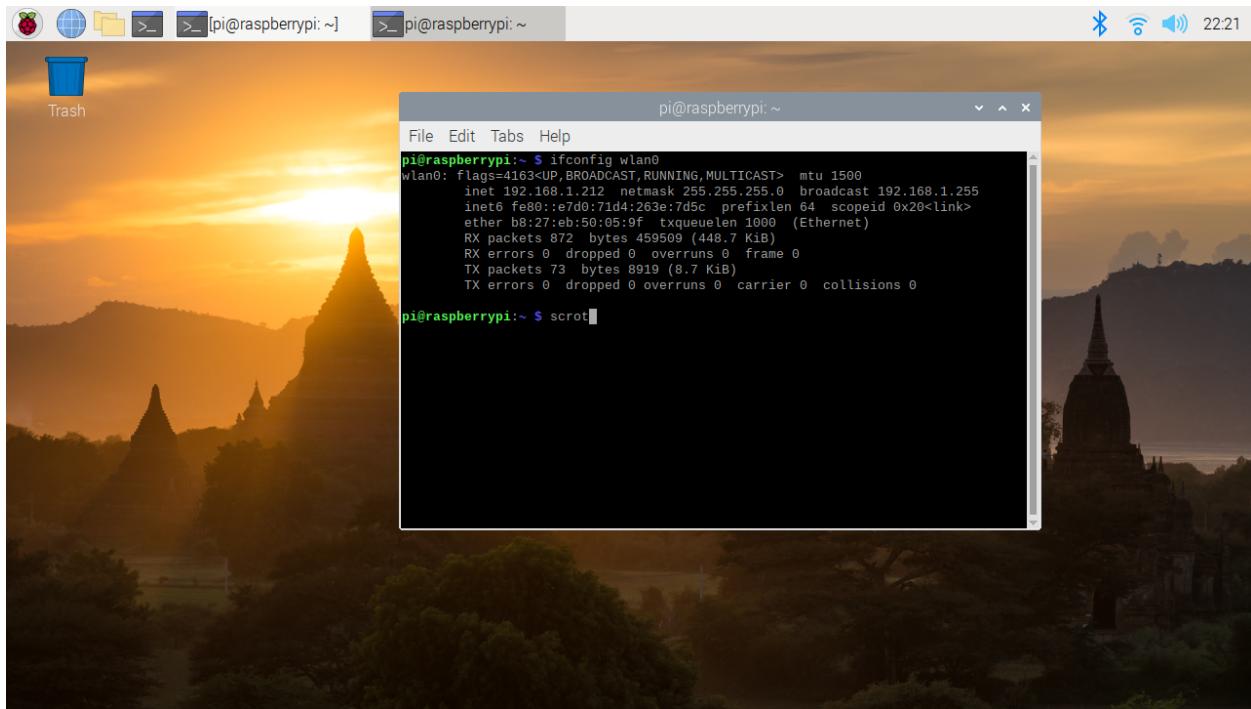
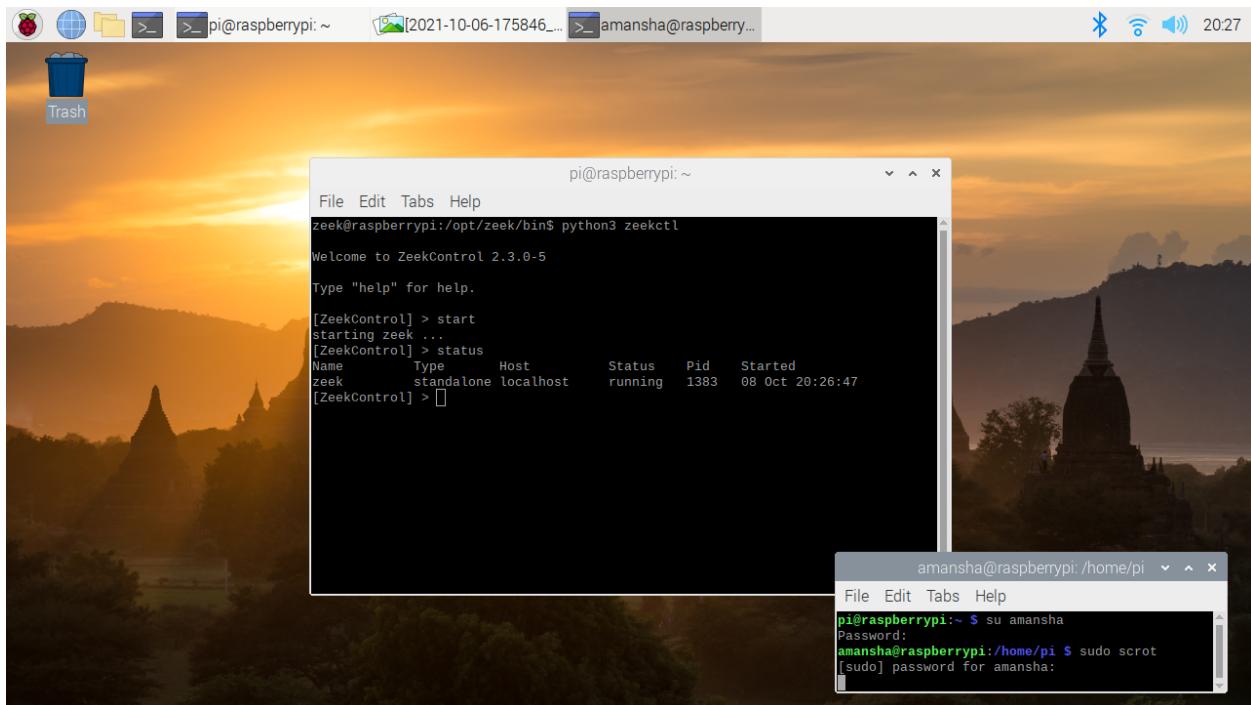


Amir Mansha
Lab #2

2.



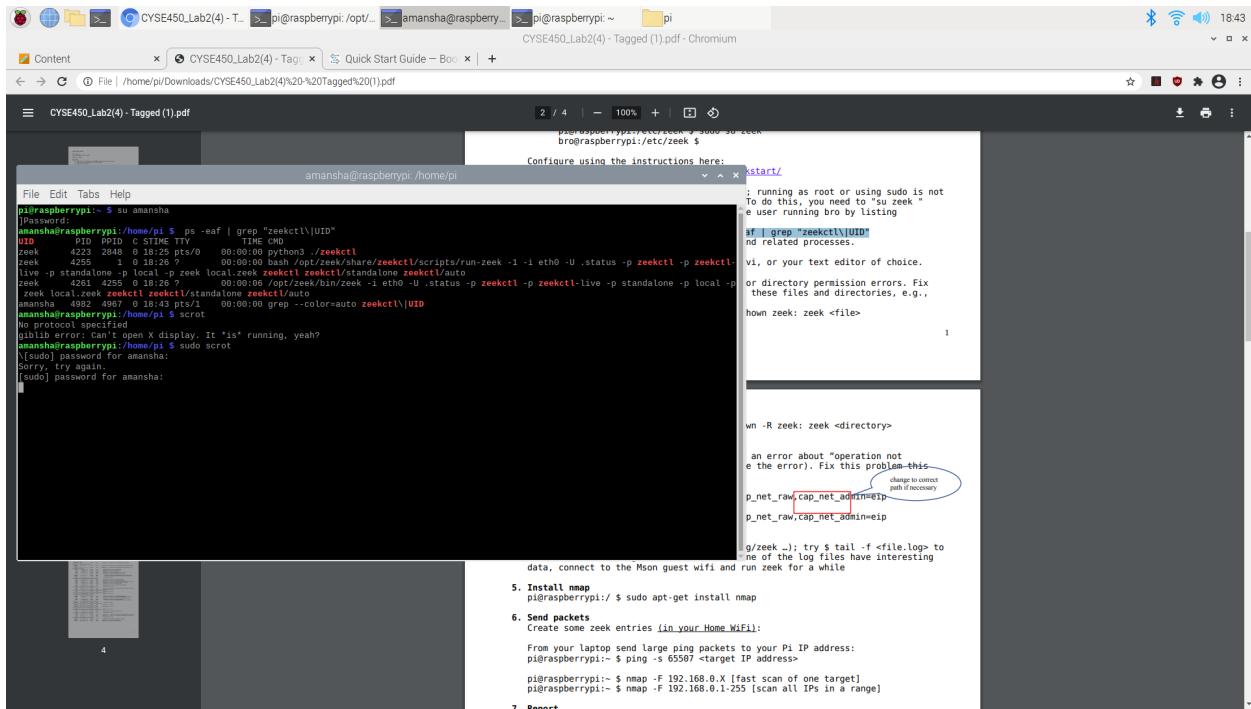
3.



Amir Mansha

Lab #2

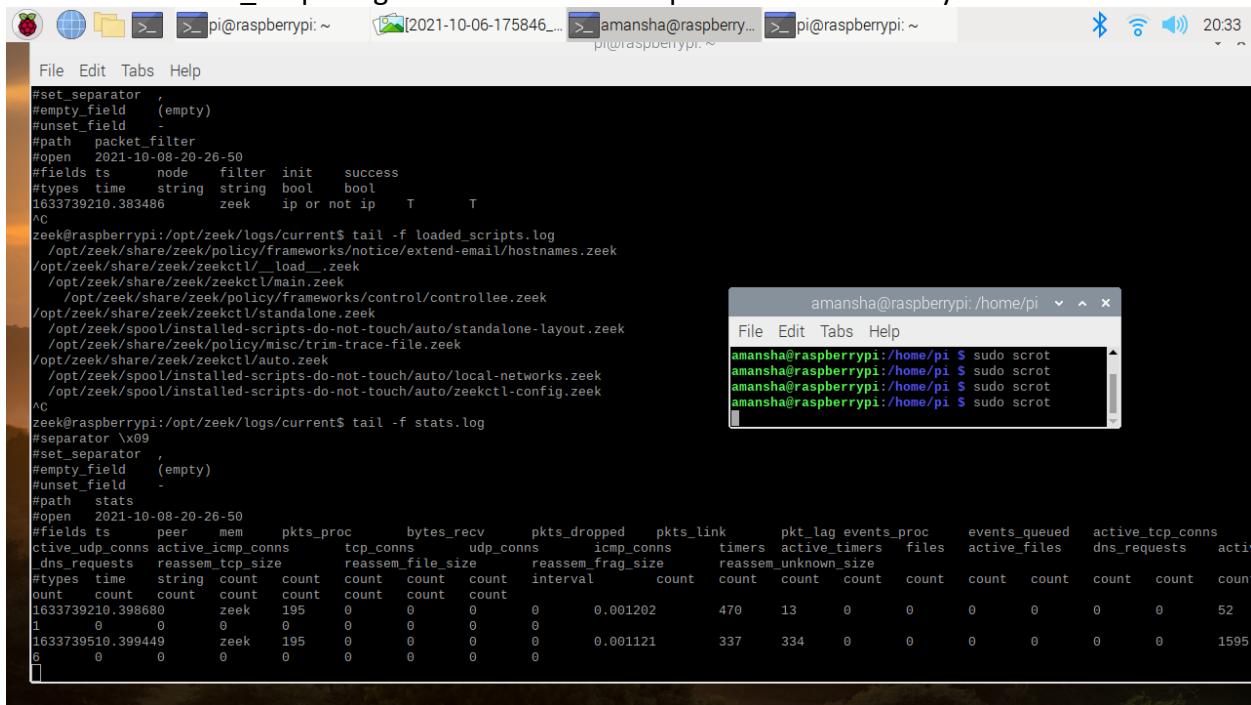
4.



The screenshot shows a Chromium browser window displaying a PDF document titled "CYSE450_Lab2(4)-Tagged(1).pdf". The document contains instructions for setting up Zeek on a Raspberry Pi. It includes a terminal session showing commands like "zeekctl live -p zeekctl-live -p standalone -p local -p zeekctl", and a note about running as root or using sudo. A tooltip highlights a specific line of code related to file paths, specifically "p_net_raw_cap_net_admin=elp", with a callout bubble pointing to it.

5.

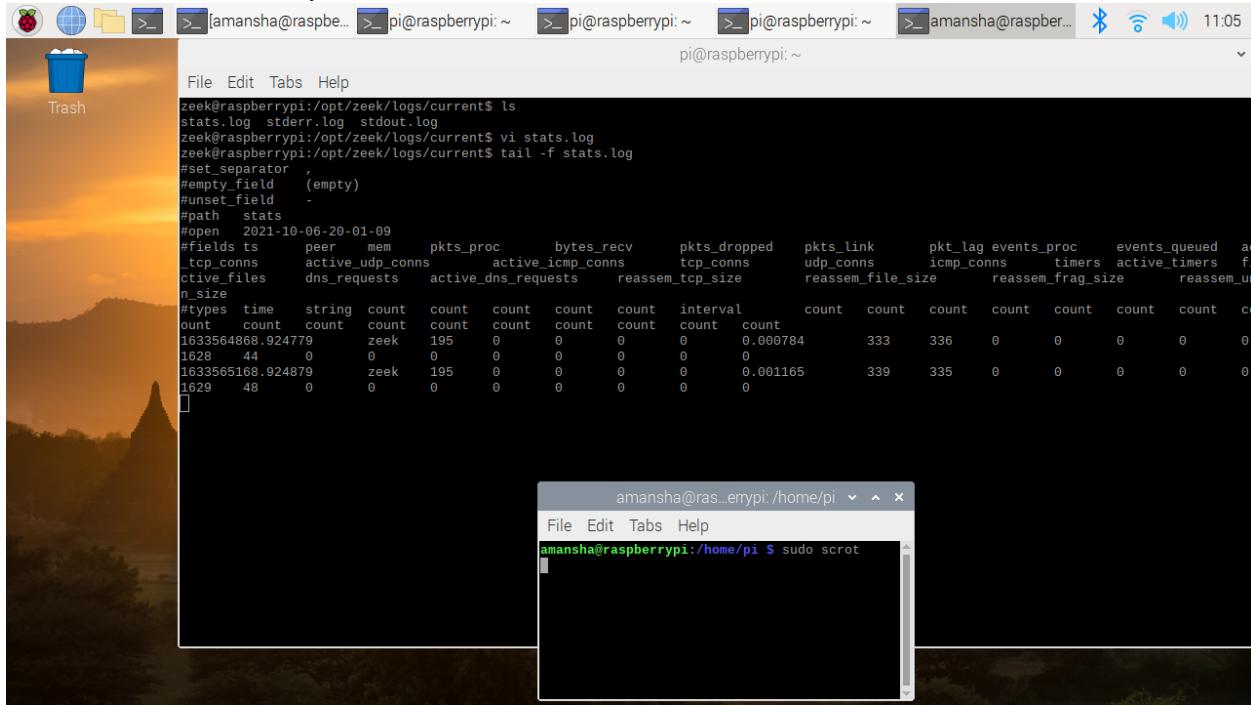
I think the Loaded_scripts.log file means all the scripts that are loaded by zeek.



The screenshot shows a terminal window with two main sections. The top section displays the contents of the "loaded_scripts.log" file, which lists various Zeek scripts and their details. The bottom section displays the "stats.log" file, which provides network statistics. A smaller terminal window is also visible in the background.

Amir Mansha
Lab #2

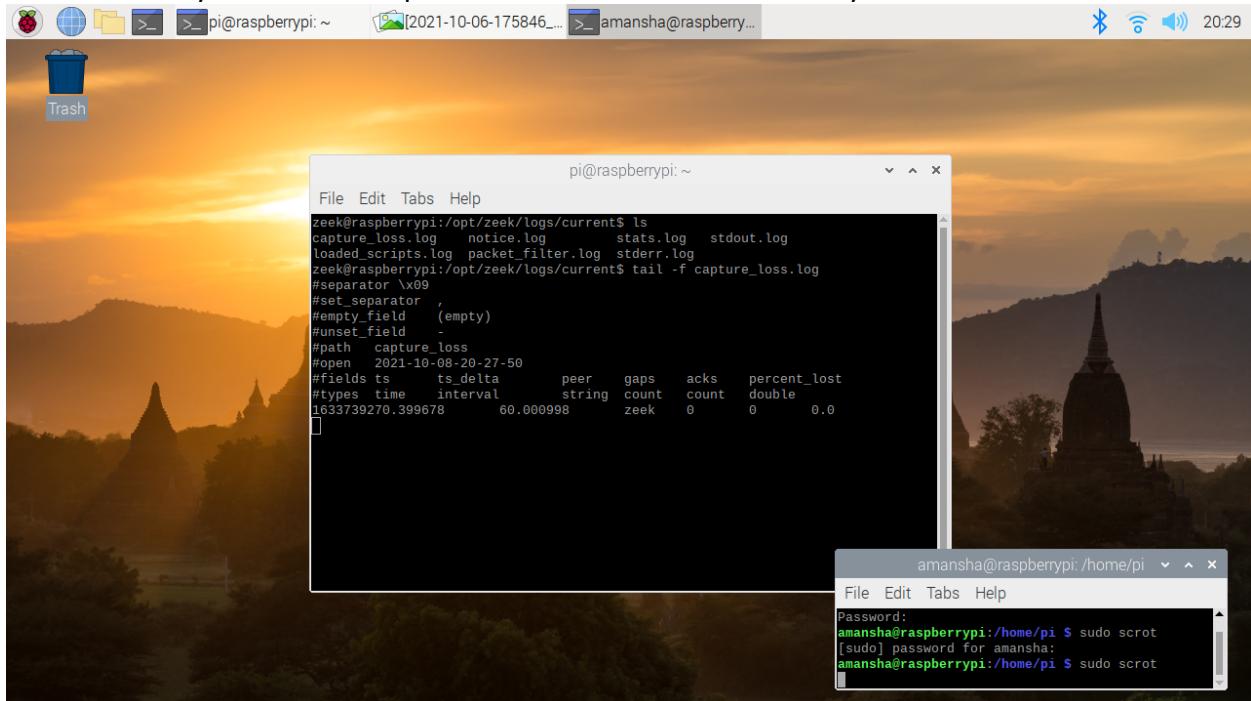
In the stats.log file there are 2 events. I think it means it logged 2 packets and their statistics such as their time stamp and time interval.



```
zeek@raspberrypi:/opt/zeek/logs/current$ ls
stats.log stderr.log stdout.log
zeek@raspberrypi:/opt/zeek/logs/current$ tail -f stats.log
#separator ,
#empty_field  (empty)
#unset_field -
#path  stats
#open 2021-10-06-20-01-09
#fields ts peer mem pkts_proc bytes_recv pkts_dropped pkts_link pkt_lag events_proc events_queued ac
_ltcp_conn active_udp_conn active_icmp_conn tcp_conn udp_conn icmp_conn timers active_timers f
ctive_files dns_requests active_dns_requests reassem_tcp_size reassem_file_size reassem_frag_size reassem_ur
n_size
#types time string count count count count count interval count count count count count count count count
count count count count count count count count count count count count count count count count count count
1633564868.924779 zeek 195 0 0 0 0 0 0.000784 333 336 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1628 44 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1633565108.924879 zeek 195 0 0 0 0 0 0.001165 339 335 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1629 48 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

```
amansha@raspberrypi:/home/pi $ sudo scrot
```

There is 1 event in the capture_loss.log file that I think it means the when the packet loss of the time rate. It says the timestamp and the time interval of the delay.



```
zeek@raspberrypi:/opt/zeek/logs/current$ ls
capture_loss.log notice.log stats.log stdout.log
loaded_scripts.log packet_filter.log stderr.log
zeek@raspberrypi:/opt/zeek/logs/current$ tail -f capture_loss.log
#separator \x09
#empty_field  (empty)
#unset_field -
#path  capture_loss
#open 2021-10-08-20-27-50
#fields ts ts_delta peer gaps acks percent_lost
#types time interval string count count double
1633739270.399678 60.000998 zeek 0 0 0.0
```

```
amansha@raspberrypi:/home/pi $ sudo scrot
```

```
Password: amansha@raspberrypi:/home/pi $ sudo scrot
[sudo] password for amansha:
amansha@raspberrypi:/home/pi $ sudo scrot
```

Amir Mansha
Lab #2

6.
I port scanned my sister's laptop.

```
pi@raspberrypi:~ $ su amansha
Password:
amansha@raspberrypi:/home/pi $ sudo scrot
[sudo] password for amansha:

pi@raspberrypi:~ $ nmap -F 192.168.1.100
Starting Nmap 7.70 ( https://nmap.org ) at 2021-10-08 10:51 EDT
Nmap scan report for 192.168.1.100
Host is up (0.022s latency).

All 100 scanned ports on 192.168.1.100 are closed

Nmap done: 1 IP address (1 host up) scanned in 2.83 seconds
pi@raspberrypi:~ $ nmap -T4 192.168.1.100
Starting Nmap 7.70 ( https://nmap.org ) at 2021-10-08 10:52 EDT
Nmap scan report for 192.168.1.100
Host is up (0.0086s latency).
Not shown: 94 closed ports
PORT      STATE      SERVICE
106/tcp   filtered  pop3pw
515/tcp   filtered  printer
3000/tcp  filtered  ppp
3128/tcp  filtered  squid-http
5900/tcp  filtered  vnc
8009/tcp  filtered  ajp13

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

Amir Mansha
Lab #2

7.

In the notice.log file, it means what zeek notices when things are unusual. Since I was in a isolated home network, zeek did not pick up that much traffic.