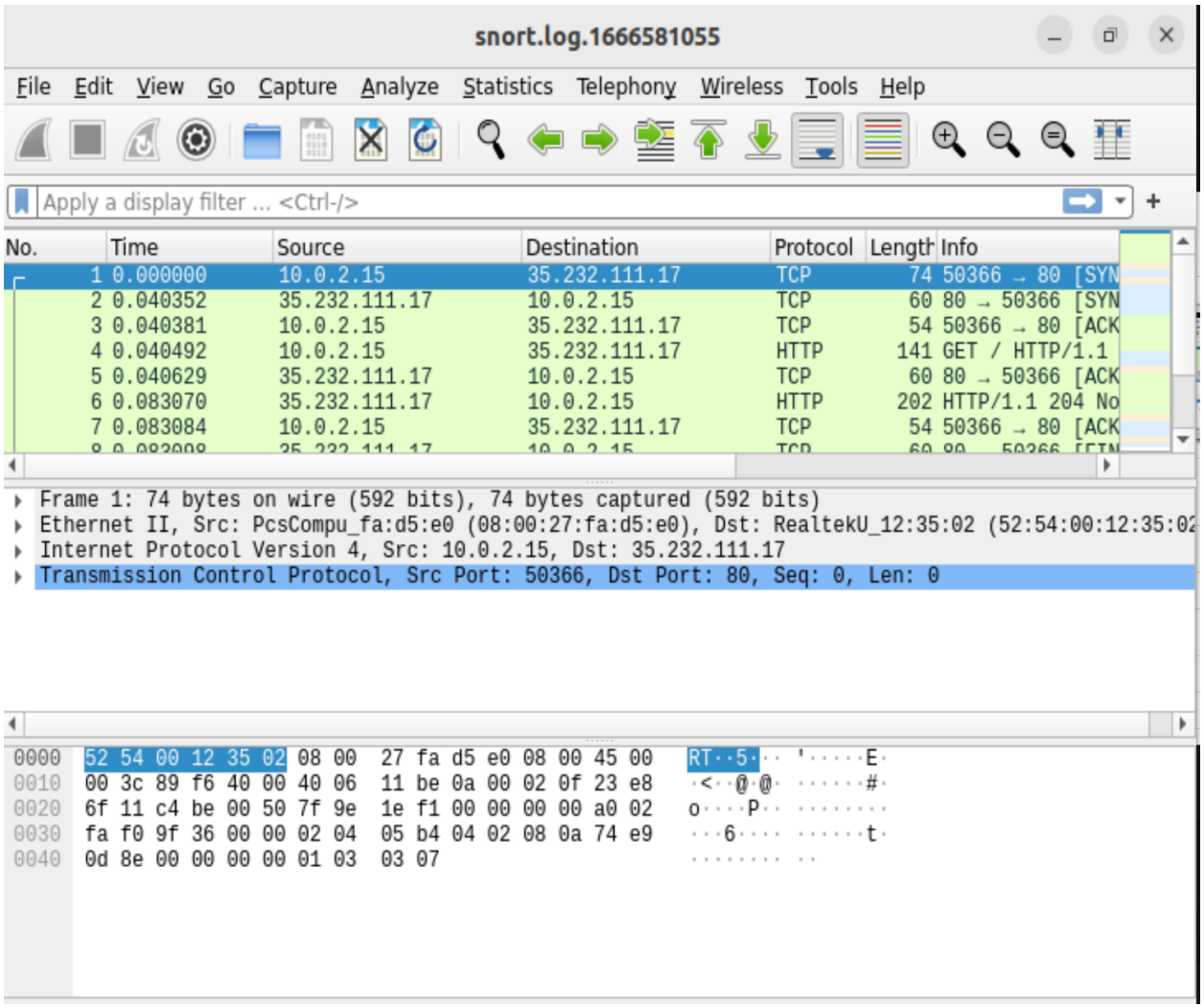

1 sudo apt upgrade
2 sudo apt update
3 sudo apt upgrade
4 sudo apt install wireshark
5 sudo apt install snort
6 snort -h
7 snort -h | less
8 man snort
9 snort -V
10 ip
11 ip a
12 sudo snort -v
13 ip
14 ip a
15 sudo snort -v
16 sudo snort -v -i ens33

```
 17  sudo snort -vd
 18  sudo snort -ve
 19  sudo snort -vde
 20  sudo snort -l
 21  ls
 22  sudo snort -l log-dir
 23  mkdir
 24  mkdir log-dir
 25  sudo snort -l log-dir
 26  ls
 27  cd log-dir
 28  cd ~
 29  cd log-dir
 30  ls
 31  cd~
 32  cd ~
 33  sudo wireshark snort.log.1666581055
 34  cd log-dir
 35  sudo wireshark snort.log.1666581055
 36  sudo gedit /etc/snort/snort2.config
```

—----------

```
johnp@johnp:~$ history
    1  sudo gedit /etc/snort/snort2.conf
    2  sudo gedit /etc/snort/rules/local.rules
    3  sudo snort -A console -A fast -c /etc/snort/snort2.config -i ens33
    4  sudo snort -A console -A fast -c /etc/snort/snort2.conf -i ens33
    5  sudo gedit /etc/snort/rules/local.rules
    6  sudo snort -A console -A fast -c /etc/snort/snort2.conf -i ens33
    7  sudo gedit /etc/snort/snort2.conf
    8  gedit /etc/snort/classification.config
    9  sudo gedit /etc/snort/rules/local.rules
   10  sudo snort -A console -A fast -c /etc/snort/snort2.conf -i ens33
   11  gedit /etc/snort/classification.config
   12  sudo snort -A console -A fast -c /etc/snort/snort2.conf -i ens33
   13  sudo ls -l /var/log/snort
   14  sudo wireshark /var/log/snort/snort.log.2.gz
   15  sudo.rm /var/log/snort/alert
   16  sudo rm /var/log/snort/alert
   17  sudo snort -A console -A full -c /etc/snort/snort2.conf -i ens33
   18  ls -l /etc/snort/rules
   19  cat /etc/snort/rules/dns.rules
```