Forensic Analysis and Incident Response with Volatility

Jared Smith
Oak Ridge National Laboratory

You've been compromised...

Your logs are inconclusive

Your dashboards are inconsistent

There are too many alerts to digest

What should you do?

Call your Incident Response team! (or contract one)

And harness the the power of *memory forensics*

Hi, I'm Jared

- Security Researcher and Project Lead at **Oak Ridge National Laboratory**
- CS PhD student at VolSec, the **University of Tennessee Computer Security Lab**
- Former Software Security Engineer/ Pentester at Cisco
- Board Member on the Knoxville Technology Council

Memory Forensics

The art of examining a host's memory (RAM) for anomalous data, often revealing indicators of compromise

Why not X instead?

- Capturing system logs and parsing out relevant info can miss key insights
- Endpoint security agents typically don't capture all system state and can also be resource-intensive
- Manual inspection by actual humans is often needed for complex incidents
- AI doesn't solve everything

State of the art tools (and free!)

- Autopsy and Sleuth Kit - https://www.sleuthkit.org/autopsy/
- **Volatility** - http://www.volatilityfoundation.org/
- Rekall - http://www.rekall-forensic.com/
- GRR - https://github.com/google/grr

Volatility

"Volatile memory extraction utility framework"

Dig into the heart of your machines

- Takes a memory (RAM) dump from every major modern OS as input
- Extracts system state
  - Includes process info, registry info (W), DLLs (W), networking info, handles (W), logs, files, syscalls, process trees, open ttys, etc.

Architecture

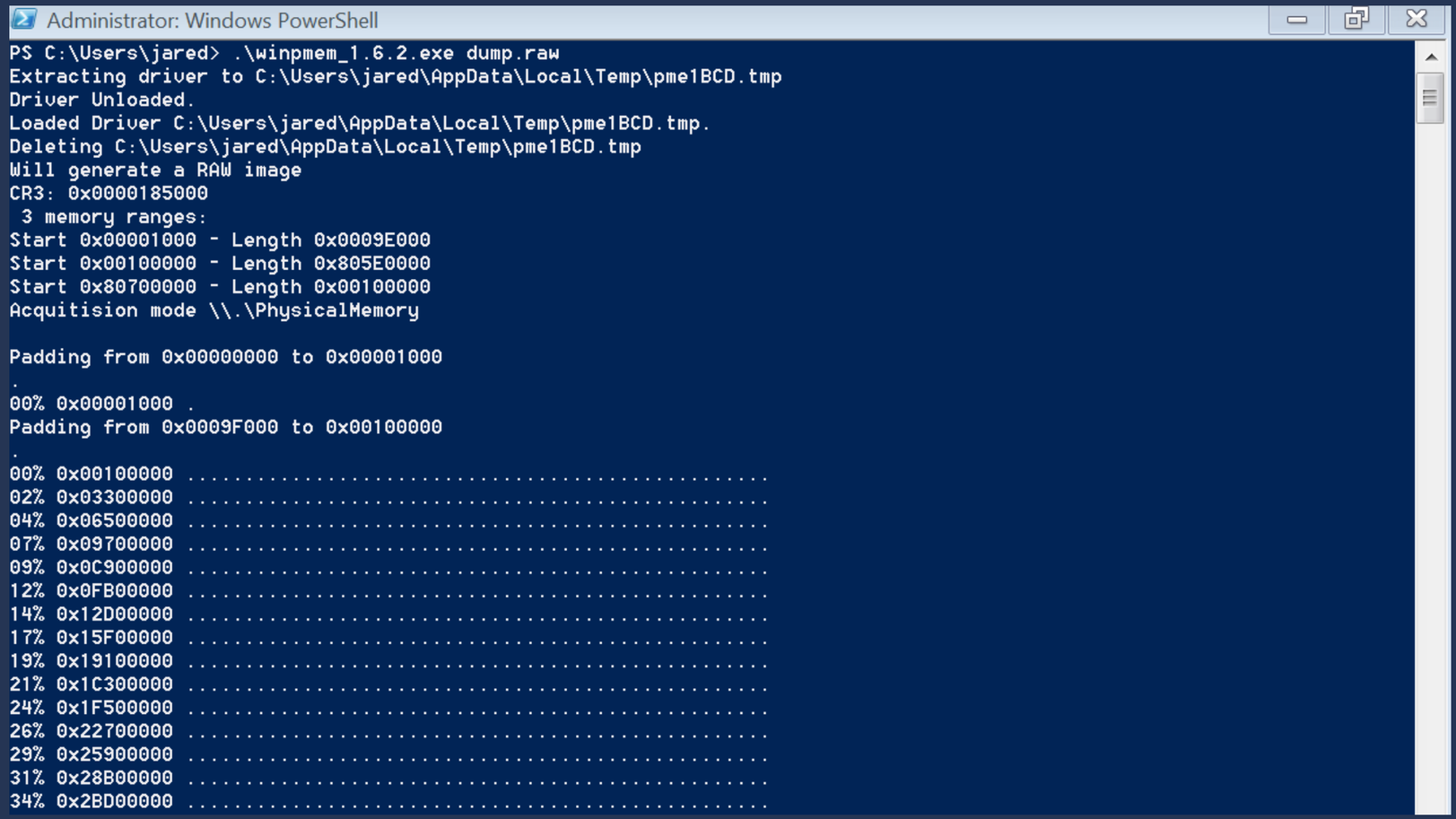
- Written in Python, cross-platform
- Represents memory images as layers of objects
  - Allows us to analyze VM images just like a regular host image
- Plugin-based architecture for core host analysis

Dependencies

- Python 2.7.x
- Imaging software
  - Pmem Acquisition Suite (http://www.rekall-forensic.com/docs/Tools/index.html)
- Download: **http://www.volatilityfoundation.org/releases**
- Source Code: **https://github.com/volatilityfoundation/volatility**

So, how do I use this?

First, get a memory image from a target machine



You now have a memory image named *dump.raw*

```
~/demo >>> ./volatility imageinfo -f dump.raw
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/Users/jared/demo/dump.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x8296ec28L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x8296fc00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2017-01-01 23:01:21 UTC+0000
     Image local date and time : 2017-01-01 18:01:21 -0500
```

Scanning the kernel debug tables reveals the OS

```
~/demo >>> ./volatility kdbgscan -f dump.raw
Volatility Foundation Volatility Framework 2.6
**************************************************
Instantiating KDBG using: /Users/jared/demo/dump.raw WinXPSP2x86 (5.1.0 32bit)
Offset (P)                    : 0x296ec28
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP1x86_23418
Version64                     : 0x296ec00 (Major: 15, Minor: 7601)
PsActiveProcessHead           : 0x82986f18
PsLoadedModuleList            : 0x8298e850
KernelBase                    : 0x82844000

**************************************************
Instantiating KDBG using: /Users/jared/demo/dump.raw WinXPSP2x86 (5.1.0 32bit)
Offset (P)                    : 0x296ec28
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP1x86
Version64                     : 0x296ec00 (Major: 15, Minor: 7601)
PsActiveProcessHead           : 0x82986f18
PsLoadedModuleList            : 0x8298e850
KernelBase                    : 0x82844000

**************************************************
Instantiating KDBG using: /Users/jared/demo/dump.raw WinXPSP2x86 (5.1.0 32bit)
Offset (P)                    : 0x296ec28
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP0x86
Version64                     : 0x296ec00 (Major: 15, Minor: 7601)
PsActiveProcessHead           : 0x82986f18
PsLoadedModuleList            : 0x8298e850
KernelBase                    : 0x82844000
```

List process info

```
~/demo >>> ./volatility pslist --profile Win7SP1x86 -f dump.raw
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x848548a8 System                    4      0     86      494 ------      0 2016-11-05 17:08:43 UTC+0000
0x85eaad40 smss.exe                276      4      2       29 ------      0 2016-11-05 17:08:43 UTC+0000
0x85cf3cd8 csrss.exe               360    344      9      550      0      0 2016-11-05 17:08:44 UTC+0000
0x848e2b30 wininit.exe             412    344      3       74      0      0 2016-11-05 17:08:44 UTC+0000
0x86a85378 services.exe            512    412      9      202      0      0 2016-11-05 17:08:44 UTC+0000
0x86a9e5a0 lsass.exe               520    412      8      550      0      0 2016-11-05 17:08:44 UTC+0000
0x86aa06f8 lsm.exe                 528    412     10      144      0      0 2016-11-05 17:08:44 UTC+0000
0x86b0cd40 svchost.exe             636    512     13      361      0      0 2016-11-05 17:08:45 UTC+0000
0x85ba6d40 vmacthlp.exe            700    512      4       63      0      0 2016-11-05 17:08:45 UTC+0000
0x85bc61c0 svchost.exe             732    512      8      266      0      0 2016-11-05 17:08:45 UTC+0000
```

```
0x84da2030 conhost.exe          3588   3548      1       33      2      0 2017-01-01 22:59:42 UTC+0000
0x84fdca30 vmtoolsd.exe         1192   3048      7      198      2      0 2017-01-01 22:59:43 UTC+0000
0x84e2f9c8 WMIADAP.exe          1480    948      5       87      0      0 2017-01-01 23:00:00 UTC+0000
0x84f21d18 WmiPrvSE.exe         2672    636      7      121      0      0 2017-01-01 23:00:00 UTC+0000
0x86e1c338 powershell.exe       3664   3048      8      375      2      0 2017-01-01 23:01:05 UTC+0000
0x84db35d0 conhost.exe          1532   3548      2       53      2      0 2017-01-01 23:01:05 UTC+0000
0x84e06030 winpmem_1.6.2.       2972   3664      1       26      2      0 2017-01-01 23:01:21 UTC+0000
```

Explore process hierarchies

```
~/demo >>> ./volatility pstree --profile Win7SP1x86 -f dump.raw
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x848e2b30:wininit.exe                               412    344      3     74 2016-11-05 17:08:44 UTC+0000
. 0x86a85378:services.exe                             512    412      9    202 2016-11-05 17:08:44 UTC+0000
.. 0x86ded2f8:TPAutoConnSvc.                         1664    512     11    142 2016-11-05 17:08:46 UTC+0000
... 0x874178c8:TPAutoConnect.                        2352   1664      4    128 2017-01-01 22:59:42 UTC+0000
.. 0x860d5030:svchost.exe                            2192    512     10    138 2016-11-05 17:10:47 UTC+0000
.. 0x86ca5a58:svchost.exe                            1172    512     21    430 2016-11-05 17:08:45 UTC+0000
.. 0x86b23820:svchost.exe                             800    512     21    456 2016-11-05 17:08:45 UTC+0000
... 0x84e7d3e8:audiodg.exe                           3892    800      7    135 2016-11-05 19:52:59 UTC+0000
.. 0x86c852d0:svchost.exe                            1064    512     16    340 2016-11-05 17:08:45 UTC+0000
.. 0x86d1e440:svchost.exe                            1332    512     21    313 2016-11-05 17:08:46 UTC+0000
.. 0x85dc24d0:svchost.exe                             948    512     45   1172 2016-11-05 17:08:45 UTC+0000
```

```
 0x84b6d240:explorer.exe                3048   1624     29    734 2017-01-01 22:59:42 UTC+0000
. 0x86e1c338:powershell.exe             3664   3048      8    375 2017-01-01 23:01:05 UTC+0000
.. 0x84e06030:winpmem_1.6.2.            2972   3664      1     26 2017-01-01 23:01:21 UTC+0000
. 0x84fdca30:vmtoolsd.exe               1192   3048      7    198 2017-01-01 22:59:43 UTC+0000
```

Parse the Windows registry

```
~/demo >>> ./volatility hivelist --profile Win7SP1x86 -f dump.raw
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0x8e1483e8 0x2a0523e8 \Device\HarddiskVolume1\Boot\BCD
0x8e1bf490 0x1ff10490 \SystemRoot\System32\Config\SOFTWARE
0x912126d0 0x2a4ab6d0 \SystemRoot\System32\Config\SECURITY
0x9664b008 0x1ddf9008 \??\C:\System Volume Information\Syscache.hve
0xa2536008 0x0cfcf008 \??\C:\Users\jared\ntuser.dat
0x898104c8 0x2d94e4c8 [no name]
0x8981a248 0x2db9a248 \REGISTRY\MACHINE\SYSTEM
0x89844008 0x2e5c6008 \REGISTRY\MACHINE\HARDWARE
0x898bd4f0 0x2706a4f0 \SystemRoot\System32\Config\DEFAULT
0x8a6235d8 0x253ab5d8 \SystemRoot\System32\Config\SAM
0x8d78b620 0x28523620 \??\C:\Users\jared\AppData\Local\Microsoft\Windows\UsrClass.dat
0x8de3a598 0x0008b598 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8debc008 0x242d8008 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
```

Dump out user hashes

```
~/demo >>> ./volatility hashdump -y 0x8981a248 -s 0x8a6235d8 --profile Win7SP1x86 -f dump.raw
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
jared:1000:aad3b435b51404eeaad3b435b51404ee:f39934a2710a469b3c63ce1487794514:::
```

Print out specific registry keys

```
~/demo >>> ./volatility printkey -K "Microsoft\Security Center\Svc" --profile Win7SP1x86 -f dump.raw
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \SystemRoot\System32\Config\SOFTWARE
Key name: Svc (S)
Last updated: 2016-11-05 17:10:48 UTC+0000

Subkeys:
  (V) Vol

Values:
REG_QWORD     VistaSp1        : (S) 128920209537502489
REG_DWORD     AntiVirusOverride : (S) 0
REG_DWORD     AntiSpywareOverride : (S) 0
REG_DWORD     FirewallOverride : (S) 0
```

Find recently executed commands

```
~/demo >>> ./volatility cmdscan --profile Win7SP1x86 -f dump.raw
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: conhost.exe Pid: 3588
CommandHistory: 0x3e0e28 Application: TPAutoConnect.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
**************************************************
CommandProcess: conhost.exe Pid: 1532
CommandHistory: 0x3d4c20 Application: powershell.exe Flags: Allocated, Reset
CommandCount: 3 LastAdded: 2 LastDisplayed: 2
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 @ 0x3ccc20: cd ~
Cmd #1 @ 0x3ccc38: clear
Cmd #2 @ 0x3cbb18: .\winpmem_1.6.2.exe dump.raw
```

Find open ttys and consoles

```
~/demo >>> ./volatility consoles --profile Win7SP1x86 -f dump.raw
Volatility Foundation Volatility Framework 2.6
**************************************************
ConsoleProcess: conhost.exe Pid: 3588
Console: 0x2481c0 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
Title: C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
AttachedProcess: TPAutoConnect. Pid: 2352 Handle: 0x5c
----
CommandHistory: 0x3e0e28 Application: TPAutoConnect.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
----
```

```
----
Screen 0x3d2918 X:80 Y:300
Dump:
ThinPrint AutoConnect component, Copyright (c) 1999-2013 Cortado AG, 8.8.776.1
************************************************
ConsoleProcess: conhost.exe Pid: 1532
Console: 0x2481c0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: Windows PowerShell
Title: Administrator: Windows PowerShell
AttachedProcess: winpmem_1.6.2. Pid: 2972 Handle: 0x54
AttachedProcess: powershell.exe Pid: 3664 Handle: 0x5c
----
CommandHistory: 0x3d5d50 Application: winpmem_1.6.2.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x54
----
CommandHistory: 0x3d4c20 Application: powershell.exe Flags: Allocated, Reset
CommandCount: 3 LastAdded: 2 LastDisplayed: 2
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 at 0x3ccc20: cd ~
Cmd #1 at 0x3ccc38: clear
Cmd #2 at 0x3cbb18: .\winpmem_1.6.2.exe dump.raw
----
```

Find open and closed threads, keys, ports, processes, files, and more

```
~/demo >>> ./volatility handles --profile Win7SP1x86 -f dump.raw
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0x848548a8      4        0x4   0x1fffff Process          System(4)
0x89819250      4        0x8    0x2001f Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\HIVELIST
0x89808e80      4        0xc    0xf000f Directory        GLOBAL??
0x8980fc58      4       0x10        0x0 Key
0x8985b478      4       0x14    0x2001f Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\PRODUCTOPTIONS
0x898100e0      4       0x18    0xf003f Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER\MEMORY MA
0x848fc4f8      4       0x1c   0x1f0001 ALPC Port        PowerMonitorPort
0x89860178      4       0x20    0x2001f Key              MACHINE\SYSTEM\SETUP
0x848fc908      4       0x24   0x1f0001 ALPC Port        PowerPort
0x8984c1e0      4       0x28    0x20019 Key              MACHINE\HARDWARE\DESCRIPTION\SYSTEM\MULTIFUNCTIONADAPTER
0x851902c8      4       0x2c   0x1fffff Thread           TID 160 PID 4
0x8985b818      4       0x30    0xf003f Key              MACHINE\SYSTEM\CONTROLSET001
0x8985b7c8      4       0x34    0xf003f Key              MACHINE\SYSTEM\CONTROLSET001\ENUM
0x8985ccb0      4       0x38    0xf003f Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\CLASS
0x8984e110      4       0x3c    0xf003f Key              MACHINE\SYSTEM\CONTROLSET001\SERVICES
0x898f99a8      4       0x40    0x20019 Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\WMI\SECURITY
0x899a98d8      4       0x44        0xe Token
0x898f29c0      4       0x48       0x11 Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\LSA
0x85db9478      4       0x4c        0x3 File             \Device\HarddiskVolume1\Windows\System32\config\SYSTEM.LOG2
0x85d8f028      4       0x50  0x2020003 File             \Device\HarddiskVolume1\Windows\System32\config\SOFTWARE
0x85d8fc78      4       0x54  0x2000003 File             \Device\HarddiskVolume1\Windows\System32\config\SOFTWARE.LOG1
0x84b6d240      4       0x58       0x2a Process          explorer.exe(3048)
```

```
0x84991ed0    520      0x944   0x100003 Semaphore
0x84b6d240    520      0x948     0x1478 Process          explorer.exe(3048)
0x84c747e8    520      0x94c   0x100003 Semaphore
0x86df74d8    520      0x954   0x100003 Semaphore
0x84dcd928    520      0x958   0x1fffff Thread         TID 628 PID 520
0x8502d310    520      0x95c   0x1f0001 ALPC Port
0x84e24c20    520      0x960   0x100003 Semaphore
0x84ab5030    520      0x964     0x1478 Process          taskhost.exe(3348)
0x86df7490    520      0x968   0x100003 Semaphore
0x84fdca30    520      0x96c     0x1478 Process          vmtoolsd.exe(1192)
0x8e146a68    528        0x4        0x3 Directory        KnownDlls
0x86ab0c18    528        0x8   0x100020 File             \Device\HarddiskVolume1\Windows\System32
0x8a9d8170    528        0xc    0x20019 Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
0x86ab3a00    528       0x10      0x804 EtwRegistration
0x86ab0a20    528       0x14   0x1f0001 ALPC Port
0x86ab38e8    528       0x18   0x100003 Semaphore
0x86ab38a0    528       0x1c   0x100003 Semaphore
0x86ab3640    528       0x20      0x804 EtwRegistration
0x86ab35d8    528       0x24      0x804 EtwRegistration
0x907091c8    528       0x28    0xf003f Key              MACHINE
0x91272ec8    528       0x2c        0xf Directory        BaseNamedObjects
```

Find loaded and unloaded kernel modules (rootkits!)

```
~/demo >>> ./volatility modules --profile Win7SP1x86 -f dump.raw
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    Base             Size File
---------- -------------------- ---------- ---------- ----
0x8484bc98 ntoskrnl.exe         0x82844000   0x412000 \SystemRoot\system32\ntkrnlpa.exe
0x8484bc20 hal.dll              0x8280d000    0x37000 \SystemRoot\system32\halmacpi.dll
0x8484bba0 kdcom.dll            0x80bb2000     0x8000 \SystemRoot\system32\kdcom.dll
0x8484bb20 mcupdate.dll         0x82e14000    0x85000 \SystemRoot\system32\mcupdate_GenuineIntel.dll
0x8484baa0 PSHED.dll            0x82e99000    0x11000 \SystemRoot\system32\PSHED.dll
0x8484ba20 BOOTVID.dll          0x82eaa000     0x8000 \SystemRoot\system32\BOOTVID.dll
0x8484b9a8 CLFS.SYS             0x82eb2000    0x42000 \SystemRoot\system32\CLFS.SYS
0x8484b930 CI.dll               0x82ef4000    0xab000 \SystemRoot\system32\CI.dll
0x8484b8b0 Wdf01000.sys         0x8861e000    0x71000 \SystemRoot\system32\drivers\Wdf01000.sys
0x8484b830 WDFLDR.SYS           0x8868f000     0xe000 \SystemRoot\system32\drivers\WDFLDR.SYS
0x8484b7b8 ACPI.sys             0x8869d000    0x48000 \SystemRoot\system32\drivers\ACPI.sys
0x8484b738 WMILIB.SYS           0x886e5000     0x9000 \SystemRoot\system32\drivers\WMILIB.SYS
0x8484b6b8 msisadrv.sys         0x886ee000     0x8000 \SystemRoot\system32\drivers\msisadrv.sys
0x84845d38 pci.sys              0x886f6000    0x2a000 \SystemRoot\system32\drivers\pci.sys
0x84845cb8 vdrvroot.sys         0x88720000     0xb000 \SystemRoot\system32\drivers\vdrvroot.sys
0x84845c38 partmgr.sys          0x8872b000    0x11000 \SystemRoot\System32\drivers\partmgr.sys
```

Inspect loaded system libraries

```
~/demo >>> ./volatility dlllist --profile Win7SP1x86 -f dump.raw
Volatility Foundation Volatility Framework 2.6
************************************************************************
System pid:      4
Unable to read PEB for task.
************************************************************************
smss.exe pid:    276
Command line : \SystemRoot\System32\smss.exe


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x477b0000    0x13000     0xffff \SystemRoot\System32\smss.exe
0x77220000   0x13c000     0xffff C:\Windows\SYSTEM32\ntdll.dll
************************************************************************
```

```
powershell.exe pid:   3664
Command line : "C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe"
Service Pack 1

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x21c60000    0x72000     0xffff C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe
0x77220000   0x13c000     0xffff C:\Windows\SYSTEM32\ntdll.dll
0x75710000    0xd4000     0xffff C:\Windows\system32\kernel32.dll
0x755d0000    0x4a000     0xffff C:\Windows\system32\KERNELBASE.dll
0x75a30000    0xa0000     0xffff C:\Windows\system32\ADVAPI32.dll
0x75ad0000    0xac000     0xffff C:\Windows\system32\msvcrt.dll
0x75810000    0x19000     0xffff C:\Windows\SYSTEM32\sechost.dll
0x76b70000    0xa1000     0xffff C:\Windows\system32\RPCRT4.dll
0x73720000    0x14000     0xffff C:\Windows\system32\ATL.DLL
0x76ef0000    0xc9000     0xffff C:\Windows\system32\USER32.dll
0x76aa0000    0x4e000     0xffff C:\Windows\system32\GDI32.dll
0x75800000     0xa000     0xffff C:\Windows\system32\LPK.dll
0x75670000    0x9d000     0xffff C:\Windows\system32\USP10.dll
0x770c0000   0x15c000     0xffff C:\Windows\system32\ole32.dll
0x76a10000    0x8f000     0xffff C:\Windows\system32\OLEAUT32.dll
0x6ec00000    0x4a000     0xffff C:\Windows\system32\mscoree.dll
```

Discover open and closed network connections

```
~/demo >>> ./volatility netscan --profile Win7SP1x86 -f dump.raw
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x7da14360         UDPv4    172.16.12.150:138              *:*                                   4        System         2017-01-01 22:59:03 UTC+0000
0x7da18448         UDPv4    127.0.0.1:1900                 *:*                                   2192     svchost.exe    2017-01-01 22:59:03 UTC+0000
0x7dda92c0         UDPv6    fe80::b5d6:514a:1609:b8b7:1900 *:*                                   2192     svchost.exe    2017-01-01 22:59:03 UTC+0000
0x7dddb748         UDPv4    172.16.12.150:137              *:*                                   4        System         2017-01-01 22:59:03 UTC+0000
0x7dde7928         UDPv4    0.0.0.0:5355                   *:*                                   1172     svchost.exe    2017-01-01 22:59:06 UTC+0000
0x7dde7928         UDPv6    :::5355                        *:*                                   1172     svchost.exe    2017-01-01 22:59:06 UTC+0000
0x7dde9418         UDPv6    ::1:60524                      *:*                                   2192     svchost.exe    2017-01-01 22:59:03 UTC+0000
0x7ddef7a0         UDPv4    0.0.0.0:0                      *:*                                   1172     svchost.exe    2017-01-01 22:59:03 UTC+0000
0x7ddef7a0         UDPv6    :::0                           *:*                                   1172     svchost.exe    2017-01-01 22:59:03 UTC+0000
0x7ddf0ab0         UDPv6    ::1:1900                       *:*                                   2192     svchost.exe    2017-01-01 22:59:03 UTC+0000
0x7e3baa28         UDPv4    172.16.12.150:1900             *:*                                   2192     svchost.exe    2017-01-01 22:59:03 UTC+0000
0x7e3e7ba8         UDPv4    127.0.0.1:60525                *:*                                   2192     svchost.exe    2017-01-01 22:59:03 UTC+0000
0x7dda1008         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        520      lsass.exe
0x7e299358         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        520      lsass.exe
0x7e299358         TCPv6    :::49156                       :::0                 LISTENING        520      lsass.exe
```

Most plugins can search by regular expressions, filter results, and dump extracted objects (like files/ processes/kernel modules/etc.) to your analysis machine.

Drawbacks

- Volatility can be slow
  - Use Rekall if you want better performance
- Images aren't automatically detected
  - Again, use Rekall if you want automatic (sometimes) detection

Benefits

- If you can use a command line interface (CLI), you can use Volatility
- You can get almost all system state data for machines under your control
- With Volatility, you get an amazing developer community

But this isn't a framework? It's not automated?!

The *possible* future

- Memory dumps taken *prior to* and *after* infections give us the ability to do a *diff* to see all known changes and semi-autonomously act on it
- This is my current work at ORNL. Talk to me later if you want more details.

Takeaways

- Volatility is a popular, effective tool for in-depth forensic analysis of hosts
- It is highly versatile, and can help you analyze everything from end user devices to AWS servers
- The future is unknown, but focusing more on incident response tooling will help when breaches do happen

Thank you for coming!

Jared Smith
Work Email: smithjm@ornl.gov
Personal Email: jared@jaredsmith.io
Twitter: @jaredthecoder
Web: jaredthecoder.com