**Establishing Digital Forensics Labs - India and USA (Standards)**

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. Since digital devices such as computers are vulnerable to attack by criminals, digital forensics is increasing in importance. Understanding digital forensic procedures will help to capture vital information which can be used to prosecute a suspect that compromises a digital device or network. The majority of organizations rely deeply on digital devices and the Internet to operate and improve their business, and these businesses depend on the digital devices to process, store and recover data. A large amount of information is produced, accumulated, and distributed via electronic means. It is necessary for forensic experts to increase their abilities to gather evidence from digital devices. Also, deciding on the specific tools for computers or other digital devices that are needed to correctly analyze evidence is crucial. The advancement of the digital forensic investigation requires a new design, improved mechanism and processes. Forensic experts are faced with growth in data. Huge amount of data has expanded and grown in recent years and attempts to consume the storage space available. Digital forensic techniques are used primarily by private organisations and law enforcement agencies to capture, preserve and analyze evidence on digital devices. Digital evidence collected at a crime scene has to be analyzed and connections between the recovered information need to be made and proven. The search for digital evidence is thus a tedious task that consumes time. An extremely large amount of evidence needs to be processed in a very limited time frame which leads to delay in processing schedules. This paper underscores the need to understand the importance of a digital forensic investigative framework. For better research and investigation, developers have created many computer forensics tools. Police departments and investigation agencies select the tools based on various factors including budget and available experts on the team. These computer forensics tools can also be classified into various categories: Disk and data capture tools, File viewers, File analysis tools, Registry analysis tools, Internet analysis tools, Email analysis tools, Mobile devices analysis tools, Mac OS analysis tools, Network forensics tools, and Database forensics tools. Popular digital forensics tools used by various law enforcement agencies in performing crime investigations.

There are seven central forensic laboratories in India, at Hyderabad, Kolkata, Chandigarh, New Delhi, Guwahati, Bhopal and Pune. The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce. The bill was passed in the budget session of 2000 and signed by President K. R. Narayanan on 9 May 2000. The bill was finalised by a group of officials headed by then Minister of Information Technology Pramod Mahajan. The original Act contained 94 sections, divided into 13 chapters and 4 schedules. The laws apply to the whole of India. If a crime involves a computer or network located in India, persons of other nationalities can also be indicted under the law. The Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to nusta editing electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and favour matters connected therewith or incidental thereto.

The American Society of Crime Laboratory Directors (ASCLD) is a nonprofit professional society of crime laboratory directors and forensic science managers dedicated to providing excellence in forensic science through leadership and innovation. The purpose of the organization is to foster professional interests, assist the development of laboratory management principles and techniques; acquire, preserve, and disseminate forensic based information; maintain and improve communication among crime laboratory directors; and to promote, encourage, and maintain the highest standards of practice in the field. The ASCLD organization began to take shape in a meeting that occurred in 1973. In the fall of 1973, a small group of some thirty crime laboratory directors, geographically representing the country, met in Quantico, Virginia. Although called there by Clarence Kelly, then Director of the FBI, it was Briggs White, Director of the FBI Laboratory, who, by his desire to bring local laboratories and the FBI Laboratory together, made it all possible. At that meeting, a steering committee under the able chairmanship of Richard Fox, was formed and met in Kansas City in the spring of 1974. A constitution was drafted, and, in the fall of 1974, in Quantico at the first meeting, ASCLD was born. Chairman – Briggs White, FBI; Vice Chairman – Richard Fox, Missouri; Secretary – Atley Peterson, ATF; Treasurer – Larry Howard, Georgia. On February 18, 1976, ASCLD became ASCLD, Inc. In the 1980’s ASCLD developed a standards subcommittee to evaluate the needs of the criminal justice system. This subcommittee eventually incorporated as a separate and distinct non-profit entity based in North Carolina and has the acronym ASCLD/LAB. ASCLD/LAB merged with ANAB in April 2016. In 1984 the FBI launched a *Computer Analysis and Response Team* and the following year a computer crime department was set up within the British Metropolitan Police fraud squad.

Modern digital societies are subject to cybercriminal activities and fraud leading to economic losses or hazards for individuals. Therefore, the new wave of forensics tools should be engineered to support heterogeneous investigations, preserve privacy, and offer scalability.