<INSERT COMPANY LOGO HERE>

Compromised Windows System

Live Data Gathering Checklist

* Run Live Collection Batch script as Administrator

Run the “Windows Live Response Collection.exe” executable and choose which option you would like (Complete, Memory Dump, Triage, Secure Complete, Secure Memory Dump, or Secure Triage) from an external USB drive connected to computer. Depending on the option you choose, this will use Belkasoft Ram Capture to create a memory dump, copy Prefetch, Event Log, Registry, MFT, USNJrnl, and Logfile related files, and perform all of the other tasks listed on this checklist (except creating an image of the device). Alternatively, you can choose to run the individual batch scripts, but the executable forces the script to run with elevated privileges and presents an easy to follow GUI

OR

* Create and save memory dump

*Use FTK Imager or Belkasoft Ram Capture to Acquire Memory*

* List process name associated with IP connection (requires elevated privileges)

Command: *netstat –anb*

* Use Last Activity View to view “last activities” that occurred on the system

Command: *LastActivityView.exe*

* Compute MD5 and SHA256 hashes of executable files in %WINDIR%\System32, %SystemDrive%\Temp\, and all files in %TEMP%

Command: *md5deep64.exe -oe -u -t –r "%WINDIR%\system32\\*"*

*md5deep64.exe" -oe -u -t -r "%SystemDrive%\Temp\\*"*

*md5deep64.exe" -u -t –r “%TEMP%\\*”*

*sha256deep64.exe -oe -u -t –r "%WINDIR%\system32\\*"*

*sha256deep64.exe" -oe -u -t -r "%SystemDrive%\Temp\\*"*

*sha256deep64.exe" -u -t –r “%TEMP%\\*”*

* Find default Gateway correlation information with ipconfig and nmap

Command: *arp –a <default gateway IP>*

Command: *nmap –A –O <default gateway IP>*

* View Processes and Path – Extended and long information

Command: *PrcView/pv.exe –el*

* View Processes and Path – Extended

Command: *PrcView/pv.exe –e*

* MS-DOS Windows code page

Command: *chcp*

* Directory listing

Command: *dir /S /O-D “%HOMEDRIVE%\”*

* Currently logged on user

Command: *whoami*

* Windows Version

Command: *ver*

* Determine system information

Command: *systeminfo*

* Determine system date/time settings

Command: *time/T && date/T && w32tm /tz*

* View scheduled tasks

Command: *schtasks /query /fo LIST /v*

* View running processes

Command: *tasklist /V*

* List loaded dlls

Command: *tasklist /M*

* List services associated with processes

Command: *tasklist /SVC*

* List Internet settings

Command: *ipconfig /all*

* List open network connections

Command: *netstat –ano*

* List DNS cache

Command: *ipconfig /displaydns*

* List ARP

Command: *arp –a*

* Find the Default Gateway MAC address

Command: *for /f "tokens=2 delims=:" %i in ('ipconfig ^| findstr /i "Default gateway" ^|findstr [0-9]') do arp -a %i*

* Find the Default Gateway info using nmap

Command: *for /f "tokens=2 delims=:" %i in ('ipconfig ^| findstr /i "Default gateway" ^|findstr [0-9]') do nmap\nmap.exe -A -O %i*

* List users

Command: *net user*

* List NetBIOS name cache

Command: *nbtstat -c*

* List netstat routing table

Command: *netstat –rn*

* List net sessions

Command: *net sessions*

* List NetBIOS sessions

Command: *nbtstat –S*

* List NetBIOS files

Command: *net file*

* List ports and executables

Command: *cports.exe*

* List hidden directories

Command: *dir /s /b /ahd “%HOMEDRIVE%\”*

* List installed software

Command: *wmic /output:Installed\_software.txt product get Name, Version*

* List system drivers

Command: *wmic /output:Loaded\_system\_drivers\_wmic.txt sysdriver list full*

* List Startup Items (more comprehensive list is contained in Sysinternals Autoruns)

Command: *wmic /output:Startup\_wmic.txt startup list full*

* List All Logons

Command: *wmic /output:All\_logons\_wmic.txt logon list full*

* List Driver Group Load Order

Command: *wmic /output:Driver\_group\_load\_order\_wmic.txt loadorder list full*

* List WMIC system info

Command: *wmic /output:system\_info\_wmic.txt os get BootDevice, CSName, EncryptionLevel, InstallDate, LastBootUpTime, Name, Version, BuildNumber, CSDVersion /value*

* Run Sysinternals Autoruns

Command: *sysinternals\autorunsc.exe*

* Run Sysinternals File Information

Command: *sysinternals\psfile.exe*

* Run Sysinternals Local and Remote System Information

Command: *sysinternals\psinfo.exe*

* Run Sysinternals Process List

Command: *sysinternals\pslist.exe*

* Run Sysinternals Logged On

Command: *sysinternals\PsLoggedon.exe*

* Run Sysinternals Local and Remote Event Log Viewer

Command: *sysinternals\psloglist.exe*

* Run Sysinternals TCP/UDP endpoint viewer

Command: *sysinternals\Tcpvcon.exe –a*

* Run Sysinternals streams to find Alternate Data Streams

Command: *sysinternals\streams.exe –a*

* Run WinAudit

Command: *WinAudit.exe /r=gsoPxuTUeERNtnzDaIbMpmdcSArCHGBLJF*

THEN

* List Mounted Drives

Command: *ftkimager.exe --list-drives*

Command: *wmic.exe diskdrive list brief /format:list*

Command: *wmic.exe logicaldisk where “drivetype!=4” get name*

Command: *wmic.exe logicaldisk where "drivetype!=4" get size, caption*

* Create image of disk

*Use “Complete\_Windows\_Live\_Response.bat” script to automatically image logical disks,*

OR

*Use FTK Imager GUI to Acquire Disk Image*

EVIDENCE NUMBER: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DATE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

EXAMINER NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_