GAQM®
Global Association for Quality Management

Certified Forensic Analyst (CFA)

Module Information

www.gaqm.org

What Modules are covered?

Module 1 - The Goal of the Forensic Investigation

The Module reviews several reasons why an investigation is needed and the plan of that investigation, based on those reasons. It also reviews the impact of the action that resulted in the complaint.

Module 2 - How to Begin a Non−Liturgical Forensic Examination

One of the first things to consider is: Do you need to isolate equipment or files? If yes, you need to move quickly on this in order to preserve any possible evidence. What you preserve and find on the equipment, most likely a PC, will be the basis of your forensic examination.

Module 3 - The Liturgical Forensic Examination:Tracing Activity on a Windows−Based Desktop

Gathering evidence for prosecution purposes is really the mode you should consider operating in when a forensic examination is needed

Module 4 - Basics of Internet Abuse

The following material was developed with a specific objective: to assist an investigator, auditor, security professional, or law enforcement professional in finding clues about a suspect's Internet activities.

Module 5 - Tools of the Trade

Ths Module addresses, discusses, and examines the tools used to secure a system throughout all stages of an incident. It also analyzes and groups these tools into three distinct groups: detection, protection, and analysis tools.

Module 6 - Network Intrusion Management and Profiling

The Module is is designed provide a guide for developing an intrusion management strategy within the Computer Emergency Response Team (CERT) function. is designed provide a guide for developing an intrusion management strategy within the Computer Emergency Response Team (CERT) function.

Module 7 - Cyber Forensics and the Legal System

The Module is developed to assist the reader in understanding and identifying where there may be problems in handling information to build a case, whether that information is committed to paper recorded on electronic media, or retained in a person's memory.

Module 8 - Federal and International Guidelines

There has also been a corresponding increase in the difficulty in catching computer criminals. Thereare a number of reasons why this is so.

Module 9 - Searching and Seizing Computers

The NIPC emphasizes the recommendation that all computer network systems administrators check relevant systems and consider applying the updated patches as necessary, especially for systems related to e−commerce or e−banking/ financial businesses.

Module 10 - Computer Crime Policy and Programs

With the explosive growth of the Internet worldwide, computer crimes increasingly are prone to have international dimensions. Some of the challenges faced by law enforcement on the international fronts

Module 11 - International Aspects of Computer Crime

The Computer Crime and Intellectual Property Section of the Department of Justice submitted comments in response to the request of the Federal Trade Commission ("FTC")

Module 12 - Privacy Issues in the High−Tech Context

The rapid growth and integration of the telecommunications infrastructure has made all of these sectors interdependent, and in the process created unprecedented risks.

Module 13 - Critical Infrastructure Protection

The national defense, public safety, economic prosperity, and quality of life have long depended on the efficient delivery of essential services — energy, banking and finance, transportation, vital human services, and telecommunications.

Module 14 - Electronic Commerce: Legal Issues.

The Electronic Commerce Working Group (ECWG) of the Department of Justice consists of lawyers from throughout the Department who are in regular contact to discuss legal issues related to electronic commerce.

Module 15 - Legal Considerations

Federal prosecutors know that deciding whether to prosecute a particular case requires the exercise of judgment and discretion, which can take years of experience to develop

Module 16 - Encryption

The nation's policy on encryption must carefully balance important competing interests. Department of Justice has a vital stake in the country's encryption policy because encryption may be used not only to protect lawful data against unauthorized intruders.

Module 17 - Intellectual Property

Federal prosecutors know that deciding whether to prosecute a particular case requires the exercise of judgment and discretion, which can take years of experience to develop.

Module 18 - Forensics Tools

In a perfect world, we would be able to protect against all possible vulnerability areas with the use of a tool, or tools.

Module 19 - Forensic and Security Assessment Tools

The Modules provides an additional resource to the reader. It lists many of the companies offering software/utilities for use in computer forensics.

Module 20 - How to Report Internet−Related Crime

Internet−related crime, like any other crime, should be reported to appropriate law enforcement investigative authorities at the local, state, federal, or international levels, depending on the scope of the crime..

Module 21 - Internet Security

The Department of Justice continually provides informal guidance to prosecutors and investigators as they work through complex substantive, procedural and practical elements of intellectual property crime cases.

(End of page)