**1. What is the primary goal of digital forensics?**

A) To manipulate digital evidence  
B) To follow a specific investigation template  
C) **To apply the scientific method to digital investigations**  
D) To ensure data destruction

**2. Which of the following is NOT a key principle of forensic methodology?**

A) Avoid contaminating evidence  
B) **Always use the same methodology regardless of context**  
C) Present facts objectively  
D) Maintain consistency and accuracy

**3. What should be done before finalizing forensic results?**

A) Keep the results private  
B) Destroy opposing party’s evidence  
C) **Have another expert review the results**  
D) Submit the findings without verification

**4. What is an important step when handling original digital evidence?**

A) Modify it to make analysis easier  
B) **Ensure that it is not altered during the investigation**  
C) Use the suspect’s computer for analysis  
D) Edit the timestamps for clarity

**5. In forensic investigations, a corporate case may focus on:**

A) Analysing financial records only  
B) Identifying malware sources  
C) **Determining file presence or misuse of resources**  
D) Investigating murders

**6. Which forensic principle states that no actions should change data that may be relied upon in court?**

A) **Principle 1**  
B) Principle 2  
C) Principle 3  
D) Principle 4

**7. Why should an audit trail be maintained during forensic investigations?**

A) **To ensure independent verification of forensic processes**  
B) To limit access to evidence  
C) To avoid data encryption  
D) To speed up investigations

**8. What should be the first step when responding to a forensic case?**

A) **Conducting interviews with relevant individuals**  
B) Imaging the hard drive  
C) Shutting down the suspect’s computer  
D) Deleting unnecessary files

**9. What is a crucial piece of equipment for forensic first responders?**

A) **Write blockers**  
B) Gaming laptops  
C) Unlicensed software tools  
D) Regular USB drives

**10. Why should a forensic investigator collect system logs?**

A) **To track user activities and system events**  
B) To increase system speed  
C) To clear unwanted files  
D) To disable security settings

**11. What is a key reason for acquiring an image of RAM?**

A) **To recover volatile data such as passwords and running processes**  
B) To clear unnecessary processes  
C) To reset the operating system  
D) To bypass system security

**12. What should be considered when documenting a forensic investigation?**

A) **Using diagrams, written notes, photographs, and videos**  
B) Keeping all findings confidential  
C) Only recording important discoveries  
D) Destroying evidence after the case is closed

**13. When transporting digital evidence, what must be ensured?**

A) **Avoid exposure to extreme temperatures**  
B) Carry it in a regular backpack  
C) Leave devices powered on  
D) Keep all cables detached

**14. What is the purpose of a write blocker?**

A) To erase digital evidence securely  
B) **To prevent accidental modifications to forensic data**  
C) To speed up data transfers  
D) To enable direct editing of forensic images

**15. What is one of the key aspects of an incident response plan?**

A) **Securing and documenting the crime scene**  
B) Immediately formatting all storage devices  
C) Deleting irrelevant system logs  
D) Restarting the system for a fresh start

**16. Which type of evidence is considered digital evidence?**

A) **Any probative information stored or transmitted in digital form**  
B) Only hard drive data  
C) Printed emails  
D) Physical evidence from a crime scene

**17. Which step should be taken before conducting a forensic examination?**

A) **Ensuring chain of custody is properly recorded**  
B) Modifying file timestamps for clarity  
C) Restoring files from backups  
D) Deleting unnecessary logs

**18. What is an important step in handling a powered-on computer at a crime scene?**

A) **Capture an image of the RAM**  
B) Immediately turn off the computer  
C) Unplug all peripherals  
D) Run an antivirus scan

**19. Which forensic technique ensures a verifiable copy of a hard drive?**

A) **Bit-for-bit imaging**  
B) Manual file copying  
C) Selective screenshot capture  
D) Disk defragmentation

**20. Why is it important to analyse internet search history in a forensic case?**

A) **To determine past user activity and intent**  
B) To remove unnecessary browsing data  
C) To increase internet speed  
D) To block unwanted websites