What is forensic science?

→ Forensic Science is an application of science, to resolve legal and crime related problems. In forensic sciences, the law and science are integrated together.

## Define Digital Forensic:

→ The application of computer science and investigate procedure, for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation of mathematics, use of validated tools, repeatedly reporting and possible expert presentation.

## Digital Forensics Process:

→ Digital forensics process can be bottled down to series of stages. These phases are as follows:

1. Proper search authority
2. Chain of custody
3. Imaging and Hashing function
4. Validation with mathematics
5. Validated tools
6. Repeatability
7. Analysis / Test
8. Linking & some activity with some specific user account.
9. Reporting
10. Possible expert presentation.

## Uses of Digital Forensics:

Criminal Investigations : (BTK Killer)

→ Bind, Torture, Kill (BTK Killer)

→ Dennis Rader

→ Murdered 10 people in Kansas (1974 to 1991)

→ Silence Broken : Wichita → Eagle Newspaper (19/03/2004)

↳ "1986, Responsible for killing a Young mother"

- Secret code: 'Rex, it will be OK.'
- Floppy file: "Test A.rtf" [.rtf → rich text file]
    - Date created : 10/02/2005
    - Date modified : 14/02/2005
    - Title : Christ Leutheran Church
    - Last saved By : Dennis
- Capture Date : 25/02/2005 (Arrested)
- Published on : Witchita Eagle Newspaper

**Civil Litigations: (e-discovery)**

**Intelligence: (Moussaoui K911)**

- Zacarias Moussaoui
- Arrested By: INS agents in Eagan, Minnesota
- pilotz123@hotmail.com
- hotmail
    - provided by microsoft like gmail and yahoo
    - Basic subscriber information needed only.
- IP address referred to "PC11" at University of Oklahoma

**Administrative Matters: (SEC)**

SEC → Security Enchange Commission.

**e-Discovery:**

e-Discovery stands for electronic discovery. It refers to any process in which data is located, secured and searched with an intend of using it as an evidence, in a civil or criminal legal case.

Devices and Elements that are applied to Digital Forensics:

Laptop
Desktop
Hard-disk
Pendrive
Mobile Devices
Private Clouds
Image
Audio
Video
Messages
Word
Powerpoint
Excel
Text
Document

Breakdown of Digital Forensics Process:

a) Search Authority:

1. To initiate a digital forensic investigation we need a proper search authority related document.
2. Search authority related document is required for collecting the digital evidence.
3. Without search authority related document, we are not allowed to investigate. If we investigate without a proper search authority related document, all the evidence which we collected are suppressed and not being considered as valid document.
4. For criminal investigation, search authority related document is warrant, issued by the court.
5. For any civil investigation, search authority related document are issued by the public procecution and the side of to be accused.

b) Chain of custody:

1. The chain of custody is issued for every digital evidence in order to maintain integrity.
2. The chain of custody is documented via forms, reports, notes and marking the actual evidence item.
3. Each time of analysis, if an item change, it should be recorded.

c) Imaging and Hashing:

1. After collecting a digital evidence, experts avoid to work on the original evidence. Rather they prefer to make a clone of the evidence. In order to preapare the clone of the evidence and exact copy of every bit of that media is done. This copying is knowns as, "Bitstring Copy". This process is called Imaging.

2. Hashing is a mathematical process via an algorithm, that produces an unique value, that is essentially the digital fingerprint, DNA of a particular file, piece of media.

d) Validated Tools:

1. Forensics tools, next to be validated or tested before they are used. So that we can ensure that this tools are capable of giving us correct results and accurate results.

2. Newly collected tools and updated tools, both need to be validated.

e) Repeatability:

1. The results of the forensics examination, should be able to be duplicated in the process, so that the separate examiner can repeat the process using same evidence, same process and same tools and come up with same results.

2. Quality assurance is a procedure and practice.

3. In the digital forensics process, which will help us to give the ~~geo~~ guarantee of accuracy based on findings.

4. Quality assurance addresses multiple issues, skill and training of examiner, security of evidence, reliability of the tools and processing the evidence in many more.

f) Analysis :

1. Linking some activity with some specific user account.
2. Determine whether any USB device is connected to your laptop or PC or not.
3. Breaking encryption.
4. Identify relationship or connection between individuals.
5. Identify the websites which has already been visited.
6. Determining whether certain files are loaded or downloaded.
7. During analysis process we recover the data.

g) Reporting :

1. In almost every context where digital forensic is used, some type of report needs to be generated.
2. Reports maybe of different forms or format.
3. The length, form, format and description of the report need to be defined or specified by the higher authority
4. Many forensics tools are used to generated reports. As we process a case, we are able to select specific artifacts, files, to be included on the report..
5. One major issue with report generation is they are often very technical. As report needs to presented before judge and jury who may not be a technical person to understand the report, Hence convincing a non technical person about a technical report is not an easy task.
6. A report should be precise, user friendly and shouldn't be stand alone. It should include abstract (zest), summary, list of items, evidence, the tools to perform the analysis finding and conclusion.

## h) Possible expect Presentation:

1. The pinacle of the forensics proces is the presentation of the findings to a judge or jury.

## Locard's Enchange Principle:

Locard's Enchang Principle says that in the physical world, when perpetraptors enter or leave a crime scene, they will leave something behind and take something with them.

Ex: DNA, latent prints, hair and fibre

In Digital Forensics: (Example)

Registry Keys and Log files → Hair and fiber

## Scientific Methods:

1. Scientific working on digital evidence
2. American academy of forensic science.
3. American society of crime labrotary directors
4. National institute of students and technology.
5. American society for testing materials.
6. Indian School of Ethical Hacking.