

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

## Topics

<i>LogFile</i> .....	508.5 – –66
<i>LogFileOperationCodes</i> .....	508.5 – –73
<i>UsnJrnl</i> .....	508.5 – –68
<b>Incident Response Steps</b> .....	508.1–20-21
1. Preparation .....	508.20–21
2. Identification .....	508.20–21
3. Containment .....	508.20–21
4. Eradication .....	508.20–21
5. Recovery .....	508.20–21
6. Lessons Learned .....	508.20–21

### Service Name

DcomLaunch .....	508.1–76
LocalServiceAndNoImpersonation .....	508.1–76
LocalServiceNetworkRestricted .....	508.1–76
LocalServiceNoNetwork .....	508.1–76
netsvcs .....	508.1–76
NetworkService .....	508.1–76
RPCSS .....	508.1–76

### Windows Process

csrss.exe .....	508.1–77
explorer.exe .....	508.1–78
lsaiso.exe .....	508.1–78
LSASS.exe .....	508.1–79
ntoskrnl.exe .....	508.1–80
RuntimeBroker.exe .....	508.1–80
services.exe .....	508.1–77
smss.exe .....	508.1–77
svchost.exe .....	508.1–76
System .....	508.1–76
taskhostw.exe .....	508.1–79
userinit.exe .....	508.1–79
wininit.exe .....	508.1–78, 508.1–80
winlogon.exe .....	508.1–79, 80

### wmic

group .....	508.1–137
netuse .....	508.1–137
process .....	508.1–137
qfe .....	508.1–137
startup .....	508.1–137
useraccount .....	508.1–137

## Categories

\$INDEX_ALLOCATION .....	508.5–57
\$INDEX_ROOT .....	508.5–57
\$STANDARD_INFORMATION ...	508.5–33, 508.5–37
\$FILE_NAME .....	508.5–33

## A

### Account

Brute Force Password Attack .....	508.2–54
-----------------------------------	----------

Built-in accounts .....	508.2–56
Enumeration .....	508.2–74
Logon Event .....	508.2–69
Tracking Administrator activity .....	508.2–58
Tracking Creation .....	508.2–60
Tracking Usage .....	508.2–46, 47
Tracking Usage (RDP) .....	508.2–64
Usage (RDP) .....	508.2–62
AceHash .....	508.1–119, 508.1–133, 508.1–138
ACMRU .....	508.4–34
Admin Shares .....	508.2–118
Destination Artifacts .....	508.2–118
Source Artifacts .....	508.2–117
ADMIN .....	508.2 – –86
ADMIN\$ .....	508.W-2.4–7
Alternate Data Stream .....	508.1–62
Alternate Data Streams (ADS) .....	508.5–51
Amcache.hve .....	508.2–17
Parsing .....	508.2–17
AmcacheDriverBinaries .....	508.2 – –25
AmcacheProgramEntries .....	508.2 – –25
AmcacheUnassociatedEntries .....	508.2 – –25
AmcacheParser.exe .....	508.2–23
AMSI → Anti-Malware Scanning Interface .....	
Analysis Scenario .....	508.2–72
AnalyzeMFT .....	508.5–37
ANONYMOUS LOGON .....	508.2–56
Anti-Forensics .....	508.5–5, 508.1–67
Defenses .....	508.5–109
Detection .....	508.5–84, 508.5–109
Anti-Malware Script Obfuscation .....	508.2–164
Anti-Virus .....	
Bypass .....	508.1–62
Logs .....	508.2–139
AppCompatCache → Application Compatibility Cache .....	
AppCompatCacheParser.exe .....	508.2–16
AppCrash .....	508.2–140
Application Compatibility Cache ..	508.2–14, 508.4–29
Application Deployment Software .....	508.2–132
APT19 .....	508.3–78
Archives (embedded timestamp) .....	508.4–54
Armoring .....	508.1–62
Artifacts .....	
Account Usage .....	508.4–40
Browser Usage .....	508.4–41
Deleted file or File Knowledge .....	508.4–34
File Opening/Creation .....	508.4–31
Network .....	508.3–112
Network Shares .....	508.2–117
OS Unusual .....	508.1–74
Physical Location .....	508.4–36
PowerShell .....	508.2–129
Program Execution .....	508.4–29
PsExec .....	508.2–120-121
Remote Desktop Protocol (RDP) ..	508.2–114-116
Remote Service .....	508.2–125
Scheduled Tasks .....	508.2–126

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

USB or Drive Usage .....	508.4–38
WMI .....	508.2–127
ASEPs .....	508.1–70
<b>at.exe</b> .....	508.1–74, 75, 508.2–123
ATT&CK .....	508.1–45
Collection .....	508.1–46
Command and Control .....	508.1–46
Credential Access .....	508.1–46
Defense Evasion .....	508.1–46
Discovery .....	508.1–46
Execution .....	508.1–46
Exfiltration .....	508.1–46
Lateral Movement .....	508.1–46
Persistence .....	508.1–46
Privilege Escalation .....	508.1–46
AutoRun .....	508.1–67
<b>AutoRunsc.exe</b> .....	508.1–100, 101
<b>autorunsc.exe</b> .....	508.1–85

## B

B-Tree .....	508.5–58
Index Rebalancing .....	508.5–61
Searching .....	508.5–58
BadRabbit .....	508.1–139
<b>base64</b> .....	508.W-1.4–9
Beacons .....	508.1–62
Behavior Detection Anomaly .....	508.1–81
BelgaSoft .....	508.3–34
Binary Padding .....	508.1–62
<b>bitsadmin.exe</b> .....	508.1–61
<b>blkls</b> .....	508.5–105
Bloodhound .....	508.2–100, 508.1–149
Browser	
Cache .....	508.4–41
Cookies .....	508.4–41
Flash & Supercookies .....	508.4–42
History .....	508.4–41
Search Terms .....	508.4–37
Session Restore .....	508.4–42
Brute-Force Password Attack .....	508.2–54
<b>bstring.exe</b> .....	508.3–181
BulkExtractor .....	508.3–36
<b>bytehist</b> .....	508.1–82

## C

Cached Credentials .....	508.1–133
Cached credentials .....	508.1–99
<b>cachedump</b> .....	508.1–133
Cain .....	508.1–138
capa .....	508.4–5, 508.4–13
Analysis Example .....	508.4–16
Behavior .....	508.4–16
Enumeration Malware Capabilities .....	508.4–14
Probable capabilities .....	508.4–16
Usage .....	508.4–15

Carving .....	508.3–189
Carving for Strings .....	508.5–103
Direct Strings .....	508.5–106
Indexed String .....	508.5–107
Certification Authority .....	508.1–69
Chat threads .....	508.3–31
CIM → Common Information Model .....	
<b>cmd.exe</b> .....	508.1–75
Cobalt Strike .....	508.2–86, 508.2–92
Named Pipes .....	508.2–92
Sacrificial Processes .....	508.2–92
Code Injection .....	508.1–74, 508.3–124
Hidden and Reflective .....	508.3–139
Reflective .....	508.3–138
Review .....	508.3–148
Code Signing .....	508.1–63, 508.1–69
Malware .....	508.1–71
Command Line Tracking .....	508.2–145
<b>COMMAND<sub>H</sub>ISTORY</b> .....	508.3 – –185
Common Information Model (CIM) .....	508.1–135
Compromise .....	508.1–39
Compromise Type .....	508.1–56
Compromising Credentials .....	508.1–119
Hashes .....	508.1–119
LSA Secrets .....	508.1–128
NTDS.DIT .....	508.1–140
Tickets .....	508.1–140
Tokens .....	508.1–128
Computer Account .....	508.2–56
<b>CONSOLE<sub>I</sub>NFORMATION</b> .....	508.3 – –185
Containment and Intelligence Development ..	508.1–24
CozyDuke .....	508.3–94
Create Triage Timeline Bodyfile .....	508.4–61
<b>CreateInstance</b> .....	508.1–79
CreateRemoteThread .....	508.3–124
creddump .....	508.1–119, 508.1–133, 508.1–138
Credential	
Attacks (evolution) .....	508.1–117
Availability .....	508.1–121
Harvesting .....	508.1–115
Credential Availability .....	508.1–121
Credential Guard .....	508.1–118, 508.1–126
CredSSP .....	508.1–99, 508.1–118
CyberChef .....	508.2–165

## D

DanderSpritz .....	508.2–109
DarkComet .....	508.3–85
Data Collection .....	508.1–40
Data Encryption .....	508.5–5
Data Exfiltration .....	508.1–40
DC Sync .....	{1143
Defending Credentials	
Cached Credentials .....	508.1–131
Hashes .....	508.1–126
LSA Secrets .....	508.1–139
Tickets .....	508.1–145

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

Tokens .....	508.1–131
Defense Manipulation .....	508.1–62
DensityScout .....	508.4–5
<b>densityscout</b> .....	508.1–82, 508.1–84
DensityScout Execution .....	508.4–10
Device Guard .....	508.1–118
Digital Signature checking .....	508.4–12
Direct Kernel Object Manipulation (DKOM) ...	508.3–157
Directory Slack Entries .....	508.5–56
Directory Table Base (DTB) .....	508.3–42
DKOM → Direct Kernel Object Manipulation .....	
DLL Hijacking	
DLL Search Order Hijacking .....	508.1–76
DLL Side-Loading .....	508.1–76
Phantom DLL Hijacking .....	508.1–76
Relative Path DLL Hijacking .....	508.1–76
DLL Injection .....	508.1–62
Allocate .....	508.3–126
Attach .....	508.3–125
Execute .....	508.3–127
DLL Lists .....	508.3–129
Domain Protected User .....	508.1–118
Domain Protected Users Group .....	508.1–126
Downloads.sqlite .....	508.4–28
Driver Acquisition .....	508.3–298
Driver Letter .....	508.4–38
DTB → Directory Table Base .....	
DumpIt .....	508.3–34
Dun and Bradstreet Rating .....	508.1–69
DWM .....	508.2–56

## E

E-mail Attachments .....	508.4–28
EchoTrail .....	508.3–66
EDR → Endpoint Detection and Response .....	
Endpoint Detection and Response (EDR) ...	508.3–23
Challenge .....	508.3–25
Importance .....	508.3–24
<b>Enter-PSSession</b> .....	508.1–97, 508.1–99
Entropy and packing analysis .....	508.4–9
Entropy and packing analysis Example .....	508.4–11
EPROCESS ..	508.3–42, 508.3–60, 508.3–66, 508.3–157
Eradication Without Proper Incident Scop- ing/Containment .....	508.1–22
Error reports .....	508.2–139
Establish Foothold .....	508.1–39
Evasion .....	508.1–62
Event Log Explorer .....	508.W-2.3–1, 508.2–77
Event Log Recovery .....	508.5–103
Bulk Extractor .....	508.5–103
Event Viewer .....	508.2–74
EventLog .....	508.2–37
Application .....	508.2–40
Clearing .....	508.2–106
Clearing (Selective) .....	508.2–106
Deletion .....	508.5–5

Forwarding .....	508.W-3.4–11
Security .....	508.2–41
Service .....	508.2–40
Tampering .....	508.5–5
Types .....	508.2–40
eventlogedit .....	508.2–109
<b>eventvwr.exe</b> .....	508.2–74
Evidence of Download .....	508.5–54
Evidence of Execution .....	508.2–5
Prefetch .....	508.2–6
EVT .....	508.2–38
EVTX .....	508.2–38
EvtxECmd .....	508.2–79
EvtxECmd Maps .....	508.2–80
Executive Process Block .....	508.3–42
Explicit Credentials	
Cobalt Strike .....	508.2–92
Tracking .....	508.2–88

## F

F-Response .....	508.3–9
SIFT .....	508.3–34
Fast forensics .....	508.4–90
fgdump .....	508.1–119
File	
Delete .....	508.5–5
Download .....	508.4–28
Handles .....	508.3–104
Wiping .....	508.5–5
File deleted .....	508.5–81
File entropy analysis .....	508.4–5
File Recovery .....	508.5–94
Carving Method .....	508.5–97
Metadata Method .....	508.5–96
VSS .....	508.5–99
File System History .....	508.5–109
File System Journaling	
<i>LogFile</i> .....	508.5 – –66
<i>UsnJrnl</i> .....	508.5 – –68
Activity Patterns .....	508.5–68
File System Journaling Overview .....	508.5–65
File <i>Objects</i> .....	508.3 – –191
Fileless	
Detection .....	508.5–93
Fileless Malware .....	508.5–5
Filename	
Hijacking .....	508.1–62
Filenames .....	508.5–56
Firmware .....	508.1–62
Fixup Array .....	508.5–38
fls .....	508.4–46, 508.4–60
Forensics (Remote) .....	508.3–5
Forensics Artifacts Review .....	508.4–26
<b>Format-Wide</b> .....	508.1–95
Frequent Compilation .....	508.1–62
FU Rootkit .....	508.3–159
<b>fxsst.dll</b> .....	508.1–76

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

## G

Get-Alias .....	508.1–95
Get-ChildItem .....	508.1–95
Get-LsaSecret.ps1 .....	508.1–138
Get-Process .....	508.1–95
Get-Service .....	508.1–95
Get-SvcFail.ps1 .....	508.1–100
Get-WmiObject .....	508.1–81, 508.1–140
GlassRAT .....	508.1–100
GoFetch .....	508.1–149
Golden Ticket .....	{1143
gpedit.msc .....	508.2–68
grep .....	508.3–182
Group Enumeration .....	508.2–74
Group Managed Service Account .....	508.1–118
GRR .....	508.3–201
gsecdump .....	508.1–119, 508.1–122, 508.1–138

## H

Handles .....	508.3–104
Hash Dumping .....	508.1–122
Hashes .....	508.1–119
Defense .....	508.1–126
Hibernation Files .....	508.3–34
Windows 10 .....	508.3–36
hibr2bin .....	508.3–36
Hiding in Plain Sight .....	508.1–60
Hunting .....	508.1–31–34
Hunting Notes .....	508.1–55
DLL Hijacking .....	508.1–78
WMI Persistence .....	508.1–83
Hunting: Automated to Manuel .....	508.1–57

## I

I/O Request Packet (IRP) .....	508.3–150
IAT → Import Address Table .....	
icat .....	508.5–53, 508.5–96
ICP.....	508.2 – –86
Identification .....	508.1–31–34
IDT → Interrupt Descriptor Table .....	
Import Address Table (IAT) .....	508.3–150
Incident Response	
Intelligence-Driven .....	508.1–39
Process .....	508.1–38
Remote .....	508.3–5
Incident Response Detection and Intelligence Loop	
508.1–27	
Incognito .....	508.1–99
Incognito mode .....	508.3–32
Index.dat .....	508.4–29, 508.4–34
Indicator of Compromise .....	508.1–49
OpenIOC .....	508.1–42
Sharing .....	508.1–49
STIX .....	508.1–41

YARA .....	508.1–51
Indx2Csv .....	508.5–63
InInitializationOrderModule List .....	508.3–129
Initial Compromise .....	508.1–39
Inline API .....	508.3–150
InLoadOrderModule List .....	508.3–129
InMemoryOrderModule List .....	508.3–129
Inode .....	508.4–109
Intelligence-Driven Incident Response .....	508.1–39
Internet Evidence Finder .....	508.3–36
Interrupt Descriptor Table (IDT) .....	508.3–150
Intrusion Methodology .....	508.1–55
Threat Hunting Assessment ..	508.3–29, 508.1–55
Triage Collection Analysis .....	508.4–3
Invoke-Command .....	508.1–97
Invoke-Phantom .....	508.2–109
Invoke-WmiMethod .....	508.2–127
IPRIP: RIP Listener Service (APT1) .....	508.1–72
IRP → I/O Request Packet .....	
istat .....	508.5–33

## J

Jump List .....	508.4–30
-----------------	----------

## K

Kansa .....	508.1–100–1110
3 <sup>rd</sup> party tools .....	508.1–110
Analysis scripts .....	508.1–107
Configuration .....	508.1–102
Get-AutoRunsc.ps1 .....	508.1–106
Get-CertStore.ps1 .....	508.1–106
Get-FlsBodyfile.ps1 .....	508.1–106
Get-Handle.ps1 .....	508.1–106
Get-LogparserStack.ps1 .....	508.1–107
Get-ProcDump.ps1 .....	508.1–106
Get-RekalPslis.ps1 .....	508.1–106
Modules .....	508.1–102
Remote .....	508.W-1.5–6
Kansa PowerShell Framework .....	508.1–80
KAPE .....	508.3–13
Collection .....	508.3–15
Target Collection .....	508.3–15
KB2871997 .....	508.1–117
KDBG → Kernel Debugger Datablock .....	
KdCopyDataBlock .....	508.3–53
Kerberoasting .....	508.1–143, {1143
Kerberos .....	508.2–70, 508.1–99
Attacks .....	508.1–143
Kerberos Attacks .....	508.1–143
Kerberos Attacks Mitigations .....	508.1–145
Kernel Debugger Datablock (KDBG) .....	508.3–42
Identification .....	508.3–52
Kernel Patch Protection .....	508.3–153
Kernel Processor Control Region (KPCR) ...	508.3–42
Kill Chain .....	508.1–39

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

Actions on Objectives .....	508.1–39
Delivery .....	508.1–39
Exploitation .....	508.1–39
Persistence .....	508.1–39
Reconnaissance .....	508.1–39
<b>kpartx</b> .....	508.W-3.1–16
KPCR → Kernel Processor Control Region .....	

## L

Last visited MRU .....	508.4–29, 508.4–32, 508.4–34
Lateral Movement .....	508.1–40
Overview .....	508.1–114
Scheduled Tasks .....	508.2–94
Shares .....	508.2–85
Tracking .....	508.2–85
Least frequency of occurrence analysis .....	508.1–107
Link (soft and hard) .....	508.5–23
LiveSSP .....	508.1–119
Living off the Land Binaries (LOLBin) .....	508.1–61
LNK file .....	508.4–25
<b>LoadLibrary</b> .....	508.3–124, 508.3–138
Local Account	
Abuse .....	508.2–72
Local Account Events .....	508.2–69
Local Admin (Limitations) .....	508.1–115
Local Administrator Password Solution (LAPS) .....	508.1–126
LOCAL SERVICE .....	508.2–56
Location: Internet Explorer .....	508.4–37
Log gap analysis .....	508.2–109
log2timeline .....	508.4–46, 508.4–72, 508.4–80
Arguments .....	508.4–80
Parser lists .....	508.4–87
Target examples .....	508.4–82
VSS .....	508.5–17
<b>LogFileParser.exe</b> .....	508.5–77
Ligon	
Error Codes .....	508.2–70
Event .....	508.2–69
Last .....	508.4–40
Session Identification .....	508.2–52
Session length .....	508.2–52
Success/Failure .....	508.4–40
Type .....	508.4–40, 508.1–121
Type Codes .....	508.2–50
LSA Secrets .....	508.1–137
LSASS .....	508.1–119
Security EventLog .....	508.2–41

## M

MACB .....	508.4–50-51, 508.4–56
mactime .....	508.4–61
MagnetForensics .....	508.3–34
Maintain presence .....	508.1–39
<b>make_oken</b> .....	508.2 – –92

Malware	
Code Signing .....	508.1–71
Common Malware Locations .....	508.1–60
Common Malware Names .....	508.1–60
Defense Evasion Techniques .....	508.1–62
Dormant .....	508.1–67
Execution .....	508.2–139
Identification .....	508.1–81
Malware Discovery .....	508.4–5
Anomaly Detection .....	508.4–5
Malware Paradox .....	508.1–54
Malware Persistence .....	508.1–69
AutoStart Locations .....	508.1–70
BIOS Flashing .....	508.1–96
DLL Hijacking .....	508.1–76
Local Group Policy .....	508.1–96
MS Office Add-in .....	508.1–96
Scheduled Tasks .....	508.1–101
Service Failure Recovery .....	508.1–100
Windows Services .....	508.1–72
WMI Event Consumers .....	508.1–79
Managed Service Account .....	508.1–117
Master File Table (MFT) .....	508.5–25
Alternate Data Streams .....	508.5–51
Analyse header and <i>STANDARD_INFORMATION</i> .....	508.5–38
Analysing <i>DATA</i> .....	508.5 – –49
Analysing <i>FILE_NAME</i> and <i>AttributesSummary</i> .....	508.5–41
Entry Allocated .....	508.5–30
Entry Attributes .....	508.5–32
Entry Unallocated .....	508.5–30
File Record Header .....	508.5–38
Records .....	508.5–27
Sequential Entries .....	508.5–31
Structure .....	508.5–26
Memory	
Acquisition .....	508.3–34
Analysis .....	508.3–42
Analysis .....	508.3–42
Compression .....	508.3–36
Description	
Advantages .....	508.3–41
Dump .....	508.3–34
Finding the first hit .....	508.3–58
Forensics .....	508.3–31
Advantages .....	508.3–32
Motivations .....	508.3–31
Windows .....	508.3–42
Hiding in Plain Sight .....	508.3–67
Offset .....	508.3–66
Page Execute ReadWrite .....	508.3–139
pslist .....	508.3–66
Virtual Machine .....	508.3–34
Metadata Entries .....	508.5–30
MetaSploit ....	508.1–119, {1129, 508.1–133, 508.1–138
Meterpreter .....	508.3–141
MFTECmd .....	508.5–33, 508.4–46, 508.5–54, 508.4–58,

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

508.5–79	
Microsoft Online Accounts .....	508.2–79
Mimikatz .....	508.1–99, 508.2–109, 508.1–118, 119, 508.1–124, 508.1–129, 508.1–138, 508.1–141
EventLog Clearing .....	508.2–109
MOF .....	508.1–141
MOF → WMI/MOF Files .....	
mofcomp.exe .....	508.1–79, 508.2–127, 508.1–150
MountPoints2 .....	508.4–55, 508.1–75, 508.2–117
MsCash2 .....	508.1–133
mstsc.exe .....	508.2–130
Mutants .....	508.3–108
Mutexs .....	508.3–108
MZ .....	508.3–141–144

## N

net.exe .....	508.1–75, 508.2–133
net1.exe .....	508.2–133
netstat.exe .....	508.1–95
NetTraveler .....	508.1–77
Network Artifacts .....	508.3–112
Review .....	508.3–118
Network History .....	508.4–37
NETWORK SERVICE .....	508.2–56
Network Shares	
Admin .....	508.2–117
Tracking .....	508.2–85
Nishang .....	508.1–138
NotPetya .....	508.1–139
NTDS.DIT .....	508.1–148
NTFS .....	508.5–21, 508.4–51
i30 .....	508.5 – –57
Directory Attributes .....	508.5–57
Features .....	508.5–23
File Deleted .....	508.5–81
System Files .....	508.5–28
Timestamp .....	508.4–51
NTLM .....	508.1–119
ntoskrnl.exe .....	508.3–150

## O

Office Recent Files .....	508.4–33
Offset .....	508.3–60
Open/Save MRU .....	508.4–31
Out-GridView .....	508.1–95
Overpass the Hash .....	{1143}

## P

Packed Executable .....	508.4–5
Packing .....	508.1–62
Page Directory Offset (PDB) .....	508.3–71
Page File .....	508.3–34
Parsing <i>i30directoryindexes</i> .....	508.5 – –63
Pass The Hash .....	508.1–124

Pass the Hash .....	508.2–72
Pass-the-hash attacks .....	508.1–119
Mitigations .....	508.1–118
Pass-the-ticket .....	508.1–141, {1143}
Password	
Last change .....	508.4–40
PatchGuard .....	508.3–153
PDB → Page Directory Offset .....	
PE .....	508.4–5
PEB → Process Environment Block .....	
PECmd.exe .....	508.2–9
pescan .....	508.1–82, 508.1–87
PID .....	508.3–75
pinfo .....	508.4–94
pinfo .....	508.4–72
Pivot Chart .....	508.4–44
Pivot Point .....	508.4–43–44
Places.sqlite .....	508.4–29
Plaso .....	508.4–72
Linux/Android/Mac Parsers .....	508.4–78
mactime .....	508.4–79
Registry Parsers .....	508.4–75
Web History Parsers .....	508.4–77
Windows Parsers .....	508.4–73
Plug-and-Play Event Log .....	508.4–39
PlugX .....	508.1–77
Poison Ivy .....	508.1–77
Poor Density Score .....	508.4–17
Ports .....	508.W-3.4–4
PowerShell .....	508.1–94
AMSI .....	508.2–164
Authentication .....	508.1–99
Basics .....	508.1–95
Command History .....	508.2–171
Command Lines .....	508.2–162
Destination Artifacts .....	508.2–131
Enabling logs .....	508.2–159
Get-WinEvent .....	508.2–176
Logs .....	508.2–157
Obfuscation .....	508.2–164
Processes .....	508.3–80
Remoting .....	508.1–97
Source Artifacts .....	508.2–129
Stealth syntax .....	508.2–162
Transcript Logs .....	508.2–167–170
PowerShell to Discover Suspicious WMI Events	508.1–81
powershell.exe .....	508.1–75, 508.2–131
PowerView .....	508.2–74
PPID .....	508.3–75
Prefetch .....	508.2–6, 508.4–30, 508.4–33
Privileged Local Account Abuse .....	508.2–72
ProcDump .....	508.1–75
Process	
Acquisition .....	508.3–198
Analysis .....	508.3–62
Anomaly .....	508.1–76
Environment Block (PEB) .....	508.3–42

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

Hollowing .....	508.3–124
Injection .....	508.1–62
Objects .....	508.3–87, 508.3–110
Process tree .....	508.3–27
Rogue .....	508.1–73
Terminated .....	508.3–73
Tracking .....	508.2–143, 144
Command Line .....	508.2–145
Profiling Account Usage .....	508.2–72
Protected Processes .....	508.1–118
PsActiveProcessHead .....	508.3–42
PsExec .....	508.1–75, 508.2–103, 508.1–119, 508.2–136
Destination Artifacts .....	508.2–120
Source Artifacts .....	508.2–118
psexesvc.exe .....	508.2–121
PsLoggedOn .....	508.1–75
psort .....	508.4–99
psort .....	508.4–72
PspCid .....	508.3–158
PSReadline .....	508.2–171
pth .....	508.2–92
PWDumpX .....	508.1–133
PWDumpX .....	508.1–119

## Q

qc .....	508.1–74
qprivs .....	508.1–74
qtriggerinfo .....	508.1–74
queryex .....	508.1–74

## R

rar.exe .....	508.1–75
RasAuto .....	508.1–100
RDP sessions termination .....	508.1–126
rdpclip.exe .....	508.2–132
Reactive Response vs Threat Hunting .....	508.1–31
Real-Time Remediation .....	508.1–30
Recent Files .....	508.4–32
RecentFileCache.bcf .....	508.2–17
Reconnaissance Tracking .....	508.2–74
Recovering Delete VSS .....	508.5–99
Recycle Bin .....	508.4–35
reg.exe .....	508.1–75, 508.2–123
Registry	
Deletion .....	508.5–5
Hiding Data .....	508.5–5
Registry Explorer .....	508.5–92
Registry Key/Value recovery .....	508.5–92
RegRipper .....	508.1–98
Rekall .....	508.1–130
Remediation .....	508.1–27–29, 508.1–35
Requirements .....	508.1–36
Steps .....	508.1–37
Remediation controls .....	508.1–27–29
Remote Credential Guard .....	508.1–118, 508.1–126

Remote Desktop Protocol (RDP)	
Logging .....	508.2–68
Source Artifacts .....	508.2–114
Usage .....	508.4–41
Remote interactive sessions .....	508.1–126
Remote Service Artifacts .....	508.2–125
Reports.wer .....	508.2–139, 508.2–142
Restricted Admin .....	508.1–118
RID 500 .....	508.2–7
rip.pl .....	508.W-3.1–18
Rogue Process Analysis .....	508.3–87
Rootkit .....	508.1–67, 508.1–74, 508.1–130
Detection .....	508.3–169
Hooking .....	508.3–150
Run MRU .....	508.4–31
runas	
Detection .....	508.2–90
Tracking .....	508.2–88
rundll32.exe .....	508.1–61

## S

SACL → System Access Control List .....	
Sakula .....	508.1–77
SAM Registry Hive .....	508.1–119
sc.exe .....	508.1–74, 75, 508.1–100, 508.2–123
Scheduled Tasks .....	508.1–74
Artifacts .....	508.2–126
Artifacts (v1.2) .....	508.2–98
Logs .....	508.2–96
Tracking .....	508.2–94
schtasks.exe .....	508.1–74, 75, 508.2–123
SCM .....	508.2–101
SCM → Service Control Manager .....	
scrcons.exe .....	508.3–80, 508.2–127
Scripting .....	508.1–92
Batch Files .....	508.1–92
PowerShell .....	508.1–112
WMIC .....	508.1–93
Search (Win7-10) .....	508.4–36
Search (XP) .....	508.4–34
Security Identifier (SID) .....	508.3–102
SeDebug .....	508.2–58
SeImpersonate .....	508.1–129
Select-String .....	508.1–95
Service Control Manager .....	508.2–101
Service Events .....	508.4–30
Service Hijacking .....	508.1–62
Services	
Suspicious .....	508.2–101
Unknown .....	508.1–74
Set-WmiInstance .....	508.1–79
SeTakeOwnership .....	508.2–58
SetWindowsHookEx .....	508.3–124
Shell bags .....	508.4–32
ShimCache .....	508.2–14, 508.5–46
shimcachemem .....	508.3–197
Shortcut (LNK) files .....	508.4–33, 508.4–39

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

---

SID → Security Identifier .....	
Sigcheck .....	508.4–5
<code>sigcheck</code> .....	508.1–82, 508.1–89
<code>sigcheck.exe</code> .....	508.4–12
Silver Ticket .....	{1143}
Skeleton Key .....	{1143}
Skype .....	508.4–28
SMB	
File copy .....	508.4–55
SMBShell .....	508.1–119
Snapshot Recovery .....	508.5–99
<i>vss<sub>c</sub>arver</i> .....	508.5 – –102
Stacking script .....	508.1–107
Strings .....	508.3–181
StuxNet .....	508.3–136, 508.1–141
SUNSPOT .....	508.1–74
Super Timeline .....	508.4–66
Analysis .....	508.4–105
Creation steps .....	508.4–102
CSV Output .....	508.4–107
Filter .....	508.4–88
Parser Presets .....	508.4–87
Recommended Columns .....	508.4–107
Targeted .....	508.4–85
Timeline Output .....	508.4–105
Suspicious Files .....	508.4–17
Suspicious Services .....	508.2–101
Swap File .....	508.3–34
Sysmon .....	508.2–179
SYSTEM .....	508.2–56
System Access Control List .....	508.2–69
System Service Descriptor Table (SSDT) ...	508.3–150
System Volume Information .....	508.5–99
SYSTEM32 .....	508.W-2.1–9
SYSWOW64 .....	508.W-2.1–9

## T

Target Collection .....	508.3–15
Task (Start time) .....	508.W-2.4–22
TDL3/TDSS .....	508.3–133
TeamViewer .....	508.2–114
Temporal proximity .....	508.4–43
TGT .....	508.2–70
Threads .....	508.3–75
Threat Hunting Process .....	508.1–31–34
Threat Intelligence .....	508.1–37
Threat Intelligence and ATTCK Mapping ...	508.1–48
Thumbnails .....	508.4–35
Thumbs.db .....	508.4–36
Tickets .....	508.1–140
Timeline	
Analysis Process .....	508.4–113
Benefits .....	508.4–22
Comparison .....	508.4–46
Context .....	508.4–45
Filesystem .....	508.4–56
Lateral Movement .....	508.4–66

Pivot Points .....	508.4–113
Process Analysis .....	508.4–47
Scope .....	508.4–113
Super Timeline .....	508.4–66
Time Rule Exception .....	508.4–54
Timesketch .....	508.4–116
Utopia and Reality .....	508.4–23–24
Timeline Bodyfile .....	508.4–60
Timeline explorer .....	508.4–109
Timestamp	
Lateral Movement Analysis .....	508.4–55
Timestamp .....	508.1–67
Detection .....	508.5–46–48
Timestamping .....	508.5–5
Timezone .....	508.4–36
Token Stealing .....	508.1–129
Tokens .....	508.1–128
Tracking	
Account Creation .....	508.2–60
Account Usage .....	508.2–46
Account Usage (RDP) .....	508.2–62
Command Line .....	508.2–144–146
Explicit Credentials runas .....	508.2–88
Lateral Movement .....	508.2–85
Network Shares .....	508.2–85
Process .....	508.2–144–146
Reconnaissance .....	508.2–74
Scheduled Tasks .....	508.2–94
Triage .....	508.4–91
Filesystem Timeline .....	508.4–50
Trusted Code .....	508.1–69
<i>tsk<sub>r</sub>ecover</i> .....	508.5 – –96
TsPkg .....	508.1–118, 119
<i>tstheme.exe</i> .....	508.2–132

## U

UMFD .....	508.2–56
USB First/Last Times .....	508.4–38
USB Key Identification .....	508.4–38
Useful filters in the Journals .....	508.5–75
User Access Control (UAC) .....	508.1–117
UserAssist .....	508.4–31
USN Journal Reason Codes .....	508.5–72

## V

VAD → Virtual Address Descriptor .....	
Velociraptor	
Artifacts .....	508.3–18, 508.3–20
Hunting .....	508.3–19
Introduction .....	508.3–16
Virtual Address Descriptor (VAD) ....	508.3–42
VirtualAllocEx .....	508.3–124
VirusTotal Hit via sigcheck .....	508.4–13
VNC .....	508.2–114
Volatility .....	508.3–36, 508.3–45
apihooks .....	508.3–166



# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

baseline	.....508.3--84
cmdline	.....508.3--92
cmdscan	.....508.3--173, 508.3--185-187
connections	.....508.3--114
connscan	.....508.3--114
consoles	.....508.3--173, 508.3--185-187
dlldump	.....508.3--173
dlllist	.....508.3--92, 93
driverbl	.....508.3--84, 508.3--164
driverirp	.....508.3--169
dumpfiles	.....508.3--173, 508.3--191
filescan	508.3--52, 508.3--173, 508.3--195
getsids	.....508.3--92, 508.3--98
handles	.....508.3--92, 508.3--104
hivelist	.....508.3--52
hollowfind	.....508.3--128
idt	.....508.3--169
imagecopy	.....508.3--36, 508.3--56
imageinfo	.....508.3--53
kdbgscan	.....508.3--53
ldrmodules	.....508.3--128, 129
malfind	.....508.3--128, 508.3--140, 508.3--146, 147
malprocfind	.....508.3--65, 508.3--89
memdump	.....508.3--173, 508.3--183
moddump	.....508.3--173
modscan	.....508.3--162
mutantscan	.....508.3--92
netscan	.....508.3--114
procdump	.....508.3--173
processbl	.....508.3--65, 508.3--84
pslist	.....508.3--52, 508.3--65, 66
psscan	....508.3--52, 508.3--65, 508.3--71
pstree	.....508.3--65, 508.3--75
psxview	.....508.3--158
servicebl	508.3--84, 508.3--92, 508.3--164
shimcachemem	.....508.3--197
sockets	.....508.3--114
sockscan	.....508.3--114
ssdt	.....508.3--153
svcsan	.....508.3--92, 508.3--164
threadmap	.....508.3--128
vaddump	.....508.3--173
Help	.....508.3--48
Image identification	.....508.3--53
Profile	.....508.3--51
Usage	.....508.3--46
Volume GUID	.....508.2--55
Volume Name	.....508.4--39
Volume Serial Number	.....508.4--39
Volume Shadow Copy	.....508.5--9
Examination	.....508.5--11
log2timeline	.....508.5--17
Recovering Delete VSS	.....508.5--99
vshadowinfo	.....508.5--13
vshadowmount	.....508.5--14
vssc <sub>arver.py</sub>	.....508.5 -- -99,100
Vulnerability	
Exploitation	.....508.2--134

### W

w3wp.exe	.....508.2--78
WannaCry	.....508.1--139
WBEM → Web-Based Enterprise Managment	.....
WCE	.....508.1--119
WDigest	.....508.1--118, 119
Web-Based Enterprise Management (WBEM)	508.1--135
WebShell	.....508.1--62, 508.3--78
What is Evil?	.....508.1--73
What is Normal?	.....508.1--73
win32k.sys	.....508.3--150
Windows 10 Memory Compression	.....508.3--189
Windows Forensics Trinity	.....508.4--25
Windows Remote Management	.....508.2--98, 508.2--123
Windows Services	.....508.1--72
0x00	.....508.1--72
0x02	.....508.1--72
Service creation	.....508.1--72
Service Replacement	.....508.1--72
Start value	.....508.1--72
Windows Time Rules	....508.5--44-45, 508.4--52
winmem <sub>aecompress.py</sub>	.....508.3 -- -189
winpmem Driver	.....508.3--34, 508.1--130
WinRM	.....508.1--97
winrm.vbs	.....508.1--75, 508.1--117
winrs.exe	.....508.2--123
Wipers	
BCWipe	.....508.5--87
Cipher	.....508.5--87
Eraser	.....508.5--87
SDelete	.....508.5--85
WMI	.....508.1--93, 508.1--135
Attacks	.....508.1--136, 508.2--148
Consumers	.....508.1--148
Database	.....508.1--146
Destination Artifacts	.....508.2--128
Event Consumer Backdoor	.....508.1--140
Event Consumers	.....508.1--79
Hunting	.....508.1--149
In Short	.....508.2--147
Investigation	.....508.1--142
Lateral Movement	...508.1--139, 508.2--151
Logs	.....508.2--156
MOF Files	.....508.1--150
Persistence Audit	.....508.2--153
PowerShell	.....508.1--144
PowerUp.ps1	.....508.2--147
Privilege Escalation	.....508.1--138, 508.2--150
Processes	.....508.3--80
PyWMIPersistenceFinder.py	.....508.1--147
Reconnaissance	.....508.2--149

# FOR508 – Advanced Incident Response, Threat Hunting, & Digital Forensics

```

    Suspicious WMI processes .....508.3--82
    WBEM AutoRecover Folder .....508.1--152
    WBEM AutoRecover Key .....508.1--154
    WMI Command Lines .....508.2--152
wmic.exe .....508.3--80, 508.1--93, 508.2--127
wmiprvse.exe .....508.3--80, 508.2--127
WordWheelQuery .....508.4--36
WriteProcessMemory .....508.3--124
WSMan .....508.2--129
wsmprovhost.exe .....508.3--80, 508.2--131

```

## Y

```

YARA .....508.4--5
  Indicators of compromise .....508.4--7
  MZ portable executable signature ..508.4--7
  Usage .....508.4--8
  YARA Pattern Matching .....508.4--6

```

## Z

```
Zbot .....508.3--167
Zero Configuration .....508.1--67
Zeus .....508.3--167
Zone.Identifier ADS .....508.5--54
```