

UNIVERSITY OF MUMBAI



Syllabus

Semester III & IV

Program: M.Sc.

Course: Forensic Science

(Digital and Cyber Forensics and IT Security)

(Credit Based Semester and Grading System with
Effect from the academic year 2013–2014)

M. Sc. Forensic Science (Digital and Cyber Forensics and IT Security)

		M.Sc.Sem III		Class Room Instruction Face to Face						50 Hrs. = 1 Credit				
Course Code		Per Week		15 Week (Per Sem.)		Per Sem. (Hrs.)		Notinal Hrs.		Total Hrs.		Credits		Total Credits
		L (60 min)	P(60 min)	Lect.	Pra.	Lect.	Pra.	Lect.	Pra.	Lect.	Pra.	Lect.	Pra.	
Theory Code	Practical Code													
PSDF301	PSDF3P1	4	4	60	60	60	60	40	40	100	100	2	2	4
PSDF302	PSDF3P2	4	4	60	60	60	60	40	40	100	100	2	2	4
PSDF303	PSDF3P3	4	4	60	60	60	60	40	40	100	100	2	2	4
PSDF304	PSDF3P4	4	4	60	60	60	60	40	40	100	100	2	2	4
PSDF305	PSDF3P5	4	4	60	60	60	60	40	40	100	100	2	2	4
PSDF306	PSDF3P6	4	4	60	60	60	60	40	40	100	100	2	2	4
Total		24	24	360	360	360	360	240	240	600	600	12	12	24

M. Sc. Forensic Science (Digital and Cyber Forensics and IT Security)

		M.Sc.Sem IV		Class Room Instruction Face to Face						50 Hrs. = 1 Credit				
Course Code		Per Week		15 Week (Per Sem.)		Per Sem. (Hrs.)		Notinal Hrs.		Total Hrs.		Credits		Total Credits
		L (60 min)	P(60 min)	Lect.	Pra.	Lect.	Pra.	Lec t.	Pra.	Lect.	Pra.	Lec t.	Pra.	
Theory Code	Practical Code													
PSDF401	PSDF4P1	4	4	60	60	60	60	40	40	100	100	2	2	4
PSDF402	PSDF4P2	4	4	60	60	60	60	40	40	100	100	2	2	4
PSDF403	PSDF4P3	4	4	60	60	60	60	40	40	100	100	2	2	4
PSDF404	PSDF4P4	4	4	60	60	60	60	40	40	100	100	2	2	4
PSDF405	PSDF4P5	4	4	60	60	60	60	40	40	100	100	2	2	4
PSDF406	PSDF4P6	4	4	60	60	60	60	40	40	100	100	2	2	4
Total		24	24	360	360	360	360	240	240	600	600	12	12	24

**M. SC. FORENSIC SCIENCE (DIGITAL AND CYBER FORENSICS AND IT
SECURITY)
SEMESTER III**

PSDF301: Vulnerability Assessment and Penetration Testing - Part I

Total Marks 100	
Lecture Per Week	Credit
4	2

Units with Description	No. lectures
Unit I: System Testing and Introduction	15
<ul style="list-style-type: none"> • Internal Intrusion Techniques, • External Intrusion Techniques, • Scanning IP pool and Discovering Devices, • Verifying the Network & Security Devices, 	
Unit II: Information Gathering and Fingerprinting	15
<ul style="list-style-type: none"> • Web Server, • Frameworks And Applications, • Enumerating Resources, • Port Scanning, • Distinguish between different OS platforms, 	
Unit III: Attacks & Exploitation	15
<ul style="list-style-type: none"> • Web Server, • Router, • Wireless Network Testing, • Buffer Overflows, • Man in the Middle Attacks, • Capturing of passwords on the network. 	
Unit IV : Security Policy and Implementation – Windows	15
<ul style="list-style-type: none"> • Domain Policies, • User Rights Managements, • Router Policies, • Firewall, • IPS, • UTM Policies, • Patch Management Automation, • Wireless Network Security, • Logging System, • Generating Periodic Reports 	

PSDF302: Virtualization and Network Forensics – Part I

Total Marks 100	
Lecture Per Week	Credit
4	2

Units with Description	No. lectures
Unit I: Virtualization	15
Introduction <ul style="list-style-type: none"> • Physical Machines • How Virtualization Works • Hypervisors • Main Categories of Virtualization • Benefits of Virtualization • Cost of Virtualization 	
Unit II: Types of Virtualization	15
Server Virtualization <ul style="list-style-type: none"> • What Is Server Virtualization? • Differences between Desktop and Server Virtualization • Common Virtual Servers Desktop Virtualization <ul style="list-style-type: none"> • What Is Desktop Virtualization? • Common Virtual Desktops • Virtual Appliances and Forensics • Virtual Desktops as a Forensic Platform 	
Unit III: Implementation of Virtualization	15
Portable Virtualization, Emulators, and Appliances <ul style="list-style-type: none"> • MojoPac • MokaFive • Preconfigured Virtual Environments • Virtual Appliance Providers • JumpBox Virtual Appliances • VirtualBox • Virtualization Hardware Devices • Virtual Privacy Machine • Virtual Emulators • Future Development 	
Unit IV : Challenges in Virtualization	15
<ul style="list-style-type: none"> • Data Centers • Security Considerations • Malware and Virtualization • Red Pill, Blue Pill, No Pill • Additional Challenges • Virtualization Drawbacks 	

PSDF303: Audit Governance Risk and Compliance – Part I

Total Marks 100	
Lecture Per Week	Credit
4	2

Units with Description	No. lectures
<p>Unit I: Audit and Methodology</p> <ul style="list-style-type: none"> • Audit Life Cycle Initiation – Commencement Discovery Stage Maturation Stage Predictive Stage • PDCA – Cycle Plan, Do, Check, Act • Types of Audit <ul style="list-style-type: none"> - Internal, - External - Mandatory and - Statutory 	15
<p>Unit II: Introduction to International Standards and Audit</p> <ul style="list-style-type: none"> • ISMS 27001 ISO Standard – Introduction and Applicability • CTCL Audit – Stock Market <ul style="list-style-type: none"> - Guideline from NSE and NSE • SOX – International Compliance – Introduction and Applicability • HIPPA – International Compliance – Introduction and Applicability 	15
<p>Unit III: Risk</p> <ul style="list-style-type: none"> • Oversight and Introduction • Common Risk Infrastructure • Risk Management Activities <ul style="list-style-type: none"> - Identification - Analysis - Remedy - Handling • Classes or Types of Risk 	15
<p>Unit IV : Risk Management</p> <ul style="list-style-type: none"> • Introduction • Method and Principles • Process • Mitigation <ul style="list-style-type: none"> - Potential risk treatments - Risk management plan • Implementation • Limitations • Types of risk management 	15

<ul style="list-style-type: none"> - For projects - For natural disasters - Of information technology - In petroleum and natural gas • Business Continuity and Planning 	
---	--

PSDF304 - Mobile and Smart Phone Forensics – Part I

Total Marks 100	
Lecture Per Week	Credit
4	2

Units with Description	No. lectures
Unit I: Mobile Forensic	15
<ul style="list-style-type: none"> • Cell phone and mobile device forensics • Understanding Mobile device forensics • Understanding acquisition procedure • Cell phone Crimes • SIM Architecture • Data Storage • Data Extraction • Files Stored on SIM • Mobile Operating System 	
Unit II: Digital Evidence	15
<ul style="list-style-type: none"> • Mobile Device Forensics • Types of Evidence on Mobile Devices • Handling Mobile Devices as Sources of Evidence • Forensic Preservation of Mobile Devices • Forensic Examination and Analysis of Mobile Devices • Forensic Acquisition and Examination of SIM Cards • Investigative Reconstruction Using Mobile Devices Future Trends 	
Unit III: Andriod and iOS Systems	15
<ul style="list-style-type: none"> • Architecture • Differentiation • Technological Composition • Introduction to Andriod Platform • Introduction to iOS Platform 	
Unit IV : Mobile File Systems and Data Structures	15
<ul style="list-style-type: none"> • Introduction • What and How of Data • Types of Memory • File Systems • Rootfs, devpts, sysfs, cgroup, yaffs2 	

<ul style="list-style-type: none"> • Procedure for handling an Android Devices • Logical Techniques VS Digital Techniques • Introduction to Mobile Malware 	
---	--

PSDF305: E-commerce and Online Dispute Resolution: International Legal Perspective

Total Marks 100	
Lecture Per Week	Credit
4	2

Units with Description	No. lectures
Unit I: E-commerce and Unfair trade Practices	15
<ul style="list-style-type: none"> • Meaning and types of e-commerce and electronic marketplace • Concept of Unfair Trade Practices • Online Misleading Advertisements • Standardization of Electronic Contract 	
Unit II: Alternate Dispute Resolution (ADR) Policy in Cyberspace	15
<ul style="list-style-type: none"> • What is ADR? Difference Between ADR and (ODR) Online Dispute Resolution • Advantages and Method of online dispute resolution • Procedural setup for ADR schemes. • Driving Force behind ODR and its core regulatory principles 	
Unit III: Global Justice System: ODR and Transboundary Disputes	15
<ul style="list-style-type: none"> • ICANN's UDRP • Case Studies • Other transnational ODR Systems • Current issues in ODR 	
Unit IV : Cyberspace Regulation and Role of UNCITRAL	15
<ul style="list-style-type: none"> • Brief about UNCITRAL • UNCITRAL Model Law on Electronic Commerce 1996 • UNCITRAL Model Law on Electronic Signatures 2001 	

PSDF306: Financial Fraud and Investigation – Part I

Total Marks 100	
Lecture Per Week	Credit
4	2

Units with Description	No. lectures
Unit I: Investigations	15
<ul style="list-style-type: none"> • Investigate allegations of fraud • Investigate internal & external theft 	

<ul style="list-style-type: none"> • Investigate allegations of bribes & kickbacks • Investigate inventory theft • Investigate fraud against senior citizens • Investigate allegations of fraud by fiduciaries, including estates & trusts, & condominium associations 	
Unit II: Investigations	15
<ul style="list-style-type: none"> • Company Backgrounds • Due Diligence • Economic Espionage • Financial Fraud • Mergers/Acquisitions 	
Unit III: Methodology	15
<ul style="list-style-type: none"> • Review internal controls to safeguard assets • Conduct small business asset protection survey & make recommendations for preserving company assets • Fraud auditing services • Uncover financial statement fraud • Conduct white-collar crime investigations • Asset record reconstruction 	
Unit IV : Analysis, Evidence and Testimony	15
<ul style="list-style-type: none"> • Prove allegations of misuse of business data and business assets by corporate directors, employees, & officers • Prove allegations of embezzlement • Prove allegations of money laundering and/or currency structuring • Provide anti-money laundering and/or fraud training • Consult on civil and/or criminal litigation matters, including asset forfeiture issues • Assist legal counsel with plea negotiations involving drug trafficking, public corruption, money laundering, & currency structuring 	

M. Sc. FORENSIC SCIENCE (DIGITAL AND CYBER FORENSICS AND IT SECURITY)
SEMESTER III
PRACTICAL

PSDF3P1: Vulnerability Assessment and Penetration Testing - Part I

Total Marks 50	
Lecture Per Week	Credit
4	2

- Installation of Back-Track OS (2 Nos.)
- Webserver and Server Hardening (2 Nos.)
- Wireless Hacking Techniques (2 Nos.)

- **Footprinting:** Tools to Extract Company's Data, WHOIS Lookup, Footprint Using Google Hacking Techniques. (2 Nos.)
- **Scanning:** Network Vulnerability Scanners, Spoofing IP Address, Proxy Tools, Http tunnel for Windows, IP Spoofing Detection (2 Nos.)

PSDF3P2: Virtualization and Network Forensics – Part I

Total Marks 50	
Lecture Per Week	Credit
4	2

- Virtual OS (2 Nos.)
- Virtual Network (2 Nos.)
- Windows Server Configuration (2 Nos.)
- Linux Server Configuration (2 Nos.)
- Google App Engine Testing (2 Nos.)

PSDF3P3: Audit Governance Risk and Compliance – Part I

Total Marks	Credit
50	2

Case Studies and Industrial Visit

Practical: PSDF3P4 - Mobile and Smart Phone Forensics – Part I

Total Marks 50	
Lecture Per Week	Credit
4	2

- Mobile Forensic (2 Nos.)
- Smartphone Forensic (2 Nos.)
- SIM analysis (2 Nos.)
- Handset Analysis (2 Nos.)
- Recovering data (2 Nos.)

PSDF3P5: E-commerce and Online Dispute Resolution: International Legal Perspective

Total Marks 50	
Lecture Per Week	Credit
4	2

PRACTICAL	Marks
Project Work - Review of Literature	25
Project Work - Progress Report	25

PSDF3P6: Financial Fraud and Investigation – Part I

Total Marks 50	
Lecture Per Week	Credit
4	2

PRACTICAL		Marks
1	a) Topic approval for synopsis b) Objective and work plan	25
2	Presentation	25

**M.Sc. FORENSIC – DIGITAL AND CYBER FORENSICS AND IT SECURITY
SEMESTER IV**

PSDF401: Vulnerability Assessment and Penetration Testing – Part II

Total Marks 100	
Lecture Per Week	Credit
4	2

Units with Description	No. lectures
Unit I: System Testing and Introduction <ul style="list-style-type: none"> • Structure of Penetration Testing, • Concepts of infrastructure Testing and • Application Testing, White Box and Black Box 	15
Unit II: Information Gathering and Fingerprinting <ul style="list-style-type: none"> • Custom Applications, • Vulnerability Scanning, • Remote Operating System Fingerprinting; • Active and Passive techniques. 	15
Unit III: Attacks & Exploitation <ul style="list-style-type: none"> • Firewall Policies bypass techniques, • Malware, • XSS Attacks, • Null Sessions, • SQL Injection, • ARP Poisoning, • Breaking into https connections. 	15
Unit IV : Security Policy and Implementation - Linux Domain Policies, User Rights Managements, Router Policies,	15

Firewall, IPS, UTM Policies, Security Suites, Patch Management Automation, Wireless Network Security, Logging System, Generating Periodic Reports	
--	--

PSDF402: Virtualization and Network Forensics – Part II

Total Marks 100	
Lecture Per Week	Credit
4	2

Units with Description	No. lectures
Unit I: Forensics - Investigating Dead Virtual Environments <ul style="list-style-type: none"> • Install Files • Remnants • Registry • Microsoft Disk Image Formats • Data to Look for • Investigator Tips 	15
Unit II: Forensics – Investigating Live Virtual Environments <ul style="list-style-type: none"> • Artifacts • Processes and Ports • Log Files • VM Memory Usage • Memory Analysis • ESXi Analysis • Microsoft Analysis Tools • Moving Forward 	15
Unit III: Cloud Computing and Forensic Challenges <ul style="list-style-type: none"> • What Is Cloud Computing? • Cloud Computing Services • Streaming Operating Systems • Application Streaming • Virtual Applications • Cloud Computing, Virtualization, and Security • Cloud Computing and Forensics 	15
Unit IV : Virtual Environments and Compliance <ul style="list-style-type: none"> • Standards • Compliance 	15

<ul style="list-style-type: none"> • Organizational Chain of Custody • Data Retention Policies 	
--	--

PSDF403: Audit Governance Risk and Compliance – Part II

Total Marks 100	
Lecture Per Week	Credit
4	2

Units with Description	No. lectures
Unit I: Governance	15
<ul style="list-style-type: none"> • Overall Management Approach • What is Governance? • Role of Senior Management • Control and Supervisory Role • Hierarchical Management • Segregation of Departments 	
Unit II: Governance Management Role	15
<ul style="list-style-type: none"> • Governance activities • Critical management, information reaching, • accurate and timely reporting • decision making, • provide the control mechanisms for ensuring strategies, directions and instructions from management. 	
Unit III: Compliance	15
<ul style="list-style-type: none"> • Conforming with stated requirements, organizational level, • management processes which identify the applicable requirements • (defined for example in laws, regulations, contracts, strategies and policies), • assess the state of compliance, • assess the risks and potential costs of non-compliance against the projected expenses to achieve compliance, prioritize and initiate any corrective 	
Unit IV : Compliance Types	15
<ul style="list-style-type: none"> • Basel II/III – Introduction and Applicability • PCI DSS – Introduction and Applicability • NIC Website Compliance Indian Government Websites • COBIT – Introduction and Applicability • Miscellaneous Compliance - Introduction and Applicability 	

PSDF404: Mobile and Smart Phone Forensics – Part II

Total Marks 100	
Lecture Per Week	Credit
4	2

Units with Description	No. lectures
Unit I: Introduction to Mobile Malware	15
<ul style="list-style-type: none"> • Types of Attacks • Taxonomy of Mobile Malware, • Phishing, • SMishing, and • Vishing , 	
Unit II: Malware Attack and Defense	15
<ul style="list-style-type: none"> • Mobile Malware, • Visual Payloads, • Timeline of Mobile Malware, • Hoaxes, and Threats, • Overview of Mobile Malware Families, • Taxonomy of Mobile Malware 	
Unit III: Threats, Hacking and Viruses in Mobile Communication	15
<ul style="list-style-type: none"> • Introduction and Overview of Mobile Communication • Attacks in Mobile • Man in the Middle • Denial of Service • Wireless Spoofing • Prevention Techniques in Mobile System • Intrusion detection in wireless • Access Control and Authentication in Mobile Communications - Overview 	
Unit IV : Overview of Mobile Communication Security	15
<ul style="list-style-type: none"> • SIM Security, • Security of Mobile Networks, • Security of GSM Networks, • Security of 3G Networks, • Security of Wireless Local Area Networks, • Security of Ad-hoc Networks, • Security Techniques for Mobile Services, • End-to-End Security Services in Mobile Communications, • Inter-system Roaming and Internetworking Security, • Securing Mobile E-Services, • Security of Satellite Services, 	

<ul style="list-style-type: none"> • Security of Mobile Sensor Networks, • Application Level Security, • Security of IP Based Applications, • Security of Mobile Payments, • Security of Multimedia Communications, • Security of Mobile Voice Communication 	
--	--

PSDF405: Protection of Personal Data in Cyberspace: International Legal Perspective

Total Marks 100	
Lecture Per Week	Credit
4	2

Units with Description	No. lectures
<p>Unit I: Role of OECD for protection of personal data</p> <ul style="list-style-type: none"> • Organisation for Economic Cooperation and Development (OECD) Guidelines on the protection of privacy and trans-border flow of personal data, 1980. • OECD guidelines for protecting consumers from fraudulent and deceptive commercial practices across borders, 2003. • Organisation for Economic Cooperation and Development (OECD) Guidelines for the security of information systems and networks 2002. • OECD Guidelines for electronic authentication, 2007. 	15
<p>Unit II: Protection of Personal Data and EU Principles</p> <ul style="list-style-type: none"> • The European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981. (ETS No. 108, Popularly Known as <i>Council of Europe</i> Convention 108) • The protection of individuals with regard to the processing of personal data and on the free movement of such data. (EU Directive 95/46/EC of 24 October 1995) • Asia-Pacific Economic Cooperation (APEC) Privacy Framework, 2004. 	15
<p>Unit III: Cyberspace Regulation and Role of United Nation</p> <ul style="list-style-type: none"> • UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990. • United Nations Convention on the Use of Electronic Communications in International Contracts. 2005 	15
<p>Unit IV : Indian Personal Data Protection Law</p> <ul style="list-style-type: none"> • Right to Privacy • Data Theft and Indian Law • Legal Measures for Protection of Personal Data 	15

- Comparison and Critique of Indian Personal Data Protection Law.
- Draft on Right to Privacy

PSDF406- Financial Fraud and Investigation – Part II

Total Marks 100	
Lecture Per Week	Credit
4	2

Units with Description	No. lectures
Unit I: Financial Frauds <ul style="list-style-type: none"> • Accounting Frauds and Types • Payroll Fraud • Financial Missappropriation Fraud • Shareholders and Partnership Dispute • Criminal Investigation • Personal Injury and Accident Claim • Business Interruption and Insurance 	15
Unit II: Analysis and Procedure <ul style="list-style-type: none"> • Organize/analyze financial records, • Organise/analyse response to search warrant records • Analyze & organize financial records to prepare tax returns • Assist legal counsel with plea negotiations regarding tax issues 	15
Unit III: Introduction to Financial Compliance <ul style="list-style-type: none"> • Accounting and Payroll • Assurance • Direct Tax • Indirect Tax • Secretarial Compliance • Labour Laws • Miscellaneous 	15
Unit IV : Frauds Investigation <ul style="list-style-type: none"> • Business/Employee Fraud • Matrimonial Dispute • Business Economic Losses • Professional Negligence • Mediation and Arbitration 	15

**M.Sc. FORENSIC – DIGITAL AND CYBER FORENSICS AND IT SECURITY
SEMESTER IV
PRACTICAL**

PSDF4P1: Vulnerability Assessment and Penetration Testing – Part II

Total Marks 50	
Lecture Per Week	Credit
4	2

Practical:

- Net-Bios Enumeration, SNMP, Linux, LDAP, NTP, SMTP Enumeration, Enumeration Countermeasures (2 Nos.)
- Intrusion Detection Tool, Honeypot Tools, Obfuscating, Honeypot Detecting Tool
- Buffer overflow Security Tools (2 Nos.)
- Application Security Assessment Tool, Network Security Assessment Tool, Wireless/Remote Access Assessment Tool, Telephony Security Assessment Tool, Testing Network-Filtering Device Too (2 Nos.)
- SQL Injection (1 No)
- XSS (1 No)

PSDF4P2: Virtualization and Network Forensics – Part II

Total Marks 50	
Lecture Per Week	Credit
4	2

Practical:

- Windows Azure, Salesforce, Amazon, etc... (2 Nos.)
- Cloud Computing Programming (2 Nos.)
- Virtual Forensics (2 Nos.)
- Cloud Computing and Configuration (2 Nos.)
- Virtual Server and Cloud Setup (Virtualization) (2 Nos.)

PSDF4P3: Audit Governance Risk and Compliance – Part II

Total Marks	Credit
50	2

Practical - Case Study and Industrial Visit

PSDF4P4: Mobile and Smart Phone Forensics – Part II

Total Marks 50	
Lecture Per Week	Credit
4	2

Practical:

- M commerce security analysis (2 Nos.)
- Mobile application testing (2 Nos.)
- Satellite phone technology (2 No.)
- Malware Analysis (2 Nos.)
- Smart phone malware analysis (2 Nos.)

PSDF4P5: Protection of Personal Data in Cyberspace: International Legal Perspective

Total Marks 50	
Lecture Per Week	Credit
4	2

PRACTICAL		Marks
1	Presentation / Poster	25
2	Viva-Voice	25

PSDF4P6: Financial Fraud and Investigation – Part II

Total Marks	Credit
50	2

Final Project Work	50 Marks
--------------------	----------

References:

PSDF301:

- Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide by Lee Allen (Chapter 1)
- The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Engebretson (Chapter 2 and 3)
- Security Policies and Implementation Issues (Information Systems Security & Assurance) by Robert Jahnsen (Chapter 5 and 7)
- Microsoft Windows Security Essentials by Darril Gibson (Chapter 1, 3,4, 5, 7,8)
- OWASP

PSDF302:

Virtualization and Forensics By Diane Barrett, Greg Kipper

Virtualization Security Protecting virtualized environment By Dave Shackleford

PSDF303:

Audit – Standards of ISMS27001, US Sarbanes-Oxley Act, HIPPA

- Crockford, Neil (1986). An Introduction to Risk Management (2 ed.). Cambridge, UK: Woodhead-Faulkner. p. 18. ISBN 0-85941-332-2
- Dorfman, Mark S. (2007). Introduction to Risk Management and Insurance (9 ed.). Englewood Cliffs, N.J: Prentice Hall. ISBN 0-13-224227-3.
- IADC HSE Case Guidelines for MODUs 3.2, section 4.7
- Roehrig, P (2006). "Bet On Governance To Manage Outsourcing Risk"

Hopkin, Paul "Fundamentals of Risk Management 2nd Edition" Kogan-Page (2012) ISBN 978-0-7494-6539-1

Risk Management ISO 30001 Standard

PSDF304:

Chapter 13: Guide to Computer Forensics and Investigations By Bill Nelson, Amelia Phillips, Christopher Stuart

Chapter 20 Digital Evidence on Mobile Devices

Digital Evidence and Computer Crime, Third Edition Eoghan Casey. Published by Elsevier Inc. All rights reserved

Android Forensic, Investigation, and Security by Andrew Hogg, Publisher Synergy

Security in Mobile Communication by Professor Noureddine Boudriga

Mobile Malware Attacks and Defense By Ken Dunham

PSDF305

1) International Trade Law by Indira Carr, Peter Stone, 4th edition, 2010, Page 103 to 136

2) Online Dispute Resolution: Challenges for Contemporary Justice by Gabrielle Kaufmann-Kohler, Thomas Schultz, 2004, pages 5 to 58, 67 to 81, 108 to 120, 131 etc.

3) Cyber Consumer Law and Unfair Trading Practices: Unfair Commercial Practices By Cristina Coteanu page 87-113.

4) Cyber Consumer Law and Unfair Trading Practices: Unfair Commercial Practices By Cristina Coteanu Page- 1- 11, 45 to 68, 137 to 150

- 5) Online Dispute Resolution for Business: B2B, ECommerce, Consumer, Employment, Insurance and other Commercial Conflict, by Colin Rule, Josse bass, 2002. Page- 203 to 214
- 6) The Law of Electronic Commerce by Jane K. Winn, Benjamín Wright, 2004.
- 7) Internationalization of E-Commerce, an electronic Journal for US Dept of State Volume 5 no.2, 2000.
- 8) E-commerce: an Indian Perspective, 3rd edition by P. T. Joseph S. J., 2008
- 9) Law Relating to Computers Internet & E-Commerce by Nandan Kamath
- 10) Information Technology Law and Practice, by Vakul Sharma.
- 11) E-Commerce: Law and Jurisdiction : The Comparative Law Yearbook ..., Issue 2002
By Dennis Campbell, Susan Woodley

PSDF306:

Forensic Accounting Standards, International Financial Reporting Standard (IFRS), ICAI.

PSDF401

1. Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide by Lee Allen (Chapter 1)
2. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Egebreton (Chapter 2 and 3)
3. Security Policies and Implementation Issues (Information Systems Security & Assurance) by Robert Jahnson (Chapter 5 and 7)
4. EC Council and OWAS Top 10

PSDF402:

1. Virtualization and Forensics By Diane Barrett, Greg Kipper
2. Virtualization Security Protecting virtualized environment By Dave Shackelford

PSDF403:

<http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf>

OCEG – Open Compliance Ethic Group – Red Book

PSDF404:

1. Chapter 13: Guide to Computer Forensics and Investigations By Bill Nelson, Amelia Phillips, Christopher Stuart
2. Chapter 20 Digital Evidence on Mobile Devices
3. Digital Evidence and Computer Crime, Third Edition Eoghan Casey. Published by Elsevier Inc. All rights reserved
4. Andriod Forensic, Investigation, and Security by Andrew Hogg, Publisher Synergy
5. Security in Mobile Communication by Professor Nouredine Boudriga
6. Mobile Malware Attacks and Defense By Ken Dunham

PSDF405:

1. International Guide to Privacy, By Jody R. Westby, American Bar Association. Section of Science & Technology Law, Pages 82 to 100)
2. OECD Guidelines on the Protection of Privacy and Trans-border Flows of ...By OECD, 2001, Page- 11 to 21.
3. Data Privacy in the Information Age by Jacqueline Klosek, 2000, Pages 27 to 48.

4. Global Privacy Protection: The First Generation by James B. Rule, G. Graham William Greenleaf
5. The United Nations Convention on the Use of Electronic Communications in International Contracts by Amelia H. Boss, Wolfgang Kilian

PSDF406:

1. Forensic Accounting and Fraud Investigation for Non-Experts by Howard Silverstone - John Wiley & Sons,
2. Fraud Auditing and Forensic Accounting by Tommie W. Singleton, Aaron J. Singleton, G. Jack Bologna, Robert J. Lindquist
3. Financial Investigation And Forensic Accounting by George A. Manning
4. A Guide to Forensic Accounting Investigation by Thomas W. Golden, Steven L. Skalak, Mona M. Clayton, Jessica S. Pill
5. Fraud Auditing and Forensic Accounting (Wiley Corporate F&A) Tommie W. Singleton (Author), Aaron J. Singleton (Author)
6. Fraud Auditing and Forensic Accounting by Tommie W. Singleton, Aaron J. Singleton, G. Jack Bologna, Robert J. Lindquist