SNS COLLEGE OF TECHNOLOGY

(Autonomous)

COIMBATORE – 35

DEPARTMENT OF COMPUTER SIENCE AND ENGINEERING (UG & PG)

Third Year Computer Science and Engineering, 5th Semester

UNIT II - CYBER FORESENICS

Topic Name : Forensics Investigation

Forensics are the scientific methods used to solve a crime. Forensic investigation is the gathering and analysis of all crime-related physical evidence in order to come to a conclusion about a suspect. Investigators will look at blood, fluid, or fingerprints, residue, hard drives, computers, or other technology to establish how a crime took place. This is a general definition, though, since there are a number of different types of forensics.

TYPES OF FORENSICS INVESTIGATION

- Forensic Accounting / Auditing
- Computer or Cyber Forensics
- Crime Scene Forensics
- Forensic Archaeology
- Forensic Dentistry
- Forensic Entomology
- Forensic Graphology
- Forensic Pathology
- Forensic Psychology
- Forensic Science
- Forensic Toxicology

Approaching a Computer Forensics Investigation

From the discussion so far, we can appreciate that computer forensics investigation is a detailed science. Now, let us understand how a forensics investigation is typically approached and the broad phases involved in the investigation. The phases involved are as follows:

- Secure the subject system (from tampering or unauthorized changes during the investigation)
- Take a copy of hard drive/disk (if applicable and appropriate)
- Identify and recover all files (including deleted files)

- Access/view/copy hidden, protected and temp files;
- Study "special" areas on the drive (e.g., the residue from previously deleted files)
- Investigate the settings and any data from applications and programs used on the system
- Consider the system as a whole from various perspectives, including its structure and overall contents
- Consider general factors relating to the user's computer and other activity and habits in the context of the investigation
- Create detailed and considered report, containing an assessment of the data and information collected.

Typical Elements Addressed in a Forensics Investigation Engagement Contract

Typically, the following important elements are addressed before while drawing up a forensics investigation engagement contract

- Authorization
- Confidentiality
- Payment
- Consent and acknowledgment
- Limitation of liability

Laboratory responsible for any accidental damages to the data or equipment in its possession including but not limited to surface scratches, deformations and cracks.

- Customer's representation: Customer needs to warrant the forensics laboratory that he/she is the owner of, and/or has the right to be in possession of, all equipment/data/media furnished to the laboratory and that collection, possession, processing and transfer of such equipment/data/media are in compliance with data protection laws to which customer is subject to.

- Legal aspects/the law side: Both the parties need to agree that the agreement shall be governed by prevailing law in every particular way including formation and interpretation and shall be deemed to have been made in the country where the contract is signed.

- Data protection: The computer forensics laboratory (engaged in the investigation) will hold the information that the customer has given verbally, electronically or in any submitted form for the purpose of the forensics investigation to be carried out as per contracted services from the forensics laboratory.

- Waiver/breach of contract: The waiver by either party of a breach or default of any of the provisions on this agreement by either party shall not be construed as a waiver of any succeeding breach of the same or other provisions, nor shall any delay or omission on the

part of either party to exercise or avail itself of any right, power or privilege that it has, or may have hereunder operates as a waiver of any breach or default by either party.

Solving a Computer Forensics Case

These are just some broad illustrative steps and they may vary depending on the specific case in hand.

- Prepare for the forensics examination.
- Talk to key people to find out what you are looking for and what the circumstances surrounding the case are.
- If you are convinced that the case has a sound foundation, start assembling your tools to collect the data in question. Identify the target media.
- Collect the data from the target media. You will be creating an exact duplicate image ofthe device in question. To do this, you will need to use an imaging software application like the commercial in Case or the open-source Sleuth Kit/Autopsy.
- To extract the contents of the computer in question, connect the computer you are investigating to a portable hard drive or other storage media and then boot the computer under investigation according to the directions for the software you are using.
- When collecting evidence, be sure to check E-Mail records as well. Quite often, these messages yield a great deal of information.
- Examine the collected evidence on the image you have created. Document anything that you find and where you found it.
- Analyze the evidence you have collected by manually looking into the storage media and, if the target system has a Windows OS, check the registry.
- Report your findings back to your client. Be sure to provide a clear, concise report; this report may end up as evidence in a court case.