CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Computer and Network Forensics: A Master's Level Curriculum

Key Message: Students learn how to combine multiple facets of digital forensics and draw conclusions to support full-scale investigations.

Executive Summary

Over the past five years, CERT's forensics team has been actively involved in real-world events and investigations as well as conducting applied research, developing guides and tools, and teaching. They came to realize that there was no academic institution that offered the education necessary for forensic analysts, network and system administrators, and law enforcement to address the forensic challenges they face when investigating sophisticated and constantly changing security incidents.

In this podcast, Kris Rush, a member of CERT's Forensics Team, discusses a new forensics and incident response track that is being offered through Carnegie Mellon's Information Networking Institute as part of the Master of Science in Information Networking degree program. The five-course curriculum combines foundational concepts with actual forensics investigations. Students walk out the door with practical experience and concrete skills that they can apply immediately.

PART 1: WHAT A STUDENT CAN EXPECT; PRACTICAL HANDS-ON EXPERIENCE

Motivation for a Graduate Level Forensics Curriculum

CERT's forensics work has evolved over the last five years, from outreach and education to working with law enforcement and the U.S. federal government on actual cases.

CERT staff is regularly called upon to tackle challenging areas and solve new problems.

CERT realized that there was no academic institution that offered the education necessary to tackle these areas and problems.

CERT's objective is to provide students with concrete skills and to develop the ability to perform forensic investigations, for either law enforcement or for their organizations.

Student Prerequisites

Students typically have a general interest in computers and a natural curiosity about how they work.

They will often have a computer background with experience in network management, software development, or other related technical skills.

What a Student Can Expect

Students obtain a general understanding of

- forensics fundamentals
- what it means to be a forensic investigator or analyst
- how to do a thorough investigation (at the disk level) and forensic casework

Students can tailor the outcome to their abilities. For example, those with greater technical expertise can learn how to develop new tools and techniques that further the field of computer forensics.

Five Courses in the Curriculum

The courses that currently make up the curriculum include

- Host-Based Forensics
- Advanced Host-Based Forensic Analysis
- Network Forensics
- Advanced Network Analysis
- Event Reconstruction and Correlation

PART 2: HOST-BASED FORENSICS

Course Content

This course teaches the challenges and skills required to perform a forensic investigation on a single host. This includes

- planning for conducting an investigation
- determining what evidence is needed
- acquiring evidence
- preserving and protecting evidence and keeping it clean and secure
- working with appropriate copies of evidence
- acquiring a forensically sound image of a computer disk
- forensic analysis

Law enforcement applications include

- looking for contraband material (such as illicit images or credit card numbers)
- identifying evidence of malicious code developed on a computer being investigated
- building proof of identity theft
- building proof of access to confidential information

Building competence in communication and reporting are essential because it is critical to be able to convey the findings of a forensic investigation to a wide range of audiences.

Interfacing with Law Enforcement

Network and system administrators are taught how to interface with law enforcement in a prerequisite course titled Applied Information Assurance. This course discusses the legal framework for computer forensics including

- capturing logs
- capturing network traffic
- handling specific events
- when to involve law enforcement
- how to maintain the value and integrity of evidence

Advanced Host-Based Forensic Analysis

This course changes from time to time to reflect the latest challenges. Current topics include

- data carving, which involves carving up a disk and piecing elements of files back together that have been found

in unallocated sectors
- small-scale digital devices and how they may yield useful forensic evidence (for example, GPS devices)

PART 3: NETWORK FORENSICS

Course Content

This course teaches the skills required to perform a forensic investigation of a network. This includes

- collection and analysis of network evidence associated with a network event. This includes
  - netflow for statistical analysis
  - identification of the behavioral characteristics of traffic
  - deep packet inspection
- analysis of static and dynamic malware. Given most malware relies on networks to propagate, such analysis can help identify where the attacker comes from and where exfiltrated information goes.
- capture of network data
- implications of various collection methods on the types of data collected

Dealing with Missing Network Data

Many times, analysts do not have access to all of the networks and network data involved in the forensic event.

Law enforcement analysts can reach out to vendors, other providers, and national governments and agencies.

In a corporate environment, analysts can ask the following questions:

- What data was being exfiltrated?
- What services were being exploited?
- Were exploits successful?
- Have we seen other incidents that use this same malware?

Answers to these questions can provide insight even when you can't access all global network data.

Advanced Network Analysis

Most students who graduate with this specialty will be working in business environments, not law enforcement. Their responsibilities will include network traffic analysis and incident handling as well as forensic investigations.

This course deals with analyzing traffic across large networks including

- collection and aggregation of traffic on large networks
- large-scale analysis of network and packet data, looking for anomalous and malicious behaviors
- analysis of a series of sessions related to an attack

PART 4: EVENT RECONSTRUCTION AND CORRELATION; STUDENT FEEDBACK

Course Content

This course

- enables students to conduct a soup-to-nuts, complete forensic investigation with a mixture of both lab and lecture
- ties together all of the elements of the preceding four courses into an actual, full-scale investigation

Students figure out how to combine multiple facets of digital forensics and draw conclusions regarding a forensic event or law enforcement case.

Early Student Feedback

Curriculum designers and instructors want to make sure that students are equipped to control networks, secure enterprises, and handle massive incidents. To address this need, the curriculum teaches concrete skills that students can put to work immediately.

This is the first year of this new curriculum. Students are surprised with course breadth and depth and the standards to which they are held, including having to solve real problems and deliver results.

In the advanced courses, students are expected to conduct real research and present new ways to solve problems. They are intrigued by having the opportunity to affect a community of practice.

Resources

Carnegie Mellon's Information Networking Institute

Computer Forensics and Incident Response track curriculum web site

CERT's Forensics web site

CERT Podcast: Computer Forensics for Business Leaders: A Primer

CERT Podcast: Computer Forensics for Business Leaders: Building Robust Policies and Processes