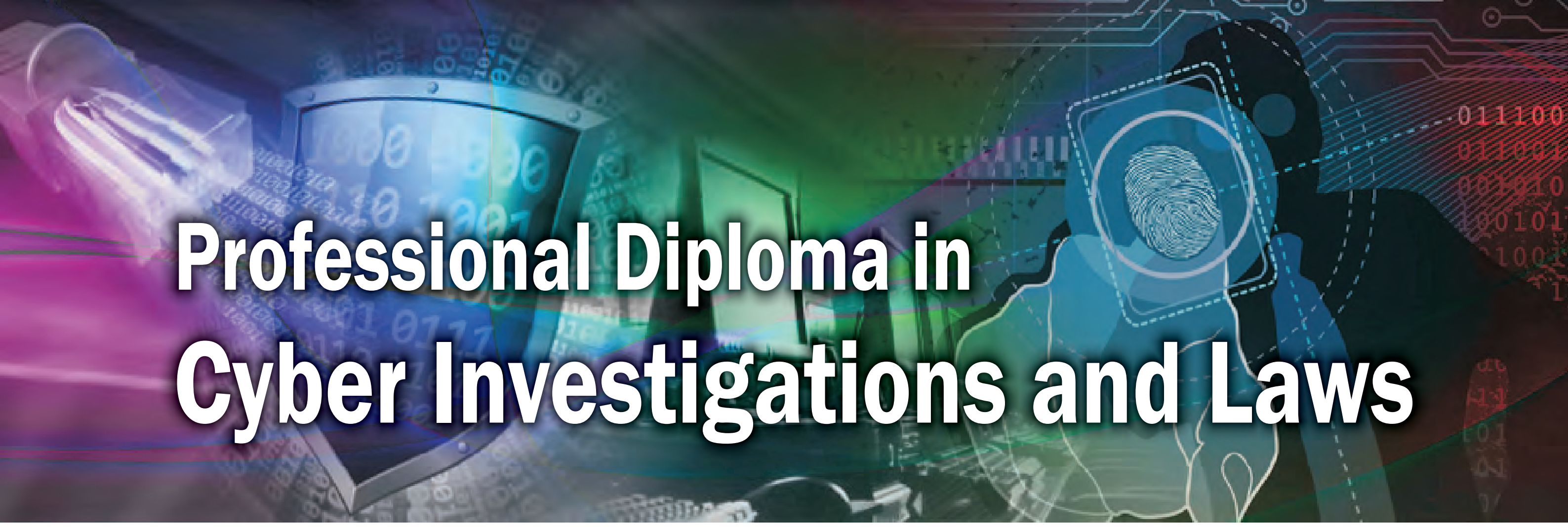

Professional Diploma in Cyber Investigations and Laws

Professional Diploma in Cyber Investigations and Laws (DCIL)

Computer and communication technologies have emerged as the backbone for mission critical infrastructure services of our society. In an effort to share information and organize operations, enterprises are creating complex networked systems and exposing their networks to customers, suppliers, and other business partners. Advanced network intricacies, and a dynamic insistence on the Internet have opened up security issues, leading to cyber crime as a major byproduct, which is a cause of concern for organizations.

Professional Diploma in Cyber Investigations and Laws aims at equipping the individuals with conceptual foundations leading to advanced understanding of computing technology, cyber forensic technology and up skilling their technical capabilities to manage the cyber security ecosystem. The cyber ecosystem is a eco-chain which starts from software design, development, bugs, testing, vulnerability assessment, hacking, digital investigation and forensic trails, and legal framework.

Scope of program

The course is designed to develop a working knowledge of the ecosystem leading to protecting the system and with new generation investigative skills supported by applicable legal framework. The course begins with security of the crime scene and concludes with the presentation of evidence. The course explores the policy and law on computer crime leading to differentiating "cybercrimes" with conventional crime and their transgressive behavior in physical space. Students are expected to recognize, appraise, classify, and demonstrate dexterity in investigating computer related crimes.

The student will apply his learning to solve problems exposed through informal appraisal, such as oral communication among students and between teacher and students. This course includes lab study designed to inflate important investigative and forensic skills. This course is mapped to various certifications exams from an industrial point of view. Cyber security being an upcoming industry calls for new areas of work including Cyber profiling, Cyber policing, Cyber Patrolling, Cyber forensics, Cyber investigation, apart from specializations like Image forensics, audio forensics, video forensics, Disk forensics, Software forensics, cloud forensics etc. Challenges to outwit the security problems exposed to the society at large.

Course structure

Theory

1. Computer Network - DCE101
2. File System & Storage Management - DCE102
3. Cyber Forensics - DCE103
4. Cyber Crime & Related Laws - DCE104
5. SIEM & Log Trails - DCE105

Practical

6. Forensics and VA lab - DCE106
7. Project - DCE107

Career path

Due to the dependency on Internet, all the major organizations are in the look out to enhance their human resource capital with higher security skill set in order to protect their business interests. Government of India has called for more than 5 lakh security professionals for national security requirements. The Police force is in the lookout for security expertise. Organizations including public sector organizations, Managed security service providers, Banking and financial industries are in the lookout for specialized security skills. Foreign nations have started to track good security skill-sets.

Laboratories

Forensics and VA Lab

1.Network forensic laboratory: Cyber Forensics Analysis encompasses the skills of not only capturing suspicious data, but also the ability to discern unusual patterns hidden within seemingly normal network traffic. This course will provide the student with a set of investigate techniques focusing on the use of vendor-neutral, tools. The focus of this lab is to understand the use of wired and wireless network traffic capture techniques as practiced by the industry. The captured traffic calls for data mining and analysis of data files, hidden data files, and encoded data files passed through the network. The scope of such analysis is to reconstruct the traffic pattern, understand traffic anomalies in terms of malformed network packets, reconstruct data files as forensic evidences and time line trends.

2.Email Forensic laboratory: Email has become the de-facto communication standard. Every email generated has transaction data embedded as email header carried by the mail to the destination system. Email header carries the footprint information about the sender's domain, and associated spam management infrastructure. From a forensic stand point it is essential to understand the mail header, the time zones and time stamp details, associated mailers and their signature patterns to reconstruct the mail transaction. The focus of this laboratory is to understand the concepts of email, the associated mail transfer agents (MTA) and mail user agents (MUA), concepts of SPAM, mail forging, apart from associated IP fingerprinting and relevant domain entries. The scope of the analysis is to reconstruct the mail transaction and provide an expert opinion on the transacted mail.

3.Forensic Imaging Laboratory: Creation of forensic disk images are in demand to understand and analyze the activities of an individual during times of crisis. The focus of this laboratory is to provide the required exposure on EnCase to as a part of the learning process apart from other similar equivalent tools. The student is expected to apply his understanding on images and analyze the provided images to generate relevant case evidences.

4.Unconventional testing laboratory: There is a lot of debate going around the term hacking and ethical hacking. Unconventional testing involves the use of tool / sensor driven testing of system and applications to understand the stability of the system and the available applications. The tools help in fingerprinting the system and the applications, enumeration, leading to an evaluation of the associated risk. The focus of the laboratory is to enable an understanding of the tools and its capabilities, deployment of the tools on test cases and understand the generated logs emitted by the considered system and / or applications. The scope of the analysis is to evaluate the security posture of the system and / or applications using the system and provide an expert opinion.

Contact for More Information

Mail to **mohammed.samiuddin@htcitmr.ac.in**
or contact +91-9840730610 / 9787401008 / 9566168196

About ITMR

Institute of Technology Management & Research (ITMR) is a division of Mamta Trust catering to the educational needs of the society along the lines of Technology Management & cutting edge research. The program is offered through ITMR, Chennai.

Institute of Technology Management & Research
(Division of Mamta Trust)
2/850, Mugaliwakkam Road, Mugaliwakkam, Chennai - 600 125, Tamil Nadu, INDIA
Admin Office: HTC Towers, No.41, GST Road, Guindy, Chennai – 600 032, Tamil Nadu, INDIA
Phone: +91 44 4345 3500 / +91 44 4345 3349

www.itmr.ac.in