Network lab

> ipconfig (ip address)

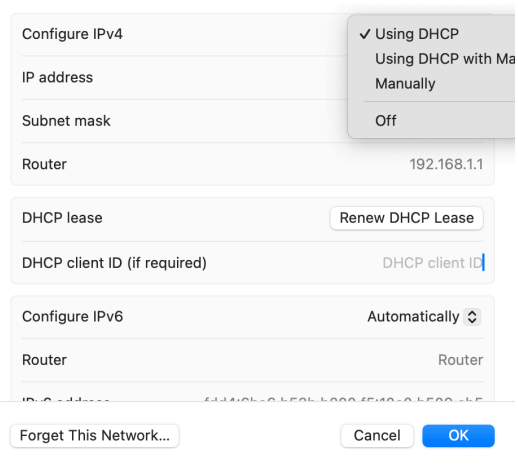
```
maryamabdelraheem@mariamMacBook-Pro ~ % ipconfig getifaddr en0
192.168.1.11
maryamabdelraheem@mariamMacBook-Pro ~ %
```

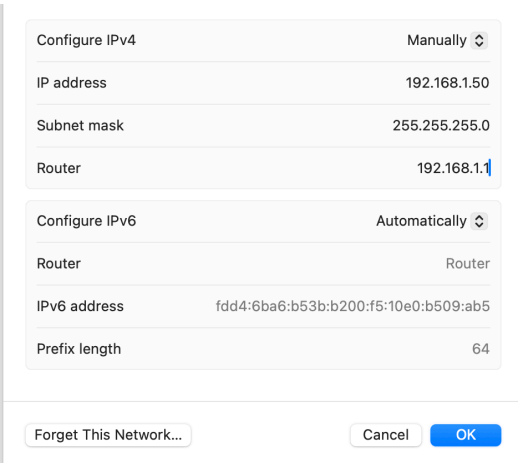
> ipconfig (Mac) == ipconfig/all & ipconfig(windows)

```
maryamabdelraheem@mariamMacBook-Pro ~ % ipconfig
usage: ipconfig <command> <args>
where <command> is one of waitall, getifaddr, ifcount, getoption, getiflist, getsummary, getpacket, getv6packet, getr
a, getdhcpduid, getdhcpiaid, set, setverbose
```

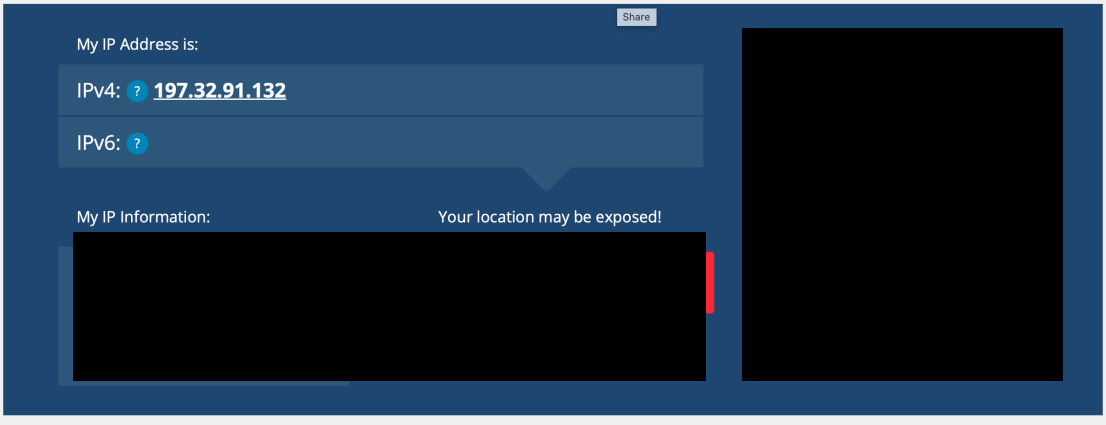
>2. Configure ip adress manually

1.open system settings > choose network> choose network > wifi





//whatismyipadress



>>3.ping command

>3.1check connectivity (ping 192.168.1.1)

```
maryamabdelraheem@mariamMacBook-Pro ~ % ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=3.766 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=3.147 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=3.707 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=3.555 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=3.619 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=4.198 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=3.845 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=4.116 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=3.759 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=3.692 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=64 time=2.491 ms
64 bytes from 192.168.1.1: icmp_seq=11 ttl=64 time=5.601 ms
64 bytes from 192.168.1.1: icmp_seq=12 ttl=64 time=6.794 ms
64 bytes from 192.168.1.1: icmp_seq=13 ttl=64 time=3.656 ms
64 bytes from 192.168.1.1: icmp_seq=14 ttl=64 time=3.659 ms
64 bytes from 192.168.1.1: icmp_seq=15 ttl=64 time=3.368 ms
64 bytes from 192.168.1.1: icmp_seq=16 ttl=64 time=3.823 ms
64 bytes from 192.168.1.1: icmp_seq=17 ttl=64 time=4.365 ms
64 bytes from 192.168.1.1: icmp_seq=18 ttl=64 time=3.622 ms
```

>3.2 check availability of website

```
maryamabdelraheem@mariamMacBook-Pro ~ % ping google.com
PING google.com (142.251.37.238): 56 data bytes
64 bytes from 142.251.37.238: icmp_seq=0 ttl=117 time=61.014 ms
64 bytes from 142.251.37.238: icmp_seq=1 ttl=117 time=61.912 ms
64 bytes from 142.251.37.238: icmp_seq=2 ttl=117 time=58.840 ms
64 bytes from 142.251.37.238: icmp_seq=3 ttl=117 time=60.326 ms
64 bytes from 142.251.37.238: icmp_seq=4 ttl=117 time=59.407 ms
64 bytes from 142.251.37.238: icmp_seq=5 ttl=117 time=62.051 ms
64 bytes from 142.251.37.238: icmp_seq=6 ttl=117 time=59.708 ms
64 bytes from 142.251.37.238: icmp_seq=7 ttl=117 time=77.731 ms
64 bytes from 142.251.37.238: icmp_seq=8 ttl=117 time=66.871 ms
64 bytes from 142.251.37.238: icmp_seq=9 ttl=117 time=61.227 ms
64 bytes from 142.251.37.238: icmp_seq=10 ttl=117 time=61.855 ms
64 bytes from 142.251.37.238: icmp_seq=11 ttl=117 time=62.276 ms
64 bytes from 142.251.37.238: icmp_seq=12 ttl=117 time=62.036 ms
^C
--- google.com ping statistics ---
13 packets transmitted, 13 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 58.840/62.712/77.731/4.732 ms
maryamabdelraheem@mariamMacBook-Pro ~ %
```

>3.3 continuous ping (the default)

```
maryamabdelraheem@mariamMacBook-Pro ~ % ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=3.587 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=3.975 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=3.063 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.442 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.442/3.267/3.975/0.576 ms
maryamabdelraheem@mariamMacBook-Pro ~ %
```

>3.4 control number of pings packets

```
maryamabdelraheem@mariamMacBook-Pro ~ % ping -c 7 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=3.546 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=4.090 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=6.677 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=4.931 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=9.810 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=4.478 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=5.398 ms

--- 192.168.1.1 ping statistics ---
7 packets transmitted, 7 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.546/5.561/9.810/1.968 ms
maryamabdelraheem@mariamMacBook-Pro ~ %
```

>3.5 control packet size

```
maryamabdelraheem@mariamMacBook-Pro ~ % ping -s 2000 163.121.25.40
PING 163.121.25.40 (163.121.25.40): 2000 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
^C
--- 163.121.25.40 ping statistics ---
9 packets transmitted, 0 packets received, 100.0% packet loss
maryamabdelraheem@mariamMacBook-Pro ~ %
```

>3.6 control packet size AND number of packets

```
maryamabdelraheem@mariamMacBook-Pro ~ % ping -s 2000 -c 6 163.121.12.40
PING 163.121.12.40 (163.121.12.40): 2000 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4

--- 163.121.12.40 ping statistics ---
6 packets transmitted, 0 packets received, 100.0% packet loss
maryamabdelraheem@mariamMacBook-Pro ~ %
```

>>4. MAC adress

```
maryamabdelraheem@mariamMacBook-Pro ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether ae:b8:e8:49:bc:2a
        inet6 fe80::181a:db0d:e2a:d234%en0 prefixlen 64 secured scopeid 0xb
        inet6 fdd4:6ba6:b53b:b200:f5:10e0:b509:ab5 prefixlen 64 autoconf secured
        inet 192.168.1.21 netmask 0xffffff00 broadcast 192.168.1.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
maryamabdelraheem@mariamMacBook-Pro ~ %
```

Or:

```
maryamabdelraheem@mariamMacBook-Pro ~ % networksetup -getmacaddress en0
Ethernet Address: 3c:06:30:31:4e:7c (Device: en0)
maryamabdelraheem@mariamMacBook-Pro ~ %
```

>>5.Get address of other devices (arp -a)

```
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=3.796 ms
^C
--- 192.168.1.1 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.637/4.827/7.367/1.321 ms
maryamabdelraheem@mariamMacBook-Pro ~ % arp -a
? (169.254.169.254) at (incomplete) on en0 [ethernet]
? (192.168.1.1) at d4:6b:a6:b5:3b:b2 on en0 ifscope [ethernet]
? (192.168.1.15) at ea:68:58:17:93:b9 on en0 ifscope [ethernet]
? (192.168.1.17) at 8e:80:8f:49:17:51 on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
mdns.mcast.net (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

>5.1 to delete(sudo arp -a -d)

>>6.opened ports and sessions

>6.1 netstat -n

```
maryamabdelraheem@mariamMacBook-Pro ~ % netstat -n
Active Internet connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  192.168.1.21.49648     13.107.213.43.443      ESTABLISHED
tcp4       0      0  192.168.1.21.49641     34.123.33.186.443      ESTABLISHED
tcp4       0      0  192.168.1.21.49620     34.123.33.186.443      ESTABLISHED
tcp4       0      0  192.168.1.21.49619     34.123.33.186.443      ESTABLISHED
tcp4       0      0  192.168.1.21.49618     34.123.33.186.443      ESTABLISHED
tcp4       0      0  192.168.1.21.49616     34.123.33.186.443      ESTABLISHED
tcp4       0      0  192.168.1.21.49586     135.225.242.134.443    ESTABLISHED
tcp4       0      0  192.168.1.21.49584     52.123.159.178.443     ESTABLISHED
tcp4       0      0  192.168.1.21.49580     74.248.74.126.443      ESTABLISHED
tcp4       0      0  192.168.1.21.49578     52.111.231.53.443      ESTABLISHED
tcp4       0      0  192.168.1.21.49572     52.123.134.244.443     ESTABLISHED
tcp4       0      0  192.168.1.21.49568     52.112.122.48.443      ESTABLISHED
tcp6       0      0  fe80::6fc1:42d4:.1025  fe80::c54b:d7e0:.1026  ESTABLISHED
tcp6       0      0  fe80::6fc1:42d4:.1024  fe80::c54b:d7e0:.1024  ESTABLISHED
tcp4       0      0  192.168.1.11.49494     34.170.65.59.443       ESTABLISHED
tcp4       0      0  192.168.1.11.49428     216.24.57.7.443        ESTABLISHED
tcp4       0      0  192.168.1.11.49427     216.24.57.7.443        ESTABLISHED
tcp6       0      0  fe80::181a:db0d:.49152 fe80::14b1:28fd:.63921 ESTABLISHED
tcp4       0      0  192.168.1.21.54161     17.248.209.16.443      TIME_WAIT
tcp4       0      0  192.168.1.21.54160     17.138.128.4.443       ESTABLISHED
tcp4       0      0  192.168.1.21.54158     17.248.209.16.443      TIME_WAIT
tcp4       0      0  192.168.1.21.54157     17.248.209.62.443      TIME_WAIT
tcp4       0      0  192.168.1.21.54156     17.248.209.62.443      TIME_WAIT
tcp4       0      0  192.168.1.21.54155     17.248.215.129.443     ESTABLISHED
tcp4       0   5487  192.168.1.21.54154     17.248.209.62.443      ESTABLISHED
tcp4       0      0  192.168.1.21.54121     172.64.155.209.443     TIME_WAIT
tcp4       0      0  192.168.1.21.54058     104.18.32.47.443       ESTABLISHED
tcp4       0      0  192.168.1.21.54056     172.64.148.171.443     ESTABLISHED
tcp4       0      0  192.168.1.21.53883     172.64.155.209.443     ESTABLISHED
tcp4       0     50  192.168.1.21.53872     104.18.39.21.443       ESTABLISHED
tcp4       0      0  192.168.1.21.53861     17.188.185.138.5223    ESTABLISHED
udp4       0      0  *.*                    *.*
udp4       0      0  *.*                    *.*
udp4       0      0  *.*                    *.*
udp4       0      0  *.56393                *.*
udp4       0      0  192.168.1.21.50013     *.*
udp4       0      0  192.168.1.21.50036     *.*
udp4       0      0  192.168.1.21.50041     *.*
udp4       0      0  192.168.1.21.50048     *.*
udp6       0      0  *.54344                *.*
udp4       0      0  *.54344                *.*
udp4       0      0  224.0.0.1.5350         *.*
udp4       0      0  *.*                    *.*
udp46      0      0  *.50088                *.*
udp46      0      0  *.50075                *.*
udp46      0      0  *.50430                *.*
udp6       0      0  *.3722                 *.*
udp4       0      0  *.*                    *.*
```

```
unexpected kind 267 which 0x10b
Registered kernel control modules
id       flags    pcbcount rcvbuf   sndbuf   name
       1       5        0     8192    32768 com.apple.network.tcp_ccdebug
       2      28        1     8192   131072 com.apple.flow-divert
       3       1       23    65536    65536 com.apple.net.netagent
       4       9        0   524288   524288 com.apple.content-filter
       5      29        6   524288   524288 com.apple.net.utun_control
       6      21        0    65536    65536 com.apple.net.ipsec_control
       7       0       47     8192     2048 com.apple.netsrc
       8      18        3     8192     2048 com.apple.network.statistics
       9       1        0     8192     2048 com.apple.network.advisory
       a       1        0    65536    65536 com.apple.net.rvi_control
       b       4        0    65536     2048 com.apple.spmi.nfc
       c       4        0    65536     2048 com.apple.uart.wlan-debug
       d       4        0     8192     2048 com.apple.uart.sk.wlan-debug
       e       4        0    65536     2048 com.apple.uart.debug-console
       f       4        0     8192     2048 com.apple.uart.sk.debug-console
```

>6.2 netstat -a

```
maryamabdelraheem@mariamMacBook-Pro ~ % netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  192.168.1.21.49672     52.182.143.215.https   ESTABLISHED
tcp4       0      0  192.168.1.21.49671     52.182.143.215.https   ESTABLISHED
tcp4       0      0  192.168.1.21.49670     52.182.143.215.https   ESTABLISHED
tcp4       0      0  192.168.1.21.49669     150.171.22.17.https    ESTABLISHED
tcp4       0      0  192.168.1.21.49668     13.89.179.13.https     ESTABLISHED
tcp4       0      0  192.168.1.21.49658     52.123.133.231.https   ESTABLISHED
tcp4       0      0  192.168.1.21.49656     20.189.173.17.https    ESTABLISHED
tcp4       0      0  192.168.1.21.49655     52.123.129.14.https    ESTABLISHED
tcp4       0      0  192.168.1.21.49654     52.123.129.14.https    ESTABLISHED
tcp4       0      0  192.168.1.21.49653     150.171.22.17.https    ESTABLISHED
tcp4       0      0  192.168.1.21.49652     20.111.1.3.https       ESTABLISHED
tcp4       0      0  192.168.1.21.49651     52.113.194.132.https   ESTABLISHED
tcp4       0      0  192.168.1.21.49650     52.123.129.14.https    ESTABLISHED
tcp4       0      0  192.168.1.21.49641     186.33.123.34.bc.https ESTABLISHED
tcp4       0      0  192.168.1.21.49620     186.33.123.34.bc.https ESTABLISHED
tcp4       0      0  192.168.1.21.49619     186.33.123.34.bc.https ESTABLISHED
tcp4       0      0  192.168.1.21.49618     186.33.123.34.bc.https ESTABLISHED
tcp4       0      0  192.168.1.21.49616     186.33.123.34.bc.https ESTABLISHED
tcp4       0      0  192.168.1.21.49586     135.225.242.134.https  ESTABLISHED
tcp4       0      0  192.168.1.21.49584     52.123.159.178.https   ESTABLISHED
tcp4       0      0  192.168.1.21.49580     74.248.74.126.https    ESTABLISHED
tcp4       0      0  192.168.1.21.49578     52.111.231.53.https    ESTABLISHED
tcp4       0      0  192.168.1.21.49572     52.123.134.244.https   ESTABLISHED
tcp4       0      0  192.168.1.21.49568     52.112.122.48.https    ESTABLISHED
^C
maryamabdelraheem@mariamMacBook-Pro ~ %
```

>6.3 filter by ipaddress
netstat -an | grep 192.168.1.1

```
maryamabdelraheem@mariamMacBook-Pro ~ % netstat -an | grep 192.168.1.1
tcp4       0      0  192.168.1.11.49494     34.170.65.59.443       ESTABLISHED
tcp4       0      0  192.168.1.11.49428     216.24.57.7.443        ESTABLISHED
tcp4       0      0  192.168.1.11.49427     216.24.57.7.443        ESTABLISHED
maryamabdelraheem@mariamMacBook-Pro ~ %
```

>>7. DNS

>7.1 nslookup 87.248.113.14

```
maryamabdelraheem@mariamMacBook-Pro ~ % nslookup 87.248.113.14
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
14.113.248.87.in-addr.arpa      name = et23-1.bas1-1-edg.amb.yahoo.com.

Authoritative answers can be found from:

maryamabdelraheem@mariamMacBook-Pro ~ %
```

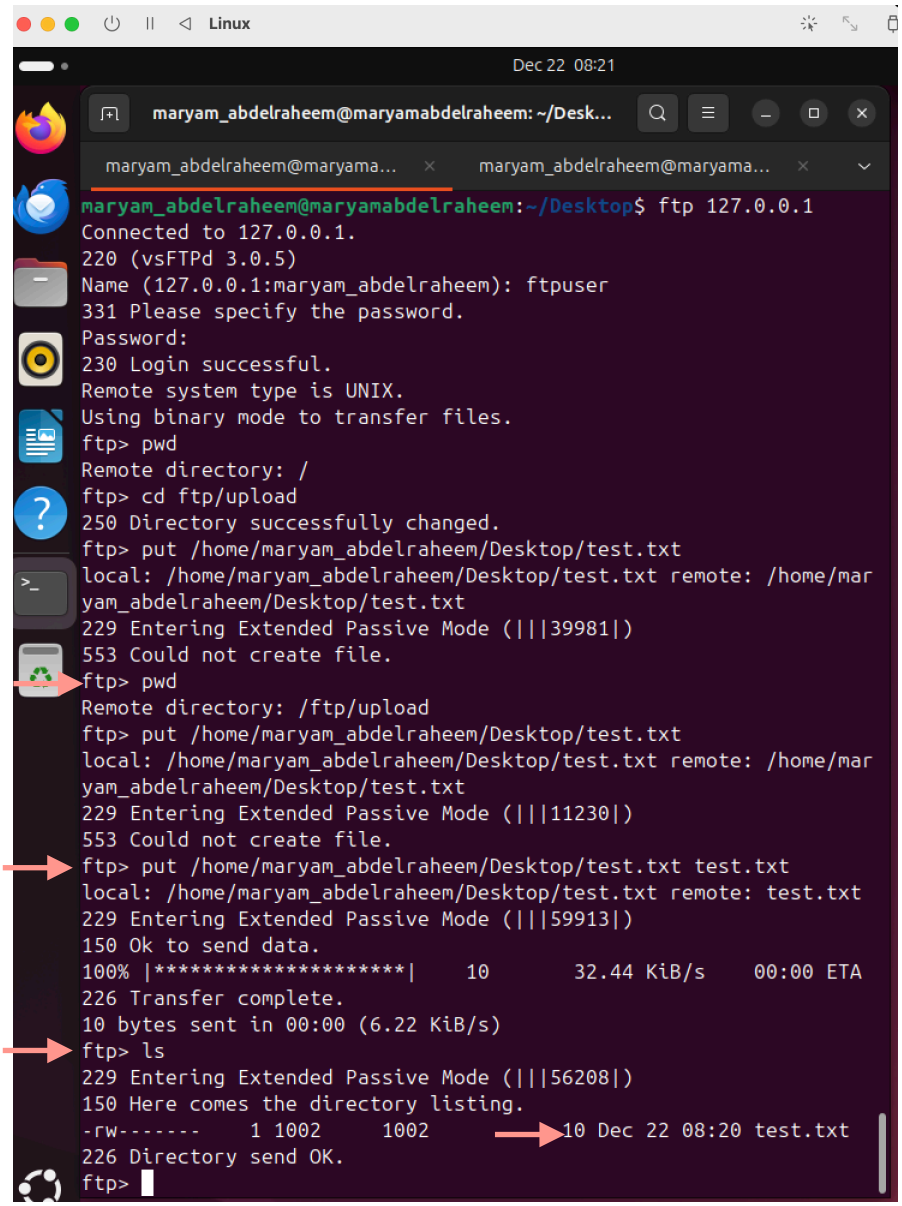
>7.2 nslookup yahoo.com

```
maryamabdelraheem@mariamMacBook-Pro ~ % nslookup yahoo.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   yahoo.com
Address: 98.137.11.164
Name:   yahoo.com
Address: 74.6.143.25
Name:   yahoo.com
Address: 74.6.231.20
Name:   yahoo.com
Address: 74.6.143.26
Name:   yahoo.com
Address: 74.6.231.21
Name:   yahoo.com
Address: 98.137.11.163

maryamabdelraheem@mariamMacBook-Pro ~ %
```

>>8.port scanning

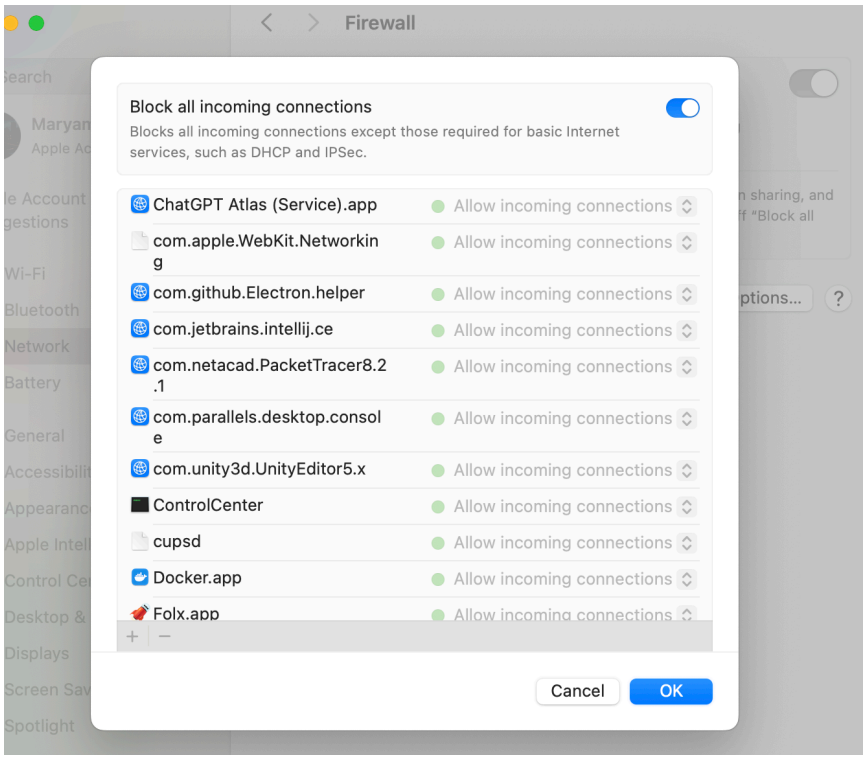
The built-in FTP service on macOS is deprecated and cannot be enabled on recent versions. Therefore, a Linux virtual machine was used to implement the FTP server with proper authentication, home directory configuration, and authorization.

>1.start ftp server



>>12. Advanced firewall options

>> 12.1 block all incoming connections

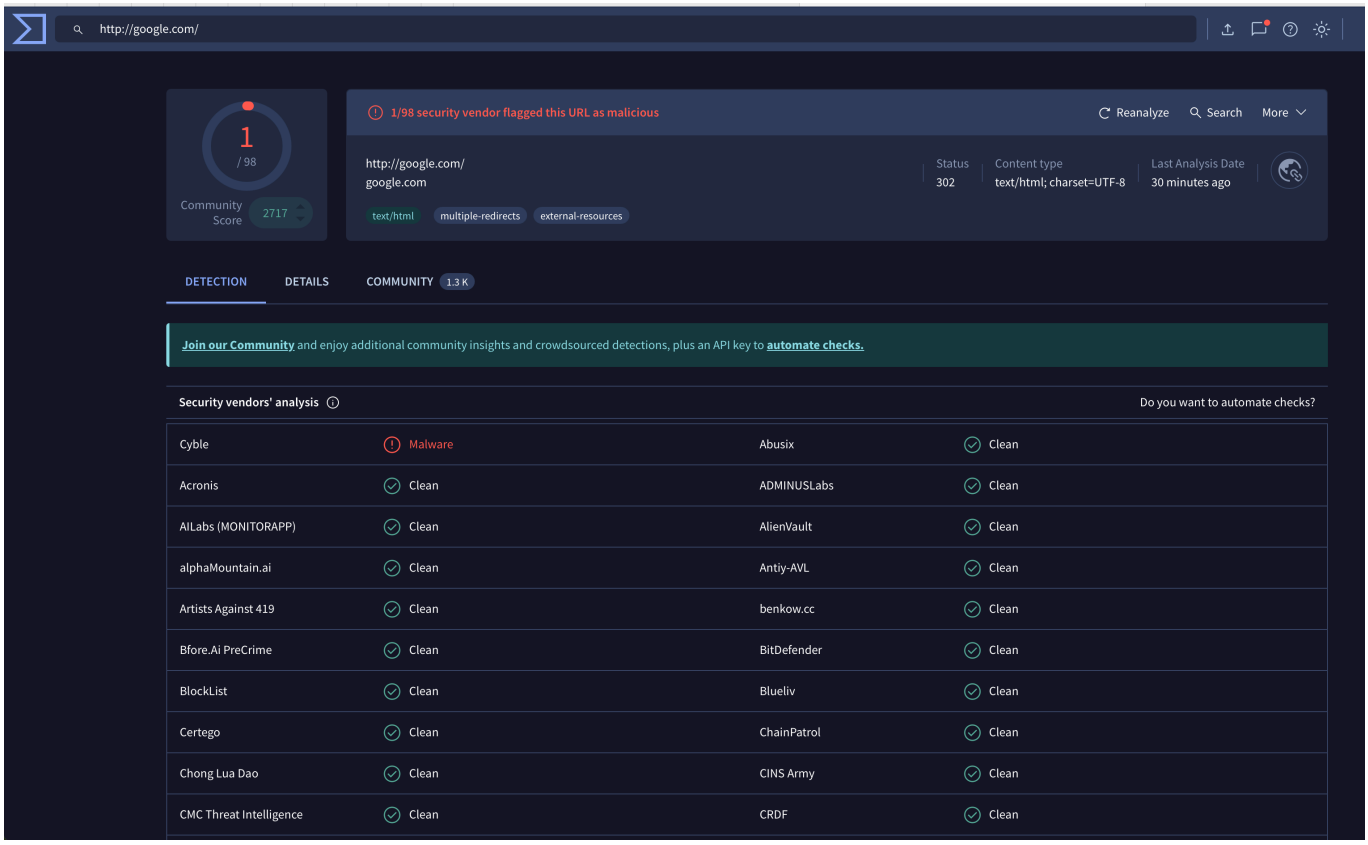


>after blocking the icmp:

```
[maryamabdelraheem@mariamMacBook-Pro ~ % ping 127.0.0.1
 PING 127.0.0.1 (127.0.0.1): 56 data bytes
 Request timeout for icmp_seq 0
 Request timeout for icmp_seq 1
 Request timeout for icmp_seq 2
 Request timeout for icmp_seq 3
 Request timeout for icmp_seq 4
 Request timeout for icmp_seq 5
 Request timeout for icmp_seq 6
```

>>13. Check malicious website and links

>>12-check



malicious software
>check on parallel app