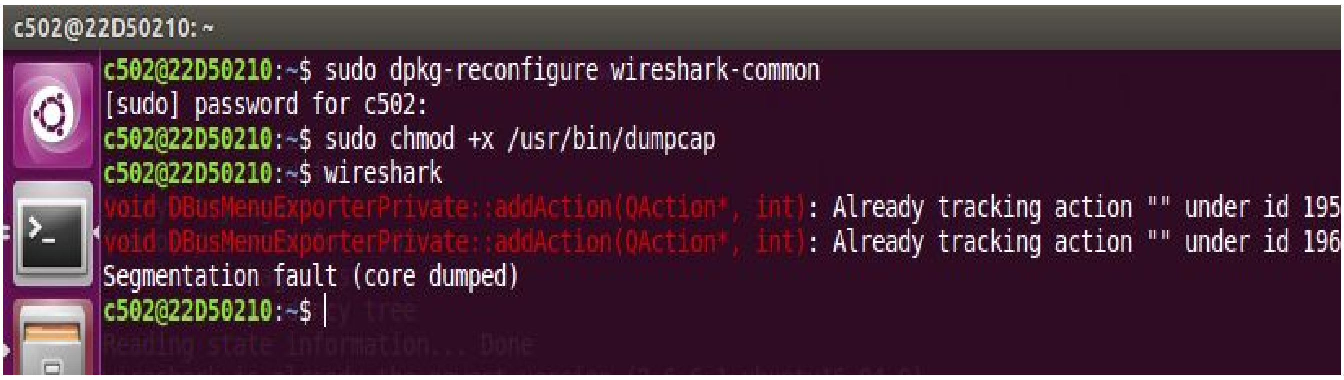
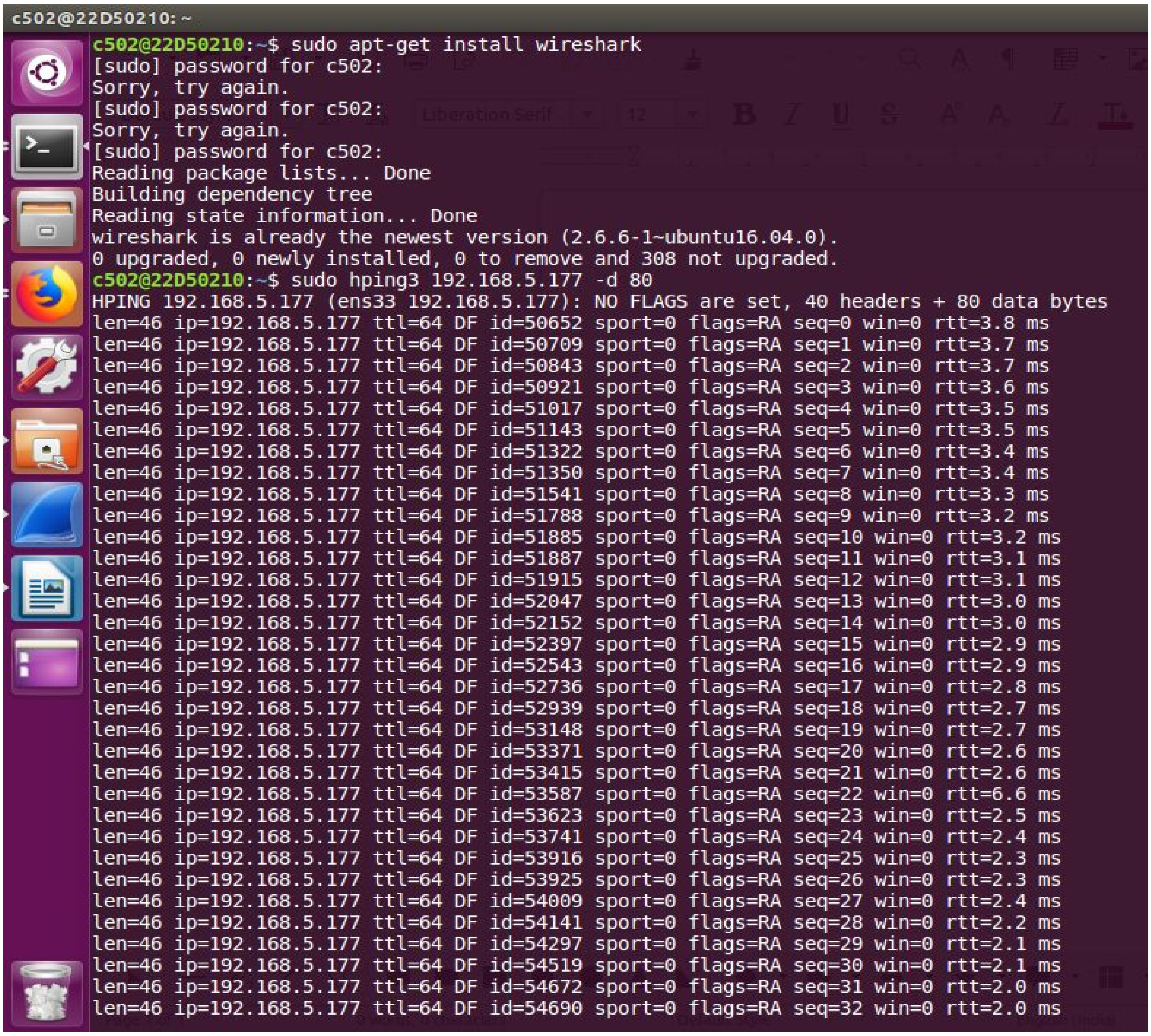
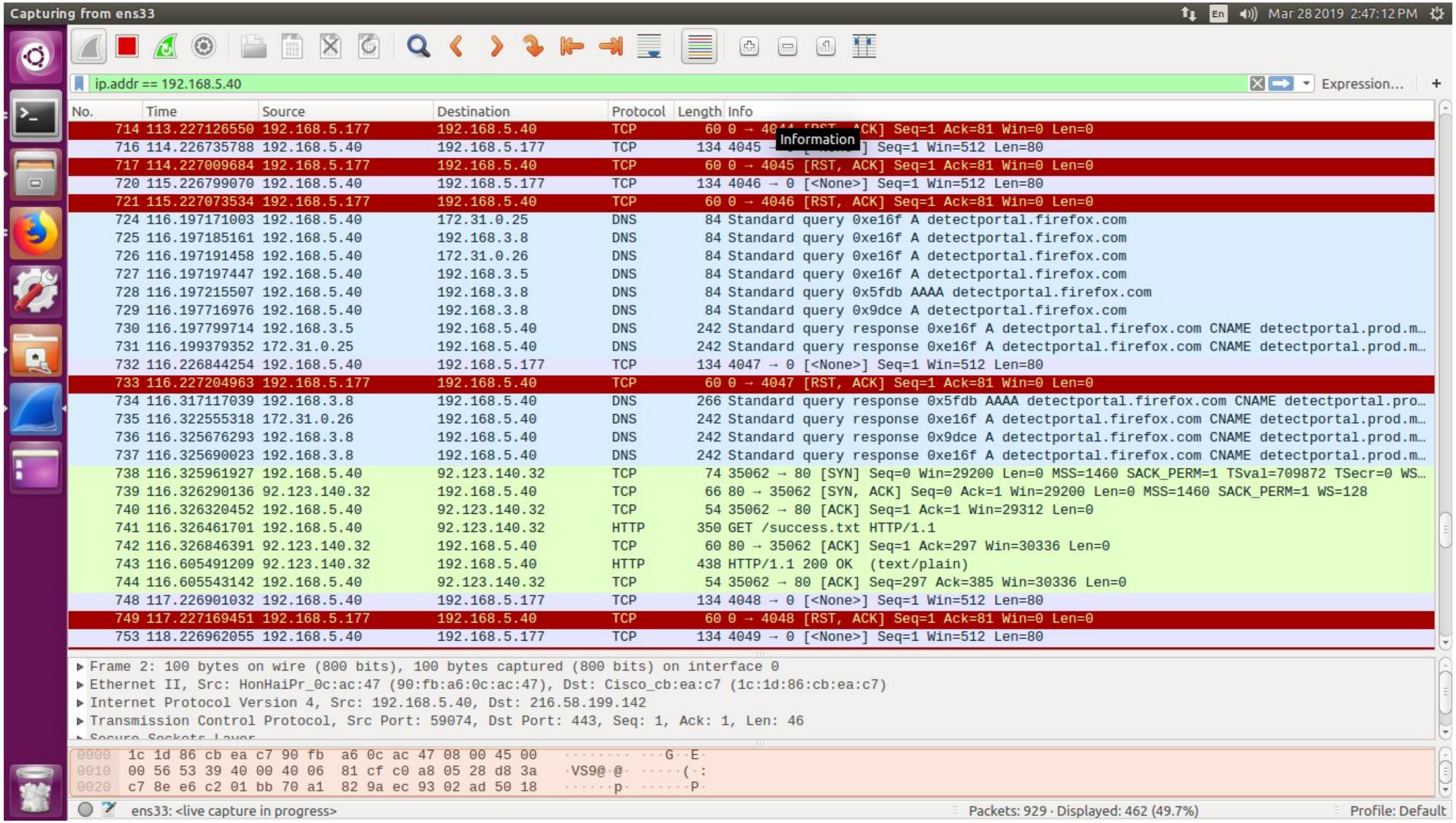
DOS ATTACK



```
c502@22D50210: ~
c502@22D50210:~$ sudo dpkg-reconfigure wireshark-common
[sudo] password for c502:
c502@22D50210:~$ sudo chmod +x /usr/bin/dumpcap
c502@22D50210:~$ wireshark
void DBusMenuExporterPrivate::addAction(QAction*, int): Already tracking action "" under id 195
void DBusMenuExporterPrivate::addAction(QAction*, int): Already tracking action "" under id 196
Segmentation fault (core dumped)
c502@22D50210:~$
```



```
c502@22D50210: ~
c502@22D50210:~$ sudo apt-get install wireshark
[sudo] password for c502:
Sorry, try again.
[sudo] password for c502:
Sorry, try again.
[sudo] password for c502:
Reading package lists... Done
Building dependency tree
Reading state information... Done
wireshark is already the newest version (2.6.6-1~ubuntu16.04.0).
0 upgraded, 0 newly installed, 0 to remove and 308 not upgraded.
c502@22D50210:~$ sudo hping3 192.168.5.177 -d 80
HPING 192.168.5.177 (ens33 192.168.5.177): NO FLAGS are set, 40 headers + 80 data bytes
len=46 ip=192.168.5.177 ttl=64 DF id=50652 sport=0 flags=RA seq=0 win=0 rtt=3.8 ms
len=46 ip=192.168.5.177 ttl=64 DF id=50709 sport=0 flags=RA seq=1 win=0 rtt=3.7 ms
len=46 ip=192.168.5.177 ttl=64 DF id=50843 sport=0 flags=RA seq=2 win=0 rtt=3.7 ms
len=46 ip=192.168.5.177 ttl=64 DF id=50921 sport=0 flags=RA seq=3 win=0 rtt=3.6 ms
len=46 ip=192.168.5.177 ttl=64 DF id=51017 sport=0 flags=RA seq=4 win=0 rtt=3.5 ms
len=46 ip=192.168.5.177 ttl=64 DF id=51143 sport=0 flags=RA seq=5 win=0 rtt=3.5 ms
len=46 ip=192.168.5.177 ttl=64 DF id=51322 sport=0 flags=RA seq=6 win=0 rtt=3.4 ms
len=46 ip=192.168.5.177 ttl=64 DF id=51350 sport=0 flags=RA seq=7 win=0 rtt=3.4 ms
len=46 ip=192.168.5.177 ttl=64 DF id=51541 sport=0 flags=RA seq=8 win=0 rtt=3.3 ms
len=46 ip=192.168.5.177 ttl=64 DF id=51788 sport=0 flags=RA seq=9 win=0 rtt=3.2 ms
len=46 ip=192.168.5.177 ttl=64 DF id=51885 sport=0 flags=RA seq=10 win=0 rtt=3.2 ms
len=46 ip=192.168.5.177 ttl=64 DF id=51887 sport=0 flags=RA seq=11 win=0 rtt=3.1 ms
len=46 ip=192.168.5.177 ttl=64 DF id=51915 sport=0 flags=RA seq=12 win=0 rtt=3.1 ms
len=46 ip=192.168.5.177 ttl=64 DF id=52047 sport=0 flags=RA seq=13 win=0 rtt=3.0 ms
len=46 ip=192.168.5.177 ttl=64 DF id=52152 sport=0 flags=RA seq=14 win=0 rtt=3.0 ms
len=46 ip=192.168.5.177 ttl=64 DF id=52397 sport=0 flags=RA seq=15 win=0 rtt=2.9 ms
len=46 ip=192.168.5.177 ttl=64 DF id=52543 sport=0 flags=RA seq=16 win=0 rtt=2.9 ms
len=46 ip=192.168.5.177 ttl=64 DF id=52736 sport=0 flags=RA seq=17 win=0 rtt=2.8 ms
len=46 ip=192.168.5.177 ttl=64 DF id=52939 sport=0 flags=RA seq=18 win=0 rtt=2.7 ms
len=46 ip=192.168.5.177 ttl=64 DF id=53148 sport=0 flags=RA seq=19 win=0 rtt=2.7 ms
len=46 ip=192.168.5.177 ttl=64 DF id=53371 sport=0 flags=RA seq=20 win=0 rtt=2.6 ms
len=46 ip=192.168.5.177 ttl=64 DF id=53415 sport=0 flags=RA seq=21 win=0 rtt=2.6 ms
len=46 ip=192.168.5.177 ttl=64 DF id=53587 sport=0 flags=RA seq=22 win=0 rtt=6.6 ms
len=46 ip=192.168.5.177 ttl=64 DF id=53623 sport=0 flags=RA seq=23 win=0 rtt=2.5 ms
len=46 ip=192.168.5.177 ttl=64 DF id=53741 sport=0 flags=RA seq=24 win=0 rtt=2.4 ms
len=46 ip=192.168.5.177 ttl=64 DF id=53916 sport=0 flags=RA seq=25 win=0 rtt=2.3 ms
len=46 ip=192.168.5.177 ttl=64 DF id=53925 sport=0 flags=RA seq=26 win=0 rtt=2.3 ms
len=46 ip=192.168.5.177 ttl=64 DF id=54009 sport=0 flags=RA seq=27 win=0 rtt=2.4 ms
len=46 ip=192.168.5.177 ttl=64 DF id=54141 sport=0 flags=RA seq=28 win=0 rtt=2.2 ms
len=46 ip=192.168.5.177 ttl=64 DF id=54297 sport=0 flags=RA seq=29 win=0 rtt=2.1 ms
len=46 ip=192.168.5.177 ttl=64 DF id=54519 sport=0 flags=RA seq=30 win=0 rtt=2.1 ms
len=46 ip=192.168.5.177 ttl=64 DF id=54672 sport=0 flags=RA seq=31 win=0 rtt=2.0 ms
len=46 ip=192.168.5.177 ttl=64 DF id=54690 sport=0 flags=RA seq=32 win=0 rtt=2.0 ms
```



```
ip.addr == 192.168.5.40
```

```
No.  Time          Source          Destination     Protocol Length Info
 714 113.227126550 192.168.5.177   192.168.5.40    TCP       60 0 → 4044 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
 716 114.226735788 192.168.5.40    192.168.5.177   TCP      134 4045 → 0 [<None>] Seq=1 Win=512 Len=80
 717 114.227009684 192.168.5.177   192.168.5.40    TCP       60 0 → 4045 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
 720 115.226799070 192.168.5.40    192.168.5.177   TCP      134 4046 → 0 [<None>] Seq=1 Win=512 Len=80
 721 115.227073534 192.168.5.177   192.168.5.40    TCP       60 0 → 4046 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
 724 116.197171003 192.168.5.40    172.31.0.25     DNS       84 Standard query 0xe16f A detectportal.firefox.com
 725 116.197185161 192.168.5.40    192.168.3.8     DNS       84 Standard query 0xe16f A detectportal.firefox.com
 726 116.197191458 192.168.5.40    172.31.0.26     DNS       84 Standard query 0xe16f A detectportal.firefox.com
 727 116.197197447 192.168.5.40    192.168.3.5     DNS       84 Standard query 0xe16f A detectportal.firefox.com
 728 116.197215507 192.168.5.40    192.168.3.8     DNS       84 Standard query 0x5fdb AAAA detectportal.firefox.com
 729 116.197716976 192.168.5.40    192.168.3.8     DNS       84 Standard query 0x9dce A detectportal.firefox.com
 730 116.197799714 192.168.3.5     192.168.5.40    DNS      242 Standard query response 0xe16f A detectportal.firefox.com CNAME detectportal.prod.m…
 731 116.199379352 172.31.0.25     192.168.5.40    DNS      242 Standard query response 0xe16f A detectportal.firefox.com CNAME detectportal.prod.m…
 732 116.226844254 192.168.5.40    192.168.5.177   TCP      134 4047 → 0 [<None>] Seq=1 Win=512 Len=80
 733 116.227204963 192.168.5.177   192.168.5.40    TCP       60 0 → 4047 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
 734 116.317117039 192.168.3.8     192.168.5.40    DNS      266 Standard query response 0x5fdb AAAA detectportal.firefox.com CNAME detectportal.pro…
 735 116.322555318 172.31.0.26     192.168.5.40    DNS      242 Standard query response 0xe16f A detectportal.firefox.com CNAME detectportal.prod.m…
 736 116.325676293 192.168.3.8     192.168.5.40    DNS      242 Standard query response 0x9dce A detectportal.firefox.com CNAME detectportal.prod.m…
 737 116.325690023 192.168.3.8     192.168.5.40    DNS      242 Standard query response 0xe16f A detectportal.firefox.com CNAME detectportal.prod.m…
 738 116.325961927 192.168.5.40    92.123.140.32   TCP       74 35062 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=709872 TSecr=0 WS…
 739 116.326290136 92.123.140.32   192.168.5.40    TCP       66 80 → 35062 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
 740 116.326320452 192.168.5.40    92.123.140.32   TCP       54 35062 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0
 741 116.326461701 192.168.5.40    92.123.140.32   HTTP     350 GET /success.txt HTTP/1.1
 742 116.326846391 92.123.140.32   192.168.5.40    TCP       60 80 → 35062 [ACK] Seq=1 Ack=297 Win=30336 Len=0
 743 116.605491209 92.123.140.32   192.168.5.40    HTTP     438 HTTP/1.1 200 OK  (text/plain)
 744 116.605543142 192.168.5.40    92.123.140.32   TCP       54 35062 → 80 [ACK] Seq=297 Ack=385 Win=30336 Len=0
 748 117.226901032 192.168.5.40    192.168.5.177   TCP      134 4048 → 0 [<None>] Seq=1 Win=512 Len=80
 749 117.227169451 192.168.5.177   192.168.5.40    TCP       60 0 → 4048 [RST, ACK] Seq=1 Ack=81 Win=0 Len=0
 753 118.226962055 192.168.5.40    192.168.5.177   TCP      134 4049 → 0 [<None>] Seq=1 Win=512 Len=80
```

```
▶ Frame 2: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
▶ Ethernet II, Src: HonHaiPr_0c:ac:47 (90:fb:a6:0c:ac:47), Dst: Cisco_cb:ea:c7 (1c:1d:86:cb:ea:c7)
▶ Internet Protocol Version 4, Src: 192.168.5.40, Dst: 216.58.199.142
▶ Transmission Control Protocol, Src Port: 59074, Dst Port: 443, Seq: 1, Ack: 1, Len: 46
▶ Secure Sockets Layer
```

```
0000  1c 1d 86 cb ea c7 90 fb  a6 0c ac 47 08 00 45 00   ········ ···G··E·
0010  00 56 53 39 40 00 40 06  81 cf c0 a8 05 28 d8 3a   ·VS9@·@· ·····(·:
0020  c7 8e e6 c2 01 bb 70 a1  82 9a ec 93 02 ad 50 18   ······p· ······P·
```

ens33: <live capture in progress>   Packets: 929 · Displayed: 462 (49.7%)   Profile: Default