DFSC 1316: digital forensic and information assurance fundamentals I

1. WHAT IS DF AND IA?

Digital Forensics (DF)

- A branch of forensic science
  - Forensic: scientific tests or techniques used in connection with the detection of crime.
- It’s about legal evidence found in computers and network devices and more
  - "what information is here?" and
  - "what is the sequence of events responsible for the present situation?"
- Digital Forensics >= Computer Forensics
  - Network Forensics
  - Mobile Device Forensics
  - etc…

DF Applications

- Criminal Investigation
  - The BTK killer: “Can I communicate with Floppy and not be traced to a computer…”.
- Civil Litigation
  - Discovery of digital evidence in civil cases.
- Intelligence
  - The up-side: counter terrorism.
  - The down-side: PRISM and Edward Snowden.
- Administrative Matters
  - Collecting evidence of computer abuse by employees.

The Forensics Process

- 5 basic steps
  - Preparation (investigator and tools)
  - Collection (data)
  - Imaging and Verifying
  - Analysis
  - Reporting

Step 1 - Preparation

- The investigator must be properly trained to perform the specific kind of investigation that is at hand.
- Tools that are used should be validated. There are many tools to be used in the process. One should determine the proper tool to be used based on the case.
  - *EnCase* by Guidance Software
  - *Forensic ToolKit (FTK)* by Access Data
  - Open Source DF tools: *SANS SIFT*, etc.

Step 2 - Collection

- Where is the digital evidence?
  - a storage medium (such as a hard disk or CD-ROM)
  - an electronic document (e.g. an email message or JPEG image)
  - a sequence of packets moving over a computer network
  - Not-so-easy-to-think-of: web page browsing histories, frequently searched phases, paired devices (which must be preserved as they are subject to change).
  - etc…

Special Handling of Collecting Digital Evidence

- Most digital information changes easily and frequently.
- It is usually difficult to detect that a change has taken place unless other measures have been taken.
- Common practice: calculate and store a cryptographic *Hash* of an evidence file for later comparison.
  - A *hash function* is any function that can be used to map data of arbitrary size to data of fixed size.

Special Handling of Collecting Digital Evidence

- Handle the original evidence as little as possible to avoid changing the data.
- Establish and maintain the chain of custody (for each evidence item from the time it is collected to the time it is presented on court).
- Documenting everything that has been done.
- Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability

More on Collecting Digital Evidence

- Some of the most valuable information obtained in the course of a forensic examination will come from the computer’s user.
  - An interview with the user can yield valuable information about the system configuration, applications, encryption keys and methodology.
  - Forensic analysis is much easier when analysts have the user's passphrases to access encrypted files, containers, and network servers.

Step 3 – Imaging/Verifying Digital Evidence

- The process of creating an exact duplicate of the original evidentiary media is often called *Imaging*.
  - Differs from a file-to-file copy.
- Verifying the Image
  - The imaging process is verified by using *Hash* algorithms.
  - At critical points throughout the analysis, the media is verified again, known as "hashing", to ensure that the evidence is still in its original state.

Step 4 - Analysis

- All digital evidence must be analyzed to determine the type of information that is stored upon it.
  - For this purpose, specialty tools are used that can display information in a format useful to investigators.
- In many investigations, numerous other tools are used to analyze specific portions of information.
  - Browser history analyzing tools.
  - System configuration analyzing tools.
  - File carving tools.

Step 5 - Reporting

- Once the analysis is complete, a report is generated.
  - Many modern forensic tools can generate automated report.
  - Human interaction is necessary to enhance readability.
  - Other formats: written report, oral testimony, or some combination of the two.
- Keep in mind
  - Report may not be read only by technicians.
  - Report may not be utilized immediately.

Examples of DF

- Chandra Levy
  - Chandra Levy was a Washington, D.C. intern who disappeared on April 30, 2001.
  - She had used the web and e-mail to make travel arrangements and communicate with her parents. Information found on her computer led police to search most of Rock Creek Park, where her body was eventually found one year later by a man walking his dog.

Examples of DF cont.

- BTK Killer
  - Dennis Rader was convicted of a string of serial killings that occurred over a period of sixteen years.
  - Towards the end of this period, Rader sent letters to the police on a floppy disk. *Metadata* within the documents implicated an author named "Dennis" at "Christ Lutheran Church"; this evidence helped lead to Rader's arrest.

Information Assurance (IA) Definition

- Conducting operations that protect and defend information and information systems by ensuring (goals):
  - Confidentiality
  - Integrity
  - Availability
  - Authentication
  - Non-repudiation

} The *CIA* triad

Goal #1 - Confidentiality

- Holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.
- Sometimes also called Privacy or Data Security
- Countermeasure:
  - Data encryption.
  - Access control.

Goal #2 - Integrity

- Maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.
  - System Integrity (hardware and software).
  - Data Integrity
- Countermeasure:
  - User access control to prevent.
  - Checksum and/or hash to detect.

Goal #3 - Availability

- State where information is in the place needed by the user, at the time the user needs it, and in the form needed by the user.
- Issues that affect availability
  - System reliability
  - Timely Delivery
- Countermeasure
  - Redundancy (hardware availability).
  - Firewalls, etc (software availability).

Goal #4 - Authentication

- To verify the identity of the user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system
- In short – to verify you are who you say you are (authentication), and grant you the right to access information (authorization).
- Countermeasure:
  - Password.
  - Biometric: figureprint, iris, etc. (por and con?)

Goal #5 - Non-Repudiaton

- Ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
- In short: one can not deny what he has done.
- Countermeasure:
  - Trusted third party (TTP), e.g., notary.
  - Asymmetric cryptography, i.e., public keying algorithm.

3 Types of Non-Repudiation

- non-repudiation of origin
  - One cannot deny he sent a message.
- non-repudiation of submission
  - Message transit point cannot deny it submitted a message for delivery.
- non-repudiation of delivery
  - Recipient cannot deny receiving a message

IA Process

- Enumeration and classification of the information to be protected
- Risk assessment – considers the probability and impact of undesired events.
- Risk management plan – mitigates, eliminates, accepts or transfers the risks.
- Evaluate and audit the plan