**Digital Evidence and Computer Crime:**

Criminals are using advanced technology to facilitate their offenses and avoid apprehension, creating new challenges for attorneys, judges, law enforcement agents, forensic examiners, and corporate security professionals.

The textbook defines digital evidence as any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi. By now, it is well known that attorneys and police are encountering progressively more digital evidence in their work.

Computers are used in two ways in criminal activities. Either a computer is used to commit a crime, or the computer itself is the target of a crime. “Digital evidence is becoming a feature of most criminal cases . . . Everything is moving in this direction" (Susan Brenner, professor of law and technology at the University of Dayton School of Law; see CNN (2005)). Child pornography, threatening letters, web phishing, identity theft, and theft of intellectual property are all crimes that leave electronic trials. Investigation into these types of crimes usually includes searching computers that are suspected of being involved in their commission. Such analysis involves sifting through huge amounts of data for specific keywords to see what happened at certain times, and hopefully providing evidence that a specific person did a specific illegal act—or that a specific person apparently did not commit an illegal act.

Computers themselves can be the victim of the crimes. This normally happens when computer systems are remotely attacked. Remote attacks have become far more common, taking advantage of increasingly complex and vulnerable network services. The CERT and US-CERT web sites have lists of vulnerabilities of network infrastructure systems that could be used to attack computer systems. Some of the attacks are also listed in these web sites.

Computer forensics involves evidence acquisition, evidence authentication, and evidence analysis. Digital evidence such as log files is often transparently created by the computer’s operating system without the knowledge of the computer operator and is often hidden from view. To find it, special forensics tool and techniques are needed. We need also keep in mind that criminals are also concerned with digital evidence and will attempt to manipulate computer systems to avoid apprehension (e.g., when an offender uses root kit to delete his/her electronic trails). This module will teach you the AAA forensic investigation methodologies using examples and specially designed tools. You need to extend these experiences and knowledge creatively to cases that you will meet in practice.

Digital evidence creates several challenges for forensic examiners. First, it is a form of evidence that can be very difficult to handle. For example, an acquired hard drive contains huge amounts of data, though only a small portion might be relevant to the case. Second, digital evidence is generally an abstraction of some event or digital object. For example, when an email related to a case is intercepted, the content of the email gives only a partial view of what occurred. Third, digital evidence can be manipulated easily. For example, the evidence could be maliciously modified by offenders or be altered accidentally by system administrators. Fourth, digital evidence is usually circumstantial. Thus, special attention should be paid to the digital evidence collection process and to the chain of evidence that we will discuss later. For example, the Predator and Prey Alert (PAPA) that has recently been developed by Florida State University can be used to achieve high-quality digital evidence for the prosecution of cyber-stalking cases. The PAPA system allows a law enforcement agent to remotely shadow a victim, advise the victim by communicating through a separate side channel, and assume control of the victim's computer in order to interact directly with the stalker.

While criminals feel safe on the Internet, they are observable and thus vulnerable. We can take this opportunity to uncover crimes in the physical world that would not be visible without the Internet. Indeed, several murderers have been identified as a result of their online actions

 (LJworld 2004). In addition, the Internet may contain digital evidence of the crime that may be not directly involved. For example, there are a growing number of sensors on the Internet such as cameras showing live highway traffic on the Web (e.g., you can view the real-time traffics in Montgomery County, Maryland, at http://www.ncsmartlink.org/cameras/; you can view regularly refreshed traffics in South Carolina at http://www.scdot.org/getting/cams/). These cameras may inadvertently capture evidence relating to a crime. Furthermore, digital networks usually contain a higher concentration of digital information about the individuals who use them, making it easier to find and collect relevant digital data. It is conceivable that a digital investigator could determine where an individual was throughout a given day using GPS information that the individual’s wireless phone transmits to his/her service provider. Organizational computer log information can also be used to determine where an employee was and what she/he was doing during a given day. The challenge is that data can be spread over a group of adjacent buildings, several cities, states, or even countries; it is difficult to find and collect all relevant digital evidence. For all but the smallest networks, it is not feasible to take a snapshot of an entire network at a given instant. Also, network traffic is transient and must be captured while it is in transit.