Glossary

Access Point (AP) Central communication point for IEEE 802.11 wireless networks.

Address Resolution Protocol (ARP) A protocol in the TCP/IP suite that is used dynamically to associate network layer IP addresses with data-link layer MAC addresses.

Ad hoc Network Networks established when Bluetooth-enabled (or similar) devices come into proximity.

Anger Excitation (aka. Sadistic) Behaviors Behaviors that evidence offender sexual gratification from victim pain and suffering. The primary motivation for the behavior is sexual; however, the sexual expression for the offender is manifested in physical aggression, or torture behavior, toward the victim.

Anger Retaliatory (aka. Anger or Displaced) Behaviors Offender behaviors that are expressions of rage, either toward a specific person, group, institution, or a symbol of either. The primary motivation for the behavior is the perception that one has been wronged or injured somehow.

Application Software that performs a specific function or gives individuals access to Internet/network services.

Application Layer Provides the interface between people and networks, allowing us to exchange e-mail, view Web pages, and utilize many other network services.

Asynchronous Transfer Mode (ATM) A connection-oriented network technology that provides gigabit-per-second throughput. This high-performance network technology can transport high-quality video, voice, and data.

Attached Resource Computer Network (ARCNET) One of the earliest local area networking technologies initially developed by Datapoint Corporation in 1977. Uses 93 ohm RG62 coaxial cable to connect computers. Early versions enabled computers to communicate at 2.5 Mbps. A newer, more versatile version called ARCNET Plus, supports 20 Mbps throughput.

Behavioral Evidence Any type of forensic evidence that is representative or suggestive of behavior.

Behavioral Evidence Analysis The process of examining forensic evidence, victimology, and crime scene characteristics for behavioral convergences before rendering a deductive criminal profile.

Behavior-Motivational Typology A motivational typology that infers the motivation (i.e., anger-retaliatory, assertive, reassurance, sadistic, profit, and precautionary) of behavior from the convergence of other concurrent behaviors. Single behaviors can be described by more than one motivational category, as they are not exclusive of each other.

Broad Targeting Any fire or explosive that is designed to inflict damage in a wide reaching fashion. There may be an intended target near the point of origin, but it may also be designed to reach beyond that primary target for other victims in the environment.

Buffer Overflow Cleverly crafted input to a program that intentionally provides more data than the program is designed to expect, causing the program to execute commands on the system.

Digital Evidence and Computer Crime, Third Edition

Used by computer intruders to gain unauthorized access to servers or escalate their privileges on a system that they have already broken into.

Bulletin Board System (BBS) An application that can run on a personal computer enabling people to connect to the computer using a modem and participate in discussions, exchange e-mail, and transfer files. These are not part of the Internet.

Collateral Victims Those victims that an offender causes to suffer loss, harm, injury, or death (usually by virtue of proximity) in the pursuit of another victim.

Computer Cracker Individuals who break into computers much like safecrackers break into safes. They find weak points and exploit them using specialized tools and techniques.

Computer Crime As defined in Federal and State Statutes: includes theft of computer services; unauthorized access to protected computers; software piracy and the alteration or theft of electronically stored information; extortion committed with the assistance of computers; obtaining unauthorized access to records from banks, credit card issuers, or customer reporting agencies; traffic in stolen passwords and transmission of destructive viruses or commands.

Corpus Delicti Literally interpreted as meaning the "body of the crime" — refers to those essential facts that show a crime has taken place.

Crime Reconstruction The determination of the actions surrounding the commission of a crime. This may be done by using the statements of witnesses, the confession of the suspect, the statement of the living victim, or by the examination and interpretation of the physical evidence. Some refer to this process as crime scene reconstruction; however, the scene is not being put back together in a rebuilding process, only the actions that are reconstructed.

Crime Scene A location where a criminal act has taken place.

Crime Scene Characteristics The discrete physical and behavioral features of a crime scene.

Crime Scene Type The nature of the relationship between offender behavior and the crime scene in the context of an entire criminal event (i.e., point of contact, primary scene, secondary scene, intermediate scene, or disposal site).

Cybercrime Any offense where the *modus operandi* or signature involves the use of a computer network in any way.

Cyberspace William Gibson coined this term in his 1984 novel *Neuromancer*. It refers to the connections and conceptual locations created using computer networks. It has become synonymous with the Internet in everyday usage.

Cyberstalking The use of computer networks for stalking and harassment behaviors. Many offenders combine their online activities with more traditional forms of stalking and harassment such as telephoning the victim and going to the victim's home.

Cybertrail Any convergence of digital evidence that is left behind by a victim or an offender. Used to infer behavioral patterns.

Data-Link Layer Provides reliable transit of data across a physical link using a network technology such as the Ethernet. Encapsulates data into frames or cells before sending them, and enables multiple computers to share a single physical medium using a media access control method like CSMA/CD.

Digital Representation of information using numbers. The representation of information using binary digits (bits) and hexadecimal values are special cases of digital representation.

Digital Evidence Encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator.

E-mail, or Email A service that enables people to send electronic messages to each other.

Equivocal Forensic Analysis A review of the entire body of physical evidence in a given case that questions all related assumptions and conclusions. The purpose of the equivocal forensic analysis is to maximize the exploitation of physical evidence accurately to inform the reconstruction of specific crime scene behaviors.

Ethernet A local area networking technology initially developed at the Xerox Corporation in the late 1970s. In 1980, Xerox, Digital Equipment Corporation, and Intel Corporation published the original 10 Mbps Ethernet specifications that were later developed by the Institute of Electrical and Electronic Engineers (IEEE) into the IEEE 802.3 Ethernet Standard that is widely used today. Ethernet uses CSMA/CD technology to control access to the physical medium (Ethernet cables).

Fiber Distribution Data Interface (FDDI) A token ring network technology that uses fiber-optic cables to transmit data by encoding it in pulses of light. FDDI supports a data rate of 100 Mbps and uses a backup fiber-optic ring that enables hosts to communicate even if a host on the network goes down.

Hardware The physical components of a computer.

High Risk Victim An individual whose personal, professional, and social life continuously exposes him/her to the danger of suffering harm or loss.

Host A computer connected to a network.

ICQ ("I Seek You") Internet service that enables individuals to convene online in a variety of ways (text chat, voice, message boards). This service also enables file transfer and e-mail exchanges.

Internet Global computer network linking smaller computer networks that enable information sharing via common communication protocols. Information may be shared using electronic mail, newsgroups, the World Wide Web, and synchronous chat. The Internet is not controlled or owned by a single country, group, organization, or individual. Many privately owned networks are not a part of the Internet.

Internet/Network Service A useful function supported by the Internet/ network such as e-mail, the Web, Usenet, or IRC. Applications give individuals access to these useful functions.

Internet Relay Chat (IRC) Internet service that enables individuals from around the world to convene and have synchronous (live) discussions. This service also enables individuals to exchange files and have private conversations. The primary networks that support this service are EFNet, Undernet, IRCnet, DALnet, SuperChat, and NewNet.

Internet Service Provider (ISP) Any company or organization that provides individuals with access to, or data storage on, the Internet.

Jurisdiction The right of a court to make decisions regarding a specific person (personal jurisdiction) or a certain matter (subject matter jurisdiction).

Locard's Exchange Principle The theory that anyone, or anything, entering a crime scene both takes something of the scene with them, and leaves something of themselves behind when they leave.

Low Risk Victim An individual whose personal, professional, and social life does not normally expose them to a possibility of suffering harm or loss.

Media Access Control (MAC) address A unique number assigned to a Network Interface Card that is used to address data at the data-link layer of a network.

Message Digest A combination of letters and numbers generated by special algorithms that take as input a digital object of any size. A file is input into a special algorithm to produce a sequence of letters and numbers that is like a digital fingerprint for that file. A good algorithm will produce a unique number for every unique file (two copies of the same file have the same message digest).

Method of Approach A term that refers to the offender's strategy for getting close to a victim.

Modem (see Modulator/Demodulator) A piece of equipment used to connect computers together using a serial line (usually a telephone line). This piece of equipment converts digital data into an analog signal (modulation) and demodulates an analog signal into digits that a computer can process.

Modus Operandi (MO) A Latin term that means, "method of operating." It refers to the behaviors that are committed by an offender for the purpose of successfully completing an offense.

An offender's *modus operandi* reflects how an offender committed their crimes. It is separate from the offender's motives, or signature aspects.

Motivational Typology Any classification system based on the general emotional, psychological, or material need satisfied by an offense or act.

Motive The emotional, psychological, or material need that impels, and is satisfied by, a behavior.

Narrow Targeting Any fire or explosive designed to inflict specific, focused, calculated amounts of damage to a specific target.

Network Interface Card (NIC) Hardware used to connect a host to the network. Every host must have at least one network interface card. Every NIC is assigned a MAC address.

Network Layer Addresses and routes information to its destination using addresses, much like a postal service that delivers letters based on the address on the envelope.

Newsgroups The online equivalent of public bulletin boards, enabling asynchronous communication that often resembles a discussion.

Peer-to-Peer Network (P2P)

Physical Evidence Any physical object that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator.

Physical Layer The actual media that carry data (e.g., telephone wires; fiber-optic cables; satellite transmissions). This layer is not concerned with what is being transported, but without it there would be no connection between computers.

Piconet A term to describe small networks established by Bluetooth-enabled (or similar) devices.

Point of Contact The location where the offender first approaches or acquires a victim.

Point of Origin The specific location at which a fire is ignited, or the specific location where a device is placed and subsequently detonated.

Port A number that TCP/IP uses to identify Internet services/application. For example, TCP/IP e-mail applications use port 25 and Usenet applications use port 119.

Power Assertive (aka Entitlement) Behaviors Offender behaviors that are intended to restore the offender's self-confidence or self-worth through the use of moderate to high aggression means. They suggest an underlying lack of confidence and a sense of personal inadequacy expressed through control, mastery, and humiliation of the victim, while demonstrating the offender's sense of authority.

Power Reassurance (aka Compensatory) Behaviors Offender behaviors intended to restore the offender's self-confidence or self-worth through the use of low aggression or even passive and self-deprecating means. They suggest an underlying lack of confidence and a sense of personal inadequacy.

Presentation Layer Formats and converts data to meet the conventions of the specific computer being used.

Primary Scene The location where the offender engaged in the majority of his or her attack or assault upon the victim or victims.

Router A host connected to two or more networks that can send network messages from one network (e.g., an Ethernet network) to another (e.g., an ATM network) provided the networks are using the same network protocol (e.g., TCP/IP).

Search Engine A database of Internet resources that can be explored using key words and phrases. Search results provide direct links to information.

Secondary Scene Any location where there may be evidence of criminal activity outside of the primary scene.

Session Layer Coordinates dialog between computers by establishing, maintaining, managing, and terminating communications.

Signature Aspects The emotional or psychological themes or needs that offenders satisfy when they commit offensive behaviors.

Signature Behaviors Acts committed by an offender that are not necessary to complete the offense. Their convergence can be used to suggest an offender's psychological or emotional needs (signature aspect). They are best understood as a reflection of the underlying personality, lifestyle, and developmental experiences of an offender.

Software Computer programs that perform some function.

Souvenir A personal item taken from a victim or a crime scene by an offender that serves as a reminder or token of remembrance representing a pleasant experience. Taking souvenirs is associated with reassurance-oriented behavior and needs.

Symbol Any item, person, or group that represents something else such as an idea, a belief, a group, or even another person.

Synchronous Chat Networks By connecting to a synchronous chat network via the Internet, individuals can interact in real time using text, audio, video, and more. Most synchronous chat networks are comprised of chat rooms, sometimes called channels, where people with similar interests gather.

Target The object of an attack from the offender's point of view.

TCP/IP A collection of internetworking protocols including the Transport Control Protocol (TCP), the User Datagram Protocol (UDP), the Internet Protocol (IP), and the Address Resolution Protocol (ARP).

Transport Layer Responsible for managing the delivery of data over a network.

Trophy A personal item taken from a victim or crime scene by an offender that is a symbol of victory, achievement, or conquest. Often associated with assertive-oriented behavior.

User's Network (Usenet) A global system of newsgroups that enables people around the world to post messages to the equivalent of an online bulletin board.

Victimology A thorough study of all available victim information. This includes items such as sex, age, height, weight, family, friends, acquaintances, education, employment, residence, and neighborhood. This also includes background information on the lifestyle of the victim such as personal habits, hobbies, and medical histories.

World Wide Web (WWW or Web) A service on the Internet providing individual users with access to a broad range of resources, including e-mail, newsgroups, and multimedia (images, text, sound, etc.).