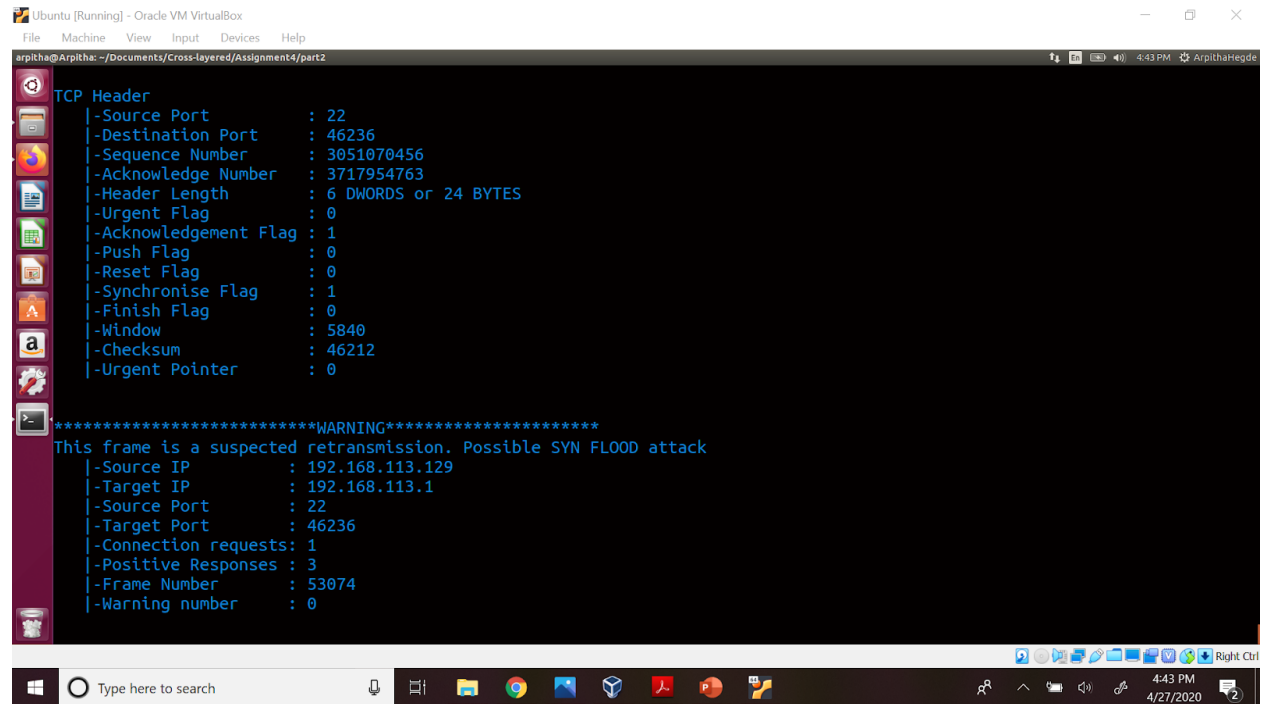


Link to the YouTube video:

<https://www.youtube.com/watch?v=VEVaH4aj5-8>

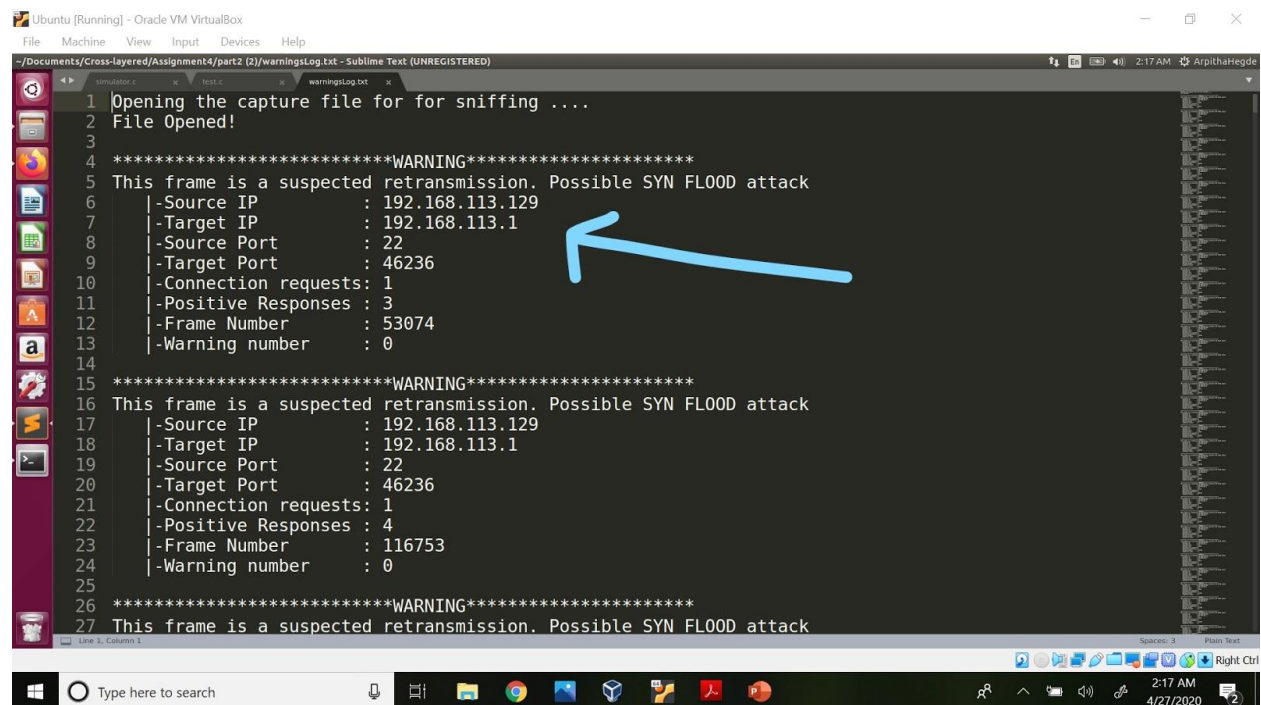
The output of the packet sniffer program has been written to warningsLog.txt (also present in the folder) which has been used to cross verify with the Wireshark logs as shown below:



The screenshot shows a terminal window titled "Ubuntu [Running] - Oracle VM VirtualBox". The user is at the prompt "arpitha@Arpitha: ~/Documents/Cross-layered/Assignment4/part2". The terminal displays the following output:

```
TCP Header
|-Source Port      : 22
|-Destination Port : 46236
|-Sequence Number  : 3051070456
|-Acknowledge Number : 3717954763
|-Header Length    : 6 DWORDS or 24 BYTES
|-Urgent Flag      : 0
|-Acknowledgement Flag : 1
|-Push Flag        : 0
|-Reset Flag       : 0
|-Synchronise Flag : 1
|-Finish Flag      : 0
|-Window           : 5840
|-Checksum         : 46212
|-Urgent Pointer    : 0

*****WARNING*****
This frame is a suspected retransmission. Possible SYN FLOOD attack
|-Source IP       : 192.168.113.129
|-Target IP       : 192.168.113.1
|-Source Port     : 22
|-Target Port     : 46236
|-Connection requests: 1
|-Positive Responses : 3
|-Frame Number    : 53074
|-Warning number   : 0
```



The screenshot shows a Sublime Text editor window titled "Sublime Text (UNREGISTERED)". The file "warningsLog.txt" is open, showing the following content:

```
1 Opening the capture file for for sniffing ....
2 File Opened!
3
4 *****WARNING*****
5 This frame is a suspected retransmission. Possible SYN FLOOD attack
6   |-Source IP       : 192.168.113.129
7   |-Target IP       : 192.168.113.1
8   |-Source Port     : 22
9   |-Target Port     : 46236
10  |-Connection requests: 1
11  |-Positive Responses : 3
12  |-Frame Number    : 53074
13  |-Warning number   : 0
14
15 *****WARNING*****
16 This frame is a suspected retransmission. Possible SYN FLOOD attack
17   |-Source IP       : 192.168.113.129
18   |-Target IP       : 192.168.113.1
19   |-Source Port     : 22
20   |-Target Port     : 46236
21  |-Connection requests: 1
22  |-Positive Responses : 4
23  |-Frame Number    : 116753
24  |-Warning number   : 0
25
26 *****WARNING*****
27 This frame is a suspected retransmission. Possible SYN FLOOD attack
```

A blue arrow points to the warning message on line 5: "This frame is a suspected retransmission. Possible SYN FLOOD attack".

part2Trace.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 192.168.113.1 && ip.dst == 192.168.113.129 && tcp.sport == 46236 && tcp.dport == 22

No.	Time	Source	Destination	Protocol	Length	Info
6888	0.000000	192.168.113.1	192.168.113.129	TCP	58	46236 → 22 [SYN] Seq=0 Win=2048 Len=0 MSS=1460

> Frame 6888: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)

> Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_3b:9d:97 (00:0c:29:3b:9d:97)

> Internet Protocol Version 4, Src: 192.168.113.1 (192.168.113.1), Dst: 192.168.113.129 (192.168.113.129)

▼ Transmission Control Protocol, Src Port: 46236, Dst Port: 22, Seq: 0, Len: 0

Source Port: 46236

Destination Port: 22

[Stream index: 29]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Sequence number (raw): 3717954762

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 0

Acknowledgment number (raw): 0

0110 = Header Length: 24 bytes (6)

> Flags: 0x002 (SYN)

Window size value: 2048

[Calculated window size: 2048]

Checksum: 0x1d3a [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

> Options: (4 bytes), Maximum segment size

> [Timestamps]

0000 00 0c 29 3b 9d 97 00 50 56 c0 00 08 00 45 00 ..):...P V.....E..

0010 00 2c 67 55 00 00 35 06 ba a3 c0 a8 71 01 c0 a8 ..gU..5.q...

part2Trace.pcap

Packets: 338852 · Displayed: 1 (0.0%)

Profile: Default

2:06 AM 4/25/2020

part2Trace.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 192.168.113.129 && ip.dst == 192.168.113.1 && tcp.sport == 22 && tcp.dport == 46236

No.	Time	Source	Destination	Protocol	Length	Info
6908	0.000000	192.168.113.129	192.168.113.1	TCP	58	22 → 46236 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
23169	3.206140	192.168.113.129	192.168.113.1	TCP	58	[TCP Retransmission] 22 → 46236 [SYN, ACK] Seq=0 Ack=1 Win=5...
53074	6.022613	192.168.113.129	192.168.113.1	TCP	58	[TCP Retransmission] 22 → 46236 [SYN, ACK] Seq=0 Ack=1 Win=5...
116753	12.289446	192.168.113.129	192.168.113.1	TCP	58	[TCP Retransmission] 22 → 46236 [SYN, ACK] Seq=0 Ack=1 Win=5...
244814	24.001461	192.168.113.129	192.168.113.1	TCP	58	[TCP Retransmission] 22 → 46236 [SYN, ACK] Seq=0 Ack=1 Win=5...
319446	48.174678	192.168.113.129	192.168.113.1	TCP	58	[TCP Retransmission] 22 → 46236 [SYN, ACK] Seq=0 Ack=1 Win=5...

Sequence number: 0 (relative sequence number)

Sequence number (raw): 3051070456

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 3717954763

0110 = Header Length: 24 bytes (6)

> Flags: 0x012 (SYN, ACK)

Window size value: 5840

[Calculated window size: 5840]

Checksum: 0xb484 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

> Options: (4 bytes), Maximum segment size

▼ [SEQ/ACK analysis]

▼ [TCP Analysis Flags]

> [Expert Info (Note/Sequence): This frame is a (suspected) retransmission]

[The RTO for this segment was: 3.206140000 seconds]

[RTO based on delta from frame: 6908]

> [Timestamps]

0000 00 50 56 c0 00 08 00 29 3b 9d 97 00 45 00 ..PV.....):....E..

0010 00 2c 00 00 40 00 06 d6 f8 c0 a8 71 81 c0 a8 ..,..@:....q...

Expert Info (.ws.expert)

Packets: 338852 · Displayed: 6 (0.0%)

Profile: Default

2:04 AM 4/25/2020