



FOR100 Fundamental Forensics for Auditors and Info Security Professionals

CPE 14.5

Two day Seminar (Seminar can be offered as a one day overview, with reduced content)

Description: Traditional forensics professionals use fingerprints, DNA typing, and ballistics analysis to make their case. Infosec professionals have to develop new tools for collecting, examining and evaluating data in an effort to establish intent, culpability, motive, means, methods and loss resulting from e-crimes. This overview seminar will introduce the attendee to the broad field of cyber forensics and present the various tools and techniques designed to maintain control over organizational assets, digital or otherwise. This seminar covers computer forensics theory and methodology. It is not limited to the use of a specific software tool.

Audience: This seminar is intended for internal and external audit professionals, General Counsels, Chief Security Officers, Controllers, InfoSec and law enforcement professionals, anyone interested in obtaining a better understanding of and general introduction to cyber forensics.

Prerequisites: Attendees should possess a basic understanding of information technology concepts. Learning level – basic. No advanced preparation is required for this seminar.

Learning Outcomes: After completing this seminar, participants will be able to:

- Identify, establish and maintain a physical "chain of custody."
- Pinpoint computer security risks and remedies.
- Determine incident responses and priorities in a cyber forensic investigation.
- Develop policies for the preservation of computer evidence.
- Implement solid computer forensics processing methods and procedures.
- Develop the documentation of computer forensics findings for executive management review.
- Coordinate Forensic Pre-Incident Preparation.
- Identify, establish and maintain a physical "chain of custody."
- Determine procedures necessary for gathering of all pertinent "Live" information.
- Identify volatile data, photos, physical media, and log files.



- Perform forensic acquisition of physical media.
- Identify various forensic toolkits and associated methodologies.
- Determine procedures necessary to conduct sound forensic analysis of the collected information.
- Identify essential components of a forensic analysis report.
- Communicate findings from a cyber forensic investigation to non-technical audiences.

Course Outline:

- Cyber Forensics Defined
- Junk Science Attack and the Investigator
- Rules of Evidence – Importance and Application to Forensic Investigations
- Establishing a Credible Chain of Custody
- Burn the Witness – Will You Be a Victim?
- Beginning an Investigation – Taking the Critical, Correct First Steps
- Investigation Methodology – The Good, the Bad, and the Dangerous
- Essential Steps in Preparing and Conducting an Investigation
- Creating a Safety Net
- Creating a Forensic Start-up Disk
- Preparing the Evidence Drive on the Processing Machine
- The Forensic Process - Taking Control of the Computer and Its Environment.
- Potential Exposures – Minimizing Your Risk and Exposure
- Uncovering Digital Evidence – Where Is It and How Do I Find It?
- Computer DNA – All You Need To Know
- Documentation Methodologies – Preserving Evidence and Creating Audit Trails
- I've Gathered Evidence Now What?
- Presenting the Evidence Report - Successfully
- Summary

Dr. Marcella's seminar is based on research and findings from his book, *Cyber Forensics*, published by Auerbach Publications, ISBN 0-8493-0955-7.

www.businessautomationconsultants.com/published-books.html