DALHOUSIE UNIVERSITY

Faculty of Computer Science

CSCI 6708 – Advanced Topics in Network Security

Name: Arka Ghosh
Banner ID: B00911033
Assignment: 02

Exercise 1

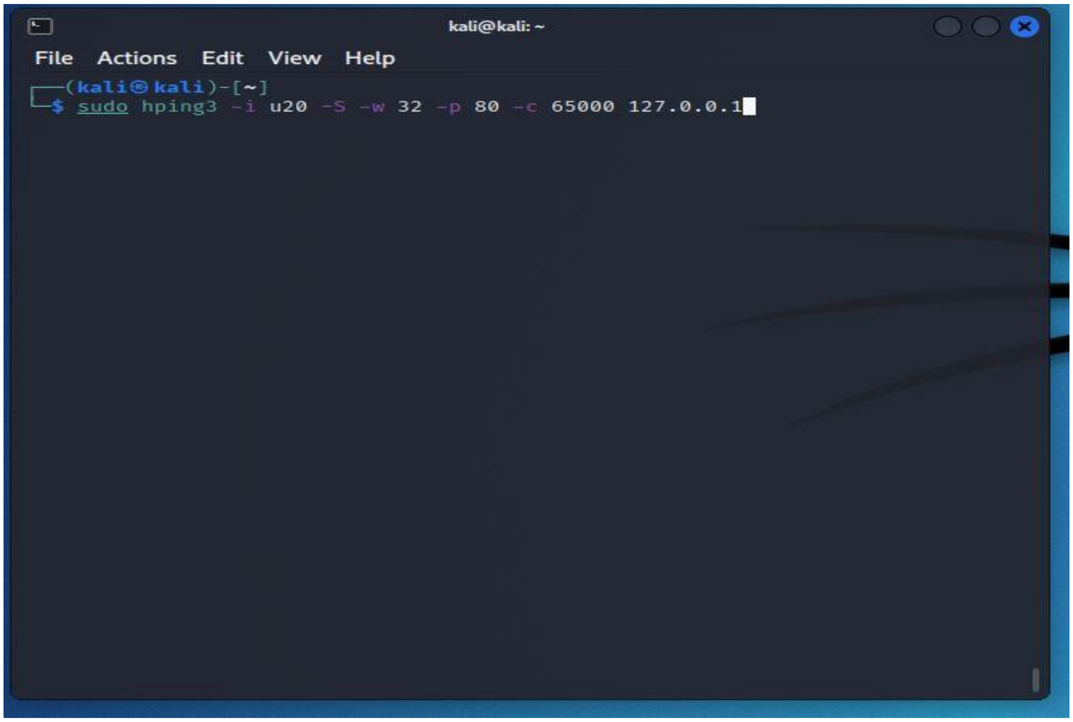
1) Ethical hackers must obtain comprehensive authorization and permission before executing any security evaluation on a system or network from the organization/owner that owns the system or network. In this regards, a written permission can be established stating the approval for the ethical hacker to perform an evaluation test [1].
2) Ethical hackers must define their scope of assessment before performing a hack. As soon as the target and goal is set, the ethical hacker should start acquiring as much information as possible about the system or network they intend to work on [2].
3) Full disclosure to the organization for whom the ethical hacker is working is considered as one of the most important principles of ethical hacking [3]. So, an ethical hacker must make every attempt possible to be as transparent as possible to the organization.
4) Organizations might impose boundaries or restriction on the activities of the ethical hackers due to the sensitivity of the information or data involved. Ethical hackers should never violate the limits and must stay within the boundaries set by the client organization while performing their tasks [4].
5) During the vulnerability assessment, it is so common for the ethical hackers to come across various confidential and sensitive information of the client organization. Ethical hackers must be very cautious about handling this information as well as are bound to maintain confidentiality of any acquired information and should not disclose any information to a third party [5].
6) Any high-risk vulnerabilities detected during testing should be reported as soon as possible by the ethical hackers. Reports are one way for a client company to assess the depth and completeness of an ethical hacker's work, as well as a mechanism for the company to improve their security through examining the data and findings. [6].
7) The ethical hackers must erase any evidence of the hack after evaluating the system for vulnerabilities [1]. This will prevent malicious attackers from exploiting the system or network through the previously identified loopholes.

Exercise 2

Experiment No. 1

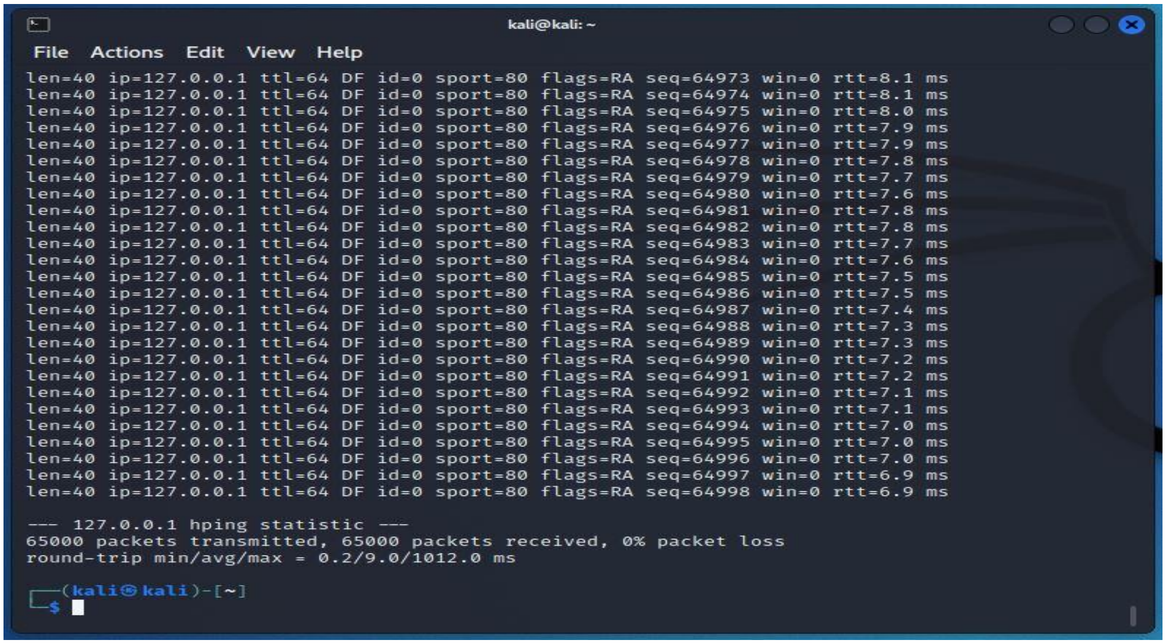
G.

Screenshot of the terminal window where the hping3 command is crafted is in the following:



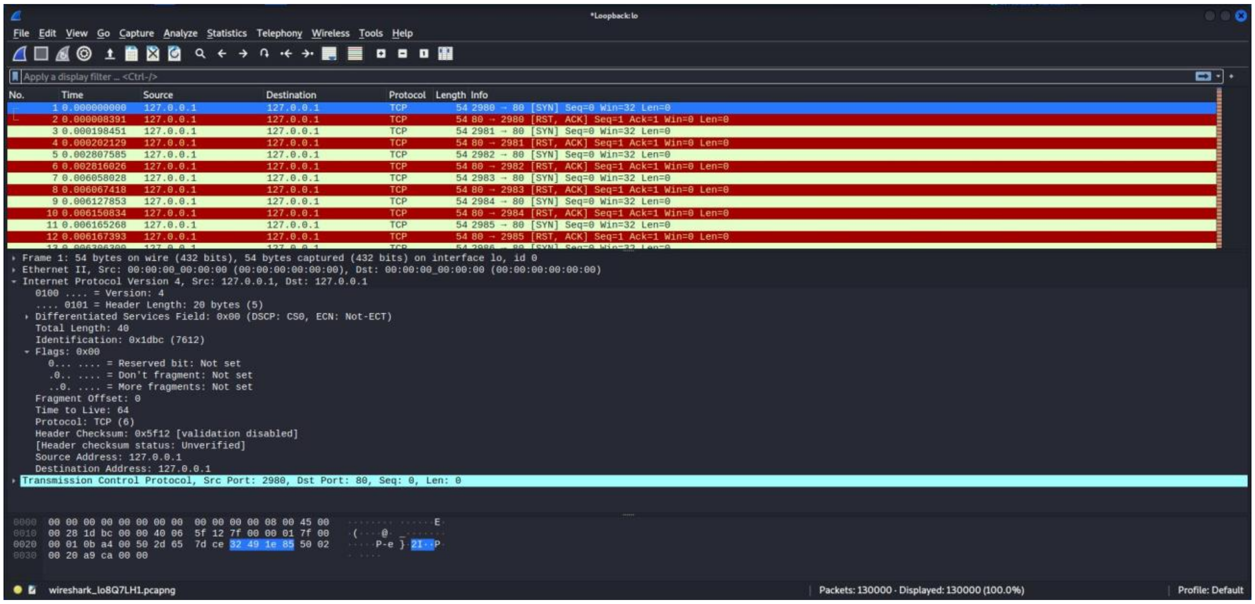
```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -i u20 -S -w 32 -p 80 -c 65000 127.0.0.1
```

Screenshot of the terminal window where the hping3 command is completed is in the following:



```
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64973 win=0 rtt=8.1 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64974 win=0 rtt=8.1 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64975 win=0 rtt=8.0 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64976 win=0 rtt=7.9 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64977 win=0 rtt=7.9 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64978 win=0 rtt=7.8 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64979 win=0 rtt=7.7 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64980 win=0 rtt=7.6 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64981 win=0 rtt=7.8 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64982 win=0 rtt=7.8 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64983 win=0 rtt=7.7 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64984 win=0 rtt=7.6 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64985 win=0 rtt=7.5 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64986 win=0 rtt=7.5 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64987 win=0 rtt=7.4 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64988 win=0 rtt=7.3 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64989 win=0 rtt=7.3 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64990 win=0 rtt=7.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64991 win=0 rtt=7.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64992 win=0 rtt=7.1 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64993 win=0 rtt=7.1 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64994 win=0 rtt=7.0 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64995 win=0 rtt=7.0 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64996 win=0 rtt=7.0 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64997 win=0 rtt=6.9 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=64998 win=0 rtt=6.9 ms

--- 127.0.0.1 hping statistic ---
65000 packets transmitted, 65000 packets received, 0% packet loss
round-trip min/avg/max = 0.2/9.0/1012.0 ms

┌──(kali㉿kali)-[~]
└─$
```

a) The Screenshot of the IP Part of the Wireshark Capture is in the following:


*Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time          Source       Destination   Protocol Length Info
    1 0.000000000   127.0.0.1    127.0.0.1     TCP      54 2980 → 80 [SYN] Seq=0 Win=32 Len=0
    2 0.000008391   127.0.0.1    127.0.0.1     TCP      54 80 → 2980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    3 0.000198451   127.0.0.1    127.0.0.1     TCP      54 2981 → 80 [SYN] Seq=0 Win=32 Len=0
    4 0.000202129   127.0.0.1    127.0.0.1     TCP      54 80 → 2981 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    5 0.002807585   127.0.0.1    127.0.0.1     TCP      54 2982 → 80 [SYN] Seq=0 Win=32 Len=0
    6 0.002816026   127.0.0.1    127.0.0.1     TCP      54 80 → 2982 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    7 0.006058028   127.0.0.1    127.0.0.1     TCP      54 2983 → 80 [SYN] Seq=0 Win=32 Len=0
    8 0.006067418   127.0.0.1    127.0.0.1     TCP      54 80 → 2983 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    9 0.006127853   127.0.0.1    127.0.0.1     TCP      54 2984 → 80 [SYN] Seq=0 Win=32 Len=0
   10 0.006150834   127.0.0.1    127.0.0.1     TCP      54 80 → 2984 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   11 0.006165268   127.0.0.1    127.0.0.1     TCP      54 2985 → 80 [SYN] Seq=0 Win=32 Len=0
   12 0.006167393   127.0.0.1    127.0.0.1     TCP      54 80 → 2985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
▸ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface lo, id 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▾ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x1dbc (7612)
  ▾ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x5f12 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 127.0.0.1
    Destination Address: 127.0.0.1
▸ Transmission Control Protocol, Src Port: 2980, Dst Port: 80, Seq: 0, Len: 0
```

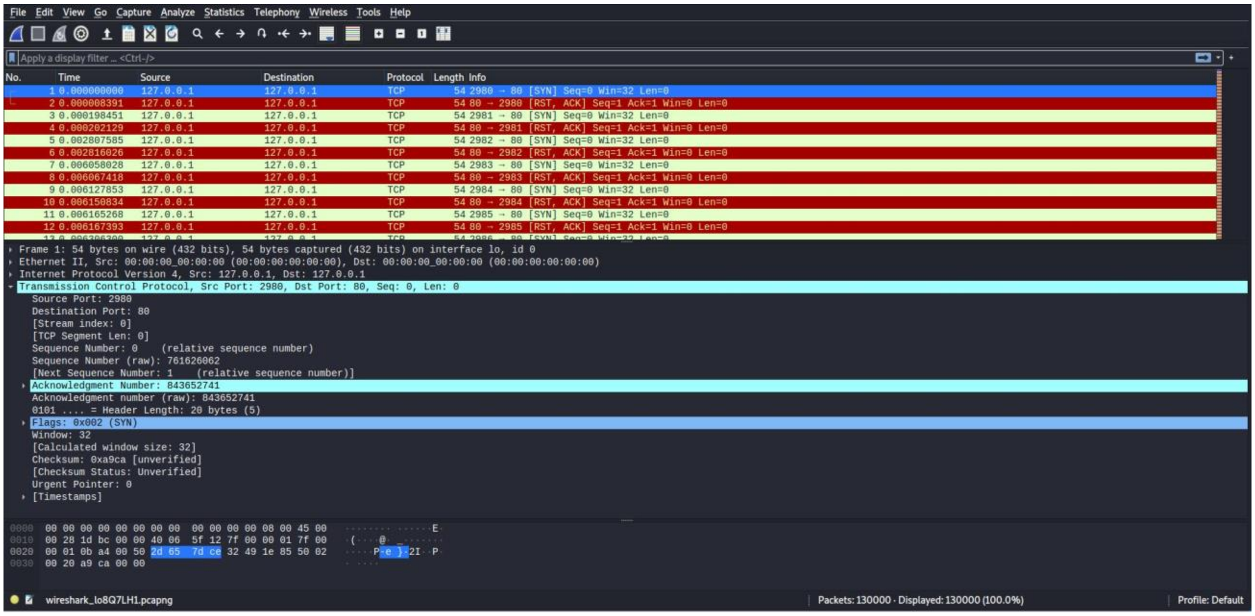
```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  00 28 1d bc 00 00 40 06  5f 12 7f 00 00 01 7f 00   ·(····@· _·······
0020  00 01 0b a4 00 50 2d 65  7d ce 32 49 1e 85 50 02   ·····P-e }·2I··P·
0030  00 20 a9 ca 00 00                                  · ····
```

wireshark_lo8Q7LH1.pcapng | Packets: 130000 · Displayed: 130000 (100.0%) | Profile: Default

The values of the source and destination IP address, protocol field, total length and header checksum in the IP part of the above mentioned wireshark capture are in the following:

- Source IP Address: 127.0.0.1
- Destination IP Address: 127.0.0.1
- Protocol Field: TCP (6)
- Total Length: 40
- Header Checksum: 0x5f12

b) The Screenshot of the TCP part of the Wireshark Capture is in the following:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time          Source       Destination   Protocol Length Info
    1 0.000000000   127.0.0.1    127.0.0.1     TCP      54 2980 → 80 [SYN] Seq=0 Win=32 Len=0
    2 0.000008391   127.0.0.1    127.0.0.1     TCP      54 80 → 2980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    3 0.000198451   127.0.0.1    127.0.0.1     TCP      54 2981 → 80 [SYN] Seq=0 Win=32 Len=0
    4 0.000202129   127.0.0.1    127.0.0.1     TCP      54 80 → 2981 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    5 0.002807585   127.0.0.1    127.0.0.1     TCP      54 2982 → 80 [SYN] Seq=0 Win=32 Len=0
    6 0.002816026   127.0.0.1    127.0.0.1     TCP      54 80 → 2982 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    7 0.006058028   127.0.0.1    127.0.0.1     TCP      54 2983 → 80 [SYN] Seq=0 Win=32 Len=0
    8 0.006067418   127.0.0.1    127.0.0.1     TCP      54 80 → 2983 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    9 0.006127853   127.0.0.1    127.0.0.1     TCP      54 2984 → 80 [SYN] Seq=0 Win=32 Len=0
   10 0.006150834   127.0.0.1    127.0.0.1     TCP      54 80 → 2984 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   11 0.006165268   127.0.0.1    127.0.0.1     TCP      54 2985 → 80 [SYN] Seq=0 Win=32 Len=0
   12 0.006167393   127.0.0.1    127.0.0.1     TCP      54 80 → 2985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
▸ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface lo, id 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▾ Transmission Control Protocol, Src Port: 2980, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 2980
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 761626062
    [Next Sequence Number: 1    (relative sequence number)]
  ▸ Acknowledgment Number: 843652741
    Acknowledgment number (raw): 843652741
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x002 (SYN)
    Window: 32
    [Calculated window size: 32]
    Checksum: 0xa9ca [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  00 28 1d bc 00 00 40 06  5f 12 7f 00 00 01 7f 00   ·(····@· _·······
0020  00 01 0b a4 00 50 2d 65  7d ce 32 49 1e 85 50 02   ·····P-e }·2I··P·
0030  00 20 a9 ca 00 00                                  · ····
```

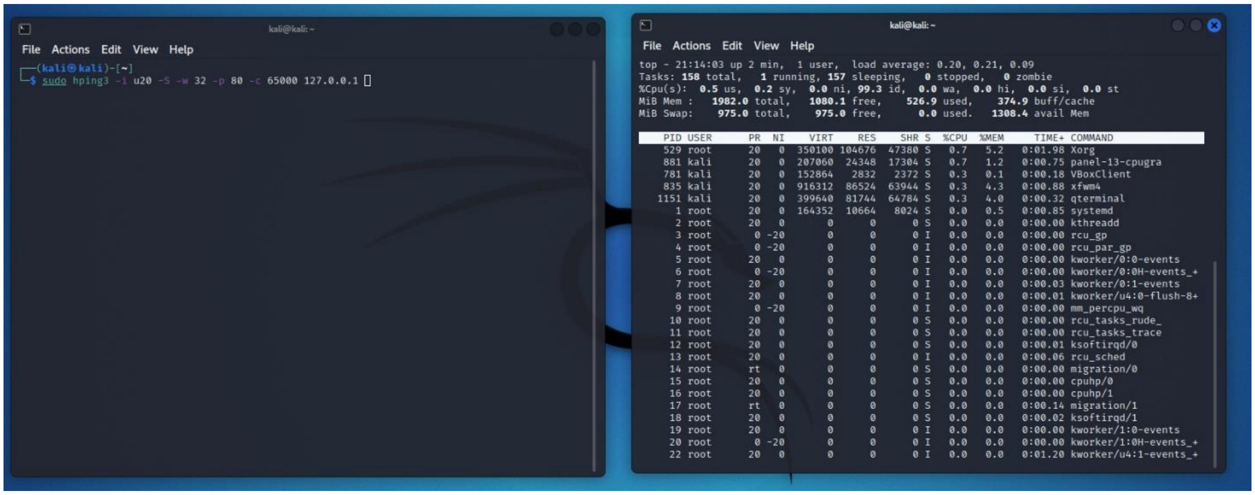
wireshark_lo8Q7LH1.pcapng | Packets: 130000 · Displayed: 130000 (100.0%) | Profile: Default

The values of the source and destination port numbers, flags that are set and window size in the TCP part of the Wireshark Capture are in the following:

- Source Port Number: 2980
- Destination Port Number: 80
- Flag: 0x002 (SYN) [Synchronisation Flag is set]
- Window Size: 32

c) The screenshot of the terminal window from the top command capture before and during the attack are provided in the following:

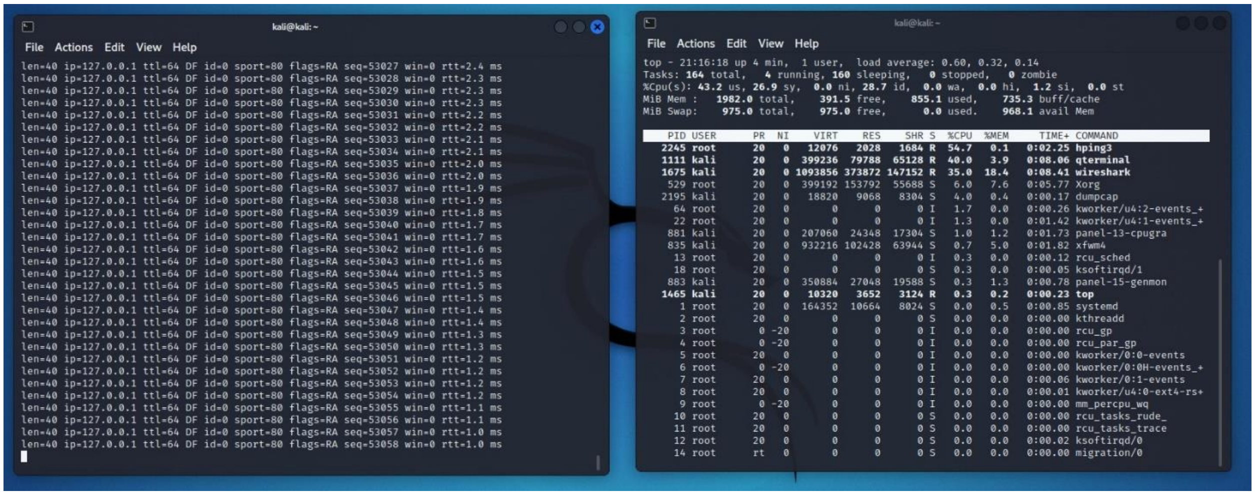
Before the Attack



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -i u20 -S -w 32 -p 80 -c 65000 127.0.0.1 
```

```
top - 21:14:03 up 2 min,  1 user,  load average: 0.20, 0.21, 0.09
Tasks: 158 total,   1 running, 157 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.5 us,  0.2 sy,  0.0 ni, 99.3 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   1982.0 total,   1080.1 free,    526.9 used,    374.9 buff/cache
MiB Swap:    975.0 total,    975.0 free,      0.0 used.   1308.4 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    529 root      20   0  350100 104676  47380 S   0.7   5.2   0:01.98 Xorg
    881 kali      20   0  207060  24348  17304 S   0.7   1.2   0:00.75 panel-13-cpugra
    781 kali      20   0  152864   2832   2372 S   0.3   0.1   0:00.18 VBoxClient
    835 kali      20   0  916312  86524  63944 S   0.3   4.3   0:00.88 xfwm4
   1151 kali      20   0  399640  81744  64784 S   0.3   4.0   0:00.32 qterminal
      1 root      20   0  164352  10664   8024 S   0.0   0.5   0:00.85 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root      20   0       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0-events
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_+
      7 root      20   0       0      0      0 I   0.0   0.0   0:00.03 kworker/0:1-events
      8 root      20   0       0      0      0 I   0.0   0.0   0:00.01 kworker/u4:0-flush-8+
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     10 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_rude_
     11 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_trace
     12 root      20   0       0      0      0 S   0.0   0.0   0:00.01 ksoftirqd/0
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.06 rcu_sched
     14 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
     15 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     16 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
     17 root      rt   0       0      0      0 S   0.0   0.0   0:00.14 migration/1
     18 root      20   0       0      0      0 S   0.0   0.0   0:00.02 ksoftirqd/1
     19 root      20   0       0      0      0 I   0.0   0.0   0:00.00 kworker/1:0-events
     20 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/1:0H-events_+
     22 root      20   0       0      0      0 I   0.0   0.0   0:01.20 kworker/u4:1-events_+
```

DuringThe Attack



```
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53027 win=0 rtt=2.4 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53028 win=0 rtt=2.3 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53029 win=0 rtt=2.3 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53030 win=0 rtt=2.3 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53031 win=0 rtt=2.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53032 win=0 rtt=2.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53033 win=0 rtt=2.1 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53034 win=0 rtt=2.1 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53035 win=0 rtt=2.0 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53036 win=0 rtt=2.0 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53037 win=0 rtt=1.9 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53038 win=0 rtt=1.9 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53039 win=0 rtt=1.8 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53040 win=0 rtt=1.7 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53041 win=0 rtt=1.7 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53042 win=0 rtt=1.6 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53043 win=0 rtt=1.6 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53044 win=0 rtt=1.5 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53045 win=0 rtt=1.5 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53046 win=0 rtt=1.5 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53047 win=0 rtt=1.4 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53048 win=0 rtt=1.4 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53049 win=0 rtt=1.3 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53050 win=0 rtt=1.3 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53051 win=0 rtt=1.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53052 win=0 rtt=1.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53053 win=0 rtt=1.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53054 win=0 rtt=1.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53055 win=0 rtt=1.1 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53056 win=0 rtt=1.1 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53057 win=0 rtt=1.0 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=53058 win=0 rtt=1.0 ms
```

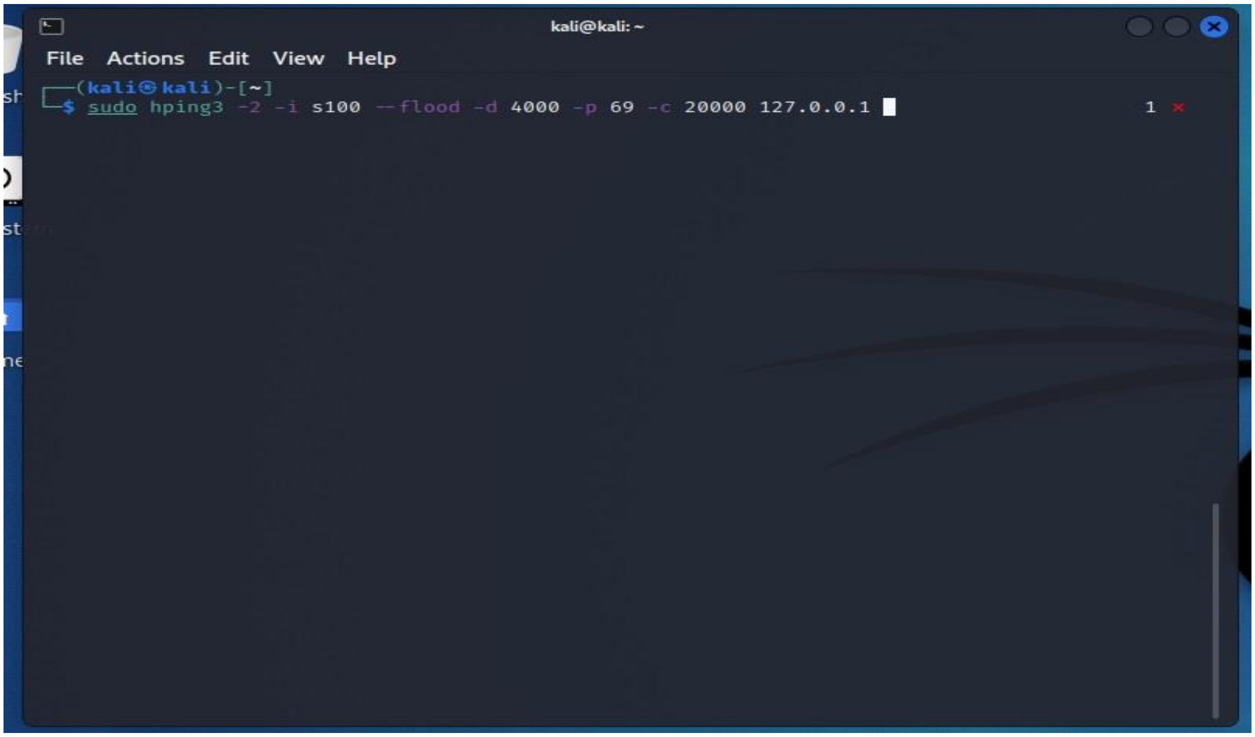
```
top - 21:16:18 up 4 min,  1 user,  load average: 0.60, 0.32, 0.14
Tasks: 164 total,   4 running, 160 sleeping,   0 stopped,   0 zombie
%Cpu(s): 43.2 us, 26.9 sy,  0.0 ni, 28.7 id,  0.0 wa,  0.0 hi,  1.2 si,  0.0 st
MiB Mem :   1982.0 total,    391.5 free,    855.1 used,    735.3 buff/cache
MiB Swap:    975.0 total,    975.0 free,      0.0 used.    968.1 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   2245 root      20   0   12076   2028   1684 R  54.7   0.1   0:02.25 hping3
   1111 kali      20   0  399236  79788  65128 R  40.0   3.9   0:08.06 qterminal
   1675 kali      20   0 1093856 373872 147152 R  35.0  18.4   0:08.41 wireshark
    529 root      20   0  399192 153792  55688 S   6.0   7.6   0:05.77 Xorg
   2195 kali      20   0   18820   9068   8304 S   4.0   0.4   0:00.17 dumpcap
     64 root      20   0       0      0      0 I   1.7   0.0   0:00.26 kworker/u4:2-events_+
     22 root      20   0       0      0      0 I   1.3   0.0   0:01.42 kworker/u4:1-events_+
    881 kali      20   0  207060  24348  17304 S   1.0   1.2   0:01.73 panel-13-cpugra
    835 kali      20   0  932216 102428  63944 S   0.7   5.0   0:01.82 xfwm4
     13 root      20   0       0      0      0 I   0.3   0.0   0:00.12 rcu_sched
     18 root      20   0       0      0      0 S   0.3   0.0   0:00.05 ksoftirqd/1
    883 kali      20   0  350884  27048  19588 S   0.3   1.3   0:00.78 panel-15-genmon
   1465 kali      20   0   10320   3652   3124 R   0.3   0.2   0:00.23 top
      1 root      20   0  164352  10664   8024 S   0.0   0.5   0:00.85 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root      20   0       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0-events
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_+
      7 root      20   0       0      0      0 I   0.0   0.0   0:00.06 kworker/0:1-events
      8 root      20   0       0      0      0 I   0.0   0.0   0:00.01 kworker/u4:0-ext4-rs+
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     10 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_rude_
     11 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_trace
     12 root      20   0       0      0      0 S   0.0   0.0   0:00.02 ksoftirqd/0
     14 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
```

Before the DoS attack, the CPU and memory utilization were lower. On the other hand, during the DoS attack, the CPU utilization increased but the memory utilization remained lower as before. As seen from the above screenshots, during the DoS attack, the CPU usage increased to 54.7% for running the DoS attack but Memory utilization remained lower as 0.1%. This means the CPU is being used more (54.7% busy) during the DoS attack.

Experiment 2

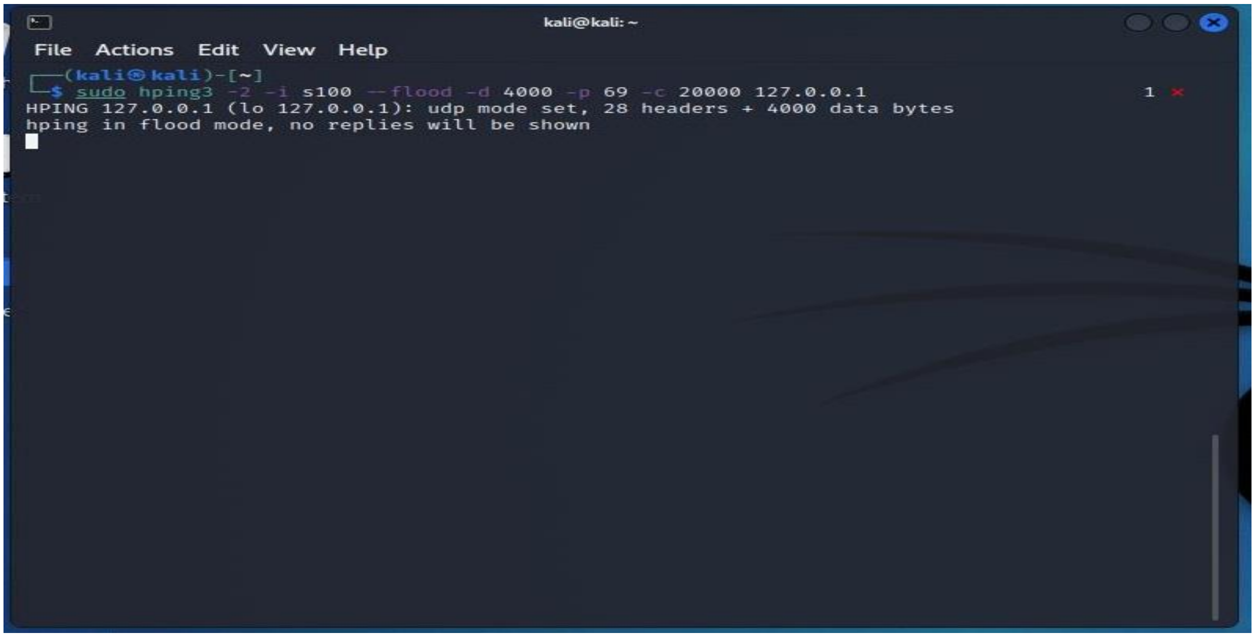
G.

Screenshot of the terminal window where the hping3 command is crafted is in the following:



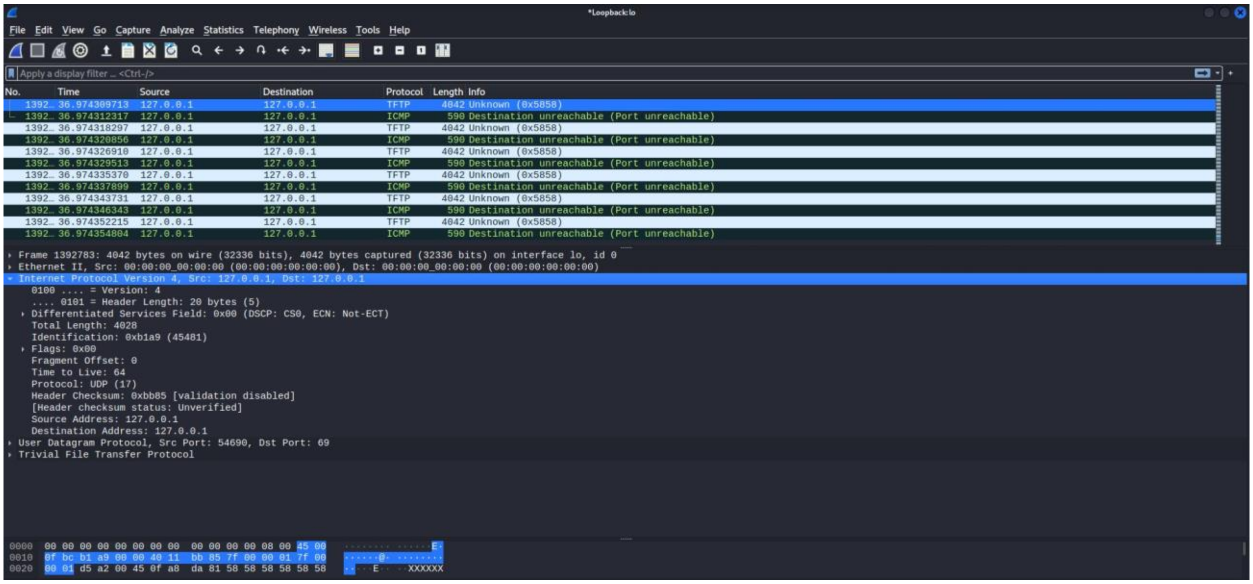
```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -2 -i s100 --flood -d 4000 -p 69 -c 20000 127.0.0.1                1 ✗
```

Screenshot of the terminal window while running the hping3 command is in the following:



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -2 -i s100 --flood -d 4000 -p 69 -c 20000 127.0.0.1                1 ✗
HPING 127.0.0.1 (lo 127.0.0.1): udp mode set, 28 headers + 4000 data bytes
hping in flood mode, no replies will be shown
```

a) The Screenshot of the IP Part of the Wireshark Capture is in the following:

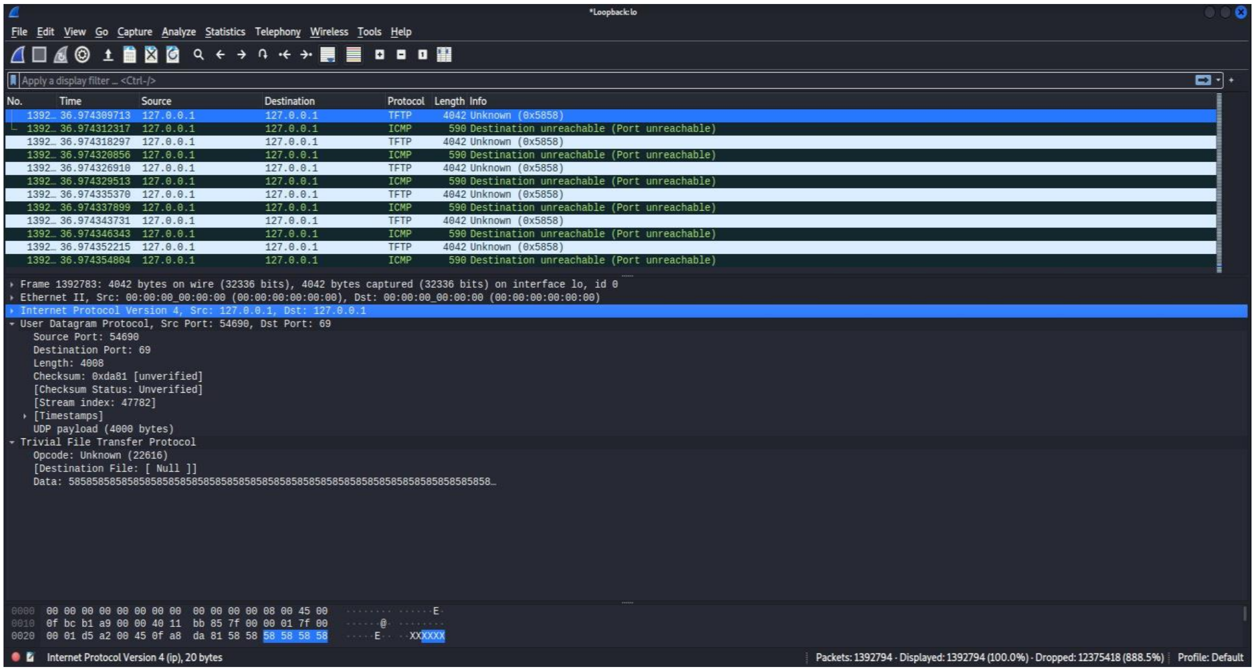

*Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time          Source      Destination  Protocol Length Info
 1392… 36.974309713  127.0.0.1   127.0.0.1    TFTP      4042 Unknown (0x5858)
 1392… 36.974312317  127.0.0.1   127.0.0.1    ICMP       590 Destination unreachable (Port unreachable)
 1392… 36.974318297  127.0.0.1   127.0.0.1    TFTP      4042 Unknown (0x5858)
 1392… 36.974320856  127.0.0.1   127.0.0.1    ICMP       590 Destination unreachable (Port unreachable)
 1392… 36.974326910  127.0.0.1   127.0.0.1    TFTP      4042 Unknown (0x5858)
 1392… 36.974329513  127.0.0.1   127.0.0.1    ICMP       590 Destination unreachable (Port unreachable)
 1392… 36.974335370  127.0.0.1   127.0.0.1    TFTP      4042 Unknown (0x5858)
 1392… 36.974337899  127.0.0.1   127.0.0.1    ICMP       590 Destination unreachable (Port unreachable)
 1392… 36.974343731  127.0.0.1   127.0.0.1    TFTP      4042 Unknown (0x5858)
 1392… 36.974346343  127.0.0.1   127.0.0.1    ICMP       590 Destination unreachable (Port unreachable)
 1392… 36.974352215  127.0.0.1   127.0.0.1    TFTP      4042 Unknown (0x5858)
 1392… 36.974354804  127.0.0.1   127.0.0.1    ICMP       590 Destination unreachable (Port unreachable)

› Frame 1392783: 4042 bytes on wire (32336 bits), 4042 bytes captured (32336 bits) on interface lo, id 0
› Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
˅ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 4028
    Identification: 0xb1a9 (45481)
  › Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xbb85 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 127.0.0.1
    Destination Address: 127.0.0.1
› User Datagram Protocol, Src Port: 54690, Dst Port: 69
› Trivial File Transfer Protocol

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  0f bc b1 a9 00 00 40 11  bb 85 7f 00 00 01 7f 00   ······@· ········
0020  00 01 d5 a2 00 45 0f a8  da 81 58 58 58 58 58 58   ·····E·· ··XXXXXX
```

The values of the source and destination IP address, protocol field, total length and header checksum in the IP part of the above mentioned wireshark capture are in the following:

- Source IP Address: 127.0.0.1
- Destination IP Address: 127.0.0.1
- Protocol Field: UDP (17)
- Total Length: 4028
- Header Checksum: 0xbb85

b) The Screenshot of the UDP part of the Wireshark Capture is in the following:


*Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

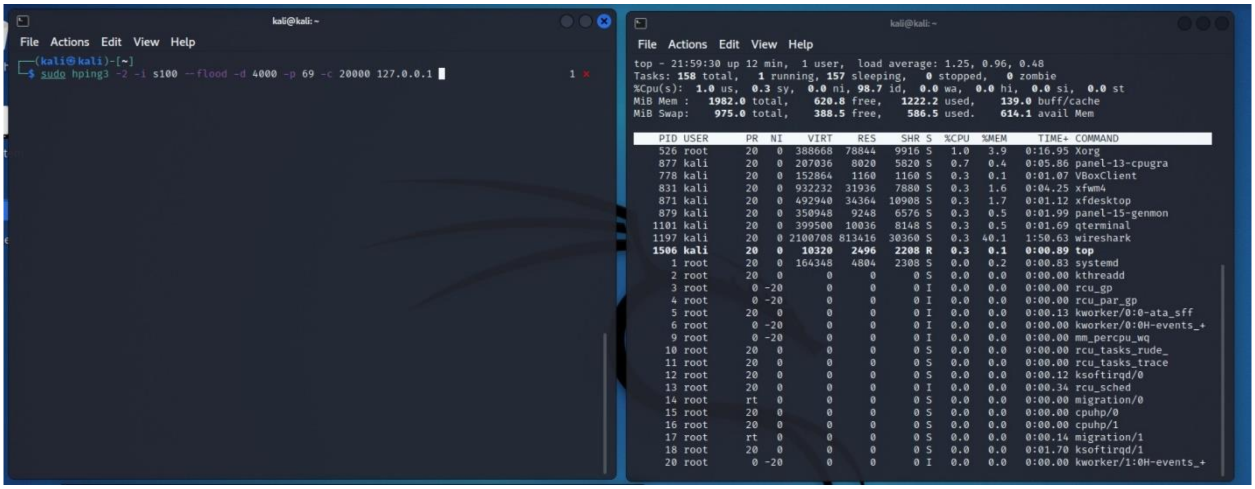
```
No.     Time          Source      Destination  Protocol Length Info
 1392… 36.974309713  127.0.0.1   127.0.0.1    TFTP      4042 Unknown (0x5858)
 1392… 36.974312317  127.0.0.1   127.0.0.1    ICMP       590 Destination unreachable (Port unreachable)
 1392… 36.974318297  127.0.0.1   127.0.0.1    TFTP      4042 Unknown (0x5858)
 1392… 36.974320856  127.0.0.1   127.0.0.1    ICMP       590 Destination unreachable (Port unreachable)
 1392… 36.974326910  127.0.0.1   127.0.0.1    TFTP      4042 Unknown (0x5858)
 1392… 36.974329513  127.0.0.1   127.0.0.1    ICMP       590 Destination unreachable (Port unreachable)
 1392… 36.974335370  127.0.0.1   127.0.0.1    TFTP      4042 Unknown (0x5858)
 1392… 36.974337899  127.0.0.1   127.0.0.1    ICMP       590 Destination unreachable (Port unreachable)
 1392… 36.974343731  127.0.0.1   127.0.0.1    TFTP      4042 Unknown (0x5858)
 1392… 36.974346343  127.0.0.1   127.0.0.1    ICMP       590 Destination unreachable (Port unreachable)
 1392… 36.974352215  127.0.0.1   127.0.0.1    TFTP      4042 Unknown (0x5858)
 1392… 36.974354804  127.0.0.1   127.0.0.1    ICMP       590 Destination unreachable (Port unreachable)

› Frame 1392783: 4042 bytes on wire (32336 bits), 4042 bytes captured (32336 bits) on interface lo, id 0
› Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
˅ User Datagram Protocol, Src Port: 54690, Dst Port: 69
    Source Port: 54690
    Destination Port: 69
    Length: 4008
    Checksum: 0xda81 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 47782]
  › [Timestamps]
    UDP payload (4000 bytes)
˅ Trivial File Transfer Protocol
    Opcode: Unknown (22616)
    [Destination File: [ Null ]]
    Data: 5858585858585858585858585858585858585858585858585858585858585858585858…

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  0f bc b1 a9 00 00 40 11  bb 85 7f 00 00 01 7f 00   ······@· ········
0020  00 01 d5 a2 00 45 0f a8  da 81 58 58 58 58 58 58   ·····E·· ··XXXXXX

Internet Protocol Version 4 (ip), 20 bytes      Packets: 1392794 · Displayed: 1392794 (100.0%) · Dropped: 12375418 (888.5%)   Profile: Default
```

The values of the source and destination port numbers, and header checksum in the UDP part of the Wireshark Capture are in the following:

- Source Port Number: 54690
- Destination Port Number: 69
- Checksum: 0xda81

c) The screenshot of the terminal window from the top command capture before and during the attack are provided in the following:

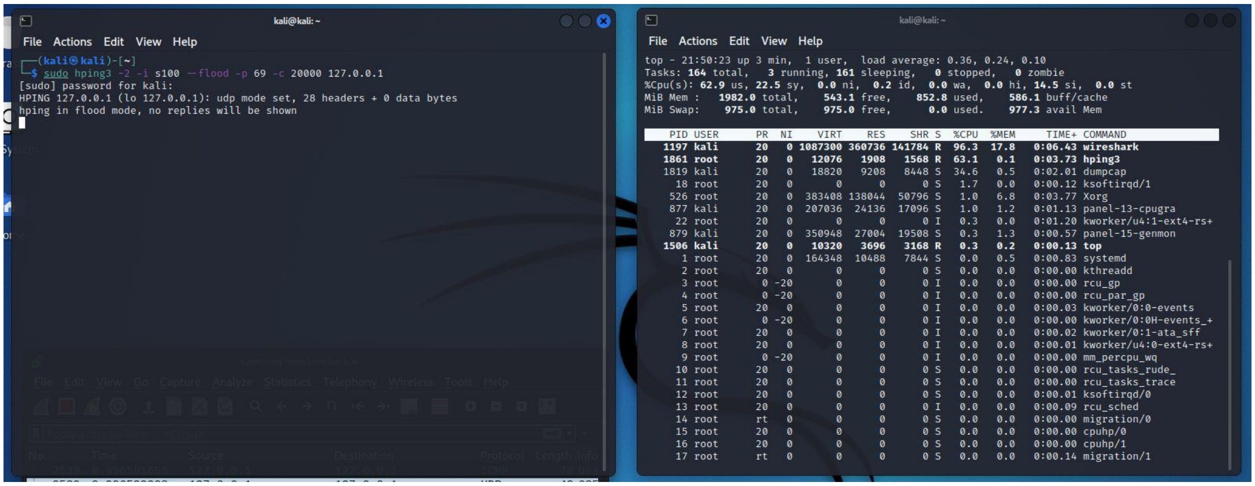
Before the Attack



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -2 -i s100 --flood -d 4000 -p 69 -c 20000 127.0.0.1          1 ✗
```

```
top - 21:59:30 up 12 min,  1 user,  load average: 1.25, 0.96, 0.48
Tasks: 158 total,   1 running, 157 sleeping,   0 stopped,   0 zombie
%Cpu(s):  1.0 us,  0.3 sy,  0.0 ni, 98.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   1982.0 total,    620.8 free,   1222.2 used,    139.0 buff/cache
MiB Swap:    975.0 total,    388.5 free,    586.5 used.    614.1 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    526 root      20   0  388668  78844   9916 S   1.0   3.9   0:16.95 Xorg
    877 kali      20   0  207036   8020   5820 S   0.7   0.4   0:05.86 panel-13-cpugra
    778 kali      20   0  152864   1160   1160 S   0.3   0.1   0:01.07 VBoxClient
    831 kali      20   0  932232  31936   7880 S   0.3   1.6   0:04.25 xfwm4
    871 kali      20   0  492940  34364  10908 S   0.3   1.7   0:01.12 xfdesktop
    879 kali      20   0  350948   9248   6576 S   0.3   0.5   0:01.99 panel-15-genmon
   1101 kali      20   0  399500  10036   8148 S   0.3   0.5   0:01.69 qterminal
   1197 kali      20   0 2100708 813416  30360 S   0.3  40.1   1:50.63 wireshark
   1506 kali      20   0   10320   2496   2208 R   0.3   0.1   0:00.89 top
      1 root      20   0  164348   4804   2308 S   0.0   0.2   0:00.83 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root      20   0       0      0      0 I   0.0   0.0   0:00.13 kworker/0:0-ata_sff
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_+
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     10 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_rude_
     11 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_trace
     12 root      20   0       0      0      0 S   0.0   0.0   0:00.12 ksoftirqd/0
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.34 rcu_sched
     14 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
     15 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     16 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
     17 root      rt   0       0      0      0 S   0.0   0.0   0:00.14 migration/1
     18 root      20   0       0      0      0 S   0.0   0.0   0:01.70 ksoftirqd/1
     20 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/1:0H-events_+
```

During the Attack



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -2 -i s100 --flood -p 69 -c 20000 127.0.0.1
[sudo] password for kali:
HPING 127.0.0.1 (lo 127.0.0.1): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

```
top - 21:50:23 up 3 min,  1 user,  load average: 0.36, 0.24, 0.10
Tasks: 164 total,   3 running, 161 sleeping,   0 stopped,   0 zombie
%Cpu(s): 62.9 us, 22.5 sy,  0.0 ni,  0.2 id,  0.0 wa,  0.0 hi, 14.5 si,  0.0 st
MiB Mem :   1982.0 total,    543.1 free,    852.8 used,    586.1 buff/cache
MiB Swap:    975.0 total,    975.0 free,      0.0 used.    977.3 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   1197 kali      20   0 1087300 360736 141784 R  96.3  17.8   0:06.43 wireshark
   1861 root      20   0   12076   1908   1568 R  63.1   0.1   0:03.73 hping3
   1819 kali      20   0   18820   9208   8448 S  34.6   0.5   0:02.01 dumpcap
     18 root      20   0       0      0      0 S   1.7   0.0   0:00.12 ksoftirqd/1
    526 root      20   0  383408 138044  50796 S   1.0   6.8   0:03.77 Xorg
    877 kali      20   0  207036  24136  17096 S   1.0   1.2   0:01.13 panel-13-cpugra
     22 root      20   0       0      0      0 I   0.3   0.0   0:01.20 kworker/u4:1-ext4-rs+
    879 kali      20   0  350948  27004  19508 S   0.3   1.3   0:00.57 panel-15-genmon
   1506 kali      20   0   10320   3696   3168 R   0.3   0.2   0:00.13 top
      1 root      20   0  164348  10488   7844 S   0.0   0.5   0:00.83 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root      20   0       0      0      0 I   0.0   0.0   0:00.03 kworker/0:0-events
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_+
      7 root      20   0       0      0      0 I   0.0   0.0   0:00.02 kworker/0:1-ata_sff
      8 root      20   0       0      0      0 I   0.0   0.0   0:00.01 kworker/u4:0-ext4-rs+
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     10 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_rude_
     11 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_trace
     12 root      20   0       0      0      0 S   0.0   0.0   0:00.01 ksoftirqd/0
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.09 rcu_sched
     14 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
     15 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     16 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
     17 root      rt   0       0      0      0 S   0.0   0.0   0:00.14 migration/1
```

The CPU utilization increased a lot during the attack for the hping command. As seen from the above screenshots, the CPU and memory utilization was lower before the UDP flood DoS attack. But during the attack, the CPU utilization increased to 63.1% which made the system freeze for a few seconds but the memory utilization remained low as before.

References

[1] "What is Ethical Hacking and Type of Ethical Hackers", 2022. [Online]. Available: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-ethical-hacking. [Accessed: 05- Feb- 2022].

[2] "A Definitive Guide to Ethical Hacking", *Indeed Career Guide*, 2021. [Online]. Available: https://www.indeed.com/career-advice/career-development/ethical-hacking. [Accessed: 09- Feb- 2022].

[3] M. Huneidy, "The Ultimate Guide to Ethical Hacking", 2022. [Online]. Available: https://0x1.gitlab.io/security/The-Ultimate-Guide-to-Ethical-Hacking/. [Accessed: 05- Feb- 2022].

[4] "What Is Ethical Hacking?", *Codecademy News*, 2022. [Online]. Available: https://www.codecademy.com/resources/blog/what-is-ethical-hacking/. [Accessed: 05- Feb- 2022].

[5] "Ethical Hacking Code of Ethics: Security, Risk & Issues - Panmore Institute", *Panmore Institute*, 2022. [Online]. Available: http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues. [Accessed: 05- Feb- 2022].

[6] "Ethical Hacking - Computing and Software Wiki", *Wiki.cas.mcmaster.ca*, 2022. [Online]. Available: http://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking#10_Commandments_of_Ethical_Hacking. [Accessed: 05- Feb- 2022].