

Table of Contents

Introduction	5
Module 1: Computer Hardware.....	6
Drives and Disks	6
The Anatomy of a Drive	6
Data Sizes	7
Data Representation	7
Binary	8
Volumes and Partitions.....	10
Disk Partitions and Disk Management Tools	11
MBR vs. GPT	13
Understanding UEFI	16
The HPA.....	19
Solid State Drive (SSD) Features	21
Understanding Windows OS structure	22
The File system.....	25
FAT	25
NTFS	25
NTFS Structure	25
Volume Boot Record	26
\$MFT (Master File Table)	30
The EFS Encryption.....	31
Windows Directory Structure	32
Virtualizing a Forensics Workstation	33
SIFT Forensic Workstation	33
Module 2: Forensic Fundamentals	43
Understanding Hashes and Encodings.....	43
Hash as a Digital Signature.....	44
The Use of Hash for Forensics.....	46
Base Encodings.....	46
ASCII	49
Windows Artifacts.....	51
Startup Files	51
Jump Lists.....	52



Thumbnail Cache	53
Shadow Copy.....	55
Prefetch and Temp Directories	55
RecentApps	57
Registry Hives.....	57
Windows Passwords - Bypassing Windows Protection	60
Encryptions in the Windows OS.....	60
BitLocker	60
NTLM.....	63
Kerberos.....	64
Cracking Windows Passwords.....	66
Cracking RAR/ZIP Passwords.....	69
Data and Files Structure.....	70
Hexadecimal Editing Tools	70
WinHex.....	70
HxD.....	75
File Structure.....	77
Headers and Trailers	77
Magic Number	78
Embedded Metadata	81
Working With Clusters	82
Slack Space	82
Unallocated and Allocated Spaces.....	82
Module 3: Collecting Evidence.....	83
Forensic Data Carving	83
Using HxD for Forensics Carving	83
Carving files from an existing File	83
Automatic File Carving Tools	92
Foremost.....	92
Scalpel	92
Bulk-Extractor	94
Collecting Information	95
Indenting evidence of program execution.....	95
Extracting Registry Artifacts.....	100
Event Viewer	101
The Audition Policy	102



Windows System Metadata.....	106
Detecting hidden files Using ADS.....	107
Self-Extracting Archives (SFX)	108
Collecting network information.....	108
Network Information	108
Network Connections	117
Sysinternals-Suite Forensic tools	117
Extracting credentials using NirSoft.....	119
Drive Data Acquisition	120
Introduction to FTK-Imager.....	120
Exploring System Files.....	122
Creating an Image	124
DD as an Alternative Image Capture Tool.....	128
Capturing Volatile-Memory	129
Capturing a Memory-File	129
Pagefile.....	129
Hiberfil.sys.....	129
Module 4: Analyzing Forensic Findings.....	130
Analyzing Captured Images.....	130
Extracting Protected Files	130
Mounting an Image as a Drive	135
Volatile Memory Capturing.....	136
MFT Dump.....	137
Identifying Potential Threats	142
Visualizing an MFT reconstruction using DMDE	143
Analyzing Prefetch Files	147
Reconstructing Explorer With ShellBags.....	149
Working With Volatile-Memory.....	152
Extracting Data from RAM	153
Identifying Network Connections	153
Dumping Processes From Memory.....	154
Registry Analysis	156
Using Alien-Registry to Analyze Registry Dumps	159
Finding User Information Using Ntuser.dat and Usrclass.dat.....	161
Using CLI to Access the Registry	162
Extracting Data From Registry	164



Forensics Findings in the Registry	168
Module 5: Data Labelling and Report Writing	169
Device Identification	169
Preservation of Data	169
Collecting Evidence	169
Examination and Analysis	169
Interpretation of Evidence Concerning the Goal	169
Documentation	169
Evidence Presentation	170
Conclusion.....	170

