

University of Washington, Tacoma  
Computer Forensics Certificate Program (Non-Credit)

**Course Three: Applied Computer Forensics: Case Studies**

Case Management Tools

Famous Case Examples

Capstone: Mock Cases/Lab Exercises

- Sample scenarios: intrusion, destruction of data, missing data
- Sample litigation contexts: civil, criminal, internal (organizational)

**Introduction**

Applying findings from a computer forensic analysis is only the first step for the high tech investigator. Computing investigations consist of the combining of recovered digital evidence with other resources such as system log files, recovered physical evidence, and learning the suspect's methods of operations. Knowing how to put all aspects of an investigation together requires the analyzing of collected evidence, organization, and leadership skills. Of all skills necessary for a successful high tech investigation, it is leadership, that is, knowing who to seek out that has additional technical skills to solve the case, then putting all together into a presentation.

**Student expectations and requirements:**

- Students are to complete one or more extensive studies of a computer forensic examine and investigation.
- Students must have the ability to define the elements of systems analysis and project management methodologies to high tech investigations.
- Students will build their curriculum vitae of their professional experiences as applied to information technology and high tech investigations.
- Students will practice leadership exercises in managing high tech investigations and make presentations to non-technical audiences.
- Students will define their organization's structures and identify their organization's subject matter experts.
- Students will know how to research new technologies to determine how to investigate potential or known investigation vulnerabilities.

Class attendance of 80% required to complete the course.

## Class 1: Class Orientation

Recommended Reading: none

- Problem Solving using Systems Analysis for High Tech Investigations
- Goals and objectives of class
- Investigation Planning
- Review of computer forensics processes
- Tools overview
- CV exercise and assignment
- Bona Fides and the Affidavit
- Case example discussion

Performing high tech investigations requires the ability to problem solve. Applying classic systems analysis processes to an investigation will provide cost effective methods of collecting and analyzing digital evidence. From the systems analysis process of planning an investigation the use of project management tools will assure successful completion of the investigation.

## Class 2: Digital Evidence Quantified and Presentation

Recommended Reading: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, by Eoghan Casey

- Exercise Systems Analysis problem discussion
- Alternative sources of evidentiary data
- Tools used for discovery demands
- Advance report writing techniques and presentations
- Case example discussion

Learning how to determine the scope of a high tech investigation is the most critical stage. If the scope of the investigation is too small important facts maybe missed. If the scope is too large, it will become difficult to manage and confusing. The investigator needs to know what tools that are available that will help in determining how to define the scope of an investigation.

## Class 3: Digital Evidence from an Enterprise

Recommended Reading: Incident Response and Computer Forensics, Second Edition, Chris Prosise, Kevin Mandia, Matt Pepe

- Exercise Systems Analysis problem discussion
- Sources of digital evidence, log files
  - Firewall
  - Proxy Server
  - VPN, etc.
- Log file preservation techniques
- Keystroke capturing techniques
- Network traffic capturing techniques
- Case example discussion

Knowing the available assets for a high tech investigation is extremely important. In any high tech investigation knowledge is the key factor for a successful investigation. It is important for the high tech investigator to understand the network technologies and the people that manage them. The high tech investigator must take a leadership role in directing these skilled people in

extracting, recovering, preserving, analyzing, and presenting the huge volumes of data that will become digital evidence.

#### Class 4: Digital Evidence Analysis and Lab Operations

- Recommended Reading: To be determined
- Exercise Systems Analysis problem discussion
- Time correlation techniques with data files and network logs
- Putting a suspect at the computer
- Computer forensics Lab Management, Procedures, and Configuration Management
- Building business cases for computer forensics operations
- Applying Quality Assurance and Quality Control to a high tech investigation
- Case example discussion

Analyzing data from several source, be it from a computer forensic disk examination to network log files will provide the investigator unique insight of a suspect's wrongful activity. Computer forensics labs must be maintained to a professional standard to ensure that digital evidence is well protected and correctly analyzed. To maintain a computer forensics lab will require the development of a business plan that must be updated regularly.

#### Class 5: Suspect Profiling Techniques

- Recommended Reading: To be determined
- Exercise Systems Analysis problem discussion
- Profiling suspects through collected computer and network data
- Advance computer forensics hardware overview
- Case example discussion

Learning the personality of the suspect of a computer crime is essential. Since criminals are creatures of habit it is necessary to learn how to recognize patterns of behavior. The examination of digital evidence from a disk drive and network log files can provide interesting facts and predictable behavior of a suspect. Knowing what tools that are available to aid in predicting a suspect's behavior and cause-and-effect relationships will enhance the investigation analysis process.

#### Class 6: Network Forensics

- Recommended Reading: Incident Response and Computer Forensics, Second Edition, Chris Prosise, Kevin Mandia, Matt Pepe
- Exercise Systems Analysis problem discussion
- Network forensics analysis tools
- Intrusion response techniques applied to forensics
- Intrusion live analysis techniques
- Case example discussion

With the increased use of the Internet it is becoming necessary for computing investigators to know how to correlate recovered disk evidence with network log data. Finding how a network server was attacked and locating related data from a suspect's computer will provides the quality information on how to build a civil and criminal case of an incident.

## Class 7: Discovery Processing

Recommended Reading: To be determined  
Exercise Systems Analysis problem discussion  
Criminal vs. Civil High Tech investigations  
Litigation support  
Case management  
Managing lawyers  
Case example discussion

Because of the increase of litigation in our society it is necessary for the high tech investigator to know how to communicate technical findings from digital evidence to a lawyer and paralegal. It is also important to know how to take charge and project-manage large scale investigations for lawyers.

## Class 8: Case Problem Identification

Recommended Reading: To be determined  
Case project  
E-Discovery product review of Attenex

Having experience in identifying the problem for high tech incidents is another step for a successful investigation. Knowing what tools to apply to a large scale investigation will help keep it on track from the beginning to the end. Asserting project management and leadership skills for the investigation will ensure successful findings.

## Class 9: Case Solution and Processing

Recommended Reading: To be determined  
Case project  
E-Discovery product review of Searchlight

Knowing how to map for success is another important factor for investigation. Applying the many tools, managing the subject matter experts, and communicating to management are the three pillars for every investigation.

## Class 10: Case Study

Recommended Reading: To be determined  
Significant Computer Case Discussion  
Case analysis presentation

An important aspect of high tech investigations is having the ability of knowing how to explain an incident or crime to non-technical people. The high tech investigator must learn how to gauge the technical information from the investigation for the intended audience. The investigator must become the teacher for items, issues, and technologies that the audience doesn't understand. Every effort must be made by the investigator to help the audience, such as lawyers, judges, and corporate management in understanding how the incident or crime occurred and how the technology works.