

CONTENTS

Acknowledgments	xiii
Introduction	xv
About the Authors	xvii
PART 1 VIRTUALIZATION	1
Chapter 1 How Virtualization Happens	3
Physical Machines	5
How Virtualization Works	5
Virtualizing Operating Systems	7
Virtualizing Hardware Platforms	8
Server Virtualization	8
Hypervisors	10
Bare-Metal Hypervisor (Type 1)	10
Embedded Hypervisor	10
Hosted Hypervisor (Type 2)	11
Main Categories of Virtualization	12
Full Virtualization	12
Paravirtualization	13
Hardware-Assisted Virtualization	14
Operating System Virtualization	14
Application Server Virtualization	16
Application Virtualization	17
Network Virtualization	18
Storage Virtualization	18
Service Virtualization	19
Benefits of Virtualization	20
Cost of Virtualization	21
Summary	23
References	23
Bibliography	24
Chapter 2 Server Virtualization	25
What Is Server Virtualization?	25
The Purpose of Server Virtualization	26
Server Virtualization: The Bigger Picture	27

Differences between Desktop and Server Virtualization	29
Common Virtual Servers	30
VMware Server	30
Microsoft Virtual Server	32
Citrix XenServer	33
Oracle VM	33
Summary	35
References	35
Bibliography	35
 Chapter 3 Desktop Virtualization	37
What Is Desktop Virtualization?	37
Why Is It Useful?	38
Common Virtual Desktops	39
VMware	39
VMware Fusion	40
Microsoft Virtual PC	42
Parallels	44
Sun VirtualBox	47
Xen	48
Virtual Appliances and Forensics	50
Penguin Sleuth Kit	50
The Revealer Toolkit	51
Intelica IP Inspect Virtual Appliance	51
Helix 2008R1	51
CAINE 0.3	52
Virtual Desktops as a Forensic Platform	53
Summary	54
Bibliography	54
 Chapter 4 Portable Virtualization, Emulators, and Appliances	57
MojoPac	58
MokaFive	62
Preconfigured Virtual Environments	66
VMware	66
Microsoft	67
Parallels	69

Xen.....	70
Virtual Appliance Providers.....	71
JumpBox Virtual Appliances.....	71
VirtualBox.....	72
Virtualization Hardware Devices.....	72
Virtual Privacy Machine.....	74
Virtual Emulators.....	75
Bochs.....	75
DOSBox.....	76
Future Development.....	78
Summary.....	78
References.....	78
Bibliography.....	78
PART 2 FORENSICS.....	81
Chapter 5 Investigating Dead Virtual Environments.....	83
Install Files.....	85
VMware Server.....	85
VMware Workstation.....	86
Microsoft Virtual PC – Microsoft Virtual PC 2007.....	86
MojoPac.....	86
MokaFive.....	88
Virtual Privacy Machine.....	90
Bochs.....	90
DOSBox.....	92
Remnants.....	92
MojoPac.....	94
MokaFive.....	95
Virtual Privacy Machine.....	96
VMware.....	97
Microsoft.....	97
Citrix Xen.....	98
Bochs.....	99
DOSBox.....	99
Virtual Appliances.....	99
Registry.....	100

MojoPac	100
MokaFive	100
Bochs	101
DOSBox	101
VMware and Microsoft	101
Microsoft Disk Image Formats	102
Data to Look for	104
Investigator Tips	106
Summary	106
References	107
Bibliography	107

Chapter 6 Investigating Live Virtual Environments	109
The Fundamentals of Investigating Live Virtual Environments	110
Best Practices	111
Virtual Environments	111
Artifacts	113
Processes and Ports	114
Virtual Environment File Ports and Processes	114
VMware and Tomcat	116
IronKey and Tor	116
SPICE	118
Log Files	118
VM Memory Usage	119
Memory Management	120
Memory Analysis	121
ESXi Analysis	123
Microsoft Analysis Tools	124
Moving Forward	125
Trace Collection for a Virtual Machine	126
Separate Swap Files Corresponding to Different Virtual Machines in a Host Computer System	126
Profile Based Creation of Virtual Machines in a Virtualization Environment	126
System and Methods for Enforcing Software License Compliance with Virtual Machines	126
System and Method for Improving Memory Locality of Virtual Machines	127

Mechanism for Providing Virtual Machines for Use by Multiple Users	127
Summary	127
References	128
Bibliography	128
Chapter 7 Finding and Imaging Virtual Environments	129
Detecting Rogue Virtual Machines	129
Alternate Data Streams and Rogue Virtual Machines	132
Is It Real or Is It Memorex?	136
Virtual Machine Traces	138
Imaging Virtual Machines	143
Snapshots	146
Snapshot Files	146
VMotion	147
Identification and Conversion Tools	147
Live View	148
WinImage	149
Virtual Forensic Computing	149
Environment to Environment Conversion	149
VM File Format Conversions	150
Summary	150
References	151
Bibliography	151
PART 3 ADVANCED VIRTUALIZATION	153
Chapter 8 Virtual Environments and Compliance	155
Standards	155
Compliance	156
Regulatory Requirements	158
Discoverability of Virtual Environment	161
Legal and Protocol Document Language	162
Organizational Chain of Custody	166
Acquisition	167
VM Snapshots versus Full Machine Imaging	167
Mounting Virtual Machines	168

Data Retention Policies	168
Virtual Machine Sprawl	169
The Dynamic Movement of VMs	170
Backup and Data Recovery	171
Summary	172
References	172
Bibliography	173

Chapter 9 Virtualization Challenges 175

Data Centers	175
Storage Area Networks, Direct Attached Storage, and Network Attached Storage	176
Cluster File Systems	177
Analysis of Cluster File Systems	181
Security Considerations	181
Technical Guidance	181
VM Threats	182
Hypervisors	183
Virtual Appliances	184
The VM	184
Networking	185
Malware and Virtualization	185
Detection	186
Red Pill, Blue Pill, No Pill	186
Blue Pill	187
Red Pill and No Pill	187
Other Rootkits	188
Other Methods of Finding VMs	189
Additional Challenges	190
Encryption	190
Solid-State Drives	191
New File Systems and Disk Types	192
Compression and Data Deduplication	192
Virtualization Drawbacks	193
Summary	194
References	194
Bibliography	195

Chapter 10 Cloud Computing and the Forensic Challenges	197
What Is Cloud Computing?	198
Multitenancy	199
Cloud Computing Services	199
Infrastructure-as-a-Service	199
Platform-as-a-Service	200
Desktops-as-a-Service	200
Software-as-a-Service	201
Other Cloud Computing Services	202
Streaming Operating Systems	203
Application Streaming	203
Virtual Applications	204
Benefits and Limitations of Virtual Applications	204
Cloud Computing, Virtualization, and Security	205
Cloud Computing and Forensics	206
Conducting a Forensic Investigation on a Cloud Environment	206
Incident Response	207
Conducting a Forensic Investigation in a Cloud Environment	208
Summary	209
Bibliography	209
 Chapter 11 Visions of the Future: Virtualization and Cloud Computing	 211
Future of Virtualization	211
Hardware Hypervisors	212
Virtual Machines Will Be Used for Antiforensics	212
Mobiles and Virtualization	212
VMware Mobile Virtualization Platform	213
The Evolving Cloud	214
Trends in Cloud Computing	214
More Robust Legal Procedures Will Be Developed	216
Data-Flow Tools Will Evolve	216
The Home Entrepreneur	217
The iPad, Tablet, and Slate	217
Autonomic Computing	218
Summary	219
Bibliography	219

Appendix: Performing Physical-to-Virtual
and Virtual-to-Virtual Migrations 221

Glossary 245

Index 251