

Incident Response

Intermediate • Three-day Instructor-led Class



AccessData[®]

This intermediate AccessData[®] training class provides the knowledge and skills necessary to use AccessData and other industry standard tools to conduct fundamental Incident Response actions on Microsoft Windows systems. Participants will learn the entire Incident Response lifecycle, from Preparation through Lessons Learned. Participants will also learn how to capture volatile and non-volatile data to properly analyze an incident.

During this three-day theory and hands-on class, participants perform the following tasks on systems running the Windows operating system:

- Use clean static binaries.
- View network connections.
- Open a list of running processes.
- Identify DLL's used by programs.
- Show a system's hostname.
- Determine what programs are scheduled to automatically start.
- View all programs and services scheduled to execute at startup.
- Identify listening ports connected to running processes.
- Export and analyze target registry hives with Registry Viewer[®].
- Locate malware not identified by antivirus signatures.
- Manipulate Windows Event Logs, including:
 - Extracting them from a running system.
 - Repairing corrupted event logs.
 - Analyzing logs in relation to an incident.
- Use FTK Imager[®] to perform the following functions:
 - Preview evidence.
 - Export data.
 - Hash data.
 - Acquire a live image of evidence data.
- View command line arguments used by malicious programs.
- Accurately identify various intrusion vectors

Participants will also explore the following areas of incident response program development and the incident response lifecycle:

- The incident response plan
- Equipment and resource requirements
- Legal advice resources
- Incident types and priorities
- Incident identification
- Containment strategies
- Host- and network-based analysis strategies
- Intruder motivations
- Evidence collection, handling, and preservation
- Volatile and non-volatile data sources
- Damage assessments
- Proper documentation

Prerequisites

This hands-on class is intended for computer security professionals who meet the following requirements:

- A basic working knowledge of AccessData Forensics Toolkit[®] (FTK[®]), Registry Viewer, and FTK Imager
- Basic knowledge of computer forensics investigations and experience with imaging digital media
- Familiarity with the Microsoft Windows environment
- AccessData Forensic BootCamp

Class Materials and Software

You will receive the student training manual and a CD containing class material.

Module 1: Introduction

Topics

- Introductions
- Class materials and software
- Prerequisites
- Class outline
- Class Information
- Sources of additional information

Module 2: Incident Response Preparation

Objectives

- Define an incident.
- Determine the need for Incident Response.
- Identify and explain each phase of the Incident Response life cycle.
- Explain the need for Incident Response preparation.
- Understand policies, plans, and procedures.
- Outline optimal team organization.
- Understand needed equipment and resources.
- Craft prevention strategies.

Module 3: Preparing Tools and Communications

Objectives

- Explain what a trusted toolkit is.
- Understand the need for a trusted toolkit.
- Explain why system binaries should not be used.
- Define trusted binaries.
- Identify how to use trusted binaries on a potentially compromised system.
- Describe types of tools that should be in an Incident Response toolkit.
- Explain why and how communications can be disrupted during an incident.
- Define Out of Band Communications.
- Describe the need for Out of Band Communications.

Module 4: Incident Types, Sources, and Signs

Objectives

- Describe each of the following incident categories:
 - Denial of Service
 - Malicious Code
 - Unauthorized Access
 - Inappropriate Usage
 - Multiple Component
- Understand the signs of an incident.
- Know the challenges of determining if an incident occurred.
- Define “Precursor.”

- Understand how a precursor can portend an incident.
- Define “Indicator.”
- Understand how an indicator can show that an incident has occurred.
- Explain how indicators can be erroneous.
- List the potential sources of an incident and their potential motivations:
 - Structured Attackers
 - Unstructured Attackers
 - Insiders

Module 5: Intrusion Identification and Prioritization

Objectives

- Define required steps in intrusion identification.
- Explain why accuracy can be challenging.
- State why incidents may not be clearly identifiable.
- Describe how the initial analysis can determine the scope of the incident.
- Explain steps that improve accuracy in the identification process.
- Identify the two factors that determine incident priority.
- Describe each severity rating level.
- Explain the best method of incident prioritization.

Module 6: Evidence

Objectives

- Define the term “Evidence.”
- Understand why evidence is critical in Incident Response.
- Explain the proper way to gather evidence.
- Determine the proper order of evidence collection.
- Explain why evidence handling is as important as collection.
- Define “Chain of Custody.”
- Explain the importance of chain of custody.
- Understand the required fields in a chain of custody form.
- Explain the difference between logical and physical images.
- Describe volatile data and the associated sources.
- Describe non-volatile data and the associated sources.

Lab

- List the logical partitions in the Windows My Computer display.
- Show the physical drives in the Windows Disk Management.
- Determine which logical partitions are on which physical drives.
- Utilize FTK Imager to create an image of a physical device.

Module 7: Volatile Data

Objectives

- Explain the purpose of a trusted command shell.
- Learn how to open a trusted command shell.
- Understand how to check for logged on users.
- List open ports and network connections.
- View running processes.
- List running services.
- Find out what tasks are scheduled to execute.
- Describe the importance of volatile memory.
- Understand how to image volatile memory.

Lab

- Open a trusted command shell.
- Execute a program from the trusted command shell.
- View system processes in Windows Tasklist.
- Execute Pslist.exe from the trusted command shell.
- Use the Process Explorer program from the trusted command shell.
- Use netstat.exe from a trusted command shell to show network status and connections.
- Run fport.exe to determine which processes are listening to specific ports.

Module 8: Non-volatile Data

- Describe live data collection.
- Understand the proper times to use live data collection.
- Describe non-volatile data.
- Use FTK Imager to:
 - Export logical files on a running system.
 - Collect protected files on a running system.
- Understand what makes up the Windows Event logs.
- Describe the Windows registry.
- Identify what useful Incident Response data can be found in the Windows registry.
- Execute basic examination of binary files.

Lab

- Use FTK Imager to preview a computer's file system.
- Export the Windows Event logs from a running system.
- Repair the corrupted Windows Event logs.
- Review the Windows Event logs for useful data.
- Export the Windows registry.
- View the Windows registry with Registry Viewer.

Module 9: Incident Notification, Documentation, and Damage Assessment

Objectives

- Explain the reasons proper incident notification is critical.
- Determine who needs to be notified within the organization.
- Determine who needs to be notified outside the organization.
- Explain the importance of documentation.
- Understand the pros and cons of an Incident Response database.
- Identify necessary victim system information to gather.
- Define "Damage Assessment".
- Understand the purpose and need for a damage assessment in the Incident Response process.
- Describe what is included in a damage assessment.
- Identify potential pitfalls with inaccurate damage assessments.

Module 10: Containment, Host Analysis, and Network Analysis Strategies

Objectives

- Understand containment in the Incident Response framework.
- Define the goal of containments.
- Describe various strategies for achieving containment.
- Explain how to choose the best containment strategy.
- Determine host analysis approach options.
- Explain importance of volatile data in host analysis.
- Describe useful non-volatile data for host analysis.
- Determine network analysis approach options.
- Understand network baselines.
- Describe the difference between network full-content and connection monitoring.
- Understand how to utilize network analysis to find affected hosts.

Lab

- Show the contents of user startup folders with FTK Imager.
- Show the content of the startup folder for all users with FTK Imager.
- Use autorun.exe within a trusted command shell to show all programs and services set to run on startup.
- Use listdlls.exe from a trusted command shell to view processes and their associated DLLs.

Module 11: Identifying the Attack Vector and the Attacker

Objectives

- Define “Attack Vector.”
- Understand the importance of locating an attack vector.
- Describe challenges in identifying the attack vector.
- Explain the process of locating the attack vector.
- Describe the rationale of identifying the attacker.
- List potential steps in the identification process.
- Explain the purpose of an attacker profile.
- State pertinent information to help create the attacker profile.
- List research resources and describe how to use them.
- Understand the need for clandestine research.
- Describe proper clandestine research processes.

Module 12: Practical 1

This module requires that you apply previously learned information to analyze a system that is potentially compromised.

Module 13: Eradication and Recovery Phases

Objectives

- Define “Eradication.”
- Define “Recovery.”
- Explain the eradication and recovery phases of the Incident Response lifecycle.
- List potential eradication and recovery actions.
- Be able to decide the correct eradication and recovery steps for the following scenarios:
 - Administrative or root access
 - Non-administrative access
 - Malicious code
 - DDOS
 - Alternate
- List the proper follow-up steps to take after recovery has been implemented.

Module 14: Practical 2

This module builds upon Practical 1. It requires the students to determine if a system has been compromised, locate all volatile and non-volatile evidence, and explain the attack vector.

Module 15: Practical 3

The final practical is a cumulative exercise that requires participants to apply information from the entire class to initiate an Incident Response and successfully execute all steps of the Incident Response lifecycle.

Module 16: Post Incident Activities

Objectives

- Describe “Lessons Learned” as it is applied to Incident Response.
- Explain the purpose of creating lessons learned.
- List the reasons to have a lessons learned meeting.
- Identify how to properly execute a Lessons Learned meeting.
- Define types of data to aggregate after an incident.
- List potential Incident Response metrics.
- Understand the purpose of evidence retention policies.
- Describe the rationale for lengthy evidence retention.

Module 17: AccessData FTK Enterprise Overview

Objectives

- FTK Enterprise Overview
- FTK Enterprise: How it works
- Collecting remote data
- Analyzing non-volatile data
- Analyzing volatile data

For a complete listing of scheduled courses or to register for available courses, see www.accessdata.com.

© 2009 AccessData Corporation – All rights reserved.

Some topics and items in this class syllabus are subject to change. This document is for information purposes only. AccessData makes no warranties, express or implied, in this document. AccessData, AccessData Certified Examiner, ACE, Distributed Network Attack, DNA, Forensic Toolkit, FTK, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are registered trademarks of AccessData Corporation in the United States and/or other countries. Other trademarks referenced are property of their respective owners.