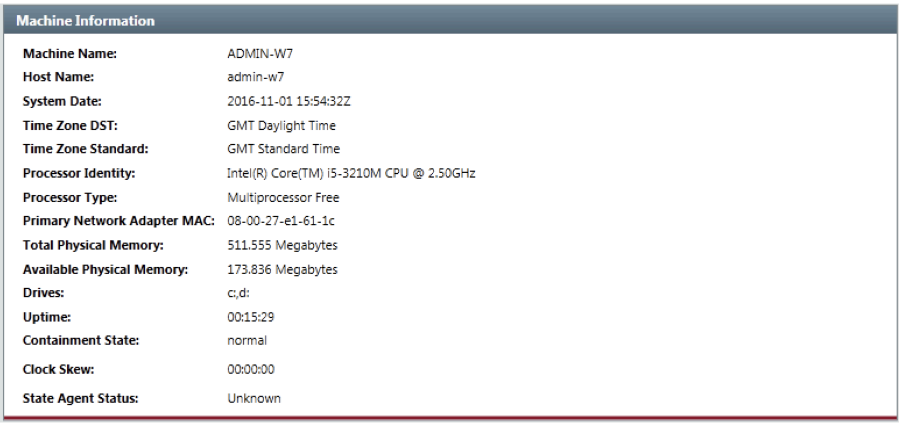
Windows using Redline

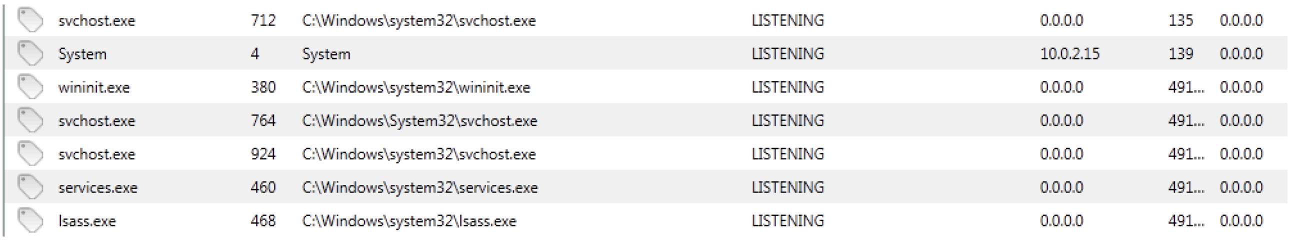
1. The system date and time.



Machine Information

Machine Name:	ADMIN-W7
Host Name:	admin-w7
System Date:	2016-11-01 15:54:32Z
Time Zone DST:	GMT Daylight Time
Time Zone Standard:	GMT Standard Time
Processor Identity:	Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz
Processor Type:	Multiprocessor Free
Primary Network Adapter MAC:	08-00-27-e1-61-1c
Total Physical Memory:	511.555 Megabytes
Available Physical Memory:	173.836 Megabytes
Drives:	c:,d:
Uptime:	00:15:29
Containment State:	normal
Clock Skew:	00:00:00
State Agent Status:	Unknown

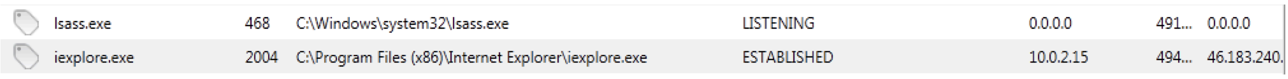
2. Current network connections.
The process name, the state of the port can be viewed. Other information such as the local ip address and remote ip address where stored in the dump for each of the processes.



svchost.exe	712	C:\Windows\system32\svchost.exe	LISTENING	0.0.0.0	135	0.0.0.0
System	4	System	LISTENING	10.0.2.15	139	0.0.0.0
wininit.exe	380	C:\Windows\system32\wininit.exe	LISTENING	0.0.0.0	491...	0.0.0.0
svchost.exe	764	C:\Windows\System32\svchost.exe	LISTENING	0.0.0.0	491...	0.0.0.0
svchost.exe	924	C:\Windows\system32\svchost.exe	LISTENING	0.0.0.0	491...	0.0.0.0
services.exe	460	C:\Windows\system32\services.exe	LISTENING	0.0.0.0	491...	0.0.0.0
lsass.exe	468	C:\Windows\system32\lsass.exe	LISTENING	0.0.0.0	491...	0.0.0.0

3. Open TCP or UDP ports.

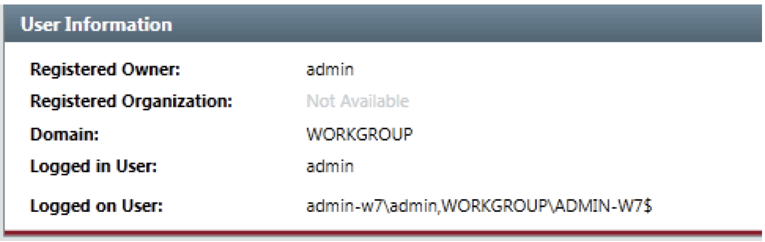
The evidence retrieved can see what ports are open. The protocols callalso be indemnified and what processes is opening the port can be retrieved as see from the image below. The process “iexplore.exe” has established a connection. Information such as the local ip address, the local port, the remote ip and the remote port is recorded.



lsass.exe	468	C:\Windows\system32\lsass.exe	LISTENING	0.0.0.0	491...	0.0.0.0
iexplore.exe	2004	C:\Program Files (x86)\Internet Explorer\iexplore.exe	ESTABLISHED	10.0.2.15	494...	46.183.240.

4. Cached NetBIOS name table.

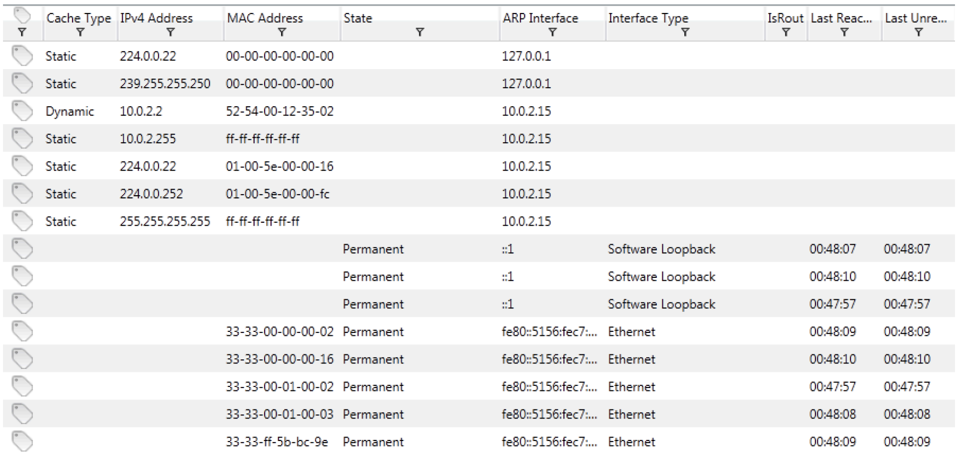
5. Users currently logged in.
Redline provides the functionality to see user information. Information such as what user was logged in, the same of the user is recorded.



User Information

Registered Owner:	admin
Registered Organization:	Not Available
Domain:	WORKGROUP
Logged in User:	admin
Logged on User:	admin-w7\admin,WORKGROUP\ADMIN-W7$

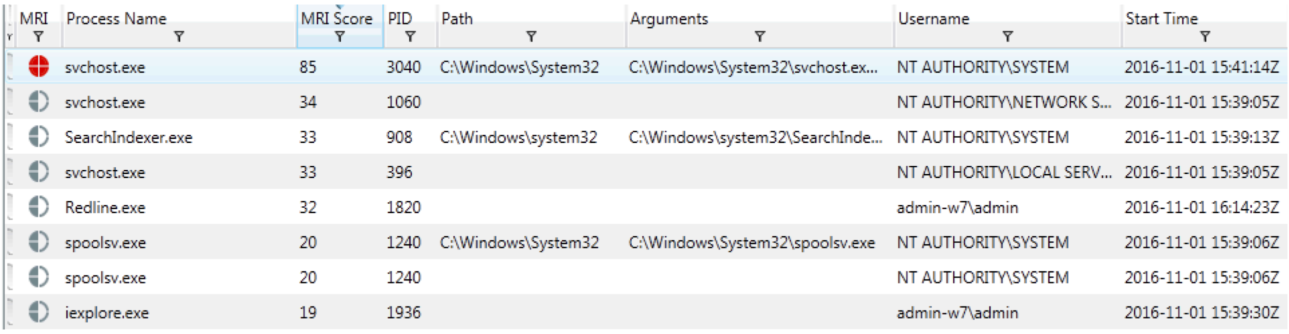
6. The intern routing table.



	Cache Type	IPv4 Address	MAC Address	State	ARP Interface	Interface Type	IsRout	Last Reac...	Last Unre...
	Static	224.0.0.22	00-00-00-00-00-00		127.0.0.1				
	Static	239.255.255.250	00-00-00-00-00-00		127.0.0.1				
	Dynamic	10.0.2.2	52-54-00-12-35-02		10.0.2.15				
	Static	10.0.2.255	ff-ff-ff-ff-ff-ff		10.0.2.15				
	Static	224.0.0.22	01-00-5e-00-00-16		10.0.2.15				
	Static	224.0.0.252	01-00-5e-00-00-fc		10.0.2.15				
	Static	255.255.255.255	ff-ff-ff-ff-ff-ff		10.0.2.15				
				Permanent	::1	Software Loopback		00:48:07	00:48:07
				Permanent	::1	Software Loopback		00:48:10	00:48:10
				Permanent	::1	Software Loopback		00:47:57	00:47:57
			33-33-00-00-00-02	Permanent	fe80::5156:fec7:...	Ethernet		00:48:09	00:48:09
			33-33-00-00-00-16	Permanent	fe80::5156:fec7:...	Ethernet		00:48:10	00:48:10
			33-33-00-01-00-02	Permanent	fe80::5156:fec7:...	Ethernet		00:47:57	00:47:57
			33-33-00-01-00-03	Permanent	fe80::5156:fec7:...	Ethernet		00:48:08	00:48:08
			33-33-ff-5b-bc-9e	Permanent	fe80::5156:fec7:...	Ethernet		00:48:09	00:48:09

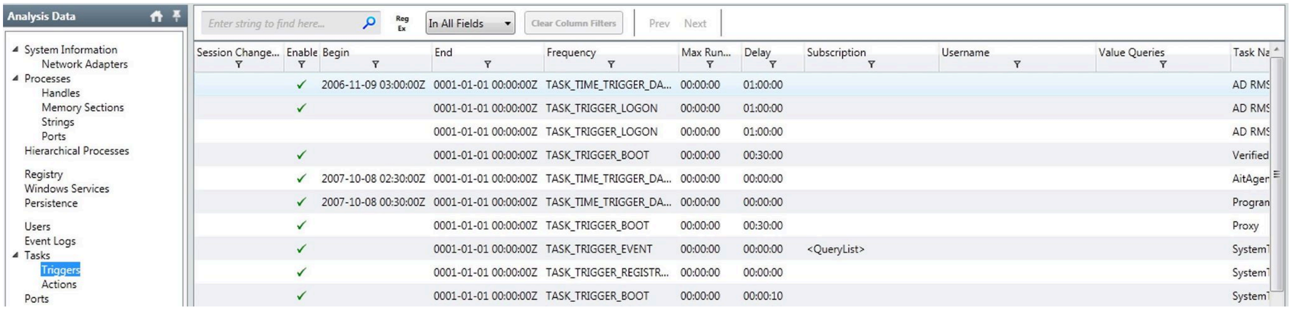
7. Running processes.

Redline provides the option to view all the running processes on the machine when the memory dump was collected. The process name, path to the process and the start time are recorded. This is useful for forensic and it provides clear information on what process were happening.



MRI	Process Name	MRI Score	PID	Path	Arguments	Username	Start Time
●	svchost.exe	85	3040	C:\Windows\System32	C:\Windows\System32\svchost.ex...	NT AUTHORITY\SYSTEM	2016-11-01 15:41:14Z
◐	svchost.exe	34	1060			NT AUTHORITY\NETWORK S...	2016-11-01 15:39:05Z
◐	SearchIndexer.exe	33	908	C:\Windows\system32	C:\Windows\system32\SearchInde...	NT AUTHORITY\SYSTEM	2016-11-01 15:39:13Z
◐	svchost.exe	33	396			NT AUTHORITY\LOCAL SERV...	2016-11-01 15:39:05Z
◐	Redline.exe	32	1820			admin-w7\admin	2016-11-01 16:14:23Z
◐	spoolsv.exe	20	1240	C:\Windows\System32	C:\Windows\System32\spoolsv.exe	NT AUTHORITY\SYSTEM	2016-11-01 15:39:06Z
◐	spoolsv.exe	20	1240			NT AUTHORITY\SYSTEM	2016-11-01 15:39:06Z
◐	iexplore.exe	19	1936			admin-w7\admin	2016-11-01 15:39:30Z

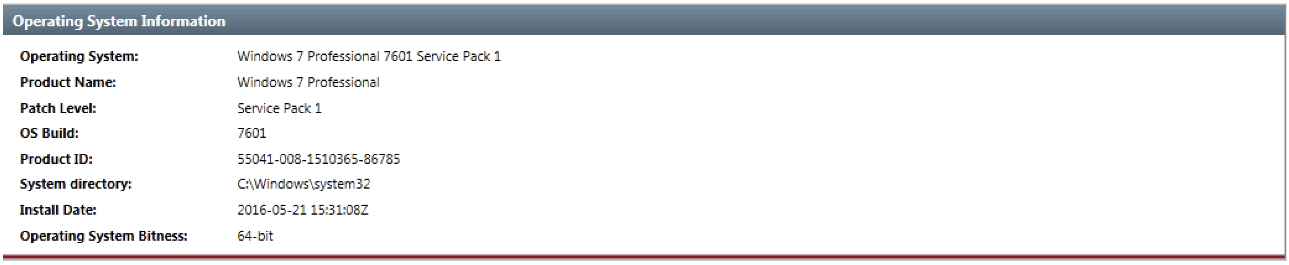
8. Schedule Jobs.
Redline retrieved the information of processes to take place. It returns information such as when the process should begin and end. Providing the date and time. Other information retrieved back is the process name. This information can be retrieved under the trigger section in the process task.



Session Change...	Enable	Begin	End	Frequency	Max Run...	Delay	Subscription	Username	Value Queries	Task Na
	✓	2006-11-09 03:00:00Z	0001-01-01 00:00:00Z	TASK_TIME_TRIGGER_DA...	00:00:00	01:00:00				AD RMS
	✓		0001-01-01 00:00:00Z	TASK_TRIGGER_LOGON	00:00:00	01:00:00				AD RMS
			0001-01-01 00:00:00Z	TASK_TRIGGER_LOGON	00:00:00	01:00:00				AD RMS
	✓		0001-01-01 00:00:00Z	TASK_TRIGGER_BOOT	00:00:00	00:30:00				Verified
	✓	2007-10-08 02:30:00Z	0001-01-01 00:00:00Z	TASK_TIME_TRIGGER_DA...	00:00:00	00:00:00				AitAger
	✓	2007-10-08 00:30:00Z	0001-01-01 00:00:00Z	TASK_TIME_TRIGGER_DA...	00:00:00	00:00:00				Progran
	✓		0001-01-01 00:00:00Z	TASK_TRIGGER_BOOT	00:00:00	00:30:00				Proxy
	✓		0001-01-01 00:00:00Z	TASK_TRIGGER_EVENT	00:00:00	00:00:00	<QueryList>			SystemT
	✓		0001-01-01 00:00:00Z	TASK_TRIGGER_REGISTR...	00:00:00	00:00:00				SystemT
	✓		0001-01-01 00:00:00Z	TASK_TRIGGER_BOOT	00:00:00	00:00:10				SystemT

Nonvolatile data

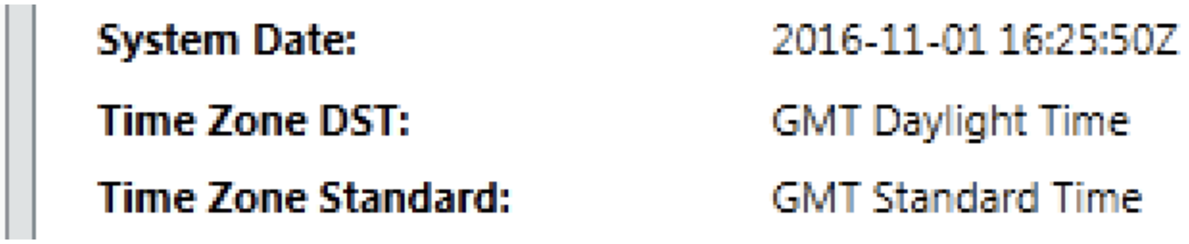
1. System version and path level.



Operating System Information

Operating System:	Windows 7 Professional 7601 Service Pack 1
Product Name:	Windows 7 Professional
Patch Level:	Service Pack 1
OS Build:	7601
Product ID:	55041-008-1510365-86785
System directory:	C:\Windows\system32
Install Date:	2016-05-21 15:31:08Z
Operating System Bitness:	64-bit

2. File system and date stamp

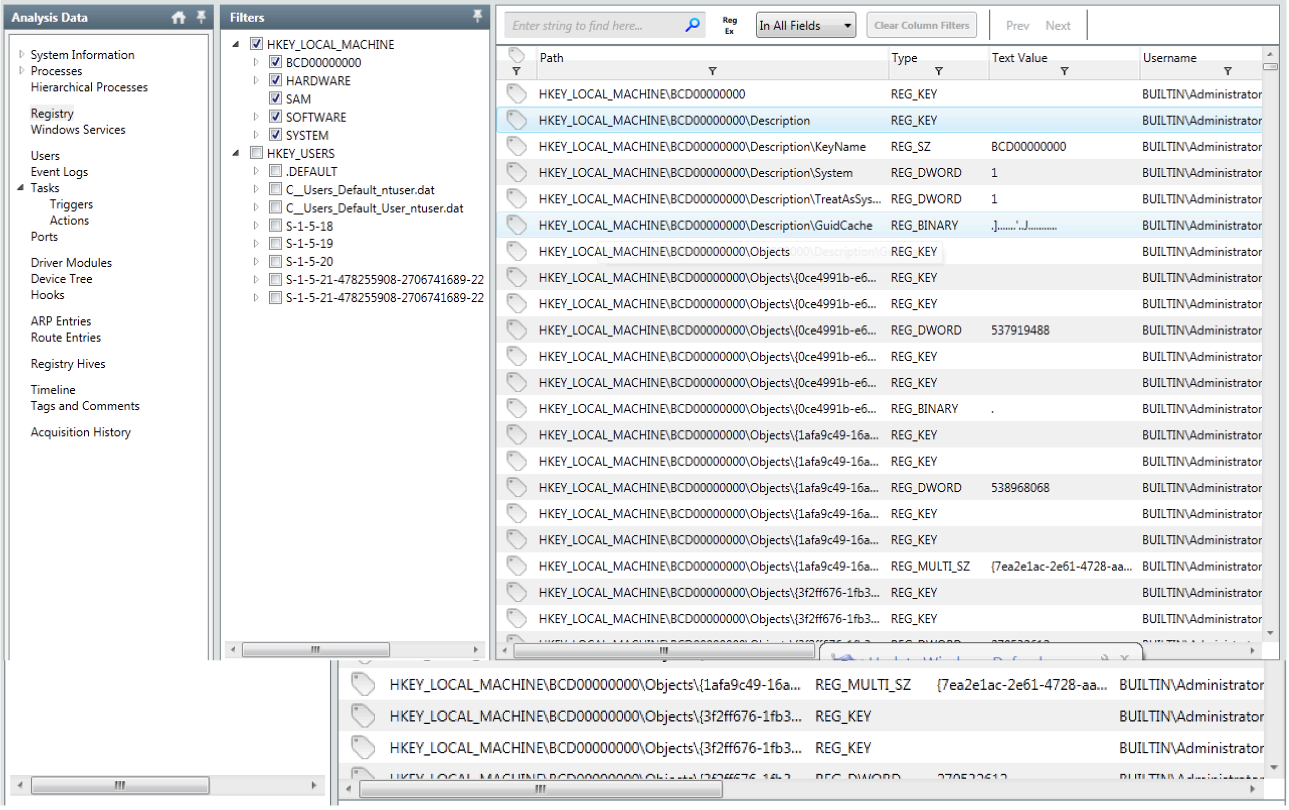


System Date:	2016-11-01 16:25:50Z
Time Zone DST:	GMT Daylight Time
Time Zone Standard:	GMT Standard Time

3. Registry data.
The following evidence can be retrieved using the redline tool. Information returned to the user is about the Operating system, information about applications, drivers, network interfaces.
pdf

4. The auditing policy.

5. The history of logins
The screen shot below can inform investigators when the last time a user was logged in. From the screenshot below, we can see that the last time “admin” logged in was on “2016-11-01” and the time was “15:39”. This information could provide investigators with a timeline incase something suspicious happened on a machine, investigators could identify a user who was logged into he system when something suspicious was happening.

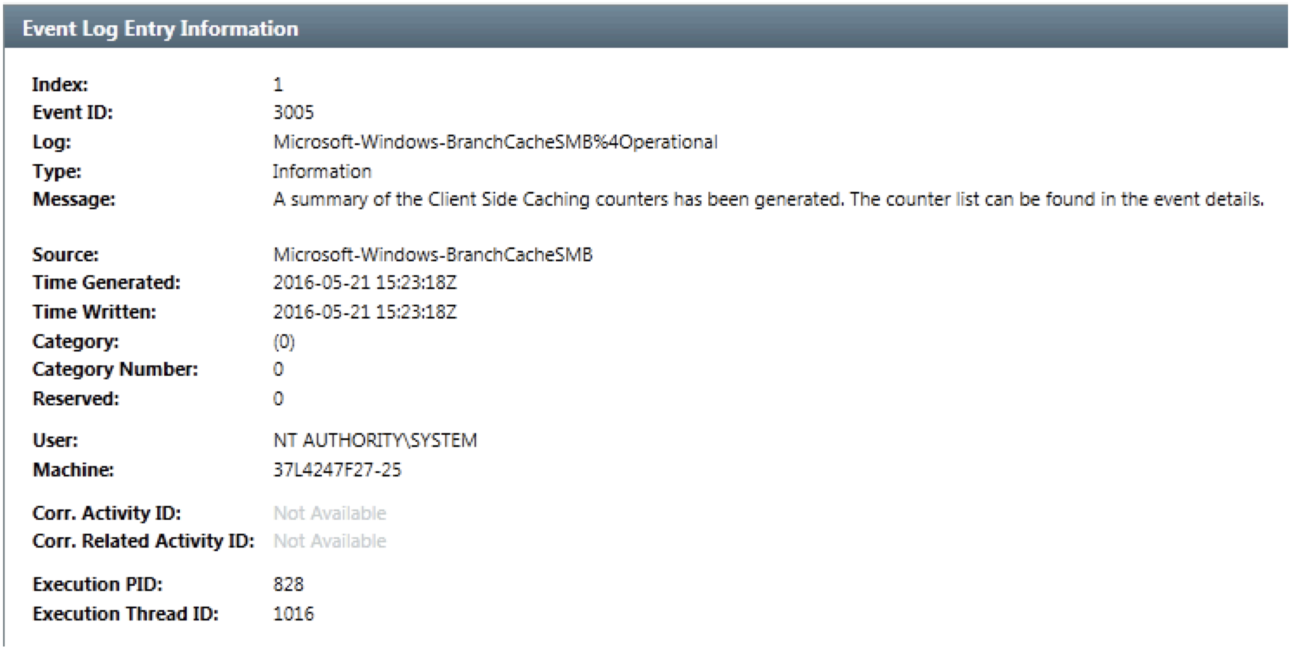


Path	Type	Text Value	Username
HKEY_LOCAL_MACHINE\BCD00000000	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Description	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Description\KeyName	REG_SZ	BCD00000000	BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Description\System	REG_DWORD	1	BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Description\TreatAsSys...	REG_DWORD	1	BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Description\GuidCache	REG_BINARY	.]......'..J..........	BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{0ce4991b-e6...	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{0ce4991b-e6...	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{0ce4991b-e6...	REG_DWORD	537919488	BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{0ce4991b-e6...	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{0ce4991b-e6...	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{0ce4991b-e6...	REG_BINARY	.	BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{1afa9c49-16a...	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{1afa9c49-16a...	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{1afa9c49-16a...	REG_DWORD	538968068	BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{1afa9c49-16a...	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{1afa9c49-16a...	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{1afa9c49-16a...	REG_MULTI_SZ	{7ea2e1ac-2e61-4728-aa...	BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{3f2ff676-1fb3...	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{3f2ff676-1fb3...	REG_KEY		BUILTIN\Administrator

HKEY_LOCAL_MACHINE\BCD00000000\Objects\{1afa9c49-16a...	REG_MULTI_SZ	{7ea2e1ac-2e61-4728-aa...	BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{3f2ff676-1fb3...	REG_KEY		BUILTIN\Administrator
HKEY_LOCAL_MACHINE\BCD00000000\Objects\{3f2ff676-1fb3...	REG_KEY		BUILTIN\Administrator

6.System event logs

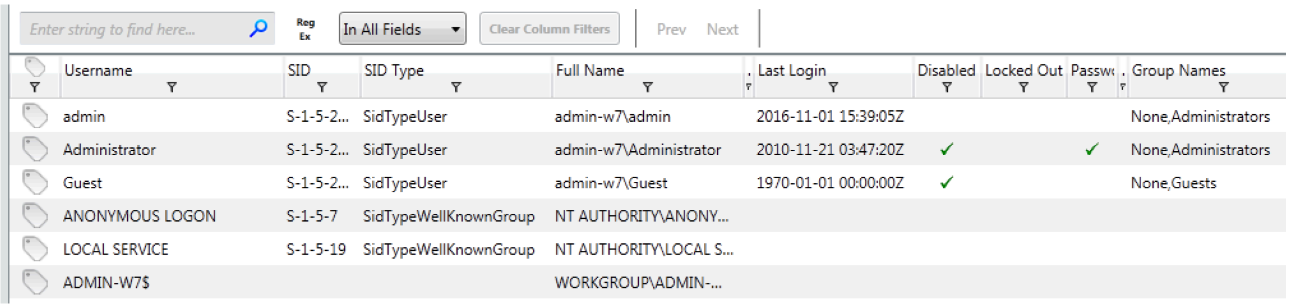
Redline was configured to collect the system even logs, the event id, the log, type and message are recorded.
The following image is an example of an event log been recorded using Redline. The event id is 3005, the machine name and the user for which when the event was logged is recorded. This type of event is an "Information" and the time is also recorded when is was generated and written.



Event Log Entry Information

Index:	1
Event ID:	3005
Log:	Microsoft-Windows-BranchCacheSMB%4Operational
Type:	Information
Message:	A summary of the Client Side Caching counters has been generated. The counter list can be found in the event details.
Source:	Microsoft-Windows-BranchCacheSMB
Time Generated:	2016-05-21 15:23:18Z
Time Written:	2016-05-21 15:23:18Z
Category:	(0)
Category Number:	0
Reserved:	0
User:	NT AUTHORITY\SYSTEM
Machine:	37L4247F27-25
Corr. Activity ID:	Not Available
Corr. Related Activity ID:	Not Available
Execution PID:	828
Execution Thread ID:	1016

7.User accounts.
Redline was able to analyse the data of the users on the system. Information such as the usernames, the last time a specific user was logged in, does the user require a password in order to log in and which group the user belongs to such as Administrator or Guest. This information can be useful to investigators to identify the time the last time a user was logged in or to see how many users exist on the machine.



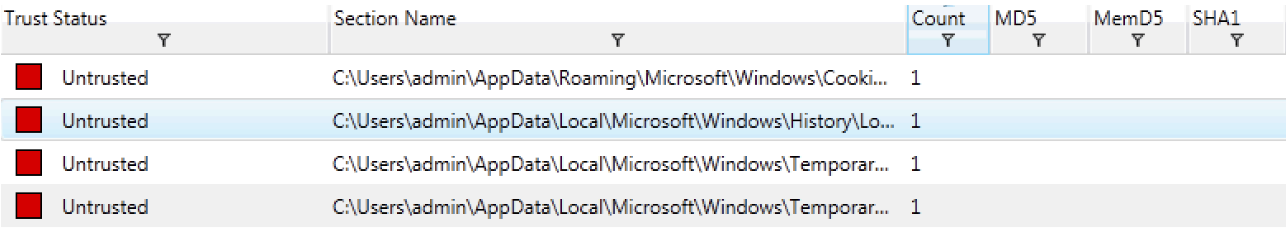
Username	SID	SID Type	Full Name	.	Last Login	Disabled	Locked Out	Passw	.	Group Names
admin	S-1-5-2...	SidTypeUser	admin-w7\admin		2016-11-01 15:39:05Z					None,Administrators
Administrator	S-1-5-2...	SidTypeUser	admin-w7\Administrator		2010-11-21 03:47:20Z	✓		✓		None,Administrators
Guest	S-1-5-2...	SidTypeUser	admin-w7\Guest		1970-01-01 00:00:00Z	✓				None,Guests
ANONYMOUS LOGON	S-1-5-7	SidTypeWellKnownGroup	NT AUTHORITY\ANONY...							
LOCAL SERVICE	S-1-5-19	SidTypeWellKnownGroup	NT AUTHORITY\LOCAL S...							
ADMIN-W7$			WORKGROUP\ADMIN-...							

8. IIS logs

9.Suspicious files

Under the processes tab, there is memory selection in redline. This tab will allow a user to identify running or completed tasks. Named memory selections are those that are mapped to files. Malware are not normally signed and are usually loaded by a single process.

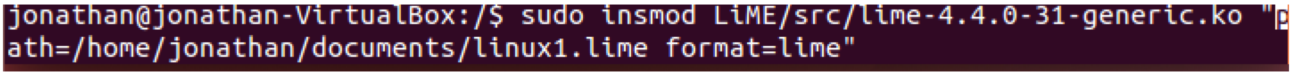
The below screenshot displays processes that are untrusted on my system. Depending on the process, malware could be present.



Trust Status	Section Name	Count	MD5	MemD5	SHA1
🟥 Untrusted	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cooki...	1			
🟥 Untrusted	C:\Users\admin\AppData\Local\Microsoft\Windows\History\Lo...	1			
🟥 Untrusted	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporar...	1			
🟥 Untrusted	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporar...	1			

Linux Live Response

To collect a live response of a linux machine, I used the tool called “Lime”. The following is how to create a linux live response. First we clone the lime from github. Once cloned, I went to the following path LIME/src. Using Linux command “make”, this compiles the files and returns .ko file.



```
jonathan@jonathan-VirtualBox:/$ sudo insmod LiME/src/lime-4.4.0-31-generic.ko "p
ath=/home/jonathan/documents/linux1.lime format=lime"
```

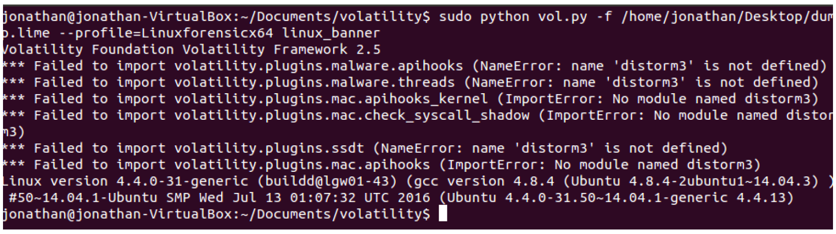
The above command will create a dump of the linux machine called linux1.lime.

Analysing volatile data

1. The system date and time.

Command: linux_banner

This command can be used to retrieve the date and time from the Linux machine. Also, other information such as the Operating system which is been used and the version can be retrieved. From the screenshot below, we can identify that the date and time was July 13 and the OS was Ubuntu version 14.04.1. The patch level of the OS is also viewable.

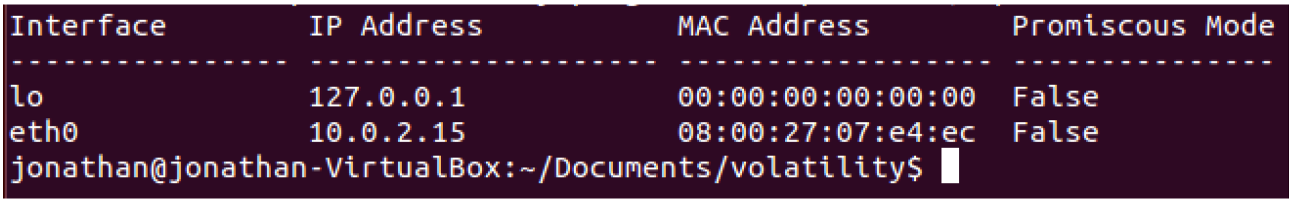


```
jonathan@jonathan-VirtualBox:~/Documents/volatility$ sudo python vol.py -f /home/jonathan/Desktop/dum
p.lime --profile=Linuxforensicx64 linux_banner
Volatility Foundation Volatility Framework 2.5
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distor
m3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Linux version 4.4.0-31-generic (buildd@lgw01-43) (gcc version 4.8.4 (Ubuntu 4.8.4-2ubuntu1~14.04.3) )
 #50~14.04.1-Ubuntu SMP Wed Jul 13 01:07:32 UTC 2016 (Ubuntu 4.4.0-31.50~14.04.1-generic 4.4.13)
jonathan@jonathan-VirtualBox:~/Documents/volatility$
```

2. Current network connections.

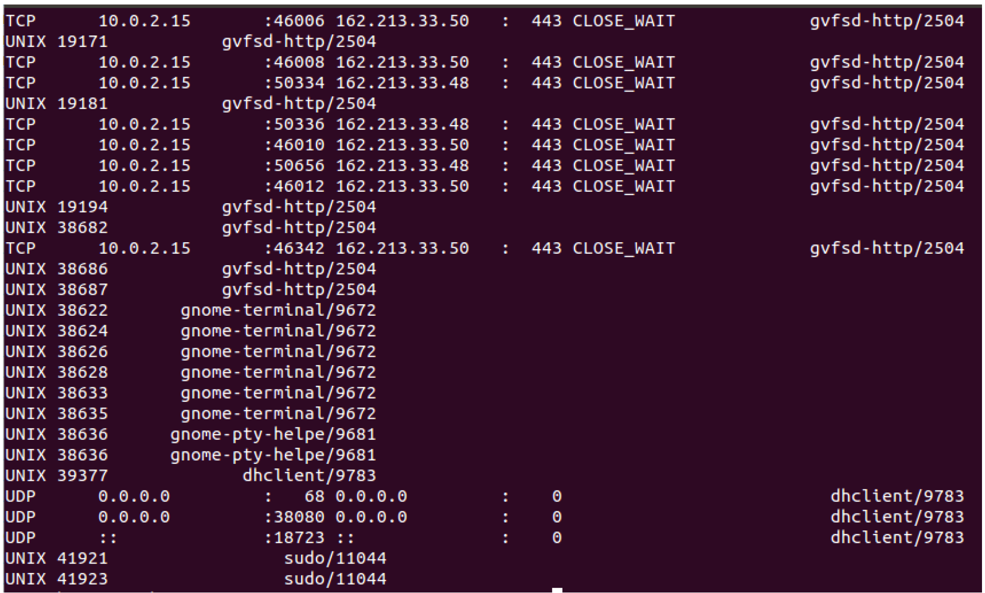
Command: linux_ifconfig

Plugin allows the user to see the active interfaces for the computer. Information such as the IP address, MAC address and promiscuous mode can be viewed.



```
Interface        IP Address           MAC Address        Promiscous Mode
---------------- -------------------- ------------------ ---------------
lo               127.0.0.1            00:00:00:00:00:00  False
eth0             10.0.2.15            08:00:27:07:e4:ec  False
jonathan@jonathan-VirtualBox:~/Documents/volatility$
```

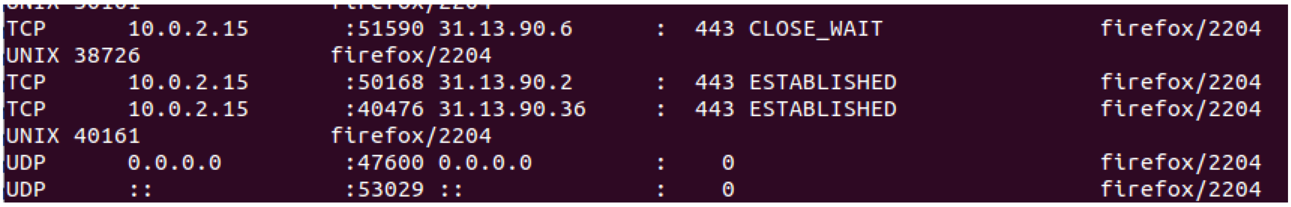
3. Open TCP or UDP port



```
TCP      10.0.2.15       :46006 162.213.33.50   :  443 CLOSE_WAIT          gvfsd-http/2504
UNIX 19171            gvfsd-http/2504
TCP      10.0.2.15       :46008 162.213.33.50   :  443 CLOSE_WAIT          gvfsd-http/2504
TCP      10.0.2.15       :50334 162.213.33.48   :  443 CLOSE_WAIT          gvfsd-http/2504
UNIX 19181            gvfsd-http/2504
TCP      10.0.2.15       :50336 162.213.33.48   :  443 CLOSE_WAIT          gvfsd-http/2504
TCP      10.0.2.15       :46010 162.213.33.50   :  443 CLOSE_WAIT          gvfsd-http/2504
TCP      10.0.2.15       :50656 162.213.33.48   :  443 CLOSE_WAIT          gvfsd-http/2504
TCP      10.0.2.15       :46012 162.213.33.50   :  443 CLOSE_WAIT          gvfsd-http/2504
UNIX 19194            gvfsd-http/2504
UNIX 38682            gvfsd-http/2504
TCP      10.0.2.15       :46342 162.213.33.50   :  443 CLOSE_WAIT          gvfsd-http/2504
UNIX 38686            gvfsd-http/2504
UNIX 38687            gvfsd-http/2504
UNIX 38622        gnome-terminal/9672
UNIX 38624        gnome-terminal/9672
UNIX 38626        gnome-terminal/9672
UNIX 38628        gnome-terminal/9672
UNIX 38633        gnome-terminal/9672
UNIX 38635        gnome-terminal/9672
UNIX 38636       gnome-pty-helpe/9681
UNIX 38636       gnome-pty-helpe/9681
UNIX 39377              dhclient/9783
UDP      0.0.0.0         :   68 0.0.0.0         :    0                       dhclient/9783
UDP      0.0.0.0         :38080 0.0.0.0         :    0                       dhclient/9783
UDP      ::              :18723 ::              :    0                       dhclient/9783
UNIX 41921                  sudo/11044
UNIX 41923                  sudo/11044
```

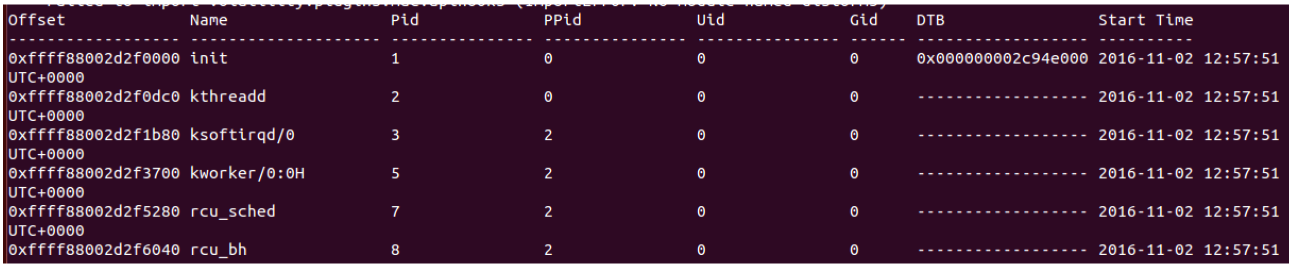
Command:

4. Which executables are opening TCP or UDP ports
Command: linux_netstat
The above command allows the User to see what ports are been opened by what programs.



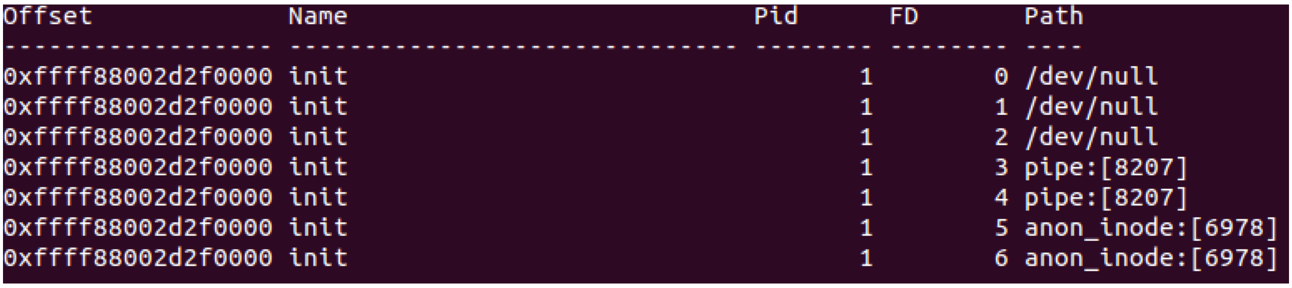
```
TCP      10.0.2.15       :51590 31.13.90.6      :  443 CLOSE_WAIT                firefox/2204
UNIX 38726              firefox/2204
TCP      10.0.2.15       :50168 31.13.90.2      :  443 ESTABLISHED               firefox/2204
TCP      10.0.2.15       :40476 31.13.90.36     :  443 ESTABLISHED               firefox/2204
UNIX 40161              firefox/2204
UDP      0.0.0.0         :47600 0.0.0.0         :    0                           firefox/2204
UDP      ::              :53029 ::              :    0                           firefox/2204
```

5 Running processes
Command: linux_pslist
The following plugin displays the list of active processes when the live memory dump was been collected. The name of the process and the start time of the process in my opinion are important information that can be retrieved from this plugin. It can provide information to an investigator on what processes where been performed on a machine.



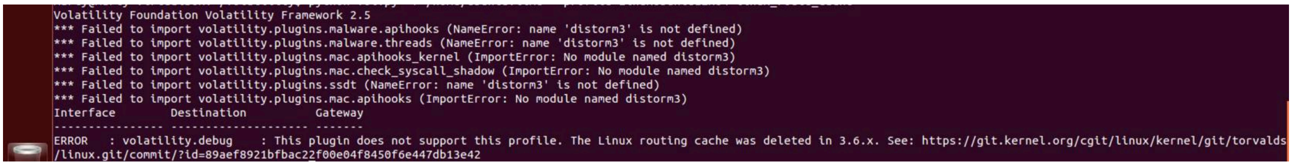
```
Offset             Name                 Pid             PPid            Uid             Gid    DTB                Start Time
------------------ -------------------- --------------- --------------- --------------- ------ ------------------ ----------
0xffff88002d2f0000 init                 1               0               0               0      0x000000002c94e000 2016-11-02 12:57:51
UTC+0000
0xffff88002d2f0dc0 kthreadd             2               0               0               0      ------------------ 2016-11-02 12:57:51
UTC+0000
0xffff88002d2f1b80 ksoftirqd/0          3               2               0               0      ------------------ 2016-11-02 12:57:51
UTC+0000
0xffff88002d2f3700 kworker/0:0H         5               2               0               0      ------------------ 2016-11-02 12:57:51
UTC+0000
0xffff88002d2f5280 rcu_sched            7               2               0               0      ------------------ 2016-11-02 12:57:51
UTC+0000
0xffff88002d2f6040 rcu_bh               8               2               0               0      ------------------ 2016-11-02 12:57:51
```

6. Open files
Command: linux_lsof
The following plugin prints a list of open file descriptors and the paths to their for each of their running process.



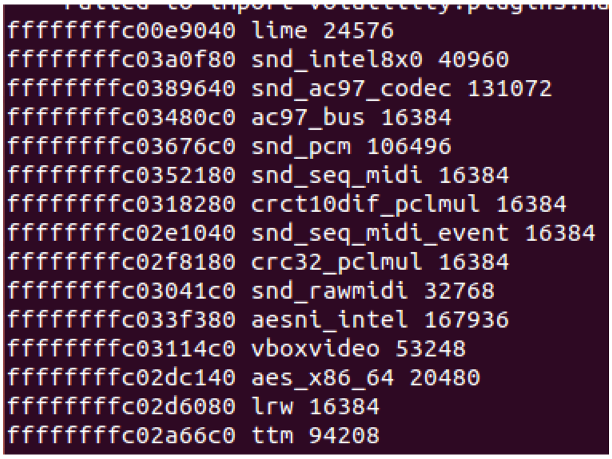
```
Offset             Name                           Pid      FD       Path
------------------ ------------------------------ -------- -------- ----
0xffff88002d2f0000 init                                  1        0 /dev/null
0xffff88002d2f0000 init                                  1        1 /dev/null
0xffff88002d2f0000 init                                  1        2 /dev/null
0xffff88002d2f0000 init                                  1        3 pipe:[8207]
0xffff88002d2f0000 init                                  1        4 pipe:[8207]
0xffff88002d2f0000 init                                  1        5 anon_inode:[6978]
0xffff88002d2f0000 init                                  1        6 anon_inode:[6978]
```

7. The internal routing table
Command: linux_route_cache



```
Volatility Foundation Volatility Framework 2.5
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Interface        Destination          Gateway
---------------- -------------------- -------
ERROR   : volatility.debug    : This plugin does not support this profile. The Linux routing cache was deleted in 3.6.x. See: https://git.kernel.org/cgit/linux/kernel/git/torvalds
/linux.git/commit/?id=89aef8921bfbac22f00e04f8450f6e447db13e42
```

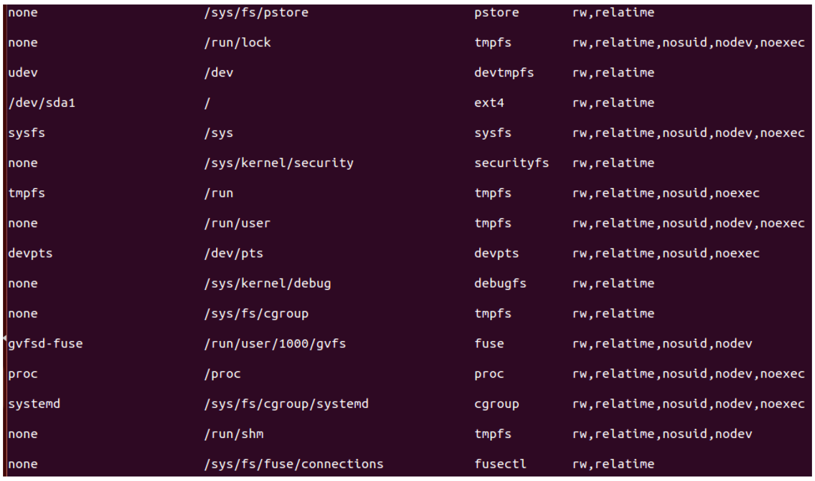
8. Loaded kernel modules
Command: linux_lsmod
The plugin prints a list of loaded kernel modules in the terminal. From the image below, information such as how many modules have been loaded can be identified. The Lime module is 24576 bytes while the ttm module is 94208 bytes.



```
ffffffffc00e9040 lime 24576
ffffffffc03a0f80 snd_intel8x0 40960
ffffffffc0389640 snd_ac97_codec 131072
ffffffffc03480c0 ac97_bus 16384
ffffffffc03676c0 snd_pcm 106496
ffffffffc0352180 snd_seq_midi 16384
ffffffffc0318280 crct10dif_pclmul 16384
ffffffffc02e1040 snd_seq_midi_event 16384
ffffffffc02f8180 crc32_pclmul 16384
ffffffffc03041c0 snd_rawmidi 32768
ffffffffc033f380 aesni_intel 167936
ffffffffc03114c0 vboxvideo 53248
ffffffffc02dc140 aes_x86_64 20480
ffffffffc02d6080 lrw 16384
ffffffffc02a66c0 ttm 94208
```

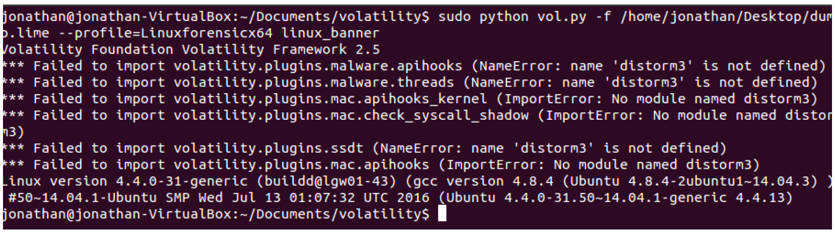
9. Mounted file systems
Command: linux_mount

For each mountpoint it prints the flags, mounted source and the path to where its it mounted too.



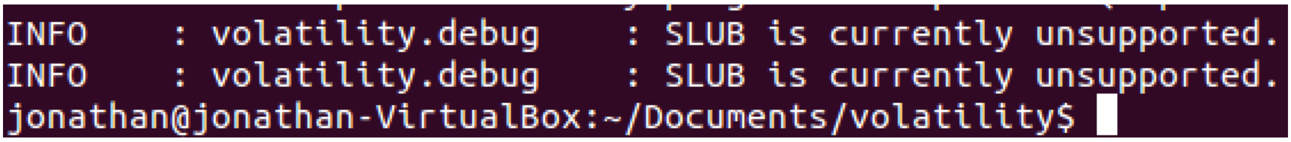
```
none                    /sys/fs/pstore                    pstore       rw,relatime
none                    /run/lock                         tmpfs        rw,relatime,nosuid,nodev,noexec
udev                    /dev                              devtmpfs     rw,relatime
/dev/sda1               /                                 ext4         rw,relatime
sysfs                   /sys                              sysfs        rw,relatime,nosuid,nodev,noexec
none                    /sys/kernel/security              securityfs   rw,relatime
tmpfs                   /run                              tmpfs        rw,relatime,nosuid,noexec
none                    /run/user                         tmpfs        rw,relatime,nosuid,nodev,noexec
devpts                  /dev/pts                          devpts       rw,relatime,nosuid,noexec
none                    /sys/kernel/debug                 debugfs      rw,relatime
none                    /sys/fs/cgroup                    tmpfs        rw,relatime
gvfsd-fuse              /run/user/1000/gvfs               fuse         rw,relatime,nosuid,nodev
proc                    /proc                             proc         rw,relatime,nosuid,nodev,noexec
systemd                 /sys/fs/cgroup/systemd            cgroup       rw,relatime,nosuid,nodev,noexec
none                    /run/shm                          tmpfs        rw,relatime,nosuid,nodev
none                    /sys/fs/fuse/connections          fusectl      rw,relatime
```

Non volatile Data.
System version and patch level. the command linux_banner will display this information.
As we can see from the image below, the system version is 14.04.1 Ubuntu and the patch level is 4.4.13. This command can also display the file system time and data stamp.



```
jonathan@jonathan-VirtualBox:~/Documents/volatility$ sudo python vol.py -f /home/jonathan/Desktop/dum
p.lime --profile=Linuxforensicx64 linux_banner
Volatility Foundation Volatility Framework 2.5
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distor
m3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Linux version 4.4.0-31-generic (buildd@lgw01-43) (gcc version 4.8.4 (Ubuntu 4.8.4-2ubuntu1~14.04.3) )
 #50~14.04.1-Ubuntu SMP Wed Jul 13 01:07:32 UTC 2016 (Ubuntu 4.4.0-31.50~14.04.1-generic 4.4.13)
jonathan@jonathan-VirtualBox:~/Documents/volatility$ 
```

File system MD5 checksum values, the plugin I would of used in linux_dentry_cache, but it is unsupported on volatility framework 2.5 which is the latest. This plugin recovers the filesystem in the memory for each mount and can also recover deleted files. It outputs the MD5 of files.

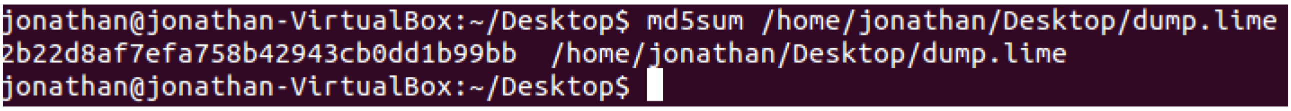


```
INFO    : volatility.debug    : SLUB is currently unsupported.
INFO    : volatility.debug    : SLUB is currently unsupported.
jonathan@jonathan-VirtualBox:~/Documents/volatility$
```

Users currently logged in.
There is no plugin to view the users who are currently logged in for volatility.

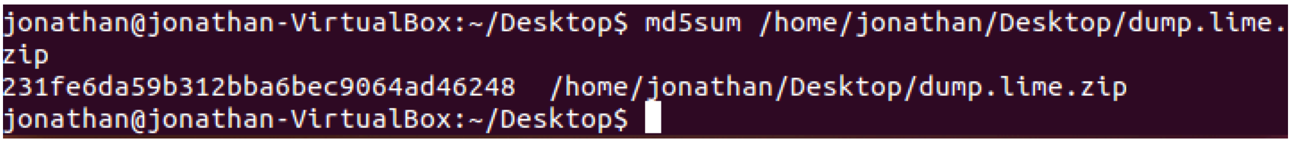
Integrity of files using hash algorithm.

For Linux live response.
lime.dump hash value.



```
jonathan@jonathan-VirtualBox:~/Desktop$ md5sum /home/jonathan/Desktop/dump.lime
2b22d8af7efa758b42943cb0dd1b99bb  /home/jonathan/Desktop/dump.lime
jonathan@jonathan-VirtualBox:~/Desktop$
```

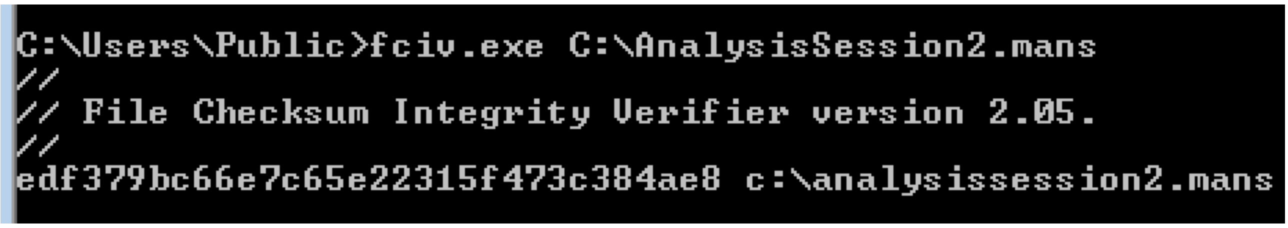
Hash value for compress zipped file.



```
jonathan@jonathan-VirtualBox:~/Desktop$ md5sum /home/jonathan/Desktop/dump.lime.
zip
231fe6da59b312bba6bec9064ad46248  /home/jonathan/Desktop/dump.lime.zip
jonathan@jonathan-VirtualBox:~/Desktop$
```

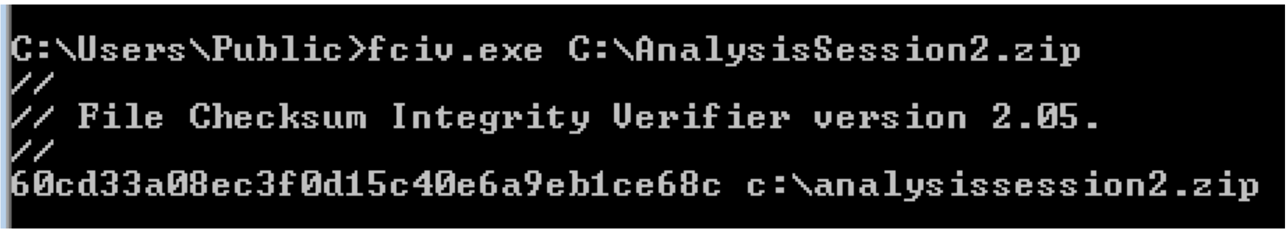
For Windows Live response.

AnalysisSession2.mans Hash value.



```
C:\Users\Public>fciv.exe C:\AnalysisSession2.mans
//
// File Checksum Integrity Verifier version 2.05.
//
edf379bc66e7c65e22315f473c384ae8 c:\analysissession2.mans
```

Compressed has value for AnalysisSession.zip



```
C:\Users\Public>fciv.exe C:\AnalysisSession2.zip
//
// File Checksum Integrity Verifier version 2.05.
//
60cd33a08ec3f0d15c40e6a9eb1ce68c c:\analysissession2.zip
```