Lab Assignment

Cybersecurity Professional Program

Digital Forensics & Incident Response

Linux Forensics

DFIR-08-L1
Forensic Acquisition

Lab Objective

Improve forensic data acquisition techniques learned during the lesson.

Lab Mission

Create a forensic acquisition CD with static binaries and use it to extract information from a Linux OS.

Lab Duration

15–25 minutes

Requirements

- Working knowledge of the Linux environment
- Knowledge of piping

Resources

- VirtualBox that includes a NAT network of:
  - Ubuntu
  - SIFT Workstation
    - Volatility
- Extra Lab Files
  - Ubuntu 20.04 SIP
  - Ubuntu 20.04

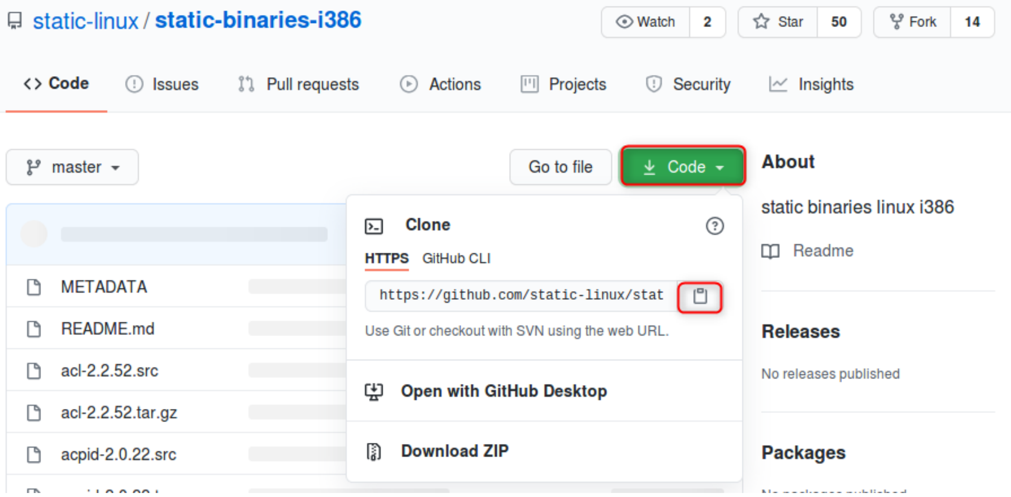
Textbook References

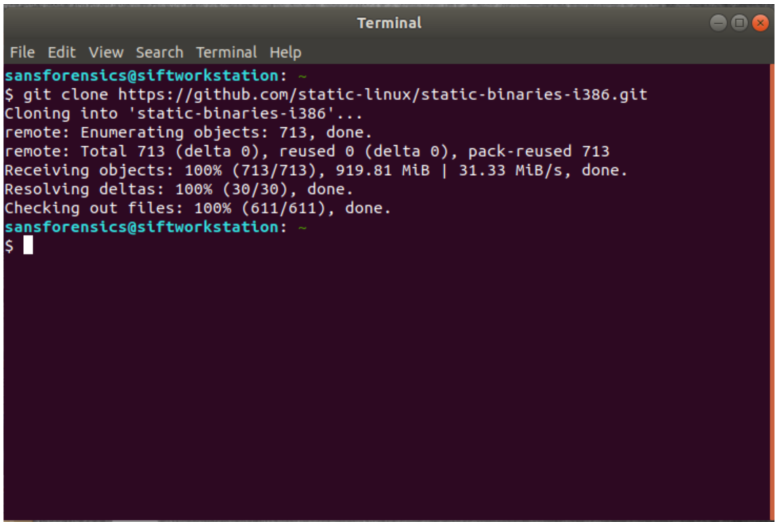
- Chapter 8: Linux Forensics
  - Section 1: Linux Live Forensics
  - Section 2: Linux Live Acquisition

Lab Task: Forensics Acquisition

Create a forensic acquisition CD with static binaries and use it to extract information from a Linux OS. (You can use the prepared rescue CD, but it is recommended that you create one on your own.)

1. Use the SIP to install Ubuntu 20.04.
2. Start the SIFT workstation and check its IP address to discover the network to which Ubuntu will be added.
3. Browse to *https://github.com/static-linux/static-binaries-i386*; copy the site to put in the terminal to download the static binaries. In the terminal, use ***git clone https://github.com/static-linux/static-binaries-i386***.

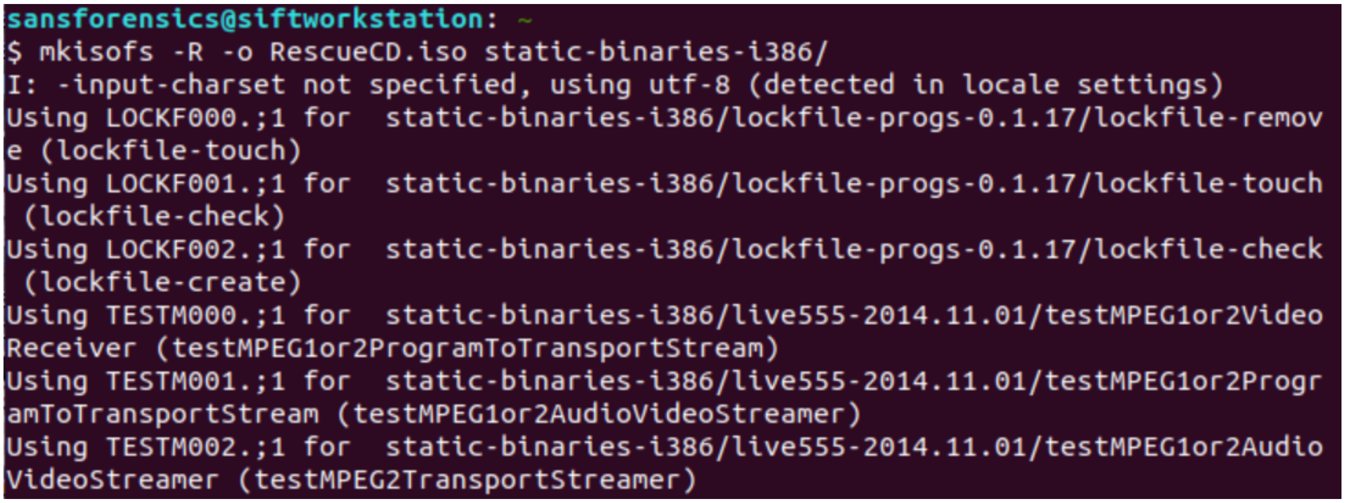




```
sansforensics@siftworkstation: ~
$ git clone https://github.com/static-linux/static-binaries-i386.git
Cloning into 'static-binaries-i386'...
remote: Enumerating objects: 713, done.
remote: Total 713 (delta 0), reused 0 (delta 0), pack-reused 713
Receiving objects: 100% (713/713), 919.81 MiB | 31.33 MiB/s, done.
Resolving deltas: 100% (30/30), done.
Checking out files: 100% (611/611), done.
sansforensics@siftworkstation: ~
$ 
```

4. Change directories to ***static-binaries-i386*** to delete the ***.src*** files and extract the rest. Use ***rm *.src*** and then list the directory. Then, to extract all the files, run this Bash script: ***for file in *.tar.gz; do tar -xvzf $file; done***.

5. Change back to the home directory and use ***mkisofs -R -o RescueCD.iso static-binaries-i386/*** to create an ISO image of the static binaries.



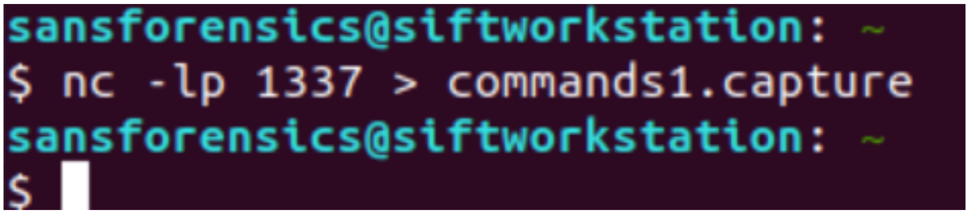
```
sansforensics@siftworkstation: ~
$ mkisofs -R -o RescueCD.iso static-binaries-i386/
I: -input-charset not specified, using utf-8 (detected in locale settings)
Using LOCKF000.;1 for  static-binaries-i386/lockfile-progs-0.1.17/lockfile-remov
e (lockfile-touch)
Using LOCKF001.;1 for  static-binaries-i386/lockfile-progs-0.1.17/lockfile-touch
 (lockfile-check)
Using LOCKF002.;1 for  static-binaries-i386/lockfile-progs-0.1.17/lockfile-check
 (lockfile-create)
Using TESTM000.;1 for  static-binaries-i386/live555-2014.11.01/testMPEG1or2Video
Receiver (testMPEG1or2ProgramToTransportStream)
Using TESTM001.;1 for  static-binaries-i386/live555-2014.11.01/testMPEG1or2Progr
amToTransportStream (testMPEG1or2AudioVideoStreamer)
Using TESTM002.;1 for  static-binaries-i386/live555-2014.11.01/testMPEG1or2Audio
VideoStreamer (testMPEG2TransportStreamer)
```

6. Install **openssh** to the Ubuntu box to transfer the created ISO file to the Ubuntu VM and mount it. Use ***sudo apt install -y openssh-server***. Then, start the SSH service with ***sudo service ssh start***.
   Note: Make sure you have two network adapters, one for internet access and the other for the internal network.

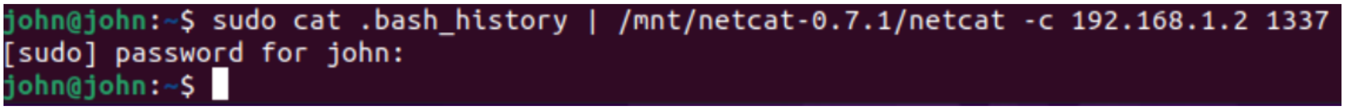
7. Transfer the ***Rescue.iso*** to Ubunto from the SIFT terminal with ***scp RescueCD.iso [boxname]@[IP]:/home/[name]/Desktop***. Once transferred, mount the ISO with ***sudo mount -o loop,ro Desktop/RescueCD.iso /mnt***. Verify that disc was mounted by listing the ***/mnt*** directory.

8. Set SIFT to listen for a connection from Ubuntu and write the data passed during the connection to a file. Connect from Ubuntu to the SIFT listener via the BusyBox directory to allow transfer of the network data, as shown in class.

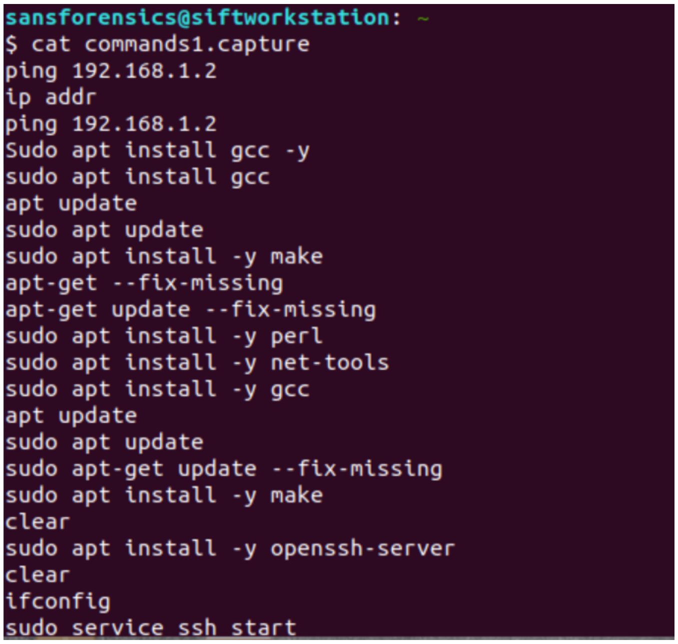
9. Obtain the following information from the Ubuntu machine. Start the capture in SIFT with ***nc -lp 1337 > commands1.capture***. Then, in Ubuntu, use ***sudo cat .bash_history | /mnt/netcat-0.7.1/netcat -c [IP] [Port]***.



```
sansforensics@siftworkstation: ~
$ nc -lp 1337 > commands1.capture
sansforensics@siftworkstation: ~
$ 
```



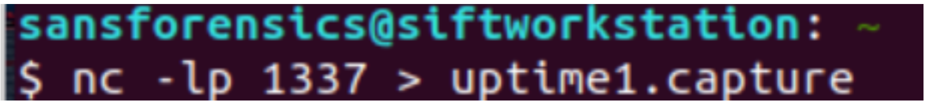
```
john@john:~$ sudo cat .bash_history | /mnt/netcat-0.7.1/netcat -c 192.168.1.2 1337
[sudo] password for john:
john@john:~$ 
```



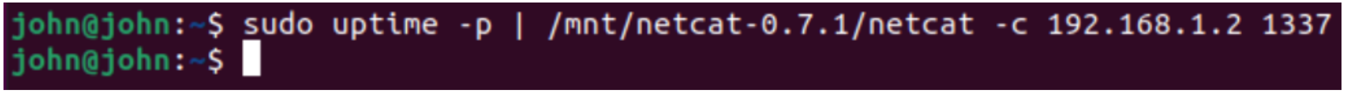
```
sansforensics@siftworkstation: ~
$ cat commands1.capture
ping 192.168.1.2
ip addr
ping 192.168.1.2
Sudo apt install gcc -y
sudo apt install gcc
apt update
sudo apt update
sudo apt install -y make
apt-get --fix-missing
apt-get update --fix-missing
sudo apt install -y perl
sudo apt install -y net-tools
sudo apt install -y gcc
apt update
sudo apt update
sudo apt-get update --fix-missing
sudo apt install -y make
clear
sudo apt install -y openssh-server
clear
ifconfig
sudo service ssh start
```

10 Obtain the list of running processes from the Ubuntu machine with ***lsof.capture***, as shown in class.

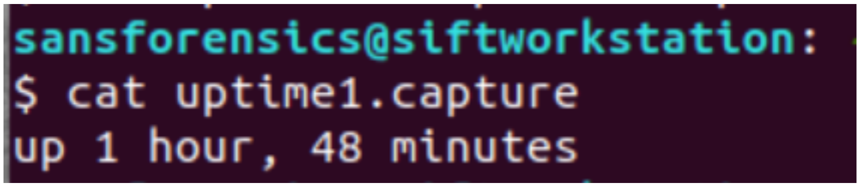
11 Obtain the system uptime from the Ubuntu machine. Start the capture in SIFT with ***nc -lp 1337 > uptime1.capture***. Then, in Ubuntu, use ***sudo uptime -p | /mnt/netcat-0.7.1/netcat -c [IP] [Port]***.



```
sansforensics@siftworkstation: ~
$ nc -lp 1337 > uptime1.capture
```



```
john@john:~$ sudo uptime -p | /mnt/netcat-0.7.1/netcat -c 192.168.1.2 1337
john@john:~$ 
```



```
sansforensics@siftworkstation:
$ cat uptime1.capture
up 1 hour, 48 minutes
```

Hints

- Use the ***ifconfig*** command to verify the connection between the machines (***ifconfig*** was introduced in NET-01).
- It is recommended to shut down the NAT NIC before using SSH in the internal network.
- Use the ***ifconfig*** command to turn on/off network interface cards.
- Ubuntu requires the installation of the OpenSSH server. Use ***apt*** commands to install it (***apt*** was introduced in LNX-04).
- To enable SSH, execute ***service ssh start*** (SSH was introduced in NET-02).
- The SSH default port is 22.
- Use ***git*** commands to clone a repository.
- The ***mkisofs -R*** flag permits execution of copied files to a mounted drive (and it will not work without it).
- Use ***scp [full path to file] [username]@[IP]:/[path to save]*** to transfer a file.
- Use ***rm *.[extension]*** to delete all files of a specific type.
- The ***wc -l*** command is used to count lines, words, or characters.
- Ubuntu credentials are configured during the installation of the operating system.
- Netcat can be used to create a listener over a given port.
- Traffic caught by Netcat can be saved to a file using the redirection **>** operator.