

Malware Forensics Field Guide for Windows Systems

Digital Forensics Field Guides

Cameron H. Malin
Eoghan Casey
James M. Aquilina

Curtis W. Rose, Technical Editor



AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an imprint of Elsevier

SYNGRESS.

Contents

Acknowledgments	xv
About the Authors	xvii
About the Technical Editor	xxi
Introduction	xxiii

1. Malware Incident Response

Introduction	2
Local versus Remote Collection	3
Volatile Data Collection Methodology	4
Preservation of Volatile Data	4
Physical Memory Acquisition on a Live Windows System	5
Acquiring Physical Memory Locally	6
GUI-based Memory Dumping Tools	7
Remote Physical Memory Acquisition	8
Collecting Subject System Details	11
Identifying Users Logged into the System	13
Collecting Process Information	18
Process Name and Process Identification	18
Process to Executable Program Mapping:	
Full System Path to Executable File	19
Process to User Mapping	20
Child Processes	20
Dependencies Loaded by Running Processes	21
Correlate Open Ports with Running Processes and Programs	22
Identifying Services and Drivers	23
Examining Running Services	24
Examining Installed Drivers	24
Determining Open Files	25
Identifying Files Opened Locally	25
Identifying Files Opened Remotely	25
Collecting Command History	26
Identifying Shares	26
Determining Scheduled Tasks	27
Collecting Clipboard Contents	27
Non-Volatile Data Collection from a Live Windows System	28
Forensic Duplication of Storage Media on a Live Windows System	29
Forensic Preservation of Select Data on a Live Windows System	29

Assess Security Configuration	30
Assess Trusted Host Relationships	30
Inspect Prefetch Files	31
Inspect Auto-starting Locations	31
Collect Event Logs	32
Logon and Logoff Events	33
Review User Account and Group Policy Information	33
Examine the File System	33
Dumping and Parsing Registry Contents	34
Remote Registry Analysis	35
Examine Web Browsing Activities	37
Examine Cookie Files	38
Inspect Protected Storage	38
Malware Artifact Discovery and Extraction from a Live Windows System	39
Extracting Suspicious Files	39
Extracting Suspicious Files with F-Response	41
Conclusions	42
Pitfalls to Avoid	43
Incident Response Tool Suites	62
Remote Collection Tools	68
Volatile Data Collection and Analysis Tools	71
Physical Memory Acquisition	71
Collecting Subject System Details	75
Identifying Users Logged into the System	75
Network Connections and Activity	76
Process Analysis	79
Handles	80
Loaded DLLs	80
Correlate Open Ports with Running Processes and Programs	81
Command-line Arguments	81
Services	81
Drivers	82
Opened Files	82
Determining Scheduled Tasks	83
Clipboard Contents	83
Non-Volatile Data Collection and Analysis Tools	84
System Security Configuration	84
Prefetch File Analysis	84
Auto-Start Locations	85
Event Logs	85
Group Policies	86
File System: Hidden Files and Alternate Data Streams	86
Dumping and Parsing Registry Contents	88
Web History	88
Malware Extraction	89
Selected Readings	91

Books	91
Papers	91
Jurisprudence/RFCs/Technical Specifications	91
2. Memory Forensics	
Introduction	93
Investigative Considerations	94
Memory Forensics Overview	94
Old School Memory Analysis	96
How Windows Memory Forensic Tools Work	98
Windows Memory Forensic Tools	98
Processes and Threads	99
Modules and Libraries	106
Open Files and Sockets	109
Various Data Structures	112
Dumping Windows Process Memory	118
Recovering Executable Files	118
Recovering Process Memory	119
Extracting Process Memory on Live Systems	120
Dissecting Windows Process Memory	121
Conclusions	126
Pitfalls to Avoid	127
Memory Forensics: Field Notes	128
Selected Readings	154
Books	154
Papers	154
Jurisprudence/RFCs/Technical Specifications	154
3. Post-Mortem Forensics	
Introduction	155
Windows Forensic Analysis Overview	156
Malware Discovery and Extraction from Windows Systems	159
Search for Known Malware	159
Survey Installed Programs	161
Examine Prefetch Files	163
Inspect Executables	164
Inspect Services, Drivers, Auto-starting Locations, and Scheduled Jobs	165
Examine Logs	166
Review User Accounts and Logon Activities	168
Examine Windows File System	169
Examine Windows Registry	170
Restore Points	171
Keyword Searching	172
Forensic Reconstruction of Compromised Windows Systems	173

Advanced Malware Discovery and Extraction from a Windows System	174
Conclusions	175
Pitfalls to Avoid	176
Windows System Examination: Field Notes	177
Mounting Forensic Duplicates	185
Forensic Examination of Window Systems	187
Timeline Generation	190
Forensic Examination of Common Sources of Information on Windows Systems	192
Selected Readings	202
Books	202
Papers	202

4. Legal Considerations

Framing The Issues	204
General Considerations	204
The Legal Landscape	204
Sources of Investigative Authority	205
Jurisdictional Authority	205
Private Authority	208
Statutory/Public Authority	209
Statutory Limits on Authority	210
Stored Data	210
Real-time Data	211
Protected Data	213
Tools for Acquiring Data	218
Business Use	219
Investigative Use	219
Dual Use	220
Acquiring Data across Borders	222
Workplace Data in Private or Civil Inquiries	222
Workplace Data in Government or Criminal Inquiries	224
Involving Law Enforcement	226
Victim Reluctance	226
Victim Misperception	227
The Law Enforcement Perspective	227
Walking the Line	228
Improving Chances for Admissibility	229
Documentation	229
Preservation	229
Chain of Custody	230
State Private Investigator and Breach Notification Statutes	231
International Resources	233
Cross-Border Investigations	233
The Federal Rules: Evidence for Digital Investigators	234

Relevance	234
Authentication	234
Best Evidence	234
Expert Testimony	235
Limitations on Waiver of the Attorney—Client Privilege	235

5. File Identification and Profiling

Introduction	237
Overview of the File Profiling Process	238
Profiling a Suspicious File	240
Command-Line Interface MD5 Tools	243
GUI MD5 Tools	243
File Similarity Indexing	245
File Visualization	246
File Signature Identification and Classification	247
File Types	247
File Signature Identification and Classification Tools	248
Anti-virus Signatures	251
Web-based Malware Scanning Services	252
Embedded Artifact Extraction: Strings, Symbolic Information, and File Metadata	255
Strings	255
Inspecting File Dependencies: Dynamic or Static Linking	259
Symbolic and Debug Information	261
Embedded File Metadata	261
File Obfuscation: Packing and Encryption Identification	267
Packers	267
Cryptors	269
Binders, Joiners, and Wrappers	272
Embedded Artifact Extraction Revisited	272
Windows Portable Executable File Format	272
Profiling Suspect Document Files	281
Profiling Adobe Portable Document Format (PDF) Files	282
PDF File Format	282
PDF Profiling Process: CLI Tools	285
PDF Profiling Process: GUI Tools	292
Profiling Microsoft (MS) Office Files	295
Microsoft Office Documents: Word, PowerPoint, Excel	295
MS Office Documents: File Format	295
MS Office Documents: Vulnerabilities and Exploits	298
MS Office Document Profiling Process	298
Deeper Profiling with OfficeMalScanner	301
Profiling Microsoft Compiled HTML Help Files (CHM)	308
CHM Profiling Process	308
Conclusion	311

Pitfalls to Avoid	313
Selected Readings	317
Papers	317
Online Resources	317
Technical Specifications	318
6. Analysis of a Malware Specimen	
Introduction	363
Goals	364
Guidelines for Examining a Malicious File Specimen	365
Establishing the Environment Baseline	365
System “Snapshots”	366
Host Integrity Monitors	366
Installation Monitors	367
Pre-Execution Preparation: System and Network Monitoring	369
Passive System and Network Monitoring	370
Active System and Network Monitoring	371
Execution Artifact Capture: Digital Impression and Trace Evidence	380
Impression Evidence	380
Trace Evidence	380
Digital Impression Evidence	380
Digital Trace Evidence	381
Executing the Malicious Code Specimen	385
Execution Trajectory Analysis: Observing Network, Process, Api, File System, and Registry Activity	386
Network Activity: Network Trajectory, Impression, and Trace Evidence	386
Environment Emulation and Adjustment: Network Trajectory Reconstruction	388
Network Trajectory Reconstruction: Chaining	389
Network Impression and Trace Evidence	390
Using a Netcat Listener	391
Examining Process Activity	393
Process Spying: Monitoring API Calls	394
“Peeping Tom”: Window Spying	395
Examining File System Activity	396
Examining Registry Activity	397
Automated Malware Analysis Frameworks	397
Online Malware Analysis Sandboxes	400
Defeating Obfuscation	402
Custom Unpacking Tools	403
Dumping a Suspect Process from Memory	404
Locating the OEP and Extracting with OllyDump	406
Reconstructing the Imports	411
Embedded Artifact Extraction Revisited	412
Examining the Suspect Program in a Disassembler	413
Advanced PE Analysis: Examining PE Resources and Dependencies	416

Interacting with and Manipulating the Malware Specimen:	
Exploring and Verifying Functionality and Purpose	422
API Hooking	422
Prompting Trigger Events	424
Client Applications	425
Event Reconstruction and Artifact Review:	
Post-Run Data Analysis	426
Passive Monitoring Artifacts	427
Active Monitoring Artifacts	429
Analyzing Captured Network Traffic	430
Analyzing API Calls	431
Physical Memory Artifacts	432
Digital Virology: Advanced Profiling Through	
Malware Taxonomy and Phylogeny	432
Context Triggered Piecewise Hashing	435
Textual and Binary Indicators of Likeness	435
Function Flowgraphs	439
Process Memory Trajectory Analysis	442
Visualization	444
Behavioral Profiling and Classification	446
Conclusion	449
Pitfalls to Avoid	450
Selected Readings	454
Books	454
Papers	454
Index	505