5 Legal Aspects of Digital Forensics

Syllabus

Understanding of legal aspects and their impact on digital forensics, Electronics discovery.

Contents

GTU : Winter-21

5.1 Understanding of Legal Aspects

- Legal search authority is the first step in the digital forensic process.
- The process of digital forensics is one of identifying malicious actions brought about by manipulation of computers, networks, and other electronic devices by criminals. This differs from standard police work as the physical mediums work in concert with software mediums to produce results that are often intangible.
- Law enforcement strives to prosecute computer crimes based upon laws that relate far more to physical evidence than digital evidence. Doing so is quite difficult, as many of the laws have not quite kept pace with the current ubiquity of computer-assisted crimes.
- Digital forensic evidence proposed for admission in court must satisfy two conditions : It must be relevant and it must be "derived by the scientific method" and "supported by appropriate validation."
- Since digital evidence usually takes the form of a writing, or at least a form which can be analogized to a writing, it must be authenticated and satisfy the requirements of the Best Evidence Rule. The Best Evidence Rule applies to information stored in computers.
- As a practical matter, a disk or tape is not directly usable by the trier of fact. Rule therefore, provides that, "if data are stored in a computer or similar device, any printout readable by sight, shown to reflect the data accurately, is an 'original'."
- Computers communicate using a packet switching system. Thus, information that is to be transmitted from sender to recipient passes through many phases.
- First it is created by the sender. Then the information to be communicated is broken down into small packets that contain some portion of the contents of the communication as well as sender's and recipient's IP addresses and some accounting information.
- The packets are individually transmitted from the sender's computer to a nearby packet switch and then from switch to switch, at each being stored momentarily and then forwarded to the next available switch in the direction of their ultimate destination.
- Different packets may take different routes through the network as they travel from sender to recipient, depending on link availability and loading in the network. Upon receipt, the packets are reassembled into an exact replica of the original file. Thus, information passes through several stages of disassembly, storing and forwarding, and reassembly, before becoming available to the recipient.

- In addition to the store and forward mechanisms inherent in the packet switching system, at the applications level there may be additional storage intervals while a file is being composed and after receipt but before being opened by the recipient. Finally, the recipient may store the file for future reference for some period of time before deleting it. What, then, constitutes an intercept in this packetized world ?

The 4th Amendment :

- The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no warrants shall issue, but on probable cause, supported by oath or affirmation and particularly describing the place to be searched and the person or things to be seized.

5.1.1 Reasonable Expectation of Privacy

- The right to privacy is an element of various legal traditions to restrain governmental and private actions that threaten the privacy of individuals.
- The reasonable expectation of privacy is an element of privacy law that determines in which places and in which activities a person has a legal right to privacy. Sometimes referred to as the "right to be left alone," a person's reasonable expectation of privacy means that someone who unreasonably and seriously compromises another's interest in keeping her affairs from being known can be held liable for that exposure or intrusion.
- Three dimensions of privacy :
  1) **Personal privacy** : Protecting a person against undue interference (such as physical searches) and information that violates his/her moral sense.
  2) **Territorial privacy** : Protecting a physical area surrounding a person that may not be violated without the acquiescence of the person.
- Safeguards : Laws referring to trespassers search warrants.
  3) **Informational privacy** : Deals with the gathering, compilation and selective dissemination of information.
- Privacy protection can be undertaken by :
  1. Privacy and data protection laws promoted by government.
  2. Self-regulation for fair information practices by codes of conducts promoted by businesses.
  3. Privacy-Enhancing Technologies (PETs) adopted by individuals.
  4. Privacy education of consumers and IT professionals.

5.1.2 The Electronic Communications Privacy Act

- The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986.
- Purpose of the electronic communications Act is to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and. to provide for matters connected therewith.
- The Act protects communications while being made, as well as records of past communications. It is also a crime to use or disclose information obtained through this illegal means.
- The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and other digital and electronic communications.
- The Wiretap Act and the ECPA answer the question of what counts as reasonable differently for electronic, and non-electronic communications.
  a) Wire communications contain the human voice and travel through a wire at some point.
  b) An oral communication is one uttered by a person with the justified expectation that it will not be intercepted by another person.
  c) Electronic communications are all non-wire, non-oral communications.
  d) The Wiretap Acts treatment of non-electronic communications follows the pattern the U. S. Supreme Court laid down in Berger v. New York.

Univeristy Question

1. *Write a short note on the electronic communications privacy act.* **GTU : Winter-21, Marks 3**

5.2 Indian IT Act 2000

- In India the Information Technology Act, 2000 is the Mother Legislation that deals with issues related to use of computers, computer systems, computer networks and the Internet. Amended by the Information Technology (Amendment) Act, 2008.
- In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for

e-commercc in India. And the cyber laws have a malor impact for e-businesses and the new economy in India. So, it is important to understand the various perspectives of the IT Act, 2000 and what it offers.

- The Information technology Act. 2000 also aims to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce". which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers Books Evidence Act, 1891 and the Reserve Bank of India Act. 1934 and for matters connected therewith or incidental thereto.
- The salient features of the Information Technology Act, 2000 are as follows :-

1. It is applicable to the whole of India.
2. Authentication of electronic records is possible.
3. Legal framework for affixing digital signature by use of asymmetric crypto system and hash function.
4. Issue of legal recognition of electronic records and digital signatures.
5. Retention of electronic record.
6. Publication of official gazette in electronic form.
7. Security procedure for electronic records and digital signature.
8. Licensing and regulation of certifying authorities for issuing digital signature certificates.
9. Functions and working of controller.
10. Appointment of certifying authorities and controller of certifying authorities, including recognition of foreign certifying authorities.
11. Procedure for data protection.
12. Definition of computer crimes and their penalties provided under the act.
13. Appointment of adjudicating officer for holding inquiries under the act.
14. Establishment of cyber appellate tribunal under the act.
15. Appeal from order of adjudicating officer to cyber appellate tribunal and not to any civil court and appeal from order of cyber appellate tribunal to high court.

5.2.1 Objective and Scope of IT Act 2000

Objectives of the act are :

1. To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce" in place of paper based methods of communication;
2. To give legal recognition to digital signatures for authentication of any information or matter which requires authentication under any law.
3. To facilitate electronic filing of documents with government departments.
4. To facilitate electronic storage of data.
5. To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions.
6. To give legal recognition for keeping of books of accounts by banker's in electronic form.
7. To amend the Indian Penal Code, the Indian EvidenceAct, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934.

5.2.2 Importance of IT Act

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects.
  a) Firstly, the implication of these provisions for the e-businesses is that email is now a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
  b) Companies are now able to carry out electronic commerce using the legal infrastructure provided by the act.
  c) Digital signatures have been given legal validity and sanction in the act.
  d) The act opens the doors for the entry of corporate companies in the business of being certifying authorities for issuing digital signature certificates.
  e) The act now allows government to issue notification on the web thus heralding e-governance.
  f) The act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate. Government in electronic form by means of such electronic form as may be prescribed by the appropriate government.
  g) The IT act also addresses the important issues of security, which are critical to the success of electronic transactions. The act has given a legal definition to the concept of secure digital signatures that would be required to be passed

through a system of a security procedure, as stipulated by the government at a later date. Under the IT act, 2000, it is possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the act is in the form of monetary damages, not exceeding ₹ 5 crores.

5.3 eDiscovery

GTU : Winter-21

- **eDiscovery is also known** as Electronic discovery. It is a procedure by which parties involved in a legal case preserve, collect, review and exchange information in electronic formats for the purpose of using it as evidence.
- Discovery is the term used for the initial phase of litigation where the parties in a dispute are required to provide each other relevant information and records, along with all other evidence related to the case.
- Examples of the types of Electronically Stored Information (ESI) included are emails, instant messaging chats, documents, accounting databases, CAD/CAM files, Web sites, and any other electronic information that could be relevant evidence in a lawsuit. Also included in ediscovery are "raw data" and "metadata," which forensic investigators can review for hidden evidence.
- The Electronic Discovery Reference Model (EDRM) has provided the foundation for the eDiscovery process since 2005. The first four stages concern the information collection and preservation functions :
  1. **Information governance** : Information governance focuses on ESI management from initial creation through final disposition with the reduction of eDiscovery costs in advance of litigation as the goal.
  2. **Identification** : In this stage, the team identifies the project's technical issues and potential scope to begin to identify relevant evidence. The focus is on locating potential sources of ESI, custodians and locations of discoverable evidence, and the volume of potentially discoverable data.
  3. **Preservation** : In the course of routine business, ESI is frequently deleted, but deleting potentially discoverable information may be spoliation, sometimes a sanctionable offense. Proper preservation of ESI that is discoverable for litigation ensures evidence is not destroyed or altered.
  4. **Collection** : Despite the challenges, it is essential to avoid altering evidence by collecting ESI in a forensically sound manner.
- The remaining stages deal with the data analysis and presentation side of things :
  5. **Processing** : ESI may be converted to formats that are more easily reviewed yet forensically secure. Meanwhile, the native documents can be subject to forensic analysis and preserved.

6. **Review :** Relevant evidence must be available for review by parties while privileged information remains protected against accidental production.
7. **Analysis :** Attorneys must provide context for ESI and its content with their analysis, identifying key custodians, discussions, patterns and subjects.
8. **Production :** ESI must be produced to the right parties in the correct formats, whether it be electronic production or via disks or hard drives.
9. **Presentation :** A relatively small proportion of ESI is ultimately produced in a hearing, deposition or trial and the parties must present this relevant evidence effectively.

University Question

1. *Write a brief note on eDiscovery.* **GTU : Winter-21, Marks 3**

❑❑❑

6 Understanding of Digital Forensic Tools

Syllabus

Quality assurance, Tool validation, Tool selection, Hardware and Software tools.

Contents

6.1 Quality Assurance

- Quality assurance is defined as "a well-documented system of protocols used to assure the accuracy and reliability of analytical results".
- Good QA program will cover a wide array of subjects including peer reviews of reports, evidence handling, case documentation, and training of lab personnel.
- The quality management system is the consolidation of practices and procedures used to ensure the quality of the work and products that the organization produces.
  1. **Administrative review** : All digital forensic examination reports must be administratively reviewed for consistency with agency policy and for editorial correctness.
  2. **Technical review** : At least 10 percent of final digital forensic examination reports must be technically reviewed by another qualified digital forensic examiner (peer reviewed) before the reports are published.
- The reviewing examiner may be from the same or a different organization. The purpose of the technical review is to ensure the following :
  1. The report is clear and understandable.
  2. The procedures performed were adequately documented and forensically sound.
  3. The exam documentation was sufficiently detailed to enable reproduction of the results.
  4. The interpretations and conclusions of the examiner were reasonable, supported by the examination documentation, and scientifically valid.
- In a proficiency test, examiners must demonstrate their competence with mock evidence. There are four types of proficiency tests :
  1. **Open test** : The analyst(s) and technical support personnel are aware they are being tested.
  2. **Blind test** : The analyst(s) and technical support personnel are not aware they are being tested.
  3. **Internal test** : Conducted by the agency itself.
  4. **External test** : Conducted by an agency independent of the agency being tested.

6.2 Tool Validation

GTU : Winter-21

- Tools are used to analyze digital data and prove or disprove criminal activity. It is used in 2 of the 3 phases of computer forensics.

- Acquiring digital data for forensic examination is a critical phase of the forensic process. Forensic personnel will often have only one opportunity to obtain the data, and using untested tools could unintentionally alter the data.
- To the extent possible, organizations should ensure the tools they use to acquire digital evidence are validated to operate as intended and accurately acquire the data. The validation testing may be performed by the organization or other reputable entity (for example, another digital forensic laboratory).
- The organization performing the validation test must document the test, including the requirements that were tested, the expected results, and the actual results of the testing. To comply with this standard, the organization must be able to produce the report if requested.

1. **Documentation** : All the paperwork associated with a specific case is collected into a case file. The case file will contain all of the documentation pertaining to the case, including paperwork generated by the examiner and others.

- Documentation include case submission forms, requests for assistance, examiners' notes, crime scene reports, case reports, copy of the search authority, chain of custody etc.

2. **Forms** : Preprinted forms are widely used in both the field and the lab. Forms ensure all the necessary information is captured in a uniform manner. Forms are used to describe the evidence in detail (make, model, serial number, etc.), document the chain of custody, request an examination, and so on.
3. **Examiner's final report** : The examiner's final report is the formal document that is delivered to prosecutors, investigators, opposing counsel, and so on at or near the end of an investigation.

University Question

1. *Explain tool validation in context of quality assurance.* **GTU : Winter-21, Marks 4**

6.3 Tool Selection

GTU : Winter-21

- The field of computer forensic investigation includes the capture and analysis of digital data to either prove a crime has or has not been committed. The range of crimes can include computer related crime as well as other crimes that have left evidence in digital formats.
- The National Institute of Standards and Technology (NIST) and the National Institute of Justice (NIJ) developed Computer Forensic Tool Testing Project (CFTT) for selecting forensic tools.

- The primary goal of the tool catalog is to provide an easily searchable catalog of forensic tools. This enables practitioners to find tools that meet their specific technical needs. The Catalog provides the ability to search by technical parameters based on specific digital forensics functions, such as disk imaging or deleted file recovery.
- There are two basic types of data that are collected, persistent data and volatile data. Persistent data is that which is stored on a hard drive or another medium and is preserved when the computer is turned off. Volatile data is any data that is stored in memory or exist in transit and will be lost when the computer is turned off. Volatile data might be key evidence, so it is important that if the computer is on at the scene of the crime it remain on. There are a variety of tools used to collect data.
- Tools are used to analyze digital data and prove or disprove criminal activity. It is used in 2 of the 3 phases of computer forensics.
  1. **Acquisition** - Images systems and gathers evidence
  2. **Analysis** - Examines data and recovers deleted content
  3. **Presentation** - Tools not used

Computer Forensic Tools Capabilities

1. Recover deleted files.
2. Find out what external devices have been attached and what users accessed them.
3. Determine what programs ran.
4. Recover web pages.
5. Recover emails and users who read them.
6. Recover chat logs.
7. Determine file servers used.
8. Discover document's hidden history.
9. Recover phone records and SMS text messages from mobile devices.

6.3.1 Hardware and Software Tools

- Types of computer forensics tools :
  1. **Hardware forensic tools :** Range from single-purpose components to complete computer systems and servers.
  2. **Software forensic tools :** There are two types of software forensic tools. Command-line applications and GUI applications are two types. It is commonly used to copy data from a suspect's disk drive to an image file.

- Tasks performed by computer forensics tools :
  1. Acquisition 2. Validation and discrimination 3. Extraction
  4. Reconstruction 5. Reporting

1. **Acquisition :** The acquisition phase is concerned with capturing the state of a digital system for later analysis. This is similar to the collection of physical evidence from a crime scene, e.g., taking photographs, collecting fingerprints, fibres, blood samples, etc. Sub-functions in the acquisition category include Physical data copy, Logical data copy, Data acquisition format, Command-line acquisition, GUI acquisition and Remote acquisition.
2. **Validation and Discrimination :** Ensuring the integrity of data being copied is the validation process. In discrimination of data, which involves sorting and searching through all investigation data. The process of validating data is what allows discrimination of data. The sub-functions of the validation and discrimination function are Hashing, Filtering and Analyzing file headers.
3. **Extraction :** The extraction function is the recovery task in a computing investigation. The sub-functions of extraction are used in investigations are Data viewing, Keyword searching, Decompressing, Carving, Decrypting and Bookmarking.
4. **Reconstruction :** The purpose of having a reconstruction feature in a forensics tool is to re-create a suspect drive to show what happened during a crime or an incident. Another reason for duplicating a suspect drive is to create a copy for other computer investigators, who might need a fully functional copy of the drive so that they can perform their own acquisition, test, and analysis of the evidence. These are the subfunctions of reconstruction : Disk-to-disk copy, Image-to-disk copy, Partition-to-partition copy and Image-to-partition copy.
5. **Reporting :** To complete a forensics disk analysis and examination, you need to create a report. Before Windows forensics tools were available, this process required copying data from a suspect drive and extracting the digital evidence manually. The investigator then copied the evidence to a separate program, such as a word processor, to create a report.

6.3.2 Tools

1. The Sleuth Kit (TSK)

- The Sleuth Kit (TSK) is a library and collection of Unix- and Windows-based tools and utilities to allow for the forensic analysis of computer systems. It allows examination of DOS, BSD, Mac, Sun, GPT partitions and disks.

- It also includes the autopsy forensic browser as a graphical analysis tool and supports integration with SQLite database. It can be run on live Windows systems for incident response.
- With this kit, the user can examine the computer file systems through a non-intrusive approach that is not dependent on the investigated machine operating system to process the file system, deleted and hidden from files DOS, BSD, Mac, Sun and Linux partitions.
- The results generated by Sleuth Kit tools are used by another tool. The autopsy forensic browser which presents such details as image integrity, keyword searches and other automatized operations about the investigated partition through a graphical interface.
- The Sleuth Kit was written in C and Perl and uses an aspect of the TCT code.

2. The Coroner's Toolkit (TCT)

- The TCT tools do not recognize NTFS, FAT or EXT3 partitions, making them of little use when performing forensic investigations in machines with Microsoft Windows and/or Linux operating systems with EXT3 file systems.
- Investigating Windows (FAT) partitions with TCT is only possible with a conversion to EXT2 format, demanding alterations on the i-nodes table of the investigated partition. This activity is not always possible with data analysis.

3. FTK TOOL

- FTK can analyze data from several sources, including image files from other vendors. FTK also produces a case log file, where you can maintain a detailed log of all activities during the examination such as keyword searches and data extractions.
- FTK provides two options for searching for keywords. One option is an indexed search, which catalogs all words on the evidence drive so that FTK can find them quickly. The other option is live search, which can locate items such as text hidden in unallocated space that might not turn up in an indexed search.

4. Maresware

- Maresware computer forensics software provides an essential set of tools for investigating computer records and securing private information. It is highly flexible to meet the needs of all types of investigators including : law enforcement, intelligence agency, private investigator, corporate security officers and human resources personnel.
- It is used within a forensic paradigm, the software enables discovery of evidence for use in criminal or civil legal proceedings. Internal investigators can develop

documentation to support disciplinary actions, yet do so non-invasively, to preserve evidence that could end up in court.

Functions of Maresware

a. Discovery of "hidden" files(such as NTFS Alternate Data Streams)
b. For incident response purposes
c. Evaluation of timelines
d. Key word searching
e. Files verification
f. Drive wiping for information privacy and security
g. File reformatting
h. Documenting all the examiner's steps and procedures

5. ProDiscover Basic

- ProDiscover basic from technology pathways is a forensics data analysis tool. It can be used to acquire and analyze data from several different file systems such as Microsoft FAT and NTFS, Linux Ext2 and Ext3 and other UNIX file system.

University Question

1. *Explain various tool selection methods in context of digital forensic.* **GTU : Winter-21, Marks 4**

❑❑❑