After executing the command "tcpflow -r intrusion.pcap", different results occur depending on whether TCPFlow 1.5.1 or 1.6.1 is used.

Running tcpflow on intrusion.pcap throws violations with V1.6.1 but not with V1.5.1:

TCPFlow 1.5.1: No violations

```
⊞
                                        root@kali: ~/data/NTA/tcpflow_1
       Li:~# cd /root/data/NTA
     cali:~/data/NTA# mkdir tcpflow_1
    gkali:~/data/NTA# cd tcpflow_1
    kali:~/data/NTA/tcpflow_1# tcpflow -r ../intrusion.pcap
reportfilename: ./report.xml
         :~/data/NTA/tcpflow_1# ls -l
total 15468
rw-r--r-- 1 root root
                          1106 Mar 30
                                        2007 061.172.250.048.01246-192.168.003.101.0
                                        2007 061.172.250.048.01248-192.168.003.101.0
 rw-r--r-- 1 root root
                           469 Mar 30
                                        2007 061.172.250.048.01250-192.168.003.101.0
 rw-r--r-- 1 root root
                            89 Mar 30
 rw-r--r-- 1 root root
                         14854 Mar 30
                                        2007 061.172.250.048.02005-192.168.003.100.0
```

## TCPFlow 1.6.1: TCP PROTOCOL VIOLATION

```
[~/data/NTA/tcpflow_1]
    tcpflow -r ../intrusion.pcap
reportfilename: ./report.xml
tcpflow: TCP PROTOCOL VIOLATION: SYN with data! (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data! (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data!
tcpflow: TCP PROTOCOL VIOLATION: SYN with data!
                                                 (length=2)
tcpflow: TCP PROTOCOL VIOLATION:
                                 SYN with data!
                                                 (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data!
                                                 (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data!
                                                 (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data!
                                                 (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data!
                                                 (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data!
                                                 (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data!
                                                 (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data!
                                                (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data! (length=2)
tcpflow: TCP PROTOCOL VIOLATION: SYN with data! (length=2)
```

The number of flows generated via V1.6.1 is different from V1.5.1

## TCPFlow 1.5.1: 1220 flows

```
-rw-r--r-- 1 root root 9648 Mar 30 2007 216.239.037.104.00080-192.168.003.100.01140
root@kali:-/data/NTA/tcpflow_1# ls -1 | wc -l
1220
root@kali:-/data/NTA/tcpflow_1#
```

## TCPFlow 1.6.1: 3201 flows

```
-[~/data/NTA/tcpflow_1]
   rm report.xml
                  )-[~/data/NTA/tcpflow_1]
                   -[~/data/NTA/tcpflow_1]
   ls *06667* -l
-rw-r--r-- 1 root root 31955 Mar 30 2007 066.225.225.225.06667-192.168.003.101.38922
-rw-r--r-- 1 root root
                           6 Mar 30 2007 192.168.003.001.06667-192.168.003.100.02347
                           6 Mar 30 2007 192.168.003.005.06667-192.168.003.100.02348
-rw-r--r-- 1 root root
                           6 Mar 30 2007 192.168.003.005.06667-192.168.003.100.02348c1
-rw-r--r--
            root root
                           6 Mar 30
                                      2007 192.168.003.005.06667-192.168.003.100.02348c2
-rw-r--r--
            root root
                           6 Mar 30 2007 192.168.003.050.06667-192.168.003.100.02349
-rw-r--r-- 1
            root root
                           6 Mar 30
                                      2007 192.168.003.076.06667-192.168.003.100.02350
-rw-r--r-- 1 root root
                           6 Mar 30 2007 192.168.003.088.06667-192.168.003.100.02351
-rw-r--r-- 1 root root
                        9166 Mar 30 2007 192.168.003.101.38922-066.225.225.225.06667
-rw-r--r-- 1 root root
                           6 Mar 30 2007 192.168.003.200.06667-192.168.003.100.02354
   (root@kali2023)-[~/data/NTA/tcpflow_1]
cat 192.168.003.001.06667-192.168.003.100.02347
```