Department of Forensic Science
Second Year Advanced Diploma Program (PG)

Title: **Advanced Diploma in Cyber forensics and cyber Laws in Digital crime investigation.**

1. Year of Implementation: 2022
2. Duration: One Year
3. Pattern: Semester
4. Medium of Instruction: English
5. Contact hours: 7 hours/week
8. Structure of Course:

Year	Semester	Course No.	Course Code	Contact Hours	Credits (1Credit=15 H)	Total Marks
1	I	FST I	AD*T 101	30	2	75
		FSL I	AD* L102	60	2	150
	II	FST II	AD*T 201	30	2	75
		FSL II	AD* L202	60	2	150
	Annual	FSP I	AD*P101	60	2	150
	Industrial and or Incubation and or Research and or Field Training			60	2	-
		Total		**270**	**12**	**600**

Year	Semester	Course No.	Course Code	Contact Hours	Credits (1Credit=15 H)	Total Marks
2	III	FST III	AD*T 301	30	2	75
		FSL III	AD* L302	60	2	150
	IV	FST IV	AD*T 401	30	2	75
		FSL IV	AD* L402	60	2	150
	Annual	FSP I	AD*P201	60	2	150
	Industrial and or Incubation and or Research and or Field Training			60	2	-
		Total		**270**	**12**	**600**

Total No. of Papers: Theory: 04, Practical: 04,
Project: 02 Number of Lectures per week: 08
Theory: Semester, Practical and Project: Annual
PT: Paper Theory, PL: Paper Lab, PP: Paper Project, AD: Advance Diploma,
FS: Forensic Science

Semester III

FST-I: ADFST 301: Title: Cybercrime and related Laws

(Contact Hrs.: 30 Credits: 2)

Learning Objectives:
Students will be able to

1. Learn Importance of Cyber law.
2. Learn knowledge of cyberspace, cybercrime and related laws.
3. Learn knowledge of different electronic records and governance.

Unit I: Introduction to Cyberspace, Cybercrime and Cyber Law

The World Wide Web, Web Centric Business, E Business Architecture, Models of E Business,

E Commerce, Threats to virtual world. Cyber Crimes& social media, Cyber Squatting, Cyber Espionage, Cyber Warfare, Cyber Terrorism, Cyber Defamation. Online Safety for women and children, Misuse of individual information. Objectives, Applicability, Non applicability and Definitions of the Information Technology Act, 2000.

Unit II: Regulatory Framework of Information and Technology Act 2000

Digital Signature, E Signature, Electronic Records, Electronic Evidence and Electronic Governance. Controller, Certifying Authority and Cyber Appellate Tribunal.(Rules announced under the Act)
Offences under the Information and Technology Act 2000, Penalty and adjudication.
Punishments for contraventions under the Information Technology Act 2000 (Case Laws, Rules and recent judicial pronouncements to be discussed).Limitations of Cyber Law.

Learning Outcomes:

1. To learn Importance of Cyber Law.
2. To enhance knowledge of cyberspace, cybercrime and related laws.
3. To enhance knowledge of different electronic records and governance.

Reference Books:

1. Craig, B. Cyber Law: The Law of the Internet and Information Technology. Pearson Education
2. Paintal, D. Law of Information Technology. New Delhi: Taxmann Publications Pvt. Ltd.
3. Lindsay, D. (2007). International domain name law: ICANN and the UDRP. Oxford: Hart Publishing.
4. Sharma J. P, & Kanojia S. (2016). Cyber Laws. New Delhi: Ane Books Pvt. Ltd.
5. Duggal, P. Cyber Laws. (2016) Universal Law Publishing.
6. Kamath, N. (2004). Law relating to computers, internet and e-commerce: A guide to Cyber Laws and the Information Technology Act, 2000 with rules, regulations and notifications (2nd ed.). Delhi: Universal Law Publishing Co.
7. Stephenson, P.R. & Gilbert, K. Investigating computer- related crime a handbook for corporate investigators. Boca Raton, FL: Taylor & Francis.
8. Prosise, C. & Mandia, K. (2003). Incident response & computer forensics (2nd ed.). New York, NY: McGraw-Hill Companies.

ADFSL 302: (Practical): Cybercrime and related Laws

Lab (Contact Hrs. - 60 Credits: 02)

Course Objectives: -

Students will able to:-

1. Understand Cybercrime and their preventions.
2. Understand Security feature of cybercrime.

List of Practical's (10)

1. To understand a Secure E-commerce Infrastructure for Customer Trust.
2. To Identify and Prevent Malware, Phishing, and Other Threats.
3. To understand social engineering attacks.
4. To Understanding the Risks and Taking Action about the Social Media and Cyber Extortion.
5. To understand the Digital Signatures: Enhancing Security and Efficiency in Online Transactions.
6. To understand the Electronic Evidence and Data Protection.
7. To understand the blockchain concept for electronic transactions.
8. To explore the Impacts and Prevention of Misuse of Individual Information.
9. To understand cyber Terrorism and the challenge of Attribution.
10. To create a Online Safety for Women: Addressing Cyber stalking, Harassment, and Abuse

Learning Outcomes:

Upon successful completion of the course, the students will be able

1. To extend knowledge of cybercrime and prevention techniques.
2. To learn Importance of Cyber Security.

Reference Books:

1. Craig, B. Cyber Law: The Law of the Internet and Information Technology. Pearson Education
2. Paintal, D. Law of Information Technology. New Delhi: Taxmann Publications Pvt. Ltd.
3. Lindsay, D. (2007). International domain name law: ICANN and the UDRP. Oxford: Hart Publishing.
4. Sharma J. P, & Kanojia S. (2016). Cyber Laws. New Delhi: Ane Books Pvt. Ltd.
5. Duggal, P. Cyber Laws. (2016) Universal Law Publishing.
6. Kamath, N. (2004). Law relating to computers, internet and e-commerce: A guide to Cyber Laws and the Information Technology Act, 2000 with rules, regulations and notifications (2nd

ed.). Delhi: Universal Law Publishing Co.
7. Stephenson, P.R. & Gilbert, K. Investigating computer- related crime a handbook for corporate investigators. Boca Raton, FL: Taylor & Francis.
8. Prosise, C. & Mandia, K. (2003). Incident response & computer forensics (2nd ed.). New York, NY: McGraw-Hill Companies.

Semester IV

AST-II: ADFST 401: Title: Cyber Forensics

(Contact Hrs: 30

Credits: 2)

Course Objectives: - **Learning Objectives:**

Students will be able to

1. Learn about the data recovery and crime scene ethics..
2. Learn knowledge of cyber forensic investigating techniques.

Unit 1: Data Recovery Tools and their Procedures and Ethics

Evidence Recovery- Introduction to Deleted File Recovery, Formatted Partition Recovery, Data Recovery Tools, Data Recovery Procedures and Ethics, Gathering Evidence- Precautions, Preserving and safely handling original media for its admissibility, Document a Chain of Custody and its importance, complete time line analysis of computer files based on File creation, file modification and file access, Recover Internet Usage Data,
Data Protection and Privacy, Recover Swap Files/Temporary Files/Cache Files.

Unit 2: Cyber Forensics Investigation

Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering Deleted evidences, Password Cracking, Hashcat. Work on open Source, Commercial tools. Introduction to Encase Forensic Edition, Forensic Toolkit etc, Use computer forensics software tools to cross validate findings in computer evidence-related cases.

Learning Outcomes:

students should be able to:

1. To enhance knowledge of data recovery and their ethics in crime scene investigation.
2. To enhance knowledge of cyber forensic investigating techniques.

Reference Books:

1. Craig, B. Cyber Law: The Law of the Internet and Information Technology. Pearson Education
2. Paintal, D. Law of Information Technology. New Delhi: Taxmann Publications Pvt. Ltd.
3. Lindsay, D. (2007). International domain name law: ICANN and the UDRP. Oxford: Hart Publishing.
4. Sharma J. P, & Kanojia S. (2016). Cyber Laws. New Delhi: Ane Books Pvt. Ltd.
5. Duggal, P. Cyber Laws. (2016) Universal Law Publishing.

6. Kamath, N. (2004). Law relating to computers, internet and e-commerce: A guide to Cyber Laws and the Information Technology Act, 2000 with rules, regulations and notifications (2nd ed.). Delhi: Universal Law Publishing Co.
7. Stephenson, P.R. & Gilbert, K. Investigating computer- related crime a handbook for corporate investigators. Boca Raton, FL: Taylor & Francis.
8. Prosise, C. & Mandia, K. (2003). Incident response & computer forensics (2nd ed.). New York, NY: McGraw-Hill Companies.

ADFSL 402: (Practical): Cyber Forensics

(Contact Hrs. 60 Credits: 02)

Students will be able to

1. Learn about the data recovery software.
2. Learn knowledge of cyber forensic investigating techniques.

List of Practical's (10)

1. To recover the data by using data recovery tools.
2. To understand encryption and decryption methods.
3. To understand the Gathering Evidence- Precautions, Preserving and safely handling original media for its admissibility.
4. To create an image using FTK.
5. To crack the password using hashcat.
6. To understand the wireshark tool and capture the network traffic
7. To investigate the network traffic.
8. To investigate an Email and identify phishing email.
9. To understand the UFED for mobile data acquisition
10. To understand Hash value, calculate and validate the hash for digital evidences.

Learning Outcomes:

Upon successful completion of the course, the students will be able

1. To extend knowledge of data recovery software.
2. To understand about the cyber forensic investigating techniques.

Reference Books:

1. Duggal, P. Cyber Laws. (2016) Universal Law Publishing.
2. Kamath, N. (2004). Law relating to computers, internet and e-commerce: A guide to Cyber Laws and the Information Technology Act, 2000 with rules, regulations and notifications (2nd ed.). Delhi: Universal Law Publishing Co.
3. Stephenson, P.R. & Gilbert, K. Investigating computer- related crime a handbook for corporate investigators. Boca Raton, FL: Taylor & Francis.
4. Prosise, C. & Mandia, K. (2003). Incident response & computer forensics (2nd ed.). New York, NY: McGraw-Hill Companies.