<INSERT COMPANY LOGO HERE>

Compromised OSX System

Live Data Gathering Checklist

* Run Live Collection script

Run the applicable BriMor Labs Live Response script, “Complete\_OSX\_Live\_Response.sh”, “Memory\_Dump\_OSX\_Live\_Response.sh”, or “Triage\_OSX\_Live\_Response.sh” from an external USB drive connected to computer. This script will perform functions such as copying Logs to the external USB drive and collecting information such as date, time, logged in users, process tree, system uptime, etc.

The Complete and Memory Dump versions both require administrative privileges to collect the disk image & memory dump or just the memory dump, respectively

OR

* Create memory dump (using your tool of choice or osxpmem)

Command: *sudo bash*

Command: *unzip osxpmem\_2.1.zip*

Command: *kextload osxpmem.app/MacPmem.kext/*

Command: *./osxpmem.app/osxpmem --elf -o "/outputfolder/memory.dmp"*

Command: *kextunload osxpmem.app/MacPmem.kext*

Command: *rm -rf "/osxpmem\_2.1/\*"*

Command: *sudo bash*

Command: *cp –r /etc/cron\**

* Copy contents of “log” folders

Command: *cp /var/log/\*.log\**

Command: *cp –r /etc/cron\**

* Determine date on the system

Command: *date*

* Determine hostname of the system

Command: *hostname*

* Determine logged in users on the system

Command: *who*

* Determine running processes on the system

Command: *ps auxwww*

* Determine mounted disks/items

Command: *mount*

* Review output of disk utility

Command: *diskutil*

* Determine loaded kernel extensions

Command: *kextstat –l*

* Review contents of /etc/passwd

Command: *cat /etc/passwd*

* Review contents of /etc/group

Command: *cat /etc/group*

* Review .bash\_history for each user

Command: *cat /Users/<USERNAME>/.bash\_history*

* Review .sh\_history for each user

Command: *cat /Users/<USERNAME>/.sh\_history*

* Review Launch Agents for each user

Command: *ls –al /Users/<USERNAME>/Library/LaunchAgents/ | grep –v ^d*

* Review loginwindow.plist for each user

Command: *plutil –convert json -r \* /Users/<USERNAME>/Library/Preferences/loginwindow.plist*

* Review AddressBookMe.plist for each user

Command: *plutil –convert json -r \* /Users/<USERNAME>/Library/Preferences/AddressBookMe.plist*

* Review AddressBook.plist for each user

Command: *plutil –convert json -r \* /Users/<USERNAME>/Library/Preferences/AddressBook.plist*

* Review Launched Login Items for each user

Command: *plutil –convert json -r \* /Users/<USERNAME>/Library/Preferences/com.apple.loginitems.plist*

* Review Recent Items for each user

Command: *plutil –convert json –r \* /Users/<USERNAME>/Library/Preferences/com.apple.recentitems.plist*

* Determine System startup items

Command: *ls –laR /System/Library/StartupItems | grep –v ^d*

* Determine Library startup items

Command: *ls –laR /Library/StartupItems | grep –v ^d*

* Determine System launch agents

Command: *ls –laR /System/Library/LaunchAgents | grep –v ^d*

* Determine System launch daemons

Command: *ls –laR /System/Library/LaunchDaemons | grep –v ^d*

* Determine Library launch agents

Command: *ls –laR /Library/LaunchAgents | grep –v ^d*

* Determine Library launch daemons

Command: *ls –laR /Library/LaunchDaemons | grep –v ^d*

* Determine Application login items

Command: *find /Applications/ -name LogInItems -exec ls -lsct {} \;*

* Determine current network connections

Command: *netstat*

* Determine list of open files and network connections

Command: *lsof –i*

* Determine DNS configuration

Command: *scutil --dns*

* Determine routing table

Command: *netstat -rn*

* Determine ARP table

Command: *arp -an*

* Review network interface information

Command: *ifconfig -a*

Command: *ifconfig -L*

* Review allowed hosts

Command: *cat /etc/hosts.allow*

* Determine wireless access points

Command: *defaults read /Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist |sed 's|\./|`pwd`/|g' | sed 's|.plist||g'|grep 'LastConnected' -A 9*

* Review firewall configuration

Command: *plutil -convert json -r \* /Library/Preferences/com.apple.alf.plist*

* Review NAT configuration

Command: *plutil –convert json –r \* /Library/Preferences/SystemConfiguration/com.apple.nat.plist*

* Review SMB configuration

Command: *plutil –convert json -r \* /Library/Preferences/SystemConfiguration/com.apple.smb.server.plist*

THEN

* Create image of disk

*USING YOUR TOOL OF CHOICE*

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

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

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