All the models the general steps followed for investigation are..

1. Identification of proof
2. Preservation of its authentication of data
3. Preparation…of tools, techniques methods and so on
4. Approaching strategy…planning for it
5. Collection…right data or proof
6. Examination….trying to find what is required
7. Analysis……. Trying to understand
8. Presentation….documentation in legal language

Benefits of digital forensic

1. To produce evidence in court which can lead to the punishment of the culprit
2. It also helps the companies to capture important information if their computer systems or network systems are compromised
3. Efficiently tracking down cyber criminals from wherever in the world
4. Helps the organization in protecting their information and data thus indirectly their money and valuable time
5. Allows to extract, process, and interpret the factual evidence so it proves the cybercriminals actions in the court of law
6. As it is defined as science thus it leads to the use of standard and acceptable techniques, methods, processes and frameworks by the investigators
7. because of this science it is possible to recover the data which has be changed or destroyed by the cybercriminals

Disadvantages of digital forensic

1. It becomes a very difficult task for the investigator to prove that the digital evidence available is not tampered
2. acquiring digital records, storing and maintaining them is a costly affair
3. the investigators and legal practitioners should also have a good computer knowledge so as to understand and accept the evidence.
4. If the tools , techniques, methods, etc are not as per the specific standards then the evidence collected by it may not be accepted in the court of law.
5. there are always chances that the digital data may change, get deleted or modified when digital evidence is getting collected by the investigator
6. the digital forensic expert charges are on hourly basis, but the actual activity starting from identification to document presenting in the court of law takes a very period
7. from the crime scene a copy of the required data is taken and not the original data. This mapping has to be done very accurately without any modification
8. the final finding if not documented properly may not stand in the court of law

Chain of Custody

1. It is a logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases.
2. Each step in this chain is important for presenting the final evidence
3. the chain of custody in case of digital forensic means, the paper trail( series of documents that shown the recorded of all the activities) or forensic links or chronological documentation of the evidence
4. It indicated the collection, sequence of control, transfer and Analysis
5. It also documents the details of each person who handles the evidence, data and time it was collected or transferred and also the purpose of transfer
6. It basically demonstrates a trust between the client and the court of law that the evidence has not been tampered.

Importance of chain of custody

1. The examiner or the investigator can preserve the integrity of the data
2. It also prevents the evidence from being altered, modified or deleted
3. Suppose the investigator obtains the metadata but is not able to get any useful information from the metadata then the chain of custody helps to identify where the possible evidence may lie, where it came from, who created it.
4. It also helps to prove from the metadata as to what type of equipment could have been used.
5. It also helps the court to believe in the evidence submitted to the court.

Chain of custody process

1. Data collection:
2. Examination
3. Analysis
4. Reporting

Procedure to establish Chain of Custody:

1. Save the original material:
2. Take photos of the physical evidence:
3. screenshots of the digital evidence:
4. Document date, time, and any other information on the receipt of the evidence.
5. Inject a bit-for-bit clone of digital evidence content into forensic computers:

this is done to find the effect and evaluate the amount of loss increased by the company

1. Perform a hash test analysis to authenticate the working clone:

this is done to authenticate the evidence copy with the original

How can the Chain of Custody be assured?

1. Never ever work with the Original Evidence:
2. Ensuring storage media is sterilized:
3. Document any extra scope:
4. Consider the safety of the personnel at the scene:

sub categories of anti-forensic methods

1. data hiding,
2. artifact wiping,
3. Disk cleaning utilities
4. File cleaning utilities
5. Disk destruction
6. trail obfuscation

Rules to be followed in digital forensics:

1. Honesty toward investigation:
2. Handle the digital evidence with care:
3. Compliance with standard laws and professional norms: