

Exam Name - Certified Forensic Analyst (CFA)[™]

Sample Exam

1. Which email client uses .dbx files that a forensic analyst may need to examine?

- A. Microsoft Outlook
- B. Microsoft Outlook Express
- C. Mozilla Thunderbird
- D. Eudora

Answer **B**

2. What is Technical Steganography?

- A. Hiding messages via physical or chemical methods
- B. Hiding messages in written text
- C. Using Java to embed hidden messages
- D. Hiding messages with visual symbols

Answer **A**

3. What is the primary role of computer forensics?

- A. Maximize investigative cost
- B. Harden perimeter security
- C. Monitor employee behavior
- D. Extract, process, and interpret factual evidence for court

Answer **D**

4. What is a rainbow table used for?

- A. Storing email logs
- B. Encrypting message traffic
- C. Converting large wordlists into hashes for password cracking
- D. Storing NetBIOS names

Answer **C**

5. Which system file logs deleted file entries in Recycle Bin when INFO2 is removed?

- A. LOGINFO2
- B. LOGINFO1
- C. INFO2
- D. INFO1

Answer **D**

6. What is the first step in cracking a password?

- A. Generate a wordlist (e.g. via dictionary)
- B. Hash the wordlist
- C. Compare hashed words against target password
- D. Cracker reveals plaintext

Answer **A**