UNIVERSITY OF MUMBAI
No. UG/306 of 2017-18

CIRCULAR:-

Attention of the Principals of the affiliated Colleges in Science and Law and the Heads of the recognized Science Institutions is invited to this office Circular No. UG/113 of 2016-17, dated 25th, 2016 relating to syllabus of the Post Graduate Diploma in Digital and Cyber Forensic and Related Law. They are hereby informed that the recommendations made by Board of Studies in Forensic Science, under the Faculty of Science and Technology at its meeting held on 7th June, 2017 have been accepted by the Academic Council at its meeting held on 30th July, 2017 **vide** item No.4.4 and that in accordance therewith, the revised syllabus of Post Graduate Diploma in Digital and Cyber Forensic and Related Law (Sem. I & II) in Forensic Science, has been brought into force with effect from the academic year 2017-18, accordingly. (The same is available on the University's website : www.mu.ac.in)

(Dr. Dinesh Kamble)
I/c REGISTRAR

MUMBAI – 400 032
8th December, 2017
To

The Principals of the affiliated Colleges in Science and Law and the Heads of the recognized Science Institutions.

A.C/4.4/30/07/2017

****

No. UG/306 -A of 2017 MUMBAI-400 032 8th December, 2017

Copy forwarded with Compliments for information to:-

1) The Co-ordinator, Faculty of Science & Technology,
2) The Chairman, Board of Studies in Forensic Science .
3) The Director, Board of Examinations and Evaluation,
4) The Director, Board of Students Development,
5) The Co-Ordinator, University Computerization Centre,

(Dr. Dinesh Kamble)
I/c REGISTRAR

Academic Council :
Item No. :

UNIVERSITY OF MUMBAI

Syllabus for
Post Graduate Diploma in
Digital and Cyber Forensics
and Related Law

(Credit Based Semester and Grading System
with effect from the Academic Year 2017-2018)

Revised Syllabus for Post Graduate Diploma in Digital and Cyber Forensics and Related Law

O : Title of the Course	: Post Graduate Diploma in Digital and Cyber Forensics and Related Law
O : Eligibility	: The candidate who has passed Bachelor Degree from any Faculty with Subjects like Information Technology / Computer Science / Computer Application / Bioinformatics / Statistics / Mathematics / Electronics / Telecommunication / Physics / Chemistry / Forensic Science as one of the Subjects
R : Duration of the Course	: One Year (Full Time)
R : Fee Structure	: As per the University Circulars
R:Intake Capacity	: 40 (Forty)
R :Teacher Qualifications	:As per the U.G.C./ State Government Norms
R :Standard of Passing	:

a. Candidate who secures minimum 50% marks in each subject/paper be declared to have passed the examination in that subject.
b. A candidate who fails to secure 50% marks in a subject/Paper will be allowed to reappear in that subject/paper.
c. Candidate can carry forward at his/her option the marks in the subject/paper in which he/she has passed, in such a case student is entitled for award of class.
d. Candidate who secures a minimum of 50% marks in each paper and an aggregate of 60% and above marks on the whole shall be declared to have passed the examination in the First Class.
e. Candidate who secures a minimum of 50% marks in each paper and an aggregate of 70% and above marks on the whole shall be declared to have passed the examination in First Class with Distinction.

Medium of Instruction	: English

Revised Syllabus for Post Graduate Diploma in Digital and Cyber Forensics and Related Law

Scheme of Examination

Semester I

Paper	Title Of Paper	Maximum Marks	Minimum Passing Marks	Lectures (1 Hour Duration)	Paper Code
I	Computer Forensics – I	100	50	60	PGDCF101
II	Cyber Security – I	100	50	60	PGDCF102
III	Mobile Forensics – I	100	50	60	PGDCF103
IV	Cyber Law – I	100	50	60	PGDCF104
V	Cyber Forensic Practical –I	100	50	60	PGDCF106
VI	Cyber Forensic Practical –II	100	50	60	PGDCF106
---	**Grand Total**	**600**	**---**	**360**	**---**

Semester II

Paper	Title Of Paper	Maximum Marks	Minimum Passing Marks	Lectures (1 Hour Duration)	Paper Code
I	Computer Forensics – II	100	50	60	PGDCF 201
II	Cyber Security – II	100	50	60	PGDCF 202
III	Mobile Forensics – II	100	50	60	PGDCF 203
IV	Cyber Law – II	100	50	60	PGDCF 204
V	Cyber Forensic Practical –III	100	50	60	PGDCF 205
VI	Cyber Forensic Practical – IV	100	50	60	PGDCF 206
---	**Grand Total**	**600**	**---**	**360**	**---**

Revised Syllabus for Post Graduate Diploma in Digital and Cyber Forensics and Related Law

Scheme of Assessment

Theory

Assessment Type	Allocation of Marks		Total Marks
Internal Assessment	1. Periodical Class Test 2. Attendance and Participation 3. Overall Conduct as a Student	20 Marks 10 Marks 10 Marks	40 Marks
Semester End Examination	Question Paper Pattern - 1. Attempt any TWO of the following (Unit I) 2. Attempt any TWO of the following (Unit II) 3. Attempt any TWO of the following (Unit III) 4. Attempt any TWO of the following (Unit IV) 5. Attempt any THREE of the following (Unit I to IV)	 12 Marks 12 Marks 12 Marks 12 Marks 12 Marks	60 Marks
		Total	**100 Marks**

Practical

Paper	Allocation of Marks		Total Marks
V & VI	Practical Paper Pattern - 1. Assignment No. 1 2. Assignment No. 2 3. Practical Journal 4. Viva	 40 Marks 40 Marks 10 Marks 10 Marks	100 Marks

Revised Syllabus for Post Graduate Diploma in Digital and Cyber Forensics and Related Law

Semester I - Credits

Class	Title	Class Room Instruction Face to Face						50 Hours = 1 Credit				
P.G.D. D.C.F & R.L. Sem. –I		Per Week		15Weeks (Per Semester)		Per Semester (Hours)		Notional (Hours)		Credits		Total Credits
		L (60 Min)	P (60 Min)	L	P	L	P	L	P	L	P	
PGDCF 101	Computer Forensics – I	4		60		60		200		4		4
PGDCF 102	Cyber Security – I	4		60		60		200		4		4
PGDCF 103	Mobile Forensics – I	4		60		60		200		4		4
PGDCF 104	Cyber Law – I	4		60		60		200		4		4
PGDCF 105	Cyber Forensics Practical - I		4		60		60		100		2	2
PGDCF 106	Cyber Forensics Practical - II		4		60		60		100		2	2
Total	**--**	**16**	**08**	**240**	**120**	**240**	**120**	**800**	**200**	**16**	**04**	**20**

Revised Syllabus for Post Graduate Diploma in Digital and Cyber Forensics and Related Law

Semester I – Theory

PGDCF 101	Computer Forensics– I	4 Credits (60 Lect.)
Unit I	**Computer Basics– I** **Understanding Computer Hardware :** Looking Inside the Machine**,** Components of a Digital Computer, The Role of the Motherboard, The Roles of the Processor and Memory**,** The Role of Storage Media, Why This Matters to the Investigator**,** The Language of the Machine, Wandering Through a World of Numbers, Who's on Which Base? **Understanding the Binary Numbering System :** Converting Between Binary and Decimal**,** Converting Between Binary and Hexadecimal, Converting Text to Binary, Encoding Nontext Files, Why This Matters to the Investigator	**15 L**
Unit II	**Computer Basics – II** **Understanding Computer Operating Systems :** Understanding the Role of the Operating System Software**,** Differentiating Between Multitasking and Multiprocessing Types**,** Multitasking, Multiprocessing**,** Differentiating Between Proprietary and Open Source Operating Systems **An Overview of Commonly Used Operating Systems :** Understanding DOS**,** Windows 1.*x* Through 3.*x*, Windows 9*x* (95, 95b, 95c, 98, 98SE, and ME), Windows NT, Windows 2000, Windows XP, Linux/UNIX, Other Operating Systems **Understanding File Systems :** FAT12, FAT16, VFAT, FAT32, NTFS, Other File Systems	**15 L**
Unit III	**Networking Basics– I** **Understanding How Computers Communicate on a Network :** Sending Bits and Bytes Across a Network, Digital and Analog Signaling Methods, How Multiplexing Works, Directional Factors**,** Timing Factors, Signal Interference, Packets, Segments, Datagrams, and Frames, Access Control Methods, Network Types and Topologies, Why This Matters to the Investigator **Understanding Networking Models and Standards :** The OSI Networking Model, The DoD Networking Model, The Physical/Data Link Layer Standards, Why This Matters to the Investigator	**15 L**
Unit IV	**Networking Basics – II** **Understanding Network Hardware :** The Role of the NIC**,** The Role of the Network Media**,** The Roles of Network Connectivity Devices, Why This Matters to the Investigator **Understanding Network Software** **Understanding Client/Server Computing :** Server Software**,** Client Software**,** Network File Systems and File Sharing Protocols**,** A Matter of (Networking) Protocol **Understanding the TCP/IP Protocols Used on the Internet :** The	**15 L**

	Need for Standardized Protocols**,** A Brief History of TCP/IP**,** The Internet Protocol and IP Addressing**,** How Routing Works**,** The Transport Layer Protocols**,** The MAC Address**,** Name Resolution**,** TCP/IP Utilities**,** Network Monitoring Tools, Why This Matters to the Investigator	

PGDCF 102	**Cyber Security– I**	**4 Credits (60 Lect.)**
Unit I	**Basics of Security– I** Introduction to Security, Networking Basics, Data Gathering with Google	**15 L**
Unit II	**Basics of Security – II** Foot Printing, Scanning, Windows Security, Linux security	**15 L**
Unit III	**Basic Network Security– I** Theory of Proxy Server, Malwares and Trojans, Denial of Service	**15 L**
Unit IV	**Basic Network Security – II** Sniffers and Tools, Steganography and Steganalysis, Basics of Cryptography, Wireless Security and Attacks	**15 L**

PGDCF 103	Mobile Forensics - I	4 Credits (60 Lect.)
Unit I	**Introduction to Mobile Forensics– I** **Mobile Phone Basics** **Inside Mobile devices :** Cell Phone Crime**,** SIM Card**,** SIM Security **Mobile forensics :** Mobile forensic & its challenges **Mobile phone evidence extraction process :** The evidence intake phase, The identification phase**,** The preparation phase, The isolation phase, The processing phase, The verification phase, The document and reporting phase, The presentation phase **Practical mobile forensic approaches :** Mobile operating systems overview**,** Mobile forensic tool leveling system**,** Data acquisition methods	**15 L**
Unit II	**Introduction to Mobile Forensics – II** **Potential evidence stored on mobile phones** **Rules of evidence :** Admissible**,** Authentic**,** Complete**,** Reliable**,** Believable **Good forensic practices :** Securing the evidence**,** Preserving the evidence**,** Documenting the evidence**,** Documenting all changes **Windows Phone Forensics :** Windows Phone OS**,** Windows Phone file system **BlackBerry Forensics :** BlackBerry OS**,** BlackBerry analysis	**15 L**
Unit III	**Android Forensics - I** **The Android model :** The Linux kernel layer**,** Libraries**,** Dalvik virtual machine**,** The application framework layer**,** The applications layer **Android security :** Secure kernel**,** The permission model**,** Application sandbox**,** Secure interprocess communication**,** Application signing **Android file hierarchy** **Android file system :** Android file system analysis**,** Extended File System – EXT	**15 L**
Unit IV	**Android Forensics – II** **Android Forensic Setup and Pre Data Extraction Techniques :** A forensic environment setup**,** Screen lock bypassing techniques**,** Gaining root access **Android Data Extraction Techniques :** Imaging an Android Phone**,** Data extraction techniques **Android Data Recovery Techniques :** Data recovery**,** Overview of Forensic Tools**,** Forensic tools overview**,** Cellebrite – UFED**,** MOBILedit**,** Autopsy	**15 L**

PGDCF 104	Cyber Law– I	4 Credits (60 Lect.)
Unit I	**Cyber Forensic and Computer Crimes– I** **Introduction :** Conventional Crime**,** Cyber Crime**,** Reasons for Cyber Crime**,** Classification of Conventional and Cyber Crime**,** Distinction between Conventional and Cyber Crime**,** Cyber CriminalMode and Manner of Committing Cyber Crime**,** Computer Crime Prevention Measures **Crimes targeting Computers :** Unauthorized Access**,** Packet Sniffing**,** Malicious Codes including Trojans, Viruses, Logic Bombs, etc.	**15 L**
Unit II	**Cyber Forensic and Computer Crimes – II** Online based Cyber Crimes**,** Phishing and its Variants**,** Web Spoofing and E-mail Spoofing**,** Cyber Stalking**,** Web defacement**,** Financial Crimes, ATM and Card Crimes etc.**,** Spamming**,** Commercial espionage and Commercial Extortion online**,** Software and Hardware Piracy**,** Money Laundering**,** Fraud and Cheating	**15 L**
Unit III	**Provisions in Indian Laws– I** **Provisions in Indian Laws :** Penalties Under IT Act**,** Offences Under IT Act **Establishment of Authorities under IT Act and their functions, powers, etc. :** Controller, Certifying Authorities, Cyber Regulation Appellate Tribunal, Adjudicating officer	**15 L**
Unit IV	**Provisions in Indian Laws – II** Investigation of Cyber Crimes, Agencies for Investigation in India, their Powers and their Constitution as per Indian Laws, Procedures followed by First Responders, Evidence Collection and Seizure Procedures of Digital mediums	**15 L**

Revised Syllabus for Post Graduate Diploma in Digital and Cyber Forensics and Related Law

Semester I - Practical

PGDCF 105	Cyber Forensics Practical–I [Credits: 02 Practical/Week: 04]
1	Study and Analysis of Network.
2	Study of Network Related Commands (Windows)
3	Study of Network related Commands(Linux)
4	Collecting Information about given Domain
5	Crawling through Websites and Banner Grabbing
6	Using Google Search in Information Collection.
7	Network Scanning
8	Steganography
9	Remote Administration in Windows
10	Listing and Tracking Network Related Process.

PGDCF 106	Cyber Forensics Practical–II [Credits: 02 Practical/Week: 04]
1	Windows Log Analysis
2	Linux Log Analysis
3	Study of Windows Registry
4	Mobile/ Smart Phone Forensic Practical I
5	Mobile/ Smart Phone Forensic Practical II
6	Mobile/ Smart Phone Forensic Practical III
7	Mobile/ Smart Phone Forensic Practical IV

Revised Syllabus for Post Graduate Diploma in Digital and Cyber Forensics and Related Law

Semester II - Credits

Class	Title	Class Room Instruction Face to Face						50 Hours = 1 Credit				
P.G.D. D.C.F & R.L. Sem. – II		Per Week		15 Weeks (Per Semester)		Per Semester (Hours)		Notional (Hours)		Credits		Total Credits
		L (60 Min)	P (60 Min)	L	P	L	P	L	P	L	P	
PGDCF 201	Computer Forensics – II	4		60		60		200		4		4
PGDCF 202	Cyber Security – II	4		60		60		200		4		4
PGDCF 203	Mobile Forensics – II	4		60		60		200		4		4
PGDCF 204	Cyber Law – II	4		60		60		200		4		4
PGDCF 205	Cyber Forensics Practical - III		4		60		60		100		2	2
PGDCF 206	Cyber Forensics Practical - IV		4		60		60		100		2	2
Total	**--**	**16**	**8**	**240**	**120**	**240-**	**120**	**800**	**200**	**16**	**04**	**20**

Revised Syllabus for Post Graduate Diploma in Digital and Cyber Forensics and Related Law

Semester II - Theory

PGDCF 201	Computer Forensics – II	4 Credits (60 Lect.)
Unit I	**Computer Forensics Technology - I** **Computer Forensic Fundamentals :** Introduction to Computer Forensics**,** Use of Computer Forensics in Law Enforcement**,** Computer Forensic Services **Types of Computer Forensic Technology :** Types of Military Computer Forensic Technology**,** Types of Law Enforcement : Computer Forensic Technology**,** Types of Business Computer Forensic Technology**,** Specialized Forensic Techniques **Types of Computer Forensics Systems :** Internet Security Systems, Intrusion Detection Systems**,** Firewall Security Systems**,** Storage Area Network Security Systems**,** Network Disaster Recovery Systems**,** Public Key Infrastructure Systems**,** Wireless Network Security Systems**,** Satellite Encryption Security Systems**,** Instant Messaging (IM) Security Systems**,** Net Privacy Systems**,** Identity Management Security Systems**,** Identity Theft**,** Biometric Security Systems**,** Homeland Security Systems	**15 L**
Unit II	**Computer Forensics Technology – II** **Data Recovery :** Data Recovery Defined**,** Data Backup and Recovery**,** The Role of Backup in Data Recovery**,** The Data-Recovery Solution**,** Hiding and Recovering Hidden Data **Evidence Collection and Data Seizure :** Why Collect Evidence**,** Collection Options**,** Obstacles**,** Types of Evidence**,** The Rules of Evidence**,** Volatile Evidence**,** General Procedure**,** Collection and Archiving**,** Methods of Collection**,** Artifacts**,** Collection Steps**,** Controlling Contamination**,** Reconstructing the Attack	**15 L**
Unit III	**Operating System Investigation – I** Window, Windows Everywhere, NTFS Overview, Forensic Analysis of NTFS MF, Metadata, Artifacts of User Activities, Deletion and Destruction of Data, Windows Internet and Communications Activities, Windows Process Memory, Bitlocker and EFS, RAIDs and Dynamic Disks	**15 L**
Unit IV	**Operating System Investigation – II** Introduction to Unix, Boot Process, Forensic Duplication Consideration, File Systems, User Accounts, System Configuration, Artifacts of User Activities, Internet Communications, Firefox 3, Cache, Saved Sessions, E-Mail Analysis, Chat Analysis, Memory and Swap Space	**15 L**

PGDCF 202	Cyber Security– II	4 Credits (60 Lect.)
Unit I	**Advanced Network Security – I** Firewall, IDS and IPS, Theory of Vulnerability Assessment	**15 L**
Unit II	**Advanced Network Security – II** Introduction to Penetration Testing, Session Hijacking	**15 L**
Unit III	**Database and Other Security - I** Introduction to Web Server, SQL Security and Attacks, Cross Side Scripting	**15 L**
Unit IV	**Database and Other Security - II** Reverse Engineering, Email Analysis and Sending Fake Email, Incident Response	**15 L**

PGDCF 203	Mobile Forensics - II	4 Credits (60 Lect.)
Unit I	**iOS Forensics –I** **Understanding the Internals of iOS Devices :** iPhone models, iPhone hardware**,** iPad models**,** iPad hardware**,** File system**,** The HFS Plus file system**,** Disk layout**,** iPhone operating system **Data Acquisition from iOS Devices :** Operating modes of iOS devices**,** Physical acquisition **Difference between Android and iOS**	**15 L**
Unit II	**iOS Forensics – II** **iOS Data Analysis and Recovery :** Timestamps, SQLite databases**,** Property lists**,** Other important files**,** Recovering deleted SQLite records **Overview of iOS Forensic Tools and its features :** Elcomsoft iOS Forensic Toolkit, Oxygen Forensic Suite 2014**,** Cellebrite UFED Physical Analyzer**,** Paraben iRecovery Stick	**15 L**
Unit III	**Mobile Malware Analysis** **Introduction to Mobile Malware :** Toll fraud, SMS spoofing **Phishing :** Types of phishing, Spear phishing**,** How spear phishing works, Other examples**,** How it works**,** The mobile user's security **Virus/worms/others** **Future threats** **Steps you can take to protect yourself**	**15 L**
Unit IV	**Mobile Malware Analysis** **Android Malware Threats, Hoaxes, and Taxonomy** **Analyzing Mobile Malware :** Learning about Dynamic Analysis**,** Static Analysis**,** Android app analysis**,** Analysis Technique**,** Android app analysis**,** Android manifest and permissions, Reverse engineering Android apps **Overview of App Analysis tools**	**15 L**

PGDCF 204	Cyber Law– II	4 Credits (60 Lect.)
Unit I	**E-Commerce and E-Governance - I** International Organizations and Their Roles, ICANN, UDRP Dispute Resolution Policy, WTO and TRIPS, UNICITRAL Model LAW	**15 L**
Unit II	**E-Commerce and E-Governance– II** IT Act, Digital Signature, E-Commerce, E-Governance, Evolution of IT Act; Genesis and Necessity, Digital/ Electronic Signature - Analysis in the background of Indian Laws, E-Commerce; Issues and Provisions in Indian Law, E-Governance; Concept and Practicality in India, E-Taxation issues in Cyberspace	**15 L**
Unit III	**Intellectual Property Rights in Digital Medium – I** Domain Names and Trademark Disputes**,** Concept of Trademark/Domain Name**,** Cyber Squatting**,** Reverse Hijacking	**15 L**
Unit IV	**Intellectual Property Rights in Digital Medium – II** Concept of Copyright and Patent in Cyberspace, Copyright in the Digital Medium, Copyright in Computer Programmes, Copyright and WIPO Treaties	**15 L**

Revised Syllabus of Post Graduate Diploma in Digital and Cyber Forensics and Related Law

Semester II - Practical

PGDCF 205	Cyber Forensics Practical–III [Credits: 02 Practical/Week: 04]
1	Study of Network Attacks
2	Study of Wireless Network and Attacks
3	Firewall Configuration
4	Study of IDS/IPS
5	Study of web server
6	Study of SQL Injections
7	Study of XSS
8	Introduction to penetration testing
9	Reverse Engineering
10	Incident Response

PGDCF 206	Cyber Forensics Practical – IV [Credits: 02 Practical/Week: 04]
1	Mobile/ Smart Phone Forensic Practical – V
2	Mobile/ Smart Phone Forensic Practical – VI
3	Mobile/ Smart Phone Forensic Practical – VIII
4	Windows Investigation Practical – I
5	Windows Investigation Practical – II
6	Linux Investigation Practical – I
7	Linux Investigation Practical – II
8	Email Investigation

Revised Syllabus of Post Graduate Diploma in Digital and Cyber Forensics and Related Law

Semester I and II - References

PGDCF101 : ComputerForensics –I
PGDCF 201 : Computer Forensics - II

Sr. No.	Suggested Readings
1	Computer Forensics – Computer Crime Scene Investigation, Second Edition, John R. Vacca, Charles River Media Inc., ISBN 1-58450-389-0
2	Scene of the Cybercrime – Computer Forensics Handbook, Debra Littlejohn Shinder, Ed Tittel, Syngress Publishing Inc., 2002, ISBN 1-931836-65-5
3	Handbook of Digital Forensics and Investigation, Edited by Eoghan Casay, Elsevier Academic Press, ISBN 13 : 978-0-12-374267-4

Sr. No.	Additional Suggested Readings
1	Computer Forensics for Dummies
2	Cyber Crime Investigations by Anthony Ryes
3	Computer Forensics : A Field Manual for Cancelling, Examining, and Preserving Evidence of Computer Crimes by Albert J. Marcella
4	Cyber Crime Investigator's Field Guide by Bruce Middleton
5	Digital Forensics : Digital Evidence in Criminal Investigation by Angus M. Marshall
6	Digital Forensics for Network, Internet and Cloud Computing by Clint P. Garrison
7	A Practical Guide to Computer Forensics Investigations by Dr. Darren R. Heyes

PGDCF 102 : Cyber Security– I
PGDCF 202 : Cyber Security - II

Sr. No.	Suggested Readings
1	Certified Information (Security Expert, Main Book, Innobuss Knowledge Solutions (P) Ltd.

Sr. No.	Additional Suggested Readings
1	Certified Ethical Hacker Manual
2	www.hackthissite.org

PGDCF 103 : Mobile Forensics– I
PGDCF 203 : Mobile Forensics - II

Sr. No.	Suggested Readings
1	Practical Mobile Forensics, Satish Bommisetty, Rohit Tamma, Heather Mahalik, Packt Publishing Ltd., 2014,ISBN 978-1-78328-831-1
2	Learning iOS Forensics, Mattia Epifani, Pasquale Stirparo,Packt Publishing Ltd, 2015 ISBN 978-1-78355-351-8
3	Guide to Computer Forensics and Investigations, Fourth Edition, Bill Nelson, Amelia Phillips, Christopher Steuart, Cengage Learning,2010,ISBN-13: 978-1-435-49883-9 ,ISBN-10: 1-435-49883-6
4	Wireless Crime and Forensic Investigation, Gregory Kipper,Auerbach Publications
5	Mobile Malware Attacks and Defense, Ken Dunham, Syngress Publishing, Inc.,ISBN 978-1-59749-298-0

Sr. No.	Additional Suggested Readings
1	Digital Evidence and Computer Crime, Third Edition Eoghan Casey.Published by Elsevier Inc
2	Andriod Forensic, Investigation, and Security by Andrew Hogg, Publisher Synergy
3	iPhone and iOS Forensics Investigation, Analysis and Mobile Security for Apple iPhone, iPad, and iOS Devices by Andrew Hoog, Katie Strzempka ,Publisher Synergy
4	Mobile phone security and forensics: A practical approach *by* Iosif I. Androulidakis, Springer publications, 2012
5	The basics of digital forensics : the primer for getting started in digital forensics, John Sammons., Syngress publisher ,2012

PGDCF 104 : Cyber Law – I
PGDCF 204 : Cyber Law – II

Sr. No.	Suggested Readings
1	The Law of Evidence, Dr. Sr. Myneni, New Edition, Asian Law House, 2010.
2	E-Commerce – The Cutting Edge of Business, Second Edition, Bajaj Nagar, Tata McGraw Hill, 2011.
3	Information Technology Law and Practice by Vakul Sharma- Universal Law Publishing Co. Pvt. Ltd.
4	The Code of Criminal Procedure, 21st Edition, Ratanlal and Dirajlal, Lexus Nexis, 2009.
5	Law Relating to Intellectual Property, Dr. B.L. Wadehra, Fifth Edition, Universal Law Publication, 2011.

Sr. No.	Additional Suggested Readings
1	Cyber Law in India by Farooq Ahmad- Pioneer Books
2	The Indian Cyber Law by Suresh T. Vishwanathan- Bharat Law House New Delhi
3	Guide to Cyber and E- Commerce Laws by P.M. Bukshi and R.K. Suri- Bharat Law House, New Delhi
4	Guide to Cyber Laws by Rodney D. Ryder- Wadhwa and Company, Nagpur
5	The Regulation of Cyberspace by Andrew Murray, 2006- Routledge –Cavendish