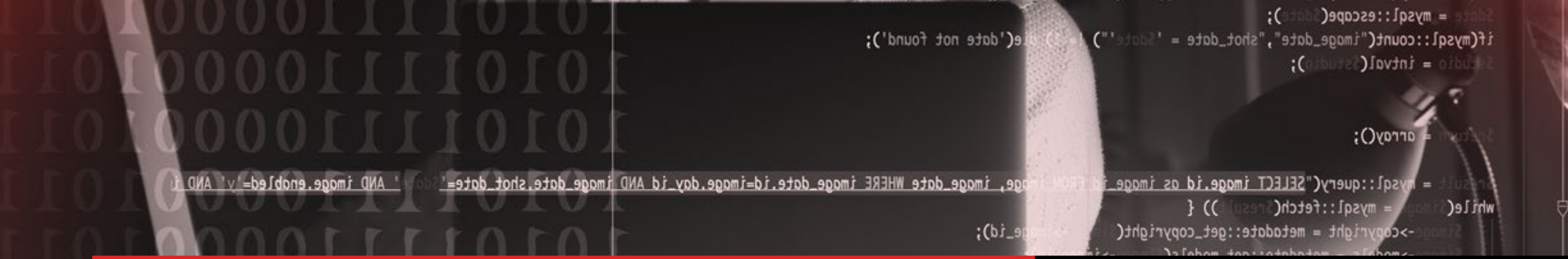

EC-COUNCIL | ASSOCIATE

CERTIPORT®
A PEARSON VUE BUSINESS

CYBER FORENSICS ASSOCIATE EXAM OBJECTIVES

1 Analysis

1.1 Analyze forensic images

1.2 Apply procedural concepts required to use forensic tools

1.3 Apply basic malware analysis using NIST accepted forensic techniques and tools

1.4 Identify anti-forensics techniques

1.5 Determine the important content of event logs in forensics

2 Discovery

2.1 Apply procedural concepts necessary to detect a hidden message inside a picture

2.2 Analyze a conversation between two endpoints from a PCAP file

2.3 Recognize that devices are kept in the same state as they were found

2.4 Determine how to gather evidence in a forensically sound manner

2.5 Apply procedural concepts required to discover evidence on different file systems

2.6 Apply procedural concepts required to gather evidence on different operating systems

2.7 Identify proper steps in network capture

2.8 Given a scenario, determine evidence of email crimes

3 Evidence

3.1 Determine and report logon/logoff times for a specific user

3.2 Verify the authenticity of evidence (e.g., hash value)

3.3 Summarize the proper handling of evidence

3.4 Outline the process for creating a forensically sound image

3.5 Apply evidence collection to the chain of custody

3.6 Discriminate between a live acquisition and static acquisition

4 Documentation and Reporting

4.1 Apply forensic investigation methodology

4.2 Identify the steps necessary to validate an emergency contact list for incident response

4.3 Analyze a scene to determine what should be visually documented

4.4 Report findings from a malware analysis

4.5 Identify the elements of a complete forensics report

4.6 Communicate the results of an investigation to an internal team

5 Cyber Forensics Fundamentals

5.1 Identify different types of cybercrimes

5.2 Communicate incident handling and the response process

5.3 Distinguish between steganography and cryptography

C|FA™
CYBER FORENSICS ASSOCIATE