Certificate Course in Cyber Forensics (CCCF)

Course Duration: 150 Hrs – 45 WORKING days

Course start: 19/12/2021

Prerequisite:

Basic Knowledge of operating systems (Windows/Linux), Computer networks (TCP/IP Suite), and network infrastructures like server architectures, routers, firewalls, IDS etc.

Eligibility Criteria: Any Engineering /Science graduate with mathematics up to 10+2 level

Syllabus

Introduction to Cyber Forensics

The various tools (both hardware and software) installed at the lab should be able to identify, understand and analyze the various electronic evidences currently observed in crime scene investigations. The cyber forensics discipline is classified into disk forensics, mobile forensics, memory forensics or network forensics depending on the type of evidence analyzed. The various hardware and software tools needed for each category are detailed as below.

- **Disk Forensics** - For analysis of hard disks, pen drives and memory cards, disk analysis tools are needed. The NIST standard recommends write blocking facility while seizing a disk. The analysis will be carried on the forensics image of the suspect device
- **Mobile Phone Forensics** - It covers the set of evidences that include mobile related information. The mobile related information comes at the handset, the SIM Card or the network operator. The procedure for seizure and analysis of Mobile Phones is completely different from disk-based evidences. Hence the set of standards formulated for such devices are different as per the NIST standards
- **Memory Forensics** - The live condition of a running machine can be assessed by analyzing the memory. The memory stores information about the currently running process, passwords, time- date information and malicious codes in memory. The forensics procedure is entirely different from mobile and disk forensics procedures
- **Network Forensics** - Network forensics analyses the packets traversing through a network in online or offline mode, analyses network related logs and analyses the source of emails
- **Network Management System DARPAN with SARAN** - DARPAN Series 3 (S3) is a policy based autonomic network and cloud management suite of

solutions for heterogeneous multi-vendor IP networks. The system supports both centralized and distributed hierarchical management and is suitable for any size network ranging from small Local Area Network (LAN) to large geographically distributed multi-site enterprise networks and SARAN acts as the Next Generation Service Desk with a facility to raise tickets based on issues and track the status of issues until resolved

- **Digital Evidence Management System (DEMS)** - It is a web-based Evidence Management System. The DEMS is mainly targeted for law enforcement agencies and analysis labs for managing large volume of digital evidences including the chain of custody. It shall also be used for enterprises or government departments, who have to handle digital evidences