Chapter 1
Digital Forensics and Cyber Law Enforcement

K. S. Umadevi
VIT University, India

Geraldine Bessie Amali
VIT University, India

Latha Subramanian
University of Madras, India

ABSTRACT

Security, safety, and privacy are of paramount importance to anyone who likes to crawl on the web. Keeping the best interest of the internet users in mind, India has laid down very solid foundations to safeguard its people from cyberattacks and cyber terrorism. The word "cyber law" encompasses all the cases, statutes, and constitutional provisions that affect persons and institutions who control the entry to cyberspace, provide access to cyberspace, create the hardware and software that enable people to access cyberspace or use their own devices to go "online" and enter cyberspace. Cyber crimes are unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation, and mischief, all of which are subject to the Indian Penal Code.

DOI: 10.4018/978-1-5225-8241-0.ch001

INTRODUCTION TO DIGITAL FORENSICS

The field of digital forensics is consistently growing and there is a huge demand over the last few years, since the usage of computers and mobiles is exponentially growing. Digital forensics deals with investigating these technological devices and monitoring whether something is hacked or likely to be hacked. The end user might not be aware or interested in knowing about these dangers. A deleted photo or a video from your mobile phone or computer in the hands of a hacker is a serious issue. Hence this field is constantly growing to cope with the possible threats. Along with growing demand for new technology in mobile industries, the malware or spyware are also growing. These malware or spyware are capable of monitoring user activities including text messages, emails, phone calls, user locations and so on. As per McAfee report on mobile threats – 2018, one of the most significant threats is Android Grabos. Android Grabos pushes unwanted apps into unsuspected pay per download scam. It was estimated that by the time Google play store identified and removed nearly 144 apps around 17.5 million smart phone users had already downloaded these apps (McAfee mobile threat report, 2018). Including Apple all the app stores are affected by malwares and they remove the dead apps if it poses a security and/or privacy threat to the user without any disclosure of information.

EVOLUTION OF DIGITAL FORENSICS

Modern electronic computer has evolved from the late of the 1900s. As per the history of computing project 1947 considered as the starting of the industrial era of computing and still, we are in the mid of it. Digital forensics has a much shorter history. Industries, research centers, universities needed a large infrastructure set up to meet their requirements, till 1980s computers were used by their appliances only. A textbook "Crime by computers" authored by Donn Parker in 1976 describes the investigation and prosecution carried out using computer data and information (Pollitt, 2010). It further adds that system administrators are solely responsible for securing the networked system and data contained in it. Several organizations like Department of Defense, Internal Revenue Service (IRS) and Federal Bureau of Investigation (FBI) created groups and trained the volunteers of law enforcement to assist the investigators to gain the information by assessing logs and other data from the networked system. But during the 1990s, Cliff Stoll's highlighted how the government agencies shillyshallied in conducting the investigation procedure (Pollitt, M, 2010).

The rise of IBM PCs paved the way for many computer hobbyists. It further resulted in the formation of the first organization on digital forensics named The