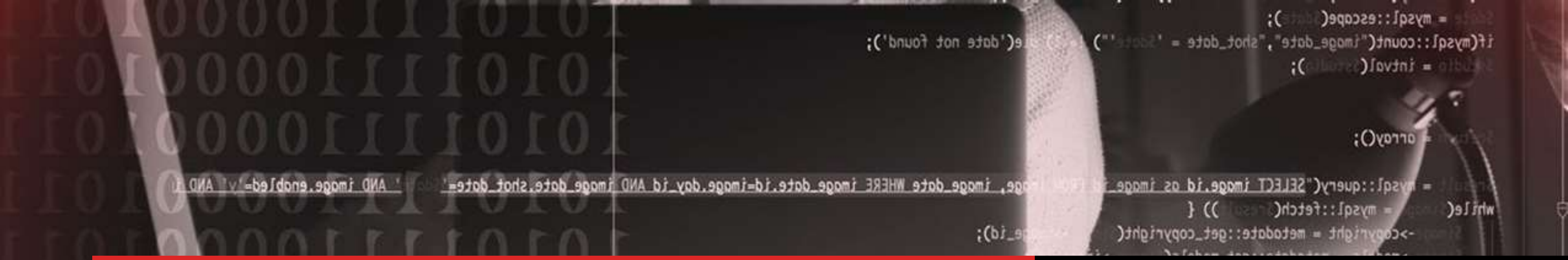

EC-COUNCIL | ASSOCIATE

MODERN THEORY INSTITUTE

Modern Education for the Evolving Learner

CYBER FORENSICS ASSOCIATE EXAM OBJECTIVES

1 Analysis

11 Analyze forensic images

12 Apply procedural concepts required to use forensic tools

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

14 Identify anti-forensics techniques

15 Determine the important content of event logs in forensics

2 Discovery

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

22 Analyze a conversation between two endpoints from a PCAP file

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

24 Determine how to gather evidence in a forensically sound manner

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

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

27 Identify proper steps in network capture

28 Given a scenario, determine evidence of email crimes

3 Evidence

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

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

33 Summarize the proper handling of evidence

34 Outline the process for creating a forensically sound image

35 Apply evidence collection to the chain of custody

36 Discriminate between a live acquisition and static acquisition

4 Documentation and Reporting

41 Apply forensic investigation methodology

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

43 Analyze a scene to determine what should be visually documented

44 Report findings from a malware analysis

45 Identify the elements of a complete forensics report

46 Communicate the results of an investigation to an internal team

5 Cyber Forensics Fundamentals

51 Identify different types of cybercrimes

52 Communicate incident handling and the response process

53 Distinguish between steganography and cryptography

CFA™

CYBER FORENSICS ASSOCIATE