Digital Forensic Question Bank

1. **Enhanced Digital Investigation Process Model(EDIP)**
2. **Types of Digital Forensics.**
3. **Explain different techniques of recovery of files?**
4. **How will you secure your email account?**
5. **Email:**

    -email forensic[imp]

    -email recovery[imp]

    -email forensic analysis steps / methods / procedure

    -email work as evidence?

    -Working of email

    -email protocol

    -email security

    -email spoofing-short note[imp]

    -email spamming-short note[imp]

    -email trace

5.***Intrusion Detection System(IDS) & also explain different types of IDS?[Hidden Question]*****(Imp for 10 marks)**

[Points:

Advantage:

i. Visibility

ii. Defence

iii. Response Capabilities

iv. Tracking of virus Propogation

v. Help in evidence

Disadvantage:

i. More Maintenance is required

ii. False Positives

iii. False Negative

iv. Staff Requirement

6. **What is Cloud forensic, opportunities of cloud forensics?**

-Explain 3 dimension of cloud forensics?

-Challenges in cloud forensics?

[Imp Note: Do not explain cloud computing in detail only cloud forensics definition is required]

7. **What is Cybercrime? Explain different types of Email-Service Protocols**

8. **What is steganography? Explain different types of steganography**

9. **What is Digital Evidence? Explain different types of digital evidence**

10. **Shortnote:**

i. Call forging

ii. Bluesnarfing

11. **Forensic Duplication:**

-What is forensic duplication?

-Explain thumb rules of forensic duplication?

-Explain necessity of forensic duplication?

-Explain important terms in forensic duplication?

-Restored image or Mirror image

-Explain Necessity of forensic duplication & also explain forensic duplication examples

12. **Evidence handling Procedure:**

-Evidence System description

-Digital Photo

-Evidence Tags

-Evidence Storage

-Evidence logs

-Counting copies

-Evidence Backup

-Evidence Decomposition

-Evidence Audit

-Evidence Safe

-Shipping Evidence Medicine

-Procedure

13. **Stagna Analysis[imp]**
14. **Hiding data methods[imp]**
15. **Methods of Hiding Data:**

-Watermarking

16. **Various Phases/Models/Framework *[V.V.Imp]:***

-Models:

-ECSI(Electronic Scene Investigation)

a. Collection

b. Examine

c. Analysis

d. Report

-DFRWS(Digital Forensic research Workshop)

Six Steps:

a. Identification

b. Preservation

c. Collection

d. Examination

e. Analysis

f. Presentation

-ADFM(Abstract Digital Forensic Models)

a. Preparation

b. Approach

c. Strategy

d. Returning Evidence

-IDIP(Integrated Digital Investigation Process)

-EDIP(Enhanced Digital Investigation Process)

-***CFFTPM(Computer Forensic Field Triage Process Model)***

-***CPCFIM(Common Phases of Computer Forensic Investigation Model)***

17. **Abstraction[imp]**

18. **What is mobile forensic? Explain different data can be used as evidence in mobile forensics?**

-Mobile Forensic Procedures:

Step 1: File present in Sim card

Step 2: Device Data

Step 3: File present in external memory dump

Step 4: Evidence in memory card

Step 5: Evidence in Operator's Framework