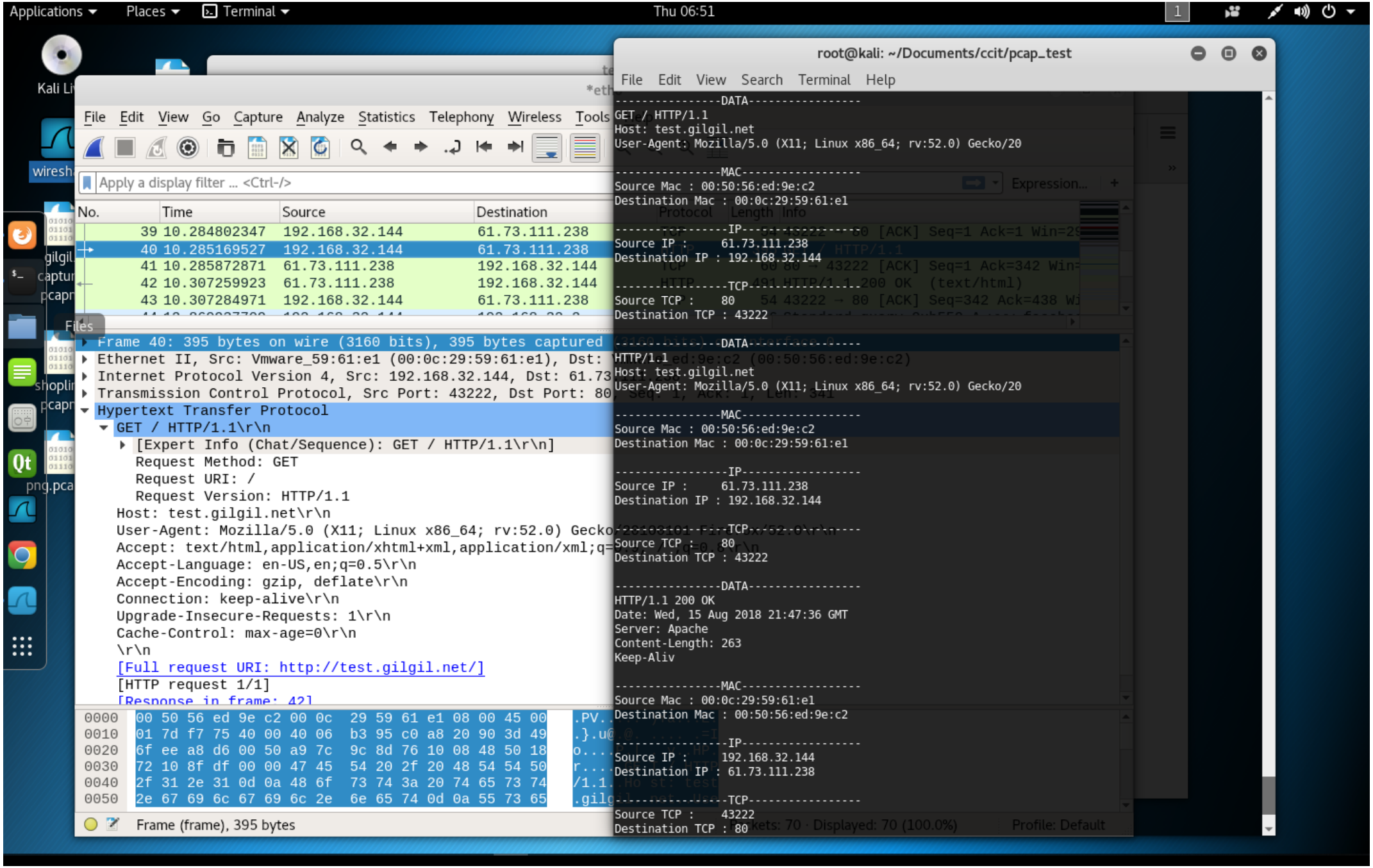
Dummy Interface

완벽한 디버깅을 원하신다면
더미 인터페이스를 이용하세요!

2018/08/16

정재훈
team S.C.P

- 와샵과 프로그래밍한 것과의 차이
- 덤프파일 Replay


Applications
Places
Terminal
Thu 06:51
root@kali: ~/Documents/ccit/pcap_test
File Edit View Search Terminal Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools
Apply a display filter ... <Ctrl-/>
No. Time Source Destination
39 10.284802347 192.168.32.144 61.73.111.238
40 10.285169527 192.168.32.144 61.73.111.238
41 10.285872871 61.73.111.238 192.168.32.144
42 10.307259923 61.73.111.238 192.168.32.144
43 10.307284971 192.168.32.144 61.73.111.238
Frame 40: 395 bytes on wire (3160 bits), 395 bytes captured
Ethernet II, Src: Vmware_59:61:e1 (00:0c:29:59:61:e1), Dst:
Internet Protocol Version 4, Src: 192.168.32.144, Dst: 61.73
Transmission Control Protocol, Src Port: 43222, Dst Port: 80
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
Request Method: GET
Request URI: /
Request Version: HTTP/1.1
Host: test.gilgil.net\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
Cache-Control: max-age=0\r\n
\r\n
[Full request URI: http://test.gilgil.net/]
[HTTP request 1/1]
0000 00 50 56 ed 9e c2 00 0c 29 59 61 e1 08 00 45 00
0010 01 7d f7 75 40 00 40 06 b3 95 c0 a8 20 90 3d 49
0020 6f ee a8 d6 00 50 a9 7c 9c 8d 76 10 08 48 50 18
0030 72 10 8f df 00 00 47 45 54 20 2f 20 48 54 54 50
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74
0050 2e 67 69 6c 67 69 6c 2e 6e 65 74 0d 0a 55 73 65
Frame (frame), 395 bytes
Packets: 70 · Displayed: 70 (100.0%)
Profile: Default
----------DATA----------
GET / HTTP/1.1
Host: test.gilgil.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20
----------MAC----------
Source Mac : 00:50:56:ed:9e:c2
Destination Mac : 00:0c:29:59:61:e1
----------IP----------
Source IP : 61.73.111.238
Destination IP : 192.168.32.144
----------TCP----------
Source TCP : 80
Destination TCP : 43222
----------DATA----------
HTTP/1.1
Host: test.gilgil.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20
----------MAC----------
Source Mac : 00:50:56:ed:9e:c2
Destination Mac : 00:0c:29:59:61:e1
----------IP----------
Source IP : 61.73.111.238
Destination IP : 192.168.32.144
----------TCP----------
Source TCP : 80
Destination TCP : 43222
----------DATA----------
HTTP/1.1 200 OK
Date: Wed, 15 Aug 2018 21:47:36 GMT
Server: Apache
Content-Length: 263
Keep-Aliv
----------MAC----------
Source Mac : 00:0c:29:59:61:e1
Destination Mac : 00:50:56:ed:9e:c2
----------IP----------
Source IP : 192.168.32.144
Destination IP : 61.73.111.238
----------TCP----------
Source TCP : 43222
Destination TCP : 80

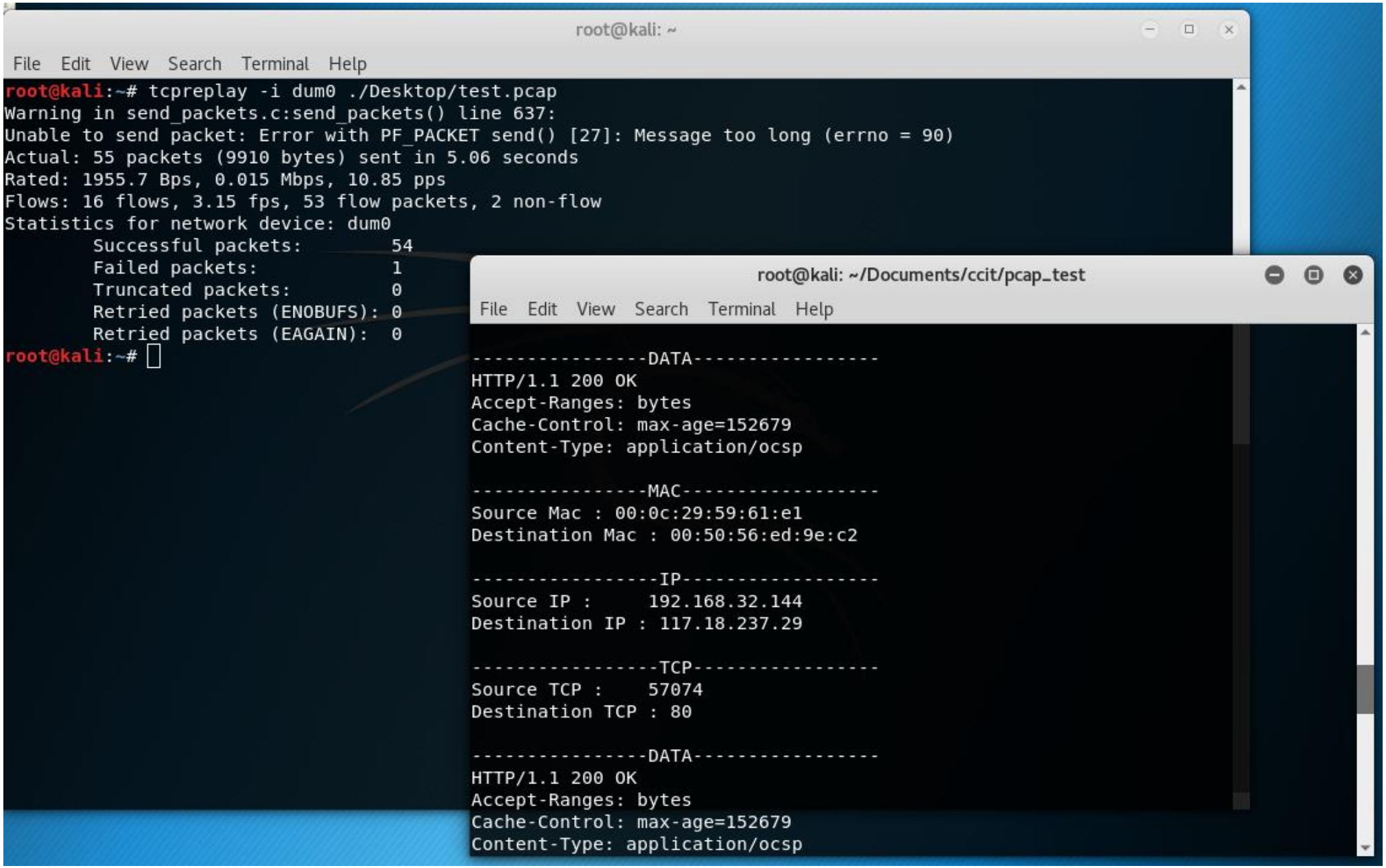
- modprobe dummy
- ip link add dum0 type dummy
- ifconfig dum0 up

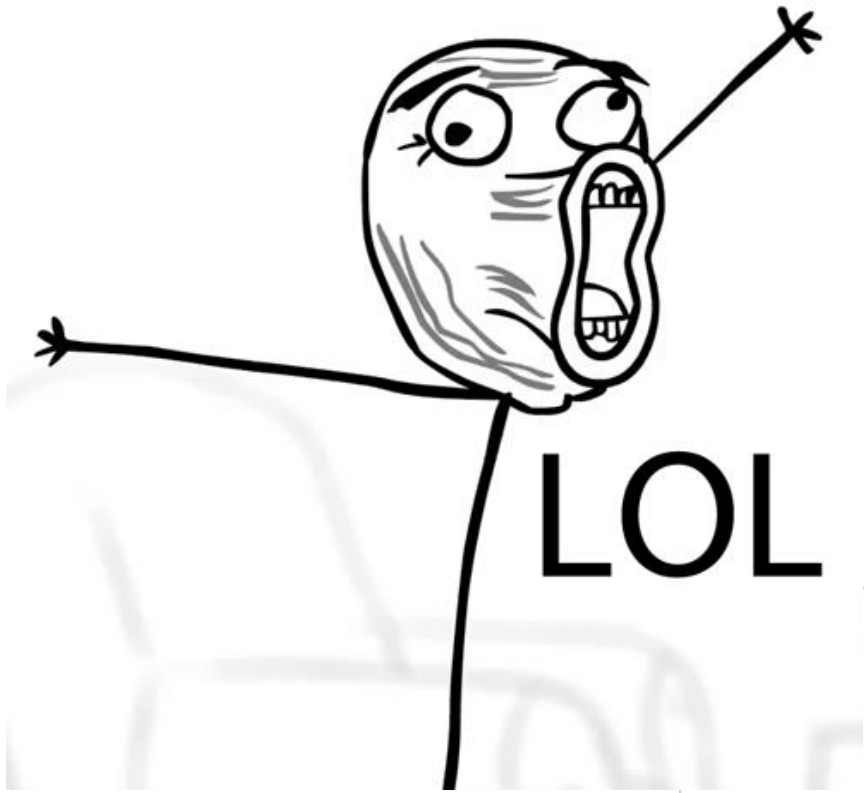
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.144  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::20c:29ff:fe59:61e1  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:59:61:e1  txqueuelen 1000  (Ethernet)
        RX packets 19  bytes 1576 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 1790 (1.7 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 18  bytes 1038 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1038 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
root@kali:~# modprobe dummy
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.144  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::20c:29ff:fe59:61e1  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:59:61:e1  txqueuelen 1000  (Ethernet)
        RX packets 11435  bytes 17143393 (16.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2777  bytes 168868 (164.9 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 18  bytes 1038 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1038 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
root@kali:~# ip link add dum0 type dummy
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.144  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::20c:29ff:fe59:61e1  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:59:61:e1  txqueuelen 1000  (Ethernet)
        RX packets 11435  bytes 17143393 (16.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2777  bytes 168868 (164.9 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 18  bytes 1038 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1038 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
root@kali:~# ifconfig dum0 up
root@kali:~# ifconfig
dum0: flags=195<UP,BROADCAST,RUNNING,NOARP>  mtu 1500
        inet6 fe80::6052:1aff:feed:249c  prefixlen 64  scopeid 0x20<link>
        ether 62:52:1a:ed:24:9c  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1  bytes 70 (70.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.144  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::20c:29ff:fe59:61e1  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:59:61:e1  txqueuelen 1000  (Ethernet)
        RX packets 11435  bytes 17143393 (16.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2777  bytes 168868 (164.9 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 18  bytes 1038 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1038 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# tcpreplay -i dum0 ./Desktop/test.pcap
Warning in send_packets.c:send_packets() line 637:
Unable to send packet: Error with PF_PACKET send() [27]: Message too long (errno = 90)
Actual: 55 packets (9910 bytes) sent in 5.06 seconds
Rated: 1955.7 Bps, 0.015 Mbps, 10.85 pps
Flows: 16 flows, 3.15 fps, 53 flow packets, 2 non-flow
Statistics for network device: dum0
Successful packets: 54
Failed packets: 1
Truncated packets: 0
Retried packets (ENOBUFS): 0
Retried packets (EAGAIN): 0
root@kali:~#
root@kali: ~/Documents/ccit/pcap_test
File Edit View Search Terminal Help
----------DATA----------
HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: max-age=152679
Content-Type: application/ocsp
----------MAC----------
Source Mac : 00:0c:29:59:61:e1
Destination Mac : 00:50:56:ed:9e:c2
----------IP----------
Source IP : 192.168.32.144
Destination IP : 117.18.237.29
----------TCP----------
Source TCP : 57074
Destination TCP : 80
----------DATA----------
HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: max-age=152679
Content-Type: application/ocsp


LOL