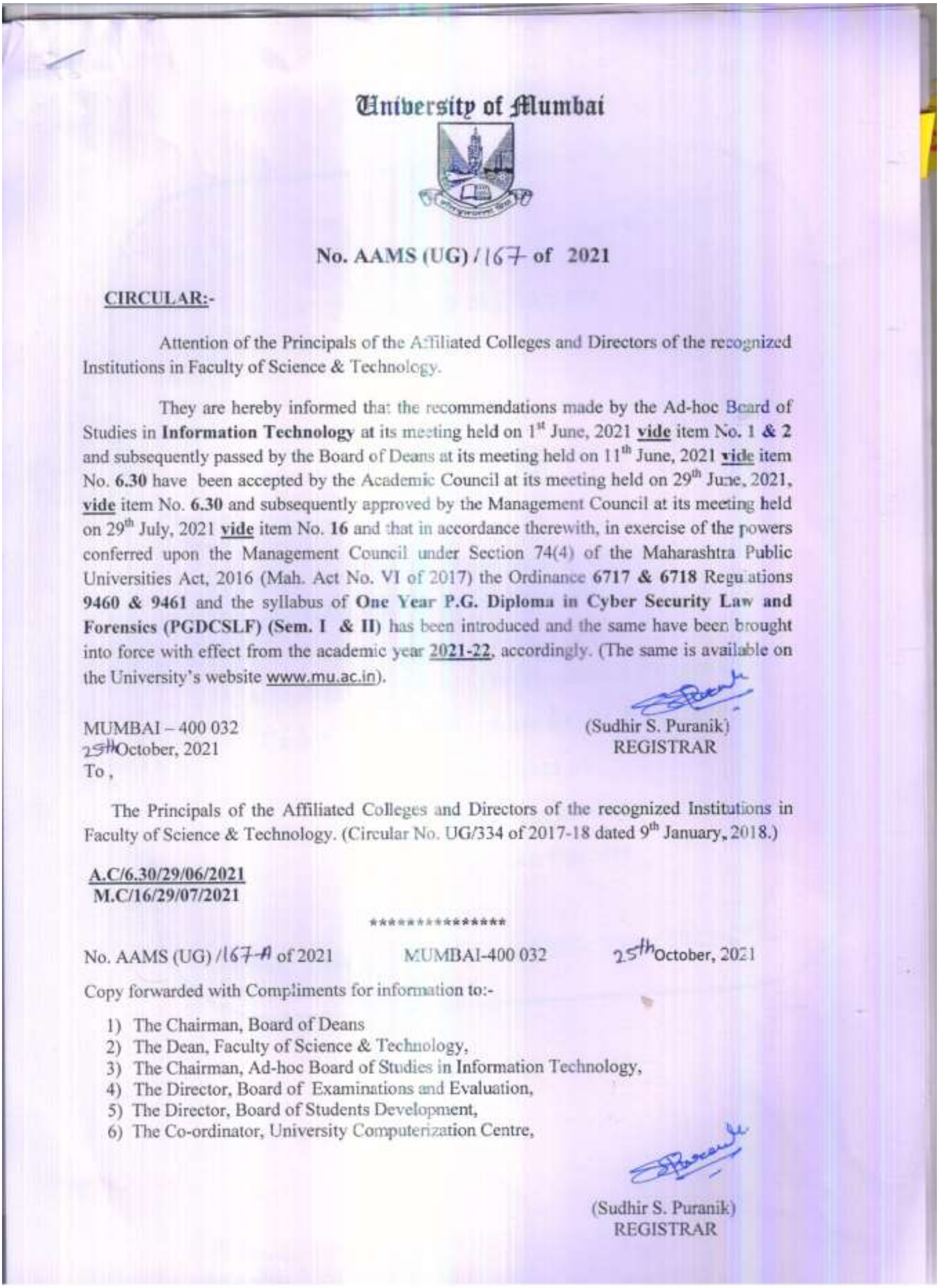


University of Mumbai

No. AAMS (UG) / 167 of 2021

CIRCULAR:-

Attention of the Principals of the Affiliated Colleges and Directors of the recognized Institutions in Faculty of Science & Technology.

They are hereby informed that the recommendations made by the Ad-hoc Board of Studies in **Information Technology** at its meeting held on 1st June, 2021 **vide** item No. 1 **& 2** and subsequently passed by the Board of Deans at its meeting held on 11th June, 2021 **vide** item No. **6.30** have been accepted by the Academic Council at its meeting held on 29th June, 2021, **vide** item No. **6.30** and subsequently approved by the Management Council at its meeting held on 29th July, 2021 **vide** item No. **16** and that in accordance therewith, in exercise of the powers conferred upon the Management Council under Section 74(4) of the Maharashtra Public Universities Act, 2016 (Mah. Act No. VI of 2017) the Ordinance **6717 & 6718** Regulations **9460 & 9461** and the syllabus of **One Year P.G. Diploma in Cyber Security Law and Forensics (PGDCSLF) (Sem. I & II)** has been introduced and the same have been brought into force with effect from the academic year **2021-22**, accordingly. (The same is available on the University's website www.mu.ac.in).

MUMBAI – 400 032
25th October, 2021

(Sudhir S. Puranik)
REGISTRAR

To,

The Principals of the Affiliated Colleges and Directors of the recognized Institutions in Faculty of Science & Technology. (Circular No. UG/334 of 2017-18 dated 9th January, 2018.)

A.C/6.30/29/06/2021
M.C/16/29/07/2021

****

No. AAMS (UG) /167-A of 2021 MUMBAI-400 032 25th October, 2021

Copy forwarded with Compliments for information to:-

1) The Chairman, Board of Deans
2) The Dean, Faculty of Science & Technology,
3) The Chairman, Ad-hoc Board of Studies in Information Technology,
4) The Director, Board of Examinations and Evaluation,
5) The Director, Board of Students Development,
6) The Co-ordinator, University Computerization Centre,

(Sudhir S. Puranik)
REGISTRAR

Copy to :-

1. The Deputy Registrar, Academic Authorities Meetings and Services (AAMS),
2. The Deputy Registrar, College Affiliations & Development Department (CAD),
3. The Deputy Registrar, (Admissions, Enrolment, Eligibility and Migration Department (AEM),
4. The Deputy Registrar, Research Administration & Promotion Cell (RAPC),
5. The Deputy Registrar, Executive Authorities Section (EA),
6. The Deputy Registrar, PRO, Fort, (Publication Section),
7. The Deputy Registrar, (Special Cell),
8. The Deputy Registrar, Fort/ Vidyanagari Administration Department (FAD) (VAD), Record Section,
9. The Director, Institute of Distance and Open Learning (IDOL Admin), Vidyanagari,

They are requested to treat this as action taken report on the concerned resolution adopted by the Academic Council referred to in the above circular and that on separate Action Taken Report will be sent in this connection.

1. P.A to Hon'ble Vice-Chancellor,
2. P.A Pro-Vice-Chancellor,
3. P.A to Registrar,
4. All Deans of all Faculties,
5. P.A to Finance & Account Officers, (F.& A.O),
6. P.A to Director, Board of Examinations and Evaluation,
7. P.A to Director, Innovation, Incubation and Linkages,
8. P.A to Director, Board of Lifelong Learning and Extension (BLLE),
9. The Director, Dept. of Information and Communication Technology (DICT) (CCF & UCC), Vidyanagari,
10. The Director of Board of Student Development,
11. The Director, Department of Students Walfare (DSD),
12. All Deputy Registrar, Examination House,
13. The Deputy Registrars, Finance & Accounts Section,
14. The Assistant Registrar, Administrative sub-Campus Thane,
15. The Assistant Registrar, School of Engg. & Applied Sciences, Kalyan,
16. The Assistant Registrar, Ratnagiri sub-centre, Ratnagiri,
17. The Assistant Registrar, Constituent Colleges Unit,
18. BUCTU,
19. The Receptionist,
20. The Telephone Operator,
21. The Secretary MUASA

for information.

AC no. 29/06/2021
Item No. 6.30

University of Mumbai

Syllabus for New PG Diploma in Cyber Security Law and Forensics (PGDCSLF)

Semester I and II

A Special Executive Development Program

Under the Semester based CBCS Pattern

In the subject of

Information Technology

Under Science Faculty

(With Effect from the academic Year 2021-2022)

New AC 29/06/2021

Item No: 6.30

UNIVERSITY OF MUMBAI

Syllabus for Approval

Sr. No.	Heading	Particulars
1.	Title of the Course O.6717	P.G.Diploma in Cyber Security Law and Forensics (PGDCSLF) (Special Executive Development Program)
2.	Eligibility for Admission O.6718	Those who have completed Under graduate in any faculty from recognized University (knowledge of computer is Preferable).
3.	Passing Marks R - 9460	40%
4.	Ordinances / Regulations (if, any)	New Ordinances to be placed here.
5.	Number of years / Semesters R - 9461	One year – Two Semesters
6.	Level	~~P.G.~~ / ~~U.G.~~ /P.G. Diploma / ~~Diploma~~ / ~~Certificate~~ (Strike out which is not applicable)
7.	Pattern	~~Yearly /~~ Semester, ~~Choice Based~~ (Strike out which is not applicable)
8.	Status	New / ~~Revised~~
9.	To be implemented from Academic year	From the Academic Year **2021 – 2022**

Date: April 17, 2020

Signature:_________________

Name of the BoS Chairperson ~~/ Dean~~:

Dr. (Mrs.) R. Srivaramangai

(rsrimangai@udit.mu.ac.in)

Academic Council 29/06/2021
Item No: 6.30

P.G.Diploma in Cyber Security, Law and Forensics (PGDCSLF)

Course Duration : 1 year No. of Seats :30 Total Fees : 80000

Preamble : Reports of extensive data breaches or other elaborate cybercrimes are increasing worldwide. The complexity and scope of these cases can present challenges that might seem insurmountable for most local law enforcement agencies. Law enforcement agencies across the globe have also experienced a rise in hacktivism. One of the critical issues facing all law enforcement organizations is the exponential increase of various types of digital evidence the agencies need to collect and store, including reports, pictures, videos, and other electronic records. DIT has helped train police officers at various levels through a number of its programs that include training and forensic facilities at CBI, NPA, and some of the state police centers. As a social responsibility the educational institutions should also come forward in imparting training to Law enforcement with the help of IT.

Objective: The main objective of this program is to have a unique training programme for Law enforcement personnel in the latest technological concepts and tools with more practical exposure in the areas of cyber security, cyber law and cyber forensics.

Course Duration: 1 year

Fee Structure

Head	Amount in Rs
Tuition Fees	40000/-
Laboratory Fee	20000/-
Library and Other Fee	10000/-
Examination fees	8000/-
Certificate fees	2000/-
Total	

Eligibility: Under graduate in any faculty from recognized University with minimum 40 % of passing in aggregate (knowledge of computer is Preferable).

Admission Procedure: Merit list based on UG pass percentage

Required of Teaching and Non teaching staff

Course faculty : - Coordinator, CHB based faculty as per the subject requirements approximately 6 CHB visiting faculties from industries, office staff, peon

Justification for the fee:

Income	**Expenditure**	
Course Fees : 30 students X 80,000 = 2400000	Theory Lectures 50 hrs X Rs. 3000 X 5 subjects	750000
Application Fees : Rs.100 per form If approximately 50 forms received then the income may be 50 x 100 = 5000	Practical Sessions 50 hrs X RS.3000 X 5 subjects	750000
	Approximate Exam assessment remuneration	6600
	Paper setting Practical and theory	15000
	Remuneration to clerk and peon 12000+8000=20000*12=240000	240000
	Infrastructure Requirements (Initial Investment 30 computers with 11th generation i7 processors) + Apprx. 30000 for VMware subscription per year + Software tools licenses apprx. Rs. 2 lakhs per year	32,30000
	Advertisements	100000
2405000		**5091600/-**

Remuneration

Coordinator :-Rs 10,000/ month

Course faculty : - Rs 3000/- per lecture hour : Industry experts with minimum 3 years of extensive work experience in the above fields

Non teaching staff :- Accountant and Office staff Rs12000 per month, Peon Rs8000/- per month

Non teaching staff :- Office staff Rs 12000 per month, Peon Rs 8000/- per month (As per University Norms)

Role of Coordinator : Overall coordination of the programme right from advertisement, admission, to scheduling lectures and examinations. Need to take one course with its practical as a part of coordinator-ship. Additional courses taken will be paid as per CHB basis

Role of Faculty :

Lectures to be taken as per the syllabus. Conduct Internal examinations. Should be a part of external examinations as well

Role of Accountant and Office Staff: Incharge of Income and Expenditure of the programme and preparing the balance sheet. Office administration in coordination with the coordinator to be done by the Office Staff

Examination remuneration to be paid as per the University Examination ordinances from the department budget head “Remunerations for examinations”.

Semester I

Theory			Practical	
Course Code	Course Name	Credits	Course Code	Credits
PGDCSLF101	Introduction to Digital devices and networks	2	PGDCSLF1P1	2
PGDCSLF102	Introduction to Cyber law, Electronic Evidence, Data privacy law and types of cybercrime	2	PGDCSLF1P2	2
PGDCSLF103	Cybercrime investigation – I (Crime Scene Management and Incident response)	2	PGDCSLF1P3	2
PGDCSLF104	Cybercrime investigation – II	2	PGDCSLF1P4	2
PGDCSLF105	Forensic technologies and Digital forensics	2	PGDCSLF1P5	2

Semester II

Theory			Practical	
Course Code	Course Name	Credits	Course Code	Credits
PGDCSLF201	IT Act 2000, IT Act Amendments and IPR in cyberspace	2	PGDCSLF2P1	2
PGDCSLF202	Cyber Psychology and Ethics	2	PGDCSLF2P2	2
PGDCSLF203	Cyber Security Technology and Regulations	2	PGDCSLF2P3	2
PGDCSLF204	Crime Scene Management Practical	2	PGDCSLF2P4	2
PGDCSLF205	Dark web and Cyber warfare	2	PGDCSLF2P5	2

All practical will be based on the concepts in theory and the department has the freedom of framing and updating the practical list as and when required. We can include case studies / practical as per subject requirement)

SEMESTER I

P. G. Diploma in Cyber Security, Law and Forensics (PGDCSLF)		**Semester – I**	
Course Name: Introduction to Digital devices and networks		**Course Code:** **PGDCSLF101**	
Periods per week (1 Period is 60 minutes)		4	
Credits		4	
		Hours	**Marks**
Evaluation System	**Theory Examination**	2	40
	Internal	--	60

Course Objectives:

1. Upon the successful completion of this course, the student will be able to:
2. To Focus on information sharing and networks.
3. To Introduce flow of data, categories of network, different topologies.
4. To Focus on different digital devices and their applications

Unit	Details	Lectures
I	**Computer** – Classification of computers, features and specifications of various computer generations, functionalities of a computer, data processing and storage.,Hardware components and their uses, Introduction to types of computing devices – desktops, laptops, MacBook, iMac,All in One computers, tablets, wearable devices. Different Operating Systems and their relevance to Law Enforcement Officers. Demo of disassembling a Computer and showing various components and peripherals. Types of Data Storage – primary, secondary etc. Types of storage device technology – magnetic tapes, flash (Semiconductor memories), difference between mobile phone storage and computer storage etc.	**10**
II	**Hard Disk Drive overview** – physical and logical structure, Types of Hard Disk Drive interfaces – SATA, IDE, SCSI, SSD etc., Parts of Hard Disk Drive – spindle, disk, Structure of Hard Disk Drive – sector, track, cluster size etc., Hard Disk Drive data addressing, metadata, disk capacity, calculation and measuring performance of Hard Disk Drive. Partitioning and formatting of Hard Disk Drive – low level and high level formatting. Boot process – master boot record, types of Operating System, file systems, understanding File System, shared disk file systems, special purpose file systems, etc. CDROM/DVD file system – CDFS, ISO, Joliet, and UDF.	**10**
III	**Introduction to Computer Networks:** Need of computer,networks,Different types of computer networks,Bluetooth technology / Wi-Fi technology / WiMAX technology,HAN / PAN, LAN, MAN, WAN,Network Architecture and topology,Networking devices – Firewalls, Hub, Bridge, Switch, Routers, IDS/IPS etc.,Concept of physical addressing system,Identification of MAC Addresses,Concept	**10**

	of logical addressing system,Types of IP Addresses – static, dynamic, public, private,Concept of IP address assignment – DHCP, static, Types of IP address versions - Ipv4, Ipv6, difference between IPv4 and IPv6. Intranet vs Internet vs Extranet, Concept of website, DNS and URLs, Identification of IP address of a user device or website	
IV	**Introduction to Mobile Devices:** Basics of Mobile phone & communications: Components of Cellular Network,, Different Mobile Devices, Hardware Characteristics of Mobile Devices, Software Characteristics of Mobile Devices, Mobile Operating Systems : Classification of Mobile Operating Systems (WebOS, Symbian OS, Android OS,RIM BlackBerry OS, Windows Phone 7, Apple iOS), difference between desktop operating system and mobile operating system.	**10**
V	**CCTV and BOTS:** Video Enhancement, Demultiplexing, Footage Restoration, Visual Authentication, Enhancement & Speed Correction, Format Conversion, Audio Enhancement, Tampering Investigations, Alexa Devices (BOT).	**10**

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	E-Discovery: Introduction to Digital Evidence	Amelia Phillips, Ronald Godfrey, Christopher Steuart, Christine Brown.	Security Pub ISBN-13: 978-1285427423	1st	2000
2.	Practical Guide to Digital Forensics Investigations	Darren Hayes	Pearson	2nd	2020
3.	Data communication & Networking	Bahrouz Forouzan	PHI	2nd	2005
4.	Computer Networks	Andrew S. Tanenbaum	Pearson	1st	2001

Course Outcome:

- On successful completion of the course, the student will be having the basic knowledge of data sharing, transmission media and their protocols.
- Students will have the basic knowledge of computer networks and digital devices.

P. G. Diploma in Cyber Security, Law and Forensics (PGDCSLF)		**Semester – I**	
Course Name: Introduction to Cyber law, Electronic Evidence, Data privacy law		**Course Code: PGDCSLF102**	
Periods per week (1 Period is 60 minutes)		4	
Credits		2	
		Hours	**Marks**
Evaluation System	**Theory Examination**	2	40
	Internal	--	60

Course Objectives:

1. Introduce the basics of Cyber Law with reference to the IT Act and its amendments.
2. Explain the types of digital evidence
3. Demonstrate the processes for data carving.
4. Demonstrate the process for data collection and analysis.
5. Analyse the varying levels of freedom in data privacy.

Unit	Details	Lectures
I	**Introduction to IT Act and IT Act Amendments:** Cybercrimes and their respective sections., Section 79, Government Examiner of Digital Evidence. Requirement of certification under different sections. Understanding the report given by cyber forensics. Relevant sections of Indian Evidence Act, Admissibility of electronic evidence, Frame proper notice with clauses, Indian Penal Code and cybercrimes, Code of Criminal Procedure 1973 – search and seizure provisions, examination of witnesses through audio and video by police Section 46 the role of adj. officer - IT Act , Difference between 79 3b IT, 91 Cr PC and 149 Cr PC, Relevant International laws and acts Mutual Legal Assistance Treaty, Letter Rogatory , Procedural aspects of law, Federal laws, GDPR, TRIPS and other global law practices related to IT Act., CERT.IN, MEITY, TERM, TRAI, ICANN / IANA etc.	**10**
II	**Digital Evidence:** Digital evidence – definition, characteristics, types, source of digital evidence etc. Classification of Digital evidence – user created, user protected and system created. Difference between volatile and non-volatile memory, Rules of Evidence – best evidence rule, hearsay evidence etc., Traditional forensic evidence vs digital evidence Cyber forensics – definition, classification, Cyber forensics v/s traditional forensics – Locard’s Exchange Principle, Daubert’s Rule, Repeatability and Reproducibility, peer review techniques, Introduction to forensic tools, techniques and technology. Discussion on its application to Computer Systems, Network, communication devices, volatile memory, storage systems, Internet Data, Cloud, SCADA Systems and Databases Computer Forensic Imaging and Hashing, Anti-forensics - Data hiding techniques	**10**

	Data carving: Hashing – importance, process, algorithm and tools. Best practices – ACPO, Interpol, STCIA, DOJ guidelines and best practices in Indian environment. Responsive toolkit – preparation, portable software tools, validation of tools, things to carry. Cyber forensics process – Identify, preview, acquire, authenticate, analyze and document. Areas to search – Active files, deleted files, slack space, unallocated space, hibernation file, page file, metadata and registry etc. Steps in crime scene investigation – securing crime scene, interviews, shutdown process, collecting evidence, packaging and transportation Process model – triage process, dual process model and utility Collection of important data – tools and techniques for collecting volatile data from RAM from a live system.	
III	**Mobile forensics -** Mobile Forensics Definition, Information available in Mobile Phones, Memory Considerations in Mobiles, Subscriber Identity Module (SIM), SIM File System, Integrated Circuit Card Identification (ICCID), International Mobile Equipment Identifier (IMEI), International Mobile Subscriber Identity (IMSI), Electronic Serial Number (ESN), difference between mobile forensics and computer forensics, identification, isolation of mobile devices, search and seizure of mobile devices, acquisition methods (physical, logical, file system, JTAG, Chip off), Analysis of mobile images, understanding a mobile forensic report. Imaging the drive at scene of crime using various tools and techniques – Use of write blocker devices, imaging, cloning, hashing, authentication of evidence, CRC, tools for hashing Volatile data capture and analysis – Capturing system info, network info. Packaging and transportation and preservation Documentation – seizure memo, Chain of Custody, forwarding note to FSL, 65 B, etc.	**10**
IV	**Fundamental Concept of Data Privacy:** , Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in different domains-medical, financial, etc	**10**
V	**Technology, Policy, Privacy and Freedom:** Medical privacy legislation, policies and best practices, Examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants.	**10**

Books and References:					
Sr. No.	**Title**	**Author/s**	**Publisher**	**Edition**	**Year**
1.	Cyber Law and Cyber Crime	Adv.(Dr) Prashant Mali	SnowWhite / Cyber Infomedia	2nd	2020
2.	Digital Evidence and Computer Crime	Eoghan Casey	Academic Press	2nd	2004

3.	The Complete Book of Data Anonymization: From Planning to Implementation	B. Raghunathan	Auerbach Pub	1st	2013
4.	Guide to Cyber Laws	Rodney D. Ryder	Wadhwa and Compan		2009
5.	Security and Incident Response	Keith J. Jones, Richard Bejtloich and Curtis W. Rose		1st	

Course Outcomes:

After completion of the course, a student should be able to:

- Articulate the various IT Acts pertinent to Data Privacy and Security.
- Explain what constitutes digital evidence.
- Identify the best practices for data carving.
- Use appropriate process model for data collection and analysis.
- Analyse the levels of freedom in data privacy with respect to the roles of the actors and the context.

P. G. Diploma in Cyber Security, Law and Forensics (PGDCSLF)		**Semester – I**	
Course Name: Cybercrime investigation – I (Crime Scene Management and Incident response)		**Course Code:** **PGDCSLF103**	
Periods per week (1 Period is 60 minutes)		4	
Credits		4	
		Hours	**Marks**
Evaluation System	**Theory Examination**	2	40
	Internal	--	60

Course Objectives:

1. Present an overview of types of cybercrime.
2. Analyse the different crimes that pertain to use of Emails, various Social Media platforms, dark Web.
3. Identify strategies to track, document and use Emails, Social Media platforms, and the dark web, data as evidence.

Unit	Details	Lectures
I	**Cybercrimes and cybercrime investigation:** Cyber-crime- Scope, characteristics and landscape over the years and present scenarios in cyber space. Development of cyber-crime,Classification of cyber-crime cyber criminals – Individual criminals / Organized criminals / sponsored criminals / hired criminals ,Various types of cybercrimes and their modus operandi and predictive policing,Challenges to investigators / Challenges in investigations,Safeguarding from cyber crimes,Investigation of the most common cybercrimes reported to LEA,Emerging trends in cybercrime Dos and don'ts while investigating cybercrime complaints,Difference between investigation of traditional crime and cyber crime,Common mistakes done by IO (Crime Scene, Search and Seizure, transportation, labeling, documentation – incorrect entries in seizure memo, irregularities in seizure memo, irrelevant or vague questions in forwarding note to FSL) Importance of documentation	**10**
II	**Email Investigation:** Working of Email.,Types of email, configurations – IMAP / POP., Various parts of an email. Components of an email header. Email header analysis. Differences between emails headers of various service providers. Identifying spoofed email, phishing email. Step action guide on Email tracking and tracing. Requesting details from intermediaries. Collection of email as an evidence – single email, multiple emails, entire mailbox etc. Presentation of email as an evidence in court. Restoring deleted emails	**10**

	from web and app. Challenges such as proxy and VPN. Regaining access to hacked email IDs. Email tracking through lawful interception under 91 C.R.P.C. Email tracking through extra lawful interception. Cyber Crimes, Types of Cybercrime, Hacking, Attack vectors, Cyberspace and Criminal Behavior, Clarification of Terms, Traditional Problems Associated with Computer Crime, Introduction to Incident Response	
III	**Social Media related investigations** **Facebook related investigations:** o Identity theft related cases o Difference type of cybercrime associated (Cyber stalking / Bullying / Harassment) o Content investigation (obscenity / nudity / defamatory related cases) o Content removal o FB live stream blocking methods o Accused character estimation through FB o Missing people/human trafficking surveillance in FB o FB posts share-tag-comment-like related offences o Facebook analytics o Downloading complete profile from Facebook. o Facebook for law enforcements o Collection, preservation of digital evidences, presentation in the court of law **Twitter Related investigations:** o Identity theft related cases o Difference type of cybercrime associated (Cyber stalking / Bullying / Harassment) o Content investigation (obscenity / nudity / defamatory related cases) o Content removal o Investigation on Tweet, Retweet, Tags, Handlers o Twitter Analytics o Web patrolling using Twitter o Downloading complete tweets from a profile, keyword etc. o Sentiment analysis o Collection, preservation of digital evidences, presentation in the court of law **Instagram Related Investigations:** o Identity theft related cases o Difference types of cybercrime associated (Cyber stalking / Bullying / Harassment) o Content investigation (obscenity / nudity / defamatory related cases) o Content removal o Downloading complete content o Instagram for law enforcement o Collection, preservation of digital evidences,	**10**

	presentation in the court of law **Linkedin Related Investigations:** o Identity theft related cases o Cyber stalking / harassment. o Content investigation o Content removal o Job frauds o Downloading complete user data o Collection, preservation of digital evidences, presentation in the court of law **Snapchat Related Investigations:** o Identity theft related cases o Cyber stalking / Cyber Bullying / harassment. o Content investigation (obscenity / nudity / defamatory related cases) o Content investigation o Content removal o Downloading complete user data o Collection, preservation of digital evidences, presentation in the court of law **Youtube Related Investigations:** o Content investigation (obscenity / nudity / defamatory related cases) o Copyright infringement related cases. o Youtube Video content removal o Youtube Tracing video uploaded user details o Youtube Video comment analysis o Youtube video tracking through geolocation/geotagging o Collection, preservation of digital evidences, presentation in the court of law **Matrimonial / Dating / Adultery Related Investigations:** o Content investigation (obscenity / nudity / defamatory related cases) o Tinder / Happn / Locanto / Tagged / Escort Services Related Apps / Websites o Collection, preservation of digital evidences, presentation in the court of law **Other Social Media Apps / Websites Related Investigations:** o **Tiktok / Sharechat / Musically** o **Games Related Investigations – Blue Whale, PubG, Fortnite, MoMo Games** o **Advisory content for Cyber Safety Awareness**	

IV	**Investigation of Fin-Tech related cases**: Various kinds of Fin-Tech options available in India,Common misconceptions,Investigating e-wallets Investigating ATM related frauds,Investigating OTP related frauds, Investigating Payment gateways, Investigating identity theft related cases Database forensics, Job frauds, Gambling, Betting, Financial transactions for illegal activities **WhatsApp / Telegram investigations:** Live WhatsApp investigation-digital foot prints, Deleted WhatsApp chat retrieving methods, WhatsApp-cloud chatting extraction methods, WhatsApp image or video offences related investigation, Cyber harassment through WhatsApp, Investigation on WhatsApp groups, Spy on WhatsApp groups through masking, methods-left-extreme-fundamental-radical groups, How to request details from WhatsApp via legal approach, Originator of post (Content, Image, Video), WhatsApp Call Investigations (Audio, Video).	10
V	**Introduction to location / cloud based investigations:** Introduction to Location Based Services., Types of Location Based Services. Triangulation and GPS Techniques to pinpoint the actual location of the criminals., By using CDR and Cell ID. By using Triangulation techniques. By using GPS tagging on photographs. By using Google Photos. Etc. By using WhatsApp, Facebook, Viber etc. Types of cloud service providers (Android / Apple / Blackberry etc.) Tracking of missing / stolen mobile phones or tablets, Gathering data created using various Google services, Requesting details from Google via legal approach Introduction to Location Based Services. Retrieval of data from Google / iCloud /Microsoft cloud services. Tracing missing/stolen mobile By Using IMEI No. Tracing missing/stolen mobile By Using MAC No. **Introduction to Dark Web Investigations** Introduction of Deep & Dark Net. Surface Internet vs Deep Internet. Indexed Website vs Non Indexed Websites. Red Rooms, Galaxy, Hidden WIKI, Wiki leaks, Silk Road, Pandora other Onion links. Modus operandi of cyber-crimes committed using Dark Web. Working principle of Block Chain. Concepts of Crypto currencies and mechanism behind it. Wallet Tracking, Public Key vs Private Key (Wrt Crypto Currencies) Introduction to track cryptocurrencies. Challenges in investigations.	10

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives		2018
2.	Digital Forensics and Incident Response	Gerard Johansen	Gerard Johansen	2nd	2020
3.	Security and Incident	Keith J. Jones,		1st	

	Response	Richard Bejtloich and Curtis W. Rose			
4.	First Responder’s Guide to Computer Forensics	Richard Nolan	Carnegi Mellon	1st	2005
5.	Computer Forensics and Cyber Crime	Marjie T. Britz	Pearson	3rd	2009

Course Outcomes:

After completion of the course, a student should be able to:

- Articulate an overview of types of cybercrime.
- Analyse the different crimes that pertain to use of Emails, various Social Media platforms, and the dark web.
- Identify strategies to track, document and use Emails and Social Media platforms as evidence.

P. G. Diploma in Cyber Security, Law and Forensics (PGDCSLF)		Semester – I	
Course Name: Cybercrime investigation – II		**Course Code: PGDCSLF104**	
Periods per week (1 Period is 60 minutes)		4	
Credits		4	
		Hours	**Marks**
Evaluation System	**Theory Examination**	2	40
	Internal	--	60

Course Objectives:

1. Present an overview of Dark Web Investigations.
2. Present an overview of Cyber Terrorism and Network Forensics.

Unit	Details	Lectures
I	**Dark Web Investigations:** Introduction of Deep & Dark Net., Surface Internet vs Deep Internet., Indexed Website vs Non Indexed Websites. Red Rooms, Galaxy, Hidden WIKI, Wiki leaks, Silk Road, Pandora other Onion links. Modus operandi of cyber-crimes committed using Dark Web. Working principle of Block Chain. Concepts of Crypto currencies and mechanism behind it. Wallet Tracking, Public Key vs Private Key (Wrt Crypto Currencies), Introduction to track cryptocurrencies. Challenges in investigations.	**10**
II	**Cyber Terrorism:** Misuse of Internet by terrorists, Recruitment, spread of propaganda on Internet, Phony websites & Cyber Herding, Web crawlers and use of data mining, Proactive measures to combat misuse of Internet by the terrorists. **Network Forensics:** Network Evidence Types and Sources, Network Packet Capture, Encapsulation and decapsulation methods, Session reconstruction for protocols – TCP and HTTP, Log collection, aggregation, and analysis, Wireless Packet Analysis, Challenges - Encoding, Encryption, VPN, MITM - Man-in-the-Middle Methods, Tools.	**10**
III	Investigation of critical information infrastructure (CII) related crimes: SCADA Networks, Railway Networks, Power Grid Networks, Water Grid Networks, Nuclear Power Plants, defense networks **Arriving at the Scene: Initial Response/ Prioritization of Effort**s : Initial Response/ Receipt of Information, Safety Procedures , Emergency Care, Secure and Control Persons at the Scene , Boundaries: Identify, Establish, Protect and Secure, Turn Over Control of the Scene and Brief Investigator(s) in Charge, Document Actions and Observations, Establish a Command Post (Incident Command System) and Make Notifications, Manage Witnesses, Preliminary Documentation and Evaluation of the Scene, Conduct Scene Assessment, Conduct Scene “Walk-Through” and Initial Documentation , Note-Taking and Logs	**10**
IV	**Processing the Scene:** Determine Team Composition, Ensure Contamination Control, Documentation , Sketching , Photography,	**10**

	Videography, Prioritize Collection of Evidence, Crime Scene Search Methods, Collect, Preserve, Inventory, Package, Transport, and Submit Evidence, Detailed Crime Scene Evidence Collection	
V	**Completing and Recording the Crime Scene Investigation** : Establish Crime Scene Debriefing Team, Perform Final Survey of the Crime Scene, Documentation of the Crime Scene, Acknowledge Specialized Crime Scene Circumstances, Crime Scene Investigation in Correctional and Custodial Facilities, Time-Limited Crime Scene Investigation **Crime Scene Equipment:** Initial Responding Officer(s), Crime Scene Investigator/Evidence Technician, Evidence Collection Kits (Examples)	**10**

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Crime Scene Investigation A Guide for Law Enforcement	Kevin Lothridge, Frank Fitzpatrick	National Forensic Science Technology Center	1st	2013
2.	Practical Crime Scene Processing and Investigation,	Ross M. Gardner, Donna Krouskup	CRC Press	Third Edition	2019
3.	Computer Forensics: Principals and Practices	Linda Volonino, Reynaldo Anzaldua and Jana Godwin	Pearson Prentice – Hall	1st	2007
4.	Computer Forensics: Computer Crime Scene Investigation	John R. Vacca, Charles	River Media	2nd	2005
5.	Cyber Forensics - Concepts and Approaches	Ravi Kumar & B Jain	ICFAI press	1st	2009
6.	Computer Forensics: Investigating Network Intrusions and Cyber Crime	Ec-Council Press Series: Computer Forensics	EC-Council	2nd	2010

Course Outcomes:

- Discuss data and identify data sources
- Describe and discuss digital evidence
- Compare and contrast the differences between digital evidence and traditional evidence
- Discuss the ways in which digital evidence is authenticated
- Describe and critique digital forensics process models
- Critically evaluate standards and good practices for digital evidence and digital forensics

P. G. Diploma in Cyber Security, Law and Forensics (PGDCSLF)		**Semester – I**	
Course Name: Forensic technologies and Digital forensics		**Course Code: PGDCSLF105**	
Periods per week (1 Period is 60 minutes)		4	
Credits		4	
		Hours	**Marks**
Evaluation System	**Theory Examination**	2	40
	Internal	--	60

Course Objectives:

1. Describe digital forensics and relate it to an investigative process.
2. Explain the legal issues of preparing for and performing digital forensic analysis based on the investigator's position and duty.
3. Perform basic digital forensics.
4. Demonstrate use of digital forensics tools.
5. Guide a digital forensics exercise.
6. Recognize the state of the practice and the gaps in technology, policy, and legal issues.

Unit	Details	Lectures
I	Computer forensics fundamentals, Benefits of forensics, computer crimes, computer forensics evidence and courts, legal concerns and private issues. Introduction to legal issues, context, and digital forensics, Media Analysis: disk structure, file systems (NTFS, EXT 2/3, HFS), and physical layer issues.	**12**
II	Understanding Computing Investigations – Procedure for corporate High-Tech investigations, understanding data recovery work station and software, conducting and investigations.	**12**
III	Data acquisition- understanding storage formats and digital evidence, determining the best acquisition method, acquisition tools, validating data acquisitions, performing RAID data acquisitions, remote network acquisition tools, other forensics acquisitions tools.	**12**
IV	Processing crimes and incident scenes, securing a computer incident or crime, seizing digital evidence at scene, storing digital evidence, obtaining digital hash, reviewing case.	**12**
V	Current computer forensics tools- software, hardware tools, validating and testing forensic software, addressing data-hiding techniques, performing remote acquisitions, E-Mail investigations- investigating email crime and violations, understanding E-Mail servers, specialized E-Mail forensics tool.	**12**

Books and References:					
Sr. No.	**Title**	**Author/s**	**Publisher**	**Edition**	**Year**
1.	Computer Forensics: Incident Response Essentials	Warren G. Kruse II and Jay G. Heise	Addison Wesley	1st	2002
2.	Guide to Computer Forensics and Investigations	Nelson, B, Phillips, A, Enfinger, F, Stuart, C.	Thomson Course Technology	2nd	2006
3.	Computer Forensics, Computer Crime Scene Investigation	Vacca, J	Charles River Media	2nd	2005
4.	The Best Damn Cybercrime and Digital Forensics	Book Perio,Jack Wiles, Anthony Reyes , Jesse Varsalone	Syngress Publishing	1st	2007
5.	Computer Evidence and Computer Crime: Forensic Science, Computers, and the Internet	Casey, Eoghan	Cambridge University Press	1st	2000

Course Outcomes:

After completion of the course, a student should be able to:

- Know how to apply forensic analysis tools to recover important evidence for identifying computer crime.
- To be well-trained as next-generation computer crime investigators.
- Know how to apply the skills of forensic investigation
- know how to apply the forensic tools for forensic investigation

SEMESTER II

P. G. Diploma in Cyber Security, Law and Forensics (PGDCSLF)		**Semester – II**	
Course Name: IT Act 2000, IT Act Amendments and IPR in cyberspace		**Course Code: PGDCSLF201**	
Periods per week (1 Period is 60 minutes)		4	
Credits		4	
		Hours	**Marks**
Evaluation System	**Theory Examination**	2	40
	Internal	--	60

Course Objectives:

1. To understand the ethics and laws by which cyberspace is governed in our country and worldwide
2. To understand the Cr.PC and Indian Evidence Law
3. To disseminate knowledge on patents, patent regime in India and abroad and registration aspects
4. To aware about current trends in IPR and Govt. steps in fostering IPR

Unit	Details	Lectures
I	Cyber Space- Fundamental definitions -Interface of Technology and Law – Jurisprudence and-Jurisdiction in Cyber Space - Indian Context of Jurisdiction - Enforcement agencies – Need for IT act - UNCITRAL – E-Commerce basics, Information Technology Act, 2000 - Aims and Objects — Overview of the Act – Jurisdiction, New types of cyber crimes. Introduction to Indian Evidence Act, introduction to IT rules 2021	**12**
II	Electronic Governance – Legal Recognition of Electronic Records and Electronic Evidence -Digital/ electronic/ e-sign (Aadhaar) Signature - Securing Electronic records and secure digital signatures - Duties of Subscribers - Role of Certifying Authorities - Regulators (SEBI/RBI/AMPHI/IRDA) regulations for cyber space, Internet Service Providers and their Liability– Powers of Police under the Act – Impact of the Act on other Laws .	**12**
III	Cr.P.C and Indian Evidence Law - Cyber crimes under the Information Technology Act,2000 - Cyber crimes under International Law - Hacking Child Pornography, Cyber Stalking, Denial of service Attack, Virus Dissemination, Software Piracy, Internet Relay Chat (IRC) Crime, Credit Card Fraud, Net Extortion, Phishing etc - Cyber TerrorismViolation of Privacy on Internet - Data Protection and Privacy – Indian Court cases. Importance of Section 65 B-certificate under Indian Evidence Act (IEA)	**12**
IV	Intellectual Property Rights – Copyrights- Software – Copyrights vs Patents debate - Authorship and Assignment Issues - Copyright in Internet - Multimedia and Copyright issues - Plagiarism- Software Piracy - Trademarks - Trademarks in Internet – Copyright and Trademark cases, Domain names -registration - Domain Name Disputes-Cyber Squatting-IPR cases, WIPO arbitration	**12**
V	Patents - Understanding Patents - IP Types - European Position on Computer related Patents, Legal position on Computer related Patents - Indian Position on Patents – Case Law.	**12**

Books and References:					
Sr. No.	**Title**	**Author/s**	**Publisher**	**Edition**	**Year**
1.	Cyber Law and Cyber Crime	Adv.(Dr) Prashant Mali	SnowWhite / Cyber Infomedia	2nd	2020
2.	Cyber Laws	Justice Yatindra Singh	Universal Law Publishing Co	1st	2005
3.	Information Technology Law(Cyber Laws)	S.R.Myneni	Asia Law House	1st	2006
4.	Internet Law-Text and Material	Chris Reed	Cambridge University Pres	1st	2004
5.	Cyber Law- the Indian perspective U	Pawan Duggal	Universal Law Publishing Co	1st	2002
6	Intellectual Property Rights. India	Neeraj, P., & Khusdeep, D.	PHI learning Private Limited.	2nd	2014
7	WIPO Intellectual property Handbook	*Handbook*	World Intellectual Property Organisation		2004

Course Outcomes:

After completion of the course, a student should be able to:

- Learn the general principles in legal research and types of research
- Learn various legal research methods
- Understand the legal research processes and legal source
- Learn writing legal reports
- get an adequate knowledge on patent and copyright
- Understand the Patent and policies

P. G. Diploma in Cyber Security, Law and Forensics (PGDCSLF)		**Semester – II**	
Course Name: Cyber Psychology and Ethics		**Course Code: PGDCSLF202**	
Periods per week (1 Period is 60 minutes)		4	
Credits		4	
		Hours	**Marks**
Evaluation System	**Theory Examination**	2	40
	Internal	--	60

Course Objectives:

1. To acquaint learners with basic psychological terminology used in forensic psychology and cyber psychology
2. Understand and apply psychological assessment system
3. Interpret psychological profiles of offenders
4. Understand apply techniques to psychologically help the victims.
5. Apply psychological principles for public awareness and society.

Unit	Details	Lectures
I	**Understanding Psychology and Cybersecurity** Basic Principals of Psychology. Introduction to Forensic psychology. Ethical aspects of Psychological assessment and counselling Professional aspects of psychological assessment and counselling Documentation of the assessment and its utility as evidence.	**12**

II	**Psychology of Offenders** Motivations for Cybercrime Individual Differences (Personality), Social and Contextual Aspects, Observer described characteristics. Eye-witness testimony. Crime types and Psychology: instrumental crimes (ultimate aim is not harming victim) and expressive crimes (intent of harming the victim). Online dating, relationships, sex and related crimes. Financial Crimes.	**12**
III	**Forensic and Psychological Assessment** Psychological Profiling of Offenders. Detection of Malingering and Deception Personality Profile: FFM, Dark Tried, Clinical profiles. Interpreting profiles. Profiling and Linking Crimes: Sex crimes, revenge porn, and child pornography; Cyberbullying and Cyberstalking; Identity Theft; Financial crimes. Use of Brain mapping signatures: BEOS Psychological techniques for dealing with Offenders.	**12**
IV	**Psychological Reaction of Victim and Victim Counselling** Psychological Reactions for Cyberbullying and Cyberstalking, Revenge Porn, Identity Theft, Financial Loss. Cyber terrorism. Basic communication Skills. Crisis Intervention, Dealing with Loss and Grief. Psycho-education. Supportive Psychotherapy. Cognitive-Behaviour Interventions. Suicide/ Homicide risk assessments. Supporting further steps, Corrective action.	**12**

V	**Public Awareness and Society** Psychological Aspects of Decision-Making: Financial, Interpersonal (romantic and sexual relations). Using Psychological Principles for Prevention of Cybercrime. Educating Parents, Schools and Colleges: Financial Crimes and Sex-crimes in cyber space. Principles of large scale awareness and advocacy.	**12**

Books and References:

Sr. No.	**Title**	**Author/s**	**Publisher**	**Edition**	**Year**
1.	Cybercrime: Psychology of Online Offenders	Kirwan, G., & Power, A.	Cambridge University Press.	1st	2012
2.	Cyberpsychology: The Study of Individuals, Society and Digital Technologies	Whitty, M. and Young, G.	BPS Blackwell	1st edition	2016
3.	The psychology of Cybercrime.	Kirwan, G., & Power, A.	Information Science Reference	1st	2012
4	Forensic psychology	Scott, Adrian	Palgrave MacMillan.	1st	2010
5	Forensic Psychology (4 Vol set)	Bull, R. (ed)	Sage publications	1st	2011

6	Investigative Psychology: Offender Profiling and the Analysis of Criminal Action	Canter, D. and Youngs, D.	Wiley	1st	2009
7	The Cyber Effect	Aiken, M.	John Murray	1st	2016
8	Handbook of crime prevention and community safety	N. Tilley & A. Sidebottom (Eds.),	Routledge.	1st edition	2005

Course Outcomes:

After completion of the course, a student should be able to:

- Apply understanding of Psychological Intervention for dealing with Victims
- Apply understanding of Psychological Intervention for dealing with Offenders
- Apply understanding of Psychological Intervention for educating society at large
- Using psychological profiling typologies of online crime
    - Cybertrespass - hackers, crackers, breakers and online scammers, Cyberterrorism, Cyberdeception and theft – including identity theft and fraud, Cyberpornography and obscenity - from child to adult pornography and trafficking online, Cyberviolence – stalking, bullying, harassment, domestic abuse and hate speech
    - Classwork: Interpret Five profiles of different crimes as a class activity
    - Classwork: Learn to interpret reports of at least two kinds of psychological assessment

· Interpret psychological profiles of offenders.

· Understand and apply ethical and Professional aspects of the psychological intervention.

P. G. Diploma in Cyber Security, Law and Forensics (PGDCSLF)		**Semester – II**	
Course Name: Cyber Security Technology and Regulations		**Course Code: PGDCSLF203**	
Periods per week (1 Period is 60 minutes)		4	
Credits		4	
		Hours	**Marks**
Evaluation System	**Theory Examination**	2	40
	Internal	--	60

Course Objectives:

1. To train the learners with hacking skills and practising the professional ethics
2. To provide the knowledge of tools and techniques used by hackers and information security professionals alike to break into an organization.
3. To learn to secure the system and protect from the cyber attacks
4. To perform the network analysis using the forensic analysis tool

Unit	Details	Lectures
I	Ethical hacking process, Hackers behaviour & mindset, Maintaining Anonymity, Hacking Methodology, Information Gathering, Active and Passive Sniffing, Physical security vulnerabilities and countermeasures. Internal and External testing. Preparation of Ethical Hacking and Penetration Test Reports and Documents.	**12**
II	Social Engineering attacks and countermeasures. Password attacks, Privilege Escalation and Executing Applications, Network Infrastructure Vulnerabilities, IP spoofing, DNS spoofing, Wireless Hacking: Wireless footprint, Wireless scanning and enumeration, Gaining access (hacking 802.11), WEP, WPA, WPA2.	**12**
III	DoS attacks. Web server and application vulnerabilities, SQL injection attacks, Vulnerability Analysis and Reverse Engineering, Buffer overflow attacks. Client-side browser exploits, Exploiting Windows Access Control Model for Local Elevation Privilege. Exploiting vulnerabilities in Mobile Application	**12**

IV	Malware Forensics Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries , Identifying Packers using PEiD, Registry Forensics with Reg Ripper Plu-gins:, Bypassing Poison Ivy's Locked Files, Bypassing Conficker's File System ACL Restrictions, Detecting Rogue PKI Certificates. **Memory Forensics and Volatility** Memory Dumping with MoonSols Windows Memory Toolkit, Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps, Code Injection and Extraction, Detecting and Capturing Suspicious Loaded DLLs, Finding Artifacts in Process Memory, Identifying Injected Code, Using WHOIS to Research Domains, DNS Hostname Resolution, Querying, Passive DNS, Checking DNS Records, Reverse IP Search New Course Form, Creating Static Maps, Creating Interactive Maps. Case study of Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA	**12**
V	**Introduction to Met**reter, Introduction to Armitage, Installing and using Kali Linux Distribution, Introduction to penetration testing tools in Kali Linux. Case Studies of recent vulnerabilities and attacks, parrot.	**12**

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1	Ethical Hacking and Penetration Testing Guide	Baloch, R	CRC Press	1st	2015
2	Computer Forensics: Investigating Network Intrusions and Cybercrime,	E.C Council	Cengage Learning	2nd	2010
3	The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory	Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters	Wiley	1st	2014
4	A Electronic Discovery and Digital Evidence in a Nut Shell	Daniel J Capra,Shira A scheindlin	The Sedona Conerence-Academic Press.	1st	2009
5	Anti-Hacker Tool Kit	Mike Shema	Mike Shema	1st	2007

Course Outcomes:

After completion of the course, a student should be able to:

- understand how our defense measure works and then to scan their networks & attack their own

- To identify the different threats posed by hackers and other malicious attackers and how to protect our network & devices from those attacks.
- analyze the attacks and counterfeit them
- apply the forensic tools required for ethical hacking

P. G. Diploma in Cyber Security, Law and Forensics (PGDCSLF)		**Semester – I**	
Course Name: Crime Scene Management Practical		**Course Code: PGDCSLF105**	
Periods per week (1 Period is 60 minutes)		4	
Credits		4	
		Hours	**Marks**
Evaluation System	**Theory Examination**	2	40
	Internal	--	60

Course Objectives:

- Crime scene management skills are an extremely significant task component of investigation because evidence that originates at the crime scene will provide a picture of events for the court to consider in its deliberations.
- The significance of forensic science to human society.
- The fundamental principles and functions of forensic science
- The divisions in a forensic science laboratory.
- The working of the forensic establishments in India and abroad.

Unit	Details	Lectures
I	Primary Survey, Barrication, Scene Documentation, Forensic Photography – scene photography and its method, Identification	**12**
II	Recognition and Recovery of evidences, Basic types of evidence-visible, plastic , latent, micro & macro, trace and ultra-trace, pattern, fragile and digital evidence. Method for Search ,Collection (preservation), Handling packaging , Important evidence such as Impression evidence	**12**
III	Panchnaama (Spot Investigations and recording) - conducting, recording, authenticating with Pancha's, recovery of hard disk, mobile phone, CCTV (DVR) , electronic devices.	**12**
IV	Practical Scene videography (Clockwise and anti-Clockwise videography) special segment videography, CCTV(DVR machine) handling and export of logs and video files. Handling of voice recorder and specimen voice recording.	**12**
V	Crime Scene - Onsite Forensic Investigation Tools, Live data acquisition from standalone computer , network server, mobile phone, triage data acquisition	**12**

Books and References:					
Sr. No.	**Title**	**Author/s**	**Publisher**	**Edition**	**Year**
1.	Forensic Science in India : A vision for the Twenty First Centrury	B.B. Nanda and R.K Tiwari	Select publisher	1st	2001
2.	An Introduction to Forensic Sciences	W.G. Eckert and R.K. Wright	CRC Press	2nd	1997
3.	Fisher's Techniques of Crime scene Investigation	R. Saferstein, M.L. Hastrup and C.Hald	CRC Press	2nd	2013
4.	Fisher's Techniques of Crime Scene Investigation	W.J. Tilstone, M.L. Hastrup and C.Hald	CRC Press	2nd	2013
5.	Crime Scene Investigation: A Guide for Law Enforcement	Janet Reno,Daniel Marcus Acting Associate, Laurie Robinson, General Noël Brennan, General Jeremy Travis	Department of Justice Response Center	1st	2000

Course Outcomes:

After completion of the course, a student should be able to:

- handle the crime scenes with standard operating procedures
- implement the skills use to investigate different types of crime scenes such as CCTV and other digital evidence.
- apply the skills for data recovery at the crime scene
- apply skills used for data acquisition using forensic tools

P. G. Diploma in Cyber Security, Law and Forensics (PGDCSLF)		**Semester – I**	
Course Name: Dark web and Cyber warfare		**Course Code: PGDCSLF205**	
Periods per week (1 Period is 60 minutes)		4	
Credits		4	
		Hours	**Marks**
Evaluation System	**Theory Examination**	2	40
	Internal	--	60

Course Objectives:

1. To have deep understanding of the web
2. To gain knowledge on the working of Dark Web
3. To identify the security aspects of dark net.
4. To understand the operational procedures of cyber war and to have clarity on defense mechanism

Unit	Details	Lectures
I	Introduction. Surface Web, Deep Web and Dark Web. Usage of Dark Web. Working of dark web.The TOR browser and its history. Introduction to cyber weapons and its types, types of cyber attacks, types of state and non-state actors. Known cyber gang and non-state actor group.	**12**
II	Cryptocurrency and other currencies used in dark web, known market places on dark net, Silk Road case study	**12**
III	Anatomy of a Ransomware attack, Ransomware as a service. Wannacry, Locky. Sodinokibi - ransomware. Case study of ransomware attacks across the world, Selling access to servers. Renting Infrastructure. Selling Financial Details. Selling Personal Details.	**12**
IV	Identifying Darknet Cybersecurity risks.Dark web intelligence. The gray areas. Policing the shadows. Need for new regulations. Open source Intelligence (OSINT) tools. Intra-country data exchange of cyber criminals and regulations around it.	**12**
V	Cyber warfare, Security Measures, Dealing with Cyber terrorists, Stages of Defense: Prevention, Incident Management, Mitigating an Attack, Damage Limitation and Consequence Management. International cyber crime treaties. Law against darkweb and cyber warfare: World and Indian Scenario	**12**

Books and References:					
Sr. No.	**Title**	**Author/s**	**Publisher**	**Edition**	**Year**
1. .	Dark Web Investigation (Security Informatics and Law Enforcement)	Babak Akhgar (Editor), Marco Gercke (Editor), Stefanos Vrochidis (Editor)	Springer	1st	2021
2.	Inside the Dark Web	Erdal Ozkaya and Rafiqul Islam	CRC Press	1st	2020
3.	Tor and the Dark Net	James Smith	CRC Presss	1st	2016
4.	Online Privacy An Introduction to TOR Network and Online Security: How to stay anonymous in the Internet	Wiliam Rowley	--	1st	2016
5	Tor And The Deep Web	Leonard Eddison	The Complete Guide To Stay Anonymous In The Dark Net	1st	2018

Course Outcomes:

After completion of the course, a student should be able to:

- Able to work in Law enforcement for cyber crime investigation w.r.t to dark web and warfare
- able to understand the deep / dark web attacks
- able to identify the dark web attacks and handle the scenario
- able to use the deep web operating system and apply the security measures

Evaluation Scheme

- **Both Internal and External Examination will be conducted by the department**
- **The result declaration, marksheet and the Diploma will be awarded by the department**

Internal Evaluation (60 Marks)

The internal assessment marks shall be awarded as follows:

1. **Unitwise Quiz (10 Marks each unit): 10 marks Average**
2. **Problem Solving or Assignments(Practical based):20 Marks**
3. **Personation of topics assigned related to subject: 20 Marks**

External Examination: (40 marks) : Online MCQ as per the following format

	All questions are compulsory	
Q1	**(Based on Unit 1) 8 sub questions**	**8**
Q2	**(Based on Unit 2) 8 sub questions**	**8**
Q3	**(Based on Unit 3) 8 sub questions**	**8**
Q4	**(Based on Unit 4) 8 sub questions**	**8**
Q5	**(Based on Unit 5) 8 sub questions**	**8**

Practical Evaluation (50 marks)

A Certified copy of hard-bound journal is essential to appear for the practical examination.

1.	**Practical Question 1**	**20**
2.	**Practical Question 2**	**20**
3.	**Journal**	**5**
4.	**Viva Voce**	**5**

OR

1.	**Practical Question**	**40**
2.	**Journal**	**5**
3.	**Viva Voce**	**5**

Project Documentation and Viva Voce Evaluation

The documentation should be checked for plagiarism and as per UGC guidelines, should be less than 10%.

1.	**Documentation Report (1 to 4)**	**20**
2.	**Innovation in the topic**	**10**

3.	**Documentation/Topic presentation and viva voce**	**20**

Project Implementation and Viva Voce Evaluation

1.	**Documentation Report (5 to last)**	**20**
2.	**Implementation**	**10**
3.	**Relevance of the topic**	**10**
4.	**Viva Voce**	**10**

Appendix – 1

Project Documentation and Viva-voce (Semester II)

Goals of the course Project Documentation and Viva-Voce

The student should:

- be able to apply relevant knowledge and abilities, within the main field of study, to a given problem
- within given constraints, even with limited information, independently analyse and discuss complex inquiries/problems and handle larger problems on the advanced level within the main field of study
- reflect on, evaluate and critically review one’s own and others’ scientific results
- be able to document and present one’s own work with strict requirements on structure, format, and language usage
- be able to identify one’s need for further knowledge and continuously develop one’s own knowledge

To start the project:

- Start thinking early in the programme about suitable projects.
- Read the instructions for the project.
- Attend and listen to other student´s final oral presentations.
- Look at the finished reports.
- Talk to senior master students.
- Attend possible information events (workshops / seminars / conferences etc.) about the related topics.

Application and approval:

- Read all the detailed information about project.
- Finalise finding a place and supervisor.
- Check with the coordinator about subject/project, place and supervisor.
- Write the project proposal and plan along with the supervisor.
- Fill out the application together with the supervisor.
- Hand over the complete application, proposal and plan to the coordinator.
- Get an acknowledgement and approval from the coordinator to start the project.

During the project:

- Search, gather and read information and literature about the theory.
- Document well the practical work and your results.
- Take part in seminars and the running follow-ups/supervision.

- Think early on about disposition and writing of the final report.
- Discuss your thoughts with the supervisor and others.
- Read the SOP and the rest you need again.
- Plan for and do the mid-term reporting to the coordinator/examiner.
- Do a mid-term report also at the work-place (can be a requirement in some work-places).
- Write the first draft of the final report and rewrite it based on feedback from the supervisor and possibly others.
- Plan for the final presentation of the report.

Finishing the project:

- Finish the report and obtain an OK from the supervisor.
- Ask the supervisor to send the certificate and feedback form to the coordinator.
- Attend the pre-final oral presentation arranged by the Coordinator.
- Rewrite the final report again based on feedback from the opponents and possibly others.
- Prepare a title page and a popular science summary for your report.
- Send the completed final report to the coordinator (via plagiarism software)
- Rewrite the report based on possible feedback from the coordinator.
- Appear for the final exam.

Project Proposal/research plan

- The student should spend the first 1-2 weeks writing a 1-2 pages project plan containing:
  - Short background of the project
  - Aims of the project
  - Short description of methods that will be used
  - Estimated time schedule for the project
- The research plan should be handed in to the supervisor and the coordinator.
- Writing the project plan will help you plan your project work and get you started in finding information and understanding of methods needed to perform the project.

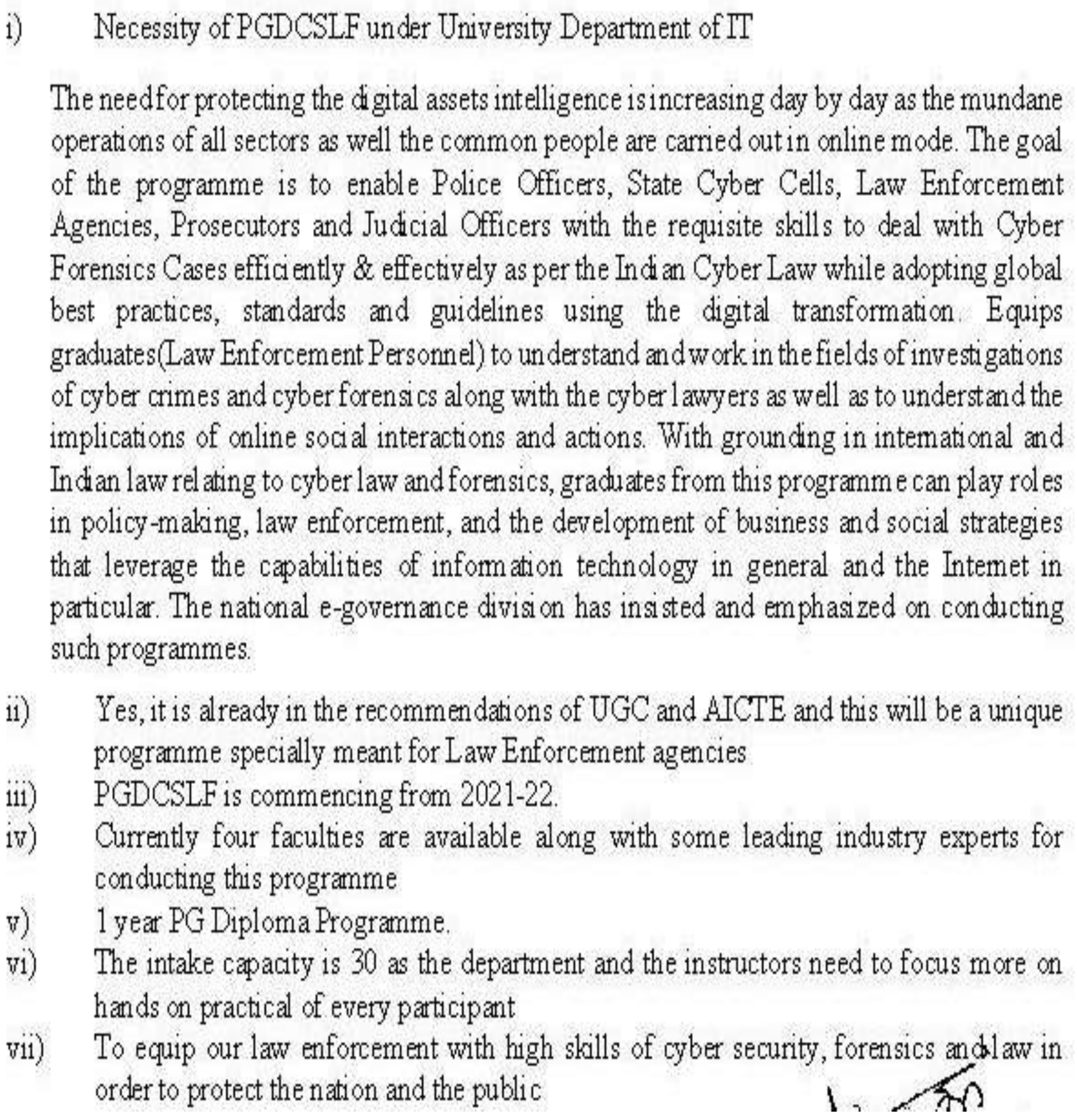
Project Documentation

The documentation should contain:

- Introduction - that should contain a technical and social (when possible) motivation of the project topic.
- Description of the problems/topics.
- Status of the research/knowledge in the field and literature review.
- Description of the methodology/approach. (The actual structure of the s here depends on the topic of the documentation.)
- Results - must always contain analyses of results and associated uncertainties.
- Conclusions and proposals for the future work.
- Appendices (when needed).
- Bibliography - references and links.

(Appendix ‘B’)

New ordinances 6717 & 6718 relating to the One Year P.G. Diploma in Cyber Security Law and Forensics (PGDCSLF)



i) Necessity of PGDCSLF under University Department of IT

The need for protecting the digital assets intelligence is increasing day by day as the mundane operations of all sectors as well the common people are carried out in online mode. The goal of the programme is to enable Police Officers, State Cyber Cells, Law Enforcement Agencies, Prosecutors and Judicial Officers with the requisite skills to deal with Cyber Forensics Cases efficiently & effectively as per the Indian Cyber Law while adopting global best practices, standards and guidelines using the digital transformation. Equips graduates(Law Enforcement Personnel) to understand and work in the fields of investigations of cyber crimes and cyber forensics along with the cyber lawyers as well as to understand the implications of online social interactions and actions. With grounding in international and Indian law relating to cyber law and forensics, graduates from this programme can play roles in policy-making, law enforcement, and the development of business and social strategies that leverage the capabilities of information technology in general and the Internet in particular. The national e-governance division has insisted and emphasized on conducting such programmes.

ii) Yes, it is already in the recommendations of UGC and AICTE and this will be a unique programme specially meant for Law Enforcement agencies

iii) PGDCSLF is commencing from 2021-22.

iv) Currently four faculties are available along with some leading industry experts for conducting this programme

v) 1 year PG Diploma Programme.

vi) The intake capacity is 30 as the department and the instructors need to focus more on hands on practical of every participant

vii) To equip our law enforcement with high skills of cyber security, forensics and law in order to protect the nation and the public