1. Define the term “Computer Forensics”.

Computer forensic science, computer forensics, and digital forensics may be defined as the methodological, scientific, and legally sound process of examining computer media and networks for the identification, extraction, authentication, examination, interpretation, preservation, and analysis of evidence. It also involves collection and presentation of computer-related evidence. Computer evidence can be useful in criminal cases, civil disputes, and human resources/employment proceedings.

2. What are the roles of a Computer in a Crime?

o A computer can play one of three roles in a computer crime.

o A computer can be the target of the crime,

o It can be the instrument of the crime, or

o It can serve as an evidence repository storing valuable information about the crime.

3. State the objectives of Computer Forensics.

o The objective of Computer Forensics is to recover, analyze, and present computer-based material in such a way that it is useable as evidence in a court of law.

4. Who Can Use Computer Forensic Evidence?

o Criminal Prosecutors

o Civil litigations

o Corporations

o Law enforcement officials

5. Mention some problems with Computer Forensic Evidence.

o Computer data changes moment by moment.

o Computer data is invisible to the human eye; it can only be viewed indirectly

after appropriate procedures.

o The process of collecting computer data may change it—in significant ways.

o The processes of opening a file or printing it out are not always neutral.

o Computer and telecommunications technologies are always changing so that forensic processes can seldom be fixed for very long

6. Define Computer Crime and digital crime.

o Computer crime has been traditionally defined as any criminal act committed via computer.

o Computer-related crime has been defined as any criminal act in which a computer is involved, even peripherally.

o Cybercrime has traditionally encompassed abuses and misuses of computer systems or computers connected to the Internet which result in direct and/or concomitant losses.

o Digital crime, a relatively new term, includes any criminal activity which involves the unauthorized access, dissemination, manipulation, destruction, or corruption of electronically stored data.

7 What Is Phreaking?

o Phreaking involves the manipulation of telecommunications carriers to gain knowledge of telecommunications, and/or theft of applicable services. It is also known as telecommunications fraud, and includes any activity that incorporates the illegal use or manipulation of access codes, access tones, PBXs, or switches.

8. State the motivations for computer intrusion or theft of information in contemporary society.

o Boredom (informational voyeurism)

o Intellectual challenge (mining for knowledge—pure hackers),

o Revenge (insiders, disgruntled employees, etc.),

o Sexual gratification (stalking (nuisance), harassment, etc.),

o Economic (criminals), and

o Political (Hacktivists, terrorists, spies, etc.).

9. List some digital forensics tools.

–Drive Spy and Image

–FTK

–X-Ways Forensics

10. What is CMOS?

o CMOS denotes Complementary Metal Oxide Semiconductor. The Computer stores system configuration and date and time information in the CMOS.

11. What methods are available for recovering passwords?

o The three ways to recover passwords:

 Dictionary attacks

 Brute-force attacks

 Rainbows tables

12. Give the hierarchy of Contemporary Cybercriminals

There are five general categories of cybercriminals in today‘s society:

- Script kiddies,
- Cyberpunks,
- Hackers/crackers,
- Cybercriminal organizations, and
- Hacktivists
-

13. State the types of computer records.

Computer records are usually divided into:

–Computer-generated records

–Computer-stored records

14. What is FIOA?

 FOIA: Freedom of Information Act , allows citizens to request copies of public documents created by federal agencies.

15. List the tasks of a Computer Forensics Examination Protocol

o Perform the investigation with a GUI tool

o Verify your results with a disk editor

o Compare hash values obtained with both tools