of Computer Forensics – Network Forensics, Mobile Forensics, Social Media Forensics and E-mail Forensics. Services offered by Digital Forensics. First Responder – Role, Toolkit and Do‟s and Don‟ts

Unit II:
Introduction to Cyber Crime Investigation, Procedure for Search and seizure of digital evidence in cyber-crime incident- Forensics Investigation Process- Pre search consideration, Acquisition, Duplication & Preservation of evidences, Examination and Analysis of evidences, Storing of Evidences, Documentation and Reporting, Maintaining the Chain of Custody.

Chairperson	Chairperson	Controller of Examinations	Joint Registrar
Board of Studies- Forensic Science	Faculty of Studies- Sciences	Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth
Shri Vaishnav Vidyapeeth	Shri Vaishnav Vidyapeeth	Vishwavidyalaya, Indore	Vishwavidyalaya, Indore
Vishwavidyalaya, Indore	Vishwavidyalaya, Indore		

Unit III:

Data Acquisition of live system, Shutdown Systems and Remote systems, servers. E-mail Investigations, Password Cracking. Seizing and preserving mobile devices. Methods of data acquisition of evidence from mobile devices. Data Acquisition and Evidence Gathering from social media. Performing Data Acquisition of encrypted systems. Challenges and issues in cyber-crime investigation

Unit IV:

Analysis of Digital Evidence 18 Search and Seizure of Volatile and Non-volatile Digital Evidence, Imaging and Hashing of Digital Evidence, Introduction to Deleted File Recovery, Steganography and Steganalysis, Data Recovery Tools and Procedures, Duplication and Preservation of Digital Evidence, Recover Internet Usage Data, Recover Swap files/Temporary Files/Cache Files. Software and Hardware tools used in cybercrime investigation – Open Source and Proprietary tools. Importance of Log Analysis in forensic analysis. Understanding Storage Formats for Digital Evidence – Raw Format, Proprietary Formats, Advanced Forensic Formats.

Unit V:

Windows Systems Artifacts: File Systems, Registry, Event logs, Shortcut files, Executables. Alternate Data Streams (ADS), Hidden files, Slack Space, Disk Encryption, Windows registry, startup tasks, jump lists, Volume Shadow, shell bags, LNK files, Recycle Bin Forensics (INFO, $i, $r files). Forensic Analysis of the Registry – Use of registry viewers, Regedit. Extracting USB related artifacts and examination of protected storages. Linux System Artifact: Ownership and Permissions, Hidden files, User Accounts and Logs.

List of Practical:

1. Search and seizure of volatile and non-volatile evidence in a cyber-crime incident.
2. Acquisition, Duplication & Preservation of given digital evidence.
3. Examination and Analysis of given evidence.
4. Using software tools for digital evidence.
5. Any other practical/ visit may be conducted based on the syllabus.

Suggested Readings:

1. Gerard Johansen "Digital Forensics and Incident Response" Packt Publisher, 2017.
2. Electronic Crime Scene Investigation A guide for First Responders, US Dept. Justice.
3. Chris Prosise& Kevin Mandia, Incident Response & Computer Forensics,McGraw-Hill Publication.