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 2015-2016)

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	: Bachelor Degree in Science, Psychology, Law, Engineering, IT, Computer Science, Medical Science
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

Fee Structure

Particular	Amount
Government Share	460
University Share	540
Other Fees/ Extra-Curricular Activities	250
Laboratory Fees	6000
Gymkhana Fees	1000
Vice Chancellor's Fund	400
Magazine Fees	20
ID Card and Library Card	50
Group Insurance	40
Student Welfare Fund	50
University Sports and Cultural Activities	30
Development Fund	500
Disaster Relief Fund	10
Utility Fees	250
Computer/ Internet	500
E-Suvidha	50
E-Charges	20
Project Fees	2000
Registration Fees	875
Sub Total	13145
Refundable	
Caution Money	150
Library Deposit	250
Laboratory Deposit	400
Sub Total	800
Total Rs.	**13945**
Wherever Applicable	
Form and Prospectus Fees	100
Admission Processing Fees	200
Transfer Certificate	100
Bonafide Certificate	020
No Objection Certificate	020
Alumni Association Fees	100
(To be collected from the Student at the time of Admission)	

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	PGDCF 101
II	Cyber Security – I	100	50	60	PGDCF 102
III	Mobile Forensics – I	100	50	60	PGDCF 103
IV	Cyber Law – I	100	50	60	PGDCF 104
V	Cyber Forensic Practical - I	100	50	60	PGDCF 105
VI	Cyber Forensic Practical – II	100	50	60	PGDCF 106
---	**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	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
VI	Practical Paper Pattern – 1. Case Documentation 2. Field Visit Report 3. Project/Case Work 4. Project/Case Presentation 5. Viva	 20 Marks 20 Marks 20 Marks 20 Marks 20 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		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 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

Course Code	Title	Credits
PGDCF 101	**Computer Forensics – I**	**4**
Unit No.	**Contents of Unit**	**No. of Lectures**
Unit I	**Computer Basics – I** 1.1. Introduction 1.2. Understanding Computer Hardware 1.2.1 Looking Inside the Machine 1.2.2 Components of a Digital Computer 1.2.3 The Role of the Motherboard 1.2.4 The Roles of the Processor and Memory 1.2.5 The Role of Storage Media 1.2.6 Why This Matters to the Investigator 1.2.7 The Language of the Machine 1.2.8 Wandering Through a World of Numbers 1.2.9 Who's on Which Base? 1.3. Understanding the Binary Numbering System 1.3.1 Converting Between Binary and Decimal 1.3.2 Converting Between Binary and Hexadecimal 1.3.3 Converting Text to Binary 1.3.4 Encoding Nontext Files 1.3.5 Why This Matters to the Investigator	**15**
Unit II	**Computer Basics – II** 2.1. Understanding Computer Operating Systems 2.1.1 Understanding the Role of the Operating System Software 2.1.2 Differentiating Between Multitasking and Multiprocessing Types 2.1.3 Multitasking 2.1.4 Multiprocessing 2.1.5 Differentiating Between Proprietary and Open Source Operating Systems 2.2. An Overview of Commonly Used Operating Systems 2.2.1 Understanding DOS 2.2.2 Windows 1.*x* Through 3.*x* 2.2.3 Windows 9*x* (95, 95b, 95c, 98, 98SE, and ME) 2.2.4 Windows NT 2.2.5 Windows 2000 2.2.6 Windows XP 2.2.7 Linux/UNIX 2.2.8 Other Operating Systems 2.3. Understanding File Systems	**15**

	2.3.1 FAT12 2.3.2 FAT16 2.3.3 VFAT 2.3.4 FAT32 2.3.5 NTFS 2.3.6 Other File Systems	
Unit III	**Networking Basics – I** 3.1. Introduction 3.2. Understanding How Computers Communicate on a Network 3.2.1 Sending Bits and Bytes Across a Network 3.2.2 Digital and Analog Signaling Methods 3.2.3 How Multiplexing Works 3.2.4 Directional Factors 3.2.5 Timing Factors 3.2.6 Signal Interference 3.2.7 Packets, Segments, Datagrams, and Frames 3.2.8 Access Control Methods 3.2.9 Network Types and Topologies 3.2.10 Why This Matters to the Investigator 3.3. Understanding Networking Models and Standards 3.3.1 The OSI Networking Model 3.3.2 The DoD Networking Model 3.3.3 The Physical/Data Link Layer Standards 3.3.4 Why This Matters to the Investigator	**15**
Unit IV	**Networking Basics – II** 4.1. Understanding Network Hardware 4.1.1 The Role of the NIC 4.1.2 The Role of the Network Media 4.1.3 The Roles of Network Connectivity Devices 4.1.4 Why This Matters to the Investigator 4.2. Understanding Network Software 4.3. Understanding Client/Server Computing 4.3.1 Server Software 4.3.2 Client Software 4.3.3 Network File Systems and File Sharing Protocols 4.3.4 A Matter of (Networking) Protocol 4.4. Understanding the TCP/IP Protocols Used on the Internet 4.4.1 The Need for Standardized Protocols 4.4.2 A Brief History of TCP/IP 4.4.3 The Internet Protocol and IP Addressing 4.4.4 How Routing Works 4.4.5 The Transport Layer Protocols 4.4.6 The MAC Address 4.4.7 Name Resolution 4.4.8 TCP/IP Utilities 4.4.9 Network Monitoring Tools 4.4.10 Why This Matters to the Investigator	**15**

Course Code	Title	Credits
PGDCF 102	**Cyber Security – I**	**4**
Unit No.	**Contents of Unit**	**No. of Lectures**
Unit I	**Basics of Security – I** 1.1. Introduction to Security 1.2. Networking Basics 1.3. Data Gathering with Google	**15**
Unit II	**Basics of Security – II** 2.1. Foot Printing 2.2. Scanning 2.3. Windows Security 2.4. Linux security	**15**
Unit III	**Basic Network Security – I** 3.1. Theory of Proxy Server 3.2. Malwares and Trojans 3.3. Denial of Service	**15**
Unit IV	**Basic Network Security – II** 4.1. Sniffers and Tools 4.2. Steganography and Steganalysis 4.3. Basics of Cryptography 4.4. Wireless Security and Attacks	**15**

Course Code	Title	Credits
PGDCF 103	**Mobile Forensics - I**	**4**
Unit No.	**Contents of Unit**	**No. of Lectures**
Unit I	**Introduction to Mobile Forensics – I** 1.1. Mobile Phone Basics 1.2. Inside Mobile devices 1.2.1 Cell Phone Crime 1.2.2 SIM Card 1.2.3 SIM Security 1.3 Mobile forensics 1.3.1 Mobile forensic & its challenges 1.4 Mobile phone evidence extraction process 1.4.1 The evidence intake phase 1.4.2 The identification phase 1.4.3 The preparation phase, 1.4.4 The isolation phase, 1.4.5 The processing phase, 1.4.6 The verification phase, 1.4.7 The document and reporting phase , 1.4.8 The presentation phase 1.5 Practical mobile forensic approaches 1.5.1 Mobile operating systems overview 1.5.2 Mobile forensic tool leveling system 1.5.3 Data acquisition methods	**15**
Unit II	**Introduction to Mobile Forensics – II** 2.1. Potential evidence stored on mobile phones 2.2. Rules of evidence 2.2.1 Admissible 2.2.2 Authentic 2.2.3 Complete 2.2.4 Reliable 2.2.5 Believable 2.3 Good forensic practices 2.3.1 Securing the evidence 2.3.2 Preserving the evidence 2.3.3 Documenting the evidence 2.3.4 Documenting all changes 2.4 Windows Phone Forensics 2.4.1 Windows Phone OS 2.4.2 Windows Phone file system 2.4.3 Data acquisition 2.5 BlackBerry Forensics 2.5.1 BlackBerry OS 2.5.2 Data acquisition 2.5.3 BlackBerry analysis	**15**

Unit III	**Android Forensics - I** 3.1. The Android model 3.1.1 The Linux kernel layer 3.1.2 Libraries 3.1.3 Dalvik virtual machine 3.1.4 The application framework layer 3.1.5 The applications layer 3.2. Android security 3.2.1. Secure kernel 3.2.2. The permission model 3.2.3. Application sandbox 3.2.4. Secure interprocess communication 3.2.5. Application signing 3.3. Android file hierarchy 3.4. Android file system 3.4.1 Viewing file systems on an Android device 3.4.2 Extended File System – EXT	**15**
Unit IV	**Android Forensics – II** 4.1. Android Forensic Setup and Pre Data Extraction Techniques 4.1.1 A forensic environment setup 4.1.2 Screen lock bypassing techniques 4.1.3 Gaining root access 4.2. Android Data Extraction Techniques 4.2.1 Imaging an Android Phone 4.2.2 Data extraction techniques 4.3. Android Data Recovery Techniques 4.3.1. Data recovery 4.4. Android App Analysis and Overview of Forensic Tools 4.4.1 Android app analysis 4.4.2 Reverse engineering Android apps 4.4.3 Forensic tools overview 4.4.4 Cellebrite – UFED 4.4.5 MOBILedit 4.4.6 Autopsy	**15**

Course Code	Title	Credits
PGDCF 104	**Cyber Law – I**	**4**

Unit No.	Contents of Unit	No. of Lectures
Unit I	**Cyber Forensic and Computer Crimes – I** 1.1. Introduction 1.1.1 Conventional Crime 1.1.2 Cyber Crime 1.1.3 Reasons for Cyber Crime 1.1.4 Classification of Conventional and Cyber Crime 1.1.5 Distinction between Conventional and Cyber Crime 1.1.6 Cyber Criminal Mode and Manner of Committing Cyber Crime 1.1.7 Computer Crime Prevention Measures 1.2. Crimes targeting Computers 1.2.1 Unauthorized Access 1.2.2 Packet Sniffing 1.2.3 Malicious Codes including Trojans, Viruses, Logic Bombs, etc.	**15**
Unit II	**Cyber Forensic and Computer Crimes – II** 2.1. Online based Cyber Crimes 2.2. Phishing and its Variants 2.3. Web Spoofing and E-mail Spoofing 2.4. Cyber Stalking 2.5. Web defacement 2.6. Financial Crimes, ATM and Card Crimes etc. 2.7. Spamming 2.8. Commercial espionage and Commercial Extortion online 2.9. Software and Hardware Piracy 2.10. Money Laundering 2.11. Fraud and Cheating	**15**
Unit III	**Provisions in Indian Laws – I** 3.1.Provisions in Indian Laws 3.1.1 Penalties Under IT Act 3.1.2 Offences Under IT Act 3.2. Establishment of Authorities under IT Act and their functions, powers, etc. 3.2.1 Controller 3.2.2 Certifying Authorities 3.2.3 Cyber Regulation Appellate Tribunal 3.2.4 Adjudicating officer	**15**
Unit IV	**Provisions in Indian Laws – II** 4.1. Investigation of Cyber Crimes 4.2. Agencies for Investigation in India, their Powers and their Constitution as per Indian Laws 4.3. Procedures followed by First Responders 4.4. Evidence Collection and Seizure Procedures of Digital mediums	**15**

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

Semester I - Practical

Course Code	Title	Credits
PGDCF 105	**Cyber Forensics Practical – I**	**2**
Practical No.	**Title of the Practical**	**No. of Practical**
1	Study and Analysis of Network.	1
2	Study of Network Related Commands (Windows)	1
3	Study of Network related Commands(Linux)	1
4	Collecting Information about given Domain	1
5	Crawling through Websites and Banner Grabbing	1
6	Using Google Search in Information Collection.	1
7	Network Scanning	1
8	Windows/ Linux Log Analysis	1
9	Study of Windows Registry	1
10	Study of Malwares	1
11	Remote Administration in Windows	1
12	Listing and Tracking Network Related Process.	1
13	Mobile/ Smart Phone Forensic Practical I	1
14	Mobile/ Smart Phone Forensic Practical II	1
15	Mobile/ Smart Phone Forensic Practical III	1

Course Code	Title	Credits
PGDCF 106	**Cyber Forensics Practical – II**	**2**
Practical No.	**Title of the Practical**	**No. of Practical**
1	Digital and Cyber Forensic Case Documentation	02
2	Field/Industrial Visit – Report	02
3	Project/Case Work – Topic Approval for Synopsis	02
4	Project/Case Work – Objective and Work Plan	02
5	Project/Case Work – Review of Literature	04
6	Project/Case Work – Documentation and Presentation	03

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**	**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 II - Theory

Course Code	Title	Credits
PGDCF 201	**Computer Forensics – II**	**4**
Unit No.	**Contents of Unit**	**No. of Lectures**
Unit I	**Computer Forensics Technology - I** 1.1. Computer Forensic Fundamentals 1.1.1 Introduction to Computer Forensics 1.1.2 Use of Computer Forensics in Law Enforcement 1.1.3 Computer Forensic Services 1.2. Types of Computer Forensic Technology 1.2.1 Types of Military Computer Forensic Technology 1.2.2 Types of Law Enforcement : Computer Forensic Technology 1.2.3 Types of Business Computer Forensic Technology 1.2.4 Specialized Forensic Techniques 1.3. Types of Computer Forensics Systems 1.3.1 Internet Security Systems 1.3.2 Intrusion Detection Systems 1.3.3 Firewall Security Systems 1.3.4 Storage Area Network Security Systems 1.3.5 Network Disaster Recovery Systems 1.3.6 Public Key Infrastructure Systems 1.3.7 Wireless Network Security Systems 1.3.8 Satellite Encryption Security Systems 1.3.9 Instant Messaging (IM) Security Systems 1.3.10 Net Privacy Systems 1.3.11 Identity Management Security Systems 1.3.12 Identity Theft 1.3.13 Biometric Security Systems 1.3.14 Homeland Security Systems	**15**
Unit II	**Computer Forensics Technology – II** 2.1.Data Recovery 2.2.1 Data Recovery Defined 2.2.2 Data Backup and Recovery 2.2.3 The Role of Backup in Data Recovery 2.2.4 The Data-Recovery Solution 2.2.5 Hiding and Recovering Hidden Data 2.2. Evidence Collection and Data Seizure 2.2.1 Why Collect Evidence 2.2.2 Collection Options 2.2.3 Obstacles	**15**

	2.2.4 Types of Evidence 2.2.5 The Rules of Evidence 2.2.6 Volatile Evidence 2.2.7 General Procedure 2.2.8 Collection and Archiving 2.2.9 Methods of Collection 2.2.10 Artifacts 2.2.11 Collection Steps 2.2.12 Controlling Contamination 2.2.13 Reconstructing the Attack	
Unit III	**Operating System Investigation – I** 3.1.Window, Windows Everywhere 3.2.NTFS Overview 3.3.Forensic Analysis of NTFS MFT 3.4.Metadata 3.5.Artifacts of User Activities 3.6.Deletion and Destruction of Data 3.7.Windows Internet and Communications Activities 3.8.Windows Process Memory 3.9.Bitlocker and EFS 3.10. RAIDs and Dynamic Disks	**15**
Unit IV	**Operating System Investigation – II** 4.1.Introduction to Unix 4.2.Boot Process 4.3.Forensic Duplication Consideration 4.4.File Systems 4.5.User Accounts 4.6.System Configuration 4.7.Artifacts of User Activities 4.8.Internet Communications 4.9.Firefox 3 4.10. Cache 4.11. Saved Sessions 4.12. E-Mail Analysis 4.13. Chat Analysis 4.14. Memory and Swap Space	**15**

Course Code	Title	Credits
PGDCF 202	**Cyber Security – II**	**4**
Unit No.	**Contents of Unit**	**No. of Lectures**
Unit I	**Advanced Network Security – I** 1.1. Firewall 1.2. IDS and IPS 1.3. Theory of Vulnerability Assessment	**15**
Unit II	**Advanced Network Security – II** 2.1.Introduction to Penetration Testing 2.2.Session Hijacking	**15**
Unit III	**Database and Other Security - I** 3.1. Introduction to Web Server 3.2. SQL Security and Attacks 4.5.Cross Side Scripting	**15**
Unit IV	**Database and Other Security - II** 4.1. Reverse Engineering 4.2. Email Analysis and Sending Fake Email 4.1. Incident Response	**15**

Course Code	Title	Credits
PGDCF 203	**Mobile Forensics - II**	**4**
Unit No.	**Contents of Unit**	**No. of Lectures**
Unit I	**iOS Forensics – I** 1.1. Understanding the Internals of iOS Devices 1.1.1 iPhone models 1.1.2 iPhone hardware 1.1.3 iPad models 1.1.4 iPad hardware 1.1.5 File system 1.1.6 The HFS Plus file system 1.1.7 Disk layout 1.1.8 iPhone operating system 1.2. Data Acquisition from iOS Devices 1.2.1 Operating modes of iOS devices 1.2.2 Physical acquisition 1.2.3 Acquisition via a custom ramdisk 1.2.4 Acquisition via jailbreaking 1.3. Data Acquisition from iOS Backups 1.3.1 iTunes backup 1.3.2 iCloud backup	**15**
Unit II	**iOS Forensics – II** 2.1. iOS Data Analysis and Recovery 2.1.1 Timestamps 2.1.2 SQLite databases 2.1.3 Property lists 2.1.4 Other important files 2.1.5 Recovering deleted SQLite records 2.2. iOS Forensic Tools 2.2.1 Elcomsoft iOS Forensic Toolkit 2.2.2 Oxygen Forensic Suite 2014 2.2.3 Cellebrite UFED Physical Analyzer 2.2.4 Paraben iRecovery Stick 2.2.5 Open source or free methods	**15**
Unit III	**Mobile Malware Analysis – I** 3.1.Introduction to Mobile Malware 3.1.1 Mobile Malware 3.1.2 Phishing, 3.1.3 SMishing, and 3.1.4 Vishing 3.2.Malware Attack and Defense 3.2.1 Visual Payload 3.2.2 Hoaxes, and Threats 3.2.3 Taxonomy of Mobile Malware	**15**

Unit IV	**Mobile Malware Analysis – II** 4.1.Analyzing Mobile Malware 4.1.1 Learning about Dynamic Software Analysis 4.1.2 Using MobileSandbox 4.1.3 Analyzing Mobile Malware 4.2. Mobile Device Assets & MM Payloads 4.3. Forensic Investigation of MM on a Mobile Device	**15**

Course Code	Title	Credits
PGDCF 204	**Cyber Law – II**	**4**
Unit No.	**Contents of Unit**	**No. of Lectures**
Unit I	**E-Commerce and E-Governance - I** 1.1.International Organizations and Their Roles 1.2.ICANN 1.3.UDRP Dispute Resolution Policy 1.4.WTO and TRIPS 1.5.UNICITRAL Model LAW	**15**
Unit II	**E-Commerce and E-Governance – II** 2.1. IT Act, Digital Signature, E-Commerce, E-Governance 2.2. Evolution of IT Act; Genesis and Necessity 2.3.Digital/ Electronic Signature - Analysis in the background of Indian Laws 2.4.E-Commerce; Issues and Provisions in Indian Law 2.5.E-Governance; Concept and Practicality in India 2.6.E-Taxation issues in Cyberspace	**15**
Unit III	**Intellectual Property Rights in Digital Medium – I** 3.1. Domain Names and Trademark Disputes 3.2. Concept of Trademark/Domain Name 3.3.Cyber Squatting 3.4.Reverse Hijacking	**15**
Unit IV	**Intellectual Property Rights in Digital Medium – II** 4.1. Concept of Copyright and Patent in Cyberspace 4.2. Copyright in the Digital Medium 4.3. Copyright in Computer Programmes 4.4. Copyright and WIPO Treaties	**15**

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

Semester II - Practical

Course Code	Title	Credits
PGDCF 205	**Cyber Forensics Practical – III**	**2**
Practical No.	**Title of the Practical**	**No. of Practical**
1	Study of Network Attacks	1
2	Study of Stegnography	1
3	Study of Wireless Network and Attacks	1
4	Study of SQL Injections	1
5	Study of IDS/IPS	1
6	Session Hijacking	1
7	Study of Cross Side Scripting	1
8	Incident Response	1
9	Mobile/ Smart Phone Forensic Practical - IV	1
10	Mobile/ Smart Phone Forensic Practical - V	1
11	Mobile/ Smart Phone Forensic Practical - VI	1
12	Windows Investigation Practical - I	1
13	Windows Investigation Practical - II	1
14	Linux Investigation Practical - I	1
15	Linux Investigation Practical - II	1

Course Code	Title	Credits
PGDCF 206	**Cyber Forensics Practical - IV**	**2**
Practical No.	**Title of the Practical**	**No. of Practical**
1	Digital and Cyber Forensic Case Documentation	02
2	Field/Industrial Visit – Report	02
3	Project/Case Work – Progress Report and Work	05
4	Project/Case Work – Presentation/Poster/Paper	02
5	Project/Case Work – Documentation	04

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

Semester I and II - References

PGDCF 101 : Computer Forensics – I
PGDCF 201 : Computer Forensics - II

Sr. No.	Reference Books
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 References
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.	Reference Books
1	Certified Information (Security Expert, Main Book, Innobuss Knowledge Solutions (P) Ltd.

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

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

Sr. No.	Reference Books
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 References
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.	Reference Books
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 References
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