4.Digital evidence

The field of computer security includes events that provide a successful courtroom experience, which are both worthwhile and satisfactory. Investigation of a computer security incident leads to legal proceeding, such as court proceeding, where the digital evidence and documents obtained are likely used as exhibits in the trial.

To meet the requirements of the judging body and to withstand or face any challenges, it is essential to follow the evidence-handling procedure. Also, it is necessary to ensure that the evidence-handling procedures chosen are not difficult to implement at your organization as this can sometimes become an overhead for an organization.

While investigating a computer security incident, we are sometimes unsure and indecisive whether an item(viz. a chip, floppy disk, etc)should be considered as an evidence or an attachment or an addendum.

Digital devices are everywhere in today's world, helping people communicate locally and globally with ease. Most people immediately think of computers, cell phones and the Internet as the only sources for digital evidence, but any piece of technology that processes information can be used in a criminal way. For example, hand-held games can carry encoded messages between criminals and even newer household appliances, such as a refrigerator with a built-in TV, could be used to store, view and share illegal images. The important thing to know is that responders need to be able to recognize and properly seize potential digital and digital files, Digital evidence.

Digital Evidences: (Electronic 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 1s
- **Relevant Evidence:** An information which has a positive impact on the action occurred, such as the information supporting an incident.
- **Digital Evidence:** Digital evidence is any information or data that can be confident or trusted and can prove something related to a case trial, that is, indicating that a certain substance or condition is present. It is safe to use to use such information as evidence during an investigation.

4.1.1 **Digital evidence** or **Electronic evidence** is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required.

Digital evidence is also 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
- Crosses jurisdictional borders quickly and easily
- Can be altered, damaged or destroyed with little effort
- Can be time sensitive

There are many sources of digital evidence; the topic is divided into three major forensic categories of devices where evidence can be found: Internet-based, stand-alone computers or devices, and mobile devices. These areas tend to have different evidence-gathering processes,

tools and concerns, and different types of crimes tend to lend themselves to one device or the other.

Some of the popular electronic devices which are potential digital evidence are: HDD, CD/DVD media, backup tapes, USB drive, biometric scanner, digital camera, smart phone, smart card, PDA, etc.

Forms of digital evidence: Text message, emails, pictures, videos and internet searches are most common types of Digital evidences.

The digital evidence are used to establish a credible link between the attacker, victim, and the crime scene. Some of the information stored in the victim's system can be potential digital evidence, are IP address, system log-in & remote log-in details, browsing history, log files, emails, images, etc.

Digital Evidences may be in the form:

- Email Messages (may be deleted one also)
- Office file
- Deleted files of all kinds
- Encrypted file
- Compressed files
- Temp files
- Recycle Bin
- Web History
- Cache files
- Cookies
- Registry
- Unallocated Space
- Slack Space
- Web/E-Mail server access Logs
- Domain access Logs

4.1.2 Best Evidence Rule:

The original or true writing or recording must be confessed in court to prove its contents without any expectations. An original copy of the document is considered as superior evidence.

One of the rules states that if evidence is readable by sight or reflects the data accurately, such as any printout or data stored in a computer or similar devices or any other output, it is considered as "original".

It states that multiple copies of electronic files may be a part of the "original" or equivalent to the "original". The collected electronic evidence is mostly transferred to different media. Hence, many computer security professionals are dependent on this rule.

Best Evidence: The most complete copy or a copy which includes all necessary parts of evidence, which is closely related to the original evidence.
Example-A client has a copy of the original evidence media.

The "Best Evidence Rule" says that an original writing must be offered as evidence unless it is unavailable, in which case other evidence, like copies, notes, or other testimony can be used. Since the rules concerning evidence on a computer are fairly reasonable (what you can see on

the monitor is what the computer contains, computer printouts are best evidence) computer records and records obtained from a computer are best evidence.

4.1.3 Original Evidence:

The procedure adopted to deal with a situation or case takes it outside the control of the client/victim. A case with proper diligence or a case with persistence work will end up in a judicial proceeding, and we will handle the evidences accordingly.

For this purpose original evidence as the truth or real (original) copy of the evidence media which is given by victim/client.

We define best incidence as the most complete copy, which includes all the necessary parts of evidence that are closely related to the original evidence. It is also called as duplication of the evidence media. There should be an evidence protector which will store either the best evidence or original evidence for every investigation in the evidence safe.

4.2 Rules of Digital Evidence:

rule of evidence is also called as Law of evidence. It surrounds the rules and legal principles but govern all the proof of facts. This rule helps us to determine what evidence must or must at be considered by a trier of fact. The rule of evidence is also concerned with the amount, quantity and type of proof which helps us to prove in litigation. The rules may vary according to the criminal court, civil court etc.

The rule must be:

- **Admissible**: The evidence must be usable in the court.
- **Authentic**: The evidence should act positively to an incident.
- **Complete**: A proof that covers all perspectives.
- **Reliable**: There ought to be no doubt about the reality of the specialist's decision.
- **Believable**: The evidence should be understandable and believable to the jury.

Rule 103: Rule of evidence

1. Maintaining a claim of error.
2. No renewal of objection or proof.
3. Aim an offer of proof.
4. Plain error taken as notice.

Evidence collection should also be performed to ensure that it will withstand legal proceedings. Key criteria for handling such evidence are as outlined as follows:

1. The proper protocol should be followed for acquisition of the evidence irrespective of whether it physical or digital. Gentle handling should be exercised for those situations where the device may be damaged (e.g. Dropped or wet).
2. Special handling may be required for some situations. For example, when the device is actively destroying data through disk formatting, it may need to be shut down immediately to preserve the evidence. On the other hand, in some situations, it would not be appropriate to shut down the device so that the digital forensics expert can examine the device's temporary memory.
3. All artifacts, physical and/or digital should be collected, retained and transferred using a preserved chain of custody.
4. All materials should be date and time stamped, identifying who collected the evidence and the location it is being transported to after initial collection.
5. Proper logs should be maintained when transferring possession.
6. When storing evidence, suitable access controls should be implemented and tracked to certify the evidence has only been accessed by authorized individual.

4.3 Characteristics of Digital Evidence:

Characteristics of digital evidences can help and challenge investigators during investigation. The main goals in any investigation are to follow the trails that offenders le during the commission of a crime and to tie perpetrators to the victims and crime scene Although witnesses may identify a suspect, tangible evidence of an individual's involvement is usually more compelling and reliable. Forensic analysts are employed compelling links between the offender, victim, and crime scene.

1. Locard's Exchange Principle:

According to Edmond Locard's principle, when two items make contact, there will be an interchange. The Locard principle is often cited in forensic sciences and is relevant in digital forensics investigations.

When an incident takes place, a criminal will leave a hint evidence at the scene and remove a hint evidence from the scene. This alteration is known as the Locard exchange principle Many methods have been suggested in conventional forensic sciences to strongly prosecute criminals. Techniques used consists of blood analysis, DNA matching and fingerprint verification. These techniques are used to certify the existence of a suspected person at a physical scene. Based on this principle, Culley suggests that where there is a communication with a computer system, clues will be left.

According to Locard's Exchange Principle, contact between two items will result in an exchange. This principle applies to any contact at a crime scene, including between an offender and victim, between a person with a weapon, and between people and the crime scene itself. In short, there will always be evidence of the interaction, although in some cases it may not be detected easily (note that absence of evidence is not evidence of absence). This transfer occurs in both the physical and digital realms and can provide links between them as depicted in Figure 1. In the physical world, an offender might inadvertently leave fingerprints or hair at the scene and take a fiber from the scene. For instance, in a homicide case the offender may attempt to misdirect investigators by creating a suicide note on the victim's computer, and in the process leave fingerprints on the keyboard. With one such piece of evidence, investigators can demonstrate the strong possibility that the offender was at the crime scene. With two pieces of evidence the link between the offender and crime scene becomes stronger and easier to demonstrate. Digital evidence can reveal communications between suspects and the victim, online activities at key times, and other information that provides a digital dimension to the investigation.

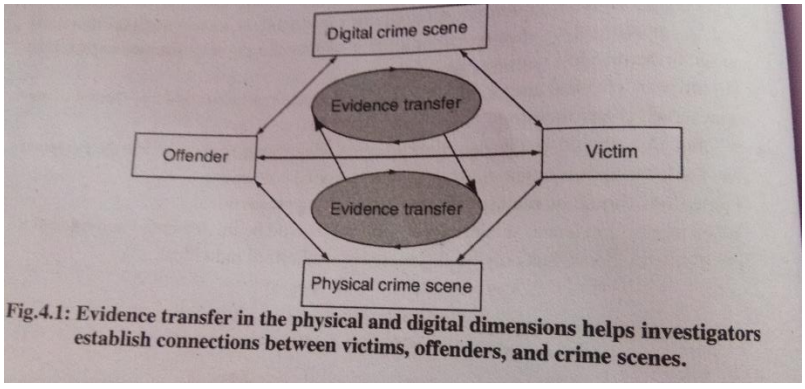

Fig.4.1: Evidence transfer in the physical and digital dimensions helps investigators establish connections between victims, offenders, and crime scenes.

In computer intrusions, the attackers will leave multiple traces of their presence throughout the environment, including in the file systems, registry, system logs, and network-level logs. Furthermore, the attackers could transfer elements of the crime scene back with them, such as stolen user passwords or PII in a file or database, Such evidence can be useful a link an individual to an intrusion.

In an e-mail harassment case, the act of sending threatening messages via a Web-based e-mail service such as Hotmail can leave a number of traces. The Web browser used to send messages will store fi les, links, and other information on the sender's hard drive along with date-time related information. Therefore, forensic analysts may find an abundance o information relating to the sent message on the offender's hard drive, including the original message contents. Additionally, investigators may be able to obtain related information from Hotmail, including Web server access logs, IP addresses, and possibly the entire message m" the sent mail folder of the offender's e-mail account.

2. Digital Stream of Bits :

Cohen refers to digital evidence as a bag of bits, which in turn can be arranged in arrays t display the information. The information in continuous bits will rarely make scene and tools are needed to show these structures logically so that it is readable.

The circumstance in which digital evidence are found also helps the investigator during the inspection. Metadata is used to portray data more specifically and is helpful in determining the background of digital evidence.

4.4 Types of Evidences:

There are many types of Evidences, each with their own specific or unique characteristics. Some major types of evidences are :

1. Illustrative evidence: Illustrative evidence is also called as demonstrative evidence. It is generally a representation of an object which is common form of proof. For example, photographs, videos, sound recordings, X-rays, maps, drawing, graphs, charts simulations, sculptors, and model.

2. Electronic Evidence: Electronic evidence is nothing but digital evidence. As we know, the use of digital evidence in trials has greatly increased .The evidences or proof that can be obtained from the electronic source is called the digital evidence.(viz. Email , hard drives etc.).

3. Documented Evidence: Documented evidence is same as demonstrative evidence. However, in documentary evidence, the proof is presented in writing (Viz. Contracts, wills, invoices etc.).

4. Explainable Evidence: This type of evidence is typically used in criminal cases in which it supports the dependent, either partially or totally removing their guilt in the case. It is also referred to as exculpatory.

5. Substantial Evidence: A proof that is introduced in the form of a physical object, whether Whole or in part is referred to as substantial evidence. It is also called as physical evidence.

Such evidence might consist of dried blood, fingerprint, and DNA samples, casts of footprints or tries at the scene of crime.

6. Testimonial: It is the kind of 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 or tries at the scene of crime, forms of evidence in the system.

4.5 Challenges in Evidence handling:

While responding to a computer security incident, a failure to adequately document is one the most common mistakes made by computer security professional's Analytical data mid never be collected, critical data may be lost or data's origin or meaning may become unknown As there are many evidences collected based on technical complexity is the fact that he properly retrieved evidence requires a paper trial.

Such documentations give an impression of having a certain quality against the natural instincts of the technical practical knowledge of individuals, who often investigate computer security incidents.

The challenges faced in the evidence handling must be properly understood by all the investigators. They should also understand how to meet these challenges. Therefore, it is essential for every organization to have formal evidence handling procedures that support computer security investigation. The most difficult task for an evidence handler is to substantiate the collected evidence at the judicial proceedings. Maintaining the chain of custody is also necessary. You must have both power and skill to validate your evidence.

4.5.1 Authentication of Evidence:

The laws of many state jurisdictions define data as Written Works and Record keeping Before introducing them as evidence, documents and recorded material must be authenticated.

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. In other words, for providing a piece of evidence of the testimony, it is necessary to have an authenticated evidence by a spectator who has a personal knowledge to its origin.

For an evidence to be admissible, it is necessary that it should be authenticated, otherwise the information cannot be presented to judging only. The matter of record is that the evidence collected by any person should meet the demand of authentication. The evidence collected must have some sort of internal documentation that records the manner of collected information.

4.5.2 Chain of Custody:

What Is the Chain of Custody in Computer Forensics?

The chain of custody in digital forensics can also be referred to as the forensic link, the paper trail, or the chronological documentation of electronic evidence. It indicates the collection, sequence of control, transfer, and analysis. It also documents each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

Why Is It Important to Maintain the Chain of Custody?

It is important to maintain the chain of custody to preserve the integrity of the evidence and prevent it from contamination, which can alter the state of the evidence. If not preserved, the evidence presented in court might be challenged and ruled inadmissible.

Importance to the Examiner:

Suppose that, as the examiner, you obtain metadata for a piece of evidence. However, you are

able to extract meaningful information from it, The fact that there is no meaningful information within the metadata does not mean that the evidence is insufficient. The chain of Custody in this case helps show where the possible evidence might lie, where it came from, who created it, and the type of equipment that was used. That way, if you want to create an example, you can get that equipment, create the exemplar, and compare it to the evidence to confirm the evidence properties.

Importance to the Court:
It is possible to have the evidence presented in court dismissed if there is à missing linking the chain of custody. It is therefore important to ensure that a wholesome and meaningful chain of custody is presented along with the evidence at the court.

What Is the Procedure to Establish the Chain of Custody?

In order to ensure that the chain of custody is as authentic as possible, a series of steps must be followed. It is important to note that, the more information a forensic expert obains concerning the evidence at hand, the more authentic is the created chain of custody. Due to this, it is important to obtain administrator information about the evidence: for instance, the administrative log, date and file info, and who accessed the files. You should ensure the following procedure is followed according to the chain of custody for electronic evidence:
• **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.

The procedure of the chain of custody might be different. depending on the jurisdiction which the evidence resides; however, the steps are largely identical to the ones outlind above.

What Considerations Are Involved with Digital Evidence?

A couple of considerations are involved when dealing with digital evidence. We shall take look at the most common and discuss globally accepted best practices.
1. Never work with the original evidence to develop procedures: The biggest

consideration with digital evidence is that the forensic expert has to make a complete copy of the evidence for forensic analysis. This cannot be overlooked because, when errors are made to working copies or comparisons are required, it will be necessary to compare the original and copies.

2. Use clean collecting media: It is important to ensure thất the examiner's storage device is forensically clean when acquiring the evidence. This prevents the original copies from damage. Think of a situation where the examiner's data evidence collecting media is infected by malware. If the malware escapes into the machine being examined, all of the evidence can become compromised.

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. It is recommended that this information be documented and brought to the attention of the case agent because the information may be needed to obtain additional search authorities. 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.

The considerations above need to be taken into account when dealing with digital evidence due to the fragile nature of the task at hand.

Chain of custody prevents evidence from being tainted; it thus establishes trustworthiness of items brought into evidence. The U.S. legal system wants the proponent of evidence to be able to demonstrate an unbroken chain of custody for items, he wants to have admitted.

Often, there is a stipulation, for example, when there is an agreement between the parties or a concession by the opponent of the evidence that allows it to be admitted without requiring testimony to prove the foundational elements. The purpose of stipulation is to move

the trial quickly forward, without pondering idle questions.
If there is a break in the chain of custody brought to the attention of the court, then the court has to decide whether the breach is so severe as to meet exclusion of the item from trial.

Alternatively, the court can decide that the Trier (trial judge or jury) need to decide the value of the evidence. To prevent a breach, a forensic investigation should follow a written policy, so that necessary deviations of the policy can be argued. The policy itself should take all reasonable (or arguably reasonable) precautions against tampering.

For example, assume that a PDA is seized from a suspected drug dealer. In the case of an PDA, there is no hard drive image to mirror, that is, the examination will have to be done un the powered-on original. The PDA can lose data, for example by disconnecting it from its battery. On seizure, the device should not be switched on. If it is seized switched on, it should be switched off in order to preserve battery power. It needs to be put into an evidence bag that does not allow access to the PDA without breaking the seal (no clear plastic bag!). The evidence needs to be tagged with all pertinent data, including the serial number of the PDA and the circumstances of the seizure. The PDA should never be returned to the accused at the scene, because the device can lose data if reset. To maintain the data in the PDA, it needs to be kept in a continuously charged mode. It should only be used to extract evidence by a competent person who can testify in court. As long as the PDA could be evidence, it needs to kept in an evidence locker. with check-out logs, so that it can be determined who had access to the PDA at any time.

Evidence Validation: The challenge is to ensure that providing or obtaining the data you have collected is similar to the data provided or presented in court. Several years pass between the collection of evidence and the production of evidence at a judiciary proceeding , which is very common. To meet the challenge of validation, it is necessary to ensure that the original media matches the forensic duplication by using MD5 hashes. The evidence for every file is nothing but the MD5 hash values that are generated for every file that contributes to the case. The verify function within the Encase application can be used while duplicating a hard drive with Encase. To perform a forensic duplication using dd, you must record MDS hash for both the original evidence media and binary files or the files which compose the forensic duplication.

Note: Evidence collection calculated by MD5 after 6 months may not be helpful.MD5 hashes Should be performed when the evidence is obtained.

4.6 Volatile Evidence: Not all the evidence on a system is going to last very long. Some d evidence is residing in storage that requires a consistent power supply: other evidence may he stored in information that is continuously changing. When collecting evidence, you should always try to proceed from the most volatile to the least. Of course, you should still take the individual circumstances into account-you shouldn't waste time extracting information from an unimportant/unaffected machine's main memory when an important or affected machine's secondary memory hasn't been examined.

You need to respond to the target system at the console during the collection of volatile data rather than access it over the network. This way the possibility of the attacker monitoring your responses is eliminated, ensuring that you are running trust commands. If you are

creating a forensic duplication of the targeted system, you should focus on obtaining the volatile system data before shutting down the system.

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

Note: Once you have collected the raw data from volatile sources you may be able to shutdown the system. {Matthew Braid, "Collecting Electronic Evidence After A System Compromise," Australian Computer Emergency Response Team}

Registers, Cache: The contents of CPU cache and registers are extremely volatile, since they changing all of the time. Literally, nanoseconds make the difference here. An examiner ds to get to the cache and register immediately and extract that evidence before it is lost.
Routing Table, ARP Cache, Process Table, Kernel Statistics, Memory: Some of these items, like the routing table and the process table, have data located on network devices. In other words, that data can change quickly while the system is in operation, so evidence must he gathered quickly. Also, kernel statistics are moving back and forth between cache and main memory, which make them highly volatile. Finally, the information located on random access memory (RAM) can be lost if there is a power spike or if power goes out. Clearly, that information must be obtained quickly.

Temporary File Systems: Even though the contents of temporary file systems have the potential to become an important part of future legal proceedings, the volatility concern is not as high here. Temporary file systems usually stick around for a while.
Disk: Even though we think that the data we place on a disk will be around forever, that is not always the case (see the SSD Forensic Analysis post from June 21). However, the likelihood that data on a disk cannot be extracted is very low.
Remote Logging and Monitoring Data that is Relevant to the System in Question: The potential for remote logging and monitoring data to change is much higher than data on a hard drive, but the information is not as vital. So, even though the volatility of the data is higher here, we still want that hard drive data first.

Physical Configuration, Network Topology, and Archival Media: Here we have items that are either not that vital in terms of the data or are not at all volatile. The physical configuration. and network topology is information that could help an investigation, but is likely not going to-have a tremendous impact. Finally, archived data is usually going to be located on a DVD or tape, so it isn't going anywhere anytime soon. It is great digital evidence to gather, but it is not

volatile.

4.7 Case Studies:

Case-1: Credit Card Fraud

State	: Tamil Nadu
City	: Chennai
Sections of Law	: Section of Law: 66 of Information Technology Act
	2000 & 120(B), 420,467,468,471 IPC.

Background:
The assistant manager (the complainant) with the fraud control unit of a large business process outsourcing (BPO) organization filed a complaint alleging that two of its employees had conspired with a credit card holder to manipulate the credit limit and as a result cheated the company of INR 0.72 million.
The BPO facility had about 350 employees. Their primary function was to issue the bank's credit cards as well as attend to customer and merchant queries. Each employee was assigned to a specific task and was only allowed to access the computer system for that specific tasl The employees were not allowed to make any changes in the credit-card holder's acco unless they received specific approvals.

Each of the employees was given a unique individual password. In case they entered an incorrect password three consecutive times then their password would get blocked and they would be issued a temporary password.

The company suspected that its employees conspired with the son (holding an add-on card) of one of the credit card holders. The modus operandi suspected by the client is as follows.

The BPO employee deliberately keyed in the wrong password three consecutive times (so that his password would get blocked) and obtained a temporary password to access the computer system. He manually reversed the transactions of the card so that it appeared that payment for the transaction has taken place. The suspect also changed the credit card holder's address so that the statement of account would never be delivered to the primary card holder.

Investigation: A procedure to find the Digital Evidence
The investigating team visited the premises of the BPO and conducted detailed examination of various persons to understand the computer system used. They learnt that in certain situations the system allowed the user to increase the financial limits placed on a credit card. The system also allowed the user to change the customer's address, blocking and unblocking of the address, authorisations for cash transactions etc.

The team analysed the attendance register which showed that the accused was present at all the times when the fraudulent entries had been entered in the system. They also analysed the system logs that showed that the accuser's ID had been used to make the changes in the system.

The team also visited the merchant establishments from where some of the transactions had taken place. The owners of these establishments identified the holder of the add-on card.

Current status: The BPO was informed of the security lapse in the software utilised. Armed with this evidence the investigating team arrested all the. accused and recovered, on their confession, six mobile phones, costly imported wrist watches, jewels, electronic items, leather accessories, credit cards, all worth INR 0. 3 million and cash INR 25000, The investigating team informed the company of the security lapses in their software so that instances like this could be avoided in the future

This case won the second runner-up position for the India Cyber Cop Award, for its investigating officer Mr S. Balu, Assistant Commissioner of Police, Crime, Chennai Police.

The case was remarkable for the excellent understanding displayed by the investigating team, of the business processes and its use in collecting digital evidence.

Case-2: Hosting Obscene Profiles

State	: Tamil Nadu
City	: Chennai
Sections of Law	: 67 of Information Technology
	Act 2000 469, 509 of the Indian Penal code

Background: The complainant stated that some unknown person had created an e-mail ID using her name and had used this ID to post messages on five Web pages describing her as a call-girl along with her contact numbers.

As a result she started receiving a lot of offending calls from men.

Investigation: A procedure to find the Digital Evidence

After the complainant heard about the Web pages with her contact details, she created a username to access and view these pages.

Using the same log-in details, the investigating team accessed the Web pages where these profiles were uploaded. The message had been posted on five groups, one of which was a public group. The investigating team obtained the access logs of the public group and the message to identify the IP addresses used to post the message. Two IP addresses were identified.

The ISP was identified with the help of publicly available Internet sites. A request was made to the ISPS to provide the details of the computer with the IP addresses at the time the messages were posted. They provided the names and addresses of two cyber cafes located in Mumbai to the police.

The Investigating team scrutinised the registers maintained by the cyber cafes and found that in one case the complainant's name had been signed into the register.

The team also cross-examined the complainant in great detail. During one of the meetings she revealed that she had refused a former college mate who had proposed marriage.

In view of the above the former college mate became the prime suspect. Using this information the investigating team, with the help of Mumbai police, arrested the suspect and seized a mobile phone from him. After the forensic examination of the SIM card and 4 phone, it was observed that phone had the complainant's telephone number that was posted on the internet. The owner of the cyber cafes also Identified the suspect as the one who had visited the cyber cafes.
Based on the facts available with the police and the sustained interrogation the suspect confessed to the crime.
Current status: The suspect was convicted of the crime and sentenced to two years of imprisonment as well as a fine.
Case - 3: Illegal money transfer

State	: Maharashtra
City	: Pune
Sections of Law	: 467,468, 471, 379,419, 420, 34 of IPC & 66 of IT ACT

Background: The accused in the case were working in a BPO, that was handling the business of a multinational bank. The accused, during the course of their work had obtained the personal identification numbers (PIN) and other confidential information of the bank's customers. Using these the accused and their accomplices, through different cyber cafes, transferred huge sums of money from the accounts of different customers to fake accounts.

Investigation: A procedure to find the Digital Evidence
On receiving the complaint the entire business process of the complainant firm was studied and a systems analysis was conducted to establish the possible source of the data theft.

The investigators were successful in arresting two people as they laid a trap in a local bank where the accused had fake accounts for illegally transferring money.

During the investigation the system server logs of the BPO were collected. The IP addresses were traced to the Internet service provider and ultimately to the cyber cafes through which illegal transfers were made.

The registers maintained in cyber cafes and the owners of cyber cafes assisted in identifying the other accused in the case. The e-mail IDs and phone call print outs were also procured and studied to establish the identity of the accused. The e-mail accounts of the arrested accused were scanned which revealed vital information to identify the other accused. Some e-mail accounts of the accused contained swift codes, which were required for internet money transfer.

All the 17 accused in the case were arrested in a short span of time. The charge sheet was submitted in the court within the stipulated time. In the entire wire transfer scam, an amount to the tune of about INR 19 million was transferred, out of this INR 9 million was blocked in transit due to timely intimation by police, INR 2 million was held in balance in one of the hank accounts opened by the accused which was frozen. In addition the police recovered cash, ornaments, vehicles and other articles amounting to INR 3 million.
During the investigation the investigating officer learned the process of wire transfer, the banking procedures and weakness in the system. The investigating officer suggested measures

Current status: Pending trial in the court.
The case won the India Cyber Cop Award, for its investigating officer Mr Sanjay Jadhav, assistant Commissioner of Police, Crime, Pune Police. The panel of judges felt that this case he most significant one for the Indian IT industry during 2005 and was investigated in a professional manner, with substantial portion of the swindled funds being immobilised, a e number of persons were arrested and the case was sent to the court for trial within 90 days.

Case-4: Fake Travel Agent

State	: Maharashtra
City	: Mumbai
Sections of Law	420, 465, 467, 468, 471, 34 of IPC r/w 143 of Indian
	Railway Act 1989.

Background: The accused in this case was posing to be a genuine railway ticket agent and, had been purchasing tickets online by using stolen credit cards of non-residents. The accused created fraudulent electronic records/ profiles, which he used to carry out the transactions. The tickets so purchased were sold for cash to other passengers. Such events occured for a period of about four months.

The online ticket booking service provider took notice of this and lodged a complaint with the cybercrime investigation cell.

Investigation: A procedure to find the Digital Evidence
The service provider gave the IP addresses, which were used for the fraudulent online bookings, to the investigating team. IP addresses were traced to cyber cafes in two locations.

The investigating team visited the cyber cafes but was not able to get the desired logs as they not maintained by the cyber cafe owners. The investigating team was able to short list Sons present at cyber cafes when the bookings were made. The respective owners of the cyber cafes were able to identify two persons who would regularly book railway tickets.

The investigating team then examined the passengers who had travelled on these tickets. They Sated that they had received the tickets from the accused and identified the delivery boy who delivered the tickets to them. On the basis of this evidence the investigating team arrested two persons who were identified in an identification parade.

Current status: The charge sheet has been submitted in the court.

Case-5: Creating Fake Profile

State	: Andhra Pradesh
City	: Hyderabad
Sections of Law	: 67 Information Technology Act 2000 507, 509 of the
	Indian Penal Code

Background: The complainant received an obscene e-mail from an unknown e-mail ID The

complainant also noticed that obscene profiles along with photographs of his daughter had been uploaded on matrimonial sites.

Investigation: A procedure to find the Digital Evidence
The investigating officer examined and recorded the statements of the complainant and his daughter. The complainant stated that his daughter was divorced and her husband had developed a grudge against them due to the failure of the marriage.

The investigating officer took the original e-mail from the complainant and extracted the IP address of the same. From the IP address he could ascertain the Internet service provider.

The IP address was traced to a cable Internet service provider in the city area of Hyderabad. The said IP address was allotted to the former husband sometime back and his house was traced with the help of the staff of ISP.

A search warrant was obtained' and the house of the accused was searched. During the search operation, a desktop computer and a handicam were seized from the premises. A forensic IT specialist assisted the investigation officer in recovering e-mails (which were sent to the complainant), using a specialised disk search tool as well as photographs (which had been posted on the Internet) from the computer and the handicam respectively. The seized computer and the handicam were sent to the forensic security laboratory for further analysis. The experts of the forensic security laboratory analysed the material and issued a report stating that: the hard disk of the seized computer contained text that was identical to that of the obscene e-mail; the computer had been used to access the matrimonial websites on which the obscene profiles were posted; the computer had been used to access the e-mail account that was used to send the obscene e-mail; the handicam seized from the accused contained images identical to the ones posted on the matrimonial Websites. Based on the report of dhe FSL it was clearly established that the accused had: created a fictious e-mail ID and had set the obscene e-mail to the complainant; posted the profiles of the victim along with the photographs on the matrimonial sites.

Current status: Based on the material and oral evidence, a charge sheet has been filed against the accused and the case is currently pending for trial.

References

1. http://www.forensicsciencesimplified.org/digital/
2. http://www.forensicsciencesimplified.org/digital/
3. https://www.helpnetsecurity.com/2007/07/20/the-rules-for-computer-forensics/ as on 28 August 2019
4. Digital Evidence and Computer Crime, Third Edition 2011 Eoghan Casey. Published by Elsevier Inc.
5. www.cse.scu.edu/-tschwarz/COEN252_13/LN/legalissues.html

Sample Multiple Choice Questions

1. The digital evidence are used to establish a credible link between……
    a. Attacker and victim and the crime scene
    b. Attacker and the crime scene
    c. victim and the crime scene

d. Attacker and Information

2 Digital evidences must follow the requirements of the……..

a. Ideal Evidence rule

b. Best Evidence Rule

c. Exchange Rule

d. All of the mentioned

3. From the two given statements I and 2, select the correct options from a-d.

1): Original media can be used to carry out digital investigation process.

2): By default, every part of the victim's computer is considered unreliable.

a. a and b both are true

b. a is true and b is false

a and b both are false

d. a is false and b is true

4. The evidences or proof that can be obtained from the electronic source is called the……

a. digital evidence

b. demonstrative evidence

c. Explainable Evidence

d. substantial evidence

5. Which of the following is not a type of volatile evidence?

a. Routing Tables

b. Main Memory

c. Log files

d. Cached Data