**1. Why must digital forensics adhere to the scientific method?**

A) To guarantee evidence remains admissible in court  
B) **To apply verifiable and repeatable investigative steps**  
C) To prioritize speed over accuracy in investigations  
D) To ensure results favour the prosecution

**2. What is a key risk of failing to verify forensic findings before submission?**

A) **Opposing parties may identify inconsistencies and challenge results**  
B) The investigation will take longer  
C) The evidence will become inadmissible in court  
D) The forensic analyst may lose access to the case files

**3. In forensic methodology, why might a strict, step-by-step process not always be applicable?**

A) **Each case has different constraints, such as time, legal requirements, and emerging technology**  
B) A standardized approach slows down investigations  
C) Investigators should have complete freedom to decide the process  
D) The methodology should change based on the desired outcome

**4. What is a crucial forensic principle regarding digital evidence?**

A) **No actions should alter data that may be relied upon in court**  
B) Digital evidence should always be copied before analysis  
C) Original data should be modified for easier access  
D) Evidence handling should prioritize convenience over procedure

**5. When conducting a forensic interview, what should be a priority?**

A) **Recording and dating the interview for potential forensic reports**  
B) Asking only general questions to avoid influencing responses  
C) Avoiding documentation to ensure confidentiality  
D) Only interviewing witnesses, not suspects or victims

**6. What is a primary reason to create an audit trail during forensic investigations?**

A) To limit access to the evidence  
B) **To allow independent verification of forensic processes**  
C) To prevent unauthorized individuals from knowing investigation steps  
D) To speed up the investigation process

**7. What is a common mistake when handling a powered-on computer at a crime scene?**

A) **Shutting it down without capturing volatile memory (RAM) first**  
B) Immediately disconnecting all peripheral devices  
C) Leaving it connected to the internet during analysis  
D) Running antivirus scans before forensic imaging

**8. Why should forensic analysts use write blockers?**

A) To speed up data analysis  
B) To permanently erase sensitive files  
C) **To prevent accidental modifications to forensic data**  
D) To allow direct modifications to forensic images

**9. What is the primary concern when transporting digital evidence?**

A) **Protecting devices from extreme temperatures and physical damage**  
B) Keeping devices powered on for quick access  
C) Removing unnecessary files before transport  
D) Encrypting all data before analysis

**10. When responding to a forensic case, why is it important to document the crime scene?**

A) **To preserve the original state of evidence for later analysis**  
B) To ensure suspects are aware of the investigation  
C) To create a summary that can replace detailed analysis  
D) To speed up evidence processing by eliminating unnecessary steps

**11. What is a major advantage of forensic imaging over manual file copying?**

A) **It captures all data, including deleted files and unallocated space**  
B) It allows faster data transfers  
C) It only copies files that are currently visible  
D) It eliminates the need for write blockers

**12. Which forensic principle ensures that digital evidence remains reliable in court?**

A) **A documented chain of custody must be maintained at all times**  
B) The evidence should be reviewed only by a single investigator  
C) The original data must be stored for at least five years  
D) Investigators should have unrestricted access to all systems

**13. What should be done if a forensic investigator finds cloud-based evidence?**

A) Ignore it, as cloud data is not considered digital evidence  
B) **Document account details and attempt to preserve relevant data**  
C) Delete irrelevant cloud files to speed up the investigation  
D) Copy only locally stored files for analysis

**14. What type of digital evidence is often found in RAM but not on a hard drive?**

A) **Active processes, encryption keys, and volatile data**  
B) Deleted user files  
C) Operating system logs  
D) Unused storage blocks

**15. Why should forensic investigators examine internet search history?**

A) To reset the system to its original state  
B) **To determine past user activity and intent**  
C) To clear unnecessary browsing data  
D) To increase internet speed during analysis

**16. What is the purpose of a forensic boot disk?**

A) **To access and analyse a suspect’s system without modifying its data**  
B) To speed up the forensic investigation process  
C) To erase evidence securely  
D) To bypass login credentials without documentation

**17. When should digital forensic investigators use a grounding mechanism?**

A) **When handling hardware to prevent static discharge damage**  
B) When transporting evidence in a vehicle  
C) When encrypting forensic data  
D) When creating a forensic image of a storage device

**18. Why is it important to check a suspect computer’s BIOS settings?**

A) To change the boot order for forensic imaging  
B) **To verify the system clock and other settings that may affect timestamps**  
C) To gain administrative access to the device  
D) To disable security settings before analysis

**19. What should forensic investigators do before imaging a hard drive?**

A) Modify system files for easier access  
B) **Ensure the target drive is wiped and formatted appropriately**  
C) Encrypt all files for security  
D) Defragment the disk for better performance

**20. Why is it essential to analyse system logs in forensic investigations?**

A) **They provide timestamps, user activity, and system events for evidence correlation**  
B) They can be used to reset the system settings  
C) They help remove unnecessary files from the investigation  
D) They increase the speed of forensic analysis

This version increases difficulty by requiring more critical thinking and deeper knowledge of forensic processes