! ! 2.4!Edition!

Cross!reference!processes!with!various!lists:! psxview! !Show!processes!in!parent/child!tree:! pstree! **&**

**Process&Information&** !Specify!–o/HHoffset=OFFSET!or!Hp/HHpid=1,2,3!! !Display!DLLs:! dlllist! !Show!command!line!arguments:! cmdline! !Display!details!on!VAD!allocations:! vadinfo![HHaddr]! !Dump!allocations!to!individual!files:! vaddump!HHdumpHdir=PATH![HHbase]! !Dump!all!valid!pages!to!a!single!file:! memdump!HHdumpHdir=PATH! !Display!open!handles:! handles!! !!!!Ht/HHobjectHtype=TYPE!!!Mutant,!File,!Key,!etc...! !!!!Hs/HHsilent!!!!!!!!!!!!!!!!!!!!!!!!!!!Hide!unnamed!handles! !Display!privileges:! privs!! !!!!Hr/HHregex=REGEX!!!!!!!!!!!Regex!privilege!name! !!!!Hs/HHsilent!!!!!!!!!!!!!!!!!!!!!!!!!!!Explicitly!enabled!only! !Display!SIDs:! getsids! !Display!environment!variables:! envars! !

**PE&File&Extraction&** !Specify!HD/HHdumpHdir!to!any!of!these!plugins!to! identify!your!desired!output!directory.!! !Dump!a!kernel!module:! moddump!! !!!!Hr/HHregex=REGEX!!!Regex!module!name!! !!!!Hb/HHbase=BASE!!!!!!!Module!base!address!! !Dump!a!process:! procdump!! !!!!Hm/HHmemory!!!!!!!!!!!Include!memory!slack! !Dump!DLLs!in!process!memory:! dlldump!! !!!!Hr/HHregex=REGEX!!!Regex!module!name!! !!!!Hb/HHbase=BASE!!!!!!!Module!base!address!! **&**

**Injected&Code&** !Specify!–o/HHoffset=OFFSET!or!Hp/HHpid=1,2,3! !Find!and!extract!injected!code!blocks:! malfind!! !!!!HD/HHdumpHdir=PATH!!!!Dump!findings!here!! !CrossHreference!DLLs!with!memory!mapped!files:! ldrmodules! !

Copyright!©!2014!The!Volatility!Foundation!

Scan!a!block!of!code!in!process!or!kernel!memory! for!imported!APIs:! impscan!! !!!!Hp/HHpid=PID!!!!!!!!!Process!ID!! !!!!Hb/HHbase=BASE!!!Base!address!to!scan! !!!!Hs/HHsize=SIZE!!!!!!!Size!to!scan!from!start!of!base! !

**Logs&/&Histories&** !Recover!event!logs!(XP/2003):!

!! Development!build!and!wiki:! github.com/volatilityfoundation!! !Download!a!stable!release:! volatilityfoundation.org!! !Read!the!book:! artofmemoryforensics.com! !Development!Team!Blog:! http://volatilityHlabs.blogspot.com!! !(Official)!Training!Contact:!

evtlogs!! !!!!HS/HHsaveHevt!!!!!!!!!!!!!!!!!!!!Save!raw!event!logs! !!!!HD/HHdumpHdir=PATH!!!Write!to!this!directory! !Recover!command!history:! cmdscan!and!consoles!! !Recover!IE!cache/Internet!history:! iehistory!! !Show!running!services:! svcscan!! !!!!Hv/HHverbose!!!!Show!ServiceDll!from!registry! !

**Networking&Information&** voltraining@memoryanalysis.net!! !Follow:!@volatility! Learn:!www.memoryanalysis.net!! !

**Basic&Usage&**

!Active!info!(XP/2003):! connections!and!sockets!! !Scan!for!residual!info!(XP/2003):! connscan!and!sockscan! !Typical!command!components:!! #!vol.py!Hf![image]!HHprofile=[profile]![plugin]! !Display!profiles,!address!spaces,!plugins:!

!Network!info!for!Vista,!2008,!and!7:**&** netscan! !

**Kernel&Memory&** #!vol.py!HHinfo! !Display!global!commandHline!options:! #!vol.py!HHhelp! !Display!pluginHspecific!arguments:! #!vol.py![plugin]!HHhelp! !Load!plugins!from!an!external!directory:! #!vol.py!HHplugins=[path]![plugin]!! !Specify!a!DTB!or!KDBG!address:! #!vol.py!HHdtb=[addr]!HHkdbg=[addr]! !Specify!an!output!file:! #!vol.py!HHoutputHfile=[file]! !

!Display!loaded!kernel!modules:! modules! !**&**Scan!for!hidden!or!residual!modules:! modscan! !Display!recently!unloaded!modules:**&** unloadedmodules! !Display!timers!and!associated!DPCs:**&** timers!! !Display!kernel!callbacks,!notification!routines:! callbacks!! !!Audit!the!SSDT!**& Image&Identification& &**Get!profile!suggestions!(OS!and!architecture):! imageinfo!! **&**Find!and!parse!the!debugger!data!block:! kdbgscan! !

**Processes&Listings&**

ssdt!! !!!!Hv/HHverbose!!!!Check!for!inline!API!hooks! !Audit!the!IDT!and!GDT:! idt!(x86!only)! gdt!(x86!only)! !Audit!driver!dispatch!(IRP)!tables:**&** driverirp!! !!!!Hr/HHregex=REGEX!!!Regex!driver!name! !Basic!active!process!listing:! pslist! !Scan!for!hidden!or!terminated!processes:! psscan! !!

!Display!device!tree!(find!stacked!drivers):! devicetree! !Print!kernel!pool!tag!usage!stats:! pooltracker! !!!!!!Ht/HHtags=TAGS!!!!!!!List!of!tags!to!analyze! !!!!!!HT/HHtagfile=FILE!!!pooltag.txt!for!labels!

! ! 2.4!Edition! **Kernel&Objects&** !Scan!for!driver!objects:! driverscan! !Scan!for!mutexes:! mutantscan!! !!!!Hs/HHsilent!!!!!Hide!unnamed!mutants! !Scan!for!used/historical!file!objects:! filescan! !Scan!for!symbolic!link!objects!(shows!drive! mappings):**&** symlinkscan! !

**Registry&** !Display!cached!hives:**&** hivelist! !Print!a!key’s!values!and!data:**&** printkey!! !!!Ho/HHhive\_offset=OFFSET!!!Hive!address!(virtual)! !!!HK/HHkey=KEY!!!!!!!!!!!!!!!!!!!!!!!!!Key!path!! !Dump!userassist!data:! userassist! !Dump!shellbags!information:! shellbags! !Dump!the!shimcache:! shimcache! !

**Timelines& &**To!create!a!timeline,!create!output!in!body!file! format.!Combine!the!data!and!run!sleuthkit’s! mactime!to!create!a!CSV!file.! !timeliner!HHoutput=body!>!time.txt! shellbags!HHoutput=body!>>!time.txt!! mftparser!HHoutput=body!>>!time.txt! !mactime!–b![time.txt]![Hd]!>!csv.txt! **&**

**Volshell&** !List!processes:! >>>!ps()! !Switch!contexts!by!pid,!offset,!or!name:! >>>!cc(pid!=!3028)! >>>!cc(offset!=!0x3eb31340,!physical=True)! >>>!cc(name!=!“explorer.exe”)! !Acquire!a!process!address!space!after!using!cc:! >>>!process\_space!=! proc().get\_process\_address\_space()! !Disassemble!data!in!an!address!space! >>>!dis(address,!length,!*space*)! !Dump!bytes,!dwords!or!qwords:! >>>!db(address,!length,!*space*)! >>>!dd(address,!length,!*space*)! >>>!dq(address,!length,!*space*)! !!

Copyright!©!2014!The!Volatility!Foundation! Display!a!type/structure:!

Dump!the!contents!of!the!clipboard:! >>>!dt(“\_EPROCESS”,!recursive!=!True)!

clipboard! !!Display!a!type/structure!instance:! >>>!dt(“\_EPROCESS”,!!0x820c92a0)!

Detect!message!hooks!(keyloggers):! messagehooks! !!Create!an!object!in!kernel!space:! >>>!thread!=!obj.Object(“\_ETHREAD”,!offset!=!!

Take!a!screen!shot!from!the!memory!dump:! screenshot!HHdumpHdir=PATH! 0x820c92a0,!vm!=!addrspace())**&** !**&**

Display!visible!and!hidden!windows:! **Dump&Conversion&** !windows!and!wintree!

!

Create!a!raw!memory!dump!from!a!hibernation,!

**Strings&** crash!dump,!firewire!acquisition,!virtualbox,! vmware!snapshot,!hpak,!or!EWF!file:! imagecopy!–O/HHoutputHimage=FILE! !Convert!any!of!the!aforementioned!file!types!to!a! Windows!crash!dump!compatible!with!Windbg:! raw2dmp!–O/HHoutputHimage=FILE! **&**

**API&Hooks&&**

!Use!GNU!strings!or!Sysinternals!strings.exe:**&** strings!Ha!Htd!FILE!>!strings.txt!! strings!Ha!Htd!Hel!FILE!>>!strings.txt!(Unicode)! !strings.exe!Hq!Ho!>!strings.txt!(Windows)! !Translate!the!string!addresses:! strings! !!!!!Hs/HHstringHfile=FILE!!!!Input!strings.txt!file! Scan!for!API!hooks:!

!!!!HS/HHscan!! apihooks!!

! !!!!HR/HHskipHkernel!!!!!!!!Don’t!check!kernel!modules! !!!!HP/HHskipHprocess!!!!!!Don’t!check!processes!! !!!!HQ/HHquick!!!!!!!!!!!!!!!!!!!!Scan!faster!!

**Password&Recovery& &** !

Dump!LSA!secrets:! **Yara&Scanning&&** !Scan!for!Yara!signatures:! yarascan!! !!!!Hp/HHpid=PID!!!!!!!!!!!!!!!!!!!!!!!Process!IDs!to!scan!!

lsadump!! !Dump!cached!domain!hashes:! cachedump!! !!!!!HK/HHkernel!!!!!!!!!!!!!!!!!!!!!!!!!!Scan!kernel!memory!

Dump!LM!and!NTLM!hashes:! !!!!HY/HHyaraHrules=RULES!!!String,!regex,!bytes,!etc.!

hashdump!(x86!only)! !!!!Hy/HHyaraHfile=FILE!!!!!!!!!!!Yara!rules!file!! !!!!!HW/HHwide!!!!!!!!!!!!!!!!!!!!!!!!!!!Match!Unicode!strings!

Extract!OpenVPN!credentials:! !!!!Hs/HHsize!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Size!of!preview!bytes!

openvpn!(github.com/Phaeilo)! !

**File&System&Resources&**

!Extract!RSA!private!keys!and!certificates:! !dumpcerts! Scan!for!MFT!records:!

!!!!Hs/HHssl!!!!!!!Parse!certificates!with!openssl!! mftparser!!

! !!!!HHoutput=body!!!!Output!body!format! !!!!HD/HHdumpHdir!!!!Dump!MFTHresident!data!! !**Disk&Encryption&&** !Extract!cached!files!(registry!hives,!executables):!

Recover!cached!TrueCrypt!passphrases:! dumpfiles!!

truecryptpassphrase!! !!!!HD/HHdumpHdir=PATH!!!!!!!Output!directory!! !!!!!Hr/HHregex=REGEX!!!!!!!!!!!!!Regex!filename!!

Triage!TrueCrypt!artifacts:! !truecryptsummary! Parse!USN!journal!records:! !usnparser!(github.com/tomspencer)!

Extract!TrueCrypt!master!keys! **&**

truecryptmaster! !**GUI&Memory&**

!

**Malware&Specific&** Sessions!(shows!RDP!logins):!! !sessions!

Dump!Zeus/Citadel!RC4!keys:! !zeusscan!and!citadelscan! Window!stations!(shows!clipboard!owners):! !wndscan!

Find!and!decode!Poison!Ivy!configs:! !poisonivyconfig! Desktops!(find!ransomware):! !Deskscan!

Decode!Java!RAT!config:! !javaratscan!(github.com/Rurik)! Display!global!and!session!atom!tables:!

! atoms!and!atomscan! !!

! ! 2.4!Edition! !!General!Investigations! Dump!the!system’s!raw!registry!hive!files! dumpfiles!Dp!4!DDregex='(config|ntuser)'!DDignoreDcase!DDname!DD!./! Create!a!Graphviz!diagram!of!processes! psscan!DDoutput=dot!DDoutputDfile=graph.dot! Create!a!color!coded!diagram!of!processes!memory! vadtree!Dp!PID!DDoutput=dot!DDoutputDfile=graph.dot! Translate!an!account!SID!to!user!name! printkey!DK!"Microsoft\\Windows!NT\\CurrentVersion\\ProfileList\\[SID]"!|!grep!ProfileImagePath! List!run!keys!for!HKLM!and!all!users! printkey!DK!"Microsoft\\Windows\\CurrentVersion\\Run"!

printkey!DK!"Software\\Microsoft\\Windows\\CurrentVersion\\Run"! Find!Unicode!hostnames!or!URLs! yarascan!DY!"/(www|http).+\.(com|net|org)/"!DDwide![DDkernel]! Find!nullDterminated!ASCII!dot!quad!IP!addresses! yarascan!DY!"/([0D9]{1,3}\.){3}[0D9]{1,3}\x00/"!DDwide![DDkernel]! Locate!and!extract!the!HOSTS!file!to!local!directory! !

Copyright!©!2014!The!Volatility!Foundation! filescan!|!egrep!hosts$!|!awk!'{print!$1}'! 0x0000000005e3c6d8! dumpfiles!DQ!0x0000000005e3c6d8!DDname!DD!./! Extract!the!admin!password!hash! hashdump!|!grep!Administrator!>!admin.txt! Malicious!Code! Check!if!a!process!has!domain!or!enterprise!admin! getsids!|!egrep!'(Domain|Enterprise)'! Identify!processes!with!raw!sockets! handles!Dt!File!|!grep!"\\Device\\RawIp\\0"! Look!for!explicit!enabled!debug!privilege!! privs!DDsilent!DDregex=debug! Identify!alternate!data!streams! mftparser!|!grep!"DATA!ADS"! Dump!MFTDresident!batch!scripts! mftparser!DD!output/!

file!output/\*!|!grep!"DOS!batch!file"! Determine!what!is!spying!on!the!clipboard! wndscan!|!grep!ClipViewer! Dump!injected!code!and!focus!on!executables! malfind!DD!output/!

file!output/\*!|!grep!PE! Trace!API!hooks!through!memory! apihooks!Dp!PID!DDquick!|!grep!'Hook!address'!

0x1da654f! echo!"dis(0x1da654f,!length!=!512)"!|!volshell!Dp!PID!! Scan!for!a!specific!mutex!on!the!system! mutantscan!|!grep![Di]![MUTANT!NAME]! Dump!injected!DLL,!fix!image!base!+!IDA!import! labels!

dlldump!DDbase=ADDR!Dp!PID!DD./!DDfix!–memory! impscan!DDbase=ADDR!Dp!PID!DDoutput=idc!>!labels.idc! Find!binaries!loaded!from!temporary!directories! envars!Dp!PID!|!grep!TEMP!|!awk!'{print!$5}'!

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp! Filter!dlllist!and!modules!output!for!the!specified!path! User!Activity! Detect!remote!mapped!shares! handles!Dt!File!|!egrep!"\\Device\\(LanmanRedirector|Mup)"! Files!on!Truecrypt!volumes! filescan!|!grep!TrueCryptVolume! Extract!ASCII!and!Unicode!clipboard!content! clipboard!|!grep!TEXT! Brute!force!search!for!command!history! yarascan!DY!"/C:\\\\.+>/"!DDwide![DDkernel]! Recently!clicked!applications!and!shortcuts! userassist!|!grep!REG\_BINARY! Find!prefetch!files!(recently!executed!programs)! mftparser!|!grep!\.pf$!|!awk!'{print!$NF}'! Kernel!Memory! Identify!hooked!driver!dispatch!tables! driverirp!DDregex=tcpip!|!grep!IRP!|!egrep!Dvi!'(tcpip|ntos)'! Look!for!hooked!SSDT!functions! ssdt!|!egrep!–vi!'(ntos|win32k)!'! Malicious!kernel!callbacks!and!timers! callbacks!|!grep!UNKNOWN!(same!with!timers)! Locate!hidden!threadDbased!kernel!rootkits! threads!DF!OrphanThread!|!grep!StartAddress! Speed!Enhancements! Find!and!set!the!kernel!DTB! psscan!|!grep!System!|!awk!'{print!$5}'!

0x00319000!(Now!use!DDdtb=0x00319000)! Find!and!set!the!KDBG!on!XPD7!and!32Dbit!8! kdbgscan!|!grep!Offset!|!grep!V!|!uniq!

Offset!(V)!:!0xf80002803070!(add!to!DDkdbg)! Find!and!set!the!KDBG!on!64Dbit!8!and!2012! kdbgscan!DDprofile=[PROFILE]!|!grep!KdCopyDataBlock!!

KdCopyDataBlock!(V)!:!0xf80281ff5ea0!(add!to!DDkdbg)! Volshell!Scripting! Create!a!process!ID!lookup!table! by\_pid!=!dict((p.UniqueProcessId,!p)!for!p!in!getprocs())!

parent\_name!=!by\_pid[PID].ImageFileName! Scan!process!memory!and!print!a!hex!dump! needles!=!["abc123",!"def456"]!

for!hit!in!proc().search\_process\_memory(needles):! !!!!!db(hit)! Extract!a!chunk!of!kernel!memory!to!disk! data!=!addrspace().zread(ADDR,!SIZE)!

with!open("output.bin",!"wb")!as!handle:! !!!!!handle.write(data)! Translate!a!kernel!address!and!seek!to!it!(raw! dumps!only)!

echo!"addrspace().vtop(0x98dfd9c8)"!|!volshell!Df![MEMDUMP]! 597989832! xxd!Ds!597989832![MEMDUMP]! Kernel!modules!with!embedded!PE!signatures! signed!=![mod!for!mod!in!getmods()!if!mod.sec\_dir()]! !

! ! 2.4!Edition!

Copyright!©!2014!The!Volatility!Foundation! Linux!Commands!

Print!the!kernel!debug!buffer:!

!

**Processes'Listings'**

CrossJreference!shared!libraries!with!memoryJ mapped!files:!

linux\_dmesg! linux\_ldrmodules! !!Audit!the!IDT:! !Check!for!process!hollowing:!

linux\_idt!(x86!only)! Basic!active!process!listing:!

linux\_process\_hollow!

**'** linux\_pslist!

!!!!!Jb/JJbase!!!!Base!address!of!ELF!file!in!memory! !!!!!!JP/JJpath!!!!Path!of!known!good!file!on!disk! List!processes!and!threads:!

! linux\_pidhashtable! !Cross!reference!processes!with!various!lists:! linux\_psxview! !Show!processes!in!parent/child!tree:! linux\_pstree! **'**

**Process'Information'** !Specify!–o/JJoffset=OFFSET!or!Jp/JJpid=1,2,3!! !Display!shared!libraries:! linux\_library\_list! !List!threads:! linux\_threads! !Show!command!line!arguments:! linux\_psaux! !**Userland'API'Hooks''**

!Scan!for!API!hooks:! linux\_apihooks!! !!!!!!Ja/JJall!!!!!!!!!!!Check!hooked!PLT!entries! !Scan!for!GOT/PLT!hooks:! linux\_plthook! !!!!!!Ja/JJall!!!!!!!!!!List!all!PLT!entries! !!!!!!Ji/JJignore!!!Libraries!to!ignore!in!processing! !

**Yara'Scanning''** !Scan!for!Yara!signatures:! linux\_yarascan!! !!!!Jp/JJpid=PID!!!!!!!!!!!!!!!!!!!!!!!Process!IDs!to!scan!! !!!!JK/JJkernel!!!!!!!!!!!!!!!!!!!!!!!!!!Scan!kernel!memory! !!!!JY/JJyaraJrules=RULES!!!String,!regex,!bytes,!etc.! !!!!Jy/JJyaraJfile=FILE!!!!!!!!!!!Yara!rules!file!! !!!!JW/JJwide!!!!!!!!!!!!!!!!!!!!!!!!!!!Match!Unicode!strings! !!!!Js/JJsize!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Size!of!preview!bytes! !

**File'System'Resources'** Display!details!on!memory!ranges:! !linux\_proc\_maps!

List!mount!points:! !linux\_mount! Dump!allocations!to!individual!files:! !linux\_dump\_map!!

Enumerate!files:! !!!!!!!!JD/JJdumpJdir=PATH!!

linux\_enumerate\_files! !!!!!!!!JJvma=ADDR!!!!!Range!to!dump! !!Extract!cached!files:! Display!open!handles:!

linux\_find\_file! linux\_lsof!

!!!!JF/JJfind=FILE!!!!!!!!!!!!!Path!of!file!to!find! !!!!Ji/JJinode=INODE!!!!!!!Address!of!inode!to!dump!! !!!!JL/JJlistfiles!!!!!!!!!!!!!!!!!!Lists!files!in!cache!! !!!!JO/JJoutputfile!!!!!!!!!!!!!File!path!to!write! **'**

**Disk'Encryption'' '** Recover!cached!Truecrypt!passphrases:! linux\_truecryptpassphrase!! !

**Strings'** !Translate!extracted!strings:! linux\_strings! !!!!Js/JJstringJfile=FILE!!!!Input!strings.txt!file! !!!!! ! **Command'History'** !Recover!command!history:! linux\_bash! !Recover!executed!binaries:! linux\_bash\_hash! !

**Networking'Information'** !Active!info:! linux\_netstat! !Interface!information:! linux\_ifconfig! !Raw!sockets:**'** linux\_list\_raw! !Routing!cache:**'** linux\_route\_cache! !!!!!JR/JJresolve!!!!DNS!resolve!destination!IPs! !Netfilter!entries:! linux\_netfilter! !ARP!cache:! linux\_arp! !

**Kernel'Memory'** !!Display!environment!variables:!

Display!loaded!kernel!modules:! linux\_psenv!and!linux\_bash\_env!

linux\_lsmod! !

!!**ELF'File'Extraction'** !Specify!JD/JJdumpJdir!to!any!of!these!plugins!to! identify!your!desired!output!directory.!! !Dump!a!kernel!module:! linux\_moddump!! !!!!Jr/JJregex=REGEX!!!Regex!module!name!! !!!!Jb/JJbase=BASE!!!!!!!Module!base!address!! !Dump!a!process:! linux\_procdump!! !Dump!shared!libraries!in!process!memory:! linux\_librarydump!! !!!!Jr/JJregex=REGEX!!!Regex!module!name!! !!!!Jb/JJbase=BASE!!!!!!!Module!base!address!! **'**

**Injected'Code'**

Check!for!system!call!hooks:! linux\_check\_syscall!! !Check!for!network!stack!hooks:! linux\_check\_afinfo! !Check!for!credential!copying:! linux\_check\_creds! !Check!for!file!operations!hooking:! linux\_check\_fop! !Check!for!inline!kernel!hooks:! linux\_check\_inline\_kernel! !Check!for!hidden!modules:! linux\_check\_modules! linux\_hidden\_modules! !Check!for!TTY!hooks:! !linux\_check\_tty! Specify!–o/JJoffset=OFFSET!or!Jp/JJpid=1,2,3! !!Check!for!malicious!keyboard!callbacks:! Find!and!extract!injected!code!blocks:!

linux\_keyboard\_notifiers! linux\_malfind! !!!! !!

! ! 2.4!Edition!

Copyright!©!2014!The!Volatility!Foundation! **Mac$OS$X$Commands$**

Print!the!kernel!debug!buffer:! **$**

CrossNreference!shared!libraries!with!memoryN mapped!files:! mac\_ldrmodules!

mac\_dmesg!

!**Processes$Listings$**

!

**Command$History$**

**API$Hooks$$** !Scan!for!API!hooks:! Basic!active!process!listing:!

!mac\_apihooks!! mac\_pslist!

Recover!command!history:!

!!!!NR/NNskipNkernel!!!!!!!!Don’t!check!kernel!modules! !mac\_bash!

!!!!NP/NNskipNprocess!!!!!!Don’t!check!processes!! List!PID!hash!table:!

!!!!!NQ/NNquick!!!!!!!!!!!!!!!!!!!!Scan!faster!! mac\_pid\_hash\_table!

Recover!executed!binaries:! !!mac\_bash\_hash!

Check!for!process!hollowing:! List!tasks:!

!

mac\_process\_hollow! mac\_tasks!

!!!!!Nb/NNbase!!!!Base!address!of!ELF!file!in!memory! !!!!!!NP/NNpath!!!!Path!of!known!good!file!on!disk! Cross!reference!processes!with!various!lists:! !mac\_psxview!

Scan!for!GOT/PLT!hooks:! !mac\_plthook! Show!processes!in!parent/child!tree:!

!!!!!!Na/NNall!!!!!!!!!!List!all!PLT!entries! mac\_pstree!

!!!!!!Ni/NNignore!!!Libraries!to!ignore!in!processing! **$**

! **Process$Information$**

**Yara$Scanning$$** !Scan!for!Yara!signatures:! mac\_yarascan!! !!!!Np/NNpid=PID!!!!!!!!!!!!!!!!!!!!!!!Process!IDs!to!scan!! !!!!NK/NNkernel!!!!!!!!!!!!!!!!!!!!!!!!!!Scan!kernel!memory! !!!!NY/NNyaraNrules=RULES!!!String,!regex,!bytes,!etc.! !!!!Ny/NNyaraNfile=FILE!!!!!!!!!!!Yara!rules!file!! !!!!NW/NNwide!!!!!!!!!!!!!!!!!!!!!!!!!!!Match!Unicode!strings! !!!!Ns/NNsize!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Size!of!preview!bytes! !

**Disk$Encryption$$ $** Recover!possible!Keychain!keys:! mac\_keychaindump! !

**File$System$Resources$** !List!mount!points:! mac\_mount! !List!cached!files!and!their!vnode!addresses:! mac\_list\_files! !Extract!cached!files:! mac\_dump\_file! !!!!!Nq/NNfile\_offset!!!!!!!Offset!of!vnode!to!dump!! !!!!!NO/NNoutputfile!!!!!File!path!to!write! !

**Strings$** !Translate!extracted!string:! mac\_strings! !!!!Ns/NNstringNfile=FILE!!!!Input!strings.txt!file! !

**User$Activity$ $** Recover!Adium!messages,!including!OTR!chat:! mac\_adium! **$**Recover!Calendar!entries:! mac\_calendar! **$**Recover!contacts:! mac\_contacts! **$ Networking$Information$** !Active!info:! mac\_netstat! !Active!info!from!network!stack:! mac\_network\_conns! !Interface!Information:! !mac\_ifconfig! Specify!–o/NNoffset=OFFSET!or!Np/NNpid=1,2,3!! !!ARP!cache:! Display!shared!libraries:!

mac\_arp! mac\_dyld\_maps! !!Route!table:! Show!command!line!arguments:!

mac\_route! mac\_psaux! !!Socket!filters:! Display!details!on!memory!ranges:!

mac\_socket\_filters! mac\_proc\_maps! !!IP!filters:! Dump!allocations!to!individual!files:!

mac\_ip\_filters! mac\_dump\_map!!

! !!!!!!ND/NNdumpNdir=PATH!! !!!!!NNmap\_address=ADDR!! !Display!open!handles:! mac\_lsof! !Display!environment!variables:! mac\_psenv!and!mac\_bash\_env! !Display!login!sessions:! mac\_list\_sessions! !

**Mach8O$File$Extraction$**

**Kernel$Memory$** !Display!loaded!kernel!modules:! mac\_lsmod! !!Check!for!kernel!API!hooks:! mac\_apihooks\_kernel! !Check!for!system!call!hooks:! mac\_check\_syscalls! !Check!for!shadow!system!call!table:! mac\_check\_syscall\_shadow! !!Specify!ND/NNdumpNdir!to!any!of!these!plugins!to!

Check!sysctl!handlers:! identify!your!desired!output!directory.!!

mac\_check\_sysctl! !!Dump!a!kernel!module:!

Check!the!trap!table:! mac\_moddump!!

mac\_check\_trap\_table! !!!!Nr/NNregex=REGEX!!!Regex!module!name!! !!!!!Nb/NNbase=BASE!!!!!!!Module!base!address!!

Check!the!mig!table:! !mac\_check\_mig\_table! Dump!a!process:! !mac\_procdump!!

Check!for!file!operations!hooking:! !mac\_check\_fop! Dump!shared!libraries!in!process!memory:! !mac\_librarydump!!

Check!for!inline!kernel!hooks:! !!!!Nb/NNbase=BASE!!!!!!!Module!base!address!!

mac\_check\_inline\_kernel! **$**

!**Injected$Code$** !Specify!–o/NNoffset=OFFSET!or!Np/NNpid=1,2,3! !Find!and!extract!injected!code!blocks:! mac\_malfind! !

Check!for!hidden!modules:! mac\_lsmod\_iokit! mac\_lsmod\_kext\_map! !Check!for!TrustedBSD!hooks:! mac\_trustedbsd! !