Vishwa Chaturvedi
20180610011 0127

4-B

PAGE No.
DATE / /

1. What is digital forensics? How a "chain of custody" concept applies in computer/ digital forensics?

Ans Digital forensics is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived for the purpose of facilitation.

Chain of custody means the chronological documentation trail etc. that indicates the custody, control, transfer, analysis and deposition of evidence, physical or electronic.

The chain of custody is also used in most evidence situations to maintain the integrity of the evidence.

It is particularly important in situations where sampling can identify the existence of contamination.

2. Discuss the roles and responsibilities of any technical operations level officers in an organisation.

→ The IT technical support officer monitors and maintains the computer system and network of an organisation.

PAGE No.
DATE / /

Responsibilities

- Install and configure computer hardware operating system & application
- Monitor and maintain computers systems and networks.
- troubleshoot system and network problems, diagnosing and solving hardware or software faults.
- Set up new user's accounts and profiles and deal with password issues.
- Solving technical and applications problems either over the phone or in person.
- Test and evaluate new technology
- Replace parts as required.

Q3 Demonstrate the roles and responsibilities of executive and middle level officers in an organisation.

Ans Executive level

- Responsible for providing strategic financial and operational leadership for the company.
- plan, develop, implement and direct the organization's operations.
- Analyze and make recommendation on the impact of long range growth initiatives, planning and introduction of new strategies & regulatory actions.
- Leading the development and implementation of the overall organization's strategy.
- Communication on behalf of the company with shareholders, government entities and public.

Middle level

- This level of management is responsible for implementing the policies and plans decided by the top management.

- establish IT policies, strategies and standards.
- Strategic planning of business growth
- Creating timeliness for the development and Development of all technological services.

Q6 Discuss various phases in computer forensics / Digital forensics.

Ans Computer forensics / Digital forensics involves the following phases.

1. Preparation and identification :-
   - In order to be processed and applied, evidence must first be identified as an evidence.
   - It involves activities like interrogatories, preventions, spoliation, disclouser and discovery, planning, discovery request.

2. Collection and recording :-
   - Digital evidence can be collected from many sources. Obvious sources include computers, cellphones, digital camera, hard drives, CD ROM, usb

devices etc.
Non-obvious includes - setting of digital thermometers, black boxes inside auto Mobiles etc.

It involves activities like drive imaging, indexing, profiling, search plans, cost estimates, risk analysis.

3. Storing and transporting:-

- Storage must be adequately secure to assure proper "chain of custody" and typically for evidence.
- Evidence is often copied and sent electronically on compacted disks or other media from place-to-place.

4. Examination / investigation:-

- It involves activities like triage images data recovery, keyword searches, hidden data review, communication, iterate.

5. Analysis, interpretation and attribution:-

- All digital evidence must be analyzed to determine the type of information.

6. Reporting:-

It involves relevant document

production, search statistic reports, Chain of custody reporting, Case log reporting.

7. Testing :-

It includes testimony preparation, presentation preparation, Testimony.

Q5. List out various context which involved for identifying digital evidence. Illustrate various guidelines for the digital evidence collection phase.

Ans There are number of contexts involved in identifying a piece of digital evidence

1. Physical context
2. Logical context
3. Legal Context

Following are some guidelines for the digital evidence collection phase:-

1. Adhere to your site's security policy and engage the appropriate incident handling and law enforcement personel.

DATE / /

2. Capture a picture of the system as accurately as possible.

3. Keep detailed notes with dates and times

4. Note the difference between the system clock and coordinated universal time.

5. Minimize changes to the data as you're collecting it.

6. Procedures should be implementable.

Q6. Explain digital forensics life cycle in detail

Ans The steps in digital forensics follow a life cycle approach and consist of following steps

1. Required Analysis:-
The preliminary step we should check our technological feasibility

2. Retrieval of Data:-
Identify the source and destination media and the data available on that is taken on to the other media for further investigation.

3. Reliability:-
Originality of data is checked. Therefore hashes of the original data is created before image creation.

4. Review of evidence:-
The analysis of this layer includes processing the disk image layout and even recovering deleted data after it has been overwritten.

5. Representation of evidence:-
Digital evidences represented in the form that can be understood by the court.

6. Repository of Data:-
After the successful investigation, the data in repository is archived for future use.

Q1. write a short note on oral evidence. and documentary evidence

→ Oral evidence :- When prog is restricted to spoken words or by gestures or motion then it is termed as oral evidence.

Oral evidence when reliable is used adequately without narration of written prog to demonstrate a reality or fact.

→ Documentary evidence :-

Any evidence which is present are documented before the court is ordered to demonstrate or show a reality.

The content of documentary evidence can be separated into three sections

1) How the subject matter of document can be demonstrated?

2) How the record is to be proved to be authentic?

3) How far and in what instance oral evidence is excluded by documentary