

CSF Quiz

Total points 8/10

The respondent's email (**en20it301038@medicaps.ac.in**) was recorded on submission of this form.

✓ What is the primary focus of Live Forensic in digital investigations? * 1/1

- ☐ Analyzing stored data
- ☒ Extracting data from volatile memory
- ☐ Examining archived files
- ☐ Recovering deleted files



✓ What is the purpose of Ram Dumping in Live Forensics? * 1/1

- ☐ Deleting volatile data
- ☒ Capturing the contents of RAM
- ☐ Recovering encrypted files
- ☐ Analyzing network traffic



✓ Which of the following is a commonly used Live Forensic tool for capturing RAM contents? *1/1

- ☐ Wireshark
- ☐ FTK Imager
- ☒ Volatility
- ☐ EnCase



✓ What is the primary source of digital evidence in Network Forensics? * 1/1

- ☐ Hard drives
- ☐ RAM
- ☒ Network traffic
- ☐ Mobile devices



✗ What is the primary source of digital evidence in Network Forensics? * 0/1

- ☐ Hard drives
- ☐ RAM
- ☒ Network traffic
- ☐ Mobile devices



Correct answer

- ☒ RAM



✗ Which tool is commonly used for analyzing network traffic in Network Forensics? *0/1

- ☒ Autopsy
- ☐ SIM cards
- ☐ Optical drives
- ☐ RAM



Correct answer

- ☒ SIM cards

✓ In Mobile Forensics, what does SIM Forensic involve? * 1/1

- ☐ Analyzing mobile applications
- ☒ Recovering data from SIM cards
- ☐ Examining GPS data
- ☐ Decrypting encrypted messages



✓ Which tool is commonly used for extracting data from mobile devices in Mobile Forensics? *1/1

- ☐ AccessData FTK
- ☒ Oxygen Forensic Detective
- ☐ Sleuth Kit
- ☐ Snort



✓ What distinguishes Live Forensics from Network Forensics? *

1/1

- ☒ Live Forensics deals with volatile data, while Network Forensics focuses on network traffic. ✓
- ☐ Network Forensics involves RAM analysis, while Live Forensics focuses on file systems.
- ☐ Live Forensics is only applicable to mobile devices, while Network Forensics is for computers.
- ☐ Network Forensics exclusively deals with encrypted data.

✓ In a comprehensive digital investigation, how might Live Forensic, Network Forensic, and Mobile Forensic approaches be integrated?

*1/1

- ☐ By analyzing only one source of evidence to maintain simplicity
- ☐ By using tools that are specific to each approach and not combining results
- ☒ By correlating findings from all three approaches for a holistic view ✓
- ☐ By avoiding Live Forensic altogether as it is considered less reliable.

This form was created inside of Medi-Caps University, Indore.

Google Forms





