Memory Forensics and the Windows Subsystem for Linux

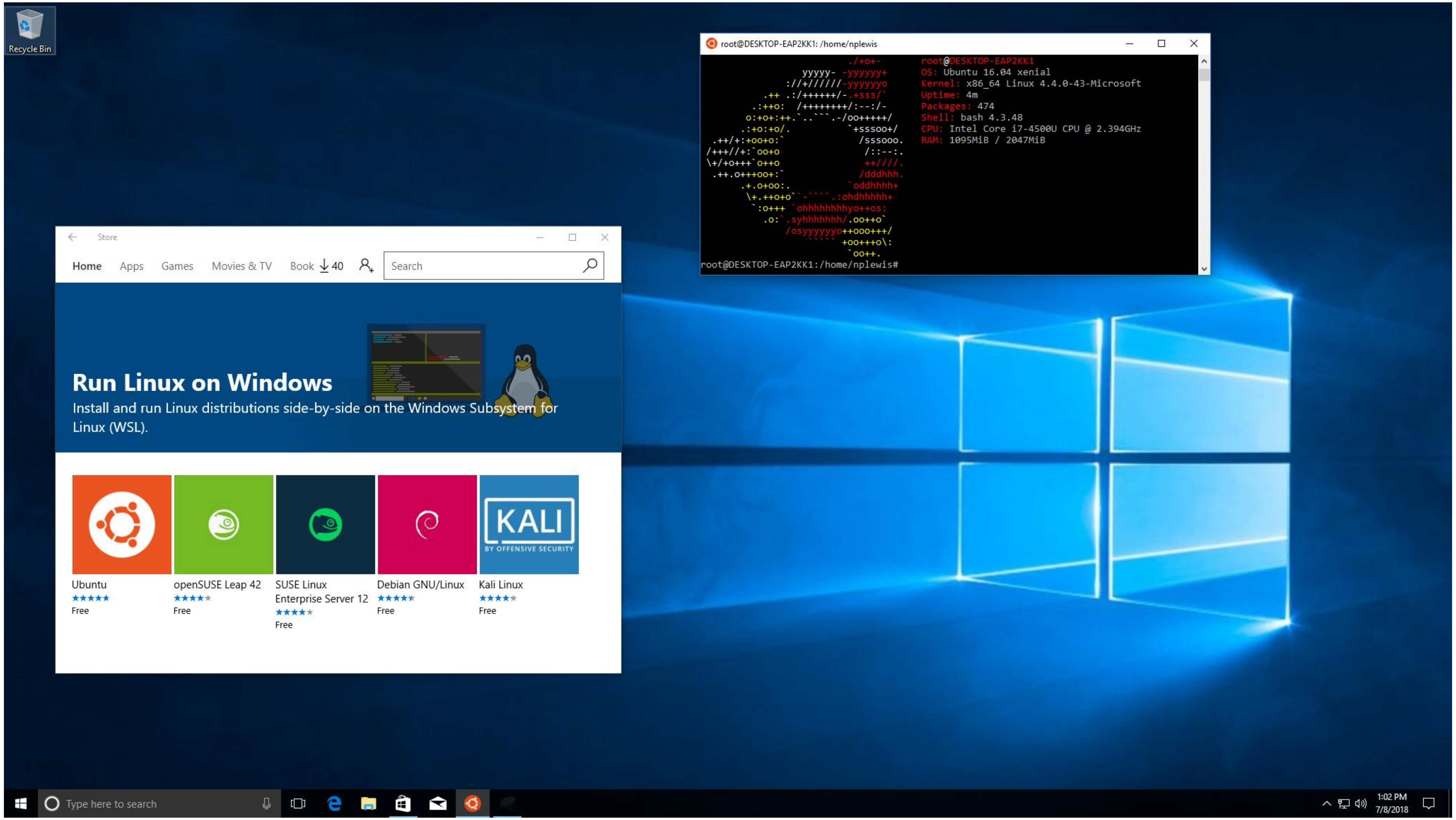
Nathan Lewis, Andrew Case, Aisha Ali-Gombe, Golden Richard III

DFRWS USA 2018

Bio

- Software Engineer at Dynetics, Inc.
- Previously at Louisiana State University
  - Master’s student, Computer Science
  - Research Interests
    - Reverse engineering
    - Memory forensics
  - Advisor: Dr. Golden Richard III
- Twitter: @nplew

Windows Subsystem for Linux (WSL)



root@DESKTOP-EAP2KK1: /home/nplewis

~~~
                          ./+o+-       root@DESKTOP-EAP2KK1
                  yyyyy- -yyyyyy+      OS: Ubuntu 16.04 xenial
               ://+//////-yyyyyyo      Kernel: x86_64 Linux 4.4.0-43-Microsoft
           .++ .:/++++++/-.+sss/`      Uptime: 4m
         .:++o:  /++++++++/:--:/-      Packages: 474
        o:+o+:++.`..```.-/oo+++++/     Shell: bash 4.3.48
       .:+o:+o/.          `+sssoo+/    CPU: Intel Core i7-4500U CPU @ 2.394GHz
  .++/+:+oo+o:`             /sssooo.   RAM: 1095MiB / 2047MiB
 /+++//+:`oo+o               /::--:.
 \+/+o+++`o++o               ++////.
  .++.o+++oo+:`             /dddhhh.
       .+.o+oo:.          `oddhhhh+
        \+.++o+o``-````.:ohdhhhhh+
         `:o+++ `ohhhhhhhyo++os:
           .o:`.syhhhhhh/.oo++o`
               /osyyyyyyo++ooo+++/
                   ``````  +oo+++o\:
                          `oo++.
root@DESKTOP-EAP2KK1:/home/nplewis#
~~~

Store

Run Linux on Windows

Install and run Linux distributions side-by-side on the Windows Subsystem for Linux (WSL).

Ubuntu ★★★★★ Free	openSUSE Leap 42 ★★★★☆ Free	SUSE Linux Enterprise Server 12 ★★★★☆ Free	Debian GNU/Linux ★★★★☆ Free	Kali Linux ★★★★☆ Free

Forensic Interest

- How are Linux applications supported?

Forensic Interest

- How are Linux applications supported?
- How can malware exploit it?

Forensic Interest

- How are Linux applications supported?
- How can malware exploit it?
- How can we analyze it?

Bashware

- 1. Enable WSL optional feature
- 2. Reboot
- 3. Install distro from app store
- 4. ???
- 5. Profit

- 1. Enable developer’s mode
- 2. Execute lxrun
- 3. ???
- Profit

Memory Analysis With Volatility

- Direct Windows kernel support

Memory Analysis With Volatility

- Direct Windows kernel support
- ELF execution support

Memory Analysis With Volatility

- Direct Windows kernel support
- ELF execution support
- Many broken plugins ☹

Plugin Example: pslist

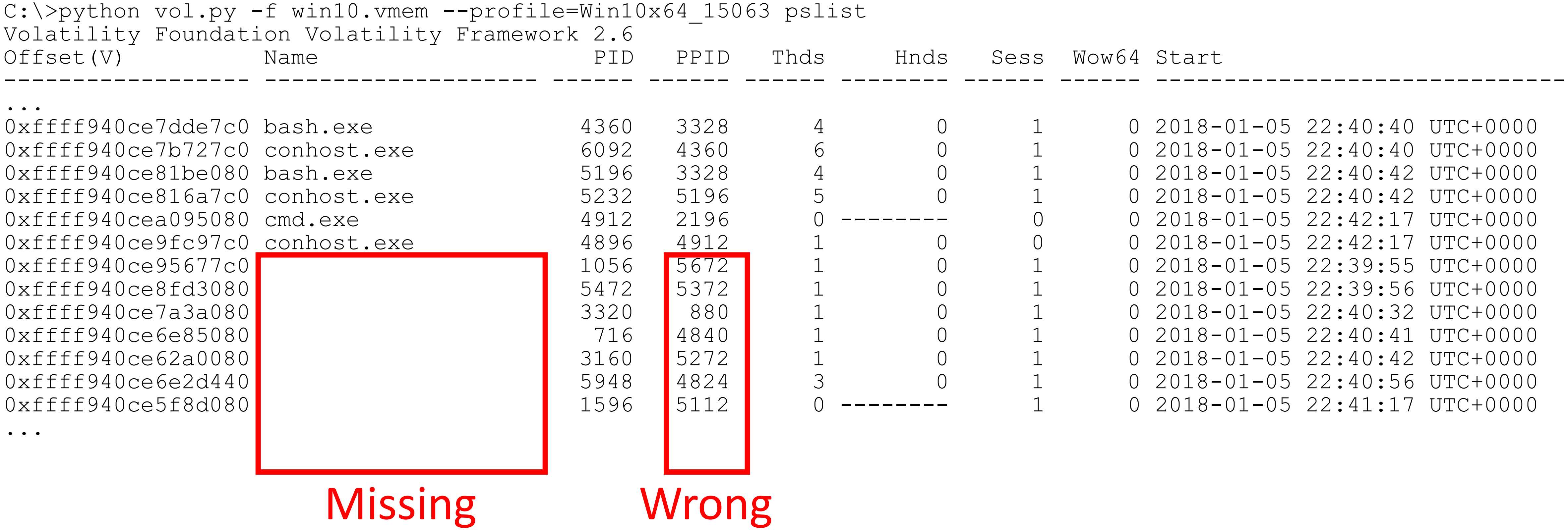
```
C:\>python vol.py -f win10.vmem --profile=Win10x64_15063 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
...
0xffff940ce7dde7c0 bash.exe               4360   3328      4        0      1      0 2018-01-05 22:40:40 UTC+0000
0xffff940ce7b727c0 conhost.exe            6092   4360      6        0      1      0 2018-01-05 22:40:40 UTC+0000
0xffff940ce81be080 bash.exe               5196   3328      4        0      1      0 2018-01-05 22:40:42 UTC+0000
0xffff940ce816a7c0 conhost.exe            5232   5196      5        0      1      0 2018-01-05 22:40:42 UTC+0000
0xffff940cea095080 cmd.exe                4912   2196      0 --------      0      0 2018-01-05 22:42:17 UTC+0000
0xffff940ce9fc97c0 conhost.exe            4896   4912      1        0      0      0 2018-01-05 22:42:17 UTC+0000
0xffff940ce95677c0                        1056   5672      1        0      1      0 2018-01-05 22:39:55 UTC+0000
0xffff940ce8fd3080                        5472   5372      1        0      1      0 2018-01-05 22:39:56 UTC+0000
0xffff940ce7a3a080                        3320    880      1        0      1      0 2018-01-05 22:40:32 UTC+0000
0xffff940ce6e85080                         716   4840      1        0      1      0 2018-01-05 22:40:41 UTC+0000
0xffff940ce62a0080                        3160   5272      1        0      1      0 2018-01-05 22:40:42 UTC+0000
0xffff940ce6e2d440                        5948   4824      3        0      1      0 2018-01-05 22:40:56 UTC+0000
0xffff940ce5f8d080                        1596   5112      0 --------      1      0 2018-01-05 22:41:17 UTC+0000
...
```

Plugin Example: pslist

```
C:\>python vol.py -f win10.vmem --profile=Win10x64_15063 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
...
0xffff940ce7dde7c0 bash.exe               4360   3328      4        0      1      0 2018-01-05 22:40:40 UTC+0000
0xffff940ce7b727c0 conhost.exe            6092   4360      6        0      1      0 2018-01-05 22:40:40 UTC+0000
0xffff940ce81be080 bash.exe               5196   3328      4        0      1      0 2018-01-05 22:40:42 UTC+0000
0xffff940ce816a7c0 conhost.exe            5232   5196      5        0      1      0 2018-01-05 22:40:42 UTC+0000
0xffff940cea095080 cmd.exe                4912   2196      0 --------      0      0 2018-01-05 22:42:17 UTC+0000
0xffff940ce9fc97c0 conhost.exe            4896   4912      1        0      0      0 2018-01-05 22:42:17 UTC+0000
0xffff940ce95677c0                        1056   5672      1        0      1      0 2018-01-05 22:39:55 UTC+0000
0xffff940ce8fd3080                        5472   5372      1        0      1      0 2018-01-05 22:39:56 UTC+0000
0xffff940ce7a3a080                        3320    880      1        0      1      0 2018-01-05 22:40:32 UTC+0000
0xffff940ce6e85080                         716   4840      1        0      1      0 2018-01-05 22:40:41 UTC+0000
0xffff940ce62a0080                        3160   5272      1        0      1      0 2018-01-05 22:40:42 UTC+0000
0xffff940ce6e2d440                        5948   4824      3        0      1      0 2018-01-05 22:40:56 UTC+0000
0xffff940ce5f8d080                        1596   5112      0 --------      1      0 2018-01-05 22:41:17 UTC+0000
...
```

Missing

Plugin Example: pslist

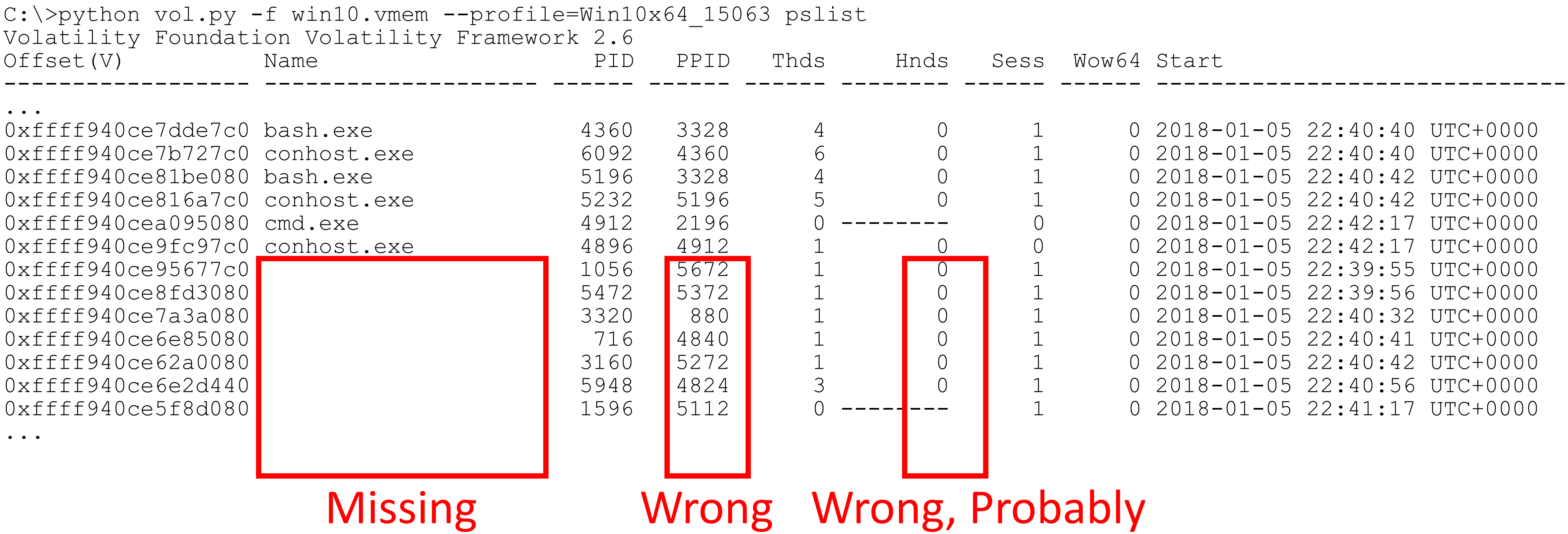


```
C:\>python vol.py -f win10.vmem --profile=Win10x64_15063 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
...
0xffff940ce7dde7c0 bash.exe               4360   3328      4        0      1      0 2018-01-05 22:40:40 UTC+0000
0xffff940ce7b727c0 conhost.exe            6092   4360      6        0      1      0 2018-01-05 22:40:40 UTC+0000
0xffff940ce81be080 bash.exe               5196   3328      4        0      1      0 2018-01-05 22:40:42 UTC+0000
0xffff940ce816a7c0 conhost.exe            5232   5196      5        0      1      0 2018-01-05 22:40:42 UTC+0000
0xffff940cea095080 cmd.exe                4912   2196      0 --------      0      0 2018-01-05 22:42:17 UTC+0000
0xffff940ce9fc97c0 conhost.exe            4896   4912      1        0      0      0 2018-01-05 22:42:17 UTC+0000
0xffff940ce95677c0                        1056   5672      1        0      1      0 2018-01-05 22:39:55 UTC+0000
0xffff940ce8fd3080                        5472   5372      1        0      1      0 2018-01-05 22:39:56 UTC+0000
0xffff940ce7a3a080                        3320    880      1        0      1      0 2018-01-05 22:40:32 UTC+0000
0xffff940ce6e85080                         716   4840      1        0      1      0 2018-01-05 22:40:41 UTC+0000
0xffff940ce62a0080                        3160   5272      1        0      1      0 2018-01-05 22:40:42 UTC+0000
0xffff940ce6e2d440                        5948   4824      3        0      1      0 2018-01-05 22:40:56 UTC+0000
0xffff940ce5f8d080                        1596   5112      0 --------      1      0 2018-01-05 22:41:17 UTC+0000
...
```

Missing

Wrong

Plugin Example: pslist



```
C:\>python vol.py -f win10.vmem --profile=Win10x64_15063 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
...
0xffff940ce7dde7c0 bash.exe               4360   3328      4        0      1      0 2018-01-05 22:40:40 UTC+0000
0xffff940ce7b727c0 conhost.exe            6092   4360      6        0      1      0 2018-01-05 22:40:40 UTC+0000
0xffff940ce81be080 bash.exe               5196   3328      4        0      1      0 2018-01-05 22:40:42 UTC+0000
0xffff940ce816a7c0 conhost.exe            5232   5196      5        0      1      0 2018-01-05 22:40:42 UTC+0000
0xffff940cea095080 cmd.exe                4912   2196      0 --------      0      0 2018-01-05 22:42:17 UTC+0000
0xffff940ce9fc97c0 conhost.exe            4896   4912      1        0      0      0 2018-01-05 22:42:17 UTC+0000
0xffff940ce95677c0                        1056   5672      1        0      1      0 2018-01-05 22:39:55 UTC+0000
0xffff940ce8fd3080                        5472   5372      1        0      1      0 2018-01-05 22:39:56 UTC+0000
0xffff940ce7a3a080                        3320    880      1        0      1      0 2018-01-05 22:40:32 UTC+0000
0xffff940ce6e85080                         716   4840      1        0      1      0 2018-01-05 22:40:41 UTC+0000
0xffff940ce62a0080                        3160   5272      1        0      1      0 2018-01-05 22:40:42 UTC+0000
0xffff940ce6e2d440                        5948   4824      3        0      1      0 2018-01-05 22:40:56 UTC+0000
0xffff940ce5f8d080                        1596   5112      0 --------      1      0 2018-01-05 22:41:17 UTC+0000
...
```

Missing

Wrong

Wrong, Probably

Plugin Example: procdump

```
C:\>python vol.py -f win10.vmem --profile=Win10x64_15063 --dump-dir procdump

Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
...
0xffff8d83822de7c0 0x00007ff7c5b30000 bash.exe             OK: executable.5676.exe
0xffff8d83811e56c0 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d8380921480 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f755080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f791080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f79b080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d83810097c0 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f6de080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d8381ffa180 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d83826967c0 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
...
```

Plugin Example: procdump

```
C:\>python vol.py -f win10.vmem --profile=Win10x64_15063 --dump-dir procdump

Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
...
0xffff8d83822de7c0 0x00007ff7c5b30000 bash.exe             OK: executable.5676.exe
0xffff8d83811e56c0 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d8380921480 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f755080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f791080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f79b080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d83810097c0 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f6de080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d8381ffa180 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d83826967c0 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
...
```

Huh?

Plugin Example: procdump

```
C:\>python vol.py -f win10.vmem --profile=Win10x64_15063 --dump-dir procdump

Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
...
0xffff8d83822de7c0 0x00007ff7c5b30000 bash.exe             OK: executable.5676.exe
0xffff8d83811e56c0 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d8380921480 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f755080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f791080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f79b080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d83810097c0 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f6de080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d8381ffa180 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d83826967c0 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
...
```

Huh?

Missing (Again!)

Plugin Example: procdump

```
C:\>python vol.py -f win10.vmem --profile=Win10x64_15063 --dump-dir procdump

Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                  Result
------------------ ------------------ --------------------- ------
...
0xffff8d83822de7c0 0x00007ff7c5b30000 bash.exe              OK: executable.5676.exe
0xffff8d83811e56c0 ------------------                       Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d8380921480 ------------------                       Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f755080 ------------------                       Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f791080 ------------------                       Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f79b080 ------------------                       Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d83810097c0 ------------------                       Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f6de080 ------------------                       Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d8381ffa180 ------------------                       Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d83826967c0 ------------------                       Error: PEB at 0x0 is unavailable (possibly due to paging)
...
```

Huh?

Missing
(Again!)

Uh oh…

Plugin Example: procdump

```
C:\>python vol.py -f win10.vmem --profile=Win10x64_15063 --dump-dir procdump

Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
...
0xffff8d83822de7c0 0x00007ff7c5b30000 bash.exe             OK: executable.5676.exe
0xffff8d83811e56c0 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d8380921480 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f755080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f791080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f79b080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d83810097c0 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d837f6de080 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d8381ffa180 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
0xffff8d83826967c0 ------------------                      Error: PEB at 0x0 is unavailable (possibly due to paging)
...
```

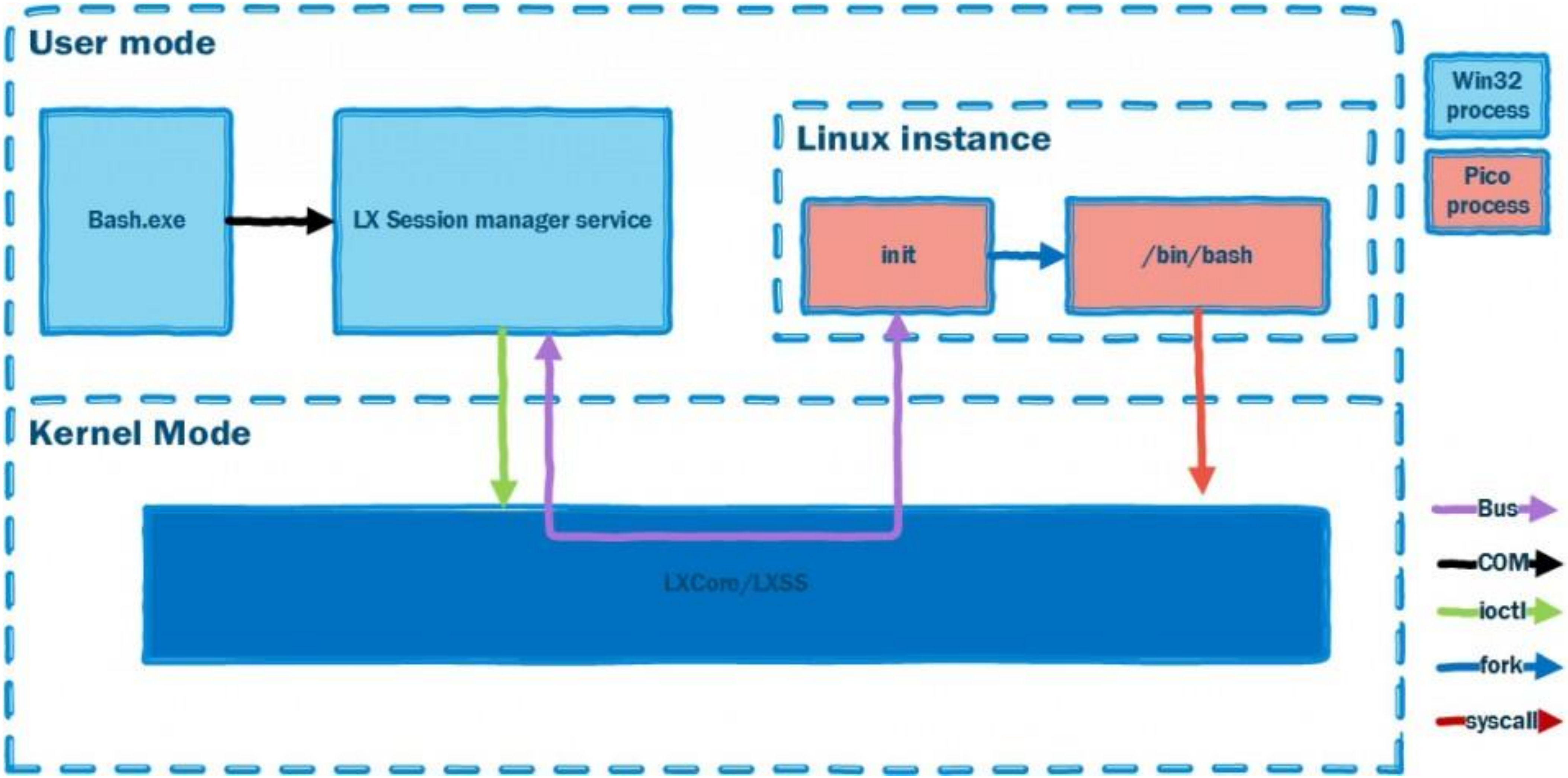
Huh?

Missing (Again!)

Uh oh…

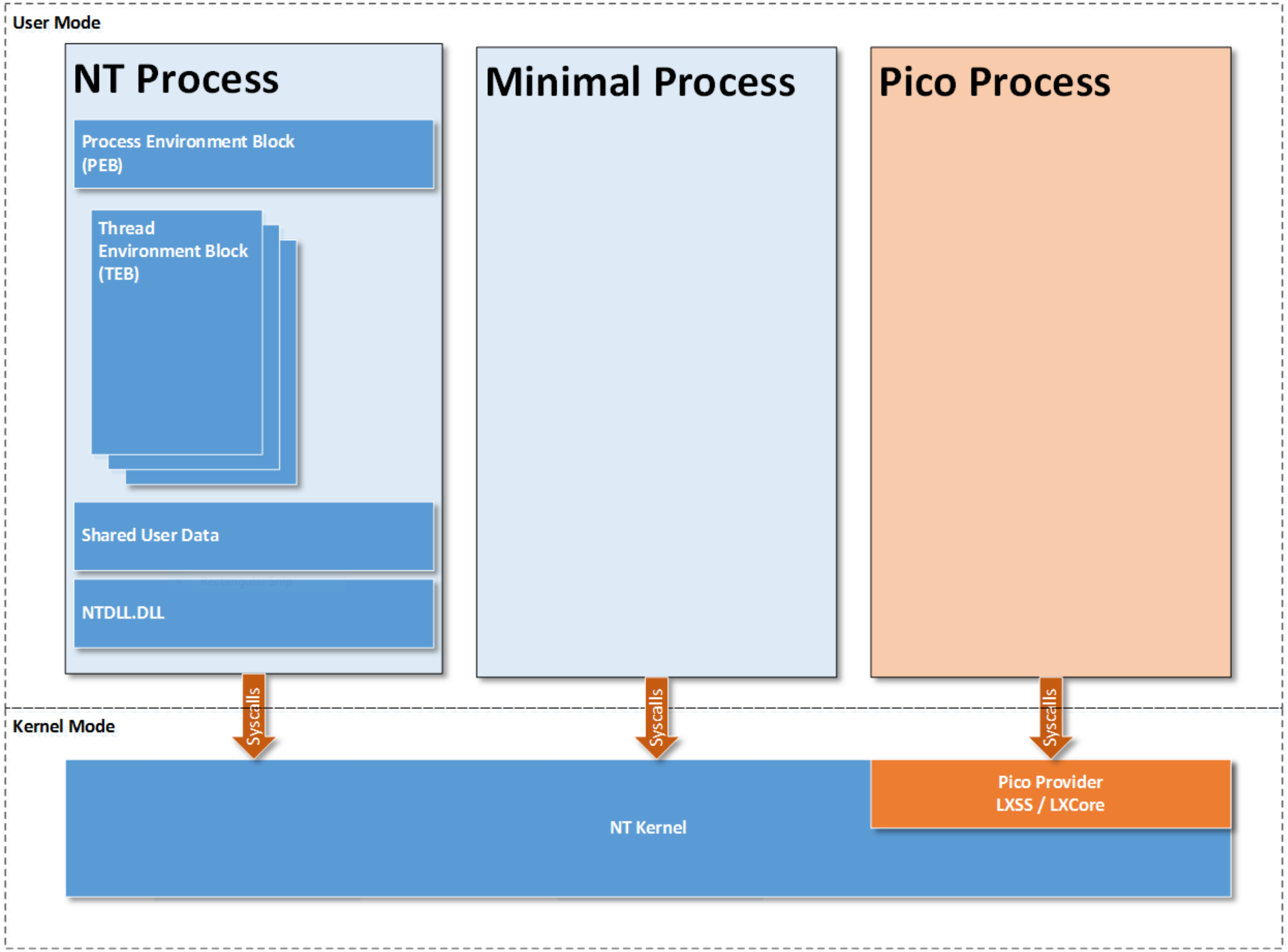
Wrong, Probably

WSL Architecture



Ref: https://blogs.msdn.microsoft.com/wsl/2016/04/22/windows-subsystem-for-linux-overview/

Windows 10 Process Types



Ref: https://blogs.msdn.microsoft.com/wsl/2016/05/23/pico-process-overview/

Identifying Pico Processes

```
>>> dt("_EPROCESS")
'_EPROCESS' (2072 bytes)
```

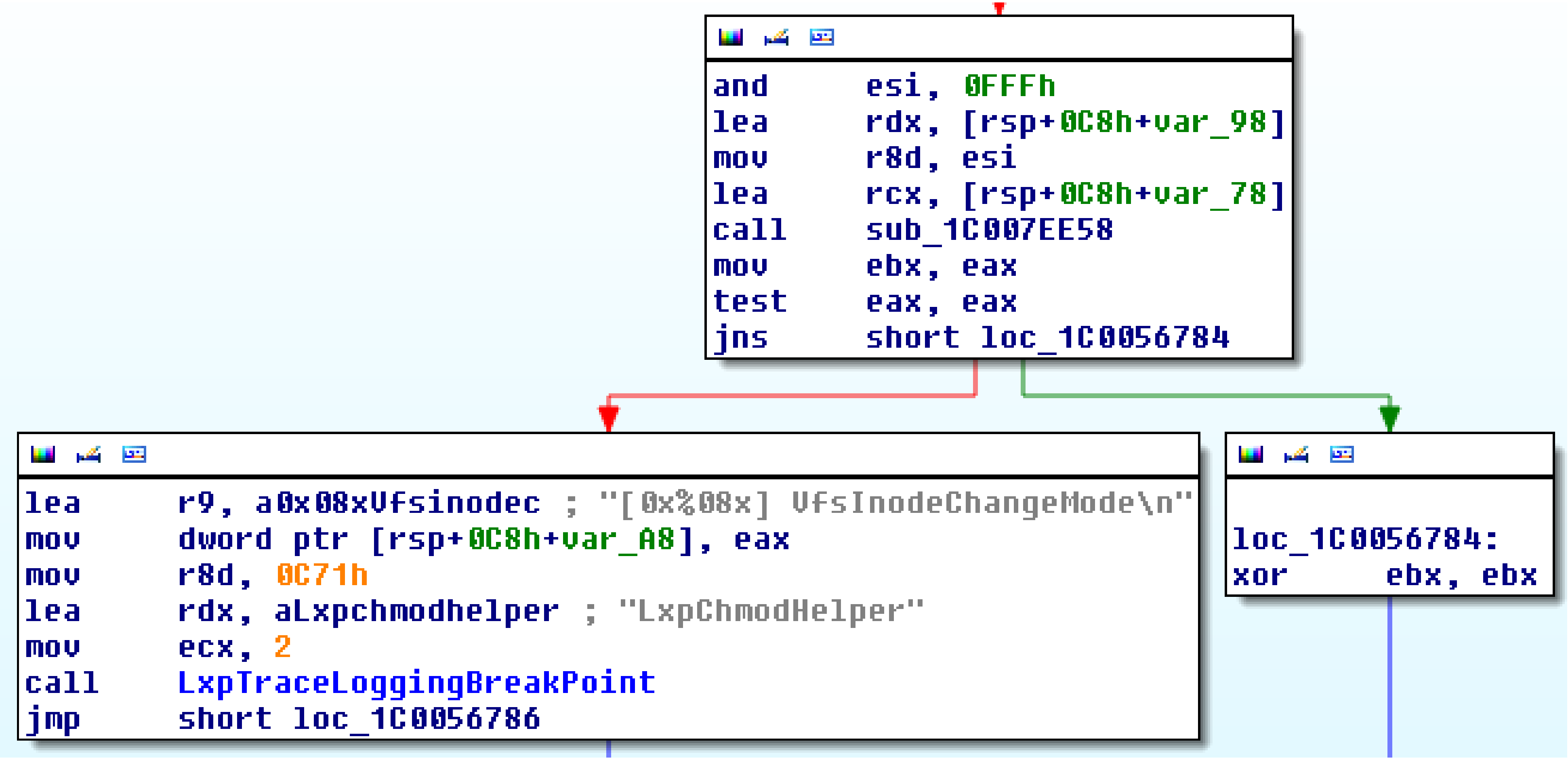
Identifying Pico Processes

```
>>> dt("_EPROCESS")
'_EPROCESS' (2072 bytes)
    ...
    0x810 : PicoCreated ['BitField', {'end_bit': 1, 'start_bit': 0, 'native_type': 'unsigned long'}]
    0x6cc : Minimal ['BitField', {'end_bit': 1, 'start_bit': 0, 'native_type': 'unsigned long'}]
```

Identifying Pico Processes

```
>>> dt("_EPROCESS")
'_EPROCESS' (2072 bytes)
  ...
  0x810 : PicoCreated ['BitField', {'end_bit': 1, 'start_bit': 0, 'native_type': 'unsigned long'}]
  0x6cc : Minimal ['BitField', {'end_bit': 1, 'start_bit': 0, 'native_type': 'unsigned long'}]
  0x710 : PicoContext ['pointer64',['void']] ←——————— ???
  ...
```

Reverse Engineering LXCore



```
and     esi, 0FFFh
lea     rdx, [rsp+0C8h+var_98]
mov     r8d, esi
lea     rcx, [rsp+0C8h+var_78]
call    sub_1C007EE58
mov     ebx, eax
test    eax, eax
jns     short loc_1C0056784
```

```
lea     r9, a0x08xVfsinodec ; "[0x%08x] VfsInodeChangeMode\n"
mov     dword ptr [rsp+0C8h+var_A8], eax
mov     r8d, 0C71h
lea     rdx, aLxpchmodhelper ; "LxpChmodHelper"
mov     ecx, 2
call    LxpTraceLoggingBreakPoint
jmp     short loc_1C0056786
```

```
loc_1C0056784:
xor     ebx, ebx
```

WSL Pico Context Artifacts

- Program name
- Linux PID
- Reference to _EPROCESS
- Reference to parent process’ PicoContext
- Main executable address
- List of shared objects
- List of file system handles
- List of threads
- Process inputs

Scanning for Artifacts

- Pool tag scanning
  - “Lx “
  - Process’ Pico Contexts
  - Threads’ Pico Contexts
- ELF executables
- Command history (/bin/bash)

New Volatility Plugins

- Processes (Basic)
  - picolist
  - picoscan
  - picotree
- Process (Inputs)
  - picobash
  - picocmdline
  - picoenvars
- Threads
  - picothreads
  - picothrdscan
- Files
  - picolsof
  - picoprocdump
  - picosolist
  - picosodump
  - picoelflist
  - picoelfdump
  - picoldrmodules

Moving Forward

- Further investigation

Moving Forward

- Further investigation
- Maintain new and existing plugins

Moving Forward

- Further investigation
- Maintain new and existing plugins
- Use new plugins!

Moving Forward

- Further investigation
- Maintain new and existing plugins
- Use new plugins!
- Explore other pico applications?

Thank You!