APPENDIX - A

TERMINOLOGY

**Antivirus/ Antimalware:** It is used to detect, remove and prevent malicious software. These software are capable to detect and destroy computer viruses and other malicious software like worms, Trojans, rootkits etc.

**Bots/ Zombie:** These are similar to worms and Trojans but are able to perform more automated tasks on behalf of their master. These computers are compromised by hackers to carry out various attacks like Denial of Services (DoS), spams etc. The network of these bots is called botnet which is used to perform coordinated attacks.

**Campus Area Network (CAN):** It is created by connecting various Local Area Network (LAN) within limited geographical area like university, institute etc. All the network devices like switches, routers, cables are owned by owner of campus or institute.

**Dataset:** It is a collection of data records in logical form like patient investigation reports, credit card transactions, network packets records etc.

**Firewall:** This is a system which monitors incoming and outgoing network traffic against some set of rules. Firewall can be hardware or software and acts as a barrier between trusted and un-trusted networks by allowing only permitted activities.

**Honeypot:** It is a trap which intentionally does not have strong security system and is set to attract hacker/ crackers to penetrate it. These systems are used to learn motives and tactics of hackers targeting different networks. Networks of honeypots are known as honeynets.

**Host:** It is a computer on a network which is used to provide some services to user. Host can be other device like smart phones, palm top, personal digital assistant etc.

**Internet:** It is a global network which is connected with millions of private, public, academic, business, and government networks. It is used to provide variety of
information and communication facilities. The various applications of Internet include World Wide Web, e-mail, telephony, hyper linked web document and file sharing etc.

**Intrusion/ Attack:** Intrusions are unauthorized access of system or network by hackers/ crackers without the consent of owner. Attacks are carried out to destroy, expose, alter or steal computer or network resources.

**Local Area Network (LAN):** It is network that connects computers and other smart devices within limited area such as building. Typically LAN connects computers and peripheral devices like network printers, network storage by same communication link.

**Malware:** It consists of two terms: malicious and software. All the software or programs used to carry out attacks and intrusions on computer, network and other resources are termed as malware. It includes viruses, worm, Trojans, rootkits, spyware, backdoors, evasion etc.

**Network Traffic:** It is data in network which can be in the form of encapsulated packets, network logs etc. Network traffic is the inbound and outbound packets travelling though a particular network link.

**Proxy Server:** This is an intermediately system which process client request and server response for performance, anonymity and security purposes. It also improves speed of web accessing by caching previously accessed web pages.