



**AccessData<sup>®</sup>**

# **AccessData Course Catalogue**



Unless otherwise noted, the companies, organizations, products, email addresses, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, email address, person, places, or events is intended or should be inferred. Complying with all copyright laws is the responsibility of the user.

No part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) or for any purpose without the express written permission of AccessData Corporation.

AccessData may have trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from AccessData, the furnishing of this document does not give you any license to these trademarks, copyrights, or other intellectual property.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright © 2010 AccessData Group, LLC.

All rights reserved.

AccessData Course Catalog  
June 13, 2010

AccessData Group, LLC.  
384 South 400 West  
Lindon, UT 84042  
U.S.A.  
[www.accessdata.com](http://www.accessdata.com)

## AccessData Trademarks

AccessData is a registered trademark of AccessData Corp.

AccessData Certified Examiner is a registered trademark of AccessData Corp.

ACE is a registered trademark of AccessData Corp.

Distributed Network Attack is a registered trademark of AccessData Corp.

DNA is a registered trademark of AccessData Corp.

Forensic Toolkit is a registered trademark of AccessData Corp.

FTK is a registered trademark of AccessData Corp.

FTK Imager is a trademark of AccessData Corp.

Password Recovery Toolkit is a registered trademark of AccessData Corp.

PRTK is a registered trademark of AccessData Corp.

Registry Viewer is a registered trademark of AccessData Corp.

Ultimate Toolkit is a registered trademark of AccessData Corp.

UTK is a registered trademark of AccessData Corp.

## Third-Party Trademarks

All third-party trademarks belong to their respective owners.



# CONTENTS

## Preface: Building Your Custom Course

Forensics Fundamentals . . . . .	2
BootCamp—FTK1 . . . . .	3
BootCamp—FTK 3 . . . . .	4
Transition Workshop—FTK 3 . . . . .	5
Case Reviewer . . . . .	6
Windows Forensics—FTK 1 . . . . .	7
Windows Forensics—FTK 3 . . . . .	8
Windows Forensics—Vista . . . . .	9
Windows Forensics Registry . . . . .	10
Internet Forensics—FTK 1 . . . . .	11
Internet Forensics—FTK 3 . . . . .	12
Applied Decryption . . . . .	13
Linux Forensics . . . . .	14
Macintosh Forensics . . . . .	15
Incident Response . . . . .	16
SilentRunner . . . . .	17

## Chapter 1: Forensics Fundamentals

What Is Computer Crime? . . . . .	20
Module Objectives . . . . .	20
Search and Seizure . . . . .	20
Module Objectives . . . . .	20
Introduction to FTK Imager . . . . .	20
Module Objectives . . . . .	21
Computer Terms and Numbering Systems . . . . .	21
Module Objectives . . . . .	21
Physical Characteristics of Digital Storage Media . . . . .	21
Module Objectives . . . . .	21
Partitioning Concepts . . . . .	22
Module Objectives . . . . .	22
Boot Process and Drive Letter Assignments . . . . .	22
Module Objectives . . . . .	23
Formatting to FAT 12, 16, and 32 . . . . .	23
Module Objectives . . . . .	23
File Allocation Table . . . . .	23
Module Objectives . . . . .	24
Saving Files in FAT . . . . .	24
Module Objectives . . . . .	24
Recovering Deleted Files . . . . .	24
Module Objectives . . . . .	25

Write Blockers and Disk Access . . . . .	25
Module Objectives . . . . .	25
Imaging . . . . .	26
Module Objectives . . . . .	26
Introduction to FTK . . . . .	26
Module Objectives . . . . .	26
<b>Chapter 2: BootCamp—FTK1</b>	
Introduction (Installing UTK) . . . . .	28
Module Objectives . . . . .	28
Working with FTK Imager . . . . .	28
Module Objectives . . . . .	29
Working with FTK—Part 1 . . . . .	29
Module Objectives . . . . .	30
Working with FTK—Part 2 . . . . .	30
Module Objectives . . . . .	30
Processing the Case . . . . .	31
Module Objectives . . . . .	31
Narrowing Your Focus . . . . .	32
Module Objectives . . . . .	32
Filtering the Case . . . . .	33
Module Objectives . . . . .	33
Case Reporting . . . . .	33
Module Objectives . . . . .	33
Registry Viewer Introduction . . . . .	34
Module Objectives . . . . .	34
Working with PRTK . . . . .	34
Module Objectives . . . . .	34
<b>Chapter 3: BootCamp—FTK3</b>	
Introduction (Installing FTK 3) . . . . .	36
Module Objectives . . . . .	36
Working with FTK Imager . . . . .	36
Module Objectives . . . . .	37
Working with Registry Viewer . . . . .	37
Module Objectives . . . . .	37
Working with FTK—Part 1 . . . . .	38
Module Objectives . . . . .	38
Working with FTK—Part 2 . . . . .	38
Module Objectives . . . . .	39
Processing the Case . . . . .	39
Module Objectives . . . . .	40
Narrowing Your Focus . . . . .	40
Module Objectives . . . . .	40

---

Filtering the Case . . . . .	41
Module Objectives. . . . .	41
Case Reporting . . . . .	41
Module Objectives. . . . .	42
Working with PRTK . . . . .	42
Module Objectives. . . . .	42
<b>Chapter 4: Transition Day—FTK3</b>	
Introduction (Installing FTK 3) . . . . .	44
Module Objectives. . . . .	44
Working with FTK—Part 1 . . . . .	44
Module Objectives. . . . .	44
Working with FTK—Part 2 . . . . .	45
Module Objectives. . . . .	45
Processing the Case . . . . .	45
Module Objectives. . . . .	45
Narrowing Your Focus . . . . .	46
Module Objectives. . . . .	46
Filtering the Case . . . . .	46
Module Objectives. . . . .	46
Case Reporting . . . . .	47
Module Objectives. . . . .	47
<b>Chapter 5: Case Reviewer</b>	
Database Management. . . . .	50
Module Objectives. . . . .	50
Working with FTK—Part 1 . . . . .	50
Module Objectives. . . . .	50
Working with FTK—Part 2 . . . . .	51
Module Objectives. . . . .	51
Case Processing . . . . .	51
Module Objectives. . . . .	51
<b>Chapter 6: Windows Forensics—FTK 1</b>	
FTK Overview . . . . .	54
Module Objectives. . . . .	54
Regular Expressions . . . . .	54
Module Objectives. . . . .	54
KFF Management . . . . .	55
Module Objectives. . . . .	55
Windows 9x Registry. . . . .	56
Module Objectives. . . . .	56
Windows 2000 and XP Registries . . . . .	56
Module Objectives. . . . .	56
Registry Access and Concerns . . . . .	57
Module Objectives. . . . .	57

---

---

Working with Registry Viewer . . . . .	57
Module Objectives. . . . .	58
Gathering Evidence and Reporting . . . . .	58
Module Objectives. . . . .	58
The Recycle Bin . . . . .	59
Module Objectives. . . . .	59
Thumbs.db Files . . . . .	60
Module Objectives. . . . .	60
Metadata . . . . .	60
Module Objectives. . . . .	60
Link and Spool Files. . . . .	61
Module Objectives. . . . .	61
PRTK Alternate Features . . . . .	61
Module Objectives. . . . .	62
Encrypting File System. . . . .	62
Module Objectives. . . . .	62
Alternate Data Streams . . . . .	63
Module Objectives. . . . .	63
<b>Chapter 7: Windows Forensics—FTK 3</b>	
Regular Expressions . . . . .	66
Module Objectives. . . . .	66
Windows Registry 101. . . . .	66
Module Objectives. . . . .	66
Windows 2000 and XP Registries . . . . .	67
Module Objectives. . . . .	67
Working with Registry Viewer . . . . .	67
Module Objectives. . . . .	68
Gathering Evidence and Reporting . . . . .	68
Module Objectives. . . . .	68
The Recycle Bin . . . . .	69
Module Objectives. . . . .	69
Thumbs.db Files . . . . .	70
Module Objectives. . . . .	70
Metadata . . . . .	70
Module Objectives. . . . .	70
Link and Spool Files. . . . .	71
Module Objectives. . . . .	71
Alternate Data Streams . . . . .	72
Module Objectives. . . . .	72
Windows XP Prefetch. . . . .	72
Module Objectives. . . . .	72
Working with PRTK . . . . .	73
Module Objectives. . . . .	73

---

PRTK Alternate Features . . . . .	73
Module Objectives. . . . .	74
Encrypting File System. . . . .	74
Module Objectives. . . . .	74
<b>Chapter 8: Windows Forensics—Vista</b>	
Understanding BitLocker Drive Encryption . . . . .	76
Module Objectives. . . . .	76
Working with GUID Partition Tables . . . . .	77
Module Objectives. . . . .	77
Vista Security and File Structure . . . . .	77
Module Objectives. . . . .	77
Windows Vista Registry—Introduction . . . . .	78
Module Objectives. . . . .	78
Windows Vista Registry—Registry File Artifacts . . . . .	78
Module Objectives. . . . .	78
Windows Vista Registry—ReadyBoost and DPAPI . . . . .	79
Module Objectives. . . . .	79
Windows Vista Event Logs . . . . .	79
Module Objectives. . . . .	80
Windows Vista Shadow Copy . . . . .	80
Module Objectives. . . . .	80
Windows Vista Recycle Bin . . . . .	81
Module Objectives. . . . .	81
Windows Vista ThumbCache . . . . .	81
Module Objectives. . . . .	81
Windows Vista Superfetch (Prefetch) . . . . .	82
Module Objectives. . . . .	82
<b>Chapter 9: Windows Forensics Registry</b>	
Registry Utilities . . . . .	84
Module Objectives. . . . .	84
Registry 201. . . . .	85
Module Objectives. . . . .	85
Preliminary Reports . . . . .	86
Module Objectives. . . . .	86
SAM Artifacts . . . . .	86
Module Objectives. . . . .	87
SYSTEM Artifacts . . . . .	87
Module Objectives. . . . .	87
SECURITY Artifacts . . . . .	88
Module Objectives. . . . .	88
SOFTWARE Artifacts . . . . .	88
Module Objectives. . . . .	89

Application Behavior 1 . . . . .	90
Module Objectives . . . . .	90
Application Behavior 2 . . . . .	91
Module Objectives . . . . .	91

**Chapter 10: Internet Forensics—FTK 1**

AOL Instant Messenger . . . . .	94
Module Objectives . . . . .	94
Firefox . . . . .	94
Module Objectives . . . . .	95
Internet Explorer . . . . .	95
Module Objectives . . . . .	95
Yahoo Messenger . . . . .	96
Module Objectives . . . . .	96
Windows Messenger . . . . .	96
Module Objectives . . . . .	96
MSN Messenger . . . . .	97
Module Objectives . . . . .	97
AOL—Information from American Online . . . . .	97
Module Objectives . . . . .	97
AOL—Information from the Computer . . . . .	98
Module Objectives . . . . .	98
AOL—Personal Filing Cabinet . . . . .	98
Module Objectives . . . . .	99
Password Recovery . . . . .	99
Module Objectives . . . . .	99

**Chapter 11: Internet Forensics—FTK 3**

AOL Instant Messenger . . . . .	102
Module Objectives . . . . .	102
Yahoo! Instant Messenger . . . . .	103
Module Objectives . . . . .	103
Windows Live Messenger . . . . .	103
Module Objectives . . . . .	104
MySpace Instant Messenger . . . . .	104
Module Objectives . . . . .	104
Skype . . . . .	105
Module Objectives . . . . .	105
Facebook . . . . .	105
Module Objectives . . . . .	106
Safari . . . . .	106
Module Objectives . . . . .	106
Firefox . . . . .	107
Module Objectives . . . . .	107

---

Internet Explorer . . . . .	107
Module Objectives. . . . .	108
LimeWire . . . . .	108
Module Objectives. . . . .	108
<b>Chapter 12: Applied Decryption</b>	
Cryptography 201 . . . . .	110
Module Objectives. . . . .	110
Decryption Technology . . . . .	110
Module Objectives. . . . .	111
DNA Interface . . . . .	111
Module Objectives. . . . .	111
Lab—Decrypting Selected Applications . . . . .	111
Module Objectives. . . . .	112
Working with PGP . . . . .	112
Module Objectives. . . . .	112
Lab—Working with Encrypted Containers. . . . .	112
Module Objectives. . . . .	113
Lab—Private Keys Revisited. . . . .	113
Module Objectives. . . . .	113
Lab—Working with Data within Data . . . . .	113
Module Objectives. . . . .	114
The AccessData Decryption Methodology . . . . .	114
Module Objectives. . . . .	114
<b>Chapter 13: Linux Forensics</b>	
Linux-Based Forensics Tools . . . . .	116
Module Objectives. . . . .	116
Live Linux CD/DVDs for Forensic Analysis . . . . .	116
Module Objectives. . . . .	116
Linux Forensics Foundations . . . . .	116
Module Objectives. . . . .	116
Introduction to Linux System Investigation . . . . .	117
Module Objectives. . . . .	117
Advanced Linux System Investigation. . . . .	117
Module Objectives. . . . .	117
Introduction to Linux Network Intrusion Investigation . . . . .	118
Module Objectives. . . . .	118
Advanced Linux Network Intrusion Investigation . . . . .	118
Module Objectives. . . . .	118

**Chapter 14: Macintosh Forensics**

Mac GPT Structure . . . . .	120
Module Objectives . . . . .	120
Obtaining the date and Time from a Mac . . . . .	120
Module Objectives . . . . .	120
Imaging a Mac . . . . .	120
Module Objectives . . . . .	120
Directory Structure—Finding Evidence . . . . .	121
Module Objectives . . . . .	121
Recovering the User Logon Password . . . . .	121
Module Objectives . . . . .	121
Application Data—Safari . . . . .	122
Module Objectives . . . . .	122
Application Data—Firefox . . . . .	122
Module Objectives . . . . .	122
Application Data—iChat . . . . .	123
Module Objectives . . . . .	123
Application Data—Apple Mail . . . . .	123
Module Objectives . . . . .	123
iPod Analysis . . . . .	124
Module Objectives . . . . .	124
iPhone Backup Recovery . . . . .	124
Module Objectives . . . . .	125

**Chapter 15: Incident Response**

Incident Response Preparation . . . . .	129
Module Objectives . . . . .	129
Preparing Tools and Communications . . . . .	129
Module Objectives . . . . .	129
Incident Types, Sources, and Signs . . . . .	130
Module Objectives . . . . .	130
Intrusion Identification and Prioritization . . . . .	130
Module Objectives . . . . .	130
Evidence . . . . .	131
Module Objectives . . . . .	131
Volatile data . . . . .	131
Module Objectives . . . . .	131
Nonvolatile Data . . . . .	132
Module Objectives . . . . .	132
Incident Notification, Documentation, and Damage Assessment . . . . .	132
Module Objectives . . . . .	132
Containment, Analysis, and Network Analysis Strategies . . . . .	133
Module Objectives . . . . .	133
Identifying the Attacker and Attack Vector . . . . .	133
Module Objectives . . . . .	133

---

Eradication and Recovery .....	134
Module Objectives.....	134
Post-Incident Activity .....	134
Module Objectives.....	134
AccessData Enterprise .....	135
Module Objectives.....	135
<b>Chapter 16: SilentRunner</b>	
Installation and Deployment.....	138
Module Objectives.....	138
The Collector Interface .....	138
Module Objectives.....	138
Configuring Data Collection .....	139
Module Objectives.....	139
Working with Network Data.....	139
Module Objectives.....	139
Data Manager and Analyzer.....	140
Module Objectives.....	140
Query the Database .....	140
Module Objectives.....	141



## Building Your Custom Course

Welcome to the AccessData Course Catalogue. This catalogue provides descriptions of the current AccessData courses and their individual modules. Using the information provided in this catalog, you can build custom courses that suit your organization's specific training needs.

The following sections provide a checklist of the individual modules included in each course. You can use this checklist to select the modules you want to include in your course.

- "Forensics Fundamentals" on page 2
- "BootCamp—FTK1" on page 3
- "BootCamp—FTK 3" on page 4
- "Transition Workshop—FTK 3" on page 5
- "Case Reviewer" on page 6
- "Windows Forensics—FTK 1" on page 7
- "Windows Forensics—FTK 3" on page 8
- "Windows Forensics—Vista" on page 9
- "Windows Forensics Registry" on page 10
- "Internet Forensics—FTK 1" on page 11
- "Internet Forensics—FTK 3" on page 12
- "Applied Decryption" on page 13
- "Linux Forensics" on page 14
- "Macintosh Forensics" on page 15
- "Incident Response" on page 16
- "SilentRunner" on page 17

To order your custom course, you can

- Download an order form from the AccessData Support Portal (<http://support.accessdata.com>) and email it to your sales representative.
- Print the checklist from the following pages and fax it to (801) 377-5426.
- Contact your AccessData sales representative.

---

## FORENSICS FUNDAMENTALS

Forensic Fundamentals focuses primarily on examining data at the physical level for a better understanding of file system function, electronic evidence handling principles, and imaging procedures. For a brief description of each module, see Chapter 1, "Forensics Fundamentals," on page 19.

Use the following checklist to select the modules you want to include in your course.

Code	Select	Module	Time
FF-01	<input type="checkbox"/>	What is Computer Crime?***	60 mins
FF-02	<input type="checkbox"/>	Search and Seizure**	60 mins
FF-03	<input type="checkbox"/>	Introduction to FTK Imager	60 mins
FF-04	<input type="checkbox"/>	Computer Terms and Numbering Systems**	60 mins
FF-05	<input type="checkbox"/>	Physical Characteristics of Digital Storage Media	60 mins
FF-06	<input type="checkbox"/>	Partitioning Concepts	60 mins
FF-07	<input type="checkbox"/>	Boot Process and Drive Letter Assignments	60 mins
FF-08	<input type="checkbox"/>	Formatting to FAT 12, 16, and 32	90 mins
FF-09	<input type="checkbox"/>	File Allocation Table	60 mins
FF-10	<input type="checkbox"/>	Saving Files in FAT	150 mins
FF-11	<input type="checkbox"/>	Recovering Deleted Files**	60 mins
FF-12	<input type="checkbox"/>	Practical—Partitioning, the FAT File System, Viewing and Interpreting Data	150 mins
FF-13	<input type="checkbox"/>	Write Blockers and Disk Access	90 mins
FF-14	<input type="checkbox"/>	Imaging	180 mins
FF-15	<input type="checkbox"/>	Introduction to FTK	90 mins

\*\*\*This module does not have a practical.

---

## BOOTCAMP—FTK1

BootCamp FTK 1 provides the knowledge and skills necessary to install, configure and effectively use Forensic Toolkit<sup>®</sup> 1 (FTK<sup>®</sup> 1), FTK Imager<sup>®</sup>, Password Recovery Toolkit<sup>®</sup> (PRTK<sup>®</sup>), and Registry Viewer<sup>®</sup>. For a brief description of each module, see Chapter 2, "BootCamp—FTK1," on page 27.

Use the following checklist to select the modules you want to include in your course.

Code	Select	Module	Time
BC1-01	<input type="checkbox"/>	Introduction (Installing UTK)	60 mins
BC1-02	<input type="checkbox"/>	Working with FTK Imager	150 mins
BC1-03	<input type="checkbox"/>	Working with FTK—Part 1	150 mins
BC1-04	<input type="checkbox"/>	Working with FTK—Part 2	150 mins
BC1-05	<input type="checkbox"/>	Processing the Case	180 mins
BC1-06	<input type="checkbox"/>	Narrowing Your Focus	90 mins
BC1-07	<input type="checkbox"/>	Filtering the Case	60 mins
BC1-08	<input type="checkbox"/>	Case Reporting	90 mins
BC1-09	<input type="checkbox"/>	Registry Viewer Introduction	60 mins
BC1-10	<input type="checkbox"/>	Working with PRTK	60 mins

---

## BOOTCAMP—FTK 3

BootCamp FTK 3 provides the knowledge and skills necessary to install, configure and effectively use Forensic Toolkit 2 (FTK 2), FTK Imager, PRTK, and Registry Viewer. For a brief description of each module, see Chapter 3, "BootCamp—FTK3," on page 35.

Use the following checklist to select the modules you want to include in your course.

---

Code	Select	Module	Time
BC3-01	<input type="checkbox"/>	Introduction (Installing FTK 3)	60 mins
BC3-02	<input type="checkbox"/>	Working with FTK Imager	150 mins
BC3-03	<input type="checkbox"/>	Working with Registry Viewer	90 mins
BC3-04	<input type="checkbox"/>	Working with FTK—Part 1	150 mins
BC3-05	<input type="checkbox"/>	Working with FTK—Part 2	150 mins
BC3-06	<input type="checkbox"/>	Processing the Case	180 mins
BC3-07	<input type="checkbox"/>	Narrowing Your Focus	90 mins
BC3-08	<input type="checkbox"/>	Filtering the Case	90 mins
BC3-09	<input type="checkbox"/>	Case Reporting	60 mins
BC3-10	<input type="checkbox"/>	Working with PRTK	90 mins

---

---

## TRANSITION WORKSHOP—FTK 3

The AccessData® Forensic Toolkit® 3 (FTK™ 3), One-Day Transition Workshop is designed to provide the knowledge and skills to enable participants to transition from FTK 1.x or FTK 2.x to FTK 3. Participants will learn how to utilize FTK 3 to process a case and locate evidence.

Use the following checklist to select the modules you want to include in your course.

---

Code	Select	Module	Time
BC3-01	<input type="checkbox"/>	Introduction (Installing FTK 3)	60 mins
BC3-02	<input type="checkbox"/>	Working with FTK—Part 1	150 mins
BC3-03	<input type="checkbox"/>	Working with FTK—Part 2	150 mins
BC3-04	<input type="checkbox"/>	Processing the Case	180 mins
BC3-05	<input type="checkbox"/>	Narrowing Your Focus	90 mins
BC3-06	<input type="checkbox"/>	Filtering the Case	90 mins
BC3-07	<input type="checkbox"/>	Case Reporting	60 mins

---

## CASE REVIEWER

The AccessData® Case Reviewer Training provides an introduction to using AccessData Case Reviewer. During this one-day, hands-on workshop, participants will perform the following tasks:

- Obtain basic analysis data in Case Reviewer.
- Bookmark evidence.
- Create and apply custom column and font settings.
- Locate and view graphics files.
- Locate, view, and search e-mail files and attachments.
- Perform indexed searches.
- Discuss regular expressions.

Use the following checklist to select the modules you want to include in your course.

---

Code	Select	Module	Time
CR-02	<input type="checkbox"/>	Database Management	
CR-02	<input type="checkbox"/>	Working with FTK—Part 1	
CR-03	<input type="checkbox"/>	Working with FTK—Part 2	
CR-04	<input type="checkbox"/>	Case Processing	

---

---

## WINDOWS FORENSICS—FTK 1

Windows Forensics FTK 1 provides the knowledge and skills necessary to use AccessData products to conduct forensic investigations on Microsoft Windows systems. Participants learn where and how to locate Windows system artifacts using FTK, FTK Imager, Registry Viewer and PRTK. For a brief description of each module, see Chapter 6, "Windows Forensics—FTK 1," on page 53.

Use the following checklist to select the modules you want to include in your course.

Code	Select	Module	Time
XP1-01	<input type="checkbox"/>	FTK Overview	60 mins
XP1-02	<input type="checkbox"/>	Regular Expressions	60 mins
XP1-03	<input type="checkbox"/>	KFF Management	60 mins
XP1-04	<input type="checkbox"/>	Windows Registry—9x**	30 mins
XP1-05	<input type="checkbox"/>	Windows Registry—Windows 2000 and XP	60 mins
XP1-06	<input type="checkbox"/>	Registry—Access and Concerns	60 mins
XP1-07	<input type="checkbox"/>	Working with Registry Viewer	90 mins
		<b>Note:</b> Module XP1-07 requires the “Registry Viewer Introduction” module from the BootCamp course.	
XP1-08	<input type="checkbox"/>	Gathering Evidence and Reporting	120 mins
XP1-09	<input type="checkbox"/>	The Recycle Bin	90 mins
XP1-10	<input type="checkbox"/>	Thumbs.db Files	60 mins
XP1-11	<input type="checkbox"/>	Metadata	60 mins
XP1-12	<input type="checkbox"/>	Link and Spool Files	90 mins
XP1-13	<input type="checkbox"/>	PRTK Alternate Features	60 mins
		<b>Note:</b> Module XP1-13 requires the “Working with PRTK” module from the BootCamp course.	
XP1-14	<input type="checkbox"/>	Encrypting File System	60 mins
XP1-15	<input type="checkbox"/>	Alternate Data Streams	60 mins

---

\*\*This module does not have a practical.

---

## WINDOWS FORENSICS—FTK 3

Windows Forensics FTK 3 provides the knowledge and skills necessary to use AccessData products to conduct forensic investigations on Microsoft Windows systems. Participants learn where and how to locate Windows system artifacts using FTK, FTK Imager, Registry Viewer, and PRTK. For a brief description of each module, see Chapter 7, "Windows Forensics—FTK 3," on page 65.

Use the following checklist to select the modules you want to include in your course.

---

Code	Select	Module	Time
XP3-01	<input type="checkbox"/>	Regular Expressions	60 mins
XP3-02	<input type="checkbox"/>	Windows Registry 101**	30 mins
XP3-03	<input type="checkbox"/>	Windows Registry—Windows 2000 and XP**	60 mins
XP3-04	<input type="checkbox"/>	Working with Registry Viewer	90 mins
XP3-05	<input type="checkbox"/>	Gathering Evidence and Reporting	120 mins
XP3-06	<input type="checkbox"/>	The Recycle Bin	90 mins
XP3-07	<input type="checkbox"/>	Thumbs.db Files	60 mins
XP3-08	<input type="checkbox"/>	Metadata	60 mins
XP3-09	<input type="checkbox"/>	Link and Spool Files	90 mins
XP3-10	<input type="checkbox"/>	Alternate Data Streams	60 mins
XP3-11	<input type="checkbox"/>	Windows XP Prefetch	60 mins
XP3-12	<input type="checkbox"/>	Working with PRTK	60 mins
XP3-13	<input type="checkbox"/>	PRTK Alternate Features	60 mins
XP3-14	<input type="checkbox"/>	Encrypting File System	60 mins

---

\*\*This module does not have a practical.

---

## WINDOWS FORENSICS—VISTA

Windows Vista provides the knowledge and skills necessary to analyze Microsoft Windows Vista operating system artifacts and file system mechanics using Forensic Toolkit (FTK), FTK Imager, Password Recovery Toolkit (PRTK), and Registry Viewer. For a brief description of each module, see Chapter 9, "Windows Forensics Registry," on page 83.

Use the following checklist to select the modules you want to include in your course.

Code	Select	Module	Time
VF-01	<input type="checkbox"/>	Understanding BitLocker Drive Encryption	120 mins
VF-02	<input type="checkbox"/>	Working with GUID Partition Tables	90 mins
VF-03	<input type="checkbox"/>	Vista Security and File Structure	120 mins
VF-04	<input type="checkbox"/>	Windows Vista Registry—Introduction	60 mins
<b>Note:</b> Modules VF-04 through VF-06 require the "Working with Registry Viewer" module from the BootCamp course.			
VF-05	<input type="checkbox"/>	Windows Vista Registry—Registry File Artifacts	90 mins
VF-06	<input type="checkbox"/>	Windows Vista Registry—ReadyBoost and DPAPI	120 mins
VF-07	<input type="checkbox"/>	Windows Vista Event Logs	60 mins
VF-08	<input type="checkbox"/>	Windows Vista Shadow Copy	90 mins
VF-09	<input type="checkbox"/>	Windows Vista Recycle Bin	90 mins
VF-10	<input type="checkbox"/>	Windows Vista ThumbCache	90 mins
VF-11	<input type="checkbox"/>	Windows Vista Superfetch (Prefetch)	90 mins

---

---

## WINDOWS FORENSICS REGISTRY

Windows Forensics Registry provides the knowledge and skills necessary to use AccessData products to conduct forensic investigations on the Microsoft Windows registry. Participants learn where and how to locate registry artifacts using Forensic Toolkit (FTK), FTK Imager, Registry Viewer, and Password Recovery Toolkit (PRTK). For a brief description of each module, see Chapter 8, "Windows Forensics—Vista," on page 75.

Use the following checklist to select the modules you want to include in your course.

---

Code	Select	Module	Time
WFR-01	<input type="checkbox"/>	Registry Utilities	90 mins
WFR-02	<input type="checkbox"/>	Registry 201	150 mins
		<b>Note:</b> Module WFR-02 requires the "Working with Registry Viewer" module from the BootCamp course.	
WFR-03	<input type="checkbox"/>	Preliminary Reports	90 mins
WFR-04	<input type="checkbox"/>	SAM Artifacts	150 mins
WFR-05	<input type="checkbox"/>	SYSTEM Artifacts	150 mins
WFR-06	<input type="checkbox"/>	SECURITY Artifacts	60 mins
WFR-07	<input type="checkbox"/>	SOFTWARE Artifacts	150 mins
WFR-08	<input type="checkbox"/>	Application Behavior 1	150 mins
WFR-09	<input type="checkbox"/>	Application Behavior 2	60 mins

---

---

## INTERNET FORENSICS—FTK 1

Internet Forensics—FTK 1 provides the knowledge and skills necessary to use AccessData tools to recover forensic information from Internet artifacts. Participants learn where and how to locate Internet artifacts using Forensic Toolkit (FTK), Registry Viewer, and Password Recovery Toolkit (PRTK). For a brief description of each module, see Chapter 10, "Internet Forensics—FTK 1," on page 93.

Use the following checklist to select the modules you want to include in your course

---

Code	Select	Module	Time
IF1-01	<input type="checkbox"/>	AOL Instant Messenger (AIM)	120 mins
IF1-02	<input type="checkbox"/>	Firefox	120 mins
IF1-03	<input type="checkbox"/>	Internet Explorer	120 mins
IF1-04	<input type="checkbox"/>	Yahoo Messenger	120 mins
IF1-05	<input type="checkbox"/>	Windows Messenger	120 mins
IF1-06	<input type="checkbox"/>	MSN Messenger	60 mins
IF1-07	<input type="checkbox"/>	AOL—Information from America Online**	60 mins
IF1-08	<input type="checkbox"/>	AOL—Information from the Computer	60 mins
IF1-09	<input type="checkbox"/>	AOL—Personal Filling Cabinet	60 mins
IF1-10	<input type="checkbox"/>	Password Recovery	120 mins

**Note:** Module IF-10 requires the “Working with PRTK” module from the BootCamp course.

---

\*\*This module does not have a practical.

## INTERNET FORENSICS—FTK 3

Internet Forensics—FTK 3 provides the knowledge and skills necessary to use AccessData tools to recover forensic information from Internet artifacts. Participants learn where and how to locate Internet artifacts using Forensic Toolkit (FTK), Registry Viewer, and Password Recovery Toolkit (PRTK). For a brief description of each module, see Chapter 11, "Internet Forensics—FTK 3," on page 101.

Use the following checklist to select the modules you want to include in your course

---

Code	Select	Module	Time
IF3-01	<input type="checkbox"/>	AOL Instant Messenger (AIM)	120 mins
IF3-02	<input type="checkbox"/>	Yahoo! Messenger	120 mins
IF3-03	<input type="checkbox"/>	Windows Live Messenger	120 mins
IF3-04	<input type="checkbox"/>	MySpace Instant Messenger	120 mins
IF3-05	<input type="checkbox"/>	Skype	120 mins
IF3-06	<input type="checkbox"/>	Facebook	120 mins
IF3-08	<input type="checkbox"/>	Safari	120 mins
IF3-09	<input type="checkbox"/>	Firefox	120 mins
IF3-10	<input type="checkbox"/>	Internet Explorer	120 mins
IF3-11	<input type="checkbox"/>	LimeWire	120 mins

---

---

## APPLIED DECRYPTION

Applied Decryption is an intensive, hands-on course that reviews current encryption technology and provides the knowledge and skills necessary to recover passwords using PRTK and DNA. For a brief description of each module, see Chapter 12, "Applied Decryption," on page 109.

Use the following checklist to select the modules you want to include in your course.

---

**Note:** All modules in this course require the "Working with PRTK" module from the BootCamp course.

---

Code	Select	Module	Time
AD-01	<input type="checkbox"/>	Cryptography 201	210 mins
AD-02	<input type="checkbox"/>	Decryption Technology	120 mins
AD-03	<input type="checkbox"/>	Working with DNA	120 mins
AD-04	<input type="checkbox"/>	Lab—Decrypting Selected Applications	210 mins
AD-05	<input type="checkbox"/>	Working with PGP	120 mins
AD-06	<input type="checkbox"/>	Lab—Working with Encrypted Containers	60 mins
AD-07	<input type="checkbox"/>	Lab—Private Keys Revisited	90 mins
AD-08	<input type="checkbox"/>	Lab—Working with Data within Data	90 mins
AD-09	<input type="checkbox"/>	The AccessData Decryption Methodology	90 mins

---

## LINUX FORENSICS

Linux Forensics is a hands-on course that reviews different types of Linux-based forensics tools available for digital investigations, forensic imaging with Linux tools, and best practices for Linux-based investigations. For a brief description of each module, see Chapter 13, "Linux Forensics," on page 115.

Use the following checklist to select the modules you want to include in your course.

---

Code	Select	Module	Time
LF-01	<input type="checkbox"/>	Linux-Based Forensics Tools	
LF-02	<input type="checkbox"/>	Live Linux CD/DVDs for Forensic Analysis	
LF-03	<input type="checkbox"/>	Linux Forensics Foundations	
LF-04	<input type="checkbox"/>	Introduction to Linux System Investigation	
LF-05	<input type="checkbox"/>	Advanced Linux System Investigation	
LF-06	<input type="checkbox"/>	Introduction to Linux Network Intrusion Investigation	
LF-07	<input type="checkbox"/>	Advanced Linux Network Intrusion Investigation	

---

---

## MACINTOSH FORENSICS

Macintosh Forensics is an intensive, hands-on course that reviews current encryption technology and provides the knowledge and skills necessary to recover passwords using PRTK and DNA. For a brief description of each module, see Chapter 12, "Applied Decryption," on page 109.

Use the following checklist to select the modules you want to include in your course.

---

Code	Select	Module	Time
MF-01	<input type="checkbox"/>	Mac GPT Structure	
MF-02	<input type="checkbox"/>	Obtaining the Date and Time from a Mac	
MF-03	<input type="checkbox"/>	Imaging a Mac	
MF-04	<input type="checkbox"/>	Directory Structure—Finding Evidence	
MF-05	<input type="checkbox"/>	Recovering the User Logon Password	
MF-06	<input type="checkbox"/>	Application Data—Safari	
MF-07	<input type="checkbox"/>	Application Data—Firefox	
MF-08	<input type="checkbox"/>	Application Data—iChat	
MF-09	<input type="checkbox"/>	Application Data—Apple Mail	
MF-10	<input type="checkbox"/>	iPod Analysis	
MF-11	<input type="checkbox"/>	iPhone Backup Recovery	

---

---

## INCIDENT RESPONSE

Incident Response 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. For a brief description of each module, see Chapter 15, "Incident Response," on page 127.

Use the following checklist to select the modules you want to include in your course.

Code	Select	Module	Time
IR-01	<input type="checkbox"/>	Incident Response Preparation	
IR-02	<input type="checkbox"/>	Preparing Tools and Communications	
IR-03	<input type="checkbox"/>	Incident Types, Sources, and Signs	
IR-04	<input type="checkbox"/>	Intrusion Identification and Prioritization	
IR-05	<input type="checkbox"/>	Evidence	
IR-06	<input type="checkbox"/>	Volatile Data	
IR-07	<input type="checkbox"/>	NonVolatile Data	
IR-08	<input type="checkbox"/>	Incident Notification, Documentation, and Damage Assessment	
IR-09	<input type="checkbox"/>	Containment, Host Analysis, and Network Analysis Strategies	
IR-10	<input type="checkbox"/>	Identifying the Attacker and Attack Vector	
IR-11	<input type="checkbox"/>	Eradication and Recovery	
IR-12	<input type="checkbox"/>	Post-Incident Activity	
IR-13	<input type="checkbox"/>	AccessData Enterprise	

---

---

## SILENTRUNNER

This class is designed for security administrators, security auditors, data center managers, IT managers, system administrators, and law enforcement investigators who are responsible for responding to and investigating network irregularities. It is designed to show the student how to collect and analyze network data from a single point of control using AccessData® SilentRunner®.

Use the following checklist to select the modules you want to include in your course.

---

Code	Select	Module	Time
SR-01	<input type="checkbox"/>	Installation and Deployment	
SR-02	<input type="checkbox"/>	The Collector Interface	
SR-03	<input type="checkbox"/>	Configuring the Collector	
SR-04	<input type="checkbox"/>	Working with Network Data	
SR-05	<input type="checkbox"/>	Data Manager	
SR-06	<input type="checkbox"/>	Query the Database	

---



## Forensics Fundamentals

Forensic Fundamentals focuses primarily on examining data at the physical level for a better understanding of file system function, electronic evidence handling principles, and imaging procedures.

The following sections provide a brief description of each module in the Forensics Fundamentals course with the corresponding module objectives.

- "What Is Computer Crime?" on page 20
- "Search and Seizure" on page 20
- "Introduction to FTK Imager" on page 20
- "Computer Terms and Numbering Systems" on page 21
- "Physical Characteristics of Digital Storage Media" on page 21
- "Partitioning Concepts" on page 22
- "Boot Process and Drive Letter Assignments" on page 22
- "Formatting to FAT 12, 16, and 32" on page 23
- "File Allocation Table" on page 23
- "Saving Files in FAT" on page 24
- "Recovering Deleted Files" on page 24
- "Write Blockers and Disk Access" on page 25
- "Imaging" on page 26
- "Introduction to FTK" on page 26

## WHAT IS COMPUTER CRIME?

Provides a basic overview of computer crime and how to recover digital evidence. It reviews sources of evidence, electronic storage devices, and operating system limitations. It also outlines the points you must consider when gathering, examining, and reporting digital evidence that will be presented in a court of law.

### Module Objectives

- Define the role of digital evidence and computers used in crime.
- Describe different physical devices and the types of data that can be stored on the devices.
- Discuss methodologies to use with large amounts of evidentiary digital data, including how to store the data and the different operating systems that may store it.
- Discuss the methods of gathering evidence and the tools available to examine and analyze that data.

## SEARCH AND SEIZURE

Provides a basic overview of search and seizure procedures for digital evidence. It includes a review of operating system functions on a hard and soft shutdowns and how they can impact digital evidence.

### Module Objectives

- Identify pre-search and pre-seizure concerns.
- Describe devices that may contain digital evidence.
- Describe seizure issues and how to take control of computer systems.
- Describe how to collect evidence for examination, analysis, and reporting findings.

## INTRODUCTION TO FTK IMAGER

Introduces FTK Imager and how it can be used for basic data acquisition functions. During the module, participants review media and storage devices, acquisition tools, and forensic image formats such as the RAW DD format and the e01 and s01 compressed image structures. Participants then use FTK Imager to preview live data and image files, export file data, create MD5 hashes, acquire data, and duplicate digital evidence to different formats.

## Module Objectives

- Review data storage devices
- Identify file system support for FTK Imager
- Describe the FTK interface
- Use the Properties and Interpreters windows
- Preview local physical devices

## COMPUTER TERMS AND NUMBERING SYSTEMS

Specifically designed for new forensic examiners. Participants first learn how computers “see” data. This starts with a discussion of Bit, Nibble, and Byte values. Participants then learn to recognize data in binary, decimal, and hexadecimal formats. They review the schemas used to display information through software applications and build to an explanation of ASCII and UNICODE characters.

## Module Objectives

- Describe how computers view data.
- Define the terms *bit*, *nibble*, *byte*, and *word*.
- Identify binary, decimal, and hexadecimal data.
- Differentiate between ASCII and Unicode characters.

## PHYSICAL CHARACTERISTICS OF DIGITAL STORAGE MEDIA

Addresses the physical characteristics associated with digital media. It includes information about physical connections on hard drives, floppy disks, and removable media as well as their logical and physical data structures.

Students are introduced to physical hardware with a discussion on legacy floppy diskettes and hard disk drives. This is followed by a detailed explanation of how data is laid out on a traditional hard disk scheme, Cylinders, Heads, and Tracks (C,H,S). The discussion examines the numbering schemes used to calculate hard disk capacities and to verify that all addressable space is accounted for when handling physical electronic evidence.

## Module Objectives

- Identify and list the physical characteristics of floppy disks and removable media.
- Describe standard hard drive technologies.
- Define how sectors, tracks, and cylinders are structured.
- Calculate storage capacities using CHS and LBA.

## PARTITIONING CONCEPTS

Introduces the concept of partitioning a hard disk drive into logical volumes to store user data. Students learn to differentiate between the physical device and a logical partition on the device. There is a discussion on the uses of partitioning as well as the concept of hiding partitions from different operating systems. Students are introduced to the Master Partition Table by a definition of its location, size, and contents at the Hex level. Common partition types are identified during the practical session.

During the practical, participants identify common partition types, create three partitions on a physical hard disk drive, and predict the partitioning outcome prior to viewing the raw data with FTK Imager.

### Module Objectives

- Differentiate between logical drives and physical drives.
- Describe the uses for partitioning.
- Discuss the elements of a Master Partition Table:
  - Location of the table
  - Size of the table
  - Size of each entry
  - Entry types
- List common partition types found on Microsoft systems.

## BOOT PROCESS AND DRIVE LETTER ASSIGNMENTS

Introduces the boot process of an Intel-based computer. It includes a detailed discussion of the Power On Self Test with a description of each check the system performs to verify that all hardware devices are functioning correctly. The discussion also addresses the forensic implications of interrupting the boot process to gain information from the system BIOS. The module then details CMOS values and discusses ways to access a password-protected system. Following a review of the boot process, participants review Microsoft's standard for assigning drive letters to logical volumes. They also learn the three rules the system applies to volumes during the boot process and identify the issues that arise when additional drives are added to an existing system.

## Module Objectives

- Describe the boot process.
- Identify the forensic importance of CMOS.
- Identify the limitations of using drive letters to define volumes.
- List and describe the rules that DOS and Windows apply to drive lettering.

## FORMATTING TO FAT 12, 16, AND 32

Introduces the process of preparing a logical volume to store data. It focuses on the File Allocation Table (FAT) file system and includes a detailed discussion of the differences between the three versions of FAT: FAT12, 16, and 32. The module also explains the function of the volume's system area and includes a discussion of how sectors are grouped into clusters (allocation units). It then discusses the differences between FAT16 and FAT32 formatted partitions. Finally, the module reviews the effects of formatting an existing volume, including and the volume updates.

During the practical, students format the logical volumes created in the previous module to different file systems, then view the system areas using FTK Imager.

## Module Objectives

- List the FAT file system components.
- List the three main areas that comprise the system area on a drive formatted to FAT.
- Identify system area differences between FAT16 and FAT32.
- Describe the concept of clusters.
- Examine the effects of the Format command on existing data.

## FILE ALLOCATION TABLE

Discusses the location and function of the File Allocation Table on FAT12, 16, and 32 volumes. It provides a brief history of FAT followed by a detailed explanation of how the FAT tracks the allocated status of clusters within the volume. Participants also learn about four possible entry types and the effects of saving or adding file data to existing files.

During the practical, students save files on a FAT16 volume, then view the volume with FTK Imager to trace out the FAT link list.

## Module Objectives

- Examine the function of the File Allocation Table (FAT).
- List the limitations of addressing clusters with FAT 12, FAT 16, and FAT 32.
- Describe the four possible FAT entry values.

## SAVING FILES IN FAT

Examines the process the operating system performs when files are saved on a FAT volume. Students learn how to read a 32-byte directory entry for both a Short File Name (SFN) and a Long File Name (LFN) entry. They also identify the sequence byte for all associated LFN fragments. The module provides a detailed examination of the different areas of file slack within clusters and reviews the effects of the creating of subfolders.

During the practical, participants save and delete files, add data to existing files, and view the volume with FTK Imager.

## Module Objectives

- Identify the key elements of a directory entry.
- Describe the rules for short and long filenames.
- Describe the concept of file slack and list the two main components.
- Describe and observe the effects of creating subdirectories.
- Create files and folders on a drive formatted to FAT16 and FAT32.

## RECOVERING DELETED FILES

Describes what happens when files are deleted in a FAT environment and how they can be recovered. Students first learn how the operating system marks a directory entry for a deleted file, what happens in the FAT to label the cluster as free, and finally what occurs on the data area of the drive where the file data resides. Students then learn how to recover deleted files—both manually and with the use of automated tools. In this discussion, students also identify the difficulties in recovering deleted fragmented files.

During the practical, students delete several files and observe the effects using FTK Imager.

## Module Objectives

- Describe the process DOS undertakes when files and folders are deleted.
- List the effects on data when files are deleted.
- Describe the process to manually recover a deleted file.
- Identify the difficulties in recovering deleted fragments of files.

## WRITE BLOCKERS AND DISK ACCESS

Explains how to access a hard drive through the operating system or direct drive access. The presentation focuses on software and hardware write blockers and includes a discussion of their corresponding pitfalls. Participants learn the importance of validating the functionality of their write block solution and review ways to validate the device on seeded data. The module also presents ways to identify host-protected areas and emphasizes that students reinforce their SOP's when they must account for all hard disk space on the suspect's media.

During the practical, students create a software write blocker (Registry key) that enables them to safely image USB media on a system running Windows XP with SP2.

## Module Objectives

- Describe drive-accessing schemes.
- Identify issues surrounding access via Int13, Direct, and Windows.
- Identify the limitations of software write blockers.
- Describe the host-protected area.
- Identify hardware write blockers, both handheld and external devices.

## IMAGING

Focuses on the need for examiners to create forensic copies of a suspect's electronic evidence into a file format that can be read by a forensic tool. The module differentiates between file-by-file and a bitstream copies of volume data. It also identifies different image formats and lists the pros and cons of each format. Finally, the module details how hashing technology can be used to validate the integrity of an image file and confirm the contents were not altered in any way during copy or analysis.

During the practical, students image a variety of media types and file systems not recognized by the Microsoft family.

### Module Objectives

- Describe the following imaging considerations:
  - File-by-file copy
  - Bit-stream image
- Describe file system considerations.
- Describe the different image formats that FTK Imager™ can produce.
- Describe the function of MD5/SHA1 and how this can be used to validate image file integrity.

## INTRODUCTION TO FTK

Provides a basic overview of the FTK interface including tab functions, menu items, toolbar functions, and data objects. It also provides an introduction to common functions, including creating a new case, managing processing options, and data carving operations.

During the practical, students enhance their knowledge of FTK functions by performing instructor-guided functions such as file exports and bookmarking evidence items.

### Module Objectives

- Identify the main FTK interface.
- Describe the function of the menu commands, toolbars, and tabs.
- Describe the process of starting a case with FTK.
- Describe the process of basic analysis:
  - File identification
  - Data carving
- Preview the Precious image.

## BootCamp—FTK 1

BootCamp FTK 1 provides the knowledge and skills necessary to install, configure, and effectively use Forensic Toolkit 1 (FTK 1), FTK Imager, Password Recovery Toolkit (PRTK), and Registry Viewer.

The following sections provide a brief description of each module in the BootCamp—FTK 1 course with the corresponding module objectives.

- "Introduction (Installing UTK)" on page 28
- "Working with FTK Imager" on page 28
- "Working with FTK—Part 1" on page 29
- "Working with FTK—Part 2" on page 30
- "Processing the Case" on page 31
- "Narrowing Your Focus" on page 32
- "Filtering the Case" on page 33
- "Case Reporting" on page 33
- "Registry Viewer Introduction" on page 34
- "Working with PRTK" on page 34

## INTRODUCTION (INSTALLING UTK)

Walks participants through the installation process for each component of the Ultimate Tool Kit (UTK). The module lists system requirements and the system changes that occur during installation, and identifies the locations of key program data stored on the local examiner's machine for backup and sharing purposes. Also discussed is the installation of the dongles drivers, including the common pitfalls of installing new driver sets and the License Manager application that controls the dongle license and subscription service. Finally, participants are given information for product upgrades and support.

During the practical, students install all the components of UTK and examine file locations.

### Module Objectives

- Identify the UTK components.
- List the FTK and PRTK system requirements.
- Identify the FTK .ini files.
- Describe how to receive upgrades and support for AccessData tools.
- Install the UTK.

## WORKING WITH FTK IMAGER

Presents an in-depth review of the FTK Imager utility with a focus on core functions related to the acquisition of electronic evidence. Students review different types of media and storage devices, software and hardware acquisition tools, and forensic image formats read and created by FTK Imager. Students also preview live data, export files and folders, generate MD5 Hash values from selected files, create forensic images of physical media, duplicate digital evidence files and, finally, validate image or drive integrity using MD5 hash values.

During the practical, students acquire an image of a thumb drive, then explore the FTK Imager features and functions discussed in the module.

## Module Objectives

- Describe standard data storage devices.
- Identify some common software and hardware acquisition tools.
- List some common forensic image formats.
- Use FTK Imager to perform the following functions:
  - Preview evidence
  - Export data files
  - Create a hash to benchmark your case evidence
  - Acquire an image of evidence data
  - Convert existing images to other formats
- Use dockable windows in FTK Imager.
- Navigate evidence items.
- Use the properties and interpreters windows.
- Validate forensic images.
- Create Custom Content Images.

## WORKING WITH FTK—PART 1

Introduces participants to the Forensic Toolkit (FTK) interface. FTK is a multifaceted forensic analysis tool that allows forensic examiners to review electronic evidence on live data or acquired images of file data. Key features include full text searching, email analysis, known file alerts, file identification, and much more.

All tab functions, menu items, and toolbar functions are reviewed in the module, followed by basic analysis of data objects and customization of the interface. Participants then review the basic skills required to create new cases and manage the case preprocessing options.

During the practical, students review the FTK interface, perform file exports, bookmark files, perform Copy Special operations, create custom column settings, and view MS Word metadata.

During the student lab, students follow a self-guided practical to independently apply the functions covered in class.

## Module Objectives

- Identify the basic interface components, including the menu and toolbar options as well as the program tabs.
- Create a case.
- Add evidence to a case.
- Obtain basic analysis data.
- Export files.
- Use the Copy Special feature to export information about case files.
- Change the Time Zone display settings.

## WORKING WITH FTK—PART 2

Reviews advanced FTK features. Students explore FTK display options and viewers, export data, manage target options, set program preferences, configure case logging options, import hash sets to the KFF, create MD5 hashes of evidence items, perform index searches, and use the Data Carve feature to recover evidence items from unallocated space and file slack.

The module also presents a “strategy of attack” that integrates FTK, PRTK, and Registry Viewer for more effective password recoveries and forensic investigations.

During the practical, students apply the concepts discussed in the presentation.

## Module Objectives

- Set program preferences in FTK.
- Configure case logging options.
- Import hash sets to the KFF.
- Use FTK analysis tools such as MD5 Hash and Full Text Indexing.
- Perform data carving searches.

## PROCESSING THE CASE

Instructs how to successfully process a case by locating the content you're looking for, clearly marking evidence items so you can access them as needed, and disseminating evidence when required. In this module, students first work with FTK within the context of a graphics case. They use column settings to locate relevant case graphics, then view the graphics in external viewers and applications. The course also requires advanced work with the Bookmark feature, including editing existing bookmark folders for inclusion in the final case report.

After working with graphics, the module turns its focus to the elements of an email case. Students learn how FTK displays and documents email artifacts, they create custom settings in FTK to display email messages in a preferred sequence, and they identify basic clues to culpability in email-orientated cases.

During the practical, students explore the FTK advanced features to view, sort, and export email and graphic artifacts from the case. They also bookmark, export, and hash files using the Graphics tab.

### Module Objectives

- Identify the elements of a graphics case.
- Navigate the FTK Graphics tab.
- Export graphics files and hash sets.
- Tag graphics files using the Bookmarks feature.
- Use the Flag Thumbnail feature.
- Identify the elements of an email case.
- Identify supported email types.
- Navigate the FTK Email tab.
- Sort email.
- Find a word or phrase in an email message or attachment.
- Export email items.

## NARROWING YOUR FOCUS

Given the sheer volume of information in most cases, it is infeasible to individually review every item in an acquired image or drive. FTK provides many options to help you efficiently and effectively narrow your focus and locate material of evidentiary value.

This module reviews search and filter options within FTK. Participants use the Known File Filter to eliminate irrelevant file items or identify contraband files of interest based on file hashes. To narrow target items, participants use the checkmark feature to select case items, then apply specific functions to the selected items such as bookmarking, Copy Special, and exporting. Students also explore the search functions within FTK using both the DTSearch advanced options and live data searching, including introduction to regular expression pattern searches.

During the practical, students apply the concepts taught during the presentation by performing keyword searches, bookmarking search results, using advanced DTSearch features on selected objects, and performing a regular expression search.

### Module Objectives

- Narrow evidence items using the Known File Filter (KFF), checked items, and filtered/ignored items.
- Perform an indexed search.
- Perform a live search.
- Import search terms from text files.
- Perform a regular expression search.

## FILTERING THE CASE

Focuses on the FTK File Filter Manager. During this module, students create and apply filters based file type, status, size, date, and time.

The practical requires students to create and apply filters to narrow the case focus.

### Module Objectives

- Explain the basic hierarchal structure of the File Filter Manager.
- Design and apply filters to narrow case evidence.
- Use filters in conjunction with containers and file lists in FTK to further narrow evidence.
- Explain the function of the Default Filter and Large Graphic Filter commonly used in case investigation.

## CASE REPORTING

When you perform a forensic investigation, you must be able to publish and disseminate your findings. FTK has a sophisticated report tool that allows you to systematically assemble and publish case information. During this module, students learn how to generate customized reports that include or exclude bookmarked objects, flagged graphics, and file management sections. The module also discusses report distribution options.

During the practical, students create multiple reports from a single case to explore all options available from the report wizard. They build from a very basic report to a detailed report that contains customized report items.

### Module Objectives

- Generate reports.
- View reports.
- Modify reports.
- Update reports.
- Distribute reports.

## REGISTRY VIEWER INTRODUCTION

Introduces the Windows registry. It begins with a discussion of the structure and differences between Windows 9x and NTx registry files, then introduces basic registry analysis within Registry Viewer. The primary focus of the module is operating system time zone information. Students identify the time zone the suspect's operating system was set to during seizure.

During the practical, students extract registry files from an image file using FTK Imager, then load the files into Registry Viewer for analysis. Students work with both a 9x and NTx system files.

### Module Objectives

- Describe which files comprise the Windows 2000/XP Registry.
- Seamlessly launch Registry Viewer from an FTK case.
- Determine a user's time zone setting.

## WORKING WITH PRTK

Introduces the PRTK 6 interface and the modules used to crack different types of applications and encrypted file data. Students review the different types of attack, the decryption process, importing custom dictionaries, defining biographical dictionaries, and creating attack profiles.

During the practical, students import dictionaries, create a custom profile, and start an attack session in PRTK.

### Module Objectives

- Navigate within the PRTK interface.
- Identify the available password recovery modules and their associated attack types.
- Import user-defined dictionaries and FTK word lists to use in a password recovery attack.
- Create biographical dictionaries.
- Set up profiles.
- Explain what a PRTK profile is and how it is used.
- Recount the AccessData Methodology.

## BootCamp—FTK3

BootCamp FTK 3 provides the knowledge and skills necessary to install, configure, and effectively use Forensic Toolkit 2 (FTK 2), FTK Imager, Password Recovery Toolkit (PRTK), and Registry Viewer.

The following sections provide a brief description of each module in the BootCamp—FTK 3 course with the corresponding module objectives.

- "Introduction (Installing FTK 3)" on page 36
- "Working with FTK Imager" on page 36
- "Working with Registry Viewer" on page 37
- "Working with FTK—Part 1" on page 38
- "Working with FTK—Part 2" on page 38
- "Processing the Case" on page 39
- "Narrowing Your Focus" on page 40
- "Filtering the Case" on page 41
- "Case Reporting" on page 41
- "Working with PRTK" on page 42

## INTRODUCTION (INSTALLING FTK 3)

Walks participants through the installation process for FTK 2. The module lists system requirements and system changes that occur during installation, and identifies the locations of key program data stored on the local examiner's machine for backup and sharing purposes. Also discussed is the installation of the dongles drivers, including the common pitfalls of installing new driver sets, and the License Manager application that controls the dongle license and subscription service. Finally, participants are given information for product upgrades and support.

During the practical, students install all the components of UTK and examine file locations.

### Module Objectives

- Identify the FTK 3 components.
- List the FTK 3 and PRTK system requirements.
- Describe how to receive upgrades and support for AccessData tools.
- Install FTK Imager, FTK 3, PRTK, Registry Viewer, and the dongle drivers.

## WORKING WITH FTK IMAGER

Provides an in-depth review of the FTK Imager utility with a focus on core functions related to the acquisition of electronic evidence. Students review different types of media and storage devices, software and hardware acquisition tools, and forensic image formats read and created by FTK Imager. Students also preview live data, export files, and folders; generate MD5 Hash values from selected files; create forensic images of physical media; duplicate digital evidence files; and validate image or drive integrity using MD5 hash values.

During the practical, students acquire an image of a thumbdrive, then explore the FTK Imager features and functions discussed in the module.

## Module Objectives

- Describe standard data storage devices.
- Identify some common software and hardware acquisition tools.
- List some common forensic image formats.
- Use FTK Imager to perform the following functions:
  - Preview evidence
  - Export data files
  - Create a hash to benchmark case evidence
  - Acquire an image of evidence data
  - Convert existing images to other formats
- Use dockable windows in FTK Imager.
- Navigate evidence items.
- Use the properties and interpreters windows.
- Validate forensic images.
- Create Custom Content Images.

## WORKING WITH REGISTRY VIEWER

Introduces the Windows registry. The module begins with a discussion of the structure and differences between Windows 9x and NTx registry files, then introduces basic registry analysis within Registry Viewer. The primary focus of the module is operating system time zone information. Students identify the time zone that the suspect's operating system was set to at seizure.

During the practical, students extract registry files from an image file using FTK Imager, then load the files into Registry Viewer for analysis. Students work with both 9x and NTx system files.

## Module Objectives

- Describe which files comprise the Windows 9x and 2000/XP/Vista Registries.
- Seamlessly launch Registry Viewer from an FTK 3 case.
- Determine a user's time zone setting.

## WORKING WITH FTK—PART 1

The Forensic Toolkit is a multifaceted forensic analysis tool that allows forensic examiners to review electronic evidence on live data or acquired images of file data. Key features include full-text searching, email analysis, known file alerts, file identification, and much more.

This module introduces participants to the FTK interface. All tab functions, menu items and toolbar functions are reviewed, followed by basic analysis of data objects and customization of the interface. Participants then review the basic skills required to create new cases and manage the case preprocessing options.

During the practical, students create new accounts, define different levels of permissions to a case, build new cases, explore the preprocessing functions, export files, use the Copy Special feature, and change the Time Zone display settings.

### Module Objectives

- Identify the basic interface components, including the menu and toolbar options as well as the program tabs.
- Create a case.
- Add evidence to a case.
- Obtain basic analysis data.
- Export files.
- Use the Copy Special feature to export information about case files.
- Change the Time Zone Display settings.

## WORKING WITH FTK—PART 2

Reviews advanced FTK features. Students explore FTK display options and viewers, export data, manage target options, set program preferences, configure case logging options, import hash sets to the KFF, create MD5 hashes of evidence items, perform index searches, and use the Data Carve feature to recover evidence items from unallocated space and file slack.

The module also presents a “strategy of attack” that integrates FTK, PRTK, and Registry Viewer for more effective password recoveries and forensic investigations.

During the practical, students apply the concepts discussed in the presentation.

## Module Objectives

- Set the Time Zone Display.
- Identify and view compound files.
- Export files and folders.
- Create custom column settings to manage the information that appears in the FTK file list.
- Use the Copy Special and Export File List features.
- Set FTK preferences.
- Create and manage bookmarks.
- Perform analysis functions, such as full-text indexing, after evidence has been added to the case.
- Perform automatic and manual data carving functions.

## PROCESSING THE CASE

To successfully process a case, you must be able to locate the content you're looking for, clearly mark evidence items so you can access them as needed, and disseminate evidence when required. In this module, students first work with FTK within the context of a graphics case. Participants use column settings to locate relevant case graphics, then view the graphics in external viewers and applications. The course also requires advanced work with the Bookmark feature, including editing existing bookmark folders for inclusion in the final case report.

After working with graphics, the module turns its focus to the elements of an email case. Students learn how FTK displays and documents email artifacts, they create custom settings in FTK to display email messages in a preferred sequence, and they identify basic clues to culpability in email-orientated cases.

During the practical, students explore the FTK advanced features to view, sort, and export email and graphic artifacts from the case. They also bookmark, export, and hash files from the Graphics tab.

## Module Objectives

- Identify the elements of a graphics case.
- Navigate the FTK Graphics tab.
- Export graphics files and hash sets.
- Tag graphics files using the Bookmarks feature.
- Use the Flag Thumbnail feature.
- Identify the elements of an email case.
- Identify supported email types.
- Navigate the FTK Email tab.
- Sort email.
- Find a word or phrase in an email message or attachment.
- Export email items.

## NARROWING YOUR FOCUS

Given the sheer volume of information in most cases, it is infeasible to individually review every item in an acquired image or drive. FTK provides many options to help you efficiently and effectively narrow your focus and locate material of evidentiary value.

This module reviews search and filter options within FTK. Participants use the Known File Filter to eliminate irrelevant file items or identify contraband files of interest based on file hashes. To narrow target items, participants use the checkmark feature to select case items, then apply specific functions to the selected items such as bookmarking, Copy Special, and exporting. Students also explore the search functions within FTK using both the DTSearch advanced options and live data searching, including introduction to regular expression pattern searches.

During the practical, students apply the concepts taught during the presentation by performing keyword searches, bookmarking search results, using advanced DTSearch features on selected objects, and performing a regular expression search.

## Module Objectives

- Narrow evidence items using the Known File Filter (KFF), checked items, and filtered/ignored items.
- Perform an indexed search.
- Perform a live search.
- Import search terms from text files.
- Perform a regular expression search.

---

## FILTERING THE CASE

Explains how to use FTK 3 filters to narrow focus to selected objects or a group of objects based on predefined criteria. The module demonstrates how to apply rules to new filters, import and export filters, nest filters, and utilize rule options. It also explains the differences between global and tab filters, how to use filters as a search tool, and how to apply filters to indexed searches or reports.

During the practical, students create filters, import and export filters, and use a Tab filter.

### Module Objectives

- Explain basic concepts of rule-based filtering in FTK.
- Define a basic filter and use it to filter data.
- Create filter rules.
- Nest filters.
- Explain the difference between global and tab filters.
- Import and export filters.
- Apply a filter to a report to customize output.
- Apply a filter to an index search.

## CASE REPORTING

When you perform a forensic investigation, you must be able to publish and disseminate your findings. FTK has a sophisticated report tool that allows you to systematically assemble and publish case information. During this module, students learn how to generate customized reports that include or exclude bookmarked objects, flagged graphics, and file management sections. The module also discusses report distribution options.

During the practical, students create multiple reports from a single case to explore all options available from the report wizard. They build from a very basic report to a detailed report that contains customized report items.

## Module Objectives

- Define a report:
  - Modify the case information.
  - Include a list of bookmarked files.
  - Export bookmarked files with the report.
  - Include thumbnails of bookmarked graphics.
  - Manage the appearance of the Bookmark section.
  - Include thumbnails of case graphics.
  - Link thumbnails to full-size graphics in the report directory.
  - Include a list of directories, subdirectories, files, and file types.
  - Include a list of case files and file properties in the report.
  - Export case files associated with specific file categories.
  - Append a registry report to the case report.
- Generate reports in PDF and HTML formats.
- Generate reports in other languages.

## WORKING WITH PRTK

Introduces the PRTK 6 interface and the modules used to crack different types of applications and encrypted file data. Students review the different types of attack and the decryption process, importing custom dictionaries, defining biographical dictionaries, and creating attack profiles.

During the practical, students import dictionaries, create a custom profile, and start an attack session in PRTK.

## Module Objectives

- Navigate within the PRTK interface.
- Identify the available password recovery modules and their associated attack types.
- Import user-defined dictionaries and FTK word lists to use in a password recovery attack.
- Create biographical dictionaries.
- Set up profiles.
- Explain what a PRTK profile is and how it is used.
- Recount the AccessData Methodology.

## Transition Day—FTK3

The AccessData® Forensic Toolkit® 3 (FTK™ 3), One-Day Transition Workshop is designed to provide the knowledge and skills to enable participants to transition from FTK 1.x or FTK 2.x to FTK 3. Participants will learn how to utilize FTK 3 to process a case and locate evidence.

The following sections provide a brief description of each module in the BootCamp—FTK 3 course with the corresponding module objectives.

- "Introduction (Installing FTK 3)" on page 44
- "Working with FTK—Part 1" on page 44
- "Working with FTK—Part 2" on page 45
- "Processing the Case" on page 45
- "Narrowing Your Focus" on page 46
- "Filtering the Case" on page 46
- "Case Reporting" on page 47

## INTRODUCTION (INSTALLING FTK 3)

Walks participants through the installation process for FTK 2. The module lists system requirements and system changes that occur during installation, and identifies the locations of key program data stored on the local examiner's machine for backup and sharing purposes. Also discussed is the installation of the dongles drivers, including the common pitfalls of installing new driver sets, and the License Manager application that controls the dongle license and subscription service. Finally, participants are given information for product upgrades and support.

During the practical, students install all the components of UTK and examine file locations.

### Module Objectives

- Identify the FTK 3 components.
- List the FTK 3 and PRTK system requirements.
- Describe how to receive upgrades and support for AccessData tools.
- Install FTK Imager, FTK 3, PRTK, Registry Viewer, and the dongle drivers.

## WORKING WITH FTK—PART 1

The Forensic Toolkit<sup>®</sup> (FTK<sup>®</sup>) is a multifaceted forensic analysis tool. It provides digital evidence analysis, full text searching, email analysis, known file alerts, and much more. Used in conjunction with the Password Recovery Toolkit<sup>®</sup> and Registry Viewer<sup>®</sup>, FTK can also help significantly reduce the time required for case analysis. The objective of this module is to introduce the basics of using FTK.

### Module Objectives

- Effectively use the Database Manager
- Create and administer users
- Back up, delete, and restore cases
- Identify the evidence processing options
- Identify the basic FTK interface components, including the menu and toolbar options as well as the program tabs
- Create a case
- Add evidence to a case
- Obtain basic analysis data

---

## WORKING WITH FTK—PART 2

This module reviews advanced FTK options and features. It also presents a “strategy of attack” that integrates FTK, PRTK, and Registry Viewer for more effective password recoveries and forensic investigations.

### Module Objectives

- Change Time Zone Display
- Identify and view compound files
- Export files and folders
- Create custom column settings to manage the information that appears in the FTK file list
- Use the Copy Special and Export File List features
- Create and manage bookmarks
- Perform analysis functions, such as full text indexing, after evidence has been added to the case
- Perform automatic and manual data carving functions
- Acquire Remote Live Evidence

## PROCESSING THE CASE

To successfully process a case, you must be able to locate the content you’re looking for, clearly mark it so you can access it as needed, and disseminate it when required.

This module details how to process a case using the powerful graphics and email features in the Forensic Toolkit® (FTK®).

### Module Objectives

- Navigate the FTK Graphics tab
- Export graphics files and hash sets
- Tag graphics files using the Bookmarks feature
- Use the Flag Thumbnail feature
- Identify supported email types
- Navigate the FTK Email tab
- Sort email
- Find a word or phrase in an email message or attachment
- Export email items
- Process Macintosh systems

## NARROWING YOUR FOCUS

This module reviews search and filter options within FTK. Participants use the Known File Filter to eliminate irrelevant file items or identify contraband files of interest based on file hashes. To narrow target items, participants use the checkmark feature to select case items, then apply specific functions to the selected items such as bookmarking, Copy Special, and exporting. Students also explore the search functions within FTK using both the DTSearch advanced options and live data searching, including introduction to regular expression pattern searches.

### Module Objectives

- Narrow evidence items using the Known File Filter (KFF), checked items, and filtered/ignored items
- Perform an indexed search
- Perform a live search
- Import search terms from text files
- Perform a regular expression search

## FILTERING THE CASE

Explains how to use FTK 3 filters to narrow focus to selected objects or a group of objects based on predefined criteria. The module demonstrates how to apply rules to new filters, import and export filters, nest filters, and utilize rule options. It also explains the differences between global and tab filters, how to use filters as a search tool, and how to apply filters to indexed searches or reports.

### Module Objectives

- Explain basic concepts of rule-based filtering in FTK
- Define a basic filter and use it to filter data
- Create filter rules
- Nest filters
- Explain the difference between global and tab filters
- Import and export filters
- Apply a filter to a report to customize output
- Apply a filter to an index search

---

## CASE REPORTING

When you perform a forensic investigation, you must be able to publish and disseminate your findings. FTK has a sophisticated report tool that allows you to systematically assemble and publish case information. During this module, students learn how to generate customized reports that include or exclude bookmarked objects, flagged graphics, and file management sections. The module also discusses report distribution options.

### Module Objectives

- Define a report
  - Modify the case information
  - Include a list of bookmarked files
  - Export bookmarked files with the report
  - Include thumbnails of bookmarked graphics
  - Manage the appearance of the Bookmark section
  - Include thumbnails of case graphics
  - Link thumbnails to full-size graphics in the report directory
  - Include a list of directories, subdirectories, files, and file types
  - Include a list of case files and file properties
  - Export case files associated with specific file categories
  - Append a registry report to the case report
- Generate reports in the following formats:
  - PDF
  - HTML
  - RTF
  - WML
  - XML
  - DOCX
  - ODF
- Generate reports in other languages



## Case Reviewer

The AccessData® Case Reviewer Training provides an introduction to using AccessData Case Reviewer. During this one-day, hands-on workshop, participants will perform the following tasks:

- Obtain basic analysis data in Case Reviewer.
- Bookmark evidence.
- Create and apply custom column and font settings.
- Locate and view graphics files.
- Locate, view, and search e-mail files and attachments.
- Perform indexed searches.
- Discuss regular expressions.

The following sections provide a brief description of each module in the Case Reviewer course with the corresponding module objectives.

- "Database Management" on page 50
- "Working with FTK—Part 1" on page 50
- "Working with FTK—Part 2" on page 51
- "Case Processing" on page 51

## DATABASE MANAGEMENT

Introduces students to the FTK Oracle database and the process of creating and managing user accounts. Participants will create users, assign user roles, and manage user rights to cases.

### Module Objectives

- Identify the components of the FTK 2 Database Management Interface.
- Create User Accounts.
- Assign rights to a case.

## WORKING WITH FTK—PART 1

This module introduces the basics of the FTK interface in Case Reviewer mode.

### Module Objectives

- Identify the following basic interface components:
  - Menu items
  - Toolbar Options
  - Tabs and Panes
  - Viewer Options
  - QuickPicks

---

## WORKING WITH FTK—PART 2

This module delves into the FTK features that are available in Case Reviewer mode. Participants will define column settings, change case time zone settings, view compound files and metadata, work with bookmarks, and use the Copy Special and Export File List features.

### Module Objectives

- Define column settings.
- Change case time zone settings.
- Set the temporary file folder.
- View compound files and their children.
- View file metadata.
- View evidence item file properties.
- Identify and process Internet/chat files in a case.
- Identify and process registry files in a case.
- Use the Copy Special feature to copy file information.
- Use the Export File List feature to export file information to a tab-delimited text file.
- Create and manage bookmarks.

## CASE PROCESSING

In this module, students work with case evidence. Participants will process graphics and email artifacts, conduct searches, and filter case files as a Case Reviewer.

### Module Objectives

- Filter case data using global and tab filters.
- Perform a live search.
- Perform a regular expression search.
- Perform an indexed search.
- Search checked files.
- Process case graphics.
- View graphics in the four FTK view modes.
- View graphics in an external viewer.
- Export hash lists.
- Process case email.



## Windows Forensics—FTK 1

The Windows Forensics FTK 1 course provides the knowledge and skills necessary to use AccessData® products to conduct forensic investigations on Microsoft Windows systems. Participants learn where and how to locate Windows system artifacts using Forensic Toolkit (FTK), FTK Imager, Registry Viewer and Password Recovery Toolkit (PRTK).

The following sections provide a brief description of each module in the Windows Forensics—FTK 1 course with the corresponding module objectives.

- "FTK Overview" on page 54
- "Regular Expressions" on page 54
- "KFF Management" on page 55
- "Windows 9x Registry" on page 56
- "Windows 2000 and XP Registries" on page 56
- "Registry Access and Concerns" on page 57
- "Working with Registry Viewer" on page 57
- "Gathering Evidence and Reporting" on page 58
- "The Recycle Bin" on page 59
- "Thumbs.db Files" on page 60
- "Metadata" on page 60
- "Link and Spool Files" on page 61
- "PRTK Alternate Features" on page 61
- "Encrypting File System" on page 62
- "Alternate Data Streams" on page 63

## FTK OVERVIEW

Provides a brief review of the FTK interface in preparation for the advanced features addressed in subsequent modules. Topics of discussion include the FTK interface, data carving data items from unallocated space and file slack, the File Filter Manager (FFM) and how it can be used to narrow an investigator's scope of focus, dtSearch functions and how they can be used to sift through large volumes of data, and an introduction to regular expressions.

During the practical, students build a test case and review key functions of the FTK application to prepare them for the Windows Forensics class.

### Module Objectives

- Navigate the FTK interface.
- List six formats the FTK Data Carving tool can recover.
- Describe the function of the File Filter Manager.
- Define the function of each dtSearch option.

## REGULAR EXPRESSIONS

Introduces the Regular Expression language and how operators and literal characters are used to find patterns of data across the suspect's evidence.

Students learn the different Operators and their function within the regular expression language, define the difference between an operator and a literal character, build basic expressions using sets and function groups, and use repeating values to maximize searching capabilities.

During the practical, students run one of the FTK default regular expressions over test data and define the hits. They then build their own expression to define a credit card search.

### Module Objectives

- Create a basic regular expression that includes the following elements:
  - Operators and Literals
  - Sets
  - Character Classes
  - Function Groups
  - Repeat Values

---

## KFF MANAGEMENT

Introduces the function and content of the Known File Filter (KFF) and demonstrates how it can be used to cull through tremendous amount of data using file hashes. The module first identifies the two sources of default hash values in the database; students then use FTK Imager and FTK to create custom hash sets and import these hash sets as either Alert or Ignore values. Students also learn how to build their own custom hash libraries and manage multiple KFF databases through FTK preferences.

During the practical, students reinforce course concepts by creating custom files, hashing them with FTK Imager, importing the values into an empty KFF, then running analysis functions within FTK using the new values. They are also required to change the alert status of existing values within the KFF database, then reprocess the case with the new KFF values.

### Module Objectives

- Describe the function of the KFF.
- List the content sources for the KFF.
- Create hash sets in FTK Imager and FTK.
- Import custom Alert or Ignorable hash sets to the KFF.
- Display hash set properties.
- Set the location of the KFF database in FTK Preferences.
- Create a KFF from an empty HDB file.
- Use the KFF Editor to change an Ignore hash set to an Alert set in the KFF.

## WINDOWS 9X REGISTRY

Introduces the Windows registry. It defines the role of the registry on Windows systems and identifies the types of evidence that can be found in registry files. Discussion focuses on the Windows 95, 98, and ME registry, providing an in depth review of the primary files that make up the registry and identifying important registry keys and values. The concept of profiles is also addressed, leading to a discussion of the forensic implications of multiple profiles on a 9x system.

During the practical, participants compare and contrast the registry structure viewed in Windows Registry Editor and AccessData's Registry Viewer.

### Module Objectives

- Describe the function of the Windows registry.
- Identify the files that make up the Windows 9x registry.
- Describe how the registry is organized.
- Identify forensic issues associated with multiple profiles on Windows 9x systems.

## WINDOWS 2000 AND XP REGISTRIES

Introduces students to the Windows NT registry. Students learn key registry files are located on Windows 2000 and XP systems and they identify the forensic evidence that can be found in each registry file. Students also learn about Security Identifiers (SIDs), how they are structured, and the forensic implications of resolving a user account to a SID. Finally, there is a discussion about the key differences between tracking user activity and system-related events on Windows 9x and NTx systems. The discussion focuses primarily on hardware devices previously mounted on the system.

During the practical, students create several user accounts, then view what happens on the system when they log in to a new account. This practical demonstrates the effects of multiple profiles on Windows 2000 and XP systems in contrast to a Windows 9x multi-profile system.

### Module Objectives

- Identify the files that make up the Windows 2000 and XP registry, list their locations, and describe the information they contain.
- Identify reasons to resolve a user to a SID.
- Identify notable tracking differences in the registry on FAT and NTFS systems.

---

## REGISTRY ACCESS AND CONCERNS

Reviews Windows 9x and NTx registry files and their associated evidence. It reviews how Microsoft protects user information within a registry file (NTUSER.DAT) and examines how this impacts software applications that are used by different accounts on the same system. A discussion about Windows' protection of active registry files leads into a demonstration of different ways to seize data from live systems (covert and overt operations). Finally, students learn about the pitfalls of the "pull the plug" approach when seizing computer hardware and how software applications update their registry values during normal operations.

During the practical, students use FTK Imager to extract active registry files from their local system.

---

**Note:** These files are later used in the Registry Viewer module.

---

### Module Objectives

- Locate registry files on Windows 9x and 2000/XP systems.
- Describe how Windows systems manage information such as instant messenger accounts for multiple user profiles.
- Describe how Windows protects active registry files.
- Describe methods of seizure that maintain the integrity of information in the registry.
- Identify overt and covert methods to access Windows registry files.
- View and export active registry files using FTK Imager and Registry Viewer.

### WORKING WITH REGISTRY VIEWER

---

**Note:** This module requires the "Working with Registry Viewer" module from the BootCamp—FTK 1 course. For more information, see "Registry Viewer Introduction" on page 34.

---

Introduces students to Registry Viewer. It includes a review of all menu items, tool bar functions, and basic operations. Students also perform advanced functions such as viewing Most Recently Used (MRU) information in chronological order and performing registry search operations.

Registry Viewer's robust reporting options are covered in great detail. Participants generate basic, single-key reports as well as detailed, customized Summary reports and they add Registry Viewer reports to FTK case reports.

## Module Objectives

- Identify the menu and toolbar options in Registry Viewer.
- Describe how Registry Viewer displays MRU lists.
- Describe the function of the Registry Viewer's common areas.
- Describe different methods to search the registry.
- Create a report in Registry Viewer and integrate the report with the FTK case report.
- Create a Summary report in Registry Viewer.
- Utilize Registry Viewer Help.
- Within FTK, view registry files and launch Registry Viewer.
- Use Registry Viewer to export registry word lists to assist password recovery.

## GATHERING EVIDENCE AND REPORTING

Focuses on gathering evidence from registry files and generating reports for case summaries. Students first compare how Registry Viewer and Windows Registry Editor display “hidden” values in the registry. The presentation then demonstrates how Registry Viewer decrypts user information contained in the Protected Storage System Provider (PSSP) key and gives users access to forensic information in the SAM, SYSTEM, and SOFTWARE registry files. The module also discusses System Restore Points in detail, outlining their function, location, and forensic importance to case investigations.

During the instructor-led practical, students use Registry Viewer to obtain forensic information from the SAM, SYSTEM, SOFTWARE, and NTUSER.DAT registry files. Students are guided through reporting techniques on single registry files, including advanced summary reports that pull from different locations within a single file. These summary reports are then saved for future use.

## Module Objectives

- Identify hidden key values in the registry.
- Decrypt user information from the PSSP key.
- Use the SAM file to determine a user's last logon time.
- Use the SYSTEM file to determine a computer's time bias.
- Use the SOFTWARE file to determine a computer's current settings.
- Describe the function of Windows restore points.
- Identify what versions of Windows maintain restore points.
- List the information stored in Windows restore points.

---

## THE RECYCLE BIN

In this module, students learn the characteristics of the Windows Recycle Bin; the differences between the Recycle Bin on Windows 9x, 2000, and XP systems; and the differences between a Recycle Bin on a FAT or NTFS volume. Additionally, the module discusses the INFO2 file in detail. It outlines the structure, byte by byte, of this administrative file and details the forensic artifacts that can be obtained within.

The module also examines the forensic issues that arise when a user deletes a single file from the Recycle Bin or empties the Recycle Bin. This leads to a discussion of orphan files and folders on NTFS volumes and how to interpret the information displayed in FTK and FTK Imager. Finally, students create a regular expression to locate INFO2 files in unallocated space.

During the instructor-led lab, students create files, send files to the Recycle Bin, then observe the results in the Recycle Bin folder using FTK. Following this exercise, students recover INFO2 data using the INFO2 regular expression.

### Module Objectives

- Describe the function of the Windows Recycle Bin.
- Identify the differences in the Recycle Bin on FAT and NTFS systems.
- List what information can be recovered from the INFO2 file.
- Describe how FTK parses and displays INFO2 files.
- Describe what happens when a file is deleted or removed from the Recycle Bin.
- Explain what happens when a user empties the Recycle Bin.
- Identify how forensic information can still be retrieved when items are removed from the Recycle Bin.
- Describe the forensic implications of files located in the Recycle Bin.
- Describe the function of the Orphan folder.
- Create a regular expression to recover unallocated INFO2 file records.

## THUMBS.DB FILES

Takes a close look at Thumbs.db files. It outlines what they are, how they get there, and their forensic implications. Students learn the characteristics of Thumbs.db files on different versions of Windows, how the database is populated, and what happens to the database entries when the original file is deleted.

Students then look at how FTK categorizes Thumbs.db files, where it displays the database information, and the optimal way to view and bookmark Thumbs.db entries for case reporting. Finally, the module discusses how EFS handles Thumbs.db files in relation to the original file data.

The practical reinforces students' understanding of the different implementations of the Thumbs.db files by reviewing all versions (Windows ME, 2000, XP, and 2003) in FTK.

### Module Objectives

- Describe how files are created in the Thumbs.db database file.
- Describe what happens to the Thumbs.db file when a graphic is deleted.
- Describe how different operating systems handle Thumbs.db files.
- Describe how Thumbs.db files handle EFS encrypted files.
- Identify how FTK classifies and displays Thumbs.db files.

## METADATA

Introduces students to metadata. The module begins by defining metadata and its purpose. This is followed by a review of the different types of metadata stored within a Microsoft Word document and the forensic value of evidence such as the document's created time, authors, and other embedded data not immediately viewed by the author. Other types of metadata are also discussed along with Fast Save and methods to view metadata outside of FTK.

The practical focuses on managing metadata in Word documents. Students create metadata, then view the results in FTK. They also create and view Fast Save edits in a Word document.

### Module Objectives

- Define metadata.
- Identify information commonly captured as metadata.
- Identify how FTK classifies and displays metadata.

---

## LINK AND SPOOL FILES

Discusses the forensic evidence associated with Windows shortcuts and print spool files. Students first learn how to recognize link files and identify common locations. The discussion then focuses on forensic evidence that can be gleaned from link files and how to interpret link file information.

The module then turns to print spool files. It outlines the path a print job takes when it is sent to a local or remote printer and demonstrates how to interrupt this path in order to maintain the print data on the system drive. Students learn about the two files Windows creates when a print job is started, their location, structure, and how to interpret the files' information.

During the practical, students examine their own Windows shortcuts for local and remote files in FTK, then examine print files by seeding the system with print job data to view in FTK.

### Module Objectives

- Define the function of a link file.
- Identify what evidentiary information is contained in link files.
- Describe how FTK parses and displays link files.
- Define the function of a spool file and its related files.
- Identify what evidentiary information is contained in spool files.

## PRTK ALTERNATE FEATURES

---

**Note:** This module requires the “Working with PRTK” module from the BootCamp—FTK 1 course. For more information, see “Working with PRTK” on page 34.

---

Introduces the student to alternate features built into PRTK. The module outlines the Windows logon password decryption process so students can obtain a suspect’s password. (In the EFS module, participants use this information to decrypt EFS files.) The module also focuses on recovering passwords stored in registry files and obtaining search queries stored in the NTUSER.DAT file. It reviews how and why you import dictionaries into PRTK and how to create a good profile.

During the practical, students enhance their understanding of PRTK by analyzing an NTUSER.DAT file, reading the information PRTK returns, importing a custom dictionary, then using the custom dictionary to create a profile against a Word document that is encrypted with extended ASCII characters.

## Module Objectives

- Describe the following feature enhancements in PRTK:
  - EFS decryption modules
  - SAM and Syskey decryption
  - Dragging-and-dropping registry files
    - PSSP information
    - Outlook and Express account passwords
    - Internet Messenger client passwords
  - Extended ASCII passwords
- Describe the process of acquiring logon passwords contained in the SAM file.

## ENCRYPTING FILE SYSTEM

Gives students an understanding of how the Encrypting File System (EFS) works and how EFS file data can be recovered. The presentation begins with a detailed outline of the process a file goes through when it is encrypted by the EFS system built into Windows 2000 and XP systems. Students learn where Windows stores the encryption and decryption keys and how to exploit weaknesses within the Windows operating system to obtain these keys and decrypt the data. Students are also given detailed instruction on the steps required for FTK to decrypt EFS file data on Windows 2000 and Windows XP SP1.

The practical requires students to apply what they have learned by seeding EFS encrypted data on an NTFS volume for processing within FTK and PRTK.

## Module Objectives

- Describe how EFS works.
- List what information is required to recover EFS-encrypted files on Windows 2000 systems.
- List what information is required to recover EFS-encrypted files on Windows XP Professional Service Pack 1 (SP1) and later systems.
- List potential problems associated with recovering EFS-encrypted data.

## ALTERNATE DATA STREAMS

Discusses another NTFS feature: alternate data streams (ADS). Students review the common uses of ADSs within the file system as well as their malicious use to hide data from Windows Explorer. Students learn how to differentiate between default data streams and an ADS associated with file record entries in the MFT. The discussion focuses on how ADSs can be created and the difficulties in detecting or removing them from the parent file entry. Finally, students learn how to process ADSs in FTK.

The practical allows students to practice the concepts discussed during the presentation by creating ADSs on regular text files, then recovering and processing this information in FTK.

### Module Objectives

- Identify the differences between named and alternate data streams.
- Identify forensic issues associated with alternate data streams.
- Identify how FTK displays alternate data streams.
- Describe how alternate data streams impact file size, disk space, and file creation date.



## Windows Forensics—FTK 3

The Windows Forensics FTK 3 course provides the knowledge and skills necessary to use AccessData® products to conduct forensic investigations on Microsoft Windows systems. Participants learn where and how to locate Windows system artifacts using Forensic Toolkit® (FTK™), FTK Imager™, Registry Viewer™, and Password Recovery Toolkit™ (PRTK™).

The following sections provide a brief description of each module in the Windows Forensics—FTK 3 course with the corresponding module objectives.

- "Regular Expressions" on page 66
- "Windows Registry 101" on page 66
- "Windows 2000 and XP Registries" on page 67
- "Working with Registry Viewer" on page 67
- "Gathering Evidence and Reporting" on page 68
- "The Recycle Bin" on page 69
- "Thumbs.db Files" on page 70
- "Metadata" on page 70
- "Link and Spool Files" on page 71
- "Alternate Data Streams" on page 72
- "Windows XP Prefetch" on page 72
- "Working with PRTK" on page 73
- "Working with PRTK" on page 73
- "Encrypting File System" on page 74

## REGULAR EXPRESSIONS

Introduces the Regular Expression language and how operators and literal characters are used to find patterns of data across the suspect's evidence.

Students learn the different Operators and their function within the regular expression language, define the difference between an operator and a literal character, build basic expressions using sets and function groups, and use repeating values to maximize searching capabilities.

During the practical, students run one of the FTK default regular expressions over test data and define the hits. They then build their own expression to define a credit card search.

### Module Objectives

- Understand basic Operators and Literals in RegEx
- Learn 10 very useful characters and concepts of RegEx++ so students can write hundreds of expressions
- Create and interpret a basic regular expression that includes Function Groups and Repeat Values
- Integrate a new RegEx into FTK for use

## WINDOWS REGISTRY 101

Introduces the Windows registry. It defines the role of the registry on Windows systems and identifies the types of evidence that can be found in registry files. Discussion provides an in-depth review of the primary files that make up the registry and identifying important registry keys and values. The concept of profiles is also addressed, leading to a discussion of the forensic implications of multiple profiles on Windows systems.

### Module Objectives

- Describe the function of the Windows registry
- Identify the files that make up the Windows registry
- Describe how the registry is organized
- Identify forensic issues associated with multiple profiles on Windows systems

## WINDOWS 2000 AND XP REGISTRIES

Introduces students to the Windows NT registry. Students learn about key registry files located on Windows 2000 and XP systems and they identify the forensic evidence that can be found in each registry file. Students also learn about Security Identifiers (SIDs), how they are structured, and the forensic implications of resolving a user account to a SID. Finally, there is a discussion about the key differences between tracking user activity and system-related events on Windows 9x and NTx systems. The discussion focuses primarily on hardware devices previously mounted on the system.

During the practical, students create several user accounts, then view what happens on the system when they log in to a new account. This practical demonstrates the effects of multiple profiles on Windows 2000 and XP systems in contrast to a Windows 9x multi-profile system.

### Module Objectives

- Identify the files that make up the Windows 2000 and XP registry, list their locations, and describe the information they contain
- Identify reasons to resolve a user to a SID
- Identify notable tracking differences in the registry on FAT and NTFS systems including a look at tracking mounted devices

### WORKING WITH REGISTRY VIEWER

Introduces students to Registry Viewer. It includes a review of all menu items, toolbar functions, and basic operations. Students also perform advanced functions such as viewing Most Recently Used (MRU) information in chronological order and performing registry search operations.

Registry Viewer's robust reporting options are covered in great detail. Participants generate basic, single-key reports as well as detailed, customized Summary reports and they also add Registry Viewer reports to FTK case reports.

## Module Objectives

- Identify the menu and toolbar options in Registry Viewer
- Describe how Registry Viewer displays MRU lists
- Describe the function of the Registry Viewer's common areas
- Describe different methods to search the registry
- Create a report in Registry Viewer
- Create a Summary report in Registry Viewer
- Utilize Registry Viewer help
- Utilize Registry Viewer help.

## GATHERING EVIDENCE AND REPORTING

Focuses on gathering evidence from registry files and generating reports for case summaries. Students first compare how Registry Viewer and Windows Registry Editor display “hidden” values in the registry. The presentation then demonstrates how Registry Viewer decrypts user information contained in the Protected Storage System Provider (PSSP) key and gives users access to forensic information in the SAM, SYSTEM, and SOFTWARE registry files. The module also discusses System Restore Points in detail, outlining their function, location, and forensic importance to case investigations.

During the instructor-led practical, students use Registry Viewer to obtain forensic information from the SAM, SYSTEM, SOFTWARE, and NTUSER.DAT registry files. Students are guided through reporting techniques on single registry files, including advanced summary reports that pull from different locations within a single file. These summary reports are then saved for future use.

## Module Objectives

- Identify hidden key values in the registry
- Decrypt user information from the PSSP key
- Use the SAM file to determine a user's last logon time
- Use the SYSTEM file to determine a computer's time bias
- Use the SOFTWARE file to determine a computer's current settings
- Describe the function of Windows restore points
- Identify what versions of Windows maintain restore points
- List the information stored in Windows restore points

---

## THE RECYCLE BIN

Discusses the characteristics of the Windows Recycle Bin; the differences between the Recycle Bin on Windows 9x, 2000, and XP systems; and the differences between a Recycle Bin on a FAT or NTFS volume. Additionally, the module discusses the INFO2 file in detail. It outlines the structure, byte by byte, of this administrative file and details the forensic artifacts that can be obtained within.

The module also examines the forensic issues that arise when a user deletes a single file from the Recycle Bin or empties the Recycle Bin. This leads to a discussion of orphan files and folders on NTFS volumes and how to interpret the information displayed in FTK and FTK Imager. Finally, students create a regular expression to locate INFO2 files in unallocated space.

During the instructor-led lab, students create files, send files to the Recycle Bin, then observe the results in the Recycle Bin folder using FTK. Following this exercise, students recover INFO2 data using the INFO2 regular expression.

### Module Objectives

- Describe the function of the Windows XP Recycle Bin
- Identify the differences in the Recycle Bin on FAT and NTFS systems
- List what information can be recovered from the INFO2 file
- Describe how FTK parses and displays INFO2 files
- Describe what happens when a file is deleted or removed from the Recycle Bin
- Explain what happens when a user empties the Recycle Bin
- Identify how forensic information can still be retrieved when items are removed from the Recycle Bin
- Describe the forensic implications of files located in the Recycle Bin
- Describe the function of the Orphan folder
- Use a regular expression to recover unallocated INFO2 file records

## THUMBS.DB FILES

Takes a close look at Thumbs.db files. It outlines what they are, how they get there, and their forensic implications. Students learn the characteristics of Thumbs.db files on different versions of Windows, how the database is populated, and what happens to the database entries when the original file is deleted.

Students then look at how FTK categorizes Thumbs.db files, where it displays the database information, and the optimal way to view and bookmark Thumbs.db entries for case reporting. Finally, the module discusses how EFS handles Thumbs.db files in relation to the original file data.

The practical requires students to recover the thumb.db archive in FTK.

### Module Objectives

- Define the Thumbs.db file
- Define Thumbs.db behavior
- Identify thumbnail graphics
- Define EFS file changes and Thumbs.db behavior

## METADATA

Introduces students to metadata. The module begins by defining metadata and its purpose. This is followed by a review of the different types of metadata stored within a Microsoft Word document and the forensic value of evidence such as the document's created time, authors, and other embedded data not immediately viewed by the author. Other types of metadata are also discussed, along with Fast Save and methods to view metadata outside of FTK.

During the practical, students review metadata in FTK.

### Module Objectives

- Define metadata
- Identify information commonly captured as metadata
- Identify how FTK classifies and displays metadata

## LINK AND SPOOL FILES

Discusses the forensic evidence associated with Windows shortcuts and print spool files. Students first learn how to recognize link files and identify common locations. The discussion then focuses on forensic evidence that can be gleaned from link files and how to interpret link file information.

The module then turns to print spool files. It outlines the path a print job takes when it is sent to a local or remote printer and demonstrates how to interrupt this path in order to maintain the print data on the system drive. Students learn about the two files Windows creates when a print job is started, their location, structure, and how to interpret the files' information.

During the lab, students recover information from links to documents and machines in the Recents folder. Students also use link files to associate a file with a removable drive. During the practical, students process SHD and SPL files to obtain information about the associated printer and print jobs.

### Module Objectives

- Define the function of a link file
- Identify what evidentiary information is contained in link files
- Describe how FTK parses and displays link files
- Define the function of a spool file and its related files
- Identify what evidentiary information is contained in spool files

## ALTERNATE DATA STREAMS

Discusses another NTFS feature: alternate data streams (ADS). Students review the common uses of ADSs within the file system as well as their malicious use to hide data from Windows Explorer. Students learn how to differentiate between default data streams and an ADS associated with file record entries in the MFT. The discussion focuses on how ADSs can be created and the difficulties in detecting or removing them from the parent file entry. Finally, students learn how to process ADSs in FTK.

The practical allows students to recover and process alternate data streams in FTK.

### Module Objectives

- Identify the differences between named and alternate data streams
- Identify forensic issues associated with alternate data streams
- Identify how Forensic Toolkit® (FTK®) displays alternate data streams
- Describe how alternate data streams impact file size, disk space, and file creation date

## WINDOWS XP PREFETCH

Describes Prefetch, Superfetch, and their related functions. Students will locate prefetch files in the file system, review prefetch settings in the Windows registry, and review the layout.ini file to recover filenames and paths of documents loaded with applications.

The practical requires students to identify prefetch values in the Windows registry and locate prefetch files in the file system. Students will then use FTK Imager to identify the dates and times that applications were launched on the computer.

### Module Objectives

- Accurately define Prefetch, Superfetch, and their related functions
- Define the forensic importance of Prefetch Registry entries, Prefetch files, and the Layout.ini file
- View and analyze pertinent Prefetch artifacts as they relate to case analysis and user behavior

---

## WORKING WITH PRTK

Introduces the PRTK 6 interface and the modules used to crack different types of applications and encrypted file data. Students review the different types of attack and the decryption process, importing custom dictionaries, defining biographical dictionaries, and creating attack profiles.

Students are also introduced to the AccessData methodology—a file recovery strategy that leverage indexed information from the case to build custom dictionaries and recover encrypted files.

During the practical, students export encrypted files from a case for recovery in PRTK. Students are required to build a biographical dictionary, an attack profile, and export the word list from FTK to create a custom dictionary in PRTK. Students then start an attack session to recover the encrypted files.

### Module Objectives

- Navigate within the PRTK interface
- Identify the available password recovery modules and their associated attack types
- Import user-defined dictionaries and FTK word lists to use in a password recovery attack
- Create biographical dictionaries
- Set up profiles
- Explain what a PRTK profile is and how it is used
- Recount the AccessData Methodology

### PRTK ALTERNATE FEATURES

Introduces the student to alternate features built into PRTK. The module outlines the Windows logon password decryption process so students can obtain a suspect's password. (In the EFS module, participants use this information to decrypt EFS files.) The module also focuses on recovering passwords stored in registry files and obtaining search queries stored in the NTUSER.DAT file. It reviews how and why you import dictionaries into PRTK and how to create a good profile.

During the practical, students enhance their understanding of PRTK by analyzing an NTUSER.DAT file, reading the information PRTK returns, importing a custom dictionary, then using the custom dictionary to create a profile against a Word document that is encrypted with extended ASCII characters.

## Module Objectives

- Describe the following feature enhancements in PRTK:
  - EFS decryption modules
  - SAM and SysKey decryption
  - Dragging-and-dropping registry files
    - PSSP information
    - Outlook and Express account passwords
    - Internet Messenger client passwords
  - Extended ASCII passwords
- Describe the process of acquiring logon passwords contained in the SAM file

## ENCRYPTING FILE SYSTEM

Gives students an understanding of how the Encrypting File System (EFS) works and how EFS file data can be recovered. The presentation begins with a detailed outline of the process a file goes through when it is encrypted by the EFS system built into Windows 2000 and XP systems. Students learn where Windows stores the encryption and decryption keys and how to exploit weaknesses within the Windows operating system to obtain these keys and decrypt the data. Students are also given detailed instruction on the steps required for FTK to decrypt EFS file data on Windows 2000 and Windows XP SP1.

The practical requires students to apply what they have learned by seeding EFS encrypted data on an NTFS volume for processing within FTK and PRTK.

## Module Objectives

- Describe how EFS works
- List what information is required to recover EFS encrypted files on Windows 2000 systems
- List what information is required to recover EFS encrypted files on Windows XP Professional Service Pack 1 (SP1) and later systems
- List potential problems associated with recovering EFS encrypted data

## Windows Forensics—Vista

The Windows Vista course provides the knowledge and skills necessary to analyze Microsoft Windows Vista operating system artifacts and file system mechanics using Forensic Toolkit<sup>®</sup> (FTK<sup>®</sup>), FTK Imager, Password Recovery Toolkit<sup>®</sup> (PRTK<sup>®</sup>), and Registry Viewer<sup>®</sup>.

The following sections provide a brief description of each module in the Windows Forensics—Vista course with the corresponding module objectives.

- "Understanding BitLocker Drive Encryption" on page 76
- "Working with GUID Partition Tables" on page 77
- "Vista Security and File Structure" on page 77
- "Windows Vista Registry—Introduction" on page 78
- "Windows Vista Registry—Registry File Artifacts" on page 78
- "Windows Vista Registry—ReadyBoost and DPAPI" on page 79
- "Windows Vista Event Logs" on page 79
- "Windows Vista Shadow Copy" on page 80
- "Windows Vista Recycle Bin" on page 81
- "Windows Vista ThumbCache" on page 81
- "Windows Vista Superfetch (Prefetch)" on page 82

## UNDERSTANDING BITLOCKER DRIVE ENCRYPTION

Explains why BitLocker encryption— incorporated in the high-end versions of Windows Vista—is likely to be the greatest concern to digital investigators. This module reviews some of the core functions related to acquiring BitLocker-encrypted evidence. Students first learn how to identify an encrypted volume. The course then presents different ways to decrypt and forensically acquire data from a BitLocked drive.

During the practical, students access a BitLocked drive using recovery keys, then image the drive using traditional techniques.

### Module Objectives

- Describe the BitLocker full volume encryption system
- Determine which versions of Vista support BitLocker
- Describe how BitLocker works, specifically:
  - How BitLocker encrypts and decrypts the drive
  - How BitLocker interacts with the system when it boots
  - When encryption and decryption occur
  - What to do when BitLocker locks out to the Recovery Mode
- Identify the requirements necessary to enable BitLocker
- Describe how a Trusted Platform Module (TPM) chip functions in the BitLocker process
- Identify which portions of the drive are encrypted
- List the user options available to protect a BitLocker drive
- Describe the Recovery Mode and what causes BitLocker to invoke it
- Identify a BitLocker drive and its accompanying recovery key sets
- Name the items to look for during search and seizure to unlock a BitLocker drive
- Identify the different imaging methods for BitLocker and when and how to apply them
- Prepare the investigative machine to image a BitLocker drive
- Successfully unlock and image a BitLocker encrypted drive

---

## WORKING WITH GUID PARTITION TABLES

Introduces the changes in the NT file system. This includes a detailed outline of the new GUID partition table scheme potentially used on Vista systems to define partition structures on hard disk drives. The module also provides a brief overview of Vista's transactional logging feature.

During the practical, students view raw data from a GPT disk using FTK Imager.

### Module Objectives

- Discuss the Vista upgrades to NTFS 3.1.
- Describe the format and structure of the GUID Partition Table HDD format system.
- Effectively read a new GPT notation.
- List the rules and limitations of a GPT.

## VISTA SECURITY AND FILE STRUCTURE

Addresses security and operating system protection, as well as the file structure and default user data locations. During this module, students are introduced to the new security model Microsoft Vista uses to protect the operating system from malicious programs. Students explore Protected Mode functions to understand Vista's underpinnings and why certain artifacts appear where they do.

The module also identifies security and file artifacts that have undergone little or no change from the Windows XP operating system.

### Module Objectives

- Describe the three-tiered layer of the new Vista security model.
- Describe and identify a reparse point in Vista.
- Effectively navigate the Vista file structure.
- Identify new locations for old Windows artifacts.

## WINDOWS VISTA REGISTRY—INTRODUCTION

---

**Note:** This module requires the “Working with Registry Viewer” module from the BootCamp—FTK 3 course. For more information, see “Working with Registry Viewer” on page 37.

---

Introduces students to the Windows Vista registry. It lists the key files that make up the Vista registry hives and explains where to locate these files on a Vista system. Students access the registry on live systems and discuss the choices first responders must make when evidence may still be accessed by the operating system.

During the practical, students extract registry files from an image file using FTK Imager.

### Module Objectives

- Define the Vista registry.
- Describe the forensics benefits of the registry.
- Describe the registry structure.
- Describe how to navigate the registry.
- Describe how to access the registry.

## WINDOWS VISTA REGISTRY—REGISTRY FILE ARTIFACTS

---

**Note:** This module requires the “Working with Registry Viewer” module from the BootCamp—FTK 3 course. For more information, see “Working with Registry Viewer” on page 37.

---

Continues the discussion of the registry in the Windows Vista operating system and discusses specific registry files of forensic importance: Security Accounts Manager (SAM), SYSTEM, SOFTWARE, SECURITY, and NTUSER.DAT. Participants search the registry for specific values, resolve users to a SID, and list changes to SAM file subkeys and values.

### Module Objectives

- Describe changes in Registry artifacts in the NTUSER.DAT file in Windows Vista.
- Locate the new Protected Storage area in the NTUSER.DAT and describe how it is encrypted.
- Locate legacy artifacts in NTUSER.DAT such as MRU lists, RecentDocs, and Comdlg32.
- Identify how to resolve a user to a SID using the SAM file.
- Describe changes to SAM file subkeys and values in Vista.

- Locate artifacts in the SYSTEM file such as TimeZoneInformation and the Last Accessed time.

## WINDOWS VISTA REGISTRY—READYBOOST AND DPAPI

---

**Note:** This module requires the “Working with Registry Viewer” module from the BootCamp—FTK 3 course. For more information, see “Working with Registry Viewer” on page 37.

---

Continues the discussion of the registry in the Windows Vista operating system. It discusses the definition, function, and forensic importance of ReadyBoost and Windows DPAPI (Protected Storage in XP and Protected Storage in Vista).

During the practical, students use PRTK to decrypt values within the registry and report back the results for case analysis. The practical also focuses on recovering ReadyBoot USB information from registry files.

### Module Objectives

- Describe what ReadyBoost is and how it functions
- Identify what USB drive information is stored in the registry and where
- Compare and contrast the Protected Storage System Provider (PSSP) in Windows 2000/XP systems with Windows Vista DPAPI
- List the steps required to decrypt the protected information located in the IntelliForms subkey
- List the steps required to break the user’s logon password

## WINDOWS VISTA EVENT LOGS

Describes the function of Windows Vista event logging and identifies forensic artifacts that may be recovered from various system-related events stored within the log files. Students list the default log files, identify their location, and read information from the log files using Vista’s built-in viewer.

During the practical, students generate events in the local logs, then review the logs on a separate machine.

## Module Objectives

- Describe the difference between Windows XP and Windows Vista event logs
- Identify where event logs are stored on Windows Vista systems
- Navigate the Windows Vista Event Viewer
- Using the Windows Vista Event Viewer, view and correlate the following types of events:
  - Shutdown
  - USB installation
  - Time change events
  - Wireless connections
  - ReadyBoost attachments

## WINDOWS VISTA SHADOW COPY

Compares the restore points found on earlier versions of Windows with the new shadow copies found on various versions of Windows Vista. Shadow copy location and management are detailed followed by a discussion of forensic artifacts that can be carved from shadow copy files.

During the practical, students use FTK to data carve deleted file data from shadow copies.

## Module Objectives

- Compare and contrast the function of restore points in Windows XP/2000 and Windows Vista.
- Describe what shadow copies are and how they are used on Vista systems.
- Use Volume Shadow Copy Administration (VSSADMIN) to manage shadow copies.
- Use the Data Carving feature in FTK 3 to recover information from shadow copies.
- List the system information stored in shadow copies.

---

## WINDOWS VISTA RECYCLE BIN

Begins with a review of the recycle bin functions on Windows XP systems, including user account deletion and the structure of the Info2 file. This is followed by a detailed look at the structure of the \$Recycle.bin found on Windows Vista systems and the relationship between the \$R and \$I file pair. Students learn about the new wiping processes the operating system undertakes when objects are deleted from the bin. This leads to a discussion about orphan files and folders on a NTFS volumes and how to interpret the corresponding information in FTK and FTK Imager.

### Module Objectives

- Compare and contrast the Windows XP Recycler with the Vista \$Recycle.Bin
- Describe the structure of the Vista \$Recycle.Bin
- Describe the process required to wipe the \$Recycle.Bin
- Describe the differences between deleted files and orphaned files
- Describe how NTFS uses the \$MFT to track individual files
- List the values used to designate file status in the \$Recycle.Bin
- Recover deleted file information

## WINDOWS VISTA THUMBCACHE

Compares Windows XP thumbs.db files with the new Vista ThumbCache files. Students learn about the Vista ThumbCache database and identify the file location within the user profile.

During the practical, students examine the architecture of ThumbCache files then review the files in FTK 3.

### Module Objectives

- Compare and contrast thumbs.db files on Windows XP and 2000 systems with ThumbCache files in Windows Vista
- Identify where all thumbnail images are stored in Windows Vista
- Review ThumbCache files in FTK
- Identify the values stored in every ThumbCache record
- Identify and analyze Windows Photo Gallery activity

## WINDOWS VISTA SUPERFETCH (PREFETCH)

Describes the function of the Windows Prefetch operation and identifies the forensic implications of data stored on application use. The discussion then focuses on the new Windows Vista Superfetch function with a detailed review of the forensic implications of data stored within the Prefetch files.

During the practical, students populate Prefetch files, then analyze the data in FTK 3.

### Module Objectives

- Accurately define Prefetch, SuperFetch\*, and their related functions
- Define the forensic importance of Prefetch Registry entries, Prefetch files, and the Layout.ini file
- View and analyze pertinent Prefetch artifacts as they relate to case analysis and user behavior

## Windows Forensics Registry

The Windows Forensics Registry course provides the knowledge and skills necessary to use AccessData products to conduct forensic investigations on the Microsoft Windows registry. Participants learn where and how to locate registry artifacts using Forensic Toolkit (FTK), FTK Imager, Registry Viewer, and Password Recovery Toolkit (PRTK).

The following sections provide a brief description of each module in the Windows Forensics—Registry course with the corresponding module objectives.

- "Registry Utilities" on page 84
- "Registry 201" on page 85
- "Preliminary Reports" on page 86
- "SAM Artifacts" on page 86
- "SYSTEM Artifacts" on page 87
- "SECURITY Artifacts" on page 88
- "SOFTWARE Artifacts" on page 88
- "Application Behavior 1" on page 90
- "Application Behavior 2" on page 91

## REGISTRY UTILITIES

Covers forensic and nonforensic access to the registry. It provides an overview of basic registry editing and backup methods using Microsoft utilities such as Regedit and Restore Points. It also includes a discussion on viewing and editing registry permissions and how they can affect a forensic investigation. The module then discusses registry acquisition using FTK and FTK Imager in detail. Following registry acquisition, the module covers the use of the AccessData Registry Viewer utility for forensic examination of logical registry files. The Registry Viewer section discusses registry navigation, viewing registry properties, searching, and reporting methods.

The practical requires hands-on use of Regedit and Registry Viewer to back up, acquire, and analyze registry files.

### Module Objectives

- Use Regedit or Regedit32 to view and edit registry settings.
- List four ways to back up the registry.
- Back up individual keys and values.
- List four ways to restore .reg files.
- Create a hive backup.
- Export registry keys and values to a text file.
- Create a set of restore points.
- Modify subkey permissions.
- Export registry files from FTK.
- Use FTK Imager to harvest live registry files.
- Use Registry Viewer to search registry values.
- Generate registry reports in Registry Viewer.

---

## REGISTRY 201

---

**Note:** This module requires the “Working with Registry Viewer” module from the BootCamp—FTK 3 course. For more information, see “Working with Registry Viewer” on page 37.

---

Provides a basic overview of the Windows registry. The module begins by defining the registry, identifying its function in the operating system, and discussing its history and the issues it creates, and then ends with a commentary on the forensic benefits of the registry. The basic composition of the registry—including the hive, key, and subkey structure—is thoroughly covered, and participants navigate the registry structure using both Regedit and Registry Viewer.

The module then examines the registry block structure—a representation of the registry as a file system within itself—and explores how the blocks and individual registry cells interrelate. This is followed by a discussion of methods, such as keyword searches and regular expressions, to locate deleted and slack data within the physical structure of the registry.

During the practical, students modify the registry, delete registry data, then recover data from unallocated registry space.

### Module Objectives

- Define the Windows registry structure and function.
- List registry issues that can cause problems with individual applications and in booting the system.
- List the forensic benefits of the registry.
- Identify the hives that make up the registry and list the types of information associated with each hive.
- Identify where the user’s NTUSER.DAT file is located.
- Identify the standard registry data types.
- Navigate the registry in regedit32.
- Navigate the registry in Registry Viewer.
- Define the registry block structure.
- Identify the seven data structures in the hbin blocks that define the registry keys, subkeys, and values.
- Track a subkey to its values.
- Recover deleted data in the registry and registry slack.

## PRELIMINARY REPORTS

Reviews FTK preliminary reports, a feature that generates preliminary reports of the registry without direct examination of the associated registry files. For more detailed reporting, the module lists types of data that are important to document for each case. Each of the basic registry files—such as SAM, SYSTEM, and SOFTWARE—are analyzed for basic information. The module then reviews the standard and summary report utilities available in Registry Viewer.

During the practical, students view preliminary data in the registry and generate reports.

### Module Objectives

- Generate a preliminary case report (PCR).
- List the registry information that should be included in a PCR.
- Describe how data is added to standard reports.
- List the types of information that can be included in summary reports.
- List the benefits of summary reports.

## SAM ARTIFACTS

Covers the forensic aspects of the Security Accounts Manager (SAM) file. It begins with a description of the SAM file and how it tracks users and system security functions. The module defines Security identifiers (SIDs) and Relative Identifiers (RIDs) and demonstrates how they can be used to track user behavior such as network logons, Recycle Bin activity, and Restore Points access. User accounts are analyzed with a focus on suspect activity and data such as passwords, usernames, date and time of logon, and logon counts. The module also discusses how to determine if a password has been applied to an account without having to boot the system. Finally, groups and custom group creation are covered with an emphasis on identifying groups that may have been created by a suspect.

During the practical, students create, remove, and modify user accounts, then view the effects to the registry.

## Module Objectives

- Identify where the SAM file is located in the registry.
- Describe the function of the SAM file.
- List what type of data is stored in the SAM file.
- Identify two ways you can access the SAM file.
- Describe the three components that make up a SID.
- List the user account information stored in the SAM file.
- Parse the F and V values to identify user login information.
- Recover a user's Windows login password.
- Recover a user account name that has been changed or deleted.
- Use the SAM and NTUSER.DAT files to identify a user's group membership.

## SYSTEM ARTIFACTS

Addresses the system artifacts available to the investigator. The SYSTEM file contains a tremendous amount of information about the physical system and operating system. This discussion covers basic artifacts such as Time Zone information, computer name, and when the system was last shutdown. It also includes a detailed analysis of how to identify devices that were attached to the system such as hard disk drives, USB devices, floppy drives, and mass storage devices; when they were first installed; and device drive size. Finally, the module covers memory management, how to determine whether a suspect has set his machine up to wipe the active swap file on shutdown, and (on Vista systems) if the last accessed date is activated.

During the practical, students experiment with different system devices, then view the changes in the registry keys.

## Module Objectives

- Identify where the SYSTEM file is located in the registry.
- Describe the function of the SYSTEM file.
- List what type of data is stored in the SYSTEM file.
- Identify the four subkeys that make up the SYSTEM control set.
- Use the SYSTEM file to recover the following information:
  - The correct time zone setting on a Windows XP or Vista machine.
  - Whether a Vista system's default setting that disables the last accessed date/time has not been turned back on.

- The computer name.
- The last shutdown time.
- Mounted devices.
- Hardware information, including floppy disks, hard disk drives, mass storage devices, and printers.
- Services available to the system.
- How memory is configured, where the swap file is located, and what are Prefetch settings.
- Link a USB device to a specific computer.

## SECURITY ARTIFACTS

Reviews the function of the SECURITY file and its associated forensic data: passwords and historical password lists. The module also demonstrates how the local user's last two passwords can potentially be recovered with a quick decryption attack on the SECURITY file rather than the standard dictionary or rainbow table attacks used on a SAM file user's password. If successful, this password recovery method is much quicker than traditional methods.

During the practical, students recover cached passwords from the SECURITY file.

### Module Objectives

- Identify where the SECURITY file is located in the registry.
- Describe the function of the SECURITY file.
- List what type of data is stored in the SECURITY file.
- Distinguish between permissions, policies, and rights.
- Identify what types of passwords can be recovered from the SECURITY file.
- Recover cached passwords.

## SOFTWARE ARTIFACTS

Provides a thorough discussion of the SOFTWARE registry file. After defining the function and location of the file, the module demonstrates how to recover the following types of information from it:

- Registered user information, including who installed the system, operating system version, and date/time of installation
- Uninstalled software information
- Startup programs (including malware) that launch during bootup or from the command line and which may be hidden from the user

- Class identifiers (CLSIDs) that can be used to identify programs (and their file associations) used by the suspect
- Wireless connections which can be used to determine the SSID of the machine hosts that the suspect has visited
- Winlogon information which can determine whether a user configured his machine to autologon
- Recycle Bin properties
- Detailed printer information

The module also addresses ReadyBoost (in Windows Vista, ReadyBoost is the use of USB drives as supplemental memory) since it identifies individual USB devices that have been attached to the machine by volume identifier and volume label.

During the practical, students recover forensic artifacts from a SOFTWARE registry file.

## Module Objectives

- Identify where the SOFTWARE file is located in the registry
- Describe the function of the SOFTWARE file
- List what type of data is stored in the SOFTWARE file
- Describe the function of the Vista ReadyBoost feature and identify what information it stores in the SOFTWARE file
- Use the SOFTWARE file to recover the following information:
  - Evidence of uninstalled software
  - Startup locations used to load applications or executable files during the boot process
  - The Class Identifiers (CLSIDs) for operating system objects such as applications and ActiveX controls
  - The Service Set Identifier (SSID) used to identify the user's wireless connection
  - Winlogon and Autologon information
  - Recycle Bin properties
  - Printer information
- Create a File Types report in Registry Viewer
- List the two types of wireless artifacts found in Windows XP
- Identify where wireless artifacts are found in Windows Vista

## APPLICATION BEHAVIOR 1

Demonstrates how to use registry components to track patterns of user behavior. Prior to looking at individual artifacts, the module discusses what happens in the file system when a user searches for a file on the Internet, views and downloads the file, then moves and shares the file. This discussion provides the groundwork to discuss advancing arguments against a Trojan Horse defense.

The module then examines user and application behavior stored in the NTUSER.DAT registry file. This file can provide a valuable record of general user behavior such as local searches and search terms; however, the information stored depends on the user's operating system and individual applications.

Other valuable sources of user behavior artifacts include Recent Documents MRU lists, Run MRU lists, and Common Dialog MRU behavior. Significant Internet Explorer browser settings and user Favorites are also discussed, as well as typed URLs and history files.

Additionally, the module teaches students how to use PRTK to access the Windows XP and Vista Protected Storage Area (PSSP) to recover email passwords, Web logon passwords, Internet search terms, and form data for the autocomplete function.

Mount points and mapped drive artifacts are also covered, as well as the use of mount points to mask the presence of another connected drive (HDD or USB).

Network connections are reviewed with an emphasis on determining what systems a user's computer may have been connected to.

UserAssist is presented to allow the investigator to determine application usage and encryption issues associated with UserAssist, and to facilitate searches for potentially uninstalled software.

The practical requires students to analyze the behavior of individual users on a Windows system.

### Module Objectives

- Use the following registry components to track patterns of user behavior:
  - NTUSER.DAT
  - Recently typed URLs in the browser
  - Recently viewed documents
  - Protected storage information that potentially contains Web login names, passwords, form data, and search queries

- Internet Explorer information
- Mount points and mapped drives
- Computer descriptions
- Workgroup Crawler
- UserAssist
- Uninstalled software
- Local search terms

## APPLICATION BEHAVIOR 2

Takes a somewhat different approach to registry artifacts. Since there are so many applications in use and they are constantly being updated and changed, an investigator must have the ability to determine what application behavior is stored in the registry for any given product version. This module teaches the methods used to make these determinations using different software utilities to view registry changes. It uses the common archiving application, WinZip, to demonstrate what Zip file artifacts are stored and where.

The practical requires students to determine the behavior and storage of artifacts for different applications.

### Module Objectives

- Outline the basic steps to follow when researching new applications for a forensic investigation.
- List some standard software tools that can help you research a new application.
- For the sample application, WinZip, use the registry to recover forensically significant information:
  - Where WinZip stores data in the registry
  - Last location extracted to
  - MRU extractions
  - Last location a zip file was created
  - Temp file location
  - Last update check
- Registered user



## Internet Forensics—FTK 1

The Internet Forensics—FTK1 course provides the knowledge and skills necessary to use AccessData tools to recover forensic information from Internet artifacts. Participants learn where and how to locate Internet artifacts using Forensic Toolkit (FTK), Registry Viewer, and Password Recovery Toolkit (PRTK).

The following sections provide a brief description of each module in the Internet Forensics—FTK 1 course with the corresponding module objectives.

- "AOL Instant Messenger" on page 94
- "Firefox" on page 94
- "Internet Explorer" on page 95
- "Yahoo Messenger" on page 96
- "Windows Messenger" on page 96
- "MSN Messenger" on page 97
- "AOL—Information from American Online" on page 97
- "AOL—Information from the Computer" on page 98
- "AOL—Personal Filing Cabinet" on page 98
- "Password Recovery" on page 99

## AOL INSTANT MESSENGER

Shows students how to recover file artifacts left behind by the AOL Instant Messaging (AIM) client, such as contact (Buddy) lists, file transfer information, and server connection times. Students also recover registry artifacts such as file transfer permissions, user profile information, and recent contacts.

During the practical, students use FTK to recover AOL file artifacts.

### Module Objectives

- Identify where AOL Instant Messenger stores the following evidentiary items in the registry:
  - Last user to be logged in to the machine
  - Registered screen names used on the machine
  - Screen names who have had contact with the local user
  - Indications of file transfer activity
  - Permissions for file sharing or file transfers
- Identify where AOL Instant Messenger stores the following evidentiary items in the file structure:
  - Buddy List location and meaning of the entries
  - Any saved instant messages
  - Direct IM
  - Linked screen names

## FIREFOX

Shows students how to recover client- and user-specific artifacts from the Firefox Internet browser application. Students identify the locations and interpret the entries for cached Web page content, cookies, bookmarks, history, typed URLs (address bar information), preferences, auto-complete and stored form data, and searches conducted with the Firefox client. Students also review the structure of a Firefox user account profile and decrypt passwords and other protected storage data using FTK and PRTK.

## Module Objectives

- Identify user data locations.
- Identify files of evidentiary interest, their location, how they are created or added to, and how they may be processed.
- Examine how Firefox stores cached Web content and how FTK handles the information.
- Identify encrypted and obfuscated information.

## INTERNET EXPLORER

Shows students how to recover user-specific information from the Internet Explorer (v6) browser client, including history, Temporary Internet Files (TIF), cookie information, preferences, favorites, and typed URLs (address bar information). Students also recover encrypted auto-complete and form data information from the registry.

During the practical, students examine Internet Explorer artifacts using FTK, Registry Viewer, and PRTK. Students also learn the necessary techniques to decrypt DPAPI-protected storage for an Internet Explorer (v7) user account.

## Module Objectives

- Identify where Internet Explorer stores the following evidentiary items in the file structure:
  - Favorites
  - Cookies
  - History
  - Temporary Internet Files
- Identify where Internet Explorer stores the following evidentiary items in the registry:
  - Typed URLs
  - Passwords
  - Protected Storage Information

## YAHOO MESSENGER

Shows students how to recover file artifacts left behind by the Yahoo! Instant Messenger client, such as file transfer information and encrypted chat files (DAT). Students also recover registry artifacts such as file transfer permissions, profile information (alias names), login information, and IMvironment information.

During the practical, students collect and bookmark Yahoo Messenger evidence using FTK and Registry Viewer.

### Module Objectives

- Distinguish between global registry items that apply to everyone and user-specific information stored in the registry.
- Identify what evidentiary items Yahoo stores in the file structure and where they are located.
- Identify what evidentiary items Yahoo stores in the registry and where they are located.

## WINDOWS MESSENGER

Familiarizes students with the functions and potential evidence associated with the Microsoft Windows Messenger client. Through a forensic examination of the Windows file structure and Windows registry, students learn how to recover and interpret artifacts generated by the client and the user. Students recover registry artifacts such as contact lists, file transfer/sharing permissions, user profile information, and passwords.

During the practical, students recover Windows Messenger artifacts using FTK and Registry Viewer.

### Module Objectives

- List the types of communication enabled by Microsoft .NET Passport technology.
- Recover information from Windows Messenger chat room activities and file exchanges.
- Identify what evidentiary items Windows Messenger stores in the file structure and where they are located.
- Identify what evidentiary items Windows Messenger stores in the registry and where they are located.
- Identify what evidentiary items Windows Messenger stores on Microsoft servers and how that information may be obtained.

---

## MSN MESSENGER

Shows students how to recover forensic artifacts from the Microsoft MSN Messenger client, including contact lists, file sharing, and message history.

During the practical, students use FTK and Registry Viewer to recover artifacts left behind by the MSN Messenger client.

### Module Objectives

- Recover information from MSN Messenger chat room activities and file exchanges.
- Identify what evidentiary items MSN Messenger stores in the file structure and where they are located.
- Identify what evidentiary items MSN Messenger stores in the registry and where they are located.
- Identify what evidentiary items MSN Messenger stores on Microsoft servers and how that information may be obtained.
- Discuss how MSN Messenger was designed for personal use and has many more features than Windows Messenger.

## AOL—INFORMATION FROM AMERICAN ONLINE

This first of three AOL modules discusses the types of information that can be obtained from America Online pursuant to a subpoena or search warrant. It details different types of service violations and recorded information and it outlines recovery techniques of instant messenger artifacts.

### Module Objectives

- List what information you can obtain from AOL with a subpoena.
- List what information you can obtain from AOL with a search warrant.
- List what information can be obtained from an AOL Terms of Service violation.
- Identify how instant message data can be recovered.

## AOL—INFORMATION FROM THE COMPUTER

This second AOL module shows students how to review the client- and user-related forensic artifacts found on systems where AOL has been used. Key areas of focus include history, address books, favorites, auto-complete and typed URLs (address bar information), AIM buddy lists, email and newsgroups, download information, archived IM and chat activity, and client logs.

During the practical, students recover AOL client- and user-related artifacts using FTK and Registry Viewer.

### Module Objectives

- Locate the following evidentiary items in the file structure:
  - Buddy Lists
  - Screen names
  - Address books
  - AOL companion information
  - Client logs / error files
  - Auto-Complete / History
  - Deleted file information
  - Connectivity information
  - Passwords (Sign-On / PFC)
  - Uninstall information (leftovers)

## AOL—PERSONAL FILING CABINET

This final AOL module shows students how to examine the AOL Personal Filing Cabinet (PFC). The module details how to interpret AOL email headers, attachments, away messages, and newsgroup activity. It also reviews AOL email retention policies to emphasize the importance of prompt legal service to preserve online evidence.

During the practical, students recover artifacts from the AOL Personal Filing Cabinet using FTK.

---

## Module Objectives

- Obtain the following information from the Personal Filing Cabinet:
  - Email messages
  - Email headers
  - Attachments
  - Favorite Places
  - Away messages
  - Newsgroup information
- Identify how long email is retained on the AOL server.
- List what types of information may be contained in an AOL message.
- Determine if a user downloaded an email attachment.
- Describe what implications Automatic AOL may have in a case.

## PASSWORD RECOVERY

---

**Note:** This module requires the “Working with PRTK” module from the BootCamp—FTK 1 course. For more information, see “Working with PRTK” on page 34.

---

Shows students how to use Password Recovery Toolkit (PRTK) to recover passwords and encrypted data from the following clients:

- America Online sign-on and Personal Filing Cabinet (PFC)
- AOL Instant Messenger (AIM) sign-on password
- YAHOO Messenger sign-on password
- Windows and MSN Messenger sign-on password
- Firefox auto-complete, form data, and 3DES Master password
- Internet Explorer auto-complete and protected storage information

## Module Objectives

- Identify the file structure and registry location of passwords and encrypted information.
- Identify the techniques used to recover encrypted information with Ultimate Toolkit (UTK).



## Internet Forensics—FTK 3

The Internet Forensics—FTK1 course provides the knowledge and skills necessary to use AccessData tools to recover forensic information from Internet artifacts. Participants learn where and how to locate Internet artifacts using Forensic Toolkit (FTK), Registry Viewer, and Password Recovery Toolkit (PRTK).

The following sections provide a brief description of each module in the Internet Forensics—FTK 1 course with the corresponding module objectives.

- "AOL Instant Messenger" on page 102
- "Yahoo! Instant Messenger" on page 103
- "Windows Live Messenger" on page 103
- "MySpace Instant Messenger" on page 104
- "Skype" on page 105
- "Facebook" on page 105
- "Safari" on page 106
- "Firefox" on page 107
- "Internet Explorer" on page 107
- "LimeWire" on page 108

## AOL INSTANT MESSENGER

Shows students how to identify where an application stores evidence of its installation and use within the Windows Vista file system and registry.

Discussion topics include:

- User accounts and passwords
- User preferences
- Evidence of file transfer and file sharing activities
- Lists of other AIM users with whom the account has had contact (Buddy List)
- Evidence of how AIM interacts with other online applications such as browser clients
- Automated and manually-recorded Instant Messenger (IM) conversations

During the practical, students use FTK to recover AOL file artifacts.

### Module Objectives

- Provide a basic overview of AOL Instant Messenger (AIM) features.
- Identify where AOL Instant Messenger stores the following evidentiary items in the file structure:
  - Buddy List location and meaning of the entries
  - Any saved instant messages
  - Direct IM
  - Linked screen names
- Identify where AOL Instant Messenger stores the following evidentiary items in the Registry:
  - Last user to be logged in to the machine
  - Registered screen names used on the machine
  - Screen names who have had contact with the local user
  - Indications of file transfer activity
  - Permissions for file sharing or file transfers

---

## YAHOO! INSTANT MESSENGER

Shows students how to recover the following artifacts:

- Installation artifacts, in both the Windows file structure and registry
- User accounts, and passwords
- User preferences
- Evidence of file transfer and file sharing activities
- Evidence of how Yahoo! Messenger interacts with other online applications such as browser clients
- Recorded Instant Messenger (IM) conversations

### Module Objectives

- Distinguish between global Registry items that apply to everyone and user-specific information stored in the Registry.
- Identify what evidentiary items Yahoo! stores in the file structure and where they are located.
- Identify what evidentiary items Yahoo! stores in the Registry and where they are located.

## WINDOWS LIVE MESSENGER

Shows students how to recover the artifacts left behind from the client's installation and subsequent use of Windows Live Messenger (WLM) in the Windows Vista environment. Special attention is given to how the WLM client also interacts with other applications within the Windows Live suite of products. Topics include:

- User accounts and passwords
- Preferences
- Evidence of file transfer, file sharing, and other application sharing activities
- Lists of other WLM users with whom the account has had contact (Contact List)
- Evidence of how WLM interacts with other online applications such as browser clients
- Automated and manually-recorded Instant Messenger (IM) conversations
- How to use AccessData's Password Recovery ToolKit (PRTK) to decrypt the WLM "contact" files

## Module Objectives

- List the user-generated artifacts created when the Windows Live suite is installed and the account is authenticated to the Windows Live servers.
- Provide an overview of Windows Live Messenger features.
- List user-generated artifacts that can be recovered from Windows Live Messenger and identify where they are located in the file structure.
- List application-generated artifacts that can be recovered from Windows Live Messenger and identify where they are located in the file structure.
- Identify what evidentiary items are created by Windows Live Messenger in the Registry and where they are located.

## MYSPACE INSTANT MESSENGER

Shows students how the stand-alone Instant Messenger (IM) client interacts with the Windows Vista operating system. Attention is given to the following topics:

- Where the client stores artifacts of its installation in both the file system and registry
- User accounts
- Display images
- File transfer/sharing activity
- Application logs
- Interaction with the MySpace social networking site
- Automated and manually-recorded IM sessions.

## Module Objectives

- Identify the MSIM client's default installation paths on a Windows Vista system.
- Recover client-based, trace evidence from the Windows Vista Registry.
- Recover the following user-generated artifacts:
  - Preferences/settings for the application
  - Contact (friend/buddy) lists
  - Profile information
  - File transfers
- Message archiving and application logging

---

**Note:** At the time this course was created, the current release of the MSIM client was version 1.0.789.0.

---

---

## SKYPE

Gives students insight into one of the more popular Instant Messaging (IM) and Internet calling applications. Discussion topics include:

- User accounts
- Preferences
- Evidence of file transfer and file sharing activities
- Lists of other Skype users with whom the account has had contact
- Evidence of how Skype interacts with other online applications such as browser clients
- Recorded Instant Messenger (IM) conversations
- A special discussion on understanding and converting the proprietary timestamp format for Skype log files

### Module Objectives

- Describe the basic features and availability of Skype.
- Identify what evidentiary items Skype creates during installation and where they are located.
- Identify what evidentiary items Skype are created by the use of the client and where they are located.

## FACEBOOK

Provides a detailed forensic overview of the Facebook social networking site. Students locate information such as the profile picture, personal information, album images and thumbnails, and wall postings and thumbnails. To facilitate the investigation, students are introduced to the Facebook JPEG Finder (FJF) to determine if graphics originated with Facebook activity and identify the potential owner or user of the image files.

This module also spends significant time on recovering friend information, invitation activity, group information and chat activity.

The lab for this module is extensive and it provides valuable tables that identify the location of significant Facebook artifacts. During the course of the lab, students create and use filters to locate Facebook artifacts such as chat files and TIF graphics. Students also use Internet Evidence Finder (IEF) by JADSoftware and Facebook JPG Finder (FJF) to locate Facebook-related artifacts. Additionally, students locate the Facebook Friend list, identify accepted friend requests, and recover chat artifacts from allocated and unallocated space.

The student practical requires students to apply the information they learned in the lab to recover specific Facebook artifacts.

## Module Objectives

- Create a profile.
- Identify the local user.
- Identify members of the friend list.
- Locate profile and album Image uploads.
- Locate friend searches and accepted invitations.
- Locate Notes, Events, and Groups.
- Locate artifacts from Allocated Chat.
- Locate artifacts from Unallocated Chat.

## SAFARI

The Safari module represents the first in the series of three browser client blocks of instruction. This module shows students how to identify and interpret the following artifacts:

- Installation artifacts
- User preferences
- Internet history
- Bookmarked Web sites
- Downloaded files and their tracking
- Internet cookie storage and permissions
- Protected storage
- Caching of temporary files

## Module Objectives

- Identify the artifacts left behind by the client's installation.
- Discuss the artifacts left behind by the user's interaction with the application including:
  - Internet history
  - Cookies
  - Favorites/Bookmarks
  - Typed URLs
  - Downloads
  - Temporary files/Cache
  - Password storage

---

## FIREFOX

The Firefox module is the second of the browser client modules. Similar to the Safari, and Internet Explorer modules, the Firefox module examines application-specific artifacts related to its installation and use. Topics include:

- Locating and interpreting the \*.sqlite file format
- Internet history
- User form data and auto-complete information
- User preferences
- Typed URLs
- Bookmarked Web sites
- Storage of temporary Internet files
- Downloaded files and the download manager
- Online searching
- Passwords
- Protected storage

### Module Objectives

- Locate files of evidentiary interest and discuss how they are created or added to.
- Process Firefox evidentiary files.
- Describe how the browser stores its cached Web content and how FTK handles the information.
- Discuss how Firefox uses encryption and obfuscation to protect sensitive information.

## INTERNET EXPLORER

Internet Explorer is the last of the three Internet browser modules. Although Internet Explorer (IE) has been available for many years, both subtle and dramatic changes have occurred during the course of its lifespan. This module focuses on Internet Explorer version 7. It reviews how the browser tracks Internet history; cookie storage and permissions; user preferences; favorites; and Temporary Internet Files. With a detailed examination of the Windows registry, the module also exposes students to the steps necessary to recover evidence from protected storage using FTK, FTK Imager, and PRTK.

## Module Objectives

- Locate the following Internet Explorer evidentiary items in the file structure:
  - Favorites
  - Cookies
  - History
  - Temporary Internet files
- Locate the following Internet Explorer evidentiary items in the Registry:
  - Typed URLs
  - Passwords
  - Protected storage information

## LIMEWIRE

Introduces students to one of the many Peer-to-Peer (P2P) clients, available for the Gnutella file sharing network. The module examines the structure and function of the Gnutella network and the LimeWire client interaction within the network architecture. Topics include:

- Installation artifacts
- User preferences
- Storage of downloaded files
- Storage and settings for shared files and directories
- Log files used by Limewire to track user network interaction

## Module Objectives

- Discuss the Gnutella Network Overview, including:
  - Architecture
  - Basic operation
  - LimeWire interaction
- Discuss LimeWire Features and Options
- Locate Installation Artifacts
- Locate User Artifacts, including:
  - Preferences
  - Downloads
  - Sharing

## Applied Decryption

Applied Decryption is an intensive, hands-on course that reviews current encryption technology and provides the knowledge and skills necessary to recover passwords using PRTK and DNA.

---

**Note:** All modules from this course require the “Working with PRTK” module from the BootCamp course. For more information, see “Working with PRTK” on page 34.

---

The following sections provide a brief description of each module in the Applied Decryption course with the corresponding module objectives.

- "Cryptography 201" on page 110
- "Decryption Technology" on page 110
- "DNA Interface" on page 111
- "Lab—Decrypting Selected Applications" on page 111
- "Working with PGP" on page 112
- "Lab—Working with Encrypted Containers" on page 112
- "Lab—Private Keys Revisited" on page 113
- "Lab—Working with Data within Data" on page 113
- "The AccessData Decryption Methodology" on page 114

## CRYPTOGRAPHY 201

Introduces advanced cryptography concepts including encryption standards and file recovery strategies. Students are guided through a basic cryptographic system, including the elements used to create a File Encryption Key (FEK), passwords, hash functions, salt, passkey, and the FEK itself. The module addresses the difficulties of attacking data encrypted with large file encryption keys or obscure/long passwords. The module also defines single key (symmetric) and key pair (asymmetric) encryption and reviews how these encryption standards are used to secure data and verify communications. Finally, the module provides a preliminary discussion of digital certificates and digital signatures in preparation for later modules.

During the practical, students conduct exercises in XOR, perform keyspace calculations, convert HEX to Binary to ASCII, and manually obtain passwords from Trillion \*.ini files.

### Module Objectives

- Define cryptography and the difficulty levels provided by different algorithms.
- List the different types of passwords and standards defined by software applications.
- Define cryptography terminology.
- Describe the concepts and theory of basic cryptography systems.
- Describe symmetric and asymmetric encryption standards.
- Describe how digital certificates and signatures are used to encrypt data.

## DECRYPTION TECHNOLOGY

Provides an overview of the AccessData decryption technology software. It outlines how Password Recovery Toolkit (PRTK) and Distributed Network Attack (DNA) recover passwords from common applications, including the types of attacks that may be employed. It also reviews PRTK and DNA features and functions, including how to start attack sessions, how to import dictionaries, how to create attack profiles, and how to report Session\Job properties information.

During the practical phase, participants review the interface and menu options in PRTK, import a custom dictionary, start a decryption session, and identify decryption options once a key is recovered.

## Module Objectives

- Describe the PRTK/DNA interface.
- Utilize the recovery modules.
- Import and use dictionaries, rules, and characters to set up an attack profile.
- Set up the DNA interface and start a job in DNA.
- List the steps to successfully break passwords.
- Describe jobs and how to analyze their properties.

## DNA INTERFACE

Provides the information necessary to deploy a DNA network and configure the options/resources required to crack passwords. The module outlines the hardware and software requirements for the DNA Supervisor and Workers, then demonstrates the DNA Supervisor interface and Worker management options. It also reviews priority options, focusing on the management of worker groups and job priority so you can allocate resources on a job-by-job basis.

During the practical, students create and manage a DNA network using the available class resources. This is followed by a review of the interface and management options.

## Module Objectives

- Plan and install a DNA network.
- Set up and manage DNA groups.
- Describe the DNA interface and preferences.
- Set up the options and resources available to crack passwords.

## LAB—DECRYPTING SELECTED APPLICATIONS

Shows students how to decrypt various software application files using a variety of recovery techniques designed to reinforce the concepts discussed in the Cryptography 201 and Decryption Technology modules. Students learn how common applications such as Microsoft Office, compression apps, and database applications encrypt their data. They also learn the corresponding methods of attack that can be used in DNA or PRTK to access the file data.

The module also addresses how to create attack profiles, including defining custom levels, so attacks are highly efficient. Students are required to define attack profiles for a variety of different scenarios, including foreign language and alternate character passwords.

## Module Objectives

- Recover extended ASCII passwords.
- Recover foreign language character set passwords.
- Recover symbol substitution passwords.
- Explore ways to exploit cryptographic systems.
- Create a concatenation dictionary.
- Perform analytical, dictionary, and statistical attacks.

## WORKING WITH PGP

Reviews digital signatures and certificates with a specific discussion about the PGP Web of Trust—including how the Web of Trust can be implemented, methods a third-party may use to infiltrate the group, and man-in-the-middle attacks.

During the practical, students install PGP, encrypt data using their own public key, export keys, and import keys to build a classroom Web of Trust. Students then attempt to access PGP-encrypted data during an instructor-facilitated lab that identifies the best methods to use when dealing with PGP-encrypted data.

## Module Objectives

- Generate public and private keys in PGP.
- Implement the web of trust with digital signatures.
- Break PGP key rings.

## LAB—WORKING WITH ENCRYPTED CONTAINERS

Introduces virtual volumes (containers). Students first learn how a virtual container file is viewed with a forensic tool when it is not mounted with the native application. This is followed by a discussion of how to recover passwords for encrypted containers so that you can natively mount the volume. The module also discusses best-practice procedures to acquire a forensic image of the mounted virtual container using FTK Imager.

During the instructor-led practical, students install BestCrypt, create an encrypted container, seed it with data, swap containers, then discuss ways to obtain the password using PRTK or DNA so they can natively mount the volume and image the drive using FTK Imager. Finally, there is a discussion of how to obtain header information from large BestCrypt volumes using AccessData decryption tools.

## Module Objectives

- Decrypt a virtually encrypted container.
- Mount the decrypted virtual container.
- Create an image of the mounted virtual container.
- Obtain header information from encrypted containers.

### LAB—PRIVATE KEYS REVISITED

Reviews the Microsoft Encrypting File System. It outlines the EFS encryption process in detail and explains how Windows protects the user's public/private keys. Students learn how a user account's private key can be exported and then imported into a Windows environment, how the password-protection layer of the exported private key can be decrypted using PRTK or DNA, and how to decrypt EFS files encrypted with the corresponding public key. Finally, students use FTK to view decrypted EFS files without having to obtain the user's logon password.

## Module Objectives

- Export private keys from the Windows environment.
- Decrypt private keys from the Windows environment.
- Hack private keys from the Windows environment.
- Decrypt EFS files without logon credentials.
- Import private keys into your processing environment.

### LAB—WORKING WITH DATA WITHIN DATA

Introduces the concept of data concealed within data and how to forensically process such files. Discussions focus on the concept of "carrier" files and "payload" data, outlining the process many steganography applications perform when inserting data into another file without changing the visual appearance or file size of the carrier file. Students discuss the challenges examiners face in detecting carrier files and best practices when dealing with the extraction of payload data.

During the practical, students install steganography applications and explore the process of creating carrier and payload files. They then statistically analyze these files with FTK Imager and observe the minor changes that occur at the hex level when payload data is added to the file. Finally, students use AccessData tools to extract encrypted data from carrier files.

## Module Objectives

- Hide data using steganography.
- Identify steganography detection methods.
- Statistically analyze source and carrier files.
- Recover payload from carrier files.

## THE ACCESSDATA DECRYPTION METHODOLOGY

Outlines decryption strategies. Students review tactics like generating dictionaries based on suspect intelligence or exporting a word list from FTK, then importing the word list in PRTK or DNA to build an attack profile.

The module briefly addresses registry artifacts and Registry Viewer, including methods to extract Intelliforms data protected with the Windows DPAPI model.

The module then focuses on the dictionary tools incorporated into PRTK and DNA, including passphrase generation and passphrase permutation, to create custom dictionaries based on suspect habits and intelligence.

The concept and function of Rainbow Tables are discussed, followed by a demonstration of their ability to recover the decryption key for a Microsoft Word document encrypted with a 40-bit algorithm.

Finally, the module reviews how to use NTAccess to successfully access an administrator-protected drive, replace the logon password with a known value, then restore the logon password to its original state so that EFS files and other data protected by logon authentication can be attacked.

## Module Objectives

- Attack encrypted documents using word lists.
- Attack encrypted documents using environment artifacts.
- Investigate and uncover suspect intelligence to attack an encrypted document.
- Create alternate dictionaries with the AccessData WebCrawler.
- Create a passphrase dictionary with the AccessData Passphrase Generator.
- Use rainbow tables to break Microsoft Word and Excel Documents.
- Use NTAccess to successfully access an administrator-protected drive and replace the log-on password. Then return the drive to its previous log-on state so that any EFS passwords or other protection that uses log-on authentication can be attacked.

## Linux Forensics

Linux Forensics is a hands-on course that reviews different types of Linux-based forensics tools available for digital investigations, forensic imaging with Linux tools, and best practices for Linux-based investigations.

The following sections provide a brief description of each module in the Linux Forensics course with the corresponding module objectives.

- "Linux-Based Forensics Tools" on page 116
- "Live Linux CD/DVDs for Forensic Analysis" on page 116
- "Linux Forensics Foundations" on page 116
- "Introduction to Linux System Investigation" on page 117
- "Advanced Linux System Investigation" on page 117
- "Introduction to Linux Network Intrusion Investigation" on page 118
- "Advanced Linux Network Intrusion Investigation" on page 118

## LINUX-BASED FORENSICS TOOLS

The module will familiarize you with the different types of Linux-based forensics tools available for digital investigations against all types of operating systems. Each student will participate in Live Demonstrations and Hands On activities with a Linux-based operating system and the installation and initial configuration of Linux-based forensic tools.

### Module Objectives

- Understand Linux based operating system characteristics and forensic abilities.
- Install and configure a Linux based operating system that is purpose built for conducting forensic investigations.
- Install and initially configure Linux-based forensic tools for conducting forensic investigations against all operating systems.

## LIVE LINUX CD/DVDS FOR FORENSIC ANALYSIS

There are several types of Live Linux CD/DVDs used in forensic analysis. This module provides live demonstrations and hands-on activities to help you understand the advantages of using live Linux operating system disks, including BackTrack, Helix, and FIRE, to conduct a forensic investigation.

### Module Objectives

- Download, validate and configure Live Linux CD/DVD installations.
- Launch Live Linux CD/DVD inside the suspect operating system.
- Boot a suspect system using a Live Linux CD/DVD.

## LINUX FORENSICS FOUNDATIONS

As a forensic investigator, you must be familiar with the forensic process. Forensic Imaging with Linux tools can provide a quick and easy way to overcome some of the typical challenges that an investigator may encounter while conducting an investigation. This module focuses on using Linux tools and techniques to perform forensic imaging of media sources. It also discusses conducting and reporting on cases that involve the Linux operating system.

### Module Objectives

- Create forensic images of all operating systems with Linux-based tools.
- Process a forensic case involving the Linux operating System.
- Report forensically viable artifacts.

---

## INTRODUCTION TO LINUX SYSTEM INVESTIGATION

As technology advances, so does the diversity of the workstation operating systems that are in use by the general public. It isn't just servers that are running Linux-based operating systems. Now, anyone can walk into an electronics store and purchase a laptop or desktop running Linux instead of Windows. This makes an investigator's job even more complex.

This module introduces the best practices and skills required to begin a full scale investigation on Linux-based operating systems. It also reviews the critical components of the Linux-based file system that are required before you can begin a Linux-based system investigation triage.

### Module Objectives

- Employ investigation best practices
- Identify the critical components of Linux-based files systems
- Extract data of evidentiary value from a Linux-based file systems
- Identify the critical components of a Linux-based operating system
- Extract data of evidentiary value from a Linux-based operating system

## ADVANCED LINUX SYSTEM INVESTIGATION

Once you have a better understanding and hands-on experience with the Linux file system and Linux operating system investigation skills you can execute more advanced analysis on Linux-based systems.

This module provides information to help you recover forensic artifacts from Firefox and other Linux-based Web browsers as well as Apache Web servers. The module also spends considerable time on security auditing techniques and solutions.

Because Linux computers are commonly the launch point of an attack, this module also identifies potential hacking tools and malware.

### Module Objectives

- Recover Internet related artifacts for forensic reporting
- Identify and analyze Linux-based application artifacts
- Recover Linux-based security mechanism artifacts for forensic reporting

## INTRODUCTION TO LINUX NETWORK INTRUSION INVESTIGATION

Building on the foundation of Linux forensic best practices, this module discusses the critical components of the Linux-based system networking and the attack vectors that may be vulnerable and Linux system network intrusion investigation triage.

### Module Objectives

- Identify a network intrusion.
- Discover sources of network intrusions.
- Perform reconnaissance.
- Extract intrusion artifacts.

## ADVANCED LINUX NETWORK INTRUSION INVESTIGATION

This module leads you through more advanced analysis on Linux-based system network intrusions such as network-enabled application analysis. You will also learn the processes, tools and skills required to recover and analyze many different types of Linux-based log files for evidence.

### Module Objectives

- Recover network-enabled application artifacts of evidentiary value.
- Identify and recover Linux-based log files.
- Analyze recovered Linux-based log files for artifact of evidentiary value.

## Macintosh Forensics

Linux Forensics is a hands-on course that provides the knowledge and skills necessary for seizure, forensic imaging, and analysis of Macintosh\* computers and Apple\* iPods. The analysis includes Mac OS X and Mac application artifacts.

The following sections provide a brief description of each module in the Macintosh Forensics course with the corresponding module objectives.

- "Mac GPT Structure" on page 120
- "Obtaining the date and Time from a Mac" on page 120
- "Imaging a Mac" on page 120
- "Directory Structure—Finding Evidence" on page 121
- "Recovering the User Logon Password" on page 121
- "Application Data—Safari" on page 122
- "Application Data—Firefox" on page 122
- "Application Data—iChat" on page 123
- "Application Data—Apple Mail" on page 123
- "iPod Analysis" on page 124
- "iPhone Backup Recovery" on page 124

## MAC GPT STRUCTURE

The module will familiarize you with the Mac OS X and the Extensible Firmware Interface (EFI). It also reviews the GUID Partition Table (GPT) partition scheme and structure.

During the classroom lab, participants use FTK Imager to navigate a Mac image. Participants identify the beginning and ending LBA, the partition name, and other key forensic artifacts.

### Module Objectives

- Describe the Macintosh Extensible Firmware Interface (EFI) and its function.
- Describe the GUID Partition Table (GPT) partition scheme and its structure.

## OBTAINING THE DATE AND TIME FROM A MAC

This module reviews ways to circumvent password protection enabled via the Open Firmware Password Utility on legacy and Intel-based Macs. By booting Mac computers in Open Firmware or Single User mode, examiners can recover the system's date and time information.

### Module Objectives

- Describe the Mac Open Firmware and how it affects password protection and bootable partitions.
- Locate the date and time in Single User Mode.

## IMAGING A MAC

This module reviews the methods of safely acquiring forensic evidence from a Mac. Participants will walk through the process of imaging a drive in Target Disk Mode using FTK Imager or using Helix 3 Pro by e-fence, a bootable DVD based on Ubuntu Linux.

During the lab, participants image a Mac drive using FTK Imager and Helix 3.

### Module Objectives

- Image a Mac for evidentiary use by various methods, such as removing the hard drive or using a bootable CD.
- Identify the advantages and disadvantages of each imaging method.
- Acquire evidence from a Mac using Helix 3.

---

## DIRECTORY STRUCTURE—FINDING EVIDENCE

This module focuses on locating forensic artifacts in the Macintosh directory structure. The module identifies key directories and their associated artifacts, including the user's directory, the user's Library directory, the cache directory, as well as system and network information. The module also directs participants on how to locate forensic evidence in binary and XML Property Lists (plist) and SQLite databases.

During the lab, participants navigate the Macintosh directory structure, plists, and SQLite databases to locate forensic artifacts.

### Module Objectives

- Identify the directory structure and location of important directories.
- Identify the user's Library directory and its content.
- Examine the Property Lists for forensic evidence.
- Examine the SQLite Databases for forensic evidence.

## RECOVERING THE USER LOGON PASSWORD

This module identifies the Macintosh password hash files and guides participants through the process of recovering the logon password. Participants are introduced to the AccessData Decryption Methodology, a process whereby the investigator indexes case evidence in FTK, then exports the case word list to build custom attack dictionaries in PRTK. These custom attack dictionaries are then used to recover system passwords, including the user logon password.

During the lab, participants will implement the AccessData Decryption Methodology on sample files to recover a user's logon password.

### Module Objectives

- Identify the Mac password hash files, where they are located, and the encryption scheme.
- Recover the logon password using various methods.

## APPLICATION DATA—SAFARI

During this module, participants will focus on the Safari application and its associated artifacts. Participants will learn what evidentiary items Safari creates and where they are located.

During the lab, participants will recover Safari bookmarks, downloaded files, browsing histories, the last browser session, and cookies.

### Module Objectives

- Identify what evidentiary items Safari creates and where they are located.
- Identify what evidentiary items are created by the use of the Safari client and where they are located, including the following:
  - Bookmarks
  - Downloads
  - Browsing histories
  - Last session
  - Cookies
- Identify what evidentiary items Safari caches and where they are located.

## APPLICATION DATA—FIREFOX

This module focuses on the Firefox application and its associated artifacts. Participants will learn what evidentiary items Firefox creates and where they are located.

During the lab, participants will recover Firefox cookies, downloaded files, form histories, browsing histories, and bookmarks.

### Module Objectives

- Identify what evidentiary items Firefox creates and where they are located.
- Identify what evidentiary items are created by the use of the Firefox client and where they are located, including the following:
  - Cookies
  - Downloads
  - Form histories
  - Browsing histories
  - Bookmarks
- Import bookmarks for forensic analysis.

---

## APPLICATION DATA—ICHAT

This module focuses on the iChat Internet chat client and its associated artifacts. Participants will learn what evidentiary items iChat creates and where they are located.

During the lab, participants will recover iChat user account data, contact information, user and contact pictures, chat transcripts, and server information.

### Module Objectives

- Identify what evidentiary items are created by the use of iChat and where they are located, including the following:
  - User account data
  - Contact information
  - User and contact pictures
  - Chat transcripts
  - Server information

## APPLICATION DATA—APPLE MAIL

This module focuses on Apple Mail and its associated artifacts. Participants will learn what evidentiary items are created by the use of Apple Mail and where they are located.

During the lab, participants will recover Apple Mail account information, messages, and attachments.

### Module Objectives

- Identify what evidentiary items are created by the use of Apple Mail and where they are located.
- Recover messages from Apple Mail.
- Recover attachments from Apple Mail.

## IPOD ANALYSIS

When the iPod device was introduced in 2001, its main purpose was to store and play digital music. Today, iPods are used for playing videos, viewing pictures, gaming, and storing files. iPods are also used as Personal Digital Assistants to store contacts and calendar information. This module provides the information investigators need to use iPod devices in forensic investigations. Participants will learn how to handle, store, and image iPods for evidentiary purposes. Participants will also learn what evidentiary items are created by the use of an iPod and where these items are located.

During the lab, participants will recover iPod artifacts including photos, contacts, and calendar information.

### Module Objectives

- Handle and store the iPod for evidentiary purposes.
- Image the iPod for evidentiary purposes.
- Identify what evidentiary items are created by the use of an iPod and where they are located, including the following:
  - Photos
  - Contacts
  - Calendars

## IPHONE BACKUP RECOVERY

iPhones are small computers that use the Macintosh OS X operating system and are capable of running hundreds of applications. The phone may contain SMS messages, call history, and voicemail as well as address books, notes, calendar events, and photos.

If an iPhone is attached to a Mac or PC computer running iTunes, the user is prompted to back up the phone. As a result, investigators may be able to document evidence contained on a user's iPhone without actually having access to the phone. This module reviews the location and naming conventions of iPhone backup files and itemizes the artifacts that may be recovered from these backup files.

During the lab, participants will recover artifacts from iPhone backup files including photos with EXIF data, calendar information, and address book information and contact icons, text messages, the voicemail and call logs, general account settings, and Property Lists.

## Module Objectives

- Locate iPhone backup files.
- Determine how backup files are named.
- Identify what evidentiary items may be recovered from the iPhone backup files, including the following:
  - Pictures
  - Call history
  - Address book
  - Notes
  - SMS messages
  - Voicemail
  - Administrative information



## Incident Response

Incident Response 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

The following sections provide a brief description of each module in the Incident Response course with the corresponding module objectives.

- "Incident Response Preparation" on page 129
- "Preparing Tools and Communications" on page 129
- "Incident Types, Sources, and Signs" on page 130
- "Intrusion Identification and Prioritization" on page 130
- "Evidence" on page 131
- "Volatile data" on page 131
- "Nonvolatile Data" on page 132
- "Incident Notification, Documentation, and Damage Assessment" on page 132
- "Containment, Analysis, and Network Analysis Strategies" on page 133
- "Identifying the Attacker and Attack Vector" on page 133
- "Eradication and Recovery" on page 134
- "Post-Incident Activity" on page 134
- "AccessData Enterprise" on page 135

---

## INCIDENT RESPONSE PREPARATION

This module provides a standard definition for a computer security incident and details the need for an incident response capability within an organization. Additionally, it provides a model for the phases of an incident response. Finally, it covers the first phase of incident response and preparation.

### Module Objectives

- Define a computer security incident.
- Explain why organizations should develop an incident response capability.
- List the four main phases of the Incident Response Life Cycle.
- Describe the purpose of an organization's Incident Response plan.
- Identify what should be done with your Standard Operating Procedures before applying them.
- Describe the main responsibility of an IR team during the IR process.
- Describe steps that can be taken to proactively prevent incidents and lessen the impact of incidents if they do occur.

## PREPARING TOOLS AND COMMUNICATIONS

Incidents occur in many forms, so the ability of an organization to develop common classifications or categories of incidents helps create standard handling procedures and policies. Organizations also need tools to help them detect the signs that an incident has occurred and to accurately determine the source of the incident.

### Module Objectives

- Build a Trusted Toolkit
  - Untrusted System Binaries
  - External Source Binaries
  - Tools
- Identify risks associated with executing your trusted toolkit from an external drive.
- Describe why you use trusted binaries when collecting data from a potentially compromised system.
- List ways you can secure your communication channels and provide alternate channels in the event of a communication disruption.

## INCIDENT TYPES, SOURCES, AND SIGNS

This module establishes a foundation for incident response. It starts by categorizing incidents to prepare for a response, and then reviews signs that determine when a response action may be necessary. Additionally, this module discusses the sources of incidents and intruder motivations—knowing your attacker should help you contain and eradicate network intruders.

### Module Objectives

- List the incident categories.
- Differentiate between precursors and indicators.
- Identify the signs that an incident has occurred.
- Identify the primary categories of incident sources.
- Identify criminal motivations that exist within the cyber-crime community.

## INTRUSION IDENTIFICATION AND PRIORITIZATION

This module reviews intrusion analysis and incident prioritization. It is not an in-depth analysis process, but rather a guide of where to look and what you need to take into consideration as you work.

### Module Objectives

- Explain how you can determine the scope of an incident.
- List the steps in the initial analysis and validation process.
- Explain why clock synchronization is important for the analyst.
- Identify the two main factors that determine incident priority.
- Identify the five commonly used severity ratings.
- Explain the purpose of an escalation procedure.

---

## EVIDENCE

The module reviews how to handle incident evidence. The cornerstone of all future actions is based on the evidence you collect. Proper collection, handling, and preservation of evidence is critical to your analysis and future prosecution. This module is very important because there are often no second chances when it comes to evidence.

### Module Objectives

- List five categories of evidence sources and give examples of each.
- Define the term “best evidence” and describe how to validate best evidence copies.
- List the factors to consider when gathering evidence.
- Explain how you can ensure that the evidence collection process does not alter the evidence.
- Describe what factors you should consider before imaging a drive.
- Describe what additional analysis is required to image a RAID drive.
- Define the difference between a logical image and a physical image.
- Describe the function of a chain of custody form.
- Identify common imaging output formats.

## VOLATILE DATA

Now that the theories behind collecting data for an incident response investigation have been covered, this module will look at hands-on methods for collecting this data. It is possible to collect the volatile data that is needed for an IR investigation through the use of many command line utilities. This module will examine the use of these utilities to perform live collections of volatile data from Windows-based systems.

### Module Objectives

- Explain the importance of using a trusted command shell when performing an IR analysis of a compromised system.
- Identify commands that can be used to perform the following functions:
  - List users currently logged on to a Windows-based system.
  - List current networked connections and listening communications ports.
  - Determine all processes currently running on your system.
  - Map an active process to a listening port.
  - View all jobs scheduled to be run on a system
- Image volatile memory.

## NONVOLATILE DATA

This module examines the use of FTK Imager to perform live collections of nonvolatile data. Additionally, it presents basic techniques for collecting and analyzing Windows Event Logs, the Windows Registry, and binary files.

### Module Objectives

- Determine when a limited collection of logical data is preferred over taking a physical image of an entire disk.
- Identify four types of Windows Event logs.
- List the files that make up the Windows registry.
- Identify the command line utility that can be used to view ASCII text within a binary file.

## INCIDENT NOTIFICATION, DOCUMENTATION, AND DAMAGE ASSESSMENT

In addition to the central Incident Response team, various individuals and units inside and outside of the organization need to be involved in the Incident Response process. Prior planning is important to this process. The organization needs to know whom to contact, what to document, as well as what information may or may not need to be collected. This module reviews all aspects of a incident notification, documentation, and damage assessment.

### Module Objectives

- Identify internal and external entities that need to be part of your Incident Response plan.
- Determine how to communicate with internal or external entities in the event of an incident.
- Identify ways to document your Incident Response and list what information should be documented.
- Explain what information is required to compile a damage assessment.

---

## CONTAINMENT, ANALYSIS, AND NETWORK ANALYSIS STRATEGIES

Containment is the next progression within the incident response lifecycle. This module reviews strategies that you can implement to contain the incident and prevent it from spreading.

The module also moves into the analysis aspect of Incident Response to start looking at hosts to find out what happened. It also touches on some network analysis steps that can be taken to determine what hosts have been affected.

### Module Objectives

- Define the goal of containment.
- Identify containment strategies associated with different types of attacks.
- Identify the factors to consider when selecting a containment strategy.
- Identify what things you should look for in a host analysis of volatile and nonvolatile data.
- Identify what information you should collect for your initial host or network analysis.

## IDENTIFYING THE ATTACKER AND ATTACK VECTOR

As part of the incident response process, you are required to work many aspects of the investigation. You should have some standardized processes and procedures to assist you, but remember that every incident is different. You must take information as it is discovered and work accordingly. Areas such as identifying an attacker may be easy in some incidents and impossible in others. Regardless of the difficulty, approach each incident with an open mind and work towards a successful resolution.

### Module Objectives

- List ways you can identify an attacker's IP address.
- Explain how you can cloak your activities when trying to locate an attacker.
- List factors you must consider before scanning an attacker's system.
- List things you can do within your network to identify the attack vector.
- List pertinent information to consider when profiling an attacker.
- Identify research resources that can help you profile an attacker.
- Identify clandestine research procedures that can help you profile an attacker.

## ERADICATION AND RECOVERY

The eradication and recovery stages are the next logical step in the incident response process. By this point you have identified the activity that has occurred on your network and systems. The containment should be ongoing or complete at this point. The eradication and recovery phases are separate, but usually run in tandem with each other. You may even get to this step and jump backwards once you find other hosts that have been compromised. Don't try to force the phases; always be flexible as you gather more information from your analysis.

### Module Objectives

- Define eradication.
- List the eradication and recovery actions you should take for the following types of incidents:
  - Administrative or root access
  - Non-administrative access
  - Malicious code
  - Distributed Denial of Service (DDOS) attacks
- Identify what follow-up actions should be taken after an eradication and recovery procedure.

## POST-INCIDENT ACTIVITY

You will probably never see two different incidents play out in the same exact manner. But you will probably see components of incidents happen again in the future. You will also see areas of the incident response process, both internal and external to the team, which could be improved in the future. These process changes will probably be applied to all future incidents, regardless of the type. This is why you need a method of creating a set of lessons learned from each incident. You also need to know how to apply what was learned to new processes. This is the only way to remain current and to improve the overall incident response process. This module will present information to assist you in reaching your goals.

### Module Objectives

- Explain the purpose of the lessons-learned meeting.
- List the metrics your IT staff should maintain to more effectively track and manage your Incident Response plan.
- List four examples of actionable data.
- Discuss the purpose for retaining evidence, how evidence should be retained, and how long you should retain your evidence records.

---

## ACCESSDATA ENTERPRISE

This module provides an overview of the capabilities of AccessData Enterprise and how it can be used for investigations supporting the incident response (IR) process.

### Module Objectives

- Identify the components of AD Enterprise.
- Provide a basic explanation of how AD Enterprise works.
- Use AD Enterprise to acquire remote data.
- Use AD Enterprise to analyze nonvolatile data.
- Discuss how AD Enterprise displays volatile data.



## SilentRunner

This class is designed for security administrators, security auditors, data center managers, IT managers, system administrators, and law enforcement investigators who are responsible for responding to and investigating network irregularities. It is designed to show the student how to collect and analyze network data from a single point of control using AccessData® SilentRunner®.

The following sections provide a brief description of each module in the SilentRunner course with the corresponding module objectives.

- "Installation and Deployment" on page 138
- "The Collector Interface" on page 138
- "Configuring Data Collection" on page 139
- "Working with Network Data" on page 139
- "Data Manager and Analyzer" on page 140
- "Query the Database" on page 140

## INSTALLATION AND DEPLOYMENT

This module reviews pre-installation planning and deployment strategies and the steps necessary to install the SilentRunner Standard Single Platform edition.

During the lab, participants install Microsoft SQL 2005 and SilentRunner.

### Module Objectives

- Describe the planning and deployment strategies for SilentRunner.
- Identify the different installation components of SilentRunner.
- Identify the difference between the Standard Edition and the Privacy Edition.
- Install the Single Platform Edition of SilentRunner.

## THE COLLECTOR INTERFACE

This module introduces the SilentRunner Collector interface. It discusses the SilentRunner Collector architecture, provides a brief overview of the Collector interface, and reviews the options in the SilentRunner Collector Configuration Manager.

During the lab, participants access the SilentRunner Collector and review the Collector Bar and Preferences.

### Module Objectives

- Effectively navigate the Collector interface.
- Identify and use the tools available in the Collector interface.

---

## CONFIGURING DATA COLLECTION

This module demonstrates how to properly configure the SilentRunner Collector. It introduces the Log Manager and provides an in-depth review of the Configuration Manager options. Participants will also configure alerts and set time zone settings.

During the lab, participants are guided through the process of configuring the Packet Viewer, Sensor Manager, and system options such as ports and protocols, filter settings, TcpDump files, and KnowledgeBase options. Participants are also required to configure and manage alerts.

### Module Objectives

- Launch the SilentRunner Collector.
- Set up automatic segmenting.
- Configure the SilentRunner Collector.
- Use alerts.

## WORKING WITH NETWORK DATA

In this module, you will configure SilentRunner. Configuring the Collector is the first step to enable the CEO to quickly identify problems and to take measures to improve network security and procedures.

During the lab, participants will work with network data, collect data from a TcpDump file, and work with the KnowledgeBase.

The student practical provides a case scenario that gives participants the opportunity to capture data to find rogue servers.

### Module Objectives

- Collect Network Data.
- Browse the KnowledgeBase.
- Manage Network Data.
- View the Network Topology.
- View Information about Transitive Relations.
- View and Record Sessions.

## DATA MANAGER AND ANALYZER

In this module, the student will be introduced to the SilentRunner Data Manager and SilentRunner Analyzer interfaces. Participants review SilentRunner Data Manager tools including Content Evaluation, Alerts, and Templates. Participants also have an opportunity to perform standard Data Manager functions such as searching transactions, selecting protocols, and performing queries.

Participants also receive a detailed review of the SilentRunner Analyzer interface and basic functions.

The lab provides a comprehensive, hands-on review of the SilentRunner Data Manager and SilentRunner Analyzer.

### Module Objectives

- Navigate the Data Manager interface
- Describe and manage Data Manager functions
- Navigate the SilentRunner Analyzer
- Describe and manage SilentRunner Analyzer functions

## QUERY THE DATABASE

This module provides an in-depth review of the Data Manager. Participants will learn how to use the Data Manager and create queries to examine network data. The module is divided into the following sections:

- Transaction Extraction
- Session Extraction
- Email Extraction
- Web Content Extraction
- IM Session Extraction
- Columnar Queries

The module is built around a scenario that demonstrates how to build and conduct queries to investigate a mock case. During the lab, participants will complete the following:

- Perform a Transaction Extraction query for specific transactions
- Perform a Transaction Extraction query for a specific IP address
- Perform a Transaction Extraction query for specific transactions with a graphical representation of the network
- Perform a Session Extraction query
- Perform a Graphical Evaluation query

- Perform an Email Evaluation query
- Perform an Email Evaluation query for a specific email address
- Perform an Email Graphics Tool query
- Perform an Email Evaluation query for all emails
- Perform an Email Evaluation Query for emails based on a specific subject
- Perform an Email Evaluation query for emails with specific attachment types
- Perform an Enhanced Email Investigator Session Extraction query
- Perform a Web Content Reconstruction query
- Perform an Enhanced HTTP Session Extraction query
- Perform an IM Chat Session Extraction query
- Perform a Columnar Manipulation query
- Perform a Network Relationship query for POP3 users

The student practical provides a case scenario that gives participants the opportunity to query the database to find rogue servers.

## Module Objectives

- Create Database Queries
- Create Email Queries
- Create Web Usage Queries
- Create Instant Message Usage Queries
- Create a Graphical Evaluation Query
- Create Columnar Queries





