Computer Forensics Education Offerings:

Computer Forensics - File System Analysis:

This course examines the structures of the most common operating systems in use today: File Allocation Table (FAT), NTFS (New Technology File System), and EXT3. The following topics will be explored for each:

1. File System Structure
2. File Allocation Methods and Algorithms
3. File System Meta-Data
4. Process of Deletion and Recovery of Files.
5. Time and Date Stamp Issues

This course can be offered as a lecture or hands-on lab. It can be customized to suit the needs of your organization and experience level of the audience.

Computer Forensics Capability Development:

This course outlines the process of enabling your organization to conduct computer forensic examinations. Some of the topics being explored in this section include:

1. Forensic Equipment Recommendations: The process of equipment acquisition does not end after the initial purchase. This course will discuss the basic items needed at inception as well as planning for the future. Budgeting and sources of funding will also be discussed.
2. Training: Developing computer forensic capabilities for your organization requires a significant investment in human capital. Training and certification options will be presented. Cost efficient ways of maintaining a continual stream of training will be discussed.
3. Physical Structure Requirements: Depending on the goals of your organization, you may want to allocate physical space to house computer forensic equipment and conduct examinations. This section will discuss recommendations for developing a computer forensics lab and the facilities issues that accompany this. Additionally, issues of business continuity disaster recovery and redundancy for this newly created section will be presented.
4. Policy and Procedure Creation: The development of policy and procedures to conduct valid examinations with good scientific practices is a fundamental component to successful computer forensics capabilities. This section will provide the framework and a policy and procedure template for your organization's needs. (Upon request, our consultants can also directly assist in the drafting of your policy and procedures).

This course can be customized to suit the needs of your organization.

Live System Analysis:

In today's computer environment, examiners are often faced with the necessity of examining live running processes and acquiring volatile data. This course will cover the times where conducting live analysis is necessary. Additionally, this course will also cover the methods necessary to accomplish acquisition of live / volatile data. The topics covered in this course include:

1. Evaluating a running system and determining the need for live analysis and volatile data acquisition.
2. Methods for acquiring running and relevant system processes.
3. Methods for acquiring Random Access Memory.
4. Methods for acquiring Hard Disk Drive or file system volume images in the live environment.
5. Order of Action for least intrusive method of acquisition.
6. Report writing following live system analysis:
    a. Justifying your actions.
    b. Documenting the order of action and analysis process.
    c. Addressing changes to the file system and live system state.

This course can be offered as a lecture or hands-on lab. It can be customized to suit the needs of your organization and experience level of the audience.

Network Forensics / Data Tapping:

Often investigations necessitate the acquisition of data located on critical mission servers. Taking a server offline that is critical to the business continuity operations of an organization is often not warranted or necessary. Acquiring data in this environment presents forensic analysts with certain challenges. This course will cover the following topics:

1. Evaluating the critically of server operations and determining a strategy for acquiring evidentiary data.
2. Acquiring limited network data.
3. Acquiring entire server images.
4. Options for acquiring large storage devices.
5. Live Networking Monitoring – Data Tapping.

This course can be offered as a lecture or hands-on lab. It can be customized to suit the needs of your organization and experience level of the audience.