MEMORY FORENSICS

Memory extraction	FTK Imager (File > Capture Memory…)

VOLATILITY

.\volatility-2.6.standalone.exe -f [image] --profile=[profile] [plugin]

General information	Help	[vol.py --info]
	Profile	[vol.py -f dump.raw imageinfo]
	Network connections	[vol.py -f dump.raw netscan] (connscan for WinXP)
	Process tree	[vol.py -f dump.raw pstree]
	Process list	[vol.py -f dump.raw pslist]
Command history	cmd.exe command history	[vol.py -f dump.raw cmdline]
	conhost.exe history	[vol.py -f dump.raw cmdscan]
		[vol.py -f dump.raw consoles]
Process memory content	Handles list	[vol.py -f dump.raw handles -p <process ID> --silent]
	Export of process executable	[vol.py -f dump.raw procdump -D <output directory> -p <process ID>]
	Export of injected malicious code	[vol.py -f dump.raw malfind -D <output directory>]
	DLL list	[vol.py -f dump.raw dlllist -p <process ID>]
	Export of loaded DLLs	[vol.py -f dump.raw dlldump -D <output directory>]
	Process memory export	[vol.py -f dump.raw memdump -p <process ID> -D <output directory>]
File system analysis	Search for files	[vol.py -f dump.raw filescan > <output file>]
	Files export	[vol.py -f dump.raw dumpfiles -Q <offset> -D <output directory>]
Registry analysis	Export of registry files	[vol.py -f dump.raw dumpregistry -D <output directory>]
	Userassist	[vol.py -f dump.raw userassist]
	Password hashes	[vol.py -f dump.raw hashdump > <output file>]
Search of strings	Strings parsing	[strings64.exe <input file> > <output file>]
	YARA scan	[vol.py -f dump.raw yarascan -Y “/(<regexp>)/”-p <process ID>]

WINDOWS FORENSICS

Drive extraction	FTK Imager Lite (File > Create Disk Image…)

Phase	Type	Artifact	Tool / Command
Initial Access	**RDP connection**	C:\Windows\System32\winevt\Logs\Security.evtx	Windows Event Viewer, Event Log Explorer
		C:\Windows\System32\winevt\Logs\Microsoft-WindowsRemoteDesktopServicesRdpCoreTS%4Operational.evtx	
		C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx	
		C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx	
	USB devices	C:\Windows\INF	USB Detective
		C:\Windows\appcompat\Programs\Amcache.hve	
		C:\%USERPROFILE%\NTUSER.DAT	
		C:\Windows\System32\config\SOFTWARE	
		C:\Windows\System32\config\SYSTEM	
	Browser history	C:\Users\%USERNAME%\AppData\Local\Microsoft\Edge\User Data\Default\History	BrowsingHistoryView, DB Browser for SQLite
		C:\Users\%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles*.default*\places.sqlite	
		C:\Users\%USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History	
	Files opening	NTUSER.DAT|Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU	RegRipper Registry Explorer
		NTUSER.DAT|Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	
		C:\Users\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations	[JLECMD.exe -f <jump list file>]
		C:\Users\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\	[LECMD.exe -f <LNK file>]
Execution	**Execution traces**	C:\Windows\Prefetch	[PECMD.exe -f <prefetch file>]
		SYSTEM|ControlSet001\Control\Session Manager\AppCompatCache	[AppCompatCacheParser.exe -f SYSTEM --csv <output directory]
		USRCLASS.DAT|Local Settings\Software\Microsoft\Windows\Shell\MUICache	RegRipper Registry Explorer
		C:\Windows\appcompat\Programs\Amcache.hve	[AmcacheParser.exe -f Amcache.hve --csv <output directory>]
		NTUSER.DAT|Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist	RegRipper Registry Explorer

Phase	Type	Artifact	Tool / Command
Persistence	**Run Keys**	NTUSER.DAT|Microsoft\Windows\CurrentVersion\Run	RegRipper Registry Explorer
		NTUSER.DAT|Microsoft\Windows\CurrentVersion\RunOnce	
		SOFTWARE|Microsoft\Windows\CurrentVersion\Run	
		SOFTWARE|Microsoft\Windows\CurrentVersion\RunOnce	
	Startup Folders	C:\Users\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	FTK Imager
		C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup	
	Tasks	C:\Windows\System32\Tasks\Task_Name	FTK Imager
		Microsoft-Windows-TaskScheduler%4Operational.evtx	Windows Event Viewer, Event Log Explorer
	Services	C:\Windows\System32\Winevt\LogsSecurity.evtx	Windows Event Viewer, Event Log Explorer
		System.evtx	
	Logon Scripts	NTUSER.DAT|Environment\UserInitMprLogonScript	RegRipper Registry Explorer
	WMI Event Subscription	C:\Windows\System32\wbem\Repository\OBJECTS.DATA	[wmi-parser.exe -i OBJECTS.DATA -o <output directory>]
Lateral Movement	**RDP connection source**	C:\Windows\System32\winevt\Logs\Security.evtx	Windows Event Viewer, Event Log Explorer
		C:\Windows\System32\winevt\Logs\Microsoft-WindowsTerminalServicesRDPClient%4Operational.evtx	
		NTUSER.DAT|Software\Microsoft\Terminal Server Client\Servers	RegRipper Registry Explorer
	RDP connection destination	C:\Windows\System32\winevt\Logs\Security.evtx	Windows Event Viewer, Event Log Explorer
		C:\Windows\System32\winevt\Logs\Microsoft-WindowsRemoteDesktopServicesRdpCoreTS%4Operational.evtx	
		C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx	
		C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx	
	Administrative Shares source	C:\Windows\System32\winevt\Logs\Security.evtx	Windows Event Viewer, Event Log Explorer
		C:\Users\%USERPROFILE%\AppData\Local\Microsoft\Windows\USRCLASS.DAT	ShellBagsExplorer
	Administrative Shares destination	C:\Windows\System32\winevt\Logs\Security.evtx	Windows Event Viewer, Event Log Explorer
	PsExec source	C:\Windows\System32\winevt\Logs\Security.evtx	Windows Event Viewer, Event Log Explorer
		NTUSER.DAT|Software\SysInternals\PsExec\EulaAccepted	RegRipper Registry Explorer
	PsExec destination	C:\Windows\System32\winevt\Logs\Security.evtx	Windows Event Viewer, Event Log Explorer
		C:\Windows\System32\winevt\Logs\System.evtx	