Chap 4 : Digital Evidence

4.1: Digital Evidences

- Definition of digital evidences
- Best Evidence Rule
- Original Evidence

Evidence

Any information that can be confident or trusted and **can prove something related to a case** in trial that is, indicating that a certain substance or condition is present.

Relevant Evidence

An information which has a positive impact on the action occurred, such as the information **supporting an incident**.

Definition of digital evidences

- Digital evidence is defined as **information and data of value to an investigation that is stored on, received or transmitted by an electronic device**

- This **evidence can be acquired when electronic devices are seized and secured for examination.**

- Digital evidence:
  - Is latent (hidden), like fingerprints or DNA evidence
  - Can be altered, damaged or destroyed with little effort
  - Can be time sensitive

“data or information that exists in digital format, that 'can prove' or 'reveal the truth' about a crime and can be relied upon and used in a court of law.”

- **Three basic forensic categories** of devices where evidence can be found:
  - Internet-based
  - stand-alone computers or devices, and
  - mobile devices.

- **Forms of Digital evidence**:
  - Email
  - Office files
  - Deleted files
  - Compressed files
  - Recycle bin
  - Web History
  - Cache files
  - Cookies etc.

Why and when is digital evidence used?

- Digital evidence may come into play in any **serious criminal investigation such as murder, rape, stalking, car-jacking, child abuse or exploitation, extortion, gambling, piracy, property crimes and terrorism**.

How It’s Done

- **Evidence that May be Gathered Digitally**:
  - **Computer documents, emails, text and instant messages, transactions, images and Internet histories are examples of information** that can be gathered from electronic devices and used very effectively as evidence.

- For example, **mobile devices use online-based based backup systems, also known as the ‘cloud’, that provide forensic investigators with access to text messages and pictures taken from a particular phone.** These systems keep an average of 1,000–1,500 or more of the last text messages sent to and received from that phone.

- In addition, **many mobile devices store information about the locations where the device travelled and when it was there. To gain this knowledge, investigators can access an average of the last 200 cell locations accessed by a mobile device**.

- **Satellite navigation systems and satellite radios in cars can provide similar information**.

- Even **photos posted to social media such as Facebook may contain location information. Photos taken with a Global Positioning System (GPS)-enabled device contain file data that shows when and exactly where a photo was taken.**

- By **gaining a access for a particular** mobile device account, investigators can collect a great deal of history related to a device and the person using it.

Who Conducts the Analysis

“Digital evidence should be examined only by those trained specifically for that purpose.”

Certified Digital Media Examiners are investigators who have the education, training and experience to properly exploit this sensitive evidence.

How Digital Devices are Collected

- **On the scene**
- **Seizing Mobile Devices**
  - **Devices should be turned off immediately and batteries needs to be put off**
  - If the device **cannot be turned off**, then it **must be isolated from its cell tower by placing it in a Faraday bag or other blocking material**, set to airplane mode, or the Wi-Fi, Bluetooth or other communications system must be disabled or removed, if possible.

- In **emergency** or life threatening situations, **information from the phone can be removed and saved at the scene**, but great care must be taken in the documentation of the action and the preservation of the data.

- When sending digital devices to the laboratory, the investigator must indicate the type of information being sought, for instance phone numbers and call histories from a cell phone, emails, documents and messages from a computer, or images on a tablet.

- **Seizing Stand Alone Computers and Equipment:**

To prevent the alteration of digital evidence during collection, first responders should first document any activity on the computer, components, or devices by taking a photograph and recording any information on the screen.

- Responders may move a mouse (without pressing buttons or moving the wheel) to determine if something is on the screen. If the computer is on, calling on a computer forensic expert is highly recommended as connections to criminal activity may be lost by turning off the computer.

- If a computer is on but is running destructive software (formatting, deleting, removing or wiping information), power to the computer should be disconnected immediately to preserve whatever is left on the machine.

- Office environments provide a **challenging collection situation** due to networking, potential loss of evidence and liabilities to the agency outside of the criminal investigation. For instance, **if a server is turned off during seizure that is providing a service to outside customers, the loss of service to the customer may be very damaging.**

- In addition, office equipment that could contain evidence such as copiers, scanners, security cameras, facsimile machines, pagers and caller ID units should be collected.

How and Where the Analysis is Performed

- Once the digital evidence has been sent to the laboratory, a qualified analyst will take the following steps to retrieve and analyse data:

Prevent contamination

- Prior to analysing digital evidence,
  - **an image or work copy of the original storage device is created.**
  - When collecting data from a suspect device, the copy must be stored on another form of media to keep the original data.
  - Analysts must use ‘clean’ storage media to prevent contamination—or the introduction of data from another source.

Isolate Wireless Devices

- **Cell phones and other wireless devices should be initially examined in an isolation chamber, if available.** This prevents connection to any networks and keeps evidence as clean as possible.

Install write-blocking software

- To prevent any change to the data on the device or media, the analyst will install a block on the working copy so that data may be viewed but nothing can be changed or added.

Select extraction methods

- Once the working copy is created, the analyst will determine the make and model of the device and select extraction software designed to most completely 'parse the data,' or view its contents.

Submit device or original media for traditional evidence examination

- When the data has been removed, the device is sent back into evidence. There may be DNA, trace, fingerprint, or other evidence that may be obtained from it and the digital analyst can now work without it.

Proceed with investigation

- At this point, the analyst will use the selected software to view data. The analyst will be able to see all the files on the drive, can see if areas are hidden and may even be able to restore organization of files allowing hidden areas to be viewed.

- Deleted files are also visible, as long as they haven’t been over-written by new data. Partially deleted files can be of value as well.

- Files on a computer or other device are not the only evidence that can be gathered. The **analyst may have to work beyond the hardware to find evidence that resides on the Internet including chat rooms, instant messaging, websites and other networks of participants or information**.
- By using the **system of Internet addresses, email header information, time stamps on messaging and other encrypted data, the analyst can piece together strings of interactions that provide a picture of activity**.

Best Evidence Rule

- In the U.S., Article X, Rule 1002, states:

“**An original writing, recording, or photograph is required in order to prove its content** unless these rules or a federal statute provides otherwise.”

- This rule applies to
  - **written evidence**, such as a lease;
  - to **audio recordings**, such as voicemail messages;
  - **video recordings**, such as wedding videos or cell phone videos and ;
  - **photographs**
  - **Any type of evidence which is able to prove itself.**

- For instance, **the amount of rent a tenant has agreed to pay can be proven by the lease**.
- Just what the lease says – should **there be a disagreement – can only be proven by the original**, which is the *best evidence*.

A rule of evidence that holds an original document, photograph, recording, or other piece of evidence is required to prove.

History of the Best Evidence Rule

- In 18th century England, **Philip Yorke – a prominent lawyer of the time** – made the argument that **no evidence should be admissible in court, unless it is ”the best that the nature of the case will allow.”**
- The rule **followed that secondary evidence would not be admitted if the original evidence existed.**
- This made a **great deal of sense at the time, as copies of documents were made by hand, often by clerks, though even people might have hand-copied a document.**
- In such a case, **there may very well have been significant error, nor could fraud be written off**.

Best Evidence Rule Misunderstood

- In some cases, the best evidence rule has been misunderstood.

- **This rule does not mean that copies of documents or other evidence can never be used in court – only that, if the actual contents of that evidence is in question, the best evidence to prove it is the original.**

Rules of Digital Evidence

- There are five rules of collecting electronic evidence. These relate to five properties that evidence must have to be useful.
  - Admissible
  - Authentic
  - Complete
  - Reliable
  - Believable

Admissible

- The evidence must be able to be used in court.

Accepted + Valid

- Failure to comply with this rule is equivalent to not collecting the evidence in the first place.

Authentic

- If you can’t tie the evidence positively with the incident, you can’t use it to prove anything.
- You **must be able to show that the evidence relates to the incident in a relevant way**.

Complete

- **It’s not enough to collect evidence that just shows one perspective of the incident. Not only should you collect evidence that can prove the attacker’s actions, but also evidence that could prove their innocence.**
- For instance, if you can show the attacker was logged in at the time of the incident, you also need to show who else was logged in, and why you think they didn’t do it.
- It is an important part of proving a case.

Reliable

- The evidence you collect must be reliable.
- Your evidence collection and analysis procedures must not cast doubt on the evidences authenticity and veracity.

Do’s and Dont’s based on above rules

- Minimize handling/corruption of original data
- Account for any changes and keep detailed logs of your actions
- Comply with the five rules of evidence
- Do not exceed your knowledge
- Follow your local security policy
- Capture as accurate an image of the system as possible
- Ensure your actions are repeatable
- Work fast
- Proceed from volatile to persistent evidence
- Don’t shutdown before collecting evidence
- Don’t run any programs on the affected system

Minimize Handling/Corruption of Original Data

- Once you’ve created **a master copy of the original data, don’t touch it** or the original **itself—always handle secondary copies**.
- Any changes made to the originals will affect the outcomes of any analysis later done to copies.
- You should **make sure you don’t run any programs that modify the access times** of all files.
- You should **also remove any external avenues for change and, in general, analyze the evidence after it has been collected.**

Account for Any Changes and Keep Detailed Logs of Your Actions

- Sometimes **evidence alteration is unavoidable**.
- In these cases, it is absolutely **essential that the nature, extent, and reasons for the changes be documented**.
- Any **changes** at all **should be accounted** for—not only **data alteration** but **also physical alteration of the originals** (i.e., the removal of hardware components).

Comply with the Five Rules of Evidence

- **The five rules are there for a reason**. If you don’t follow them, you are probably wasting your time and money.
- **Following these rules is essential to guaranteeing successful evidence collection**.

Do Not Exceed Your Knowledge

- **If you don't understand what you are doing, you can't account for any changes you make and you can't describe what exactly you did.**
- If you ever find yourself **"out of your depth,"** either go and learn more before continuing (if time is available) or find someone who knows the territory.
- **Never soldier on regardless—you're just damaging your case.**

Follow Your Local Security Policy

- **If you fail to comply with your company's security policy, you may find yourself with some difficulties.**
- Not only may you end up in trouble (and **possibly fired** if you've done something really against policy), but also you may not be able to use the evidence you've gathered.
- If in doubt, talk to those who know.

Capture as Accurate an Image of the System as Possible

- Capturing an accurate image of the system is related **to minimizing the handling or corruption of original data—differences between the original system and the master copy count as a change to the data**.
- **You must be able to account for the differences.**

Ensure That Your Actions Are Repeatable

- No one is going to believe you if they can't replicate your actions and reach the same results.
- This also means that your plan of action shouldn't be based on trial-and-error.

Work Fast

- **The faster you work, the less likely the data is going to change.**
- Volatile evidence may vanish entirely if you don’t collect it in time. This is not to say that you should rush—you must still be collecting accurate data.
- If **multiple systems** are involved, **work on them in parallel** (a team of investigators would be handy here), but each single system should still be worked on methodically. **Automation of certain tasks makes collection proceed even faster.**

Proceed from Volatile to Persistent Evidence

- Some electronic evidence is more volatile than others are.
- **Because of this, you should always try to collect the most volatile evidence first.**

Don’t Shutdown before Collecting Evidence

- **You should never, ever shutdown a system before you collect the evidence.**
- Not only do you lose any volatile evidence but also the attacker may have trojaned (trojan horse) the startup and shutdown scripts, Plug-and-Play devices may alter the system configuration and temporary file systems may be wiped out.
- **Rebooting** is even worse and should be avoided at all costs. As a general rule, until the compromised disk is finished with and restored, it should never be used as a boot disk.

Don’t Run Any Programs on the Affected System

- Because the attacker may have left trojaned programs and libraries on the system, you may inadvertently trigger **something that could change or destroy the evidence you’re looking for.**
- Any programs you use should be on read-only media (such as a CD-ROM or a write-protected floppy disk), and should be statically linked.

Types Of Digital Evidence

- There are different types of digital evidence offering unique types of information.

- They are broadly categorized into two groups:
  - Evidence from data at rest (**obtained from any device that stores digital information**).
  - Data intercepted while being transmitted (**interception of data transmission/communications**).

Types of Evidence

Direct Evidence:

- This relies directly on the sense or perception of witnesses actually testifying or being presented.
- For example: Eyewitness testimony , Videotape or audio tape

Circumstantial Evidence:

- This is evidence or circumstances that require the trier of fact to infer that something happened.
- For example:
  - Fingerprints at the crime scene
  - Blood and DNA evidence

Testimonial Evidence

- Spoken by the spectator under the oath, or written evidence given under the oath by an official declaration that is affidavit.
- This is the common forms of evidence in the system.

Physical Evidence

- In the form of a physical object
- E.g., fingerprints, blood, the murder weapon, etc.
- Also known as Substantial evidence.

Documentary Evidence

- any proof that can be presented in writing (contracts, wills, invoices, etc.)
- Including writings, photographs, etc.

Exculpatory Evidence:

- Typically used in criminal cases, this type of evidence is that which **favours the defendant**, either partially or totally removing their guilt in the case.
- In the United States, if the prosecutor or police have found evidence, it is their duty to disclose it to the defendant.
- Failure to do so can result in the case being dismissed.
- **Also known Explainable evidence**

Demonstrative Evidence

- **Representation of an object which is common form of proof.**
- Eg: X-rays,maps,charts and sketches; not really evidence in and of themselves- just visual aids for the trier of fact
- Also known as illustrative evidence

Characteristics of Digital Evidence

- Helps and challenge investigators during an investigation.

- The main goal in any investigation are
  - to **follow the trails that offenders leave during the commission of crime**
  - To **tie the victim and crime scene**.
  - Although **victim may identify a suspect, tangible evidence of an individual involvement is usually more reliable**.
  - **Forensic analysts are employed to uncover** compelling **links** between the **offender, victim and crime scene.**

- Locard’s Exchange Principle
- Digital stream of bits

Locard’s Exchange Principle

- In forensic science, **Locard's principle** holds that **the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence**.
- Dr. Locard was a pioneer in forensic science who became known as the **Sherlock Holmes of France**.
- He formulated the basic principle of forensic science as: "**Every contact leaves a trace**".

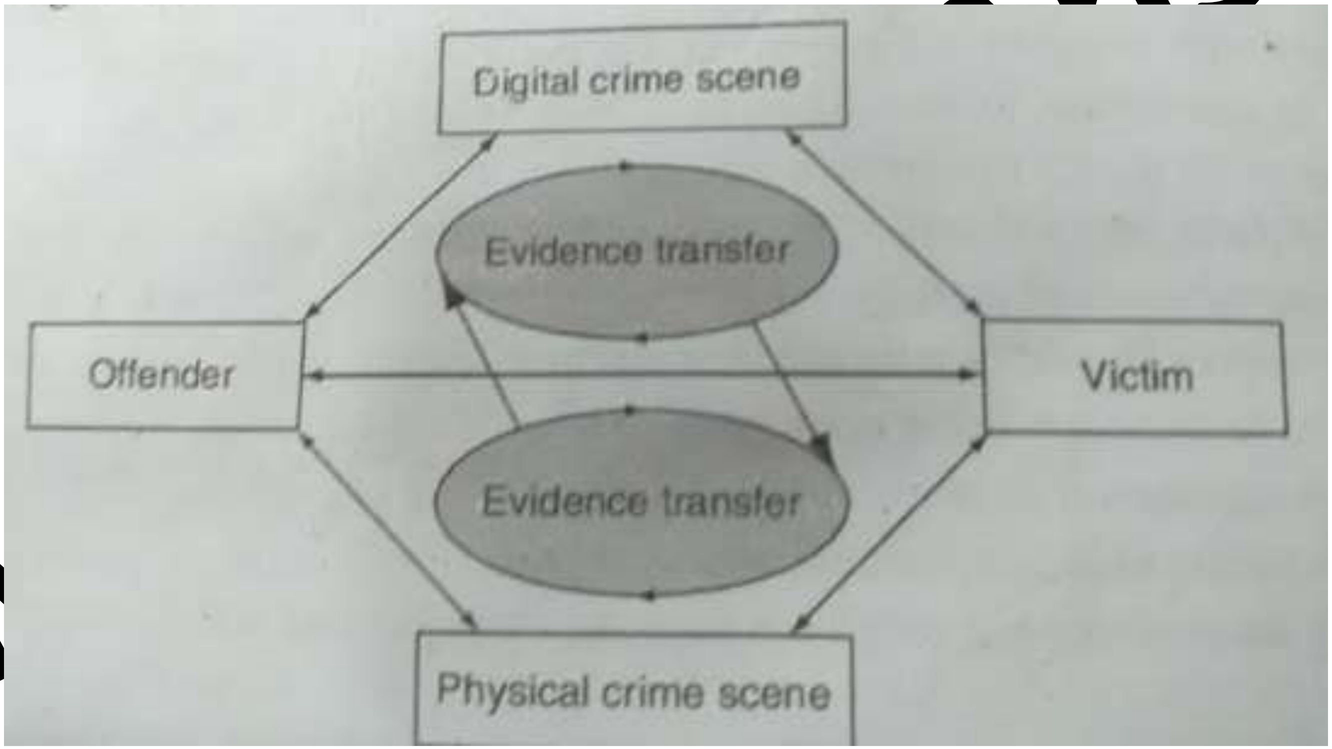
"**Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him.** Not only his **fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects**. All of these and more, **bear mute witness against him**. This is evidence that does not forget. It is not confused by the excitement of the moment. **It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value."**

Locard's Exchange Principle

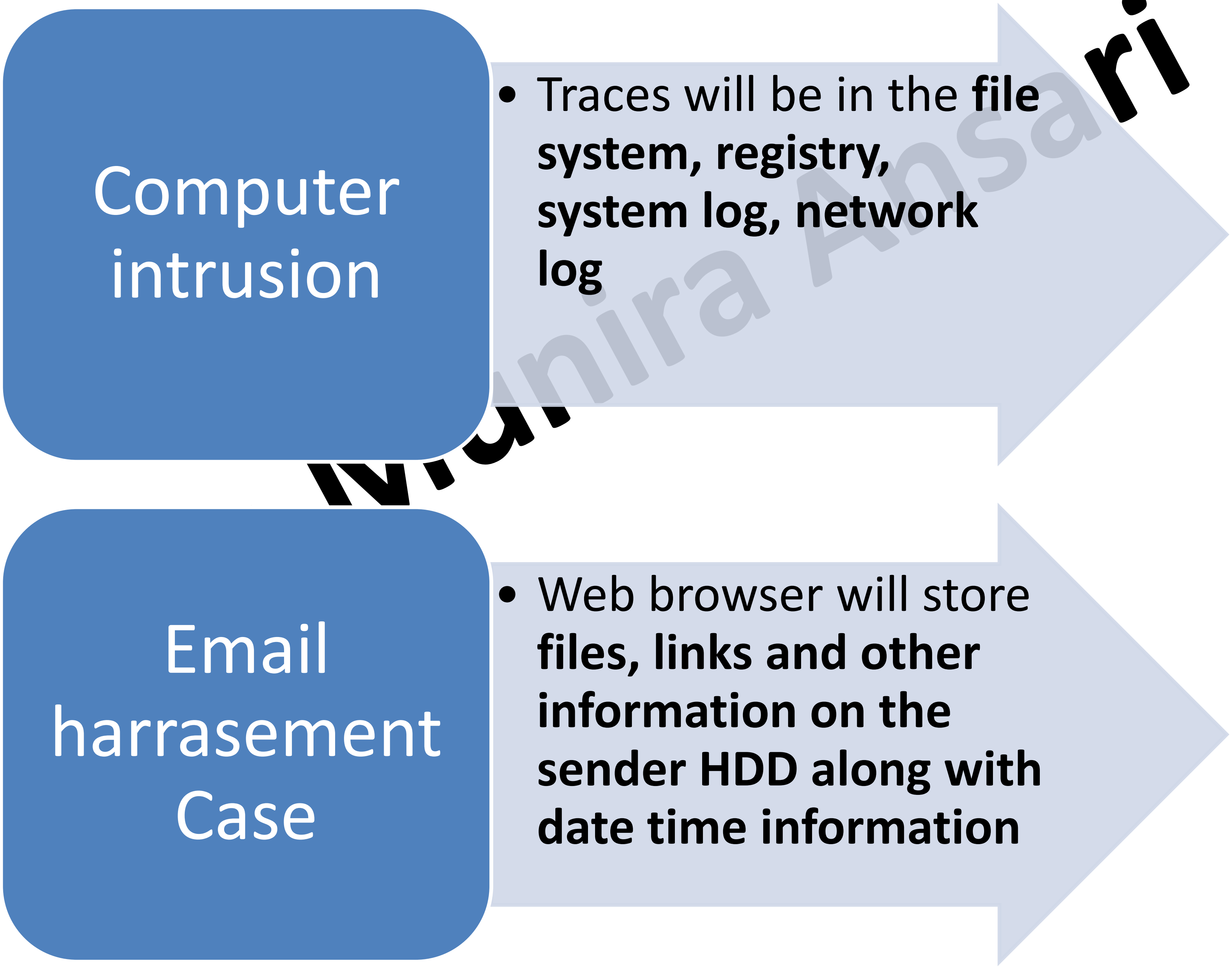
"Every Contact Leaves a Trace"

The value of trace (or contact) forensic evidence was first recognized by Edmund Locard in 1910. He was the director of the very first crime laboratory in existence, located in Lyon, France.

The Locard's Exchange Principle states that "with contact between two items, there will be an exchange."


Digital crime scene
Evidence transfer
Offender
Victim
Evidence transfer
Physical crime scene

- As per locard principle **contact between two items will result in an exchange.**
- This principle applies to **any contact at crime scene including between an offender and victim,**
- **Between a person with a weapon** , and **between people and the crime scene itself**.
- **This transfer occurs in both the physical and digital area**
- And can provide links between them.



Computer intrusion

- Traces will be in the **file system, registry, system log, network log**

Email harrasement Case

- Web browser will store **files, links and other information on the sender HDD along with date time information**

Digital Stream of Bits

- **Where digital evidence will be referred as bag of bits.**
- Which can be **arranged in array to display the information.**
- **The information are not able to make scene ,tools are required to show these structure logically so that it is readable**.

Challenges in evidence handling

- **Authentication of Evidence:**
  - The **evidence** that are collected by any person/investigator **should be collected using authenticate methods** and **techniques** because during court proceedings these will **become major** evidences **to prove the crime**.
  - Evidence collected by any person **should meet the demand of authentication**
  - **Must have some sort of internal documentation** that **records** the manner of collected **information**.

- **Chain of Custody:**
  - Forensic Link
  - **It indicates the collection, sequence of control, transfer, and analysis in chronological order.**
  - It also documents each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer

What Is the Procedure to Establish the Chain of Custody?

- **Save the original materials:**

  You should **always work on copies of the digital evidence** as opposed to the original.

  This ensures that you are able to compare your work products to the original that you preserved unmodified.

- **Take photos of physical evidence:**

  Photos of physical (electronic) evidence establish the chain of custody and make it more authentic.

- **Take screenshots of digital evidence content:**

  In cases where the evidence is intangible, taking screenshots is an effective way of establishing the chain of custody.

- **Document date, time, and any other information of receipt:**

  Recording the timestamps of whoever has had the evidence allows investigators to build a reliable timeline of where the evidence was prior to being obtained. In the event that there is a hole in the timeline, further investigation may be necessary.

- **Inject a bit-for-bit clone of digital evidence content into our forensic computers:**

  This ensures that we obtain a complete duplicate of the digital evidence in question.

- **Perform a hash test analysis to further authenticate the working clone.:**

  Performing a hash test ensures that the data we obtain from the previous bit-by-bit copy procedure is not corrupt and reflects the true nature of the original evidence. If this is not the case, then the forensic analysis may be flawed and may result in problems, thus rendering the copy non-authentic.

What Considerations Are Involved with Digital Evidence?

- 1. Never work with the original evidence to develop procedures
- 2. Use clean collecting media:
- 3. Document any extra scope:

During the course of an examination, information of evidentiary value may be found that is beyond the scope of the current legal authority.

- A comprehensive report must contain the following sections:
  - 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

- 4.**Consider safety of personnel at the scene.**

  It is advisable to always ensure the scene is properly secured before and during the search.

- In some cases, the examiner may only have the opportunity to do the following while onsite:
  - Identify the number and type of computers.
  - Determine if a network is present.
  - Interview the system administrator and users
  - Identify and document the types and volume of media, including removable media.
  - Document the location from which the media was removed.
  - Identify offsite storage areas and/or remote computing locations.
  - Identify proprietary software.
  - Determine the operating system in question.

- **Evidence Validation:**

  The challenge is to ensure that providing or obtaining the data that you have collected is similar to the data provided or presented in court.

- To meet the challenge of validation, it is necessary to ensure that the original media matches the forensic duplication

Volatile Evidence

- To determine what evidence to collect first, you should draw up an Order of Volatility—a list of evidence sources ordered by relative volatility.

- An example an Order of Volatility would be:

1. Registers and cache
2. Routing tables
3. Arp cache
4. Process table
5. Kernel statistics and modules
6. Main memory
7. Temporary file systems
8. Secondary memory
9. Router configuration
10. Network topology