

Collecting Hostname, Date, and Time

- ❑ Identify the computer name using the **hostname** command
Command:
hostname
- ❑ This command can be useful while examining logs and network traffic



```
root@ubuntu: ~
File Edit View Search Terminal Help
root@ubuntu:~# hostname
ubuntu
root@ubuntu:~#
```

- ❑ Check the **date and time** of the machine to build a proper timeline of events

Command:
date
cat /etc/timezone



```
root@ubuntu: /home/Investigator
File Edit View Search Terminal Help
root@ubuntu:/home/Investigator# date
Wed Apr 22 23:53:45 PDT 2020
root@ubuntu:/home/Investigator# cat /etc/timezone
America/Los_Angeles
root@ubuntu:/home/Investigator#
```

Collecting Hostname, Date, and Time (Cont'd)

- ❑ Alternately, you can **calculate the epoch time** (count of the number of seconds from the Unix OS starting point) of the system and convert it w.r.t your time zone

Command:

date +%s

Note: The Unix epoch timestamp begins on 1st January 1970 00:00:00 UTC (in seconds), whereas the epoch timestamps for HFS+ and Cocoa in Apple begin on 1st January 1904 00:00:00 UTC (in seconds) and 1st January 2001 00:00:00 UTC (in seconds), respectively.

```
root@james-Virtual-Machine: /home/james
root@james-Virtual-Machine:/home/james# date +%s
1598025566
root@james-Virtual-Machine:/home/james#
```

- ❑ Upon obtaining the epoch timestamp, you can use online or offline converters to convert the epoch time to original time. Here, we are doing the conversion in www.epochconverter.com

Epoch Converter - Unix Timestamp Converter - Mozilla Firefox

Epoch Converter - Unix x +

https://www.epochconverter.com

EpochConverter

Epoch & Unix Timestamp Conversion Tools

The current Unix epoch time is **1598026162**

Convert epoch to human-readable date and vice versa

1598025566 Timestamp to Human date reset

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**

GMT : Friday, August 21, 2020 3:59:26 PM

Your time zone : Friday, August 21, 2020 11:59:26 AM GMT-04:00 DST

Relative : 3 minutes ago

Yr: Mon Day Hr Min Sec PM GMT Human date to Timestamp

2020 - 8 - 21 4 : 2 : 10 PM GMT

This website uses cookies to ensure you get the best experience on our website. [Learn more](#) [Got It!](#)

Collecting Uptime Data



- The **uptime** command in Linux system displays how long the system has been running since the last restart



- This command also returns the current time, number of presently logged-in users, system load averages, etc.

Command:

uptime

```
root@ubuntu: /home/investigator
File Edit View Search Terminal Help

top - 07:06:28 up 40 min, 1 user, load average: 0.12, 0.14, 0.14
Tasks: 326 total, 2 running, 235 sleeping, 1 stopped, 0 zombie
%Cpu(s): 19.5 us, 4.0 sy, 0.0 ni, 76.4 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 2005964 total, 164548 free, 1078400 used, 763016 buff/cache
KiB Swap: 969960 total, 686168 free, 283792 used, 755996 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1536 invest+  20   0 2954208 170092 41712  R 16.2   8.5   0:52.28 /usr/bin/g+
21241 invest+  20   0 624212 31380 25060  S  3.6   1.6   0:00.11 /usr/bin/g+
1392 invest+  20   0 471512 44412 13960  S  2.0   2.2   0:23.55 /usr/lib/x+
  11 root      20   0      0      0      0   I  0.3   0.0   0:01.21 [rcu_sched]
 242 root      20   0      0      0      0   I  0.3   0.0   0:02.89 [kworker/0+
 429 root     -51   0      0      0      0   S  0.3   0.0   0:01.41 [irq/10-vn+
1397 invest+  20   0 51120 3440 1856  S  0.3   0.2   0:00.56 /usr/bin/d+
20608 invest+  20   0 802732 38272 27980  S  0.3   1.9   0:07.88 /usr/lib/g+
   1 root      20   0 225784 6984 4144  S  0.0   0.3   0:07.22 /lib/syste+
   2 root      20   0      0      0      0   S  0.0   0.0   0:00.00 [kthreadd]
   3 root      0 -20      0      0      0   I  0.0   0.0   0:00.00 [rcu_gp]
   4 root      0 -20      0      0      0   I  0.0   0.0   0:00.00 [rcu_par_g+
   6 root      0 -20      0      0      0   I  0.0   0.0   0:00.00 [kworker/0+
   7 root      20   0      0      0      0   I  0.0   0.0   0:01.59 [kworker/0+
   9 root      0 -20      0      0      0   I  0.0   0.0   0:00.00 [mm_percpu+
  10 root      20   0      0      0      0   S  0.0   0.0   0:00.69 [ksortirqd]
```

Collecting Network Information

- The following syntax displays all **Network Interface Controllers** (NICs) and associated IP addresses associated with them

Syntax:

ip addr show

Note:

- lo, ens33 are NICs
- State **UNKNOWN** – NIC is operational but there is no connection
- State **UP** – NIC is operational and there is a connection

```
root@ubuntu: ~
File Edit View Search Terminal Help

root@ubuntu:~# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:b6:8f:09 brd ff:ff:ff:ff:ff:ff
    inet 192.168.135.155/24 brd 192.168.135.255 scope global dynamic noprefixroute ens33
        valid_lft 1172sec preferred_lft 1172sec
    inet6 fe80::481d:210e:9850:a56/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@ubuntu:~#
```



```
root@ubuntu:/home/investigator# netstat -tlnp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State          I-Node   Path
tcp        0      0 *          *              LISTENING     55977       /usr/bin/sshd
tcp        0      0 *          *              LISTENING     45900       /run/user/1000/sy...
tcp        0      0 *          *              LISTENING     38957       /run/user/121/sy...
tcp        0      0 *          *              LISTENING     24155       /run/systemd/journ...
tcp        0      0 *          *              LISTENING     24157       /run/systemd/journ...
tcp        0      0 *          *              LISTENING     23991       /run/systemd/notify
tcp        0      0 *          *              LISTENING     24003       /run/systemd/journ...
tcp        0      0 *          *              LISTENING     4774       /run/user/1000/bu...
tcp        0      0 *          *              LISTENING     47421       /tmp/.ICE-unix/1432
tcp        0      0 *          *              LISTENING     46637       /0/tmp/.X11-unix/X0
tcp        0      0 *          *              LISTENING     35741       /var/run/dbus/syste...
tcp        0      0 *          *              LISTENING     47539       /run/systemd/journ...
tcp        0      0 *          *              LISTENING     46934       /run/systemd/journ...
tcp        0      0 *          *              LISTENING     44615       /run/systemd/journ...
tcp        0      0 *          *              LISTENING     35741       /var/run/dbus/syste...
tcp        0      0 *          *              LISTENING     32976       /var/run/dbus/syste...
tcp        0      0 *          *              LISTENING     63601       /run/user/1000/pul...
tcp        0      0 *          *              LISTENING     45926       /run/systemd/journ...
```

■	●
■	●
■	●

```
netstat -i
```

```

root@ubuntu:/home/investigator
File Edit View Search Terminal Help
root@ubuntu:/home/investigator# netstat -i
Kernel Interface table

```

Interface	MTU	RX-OK	RX-ERR	RX-DRP	RX-OVR	TX-OK	TX-ERR	TX-DRP	TX-OVR	Flg
ens33	1500	55705	0	0	0	30553	0	0	0	BMRU
lo	65536	10197	0	0	0	10197	0	0	0	LRU

```

root@ubuntu:/home/investigator#

```


- r displays the kernel IP routing table
- n displays the numerical addresses

```
root@ubuntu:/home/investigator
File Edit View Search Terminal Help
root@ubuntu:/home/investigator# netstat -rn
Kernel IP routing table
Destination        Gateway           Genmask          Flags   MSS Window  irtt Iface
0.0.0.0            192.168.135.2   0.0.0.0          UG      0 0 0      ens33
169.254.0.0        0.0.0.0         255.255.0.0      U       0 0 0      ens33
192.168.135.0      0.0.0.0         255.255.255.0    U       0 0 0      ens33
root@ubuntu:/home/investigator#
```

```
root@ubuntu:/home/investigator
File Edit View Search Terminal Help
root@ubuntu:/home/investigator# ip r
default via 192.168.135.2 dev ens33 proto dhcp metric 100
169.254.0.0/16 dev ens33 scope link metric 1000
192.168.135.0/24 dev ens33 proto kernel scope link src 192.168.135.136 metric 100
root@ubuntu:/home/investigator#
```

ip r

Finding Programs/Processes Associated with a Port

- To detect **intrusions**, it is necessary to collect **open port** information
- It is also important to check if there are any **programs/processes** associated with **open ports**
Command:
`netstat -tulpn`
- In the screenshot, **cupsd** is the process with PID 11806, running on port 631



```
root@ubuntu:~# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:1:631          0.0.0.0:*               LISTEN      11806/cupsd
tcp        0      0 0.0.0.0:53:53         0.0.0.0:*               LISTEN      581/systemd-resolve
udp        0      0 0.0.0.0:55216         0.0.0.0:*               LISTEN      650/avahi-daemon: r
udp        0      0 0.0.0.0:53:53         0.0.0.0:*               LISTEN      581/systemd-resolve
udp        0      0 0.0.0.0:68            0.0.0.0:*               LISTEN      13202/dhclient
udp        0      0 0.0.0.0:53:53         0.0.0.0:*               LISTEN      650/avahi-daemon: r
udp        0      0 0.0.0.0:631          0.0.0.0:*               LISTEN      11806/cups-browsed
udp6       0      0 :::5353              :::*                    LISTEN      650/avahi-daemon: r
udp6       0      0 :::52513              :::*                    LISTEN      650/avahi-daemon: r
root@ubuntu:~#
```

- Another command to list the **processes running on open ports**
Command:
`lsof -i -P -n | grep LISTEN`
- The **grep command** is used to filter ports in the LISTEN state

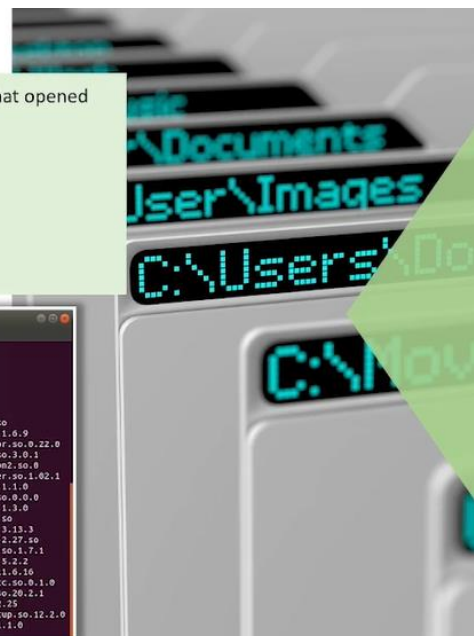


```
root@ubuntu:~# lsof -i -P -n | grep LISTEN
systemd-r 581 systemd-resolve 13u IPv4 35013 0t0 TCP 127.0.0.53:53 (LISTEN)
cupsd     11806    root      6u IPv6 409971 0t0 TCP :::1:631 (LISTEN)
cupsd     11806    root      7u IPv4 409972 0t0 TCP 127.0.0.1:631 (LISTEN)
root@ubuntu:~#
```

Collecting Data on Open Files

- You can run **lsof** command to list all open files as well as the active processes that opened them on the system
Command:
`lsof`
- To list the open files for the user currently logged into the system
Command:
`lsof -u <user_name>`

```
root@ubuntu:~# lsof
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
COMMAND PID TID USER FD TYPE DEVICE SIZE/OFF NODE NAME
systemd 1 root cwd DIR 8:1 4096 2 /
systemd 1 root rtd DIR 8:1 4096 2 /
systemd 1 root txt REG 8:1 561152 61770 /lib/systemd/systemd
systemd 1 root mem REG 8:1 1708792 661843 /lib/x86_64-linux-gnu/libn-2.27.so
systemd 1 root mem REG 8:1 121016 657004 /lib/x86_64-linux-gnu/libudev.so.1.6.9
systemd 1 root mem REG 8:1 80632 661821 /lib/x86_64-linux-gnu/libgpg-error.so.0.22.0
systemd 1 root mem REG 8:1 41304 661832 /lib/x86_64-linux-gnu/libgpg-error.so.0.22.0
systemd 1 root mem REG 8:1 34872 273191 /usr/lib/x86_64-linux-gnu/libargon2.so.0
systemd 1 root mem REG 8:1 43240 661802 /lib/x86_64-linux-gnu/libc.so.2.27
systemd 1 root mem REG 8:1 18680 661768 /lib/x86_64-linux-gnu/libattr.so.1.1.0
systemd 1 root mem REG 8:1 18712 661783 /lib/x86_64-linux-gnu/libcap-ng.so.0.0.0
systemd 1 root mem REG 8:1 27112 663830 /lib/x86_64-linux-gnu/libbsd.so.0.0.0
systemd 1 root mem REG 8:1 14560 661803 /lib/x86_64-linux-gnu/libltdl-2.27.so
systemd 1 root mem REG 8:1 464824 661902 /lib/x86_64-linux-gnu/libpcre.so.3.13.3
systemd 1 root mem REG 8:1 144876 661913 /lib/x86_64-linux-gnu/libpthread-2.27.so
systemd 1 root mem REG 8:1 112672 273833 /usr/lib/x86_64-linux-gnu/libltdl-2.27.so
systemd 1 root mem REG 8:1 153984 661840 /lib/x86_64-linux-gnu/libltdl-2.27.so
systemd 1 root mem REG 8:1 206872 661827 /lib/x86_64-linux-gnu/libltdl-2.27.so
systemd 1 root mem REG 8:1 27808 273759 /usr/lib/x86_64-linux-gnu/libltdl-2.27.so
systemd 1 root mem REG 8:1 1159864 661819 /lib/x86_64-linux-gnu/libcrypt.so.2.2.1
systemd 1 root mem REG 8:1 22768 661785 /lib/x86_64-linux-gnu/libc.so.2.27
systemd 1 root mem REG 8:1 319040 661793 /lib/x86_64-linux-gnu/libcryptsetup.so.12.2.0
systemd 1 root mem REG 8:1 31232 661758 /lib/x86_64-linux-gnu/libacl.so.1.1.0
```



Viewing Running Processes in the System



- ❑ Run the **ps** command to view the processes running on the system
- ❑ It provides a **snapshot** of the **current processes** along with detailed information, such as the **user id**, **CPU usage**, **memory usage**, and **command name**
- ❑ Check the **process tree** to determine any suspicious **child processes** and **dependencies**



```
root@ubuntu: ~  
File Edit View Search Terminal Help  
root@ubuntu:~# ps auxww  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root         1  0.0  0.3 168240 6028 ?        Ss   11:52   0:04 /sbin/init auto noprompt  
root         2  0.0  0.0      0     0 ?        S    11:52   0:00 [kthreadd]  
root         3  0.0  0.0      0     0 ?        I<   11:52   0:00 [rcu_gp]  
root         4  0.0  0.0      0     0 ?        I<   11:52   0:00 [rcu_par_gp]  
root         6  0.0  0.0      0     0 ?        I<   11:52   0:00 [kworker/0:0H-kb]  
root         9  0.0  0.0      0     0 ?        I<   11:52   0:00 [mm_percpu_wq]  
root        10  0.0  0.0      0     0 ?        S    11:52   0:01 [ksoftirqd/0]  
root        11  0.0  0.0      0     0 ?        I    11:52   0:01 [rcu_sched]  
root        12  0.0  0.0      0     0 ?        S    11:52   0:00 [migration/0]  
root        13  0.0  0.0      0     0 ?        S    11:52   0:00 [idle_inject/0]  
root        14  0.0  0.0      0     0 ?        S    11:52   0:00 [cpuhp/0]  
root        15  0.0  0.0      0     0 ?        S    11:52   0:00 [kdevtmpfs]  
root        16  0.0  0.0      0     0 ?        I<   11:52   0:00 [netns]  
root        17  0.0  0.0      0     0 ?        S    11:52   0:00 [rcu_tasks_kthre]  
root        18  0.0  0.0      0     0 ?        S    11:52   0:00 [kauditd]  
root        19  0.0  0.0      0     0 ?        S    11:52   0:00 [khungtaskd]  
root        20  0.0  0.0      0     0 ?        S    11:52   0:00 [oom_reaper]  
root        21  0.0  0.0      0     0 ?        I<   11:52   0:00 [writeback]  
root        22  0.0  0.0      0     0 ?        S    11:52   0:00 [kcompactd0]  
root        23  0.0  0.0      0     0 ?        SN   11:52   0:00 [ksmd]  
root        24  0.0  0.0      0     0 ?        SN   11:52   0:00 [khugepaged]
```

Collecting Kernel Information

- ❑ Use the following **commands** to check the Linux **kernel version** on a system:
uname -r
(or)
cat /proc/version
(or)
hostnamectl | grep Kernel



```
root@ubuntu: /home/Investigator  
File Edit View Search Terminal Help  
root@ubuntu:/home/Investigator# uname -r  
5.3.0-28-generic  
root@ubuntu:/home/Investigator# cat /proc/version  
Linux version 5.3.0-28-generic (buildd@lcy01-amd64-009) (gcc version 7.4.0  
(Ubuntu 7.4.0-1ubuntu1~18.04.1)) #30-18.04.1-Ubuntu SMP Fri Jan 17 06:14:  
09 UTC 2020  
root@ubuntu:/home/Investigator# hostnamectl | grep Kernel  
Kernel: Linux 5.3.0-28-generic  
root@ubuntu:/home/Investigator#
```

Collecting User Account Information

The `/etc/passwd` file running on a Linux system stores **local user** account information

Analyzing the `/etc/passwd` file allows the investigator to view **the user accounts** on the system

Command:

`cat /etc/passwd`

Command given to list only **usernames** in the output

`cut -d: -f1 /etc/passwd`

Each line in the output represents the **login information** of a single **user** and includes seven fields separated by colon (:) :

You can observe the following about the output format of the `/etc/passwd` file by analyzing the first entry in the screenshot:

`root` – Username

`x` – Password ('x' denotes encrypted)

`0` – User ID ('0' is reserved for root)

`0` – Group ID

`root` – User ID information

`/root` – Home directory

`/bin/bash` – Absolute path to the user's login shell

```
root@ubuntu: ~  
File Edit View Search Terminal Help  
root@ubuntu:~# cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd-netif:/usr/sbin/nologin  
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin  
syslog:x:102:106:/:home/syslog:/usr/sbin/nologin  
messagebus:x:103:107:/:nonexistent:/usr/sbin/nologin
```


A conceptual illustration of cloud storage and security. It features a central cloud with a double-headed arrow indicating data flow. Surrounding the cloud are various icons: a smartphone held by a hand, a folder with a lock, a document with a lock, a gear, and a shield with a lock. Dashed lines connect these elements, suggesting a secure and interconnected system.

- Command:**

- ❑ The following command filters out **sudo** commands

```
root@ubuntu:~  
root@ubuntu:~# cat /var/log/auth.log  
Apr 16 10:41:13 ubuntu su[2311]: pam_unix(su-session): session closed for user root  
Apr 16 10:41:13 ubuntu su[2311]: pam_unix(su-session): session closed for user root  
Apr 16 10:41:13 ubuntu systemd-logind[621]: Removed session.  
Apr 16 10:42:08 ubuntu sudo: investigator: TTY=pts/0 ; PWD=/home/investigator ; USER=root ; COMMAND=/bin/su  
Apr 16 10:42:08 ubuntu sudo: pam_unix(sudo-session): session opened for user root by (uid=0)  
Apr 16 10:42:08 ubuntu su[3337]: Successful su for root by root  
Apr 16 10:42:08 ubuntu su[3337] : /dev/pts/0 root-root  
Apr 16 10:42:09 ubuntu su[3337]: pam_unix(su-session): session opened for user root by (uid=0)  
Apr 16 10:42:08 ubuntu systemd-logind[621]: New session 3 of user root.  
Apr 16 10:42:08 ubuntu systemd-logind[621]: Session opened for user root by (uid=0)  
Apr 16 10:49:02 ubuntu systemd-logind[641]: System is powering down.  
Apr 16 10:49:02 ubuntu su[3337]: pam_unix(su-session): session closed for user root  
Apr 16 10:49:02 ubuntu su[3337]: pam_unix(su-session): session closed for user root  
Apr 16 10:49:02 ubuntu systemd-logind[641]: System is now suspended.  
Apr 16 10:49:02 ubuntu systemd-logind[641]: New seat seata.  
Apr 16 10:49:02 ubuntu systemd-logind[641]: New system buttons on /dev/input/event8 (Power Button).  
Apr 16 10:49:02 ubuntu pam-launch-environment[1]: pam_unix(pam-launch-environment:session): session opened for user gdm by (uid=0)  
Apr 16 10:49:02 ubuntu systemd-logind[641]: New session c1 of user gdm.  
Apr 16 10:49:02 ubuntu systemd-pam[systemd-user-session]: session opened for user gdm by (uid=0)  
Apr 16 10:49:02 ubuntu systemd-logind[641]: Matching system buttons on /dev/input/events (AT Translated Set 2 keyboard).  
Apr 16 10:49:57 ubuntu polkit(authority=local): Registered Authentication Agent for unix-sessionc1 (system bus: /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8).  
Apr 16 10:49:58 ubuntu gdm-password: pam_unix(gdm-password:session): session opened for user Investigator b (uid=0)  
Apr 16 10:49:58 ubuntu systemd-pam[systemd-user-session]: session opened for user Investigator by (uid=0)
```

```
root@ubuntu:~#
```

```
File Edit View Search Terminal Help
```

```
root@ubuntu:~# grep sudo /var/log/auth.log
```

```
Apr 20 10:41:31 ubuntu audit: pam_unix(auth:session): session closed for user root
```

```
Apr 20 10:42:06 ubuntu audit: Investigator : TTYpts/0 ; PwM/home/Investigator ; USER=root ; COMMAND=/bin/su -
```

```
Apr 20 10:42:07 ubuntu audit: pam_unix(session): session opened for user root by (uid=0)
```

```
Apr 20 10:49:02 ubuntu audit: pam_unix(auth:session): session closed for user root
```

```
Apr 20 10:49:03 ubuntu audit: Investigator : TTYpts/0 ; PwM/home/Investigator ; USER=root ; COMMAND=/bin/su su
```

```
Apr 20 12:23:58 ubuntu audit: pam_unix(auth:session): session opened for user root by (uid=0)
```

```
Apr 20 22:31:51 ubuntu audit: pam_unix(auth:session): session closed for user root
```

```
Apr 20 22:31:51 ubuntu audit: Investigator : TTYpts/0 ; PwM/home/Investigator ; USER=root ; COMMAND=/bin/su
```

```
Apr 20 14:58:34 ubuntu audit: pam_unix(auth:session): session opened for user root by (uid=0)
```

```
Apr 20 14:58:35 ubuntu audit: Investigator : TTYpts/0 ; PwM/home/Investigator ; USER=root ; COMMAND=/bin/su su
```

```
Apr 27 06:05:38 ubuntu audit: pam_unix(auth:session): session opened for user root by (uid=0)
```

```
Apr 27 06:36:35 ubuntu audit: pam_unix(auth:session): session closed for user root
```

```
Apr 27 06:37:19 ubuntu audit: pam_unix(auth:): authentication failed
```

```
Apr 27 06:37:02 ubuntu audit: pam_unix(auth:auth): auth could not identify password for [Investigator]
```

```
Apr 27 06:37:16 ubuntu audit: Investigator : TTYpts/0 ; PwM/home/Investigator ; USER=root ; COMMAND=/bin/su
```

```
Apr 27 06:37:19 ubuntu audit: pam_unix(session): session opened for user root by (uid=0)
```

```
Apr 27 07:03:24 ubuntu audit: Investigator : TTYpts/1 ; PwM/home/Investigator ; USER=root ; COMMAND=/bin/su
```

```
Apr 27 07:03:25 ubuntu audit: pam_unix(session): session opened for user root by (uid=0)
```

```
Apr 27 07:04:11 ubuntu audit: pam_unix(auth:session): session closed for user root
```

```
Apr 27 07:04:55 ubuntu audit: Investigator : TTYpts/1 ; PwM/home/Investigator ; USER=root ; COMMAND=/bin/su
```

```
Apr 27 07:04:56 ubuntu audit: pam_unix(session): session opened for user root by (uid=0)
```

```
Apr 27 07:05:04 ubuntu audit: pam_unix(auth:session): session closed for user root
```

```
Apr 27 07:05:05 ubuntu audit: Investigator : TTYpts/0 ; PwM/home/Investigator ; USER=root ; COMMAND=/bin/su
```

```
Apr 27 07:05:18 ubuntu audit: pam_unix(session): session opened for user root by (uid=0)
```

```
Apr 27 07:06:45 ubuntu audit: pam_unix(auth:session): session closed for user root
```

```
Apr 27 07:06:45 ubuntu audit: Investigator : TTYpts/0 ; PwM/home/Investigator ; USER=root ; COMMAND=/bin/su
```

- Command:**

```
root@ubuntu: /home/investigator/Desktop
File Edit View Search Terminal Help
root@ubuntu: /home/investigator/Desktop # w
10:52:24 up 4:14, 1 user, load average: 0.00, 0.01, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
investig:  :0               xdm      7:40    7xdm7  1:27   0.01s  /usr/lib/gdm
```

- Command:**



```

root@ubuntu: ~/home/investigator/Desktop
File Edit View Search Terminal Help

root@ubuntu: ~/home/investigator/Desktop# last -f /var/log/wtmp
Investig: 10      Tue Apr 28 04:38      gone - no logout
reboot system boot 5.3.0-28-generic Tue Apr 28 04:37      still running
Investig: 10      Tue Apr 28 04:36      04:36      (00:53)
reboot system boot 5.3.0-28-generic Tue Apr 28 03:58      04:37      (00:39)
Investig: 10      Mon Apr 27 22:55      down      (01:04)
reboot system boot 5.3.0-28-generic Mon Apr 27 22:54      00:00      (01:05)
Investig: 10      Mon Apr 27 06:05      00:00      (01:46)
reboot system boot 5.3.0-28-generic Mon Apr 27 06:04      09:51      (01:46)
Investig: 10      Mon Apr 27 04:57      down      (01:07)
reboot system boot 5.3.0-28-generic Sun Apr 26 23:32      06:04      (06:31)
Investig: 10      Sun Apr 26 22:39      23:11      (06:32)
reboot system boot 5.3.0-28-generic Sun Apr 26 22:38      23:11      (06:33)
Investig: 10      Sun Apr 26 10:19      down      (00:29)
reboot system boot 5.3.0-28-generic Sun Apr 26 10:17      10:49      (06:31)
Investig: 10      Thu Apr 23 23:13      down      (08:55)
reboot system boot 5.3.0-28-generic Thu Apr 23 22:56      08:08      (09:11)
Investig: 10      Thu Apr 23 22:56      08:08      (09:11)
reboot system boot 5.3.0-28-generic Thu Apr 23 22:36      22:56      (00:20)
Investig: 10      Thu Apr 23 12:26      12:52      (00:25)
Investig: 10      Wed Apr 22 22:25      12:24      (13:58)
reboot system boot 5.3.0-28-generic Tue Apr 21 23:26      12:52      (14:27)
Investig: 10      Tue Apr 21 23:26      11:39      (12:12)
reboot system boot 5.3.0-28-generic Tue Apr 21 23:26      11:39      (12:13)

```

Collecting System Logs Data

- ❑ On a Linux machine, the system logs are located in the directory **/var/log/syslog**
 - ❑ The **syslog configuration file** stores system messages from logging facility and collects data logs of various programs and services, including the kernel
- Command:
- ```
cat /var/log/syslog
```



```
root@ubuntu:~# cat /var/log/syslog
May 5 04:22:11 ubuntu rsyslogd: [origin software="rsyslogd" swversion="8.32.0"
x-pid="683" x-info="http://www.rsyslog.com"] rsyslogd was HUPed
May 5 04:22:14 ubuntu anacron[673]: Job 'cron.daily' terminated
May 5 04:22:14 ubuntu anacron[673]: Normal exit (1: job run)
May 5 04:23:26 ubuntu systemd[1]: Created slice User Slice of Investigator.
May 5 04:23:26 ubuntu systemd[1]: Starting User Manager for UID 1000...
May 5 04:23:26 ubuntu systemd[1]: Started Session 2 of user Investigator.
May 5 04:23:26 ubuntu systemd[1536]: Listening on GnuPG cryptographic agent and
passphrase cache (restricted).
May 5 04:23:26 ubuntu systemd[1536]: Starting D-Bus User Message Bus Socket.
May 5 04:23:27 ubuntu systemd[1536]: Listening on REST API socket for snap use
r session agent.
May 5 04:23:27 ubuntu systemd[1536]: Started Pending report trigger for Ubuntu
Report.
May 5 04:23:27 ubuntu systemd[1536]: Reached target Paths.
May 5 04:23:27 ubuntu systemd[1536]: Listening on GnuPG cryptographic agent and
passphrase cache (access for web browsers).
May 5 04:23:27 ubuntu systemd[1536]: Reached target Timers.
May 5 04:23:27 ubuntu systemd[1536]: Listening on GnuPG cryptographic agent and
passphrase cache.
May 5 04:23:27 ubuntu systemd[1536]: Listening on GnuPG cryptographic agent (ss
h-agent emulation).
May 5 04:23:27 ubuntu systemd[1536]: Listening on GnuPG network certificate man
agement daemon.
```

- ❑ Analyzing **Linux kernel logs** located at **/var/log/kern.log** can be helpful for troubleshooting custom kernels

Command:

```
cat /var/log/kern.log
```

```
root@ubuntu:~# cat /var/log/kern.log
May 4 11:53:15 ubuntu kernel: [10835.075027] usb 2-2.1: USB disconnect, device
number 4
May 4 23:19:46 ubuntu kernel: [10835.625227] e1000: ens33 NIC Link is Down
May 4 23:19:46 ubuntu kernel: [10835.650855] usb 2-2.1: New full-speed USB devi
ce number 5 using uhci_hcd
May 4 23:19:46 ubuntu kernel: [10835.665146] usb 1-1: reset high-speed USB devi
ce number 2 using ehci-pci
May 4 23:19:47 ubuntu kernel: [10835.766583] usb 2-2.1: config 1 interface 1 al
tsetting 0 endpoint 0x3 has wMaxPacketSize 0, skipping
May 4 23:19:47 ubuntu kernel: [10835.766585] usb 2-2.1: config 1 interface 1 al
tsetting 0 endpoint 0x83 has wMaxPacketSize 0, skipping
May 4 23:19:47 ubuntu kernel: [10835.778739] usb 2-2.1: New USB device found, i
dVendor=0bed, idProduct=0009, bcdDevice=1.00
May 4 23:19:47 ubuntu kernel: [10835.778751] usb 2-2.1: New USB device strings:
Manufacturer=1, Product=2, SerialNumber=3
May 4 23:19:47 ubuntu kernel: [10835.778787] usb 2-2.1: Product: Virtual Bluetoo
oth Adapter
May 4 23:19:47 ubuntu kernel: [10835.778787] usb 2-2.1: Manufacturer: VMware
May 4 23:19:47 ubuntu kernel: [10835.778787] usb 2-2.1: SerialNumber: 000650268
328
May 4 23:19:48 ubuntu kernel: [10837.634747] e1000: ens33 NIC Link is Up 1000 M
bps Full Duplex, Flow Control: None
May 4 23:19:48 ubuntu kernel: [10837.641505] IPV6: ADDRCONF(NETDEV_CHANGE): ens
33: link becomes ready
```



## Linux Log Files

| Log Location        | Content Description                                                                     |
|---------------------|-----------------------------------------------------------------------------------------|
| /var/log/auth.log   | System authorization information, including user logins and authentication mechanism    |
| /var/log/kern.log   | Initialization of kernels, kernel errors or informational messages sent from the kernel |
| /var/log/faillog    | Failed user login attempts                                                              |
| /var/log/lpr.log    | Printer logs                                                                            |
| /var/log/mail.*     | All mail server message logs                                                            |
| /var/log/mysql.*    | All MySQL server logs                                                                   |
| /var/log/apache2/*  | All Apache web server logs                                                              |
| /var/log/apport.log | Application crash report/log                                                            |
| /var/log/lighttpd/* | Lighttpd web server log files directory                                                 |
| /var/log/daemon.log | Running services, such as squid and ntpd                                                |
| /var/log/debug      | Debugging log messages                                                                  |
| /var/log/dpkg.log   | Package installation or removal logs                                                    |

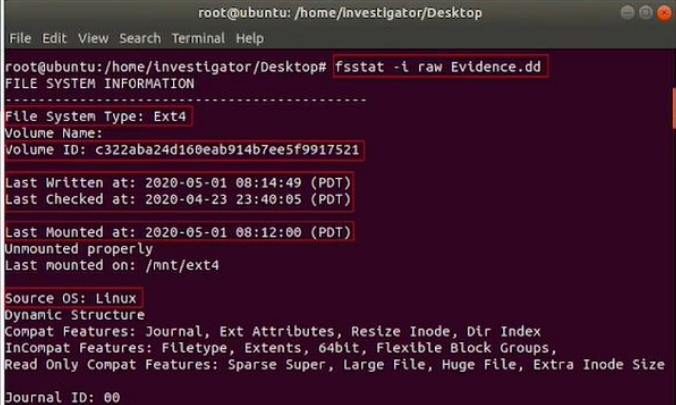


# File System Analysis Using The Sleuth Kit: **fsstat**

- ❑ In Linux systems, the **fsstat** command provides information associated with the given file system
- ❑ The output of this command is filesystem-specific and consists of several information such as the file system type, volume ID, last mounted timestamps and last mounted directory

## Command:

```
fsstat -i <input_filetype>
<filename.extension>
```



```
root@ubuntu: /home/Investigator/Desktop
File Edit View Search Terminal Help
root@ubuntu: /home/Investigator/Desktop# fsstat -i raw Evidence.dd
FILE SYSTEM INFORMATION

File System Type: Ext4
Volume Name:
Volume ID: c322aba24d160eab914b7ee5f9917521
Last Written at: 2020-05-01 08:14:49 (PDT)
Last Checked at: 2020-04-23 23:40:05 (PDT)
Last Mounted at: 2020-05-01 08:12:00 (PDT)
Unmounted properly
Last mounted on: /mnt/ext4
Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Extents, 64bit, Flexible Block Groups,
Read Only Compat Features: Sparse Super, Large File, Huge File, Extra Inode Size
Journal ID: 00
Journal Teacher: 0
```

Or Autopsy using for file system analysis

# Memory Forensics: Introduction



Memory forensics involves **forensic analysis of RAM dumps** captured from a running machine



Forensic analysis of **RAM dump** provides insights into processes running in the memory, network information, unauthorized access to the system, loaded modules, recently executed commands, injected code fragments, etc.



Such information can help the investigator **uncover malware attacks** or any other malicious behavior that has occurred on the target machine

1

2

3

**Note:** The investigator should proceed with the forensic examination based on the **information/events recorded** by the incident response team

## File System Analysis Using The Sleuth Kit: fls and istat

- ❑ Run the **fls** command to list the files and directories available in an image file
- ❑ This command is also useful to view **recently deleted files**

**Command:**

**fls -i <image\_type> <imagefile\_name>**

- ❑ Use **istat** command that displays the metadata of a file, such as MAC times, file size, and file access permissions, by specifying a particular inode number

**Command:**

**istat -f <fstype> -i <imgtype>  
<imagefile\_name> <inode\_number>**

```
root@ubuntu: /home/investigator/Desktop
File Edit View Search Terminal Help
root@ubuntu: /home/investigator/Desktop# fls -i raw Evidence.dd
d/d 11: lost+found
d/d * 12(realloc): Evidence Files
d/d 14: Audio Files
d/d 19: Image Files
d/d 56: Outlook Files
d/d 67: Songs
d/d 69: text
d/d 73: Wireshark Sample Capture Files
r/r 13: Compressed_files.rar
r/r 649: Confidential.pdf
r/r 650: Expense sheet.xlsx
r/r 651: Flowers.jpg
r/r 652: Legal_Disclaimer.htm
r/r 653: MultiplePages.pdf
r/r 654: MultiplePages-Fixed.pdf
r/r 655: New Text Document.txt
r/r 656: Tutorial.pptx
r/r 657: Word_Doc.docx
r/r 658: Word_Doc1.docx
d/d 7657: .Trash-1000
d/d 7658: .Trash-1000
```

```
root@ubuntu: /home/investigator/Desktop
File Edit View Search Terminal Help
root@ubuntu: /home/investigator/Desktop# istat -f ext4 -i raw Evidence.dd 651
Inode: 651
Allocated
Group: 0
Generation Id: 2810045526
uid / gid: 1000 / 1000
mode: rw-rw-r--
Flags: Extents,
size: 51974
num of links: 1
Inode Times:
Accessed: 2020-04-24 03:44:13.315266000 (PDT)
File Modified: 2020-04-24 06:48:00.000000000 (PDT)
Inode Modified: 2020-04-24 03:44:28.927530966 (PDT)
File Created: 2020-04-24 03:44:13.315266126 (PDT)
Direct Blocks:
152624 152625 152626 152627 152628 152629 152630 152631
152632 152633 152634 152635 152636
root@ubuntu: /home/investigator/Desktop#
```

## Malware Analysis Using Volatility Framework



- ❑ After acquiring RAM dumps from the target machine, the investigator should analyze those dumps using tools such as **Volatility** to **identify** the occurrence of **malicious activity**
- ❑ To examine memory dumps using Volatility Framework, the investigator should **create a Linux profile** that matches the kernel version of the target RAM dump (which is used for analysis)

The **pslist** plugin lists all the **processes** that were running on the machine when the memory dump was captured



**Command:**

```
python vol.py --file=<file_name> --
profile=<Linux_profile_name> linux_pslist
```

**Note:** In this case, the Linux profile is **Linux Ubuntu\_16.04 x64**

```
root@administrator-virtual-machine: /home/administrator/volatility
root@administrator-virtual-machine: /home/administrator/volatility# python vol.py --file=./ubuntu_random.dd --profile=LinuxUbuntu_16_04x64 linux_pslist
Volatility Foundation Volatility Framework 2.6.1
```

| Offset             | Name   | Start Time                   | Pid | PPid | Uid | Gid |
|--------------------|--------|------------------------------|-----|------|-----|-----|
| 0xffff9dd5baf40000 | system | 2020-05-06 08:11:23 UTC+0000 | 1   | 0    | 0   | 0   |
| 0xffff9dd5baf40000 | system | 2020-05-06 08:11:23 UTC+0000 | 2   | 0    | 0   | 0   |
| 0xffff9dd5baf40000 | system | 2020-05-06 08:11:23 UTC+0000 | 4   | 0    | 0   | 0   |
| 0xffff9dd5baf40000 | system | 2020-05-06 08:11:23 UTC+0000 | 6   | 0    | 0   | 0   |
| 0xffff9dd5baf40000 | system | 2020-05-06 08:11:23 UTC+0000 | 7   | 0    | 0   | 0   |
| 0xffff9dd5baf40000 | system | 2020-05-06 08:11:23 UTC+0000 | 8   | 0    | 0   | 0   |
| 0xffff9dd5baf40000 | system | 2020-05-06 08:11:23 UTC+0000 | 9   | 0    | 0   | 0   |
| 0xffff9dd5baf40000 | system | 2020-05-06 08:11:23 UTC+0000 | 10  | 0    | 0   | 0   |
| 0xffff9dd5baf40000 | system | 2020-05-06 08:11:23 UTC+0000 | 11  | 0    | 0   | 0   |
| 0xffff9dd5baf40000 | system | 2020-05-06 08:11:23 UTC+0000 | 12  | 0    | 0   | 0   |
| 0xffff9dd5baf40000 | system | 2020-05-06 08:11:23 UTC+0000 | 13  | 0    | 0   | 0   |

## Malware Analysis Using Volatility Framework (Cont'd)

- ❑ Use the **netstat** plugin to search for malicious network communication on the machine

**Command:**

```
python vol.py --file=<file_name> --
profile=<Linux_profile_name>
linux_netstat
```



```
root@administrator-virtual-machine: /home/administrator/volatility
```

| Protocol | Local Address   | Foreign Address | State       | Process      |
|----------|-----------------|-----------------|-------------|--------------|
| TCP      | 0.0.0.0         | 0.0.0.0         | CLOSE       | apache2/1279 |
| TCP      | ::              | ::              | LISTEN      | apache2/1279 |
| UNIX     | 23310           | lightdm/1282    |             |              |
| UNIX     | 27356           | lightdm/1282    |             |              |
| UNIX     | 30070           | 22              |             |              |
| TCP      | 0.0.0.0         | 0.0.0.0         | LISTEN      | apache2/1332 |
| TCP      | ::              | ::              | LISTEN      | apache2/1332 |
| TCP      | ::ffff:0.0.0.52 | ::ffff:0.0.0.32 | ESTABLISHED | apache2/1332 |
| TCP      | 10.0.0.52       | 10.0.0.32       | ESTABLISHED | apache2/1332 |
| TCP      | 0.0.0.0         | 0.0.0.0         | CLOSE       | apache2/1333 |
| TCP      | ::              | ::              | LISTEN      | apache2/1333 |
| TCP      | 0.0.0.0         | 0.0.0.0         | CLOSE       | apache2/1334 |
| TCP      | ::              | ::              | LISTEN      | apache2/1334 |

- ❑ The **pstree** plugin displays the parent and associated child processes generated using a malicious backdoor
- ❑ From the screenshot below, it can be observed that the **apache2** process with **PID 1279** started another **apache2** process with **PID 1332**
- ❑ This indicates that the **process** with **PID 1332** is establishing malicious communication

**Command:**

```
python vol.py --file=<file_name> --
profile=<Linux_profile_name> linux_pstree
```

```
root@administrator-virtual-machine: /home/administrator
```

| Process         | PID  | PPID |
|-----------------|------|------|
| firefox         | 2227 | 1000 |
| gvfsd-network   | 7130 | 1000 |
| gvfsd-network   | 7133 | -1   |
| gvfsd-smb-brows | 7145 | 1000 |
| polkitd         | 919  |      |
| mysqld          | 964  | 121  |
| whoopsie        | 1205 | 109  |
| agetty          | 1211 |      |
| apache2         | 1279 |      |
| apache2         | 1332 | 33   |
| sh              | 3098 | 33   |
| sh              | 3099 | 33   |
| apache2         | 1332 | 33   |
| apache2         | 1334 | 33   |
| apache2         | 1335 | 33   |
| apache2         | 1336 | 33   |
| apache2         | 2556 | 33   |
| apache2         | 2557 | 33   |
| apache2         | 2558 | 33   |
| apache2         | 2084 | 33   |



## Malware Analysis Using Volatility Framework (Cont'd)

- ❑ The **malfind** plugin helps the investigator identify any **remote/hidden code injections** in the memory

- **Command:**

```
python vol.py --file=<file_name> -
--profile=<Linux_profile_name> linux
_malfind
```

- ❑ From **psree** output, the process with **PID 1332** is identified as **malicious**. You can utilize **malfind** plugin to check whether **PID 1332** is a legitimate process.

- ❑ When **malfind** plugin is run with PID 1332, the parameter '**Protection**' shows that the process is marked with **Read, Write** and **Execute** permissions. This indicates that some **malicious code** has been **injected** into the process.

```
root@administrator-virtual-machine: /home/administrator/volatility
root@administrator-virtual-machine: /home/administrator/volatility# python vol.py --file=../ub
untu_ramdump.dd --profile=LinuxUbuntu_16_04x64 linux_malfind -p 1332
Volatility Foundation Volatility Framework 2.6.1
Process: apache2 Pid: 1332 Address: 0x7fb378b4d000 File: Anonymous Mapping
Protection: VM_READ|VM_WRITE|VM_EXEC|VM_MAYREAD|VM_MAYWRITE|VM_MAYEXEC|VM_ACCOUNT|VM_CAN_NONLINEAR
Flags: VM_READ|VM_WRITE|VM_EXEC|VM_MAYREAD|VM_MAYWRITE|VM_MAYEXEC|VM_ACCOUNT|VM_CAN_NONLINEAR

0x007fb378b4d000 70 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P.....
0x007fb378b4d010 53 41 57 41 56 41 55 48 8b df 48 81 ec b9 00 00 00 SANVAUDH..H...
0x007fb378b4d020 00 00 45 8b 43 18 48 83 e8 01 48 89 44 24 40 48 ..H.C.H...H.D5QH
0x007fb378b4d030 89 44 24 48 48 89 44 24 50 48 89 44 24 58 48 89 .DSHH.DSPH.D5XH

0x7fb378b4d000 7016 J0 0x7fb378b4d018
0x7fb378b4d002 0000 ADD [RAX], AL
0x7fb378b4d004 0000 ADD [RAX], AL
0x7fb378b4d006 0000 ADD [RAX], AL
0x7fb378b4d008 0000 ADD [RAX], AL
0x7fb378b4d00a 0000 ADD [RAX], AL
0x7fb378b4d00c 0000 ADD [RAX], AL
0x7fb378b4d00e 0000 ADD [RAX], AL
0x7fb378b4d010 53 PUSH R0X
0x7fb378b4d011 4157 PUSH R15
0x7fb378b4d013 4156 PUSH R14
0x7fb378b4d015 4155 PUSH R13
0x7fb378b4d017 55 PUSH R0P
```



## Carving Memory Dumps Using PhotoRec Tool

**PhotoRec** is an open-source tool that uses data carving techniques to **recover deleted files/lost data** from a drive or an image file

Memory dumps **contain volatile data** pertaining to logged on users, shared files, recently accessed media files and chats via social networks, accessed webpages, etc.

Identifying and extracting these files allows the forensic investigators to perform a more detailed investigation

### Carving data from the memory dump

- ❑ Run the **PhotoRec** tool and execute the below command

**Command:**  
**photorec <Imagefile\_name>**

```
root@administrator-virtual-machine: /home/administrator
root@administrator-virtual-machine: /home/administrator# photorec
ubuntu_ramdump.dd
```

## Carving Memory Dumps Using PhotoRec Tool (Cont'd)



- ❑ Use anti-malware tools to **scan** the data extracted from the memory dumps for viruses
- ❑ This enables the detection of **any malicious data** in the memory dumps that could be helpful during an investigation

### Extracting data from memory dumps using PhotoRec

```
root@administrator-virtual-machine: /home/administrator
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk ubuntu_randump.dd - 2146 MB / 2046 MiB (R0)
Partition Start End Size in sect
P Unknown 0 1 260 230 17 4191406

Pass 1 - Reading sector 1229064/4191406, 2579 files found
Elapsed time 0h00m07s - Estimated time to completion 0h00m16
txt: 1439 recovered
gz: 851 recovered
tx?: 123 recovered
elf: 73 recovered
png: 57 recovered
sqlite: 30 recovered
ttf: 3 recovered
glf: 1 recovered
tar: 1 recovered
zip: 1 recovered

Stop
```

### Data recovered from the image file

