RECALL FORENSICS SNAP SHOTS

Interactive Rekall Session

Analysis Methods

1. Individual plugin commands
2. An interactive ipython shell

```
sansforensics@siftworkstation:/cases/exercise2$ rekall -f processfu.img pslist
_EPROCESS  Name                 PID   PPID   Thds     Hnds   Sess  Wow64 Start
---------- -------------------- ----- ------ ------ -------- ------ ------ -------
---
0x825c8830 System                 4      0     55      510 -       False -
0x82254508 alg.exe              320    696      6      107      0  False 2014-0
0x8205c968 VMwareTray.exe       356    840      1       29      0  False 2014-0
0x8240f4f0 smss.exe             580      4      3       21 -       False 2014-0
```

```
win7manycmd.vmem 14:48:35> pslist
----------------------------> pslist()
_EPROCESS  Name                 PID   PPID   Thds     Hnds   Sess  Wow64 Start
---------- -------------------- ----- ------ ------ -------- ------ ------ --------
---
0x84f48bb0 System                 4      0     91      430 -       False 2012-01-
0x861a4128 smss.exe             268      4      2       29 -       False 2012-01-
0x86c47ad8 msdtc.exe            308    488     15      152      0  False 2012-01-
```

Profile Auto-detection

```
root@siftworkstation:/cases# rekal -f insider-case.vmem
--------------------------------------------------------------------------------
The Rekall Memory Forensic framework 1.3.2 (Dammastock).

"We can remember it for you wholesale!"

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License.

See http://www.rekall-forensic.com/docs/Manual/tutorial.html to get started.
--------------------------------------------------------------------------------
[1] insider-case.vmem 16:43:04>
```

No Profile Necessary

Listing Available Plugins

Get a list of applicable plugins for this memory image by typing: **`plugins.<tab>`**

```
win7manycmd.vmem 20:47:13> plugins.
Display all 114 possibilities? (y or n)
plugins.analyze_struct     plugins.find_dtb          plugins.mutantscan        plugins.services
plugins.atoms              plugins.gahti             plugins.netscan           plugins.sessions
plugins.atomscan           plugins.getservicesids    plugins.netstat           plugins.ssdt
plugins.build_index        plugins.grep              plugins.notebook          plugins.svcscan
plugins.callbacks          plugins.guess_guid        plugins.null              plugins.symlinkscan
plugins.cc                 plugins.handles           plugins.object_tree       plugins.thrdscan
plugins.cert_vad_scan      plugins.hivedump          plugins.object_types      plugins.threads
plugins.certscan           plugins.hives             plugins.p                 plugins.timers
plugins.check_pehooks      plugins.hooks_eat         plugins.pars
plugins.cmdscan            plugins.hooks_iat         plugins.pas2
plugins.consoles           plugins.hooks_inline      plugins.pedu
plugins.convert_profile    plugins.imagecopy         plugins.pein
plugins.desktops           plugins.imageinfo         plugins.pfn
plugins.devicetree         plugins.impscan           plugins.phys_
plugins.dis                plugins.info              plugins.pool_tracker      plugins.vaddump
```

For description/options > <plugin>?

Session Caching

```
fariet1.vmem 22:08:58> print session
Rekall Memory Forensics session Started on Sun Dec 21 21:36:35 2014.

Config:
{
  autodetect_threshold = 1.0
  base_filename = fariet1.vmem
  buffer_size = 20971520
  cache = {
    ObjectTypeMap = <Array 0 x Pointer @ 0x829548C0>
    PsActiveProcessHead = [_LIST_ENTRY _LIST_ENTRY] @ 0x82952E98
    PsLoadedModuleList = [_LIST_ENTRY _LIST_ENTRY] @ 0x8295A810
    default_address_space = IA32PagedMemoryPae@0x00185000 (Kernel AS@0x185000)
    idle_process = [_EPROCESS _EPROCESS] @ 0x02945540 (pid=0)
    kernel_base = 2189500416
    pslist_cache = {'Handles': set([2260281856, 2261888320, 2237786536, 2262174088,
237893952, 2256944168, 2237734208, 2261999664, 2263438400, 2256984864, 2262062752,
56827696, 2238160944, 2263164680, 2263350592, 2256770352, 2260923400, 2261631024, 2
```

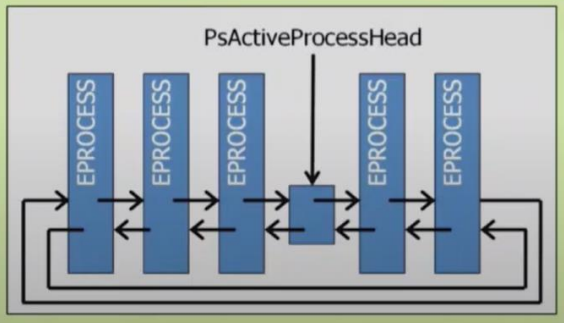
Throughout a Rekall Session, output from previous plugins is cached and referenced for greater efficiency.

Process Enumeration

pslist Using Volatility

```
In [1]: dt("_KDDEBUGGER_DATA64")
 '_KDDEBUGGER_DATA64' (832 bytes)
0x0    : Header
0x18   : KernBase
0x20   : BreakpointWithStatus
0x28   : SavedContext
0x30   : ThCallbackStack
0x32   : NextCallback
0x34   : FramePointer
0x38   : KiCallUserMode
0x40   : KeUserCallbackDispatcher
0x48   : PsLoadedModuleList
0x50   : PsActiveProcessHead
0x58   : PspCidTable
```

1. Locate Kernel Debugging Data Block
2. Follow "PSActiveProcessHead" pointer
3. Walk linked "_EPROCESS" blocks



Process Scanning with Rekall

```
0x3e484948    TPAutoConnSvc.      1768 0x86884948    504 0x3ed14340 EP    2013-06-20 19:0
0x3e4fa030    services.exe         504 0x868fa030    400 0x3ed14080 EP    2013-06-20 19:0
0x3e4fd030    lsm.exe              520 0x868fd030    400 0x3ed14100 EP    2013-06-20 19:0
0x3e742d40    svchost.exe         1256 -             440 0x3ec77260       2013-06-20 18:5
0x3e749d20    dwm.exe             1760 -             748 0x3ec772e0       2013-06-20 18:5
```

Rekall's PSScan Status Flags

```
Status flags:
  E: A known _EPROCESS address from pslist.
  P: A known pid from pslist.Scan the address space for pool allocations.
```

Know Normal (Windows Processes)

Baidu AntiVirus

	_EPROCESS	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exi
0xe00123ce18c0	System	4	0	107	-	-	FALSE	9/12/15	09:58:11+0000	-
0xe00126b26040	smss.exe	384	4	2	-	-	FALSE	9/12/15	09:58:11+0000	-
0xe00126bc18c0	svchost.exe	420	612	24	-	0	FALSE	9/12/15	09:58:14+0000	-
0xe00126b4c8c0	csrss.exe	456	448	12	-	0	FALSE	9/12/15	09:58:11+0000	-
0xe00126bb0080	wininit.exe	512	448	1	-	0	FALSE	9/12/15	09:58:12+0000	-
0xe00126bae8c0	csrss.exe	520	504	10	-	1	FALSE	9/12/15	09:58:12+0000	-
0xe00123d328c0	winlogon.exe	564	504	2	-	1	FALSE	9/12/15	09:58:13+0000	-
0xe00125ba98c0	services.exe	612	512	5	-	0	FALSE	9/12/15	09:58:14+0000	-
0xe00123d5c1c0	lsass.exe	620	512	6	-	0	FALSE	9/12/15	09:58:14+0000	-
0xe00126dd38c0	BHipsSvc.exe	1432	612	59	-	0	TRUE	9/12/15	09:58:15+0000	-
0xe00126a8c8c0	bavhm.exe	2828	1356	1	-	0	FALSE	9/12/15	09:58:25+0000	-
0xe001274648c0	explorer.exe	3480	2564	97	-	0	FALSE	9/12/15	09:59:46+0000	-
0xe00125a62080	StikyNot.exe	4104	3480	8	-	0	FALSE	9/12/15	10:00:01+0000	-
0xe00125aaa8c0	CodeMeterCC.ex	4172	3480	2	-	1	TRUE	9/12/15	10:00:01+0000	-
0xe00125253080	jusched.exe	4200	4164	1	-	0	TRUE	9/12/15	10:00:01+0000	-
0xe00125ce48c0	BavTray.exe	4288	4164	41	-	0	TRUE	9/12/15	10:00:02+0000	-
0xe00125e8b080	cmd.exe	4784	3480	1	-	0	FALSE	9/12/15	10:00:07+0000	-
0xe0012563c080	conhost.exe	4792	4784	3	-	0	FALSE	9/12/15	10:00:07+0000	-
0xe00125fab100	svchost.exe	5112	612	7	-	0	FALSE	9/12/15	10:38:54+0000	-
0xe0012b0eb8c0	rekal.exe	6000	4784	4	-	1	FALSE	9/12/15	13:13:37+0000	-

Memory Analysis with Rekall

Step 1: Identify Rogue Processes

_EPROCESS	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x84e5b880	System	4	0	86	514	-	FALSE	6/9/15 21:29:42+0000	-
0x84ebf2d8	smss.exe	256	4	2	30	-	FALSE	6/9/15 21:29:42+0000	-
0x87775090	csrss.exe	348	332	9	395	0	FALSE	6/9/15 21:29:46+0000	-
0x877d71b8	wininit.exe	392	332	3	79	0	FALSE	6/9/15 21:29:47+0000	-
0x877db090	csrss.exe	404	384	10	328	1	FALSE	6/9/15 21:29:47+0000	-
0x877fd050	winlogon.exe	440	384	3	119	1	FALSE	6/9/15 21:29:47+0000	-
0x87dc74f0	services.exe	492	392	10	198	0	FALSE	6/9/15 21:29:49+0000	-
0x87dce148	lsass.exe	508	392	7	597	0	FALSE	6/9/15 21:29:49+0000	-
0x87dd9458	lsm.exe	520	392	11	145	0	FALSE	6/9/15 21:29:50+0000	-
0x87f0a030	svchost.exe	636	492	14	371	0	FALSE	6/9/15 21:29:51+0000	-
0x87f16b68	svchost.exe	712	492	7	261	0	FALSE	6/9/15 21:29:51+0000	-
0x87f3ca20	svchost.exe	804	492	20	463	0	FALSE	6/9/15 21:29:52+0000	-
0x850ea030	DropboxUpdate.	1988	300	5	119	0	FALSE	6/9/15 21:32:10+0000	-
0x85176840	SearchIndexer.	460	492	13	631	0	FALSE	6/9/15 21:32:18+0000	-
0x8510ad40	dwm.exe	2064	836	6	197	1	FALSE	6/9/15 21:36:02+0000	-
0x85191d40	explorer.exe	2316	196	58	1021	1	FALSE	6/9/15 21:36:02+0000	-
0x851a9770	taskhost.exe	3976	492	7	154	1	FALSE	6/9/15 21:36:02+0000	-
0x850fbd40	efsui.exe	4020	508	3	92	1	FALSE	6/9/15 21:36:02+0000	-

Memory Analysis with Rekall

Step 2: Process DLLs/Handles

```
[1] Default session 18:00:48> dlllist pid=4008
----------------------------> dlllist(pid=4008)
**************************************************
explorer.exe pid: 4008
Command line : explorer.exe

     Base             Size            Load Reason/Count          Path
-------------- -------------- ------------------------------ ----
0x7ff7d43c0000       0x261000 LoadReasonStaticDependency     C:\Windows\explorer.exe
0x7ffa36fc0000       0x1ac000 LoadReasonStaticDependency     C:\Windows\SYSTEM32\ntdll.dll
0x7ffa34fc0000       0x13a000 LoadReasonDynamicLoad          C:\Windows\system32\KERNEL32.DLL
0x7ffa342f0000       0x10f000 LoadReasonStaticDependency     C:\Windows\system32\KERNELBASE.dll
0x7ffa32dd0000        0x8e000 LoadReasonDynamicLoad          C:\Windows\system32\apphelp.dll
0x7ffa34b20000        0xa7000 LoadReasonStaticDependency     C:\Windows\system32\msvcrt.dll
0x7ffa35100000        0xc1000 LoadReasonStaticDependency     C:\Windows\system32\OLEAUT32.dll
0x7ffa35610000       0x1d6000 LoadReasonStaticDependency     C:\Windows\SYSTEM32\combase.dll
0x7ffa34170000        0x45000 LoadReasonStaticDependency     C:\Windows\SYSTEM32\powrprof.dll
0x7ffa35560000        0xa5000 LoadReasonStaticDependency     C:\Windows\SYSTEM32\advapi32.dll
0x7ffa36dd0000       0x171000 LoadReasonStaticDependency     C:\Windows\system32\USER32.dll
```

Memory Analysis with Rekall

Step 3: Network Connections

```
[1] xpaj_post.img 10:46:09> netscan output="c:\\tools\\netscan_xpaj.txt"
---------------------------> netscan(output="c:\\tools\\netscan_xpaj.txt")
                     Out<7> Plugin: netscan
```

Offset(P)	Proto	Local	Remote Address	State	PID	Process Name
0xb74258f0	TCPv4	10.0.0.3:49195	108.160.172.238:443	ESTABLISHED	2968	firefox.exe
0xb747acd0	TCPv4	10.0.0.3:49271	204.95.99.109:1980	CLOSED	2940	explorer.exe
0xb74d0df8	TCPv4	10.0.0.3:49297	204.95.99.109:1980	ESTABLISHED	2940	explorer.exe
0xb74f8bc8	TCPv6	-:49199	:::443	CLOSED	2968	firefox.exe
0xb7587008	TCPv4	-:49293	69.195.129.72:80	CLOSED	1584	winpmem_1.6.2.
0xb758c008	TCPv4	10.0.0.3:49295	204.95.99.109:1980	CLOSED	2940	explorer.exe
0xb7634ac8	TCPv4	-:49181	173.194.121.30:443	CLOSED	2968	firefox.exe
0xb79ae7b0	TCPv4	127.0.0.1:49165	127.0.0.1:49164	ESTABLISHED	2968	firefox.exe
0xb79b87c8	TCPv4	127.0.0.1:49164	127.0.0.1:49165	ESTABLISHED	2968	firefox.exe

Memory Analysis with Rekall

Step 4: Signs of Code Injection

```
Process: explorer.exe Pid: 2940 Address: 0x290000
Vad Tag: VadS Protection: EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

  0x290000 55 8b ec 83 c4 ec 56 57 8b 45 08 8b f0 8d 7d ec  U.....VW.E....}.
  0x290010 a5 a5 a5 a5 a5 ff 75 f8 ff 55 f4 ff 75 fc 50 ff  ......u..U..u.P.
  0x290020 55 f0 50 ff 55 ec 5f 5e 8b e5 5d c2 04 00 8b c0  U.P.U._^..].....
  0x290030 53 56 57 55 83 c4 e8 8b e9 8b fa 8b d8 33 f6 68  SVWU.........3.h

------  ------
    0x290000        0x0 55                    PUSH EBP
    0x290001        0x1 8bec                  MOV EBP, ESP
    0x290003        0x3 83c4ec                ADD ESP, -0x14
    0x290006        0x6 56                    PUSH ESI
    0x290007        0x7 57                    PUSH EDI
    0x290008        0x8 8b4508                MOV EAX, [EBP+0x8]
    0x29000b        0xb 8bf0                  MOV ESI, EAX
    0x29000d        0xd 8d7dec                LEA EDI, [EBP-0x14]
    0x290010       0x10 a5                    MOVSD
    0x290011       0x11 a5                    MOVSD
    0x290012       0x12 a5                    MOVSD
    0x290013       0x13 a5                    MOVSD
```

Memory Analysis with Rekall

Step 5: Detect Rootkit Behaviors

```
[1] xpaj_post.img 12:59:53> ssdt output="c:\\tools\\ssdt.txt"
---------------------------> ssdt(output="c:\\tools\\ssdt.txt")
                   Out<16> Plugin: ssdt
```

********** **** Table 0 @ 0x8289652c **********

Entry	Target	Symbol
0x0	0x82a9317e	ntlNtAcceptConnectPort
0x1	0x828d9995	ntlNtAccessCheck
0x2	0x82a22c19	ntlNtAccessCheckAndAuditAlarm
0x3	0x8283d88b	ntlNtAccessCheckByType
0x4	0x82a94a55	ntlNtAccessCheckByTypeAndAuditAlarm
0x5	0x829164de	ntlNtAccessCheckByTypeResultList
0x6	0x82b05903	ntlNtAccessCheckByTypeResultListAndAuditAlarm
0x7	0x82b0594c	ntlNtAccessCheckByTypeResultListAndAuditAlarmByHandle
0x8	0x82a17435	ntlNtAddAtom
0x9	0x82b1f20e	ntlNtAddBootEntry
0xa	0x82b20463	ntlNtAddDriverEntry
0xb	0x82a0dbe5	ntlNtAdjustGroupsToken

Memory Analysis with Rekall

Step 6: Acquisition of Notable Findings

```
[1] xpaj_post.img 13:45:56> procdump dump_dir="c:\\tools"
--------------------------> procdump(dump_dir="c:\\tools")
*****************************************************
```

```
Dumping wuauclt.exe, pid: 2584   output: executable.wuauclt_exe_2584.exe
*****************************************************
Dumping explorer.exe, pid: 2940   output: executable.explorer_exe_2940.exe
*****************************************************
Dumping firefox.exe, pid: 2968   output: executable.firefox_exe_2968.exe
*****************************************************
Dumping taskhost.exe, pid: 3708   output: executable.taskhost_exe_3708.exe
*****************************************************
Dumping conhost.exe, pid: 3904   output: executable.conhost_exe_3904.exe
*****************************************************
Dumping taskhost.exe, pid: 3976   output: executable.taskhost_exe_3976.exe
*****************************************************
Dumping efsui.exe, pid: 4020   output: executable.efsui_exe_4020.exe
                    Out<18> Plugin: procdump
```

Live Analysis with Rekall (1)

Step 1

Winpmem allows for live memory analysis with manual loading of the kernel module

```
c:\Program Files\Rekall>winpmem_2.0.1.exe -l
Driver Unloaded.
CR3: 0x00001A7000
 4 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0xBFDE0000
Start 0xBFF00000 - Length 0x00100000
Start 0x100000000 - Length 0x40000000
Memory access driver left loaded since you specified t
```

Live Analysis with Rekall (2)

Step 2

Point to \\.\pmem to begin live analysis

```
c:\Program Files\Rekall>rekal.exe -f \\.\pmem

----------------------------------------------------------------------
The Rekall Memory Forensic framework 1.4.0.pre3 (Etzel).

"We can remember it for you wholesale!"

This program is free software; you can redistribute it and/or modify it
the terms of the GNU General Public License.

See http://www.rekall-forensic.com/docs/Manual/tutorial.html to get star
----------------------------------------------------------------------
[1] Default session 14:15:58> _
```

Live Analysis with Rekall (3)

Step 3

Acquisition

Memory acquisition plugin - aff4acquire

```
[1] Default session 18:55:02> aff4acquire destination="output.aff4"
----------------------------> aff4acquire(destination="output.aff4")
Will use compression: https://github.com/google/snappy
Imaging Physical Memory:s 0x1000 -
Wrote 4102 mb of Physical Memory to aff4://811edbc7-090f-447e-ad07-bd9d4
Imaging pagefile C:\pagefile.sys
Wrote pagefile.sys (4500 mb)0000 (4712 total) (65 Mb/s)
Imaging pagefile C:\swapfile.sys
Wrote swapfile.sys (256 mb)000 (192 total) (69 Mb/s)
                        Out<4> Plugin: aff4acquire
```