Computer Forensics and Digital Investigation – a brief introduction

Ulf Larson/Erland Jonsson

Defining the word forensic

- American Heritage Dictionary definition of forensic:
  - “Relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law.”
- Many methods use science and technology to investigate and establish facts.
- Forensics are used when the results of the method should be ***valid in a court of law***

Defining *Computer* forensics

- Corresponding definition for computer forensics would be:
  - "Relating to the use of computer science or technology in the investigation and establishment of facts or evidence regarding crimes committed with computers, or against computers, in a court of law."
  - or… "The art and science of applying computer science to aid the legal process"
  - or… "The application of computer investigation and analysis techniques to determine potential legal evidence"

Thus, when *computers* are involved in the process of establishing facts that should be valid in a court of law, we denote this process as "computer forensics"

The digital investigation

- However, not all investigations goes to court..
  - Corporate investigations
  - Private investigations
- ..and therefore, all investigations are not “computer forensics”
  - A better name for the investigation process is **digital investigation**, or **digital crime scene investigation**

The digital investigation

- A digital investigation takes place when a digital incident is reported and evidence needs to be found

- Analogy to physical investigation:
  - A physical investigation considers fibers, footprints, blood stains and fingerprints.
  - A digital investigation considers text files, e-mail messages, log entries and alerts.

The digital investigation: Targets

The digital investigation regards:

- Crimes committed ***against*** computers:
  - Intrusions and break-ins and insider jobs by networked attackers
- Crimes committed ***with*** computers:
  - Communication between criminals engaged in murder, kidnapping, assault, extortion, drug dealing, espionage, terrorism, child pornography.

The digital investigation: purpose

- Its purpose is to provide information about:
  - What happened
  - When did events that led to the crime occur
  - In what order did the events occur
  - What was the cause of the events
  - Who caused the events to occur
  - What enabled the events to take place
  - What was affected, how much was it affected