WINDOWS LIVE RESPONSE

A quick reference guide

This quick reference guide (QRG) provides the first steps to be taken in windows systems in case of any incident. The QRG includes the important commands to be used quickly to collect volatile and select some important non-volatile data.

Collecting Volatile Data

No.	Task	Explanation
1	Open a trusted shell (External drive):\cmd.exe	Run cmd from your TD with administrator privileges
2	Record the system date and time	From the trusted cmd on your TD type the below: • echo "Case Number #, Investigator Name: **(your name)**, Start Time and date:" >> (path where to store)\date_time.txt • echo. | date >> (path where to store)\date_time.txt • echo. | time >> (path where to store)\date_time.txt
3	Record the watch (real) date and time	• echo "Watch date and time are: : **(Enter the real time here)**" >> (path where to store)\date_time.txt
4	Determine open ports	• netstat –ano >> (path where to store)\open_ports.txt • netstat –rn >> (path where to store)\routing_table.txt
5	List apps associated with open ports	• netstat –anob >> (path where to store)\open_ports_with_apps.txt or • tcpvcon –a –c -n /accepteula >> open_ports.csv Note: Tcpvcon tool can be downloaded from Sysinternals - check Resources section
6	List all running processes and services	• List all services that are running under each process ○ tasklist /svc >> (path where to store)\open_processes1.txt ○ tasklist /v >> (path where to store)\open_processes2.txt ○ net start >> (path where to store)\services.txt **Alternatives:** • pslist /accepteula >> (path where to store)\running_processes.txt • psservice /accepteula >> (path where to store)\running_services.txt Note: these tools can be downloaded from Sysinternals - check Resources section
7	List recent connections	• arp –a >> (path where to store)\arpcache.txt • nbtstat –c >> (path where to store)\netbios_connections.txt
8	Get clipboard contents	If powershell is installed in the machine, run: • powershell get-clipboard >> (path where to store)\clipboard.txt
9	DNS cache	Ipconfig /displaydns >> (path where to store)\DNS_info.txt
10	List open files	• List remotely opened file: ○ psfile /accepteula >> open_files1.txt Note: psfile tool can be downloaded from Sysinternals - check Resources section or ○ net file >> open_files2.txt or ○ openfiles /query >> open_files3.txt Note: compare results of all tools • List local open files if applicable; Check if /local is enabled ○ openfiles /local Note: if disabled do not enable it and do not reboot the system • List current DLLs: ○ Listdlls /accepteula >> dlls_list.txt Note: listdlls tool can be downloaded from Sysinternals - check Resources section
11	Capture Memory *Optional at this stage*	• mdd_1.3.exe -o (path where to store)\memoryDump.dd or • memoryDD.bat -output (path where to store) Note: mdd_1.3.exe and memorydd.bat tools are free and can be downloaded online- check Resources section

Collecting Non-Volatile Data

No.	Task	Explanation
1	Capture IP info and system information and variables	• ipconfig /all >> (path where to store)\IP_Information.txt • systeminfo >> (path where to store)\SystemInfo.txt • set >> (path where to store)\env_var.txt
2	Determine who is logged in	• Check who is logged on locally/remotely on the machine: ○ psloggedon /accepteula >> (path where to store)\whoison.txt or ○ logonsessions /accepteula >> (path where to store)\whoison.txt Note: these tools can be downloaded from Sysinternals - check Resources section • Check sessions that are connected to the target machine • net sessions >> (path where to store)\connected_sessions.txt
3	Record creation, modification, and access times of all files	• Export all directories with files recursively with **last access** times on the target machine: ○ dir /t:a /a /s /o:d **(targetDrive):**\ >> (path where to store)\All_File_List_Access.txt • Export all directory with files recursively with **last modification** times on a target drive: ○ dir /t:w /a /s /o:d **(targetDrive):**\ >> (path where to store)\All_File_List_Modified.txt • Export all directory with files recursively with **creation** times on a target drive: dir /t:c /a /s /o:d **(targetDrive):**\ >> (path where to store)\All_File_List_Creation.txt
4	List schedule tasks	• schtasks /query /v /FO csv >> (path where to store)\schedual.csv
5	Capture the mapped drives and shares	• Net use >> (path where to store)\mapped_drives.txt • Net share >> (path where to store)\shares.txt
6	List all installed drivers	• driverquery /SI >> (path where to store)\drives.txt
7	Registry	Collect the below Hives manually by going to: • BootDrive:\Windows\System32\config\ ○ SAM ○ Security ○ Software ○ System • BootDrive:\Users\(Account name): ○ Ntuser.dat Or • mkdir (path where to store)\registry\ • robocopy BootDrive:\Windows\System32\config\ destination sam security software system • copy BootDrive:\Users\%Username%\ntuser.dat destination
8	Prefetch	Copy manually the below folder to where you save your evidences. • BootDrive:\Windows\Prefetch Or • mkdir (path where to store)\prefetch\ • Copy BootDrive:\Windows\Prefetch\ (path where to store)\prefetch\
9	Event logs	There are many Events logs, based on the incident collect the important ones, copy the event logs to where you save your evidences (manually). • BoodDrive:\Windows\System32\winevt\logs Or • mkdir (path where to store)\events\ • wevtutil epl “Event Log Name” (path where to store)\events\“Event Log Name”.evtx

After Completing the Collection

No.	Task	Explanation
1	Record system date and time (Completes your Timeline)	• echo "Time and Date of completion:" >> (path where to store)\date_time.txt • date >> (path where to store)\date_time.txt • time >> (path where to store)\date_time.txt
2	Document commands used during your response	• doskey /history > (path where to store)\history.txt
3	OPTIONAL: Capture the entire HD	Using FTK comandline imager: • ftkimager --list-drives • ftkimager source (path where to store) --e01 • ftkimager target-drive --verify Note: ftkimager tool can be downloaded from access data site - check Resources section

Resources

No	Tool/Resource	Website
1	Sysinternals Suite	• https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite
2	FTK	• Command line version: https://accessdata.com/product-download/windows-32bit-3-1-1
3	MD5deep64 and md5deep	• https://sourceforge.net/projects/md5deep/
4	ManTech Memory dd (mdd)	• https://sourceforge.net/projects/mdd/
5	Memoryze	• https://www.fireeye.com/services/freeware/memoryze.html • https://www.sans.org/blog/digital-forensics-how-to-memory-analysis-with-mandiant-memoryze/
6	Help command	• Use /? or -h command with any tool in case if you need more information • https://ss64.com/nt/help.html