Lab Exam -2

Name : P.Vishnu vardhan Reddy
Roll No : 2021BCY0043

Volatility check

```
C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility --info
Volatility Foundation Volatility Framework 2.6


Profiles
--------
VistaSP0x64           - A Profile for Windows Vista SP0 x64
VistaSP0x86           - A Profile for Windows Vista SP0 x86
VistaSP1x64           - A Profile for Windows Vista SP1 x64
VistaSP1x86           - A Profile for Windows Vista SP1 x86
VistaSP2x64           - A Profile for Windows Vista SP2 x64
VistaSP2x86           - A Profile for Windows Vista SP2 x86
Win10x64              - A Profile for Windows 10 x64
Win10x64_10586        - A Profile for Windows 10 x64 (10.0.10586.306 /
2016-04-23)
Win10x64_14393        - A Profile for Windows 10 x64 (10.0.14393.0 /
2016-07-16)
Win10x86              - A Profile for Windows 10 x86
Win10x86_10586        - A Profile for Windows 10 x86 (10.0.10586.420 /
2016-05-28)
Win10x86_14393        - A Profile for Windows 10 x86 (10.0.14393.0 /
2016-07-16)
Win2003SP0x86         - A Profile for Windows 2003 SP0 x86
Win2003SP1x64         - A Profile for Windows 2003 SP1 x64
Win2003SP1x86         - A Profile for Windows 2003 SP1 x86
Win2003SP2x64         - A Profile for Windows 2003 SP2 x64
Win2003SP2x86         - A Profile for Windows 2003 SP2 x86
Win2008R2SP0x64       - A Profile for Windows 2008 R2 SP0 x64
Win2008R2SP1x64       - A Profile for Windows 2008 R2 SP1 x64
Win2008R2SP1x64_23418 - A Profile for Windows 2008 R2 SP1 x64
(6.1.7601.23418 / 2016-04-09)
Win2008SP1x64         - A Profile for Windows 2008 SP1 x64
Win2008SP1x86         - A Profile for Windows 2008 SP1 x86
Win2008SP2x64         - A Profile for Windows 2008 SP2 x64
Win2008SP2x86         - A Profile for Windows 2008 SP2 x86
Win2012R2x64          - A Profile for Windows Server 2012 R2 x64
Win2012R2x64_18340    - A Profile for Windows Server 2012 R2 x64
(6.3.9600.18340 / 2016-05-13)
Win2012x64            - A Profile for Windows Server 2012 x64
Win2016x64_14393      - A Profile for Windows Server 2016 x64
(10.0.14393.0 / 2016-07-16)
Win7SP0x64            - A Profile for Windows 7 SP0 x64
Win7SP0x86            - A Profile for Windows 7 SP0 x86
Win7SP1x64            - A Profile for Windows 7 SP1 x64
Win7SP1x64_23418      - A Profile for Windows 7 SP1 x64 (6.1.7601.23418 /
2016-04-09)
Win7SP1x86            - A Profile for Windows 7 SP1 x86
Win7SP1x86_23418      - A Profile for Windows 7 SP1 x86 (6.1.7601.23418 /
2016-04-09)
Win81U1x64            - A Profile for Windows 8.1 Update 1 x64
Win81U1x86            - A Profile for Windows 8.1 Update 1 x86
```

```
Win8SP0x64            - A Profile for Windows 8 x64
Win8SP0x86            - A Profile for Windows 8 x86
Win8SP1x64            - A Profile for Windows 8.1 x64
Win8SP1x64_18340      - A Profile for Windows 8.1 x64 (6.3.9600.18340 /
2016-05-13)
Win8SP1x86            - A Profile for Windows 8.1 x86
WinXPSP1x64           - A Profile for Windows XP SP1 x64
WinXPSP2x64           - A Profile for Windows XP SP2 x64
WinXPSP2x86           - A Profile for Windows XP SP2 x86
WinXPSP3x86           - A Profile for Windows XP SP3 x86


Address Spaces
--------------
AMD64PagedMemory              - Standard AMD 64-bit address space.
ArmAddressSpace               - Address space for ARM processors
FileAddressSpace              - This is a direct file AS.
HPAKAddressSpace              - This AS supports the HPAK format
IA32PagedMemory               - Standard IA-32 paging address space.
IA32PagedMemoryPae            - This class implements the IA-32 PAE
paging address space. It is responsible
LimeAddressSpace              - Address space for Lime
LinuxAMD64PagedMemory         - Linux-specific AMD 64-bit address space.
MachOAddressSpace             - Address space for mach-o files to support
atc-ny memory reader
OSXPmemELF                    - This AS supports VirtualBox ELF64
coredump format
QemuCoreDumpElf               - This AS supports Qemu ELF32 and ELF64
coredump format
VMWareAddressSpace            - This AS supports VMware snapshot (VMSS)
and saved state (VMSS) files
VMWareMetaAddressSpace        - This AS supports the VMEM format with
VMSN/VMSS metadata
VirtualBoxCoreDumpElf64       - This AS supports VirtualBox ELF64
coredump format
Win10AMD64PagedMemory         - Windows 10-specific AMD 64-bit address
space.
WindowsAMD64PagedMemory       - Windows-specific AMD 64-bit address
space.
WindowsCrashDumpSpace32       - This AS supports windows Crash Dump
format
WindowsCrashDumpSpace64       - This AS supports windows Crash Dump
format
WindowsCrashDumpSpace64BitMap - This AS supports Windows BitMap Crash
Dump format
WindowsHiberFileSpace32       - This is a hibernate address space for
windows hibernation files.


Scanner Checks
--------------
CheckPoolSize           - Check pool block size
CheckPoolType           - Check the pool type
KPCRScannerCheck        - Checks the self referential pointers to find
KPCRs
MultiPrefixFinderCheck - Checks for multiple strings per page, finishing
at the offset
MultiStringFinderCheck - Checks for multiple strings per page
```

```
PoolTagCheck           - This scanner checks for the occurance of a pool
tag


Plugins
-------
amcache                    - Print AmCache information
apihooks                   - Detect API hooks in process and kernel
memory
atoms                      - Print session and window station atom tables
atomscan                   - Pool scanner for atom tables
auditpol                   - Prints out the Audit Policies from
HKLM\SECURITY\Policy\PolAdtEv
bigpools                   - Dump the big page pools using
BigPagePoolScanner
bioskbd                    - Reads the keyboard buffer from Real Mode
memory
cachedump                  - Dumps cached domain hashes from memory
callbacks                  - Print system-wide notification routines
clipboard                  - Extract the contents of the windows
clipboard
cmdline                    - Display process command-line arguments
cmdscan                    - Extract command history by scanning for
_COMMAND_HISTORY
connections                - Print list of open connections [Windows XP
and 2003 Only]
connscan                   - Pool scanner for tcp connections
consoles                   - Extract command history by scanning for
_CONSOLE_INFORMATION
crashinfo                  - Dump crash-dump information
deskscan                   - Poolscaner for tagDESKTOP (desktops)
devicetree                 - Show device tree
dlldump                    - Dump DLLs from a process address space
dlllist                    - Print list of loaded dlls for each process
driverirp                  - Driver IRP hook detection
drivermodule               - Associate driver objects to kernel modules
driverscan                 - Pool scanner for driver objects
dumpcerts                  - Dump RSA private and public SSL keys
dumpfiles                  - Extract memory mapped and cached files
dumpregistry               - Dumps registry files out to disk
editbox                    - Displays information about Edit controls.
(Listbox experimental.)
envars                     - Display process environment variables
eventhooks                 - Print details on windows event hooks
evtlogs                    - Extract Windows Event Logs (XP/2003 only)
filescan                   - Pool scanner for file objects
gahti                      - Dump the USER handle type information
gditimers                  - Print installed GDI timers and callbacks
gdt                        - Display Global Descriptor Table
getservicesids             - Get the names of services in the Registry
and return Calculated SID
getsids                    - Print the SIDs owning each process
handles                    - Print list of open handles for each process
hashdump                   - Dumps passwords hashes (LM/NTLM) from memory
hibinfo                    - Dump hibernation file information
hivedump                   - Prints out a hive
hivelist                   - Print list of registry hives.
hivescan                   - Pool scanner for registry hives
```

```
hpakextract                - Extract physical memory from an HPAK file
hpakinfo                   - Info on an HPAK file
idt                        - Display Interrupt Descriptor Table
iehistory                  - Reconstruct Internet Explorer cache /
history
imagecopy                  - Copies a physical address space out as a raw
DD image
imageinfo                  - Identify information for the image
impscan                    - Scan for calls to imported functions
joblinks                   - Print process job link information
kdbgscan                   - Search for and dump potential KDBG values
kpcrscan                   - Search for and dump potential KPCR values
ldrmodules                 - Detect unlinked DLLs
limeinfo                   - Dump Lime file format information
linux_apihooks             - Checks for userland apihooks
linux_arp                  - Print the ARP table
linux_aslr_shift           - Automatically detect the Linux ASLR shift
linux_banner               - Prints the Linux banner information
linux_bash                 - Recover bash history from bash process
memory
linux_bash_env             - Recover a process' dynamic environment
variables
linux_bash_hash            - Recover bash hash table from bash process
memory
linux_check_afinfo         - Verifies the operation function pointers of
network protocols
linux_check_creds          - Checks if any processes are sharing
credential structures
linux_check_evt_arm        - Checks the Exception Vector Table to look
for syscall table hooking
linux_check_fop            - Check file operation structures for rootkit
modifications
linux_check_idt            - Checks if the IDT has been altered
linux_check_inline_kernel  - Check for inline kernel hooks
linux_check_modules        - Compares module list to sysfs info, if
available
linux_check_syscall        - Checks if the system call table has been
altered
linux_check_syscall_arm    - Checks if the system call table has been
altered
linux_check_tty            - Checks tty devices for hooks
linux_cpuinfo              - Prints info about each active processor
linux_dentry_cache         - Gather files from the dentry cache
linux_dmesg                - Gather dmesg buffer
linux_dump_map             - Writes selected memory mappings to disk
linux_dynamic_env          - Recover a process' dynamic environment
variables
linux_elfs                 - Find ELF binaries in process mappings
linux_enumerate_files      - Lists files referenced by the filesystem
cache
linux_find_file            - Lists and recovers files from memory
linux_getcwd               - Lists current working directory of each
process
linux_hidden_modules       - Carves memory to find hidden kernel modules
linux_ifconfig             - Gathers active interfaces
linux_info_regs            - It's like 'info registers' in GDB. It prints
out all the
linux_iomem                - Provides output similar to /proc/iomem
```

```
linux_kernel_opened_files  - Lists files that are opened from within the
kernel
linux_keyboard_notifiers   - Parses the keyboard notifier call chain
linux_ldrmodules           - Compares the output of proc maps with the
list of libraries from libdl
linux_library_list         - Lists libraries loaded into a process
linux_librarydump          - Dumps shared libraries in process memory to
disk
linux_list_raw             - List applications with promiscuous sockets
linux_lsmod                - Gather loaded kernel modules
linux_lsof                 - Lists file descriptors and their path
linux_malfind              - Looks for suspicious process mappings
linux_memmap               - Dumps the memory map for linux tasks
linux_moddump              - Extract loaded kernel modules
linux_mount                - Gather mounted fs/devices
linux_mount_cache          - Gather mounted fs/devices from kmem_cache
linux_netfilter            - Lists Netfilter hooks
linux_netscan              - Carves for network connection structures
linux_netstat              - Lists open sockets
linux_pidhashtable         - Enumerates processes through the PID hash
table
linux_pkt_queues           - Writes per-process packet queues out to disk
linux_plthook              - Scan ELF binaries' PLT for hooks to non-
NEEDED images
linux_proc_maps            - Gathers process memory maps
linux_proc_maps_rb         - Gathers process maps for linux through the
mappings red-black tree
linux_procdump             - Dumps a process's executable image to disk
linux_process_hollow       - Checks for signs of process hollowing
linux_psaux                - Gathers processes along with full command
line and start time
linux_psenv                - Gathers processes along with their static
environment variables
linux_pslist               - Gather active tasks by walking the
task_struct->task list
linux_pslist_cache         - Gather tasks from the kmem_cache
linux_psscan               - Scan physical memory for processes
linux_pstree               - Shows the parent/child relationship between
processes
linux_psxview              - Find hidden processes with various process
listings
linux_recover_filesystem   - Recovers the entire cached file system from
memory
linux_route_cache          - Recovers the routing cache from memory
linux_sk_buff_cache        - Recovers packets from the sk_buff kmem_cache
linux_slabinfo             - Mimics /proc/slabinfo on a running machine
linux_strings              - Match physical offsets to virtual addresses
(may take a while, VERY verbose)
linux_threads              - Prints threads of processes
linux_tmpfs                - Recovers tmpfs filesystems from memory
linux_truecrypt_passphrase - Recovers cached Truecrypt passphrases
linux_vma_cache            - Gather VMAs from the vm_area_struct cache
linux_volshell             - Shell in the memory image
linux_yarascan             - A shell in the Linux memory image
lsadump                    - Dump (decrypted) LSA secrets from the
registry
mac_adium                  - Lists Adium messages
mac_apihooks               - Checks for API hooks in processes
```

```
mac_apihooks_kernel        - Checks to see if system call and kernel
functions are hooked
mac_arp                    - Prints the arp table
mac_bash                   - Recover bash history from bash process
memory
mac_bash_env               - Recover bash's environment variables
mac_bash_hash              - Recover bash hash table from bash process
memory
mac_calendar               - Gets calendar events from Calendar.app
mac_check_fop              - Validate File Operation Pointers
mac_check_mig_table        - Lists entires in the kernel's MIG table
mac_check_syscall_shadow   - Looks for shadow system call tables
mac_check_syscalls         - Checks to see if system call table entries
are hooked
mac_check_sysctl           - Checks for unknown sysctl handlers
mac_check_trap_table       - Checks to see if mach trap table entries are
hooked
mac_compressed_swap        - Prints Mac OS X VM compressor stats and
dumps all compressed pages
mac_contacts               - Gets contact names from Contacts.app
mac_dead_procs             - Prints terminated/de-allocated processes
mac_dead_sockets           - Prints terminated/de-allocated network
sockets
mac_dead_vnodes            - Lists freed vnode structures
mac_devfs                  - Lists files in the file cache
mac_dmesg                  - Prints the kernel debug buffer
mac_dump_file              - Dumps a specified file
mac_dump_maps              - Dumps memory ranges of process(es),
optionally including pages in compressed swap
mac_dyld_maps              - Gets memory maps of processes from dyld data
structures
mac_find_aslr_shift        - Find the ASLR shift value for 10.8+ images
mac_get_profile            - Automatically detect Mac profiles
mac_ifconfig               - Lists network interface information for all
devices
mac_interest_handlers      - Lists IOKit Interest Handlers
mac_ip_filters             - Reports any hooked IP filters
mac_kernel_classes         - Lists loaded c++ classes in the kernel
mac_kevents                - Show parent/child relationship of processes
mac_keychaindump           - Recovers possbile keychain keys. Use
chainbreaker to open related keychain files
mac_ldrmodules             - Compares the output of proc maps with the
list of libraries from libdl
mac_librarydump            - Dumps the executable of a process
mac_list_files             - Lists files in the file cache
mac_list_kauth_listeners   - Lists Kauth Scope listeners
mac_list_kauth_scopes      - Lists Kauth Scopes and their status
mac_list_raw               - List applications with promiscuous sockets
mac_list_sessions          - Enumerates sessions
mac_list_zones             - Prints active zones
mac_lsmod                  - Lists loaded kernel modules
mac_lsmod_iokit            - Lists loaded kernel modules through IOkit
mac_lsmod_kext_map         - Lists loaded kernel modules
mac_lsof                   - Lists per-process opened files
mac_machine_info           - Prints machine information about the sample
mac_malfind                - Looks for suspicious process mappings
mac_memdump                - Dump addressable memory pages to a file
```

```
mac_moddump                - Writes the specified kernel extension to
disk
mac_mount                  - Prints mounted device information
mac_netstat                - Lists active per-process network connections
mac_network_conns          - Lists network connections from kernel
network structures
mac_notesapp               - Finds contents of Notes messages
mac_notifiers              - Detects rootkits that add hooks into I/O Kit
(e.g. LogKext)
mac_orphan_threads         - Lists threads that don't map back to known
modules/processes
mac_pgrp_hash_table        - Walks the process group hash table
mac_pid_hash_table         - Walks the pid hash table
mac_print_boot_cmdline     - Prints kernel boot arguments
mac_proc_maps              - Gets memory maps of processes
mac_procdump               - Dumps the executable of a process
mac_psaux                  - Prints processes with arguments in user land
(**argv)
mac_psenv                  - Prints processes with environment in user
land (**envp)
mac_pslist                 - List Running Processes
mac_pstree                 - Show parent/child relationship of processes
mac_psxview                - Find hidden processes with various process
listings
mac_recover_filesystem     - Recover the cached filesystem
mac_route                  - Prints the routing table
mac_socket_filters         - Reports socket filters
mac_strings                - Match physical offsets to virtual addresses
(may take a while, VERY verbose)
mac_tasks                  - List Active Tasks
mac_threads                - List Process Threads
mac_threads_simple         - Lists threads along with their start time
and priority
mac_timers                 - Reports timers set by kernel drivers
mac_trustedbsd             - Lists malicious trustedbsd policies
mac_version                - Prints the Mac version
mac_vfsevents              - Lists processes filtering file system events
mac_volshell               - Shell in the memory image
mac_yarascan               - Scan memory for yara signatures
machoinfo                  - Dump Mach-O file format information
malfind                    - Find hidden and injected code
mbrparser                  - Scans for and parses potential Master Boot
Records (MBRs)
memdump                    - Dump the addressable memory for a process
memmap                     - Print the memory map
messagehooks               - List desktop and thread window message hooks
mftparser                  - Scans for and parses potential MFT entries
moddump                    - Dump a kernel driver to an executable file
sample
modscan                    - Pool scanner for kernel modules
modules                    - Print list of loaded modules
multiscan                  - Scan for various objects at once
mutantscan                 - Pool scanner for mutex objects
netscan                    - Scan a Vista (or later) image for
connections and sockets
notepad                    - List currently displayed notepad text
objtypescan                - Scan for Windows object type objects
patcher                    - Patches memory based on page scans
```

```
poolpeek                   - Configurable pool scanner plugin
pooltracker                - Show a summary of pool tag usage
printkey                   - Print a registry key, and its subkeys and
values
privs                      - Display process privileges
procdump                   - Dump a process to an executable file sample
pslist                     - Print all running processes by following the
EPROCESS lists
psscan                     - Pool scanner for process objects
pstree                     - Print process list as a tree
psxview                    - Find hidden processes with various process
listings
qemuinfo                   - Dump Qemu information
raw2dmp                    - Converts a physical memory sample to a
windbg crash dump
screenshot                 - Save a pseudo-screenshot based on GDI
windows
servicediff                - List Windows services (ala Plugx)
sessions                   - List details on _MM_SESSION_SPACE (user
logon sessions)
shellbags                  - Prints ShellBags info
shimcache                  - Parses the Application Compatibility Shim
Cache registry key
shutdowntime               - Print ShutdownTime of machine from registry
sockets                    - Print list of open sockets
sockscan                   - Pool scanner for tcp socket objects
ssdt                       - Display SSDT entries
strings                    - Match physical offsets to virtual addresses
(may take a while, VERY verbose)
svcscan                    - Scan for Windows services
symlinkscan                - Pool scanner for symlink objects
thrdscan                   - Pool scanner for thread objects
threads                    - Investigate _ETHREAD and _KTHREADs
timeliner                  - Creates a timeline from various artifacts in
memory
timers                     - Print kernel timers and associated module
DPCs
truecryptmaster            - Recover TrueCrypt 7.1a Master Keys
truecryptpassphrase        - TrueCrypt Cached Passphrase Finder
truecryptsummary           - TrueCrypt Summary
unloadedmodules            - Print list of unloaded modules
userassist                 - Print userassist registry keys and
information
userhandles                - Dump the USER handle tables
vaddump                    - Dumps out the vad sections to a file
vadinfo                    - Dump the VAD info
vadtree                    - Walk the VAD tree and display in tree format
vadwalk                    - Walk the VAD tree
vboxinfo                   - Dump virtualbox information
verinfo                    - Prints out the version information from PE
images
vmwareinfo                 - Dump VMware VMSS/VMSN information
volshell                   - Shell in the memory image
win10cookie                - Find the ObHeaderCookie value for Windows 10
windows                    - Print Desktop Windows (verbose details)
wintree                    - Print Z-Order Desktop Windows Tree
wndscan                    - Pool scanner for window stations
```

```
yarascan                  - Scan process or kernel memory with Yara
signatures
```

image info

```
C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility -f exam.vmem
imageinfo


Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG
search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated
with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace
(C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6\exam.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2011-10-10 17:06:54 UTC+0000
     Image local date and time : 2011-10-10 13:06:54 -0400
```

We can find more about it by using volatility imageinfo plugin. this command is used to identify the operating system, service pack, and hardware architecture (32 or 64 bit), but it also contains other useful information such as the DTB address and time the sample was collected.

Pslist

```
C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility -f exam.vmem
pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess
Wow64 Start                          Exit

---------- -------------------- ------ ------ ------ -------- ------ ----
-- ------------------------------ ------------------------------
0x819cc830 System                    4      0     55      162 ------
0

0x81945020 smss.exe                536      4      3       21 ------
0 2011-10-10 17:03:56 UTC+0000

0x816c6020 csrss.exe               608    536     11      355      0
0 2011-10-10 17:03:58 UTC+0000

0x813a9020 winlogon.exe            632    536     24      533      0
0 2011-10-10 17:03:58 UTC+0000
```

```
0x816da020 services.exe            676    632     16      261      0
0 2011-10-10 17:03:58 UTC+0000

0x813c4020 lsass.exe               688    632     23      336      0
0 2011-10-10 17:03:58 UTC+0000

0x81772ca8 vmacthlp.exe            832    676      1       24      0
0 2011-10-10 17:03:59 UTC+0000

0x8167e9d0 svchost.exe             848    676     20      194      0
0 2011-10-10 17:03:59 UTC+0000

0x817757f0 svchost.exe             916    676      9      217      0
0 2011-10-10 17:03:59 UTC+0000

0x816c6da0 svchost.exe             964    676     63     1058      0
0 2011-10-10 17:03:59 UTC+0000

0x815daca8 svchost.exe            1020    676      5       58      0
0 2011-10-10 17:03:59 UTC+0000

0x813aeda0 svchost.exe            1148    676     12      187      0
0 2011-10-10 17:04:00 UTC+0000

0x817937e0 spoolsv.exe            1260    676     13      140      0
0 2011-10-10 17:04:00 UTC+0000

0x81754990 VMwareService.e        1444    676      3      145      0
0 2011-10-10 17:04:00 UTC+0000

0x8136c5a0 alg.exe                1616    676      7       99      0
0 2011-10-10 17:04:01 UTC+0000

0x815c4da0 wscntfy.exe            1920    964      1       27      0
0 2011-10-10 17:04:39 UTC+0000

0x813bcda0 explorer.exe           1956   1884     18      322      0
0 2011-10-10 17:04:39 UTC+0000

0x816d63d0 VMwareTray.exe          184   1956      1       28      0
0 2011-10-10 17:04:41 UTC+0000

0x8180b478 VMwareUser.exe          192   1956      6       83      0
0 2011-10-10 17:04:41 UTC+0000

0x818233c8 reader_sl.exe           228   1956      2       26      0
0 2011-10-10 17:04:41 UTC+0000

0x815e7be0 wuauclt.exe             400    964      8      173      0
0 2011-10-10 17:04:46 UTC+0000

0x817a34b0 cmd.exe                 544   1956      1       30      0
0 2011-10-10 17:06:42 UTC+0000
```

We use pslist to list the processes of a system. This shows the offset, process name, process ID, the parent process ID, number of threads, number of handles, and date/time when the process started and exited. There are 2 processes that standout, first reader_sl.exe and second is cmd.exe.

Pstree

```
C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility -f exam.vmem
pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds
Hnds Time
-------------------------------------------------- ------ ------ ------ -
----- ----
 0x819cc830:System                                      4      0     55
162 1970-01-01 00:00:00 UTC+0000
. 0x81945020:smss.exe                                 536      4      3
21 2011-10-10 17:03:56 UTC+0000
.. 0x816c6020:csrss.exe                               608    536     11
355 2011-10-10 17:03:58 UTC+0000
.. 0x813a9020:winlogon.exe                            632    536     24
533 2011-10-10 17:03:58 UTC+0000
... 0x816da020:services.exe                           676    632     16
261 2011-10-10 17:03:58 UTC+0000
.... 0x817757f0:svchost.exe                           916    676      9
217 2011-10-10 17:03:59 UTC+0000
.... 0x81772ca8:vmacthlp.exe                          832    676      1
24 2011-10-10 17:03:59 UTC+0000
.... 0x816c6da0:svchost.exe                           964    676     63
1058 2011-10-10 17:03:59 UTC+0000
..... 0x815c4da0:wscntfy.exe                         1920    964      1
27 2011-10-10 17:04:39 UTC+0000
..... 0x815e7be0:wuauclt.exe                          400    964      8
173 2011-10-10 17:04:46 UTC+0000
.... 0x8167e9d0:svchost.exe                           848    676     20
194 2011-10-10 17:03:59 UTC+0000
.... 0x81754990:VMwareService.e                      1444    676      3
145 2011-10-10 17:04:00 UTC+0000
.... 0x8136c5a0:alg.exe                              1616    676      7
99 2011-10-10 17:04:01 UTC+0000
.... 0x813aeda0:svchost.exe                          1148    676     12
187 2011-10-10 17:04:00 UTC+0000
.... 0x817937e0:spoolsv.exe                          1260    676     13
140 2011-10-10 17:04:00 UTC+0000
.... 0x815daca8:svchost.exe                          1020    676      5
58 2011-10-10 17:03:59 UTC+0000
... 0x813c4020:lsass.exe                              688    632     23
336 2011-10-10 17:03:58 UTC+0000
 0x813bcda0:explorer.exe                             1956   1884     18
322 2011-10-10 17:04:39 UTC+0000
. 0x8180b478:VMwareUser.exe                           192   1956      6
83 2011-10-10 17:04:41 UTC+0000
. 0x817a34b0:cmd.exe                                  544   1956      1
30 2011-10-10 17:06:42 UTC+0000
. 0x816d63d0:VMwareTray.exe                           184   1956      1
28 2011-10-10 17:04:41 UTC+0000
. 0x818233c8:reader_sl.exe                            228   1956      2
26 2011-10-10 17:04:41 UTC+0000
```

To view the process listing in tree form, use the pstree command. From this, we can see explorer.exe is starting cmd.exe and reader_sl.exe.

Cmdline

```
C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility -f exam.vmem cmdline
Volatility Foundation Volatility Framework 2.6
************************************************************************
System pid:      4
************************************************************************
smss.exe pid:    536
Command line : \SystemRoot\System32\smss.exe
************************************************************************
csrss.exe pid:    608
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,3072,512 Windows=On SubSystemType=Windows
ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off
MaxRequestThreads=16
************************************************************************
winlogon.exe pid:    632
Command line : winlogon.exe
************************************************************************
services.exe pid:    676
Command line : C:\WINDOWS\system32\services.exe
************************************************************************
lsass.exe pid:    688
Command line : C:\WINDOWS\system32\lsass.exe
************************************************************************
vmacthlp.exe pid:    832
Command line : "C:\Program Files\VMware\VMware Tools\vmacthlp.exe"
************************************************************************
svchost.exe pid:    848
Command line : C:\WINDOWS\system32\svchost -k DcomLaunch
************************************************************************
svchost.exe pid:    916
Command line : C:\WINDOWS\system32\svchost -k rpcss
************************************************************************
svchost.exe pid:    964
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs
************************************************************************
svchost.exe pid:   1020
Command line : C:\WINDOWS\system32\svchost.exe -k NetworkService
************************************************************************
svchost.exe pid:   1148
Command line : C:\WINDOWS\system32\svchost.exe -k LocalService
************************************************************************
spoolsv.exe pid:   1260
Command line : C:\WINDOWS\system32\spoolsv.exe
************************************************************************
VMwareService.e pid:   1444
Command line : "C:\Program Files\VMware\VMware Tools\VMwareService.exe"
************************************************************************
alg.exe pid:   1616
Command line : C:\WINDOWS\System32\alg.exe
************************************************************************
wscntfy.exe pid:   1920
```

```
Command line : C:\WINDOWS\system32\wscntfy.exe
************************************************************************
explorer.exe pid:   1956
Command line : C:\WINDOWS\Explorer.EXE
************************************************************************
VMwareTray.exe pid:    184
Command line : "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
************************************************************************
VMwareUser.exe pid:    192
Command line : "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
************************************************************************
reader_sl.exe pid:    228
Command line : "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
************************************************************************
wuauclt.exe pid:    400
Command line : "C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer
Local\[3c4]SUSDSf6f1f89b8c664547b701fa0a7f1b4cf6
************************************************************************
cmd.exe pid:    544
Command line : "C:\WINDOWS\system32\cmd.exe"

C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility -f exam.vmem
cmdline -p 1956
Volatility Foundation Volatility Framework 2.6
************************************************************************
explorer.exe pid:   1956
Command line : C:\WINDOWS\Explorer.EXE
```

Navigate your computer's file system along with base-level tasks such as create, copy, rename, and delete: Move around your directory structure: cd Create directories: mkdir Create files (and modify their metadata): touch Copy files

Connscan

```
C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility -f exam.vmem
connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address
             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x01a25a50 0.0.0.0:1026              172.16.98.1:6666          1956

C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility -f exam.vmem
procdump -p 1956 --dump.dir .
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

volatility: error: no such option: --dump.dir

C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility -f exam.vmem
procdump -p 1956 --dump-dir .
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x813bcda0 0x01000000 explorer.exe         OK: executable.1956.exe
```

```
C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility -f exam.vmem
memdump connscan --dump-dir .
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing System [     4] to 4.dmp
************************************************************************
Writing smss.exe [   536] to 536.dmp
************************************************************************
Writing csrss.exe [   608] to 608.dmp
************************************************************************
Writing winlogon.exe [   632] to 632.dmp
************************************************************************
Writing services.exe [   676] to 676.dmp
************************************************************************
Writing lsass.exe [   688] to 688.dmp
************************************************************************
Writing vmacthlp.exe [   832] to 832.dmp
************************************************************************
Writing svchost.exe [   848] to 848.dmp
************************************************************************
Writing svchost.exe [   916] to 916.dmp
************************************************************************
Writing svchost.exe [   964] to 964.dmp
************************************************************************
Writing svchost.exe [  1020] to 1020.dmp
************************************************************************
Writing svchost.exe [  1148] to 1148.dmp
************************************************************************
Writing spoolsv.exe [  1260] to 1260.dmp
************************************************************************
Writing VMwareService.e [  1444] to 1444.dmp
************************************************************************
Writing alg.exe [  1616] to 1616.dmp
************************************************************************
Writing wscntfy.exe [  1920] to 1920.dmp
************************************************************************
Writing explorer.exe [  1956] to 1956.dmp
************************************************************************
Writing VMwareTray.exe [   184] to 184.dmp
************************************************************************
Writing VMwareUser.exe [   192] to 192.dmp
************************************************************************
Writing reader_sl.exe [   228] to 228.dmp
************************************************************************
Writing wuauclt.exe [   400] to 400.dmp
************************************************************************
Writing cmd.exe [   544] to 544.dmp
```

To display a list of connections that have been terminated, the connscan command is used.

Malware

```
C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility -f exam.vmem
svcscan | find "malware"
Volatility Foundation Volatility Framework 2.6
Service Name: malware
Display Name: malware2
```

```
Binary Path: \Driver\malware
```

For finding malware we need this command

Dlllist

```
C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility -f exam.vmem
dlllist -p 544
Volatility Foundation Volatility Framework 2.6
************************************************************************
cmd.exe pid:    544
Command line : "C:\WINDOWS\system32\cmd.exe"
Service Pack 2

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x4ad00000    0x61000     0xffff C:\WINDOWS\system32\cmd.exe
0x7c900000    0xb0000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf4000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77c10000    0x58000     0xffff C:\WINDOWS\system32\msvcrt.dll
0x77d40000    0x90000     0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000    0x46000     0xffff C:\WINDOWS\system32\GDI32.dll
0x5cb70000    0x26000        0x1 C:\WINDOWS\system32\ShimEng.dll
0x6f880000   0x1ca000        0x1 C:\WINDOWS\AppPatch\AcGenral.DLL
0x77dd0000    0x9b000       0x17 C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x91000        0xb C:\WINDOWS\system32\RPCRT4.dll
0x76b40000    0x2d000        0x2 C:\WINDOWS\system32\WINMM.dll
0x774e0000   0x13c000        0x2 C:\WINDOWS\system32\ole32.dll
0x77120000    0x8c000        0x1 C:\WINDOWS\system32\OLEAUT32.dll
0x77be0000    0x15000        0x1 C:\WINDOWS\system32\MSACM32.dll
0x77c00000     0x8000        0x3 C:\WINDOWS\system32\VERSION.dll
0x7c9c0000   0x814000        0x1 C:\WINDOWS\system32\SHELL32.dll
0x77f60000    0x76000        0x3 C:\WINDOWS\system32\SHLWAPI.dll
0x769c0000    0xb3000        0x1 C:\WINDOWS\system32\USERENV.dll
0x5ad70000    0x38000        0x1 C:\WINDOWS\system32\UxTheme.dll
0x10000000    0x59000        0x1 C:\WINDOWS\system32\mfc42ul.dll
0x71ab0000    0x17000        0x2 C:\WINDOWS\system32\WS2_32.dll
0x71aa0000     0x8000        0x1 C:\WINDOWS\system32\WS2HELP.dll
0x71f60000     0x8000        0x1 C:\WINDOWS\system32\snmpapi.dll
0x773d0000   0x102000        0x1
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84f1ff9\comctl32.dll
0x5d090000    0x97000        0x1 C:\WINDOWS\system32\comctl32.dll
0x77b40000    0x22000        0x1 C:\WINDOWS\system32\Apphelp.dll
```

DLLlist helps analysts determine if a suspect process has accessed specific DLL files during its execution.

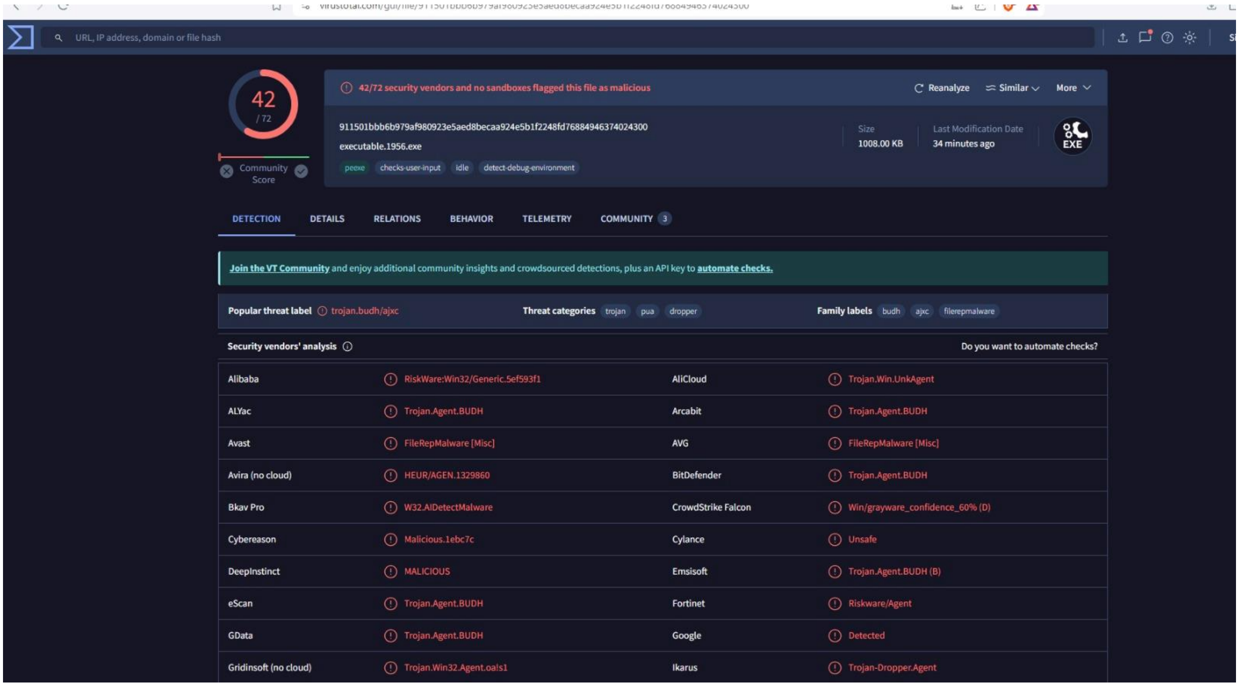
Memdump

```
C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>volatility -f exam.vmem
memdump -p 544 --dump-dir
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

volatility: error: --dump-dir option requires an argument
```

C:\Users\IIITKOTTAYAM\Desktop\volatility_2.6>

Virustotal



42/72 security vendors and no sandboxes flagged this file as malicious

911501bbb6b979af980923e5aed8becaa924e5b1f2248fd76884946374024300

executable.1956.exe

peexe checks-user-input idle detect-debug-environment

Size 1008.00 KB

Last Modification Date 34 minutes ago

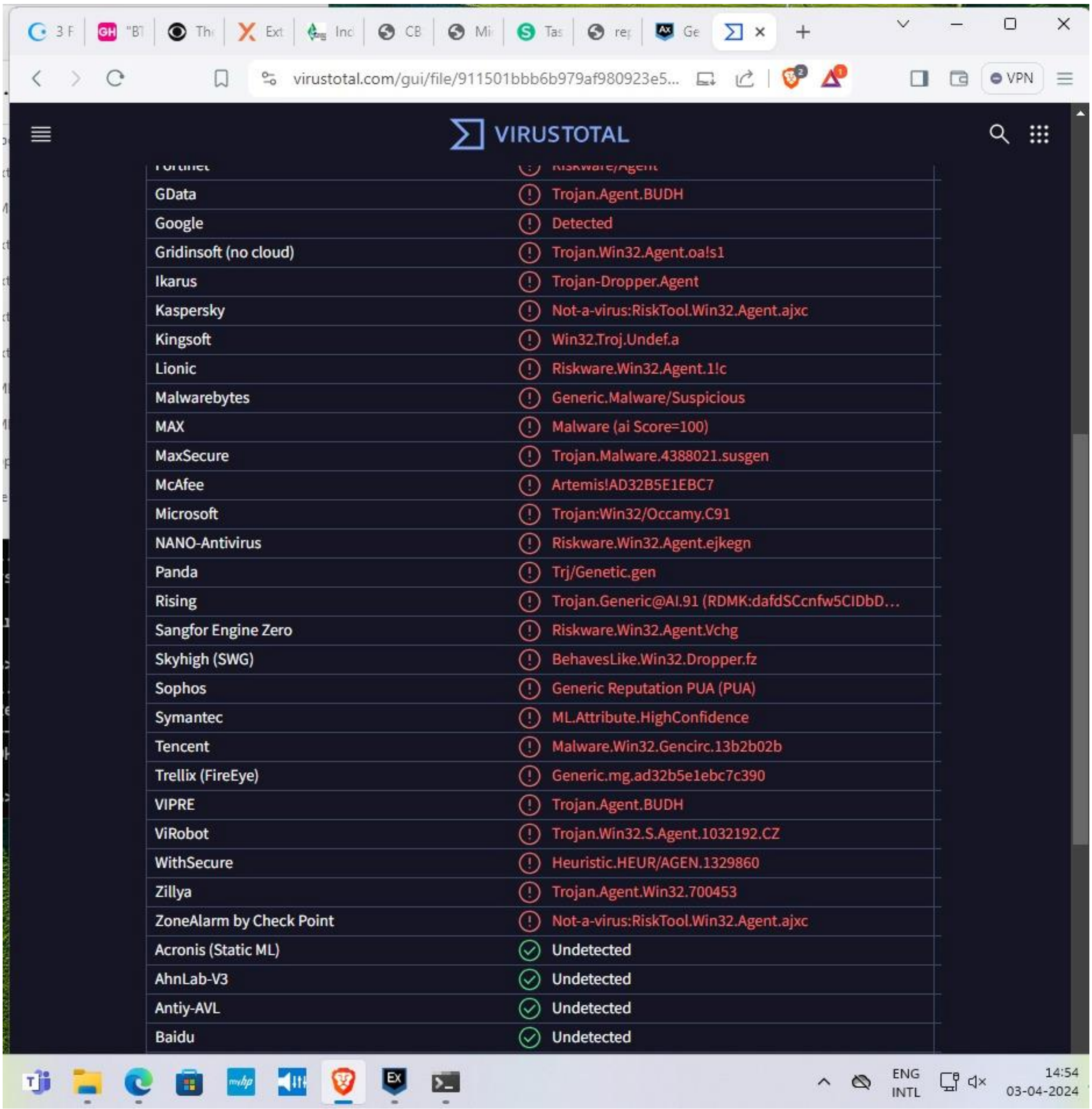
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.budh/ajxc Threat categories trojan pua dropper Family labels budh ajxc filerepmalware

Security vendors' analysis

Do you want to automate checks?

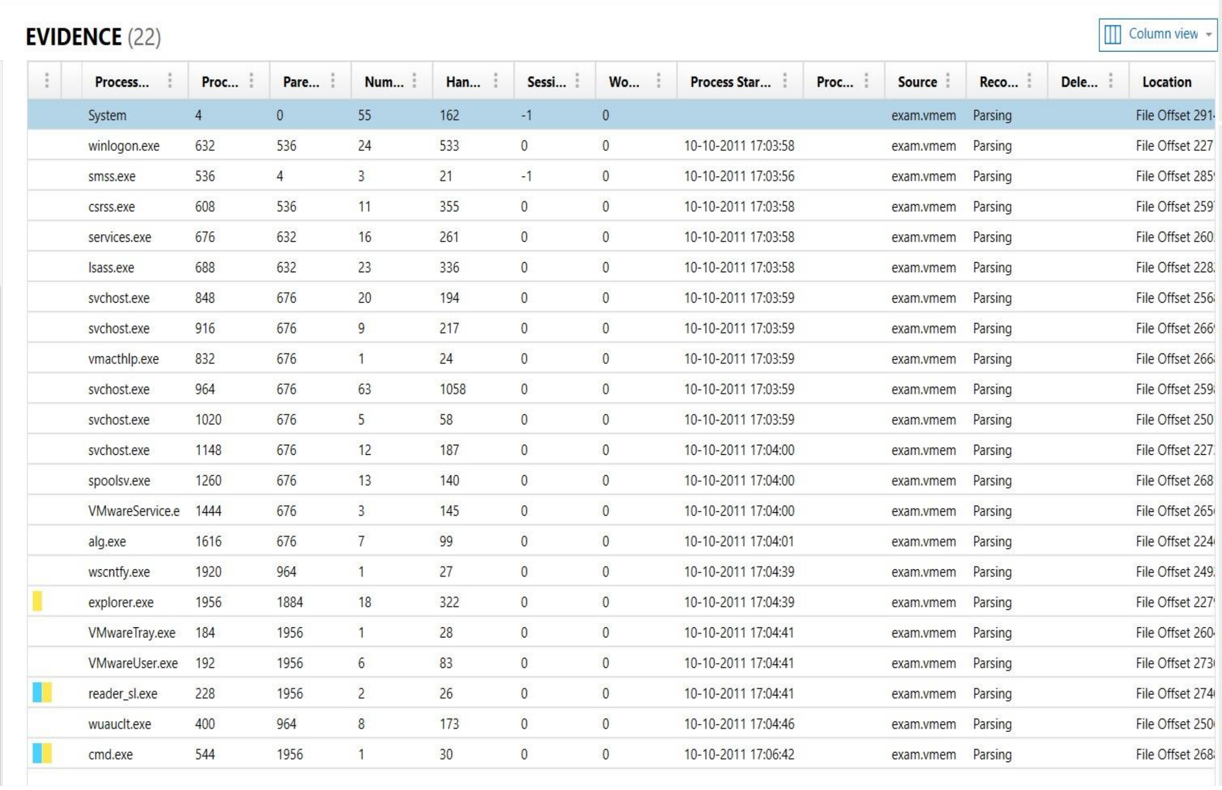
Alibaba	RiskWare:Win32/Generic.5ef593f1	AliCloud	Trojan.Win.UnkAgent
ALYac	Trojan.Agent.BUDH	Arcabit	Trojan.Agent.BUDH
Avast	FileRepMalware [Misc]	AVG	FileRepMalware [Misc]
Avira (no cloud)	HEUR/AGEN.1329860	BitDefender	Trojan.Agent.BUDH
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/grayware_confidence_60% (D)
Cybereason	Malicious.1ebc7c	Cylance	Unsafe
DeepInstinct	MALICIOUS	Emsisoft	Trojan.Agent.BUDH (B)
eScan	Trojan.Agent.BUDH	Fortinet	Riskware/Agent
GData	Trojan.Agent.BUDH	Google	Detected
Gridinsoft (no cloud)	Trojan.Win32.Agent.oa!s1	Ikarus	Trojan-Dropper.Agent



Fortinet	!	Riskware/Agent
GData	!	Trojan.Agent.BUDH
Google	!	Detected
Gridinsoft (no cloud)	!	Trojan.Win32.Agent.oa!s1
Ikarus	!	Trojan-Dropper.Agent
Kaspersky	!	Not-a-virus:RiskTool.Win32.Agent.ajxc
Kingsoft	!	Win32.Troj.Undef.a
Lionic	!	Riskware.Win32.Agent.1!c
Malwarebytes	!	Generic.Malware/Suspicious
MAX	!	Malware (ai Score=100)
MaxSecure	!	Trojan.Malware.4388021.susgen
McAfee	!	Artemis!AD32B5E1EBC7
Microsoft	!	Trojan:Win32/Occamy.C91
NANO-Antivirus	!	Riskware.Win32.Agent.ejkegn
Panda	!	Trj/Genetic.gen
Rising	!	Trojan.Generic@AI.91 (RDMK:dafdSCcnfw5CIDbD...
Sangfor Engine Zero	!	Riskware.Win32.Agent.Vchg
Skyhigh (SWG)	!	BehavesLike.Win32.Dropper.fz
Sophos	!	Generic Reputation PUA (PUA)
Symantec	!	ML.Attribute.HighConfidence
Tencent	!	Malware.Win32.Gencirc.13b2b02b
Trellix (FireEye)	!	Generic.mg.ad32b5e1ebc7c390
VIPRE	!	Trojan.Agent.BUDH
ViRobot	!	Trojan.Win32.S.Agent.1032192.CZ
WithSecure	!	Heuristic.HEUR/AGEN.1329860
Zillya	!	Trojan.Agent.Win32.700453
ZoneAlarm by Check Point	!	Not-a-virus:RiskTool.Win32.Agent.ajxc
Acronis (Static ML)	✓	Undetected
AhnLab-V3	✓	Undetected
Antiy-AVL	✓	Undetected
Baidu	✓	Undetected

Magnet axiom

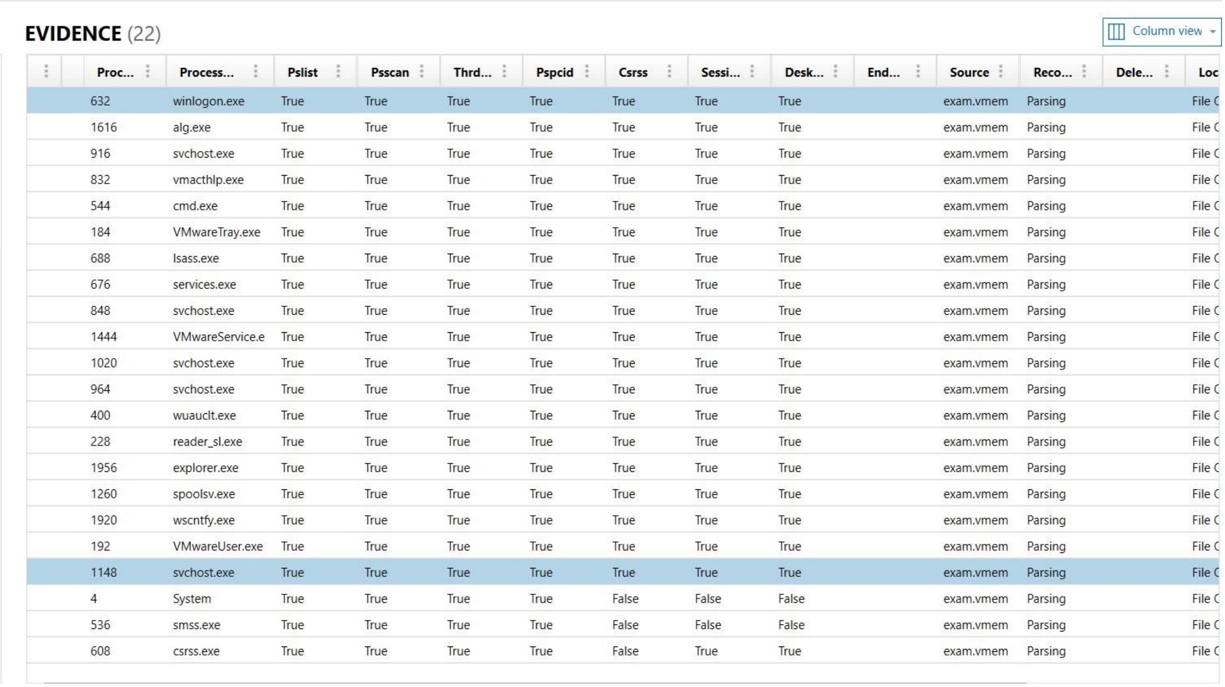
- **PSLIST**



EVIDENCE (22)

Column view

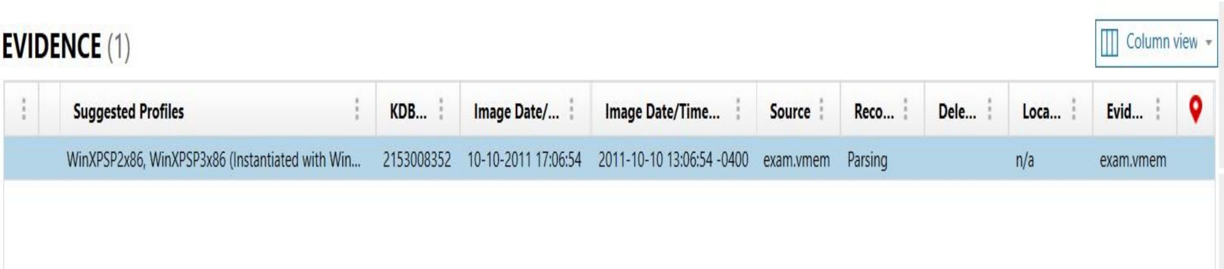
	Process...	Proc...	Pare...	Num...	Han...	Sessi...	Wo...	Process Star...	Proc...	Source	Reco...	Dele...	Location
	System	4	0	55	162	-1	0			exam.vmem	Parsing		File Offset 291
	winlogon.exe	632	536	24	533	0	0	10-10-2011 17:03:58		exam.vmem	Parsing		File Offset 227
	smss.exe	536	4	3	21	-1	0	10-10-2011 17:03:56		exam.vmem	Parsing		File Offset 285
	csrss.exe	608	536	11	355	0	0	10-10-2011 17:03:58		exam.vmem	Parsing		File Offset 259
	services.exe	676	632	16	261	0	0	10-10-2011 17:03:58		exam.vmem	Parsing		File Offset 260
	lsass.exe	688	632	23	336	0	0	10-10-2011 17:03:58		exam.vmem	Parsing		File Offset 228
	svchost.exe	848	676	20	194	0	0	10-10-2011 17:03:59		exam.vmem	Parsing		File Offset 256
	svchost.exe	916	676	9	217	0	0	10-10-2011 17:03:59		exam.vmem	Parsing		File Offset 266
	vmacthlp.exe	832	676	1	24	0	0	10-10-2011 17:03:59		exam.vmem	Parsing		File Offset 266
	svchost.exe	964	676	63	1058	0	0	10-10-2011 17:03:59		exam.vmem	Parsing		File Offset 259
	svchost.exe	1020	676	5	58	0	0	10-10-2011 17:03:59		exam.vmem	Parsing		File Offset 250
	svchost.exe	1148	676	12	187	0	0	10-10-2011 17:04:00		exam.vmem	Parsing		File Offset 227
	spoolsv.exe	1260	676	13	140	0	0	10-10-2011 17:04:00		exam.vmem	Parsing		File Offset 268
	VMwareService.e	1444	676	3	145	0	0	10-10-2011 17:04:00		exam.vmem	Parsing		File Offset 265
	alg.exe	1616	676	7	99	0	0	10-10-2011 17:04:01		exam.vmem	Parsing		File Offset 224
	wscntfy.exe	1920	964	1	27	0	0	10-10-2011 17:04:39		exam.vmem	Parsing		File Offset 249
🟨	explorer.exe	1956	1884	18	322	0	0	10-10-2011 17:04:39		exam.vmem	Parsing		File Offset 227
	VMwareTray.exe	184	1956	1	28	0	0	10-10-2011 17:04:41		exam.vmem	Parsing		File Offset 260
	VMwareUser.exe	192	1956	6	83	0	0	10-10-2011 17:04:41		exam.vmem	Parsing		File Offset 273
🟦🟨	reader_sl.exe	228	1956	2	26	0	0	10-10-2011 17:04:41		exam.vmem	Parsing		File Offset 274
	wuauclt.exe	400	964	8	173	0	0	10-10-2011 17:04:46		exam.vmem	Parsing		File Offset 250
🟦🟨	cmd.exe	544	1956	1	30	0	0	10-10-2011 17:06:42		exam.vmem	Parsing		File Offset 268



EVIDENCE (22)

Column view

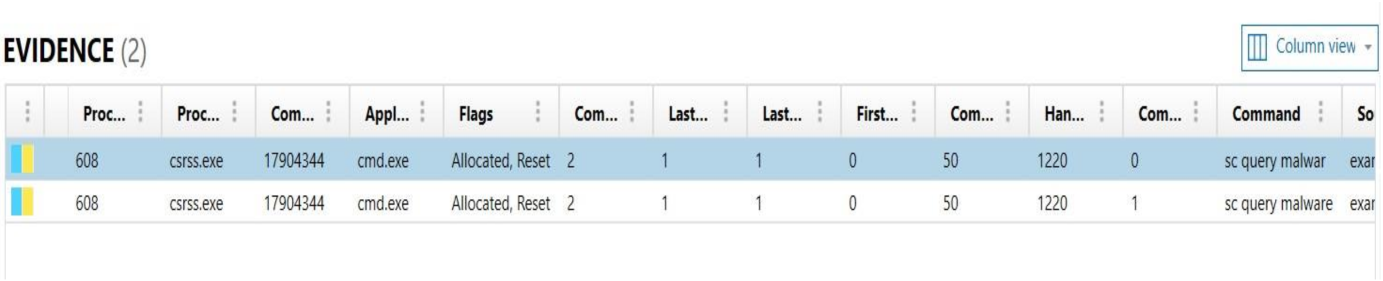
	Proc...	Process...	Pslist	Psscan	Thrd...	Pspcid	Csrss	Sessi...	Desk...	End...	Source	Reco...	Dele...	Loc
	632	winlogon.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	1616	alg.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	916	svchost.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	832	vmacthlp.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	544	cmd.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	184	VMwareTray.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	688	lsass.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	676	services.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	848	svchost.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	1444	VMwareService.e	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	1020	svchost.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	964	svchost.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	400	wuauclt.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	228	reader_sl.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	1956	explorer.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	1260	spoolsv.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	1920	wscntfy.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	192	VMwareUser.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	1148	svchost.exe	True	True	True	True	True	True	True		exam.vmem	Parsing		File C
	4	System	True	True	True	True	False	False	False		exam.vmem	Parsing		File C
	536	smss.exe	True	True	True	True	False	False	False		exam.vmem	Parsing		File C
	608	csrss.exe	True	True	True	True	False	True	True		exam.vmem	Parsing		File C



EVIDENCE (1)

	Suggested Profiles	KDB...	Image Date/...	Image Date/Time...	Source	Reco...	Dele...	Loca...	Evid...	📍
	WinXPSP2x86, WinXPSP3x86 (Instantiated with Win...	2153008352	10-10-2011 17:06:54	2011-10-10 13:06:54 -0400	exam.vmem	Parsing		n/a	exam.vmem	

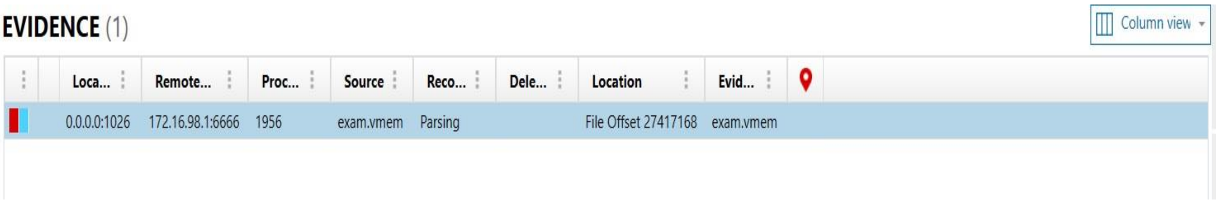
CMDSCAN



EVIDENCE (2)

	Proc...	Proc...	Com...	Appl...	Flags	Com...	Last...	Last...	First...	Com...	Han...	Com...	Command	So
🟦🟨	608	csrss.exe	17904344	cmd.exe	Allocated, Reset	2	1	1	0	50	1220	0	sc query malwar	exar
🟦🟨	608	csrss.exe	17904344	cmd.exe	Allocated, Reset	2	1	1	0	50	1220	1	sc query malware	exar

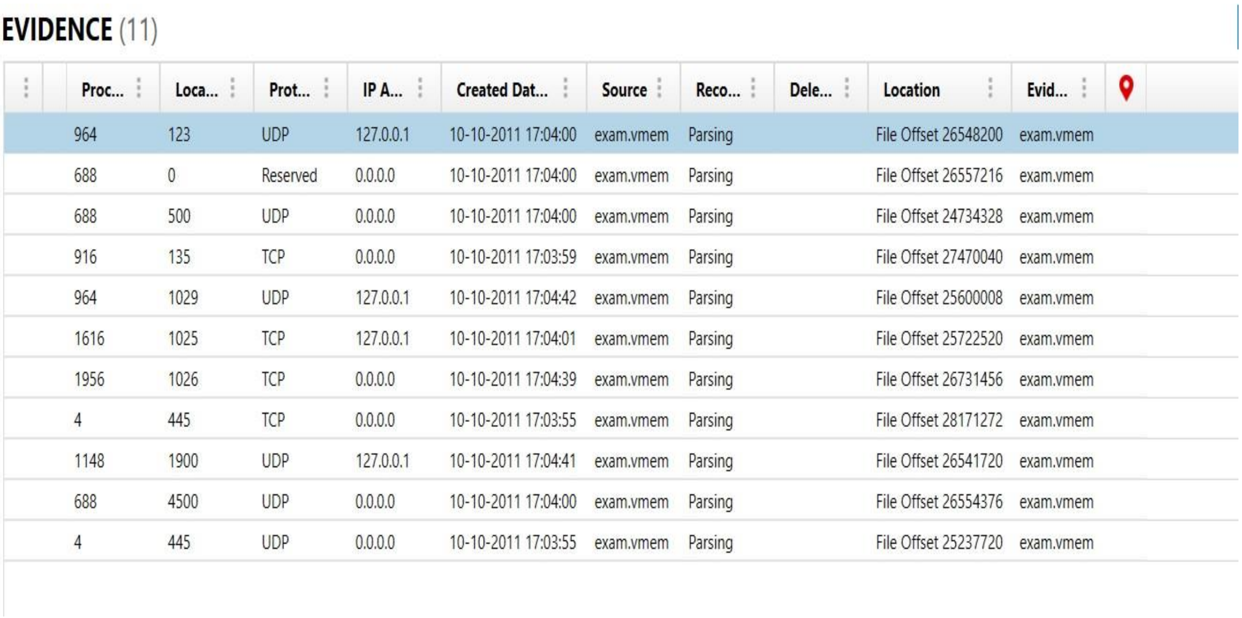
- ## CONNSCAN



EVIDENCE (1)

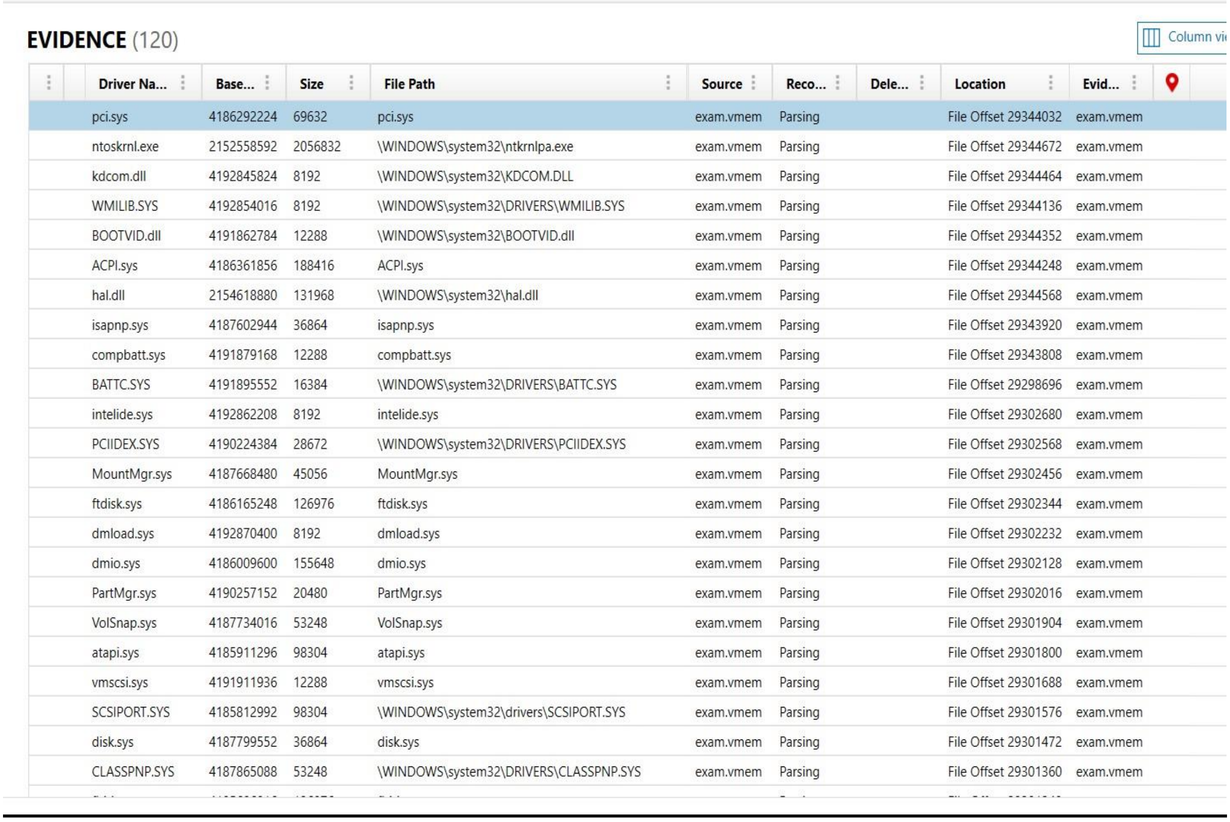
	Loca...	Remote...	Proc...	Source	Reco...	Dele...	Location	Evid...	📍
🟥🟦	0.0.0.0:1026	172.16.98.1:6666	1956	exam.vmem	Parsing		File Offset 27417168	exam.vmem	

Sockets



EVIDENCE (11)

	Proc...	Loca...	Prot...	IP A...	Created Dat...	Source	Reco...	Dele...	Location	Evid...	📍
	964	123	UDP	127.0.0.1	10-10-2011 17:04:00	exam.vmem	Parsing		File Offset 26548200	exam.vmem	
	688	0	Reserved	0.0.0.0	10-10-2011 17:04:00	exam.vmem	Parsing		File Offset 26557216	exam.vmem	
	688	500	UDP	0.0.0.0	10-10-2011 17:04:00	exam.vmem	Parsing		File Offset 24734328	exam.vmem	
	916	135	TCP	0.0.0.0	10-10-2011 17:03:59	exam.vmem	Parsing		File Offset 27470040	exam.vmem	
	964	1029	UDP	127.0.0.1	10-10-2011 17:04:42	exam.vmem	Parsing		File Offset 25600008	exam.vmem	
	1616	1025	TCP	127.0.0.1	10-10-2011 17:04:01	exam.vmem	Parsing		File Offset 25722520	exam.vmem	
	1956	1026	TCP	0.0.0.0	10-10-2011 17:04:39	exam.vmem	Parsing		File Offset 26731456	exam.vmem	
	4	445	TCP	0.0.0.0	10-10-2011 17:03:55	exam.vmem	Parsing		File Offset 28171272	exam.vmem	
	1148	1900	UDP	127.0.0.1	10-10-2011 17:04:41	exam.vmem	Parsing		File Offset 26541720	exam.vmem	
	688	4500	UDP	0.0.0.0	10-10-2011 17:04:00	exam.vmem	Parsing		File Offset 26554376	exam.vmem	
	4	445	UDP	0.0.0.0	10-10-2011 17:03:55	exam.vmem	Parsing		File Offset 25237720	exam.vmem	

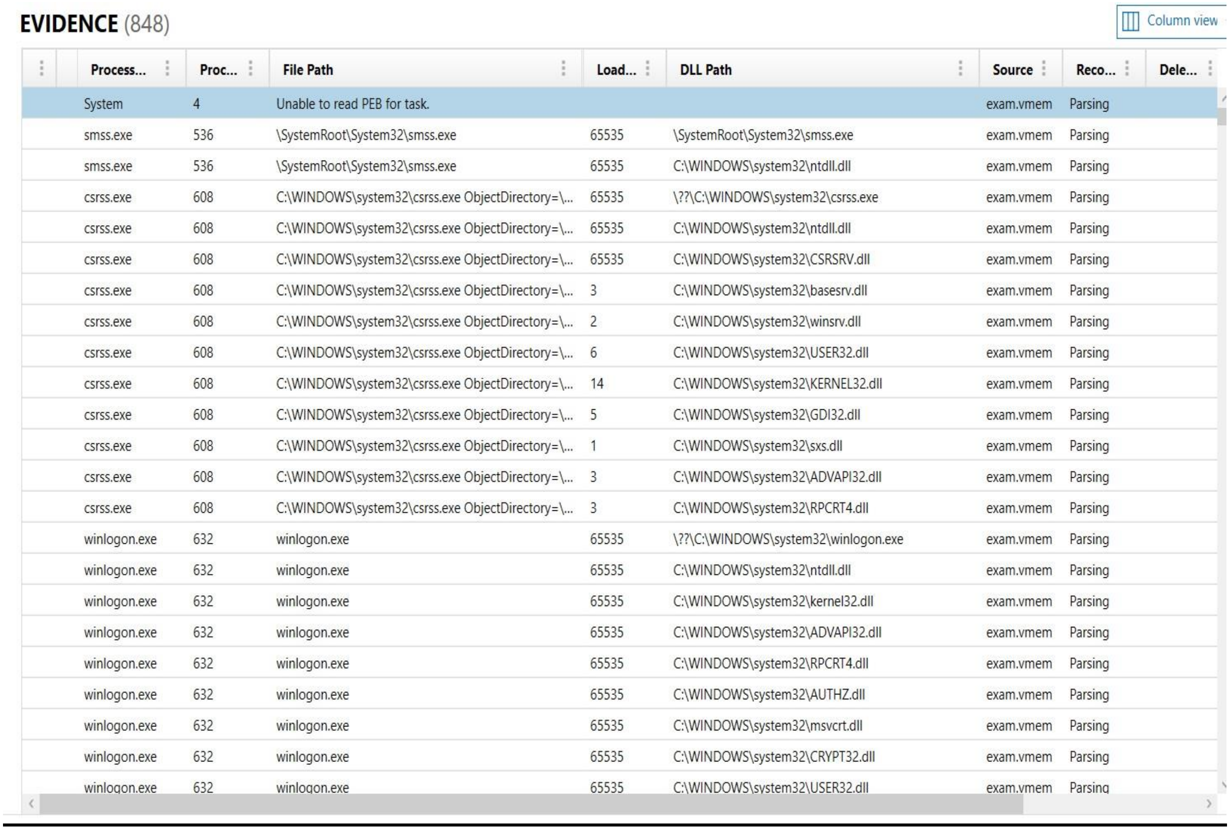


EVIDENCE (120)

Column vi

Driver Na...	Base...	Size	File Path	Source	Reco...	Dele...	Location	Evid...
pci.sys	4186292224	69632	pci.sys	exam.vmem	Parsing		File Offset 29344032	exam.vmem
ntoskrnl.exe	2152558592	2056832	\WINDOWS\system32\ntkrnlpa.exe	exam.vmem	Parsing		File Offset 29344672	exam.vmem
kdcom.dll	4192845824	8192	\WINDOWS\system32\KDCOM.DLL	exam.vmem	Parsing		File Offset 29344464	exam.vmem
WMILIB.SYS	4192854016	8192	\WINDOWS\system32\DRIVERS\WMILIB.SYS	exam.vmem	Parsing		File Offset 29344136	exam.vmem
BOOTVID.dll	4191862784	12288	\WINDOWS\system32\BOOTVID.dll	exam.vmem	Parsing		File Offset 29344352	exam.vmem
ACPI.sys	4186361856	188416	ACPI.sys	exam.vmem	Parsing		File Offset 29344248	exam.vmem
hal.dll	2154618880	131968	\WINDOWS\system32\hal.dll	exam.vmem	Parsing		File Offset 29344568	exam.vmem
isapnp.sys	4187602944	36864	isapnp.sys	exam.vmem	Parsing		File Offset 29343920	exam.vmem
compbatt.sys	4191879168	12288	compbatt.sys	exam.vmem	Parsing		File Offset 29343808	exam.vmem
BATTC.SYS	4191895552	16384	\WINDOWS\system32\DRIVERS\BATTC.SYS	exam.vmem	Parsing		File Offset 29298696	exam.vmem
intelide.sys	4192862208	8192	intelide.sys	exam.vmem	Parsing		File Offset 29302680	exam.vmem
PCIIDEX.SYS	4190224384	28672	\WINDOWS\system32\DRIVERS\PCIIDEX.SYS	exam.vmem	Parsing		File Offset 29302568	exam.vmem
MountMgr.sys	4187668480	45056	MountMgr.sys	exam.vmem	Parsing		File Offset 29302456	exam.vmem
ftdisk.sys	4186165248	126976	ftdisk.sys	exam.vmem	Parsing		File Offset 29302344	exam.vmem
dmload.sys	4192870400	8192	dmload.sys	exam.vmem	Parsing		File Offset 29302232	exam.vmem
dmio.sys	4186009600	155648	dmio.sys	exam.vmem	Parsing		File Offset 29302128	exam.vmem
PartMgr.sys	4190257152	20480	PartMgr.sys	exam.vmem	Parsing		File Offset 29302016	exam.vmem
VolSnap.sys	4187734016	53248	VolSnap.sys	exam.vmem	Parsing		File Offset 29301904	exam.vmem
atapi.sys	4185911296	98304	atapi.sys	exam.vmem	Parsing		File Offset 29301800	exam.vmem
vmscsi.sys	4191911936	12288	vmscsi.sys	exam.vmem	Parsing		File Offset 29301688	exam.vmem
SCSIPORT.SYS	4185812992	98304	\WINDOWS\system32\drivers\SCSIPORT.SYS	exam.vmem	Parsing		File Offset 29301576	exam.vmem
disk.sys	4187799552	36864	disk.sys	exam.vmem	Parsing		File Offset 29301472	exam.vmem
CLASSPNP.SYS	4187865088	53248	\WINDOWS\system32\DRIVERS\CLASSPNP.SYS	exam.vmem	Parsing		File Offset 29301360	exam.vmem

- **DLLLIST**



EVIDENCE (848)

Column view

Process...	Proc...	File Path	Load...	DLL Path	Source	Reco...	Dele...
System	4	Unable to read PEB for task.			exam.vmem	Parsing	
smss.exe	536	\SystemRoot\System32\smss.exe	65535	\SystemRoot\System32\smss.exe	exam.vmem	Parsing	
smss.exe	536	\SystemRoot\System32\smss.exe	65535	C:\WINDOWS\system32\ntdll.dll	exam.vmem	Parsing	
csrss.exe	608	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\...	65535	\??\C:\WINDOWS\system32\csrss.exe	exam.vmem	Parsing	
csrss.exe	608	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\...	65535	C:\WINDOWS\system32\ntdll.dll	exam.vmem	Parsing	
csrss.exe	608	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\...	65535	C:\WINDOWS\system32\CSRSRV.dll	exam.vmem	Parsing	
csrss.exe	608	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\...	3	C:\WINDOWS\system32\basesrv.dll	exam.vmem	Parsing	
csrss.exe	608	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\...	2	C:\WINDOWS\system32\winsrv.dll	exam.vmem	Parsing	
csrss.exe	608	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\...	6	C:\WINDOWS\system32\USER32.dll	exam.vmem	Parsing	
csrss.exe	608	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\...	14	C:\WINDOWS\system32\KERNEL32.dll	exam.vmem	Parsing	
csrss.exe	608	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\...	5	C:\WINDOWS\system32\GDI32.dll	exam.vmem	Parsing	
csrss.exe	608	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\...	1	C:\WINDOWS\system32\sxs.dll	exam.vmem	Parsing	
csrss.exe	608	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\...	3	C:\WINDOWS\system32\ADVAPI32.dll	exam.vmem	Parsing	
csrss.exe	608	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\...	3	C:\WINDOWS\system32\RPCRT4.dll	exam.vmem	Parsing	
winlogon.exe	632	winlogon.exe	65535	\??\C:\WINDOWS\system32\winlogon.exe	exam.vmem	Parsing	
winlogon.exe	632	winlogon.exe	65535	C:\WINDOWS\system32\ntdll.dll	exam.vmem	Parsing	
winlogon.exe	632	winlogon.exe	65535	C:\WINDOWS\system32\kernel32.dll	exam.vmem	Parsing	
winlogon.exe	632	winlogon.exe	65535	C:\WINDOWS\system32\ADVAPI32.dll	exam.vmem	Parsing	
winlogon.exe	632	winlogon.exe	65535	C:\WINDOWS\system32\RPCRT4.dll	exam.vmem	Parsing	
winlogon.exe	632	winlogon.exe	65535	C:\WINDOWS\system32\AUTHZ.dll	exam.vmem	Parsing	
winlogon.exe	632	winlogon.exe	65535	C:\WINDOWS\system32\msvcrt.dll	exam.vmem	Parsing	
winlogon.exe	632	winlogon.exe	65535	C:\WINDOWS\system32\CRYPT32.dll	exam.vmem	Parsing	
winlogon.exe	632	winlogon.exe	65535	C:\WINDOWS\system32\USER32.dll	exam.vmem	Parsing	

A summary of the overall findings and their implications for the case. This section may also include expert opinions or recommendations based on the evidence uncovered.