SNS COLLEGE OF TECHNOLOGY

(Autonomous)
COIMBATORE – 35

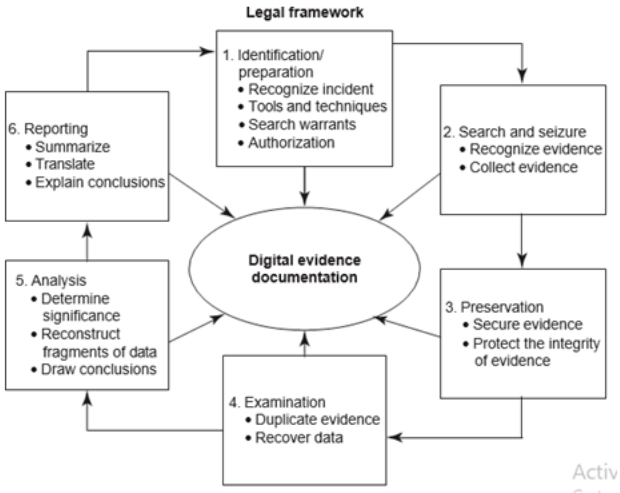
DEPARTMENT OF COMPUTER SIENCE AND ENGINEERING (UG & PG)

Third Year Computer Science and Engineering, 5th Semester

UNIT II - CYBER FORESENICS

Topic Name : Digital Forensics Lifecycle

The digital forensics process needs to be understood in the legal context starting from preparation of the evidence to testifying. Digital forensics evidence consists of exhibits, each consisting of a sequence of bits, presented by witnesses in a legal matter to help jurors establish the facts of the case and support or refute legal theories of the case.



The Phases in Computer Forensics/Digital Forensics

The investigator must be properly trained to perform the specific kind of investigation that is at hand. Tools that are used to generate reports for court 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. Broadly speaking, the forensics life cycle involves the following phases:

- Preparation and identification
- Collection and recording
- Storing and transporting
- Examination/investigation

- Analysis, interpretation and attribution
- Reporting and
- Testifying.

To mention very briefly, the process involves the following activities:

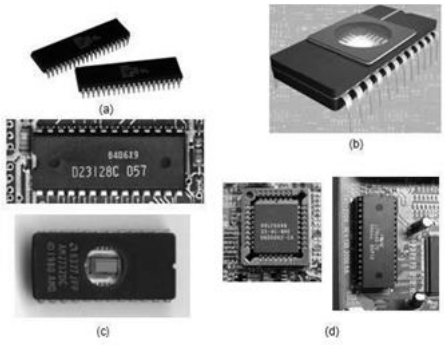
- Prepare: Case briefings engagement terms, interrogatories, spoliation prevention, disclosure and discovery planning, discovery requests.
- Record: Drive imaging, indexing, profiling, search plans, cost estimates, risk analysis.
- Investigate: Triage images, data recovery, keyword searches, hidden data review, communicate, iterate.
- Report: Oral vs. written, relevant document production, search statistic reports, chain of custody reporting, case log reporting.
- Testify: Testimony preparation, presentation preparation, testimony.

Preparing for the Evidence and Identifying the Evidence

In order to be processed and applied, evidence must first be identified asevidence. It can happen that there is an enormous amount of potential evidence available for a legal matter, and it is also possible that the vast majority of the potential evidence may never get identified.

Collecting and Recording Digital Evidence

Digital evidence can be collected from many sources. Obvious sources include computers, cell phones, digital cameras, hard drives, CD-ROM, USB memory devices and so on. Non-obvious sources include settings of digital thermometers, black boxes inside automobiles, RFID tags and webpages (which must be preserved as they are subject to change).



Storing and Transporting Digital Evidence

The following are specific practices that have been adopted in the handling of digital evidence:

1. Image computer media using a write-blocking tool to ensure that no data is added to the suspect device;
2. establish and maintain the chain of custody.

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

As a general rule, one should not examine digital information unless one has the legal authority to do so. Amateur forensics examiners should keep this in mind before starting any unauthorized investigation.

For the purpose of digital evidence examination, "imaging of electronic media" (on which the evidence is believed to be residing) becomes necessary.

Analysis, Interpretation and Attribution

Analysis, interpretation and attribution of evidence are the most difficult aspects encountered by most forensics analysts. In the digital forensics arena, there are usually only a finite number of possible event sequences that could have produced evidence.

Examples of common digital analysis types include:

- Media Analysis
- Media Management Analysis
- File System Analysis

- ApplicationAnalysis
- Network Analysis
- OS Analysis
- Executable Analysis
- Image Analysis
- Video Analysis

Reporting

The following are the broad-level elements of the report

- Identity of the reporting agency
- Case identifier or submission number
- Case investigator
- Identity of the submitter
- Date of receipt
- Date of report
- Descriptive list of items submitted for examination, including serial number, make and model
- Identity and signature of the examiner
- Brief description of steps taken during examination, such as string searches, graphics image searches and recovering erased files
- Results/conclusions.

Testifying

This phase involves presentation and cross-examination of expert witnesses. Depending on the country and legal frameworks in which a cybercrime case is registered, certain standards may apply with regard to the issues of expert witnesses.