CYBER SECURITY AND NETWORK FORENSICS

Ramesh Manza

Associate Professor,

Bio Medical Image Processing Laboratory,

Department of Computer Science and Information Technology, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad (MS) India431004 www.manzaramesh.in

manzaramesh@gmail.com

Python Digital Forensics

What is Digital Forensics?

- Digital forensics may be defined as
  - the branch of forensic science that
    - analyzes,
    - examines,
    - identifies and
    - recovers
      - the digital evidences residing on
        - » electronic devices.

What is Digital Forensics?

- It is commonly used for
  - criminal law and
  - private investigations.
- For example –
  - you can rely on digital forensics extract evidences in case
    - somebody steals some data on an
      - electronic device.

Brief Historical Review of Digital Forensics

- **1970s-1980s: First Computer Crime**
- In 1978 the first computer crime was recognized in
  - Florida Computer Crime Act,
  - which included
    - legislation against unauthorized
    - modification or deletion of data on a
      - computer system.

Brief Historical Review of Digital Forensics

- But over the time,
  - due to the advancement of technology,
    - the range of computer crimes being committed also increased.
- To deal with crimes related to
  - copyright,
  - privacy and
  - child pornography,
    - various other laws were passed.

Brief Historical Review of Digital Forensics

- **1980s-1990s: Development Decade**
- This decade was the
  - development decade for
    - digital forensics,
  - all because of the
    - first ever investigation (1986) in which
      - Cliff Stoll tracked the hacker named
        - » Markus Hess.

Brief Historical Review of Digital Forensics

- During this period,
  - two kind of digital forensics disciplines developed –
    - first was with the help of
      - ad-hoc tools and techniques developed by
        - » practitioners who took it as a hobby,
    - while the second being developed by
      - scientific community.
- In 1992,
  - the term **“Computer Forensics”** was used in
    - academic literature.

Brief Historical Review of Digital Forensics

- **2000s-2010s: Decade of Standardization**
- After the development of
  - digital forensics to a certain level,
    - there was a need of
      - making some specific standards
      - that can be followed while
        - » performing investigations.
- Accordingly,
  - various scientific agencies and
  - bodies
    - have published
      - guidelines for
        - » digital forensics.

Brief Historical Review of Digital Forensics

- In 2002,
  - Scientific Working Group on
    - Digital Evidence (SWGDE)
      - published a paper named
        - » “Best practices for Computer Forensics”.

Brief Historical Review of Digital Forensics

- Another feather in
  - the cap was a
    - European led international treaty namely
      - **"The Convention on Cybercrime"** was
        - » signed by
          - 43 nations and
          - ratified by 16 nations.
- Even after such standards,
  - still there is a need
    - to resolve some issues
      - which has been
        - » identified by
          - researchers.

Process of Digital Forensics

- **Phase 1: Acquisition or Imaging of Exhibits**

- It is very much similar to
  - taking photographs,
  - blood samples etc.
    - from a crime scene.
- For example,
  - it involves
    - capturing an image of
      - allocated and
      - unallocated
        - areas of a hard disk or RAM.

Process of Digital Forensics

Phase 2: Analysis

- The input of this phase is the
  - data acquired in the
    - acquisition phase.

- **Inculpatory evidences** –
  - These evidences support a given
    - history.

Process of Digital Forensics

Phase 2: Analysis

- **Exculpatory evidences –**
  - These evidences contradict a given
    - history.
- **Evidence of tampering –**
  - These evidences show that the
    - system was tempered to avoid
      - identification.
  - It includes
    - examining
      - the files and directory content for
        - » recovering the deleted files.

Process of Digital Forensics

Phase 3: Presentation or Reporting

- As the name suggests,
  - this phase presents the
    - conclusion and
    - corresponding evidences from the
      - investigation.

Applications of Digital Forensics

Digital forensics having two application.

- **1 Criminal Law** The evidence is collected
  - to support or
  - oppose a hypothesis in the
    - court.
  - Forensics procedures are
    - very much similar to those used in
      - criminal investigations but
    - with different legal requirements and limitations.

Applications of Digital Forensics

Digital forensics having two application.

- **2. Private Investigation**
  - Mainly corporate world uses digital forensics for
    - private investigation.
- It is used when
  - companies are suspicious that
    - employees may be performing an
      - illegal activity on their computers that is against
        - » company policy.

Branches of Digital Forensics

- The digital crime is not restricted to computers alone,
  - however hackers and criminals are using
    - small digital devices such as
      - tablets,
      - smart-phones etc.

Branches of Digital Forensics

Type of devices, digital forensics has the following branches-

- **Computer Forensics** This branch of digital forensics deals with
  - computers, embedded systems and static memories such as USB drives.
- **Mobile Forensics** This deals with
  - investigation of data from mobile devices.
  - mobile devices have an inbuilt communication system which is useful for
    - providing useful information related to location.

Branches of Digital Forensics

- **Network Forensics** This deals with the
- monitoring and analysis of computer network traffic,
  - both local and WAN(wide area network) for the purposes of
    - information gathering,
    - evidence collection, or
    - intrusion detection.
- **Database Forensics** This branch of digital forensics deals with
  - forensics study of
    - databases and
    - their metadata.

Skills Required for Digital Forensics Investigation

- Digital forensics examiners help to track
  - hackers,
  - recover stolen data,
  - follow computer attacks
    - back to their source, and
  - aid in other types of investigations
    - involving computers.

Skills Required for Digital Forensics Investigation

- **Outstanding Thinking Capabilities**

➢ A digital forensics investigator must be an

  ➢ outstanding thinker and

  ➢ should be capable of applying different

    ➢ tools and methodologies on a particular assignment for obtaining the output.

Skills Required for Digital Forensics Investigation

- **Technical Skills**

➢ A digital forensics examiner must have good technological skills because

  ➢ this field requires the knowledge of network,

    ➢ how digital system interacts.

Skills Required for Digital Forensics Investigation

- **Passionate about Cyber Security** Because
  - the field of digital forensics is all about solving cyber-crimes and
  - this is a tedious task,
  - it needs lot of passion for someone to become an ace
    - digital forensic investigator.

Skills Required for Digital Forensics Investigation

- **Communication Skills:**
  - Good communication skills are a must to
    - coordinate with various teams and
    - to extract any missing
      - data or information.

Skills Required for Digital Forensics Investigation

- **Skillful in Report Making**
  - After successful implementation of acquisition and analysis,
- a digital forensic examiner must mention
  - all the findings the final report and presentation.
- Hence he/she must have
  - good skills of
    - report making and
    - an attention to detail.

Limitations

Digital forensic investigation offers certain limitations as discussed here

- **Need to produce convincing evidences**
  - One of the major setbacks of digital forensics investigation is that
    - the examiner must have to comply with
      - standards that are required for
        - » the evidence in the court of law,
        - » as the data can be easily tampered.
- And also having knowledge of
  - legal requirements,
  - evidence handling and
  - documentation procedures to
    - present convincing evidences in the
      - court of law.

Limitations

- **Investigating Tools**
  - The effectiveness of digital investigation
    - entirely lies on
      - the expertise of
        - » digital forensics examiner and
      - the selection of proper
        - » investigation tool.

Limitations

- **Lack of technical knowledge among the audience**
  - Another limitation is that
    - some individuals are not completely familiar with
      - computer forensics;
- therefore,
  - many people do not understand this field.
- **Cost**
  - Producing digital evidences and
  - preserving them is
    - very costly.
  - Hence this process may not be chosen by many people
    - who cannot afford the cost.

- Thank you