Chapter 5
Cybercrime Investigation

Sujitha S.
Thiagarajar College of Engineering, India

Parkavi R.
Thiagarajar College of Engineering, India

ABSTRACT

This book chapter will be an introduction to hacking, DDOS attacks and Malware Analysis. This chapter will also describe about the cyber-crime against properties and Persons and will give a detailed description about the cyber security and privacy. This chapter will deal with the cyber-crime investigations, law enforcement policy and procedures. This chapter will also describe about the peer supporting programs for the law enforcement authorities and a detailed description about the control devices and techniques that are used by an officer. This chapter will give an opportunity to know about the evidence collecting procedures in cyber-crime and also the barriers to cybercrime investigations.

INTRODUCTION

Cybercrime is a crime which involves a network of computers. The computer might used in the crime, or it may be the target of the crime. These crimes may threaten a nation's security and financial health. The problems surrounding these types of crimes have become more, particularly like hacking, copyright infringement, child pornography, and child grooming. There are also some problems of secrecy when

DOI: 10.4018/978-1-5225-1941-6.ch005

private information is seized or revealed, lawfully or otherwise. A computer will be the source of evidence . Even a computer may not be directly used for criminal purpose; it may contain records of importance to criminal investigators in the form of a log file. In most countries, Cybercrime is a fast-growing area of crime. More and more criminals are abusing the speed, accessibility and obscurity of the Internet to obligate a diverse range of criminal activities that identify no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

Even though there is no single common definition of cybercrime, the law enforcement generally makes a distinction between two main types of computer-related crime:

- **Advanced Cybercrime (or High-Tech Crime):** Refined attacks against computer hardware and software
- **Cyber-Enabled Crime:** Many out-dated crimes have taken a new turn with the dawn of the Internet, such as crimes beside children, economic crimes and even terrorism also. New drifts in cybercrime are evolving all the time, with assessed costs to the global economy running to billions of dollars.

In the earlier time, the cybercrime was devoted mainly by individuals or small groups. Today, we are seeing extremely intricate cybercriminal networks fetch together individual persons across the globe in real time to obligate crimes on an extraordinary scale. Criminal groups are revolving increasingly in the Internet to enable their activities and increase their profit in the undeviating time. The crimes themselves are not essentially new – like theft, fraud, illegal betting, and sale of forged medicines – but they are developing in line with the chances presented online and therefore becoming more extensive and destructive.

Cyber law or Internet law is a word that summarizes the legal problems connected to the use of the Internet. It is less a different field of law than intellectual property or contract law, as it is the area covering many fields of law and regulation. INTERPOL is dedicated to the universal fight against cybercrime, as well as undertaking cyber-enabled crimes. Most cybercrimes are international in nature; consequently INTERPOL is the usual companion for any law enforcement agency observing to investigate these crimes on a supportive level. By working with private agencies, INTERPOL is able to provide local law enforcement with motivated cyber intelligence, derived from merging inputs on a global scale.

This chapter will help you to understand the various forms of cybercrimes, in the world, and the law enforcement authorities and the procedures for investigating cybercrime. The Figure 1 is a concept map, which explains to you about this chapter and its contents.