Christopher Smith
Assignment Example

Abstract

Examine network traffic to determine what information is exposed in transit. Sample traffic is generated and sent. The packets are observed and examined for content. The results demonstrate that all information sent is clear to read by an attacker.

Introduction

Kali Linux will be used in a VirtualBox Virtual machine. Netcat will be used to send and receive unencrypted data. Wireshark will be used for packet analysis.

Netcat listener commands used:

```
nc -l 127.0.0.1 -p 31337
```

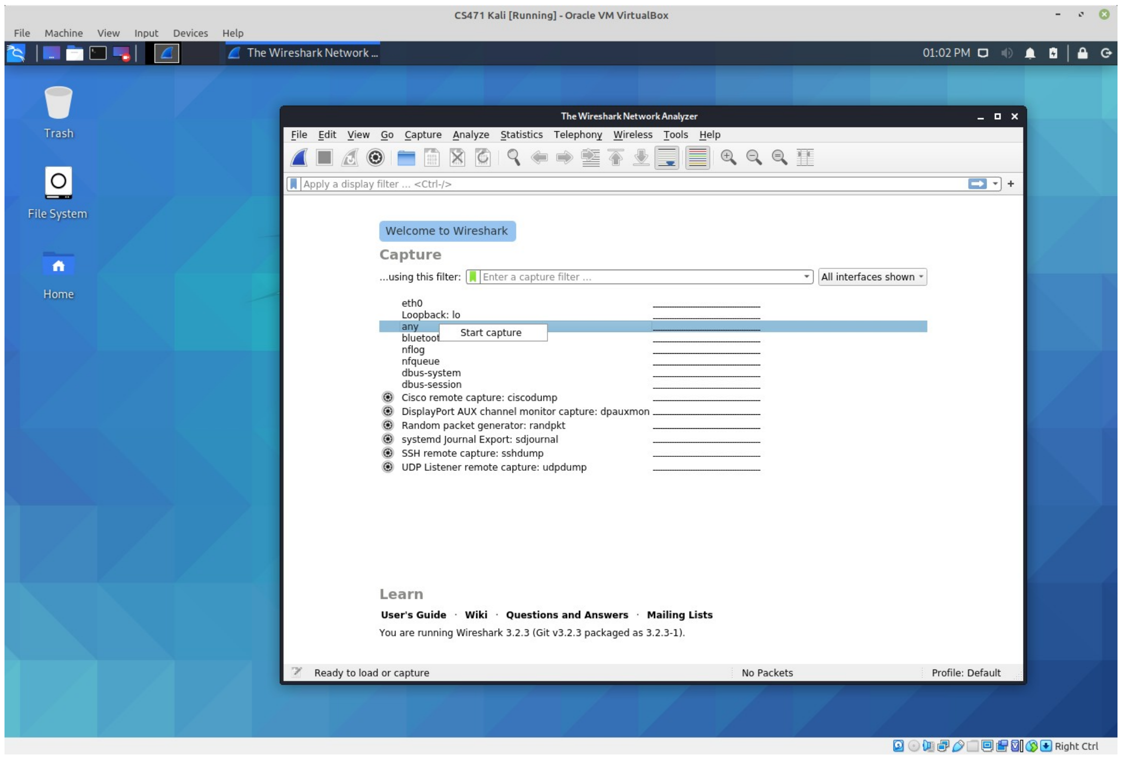
Netcat sender commands:

```
nc 127.0.0.1 -p 31337
```

WireShark run as root while capturing on the ‘any’ adapter.

Summary of Results

Starting WireShark in Kali Linux. Selecting the ‘any’ interface for packet capture.

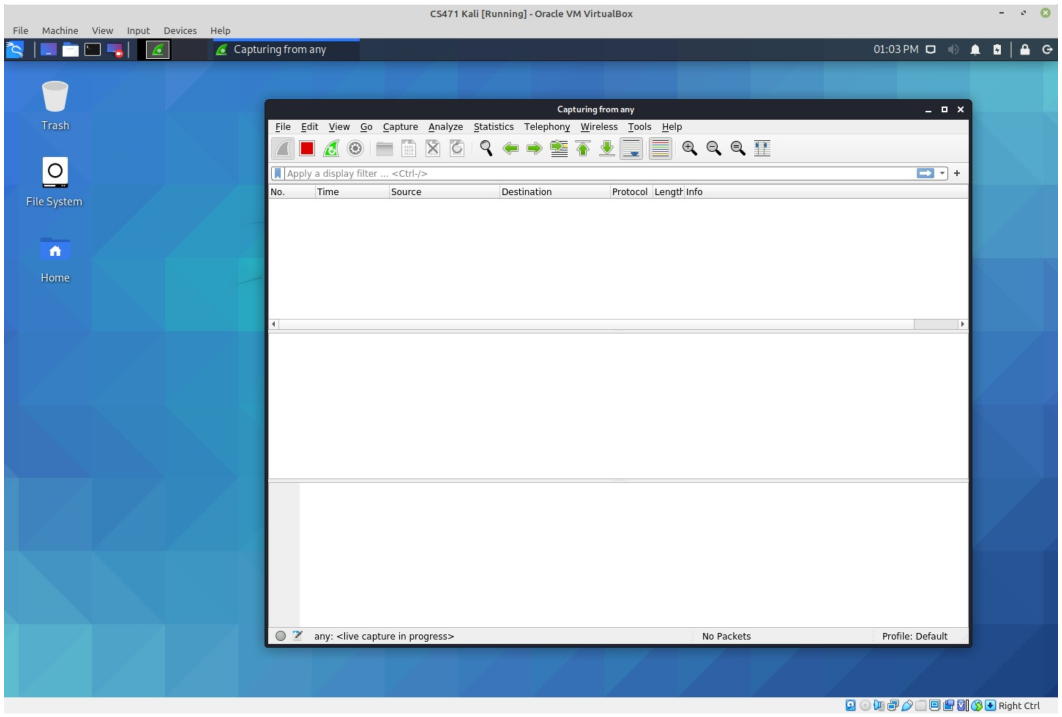

CS471 Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The Wireshark Network ...
01:02 PM
Trash
File System
Home
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Start capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Right Ctrl

```
eth0
Loopback: lo
any
bluetoot
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
```

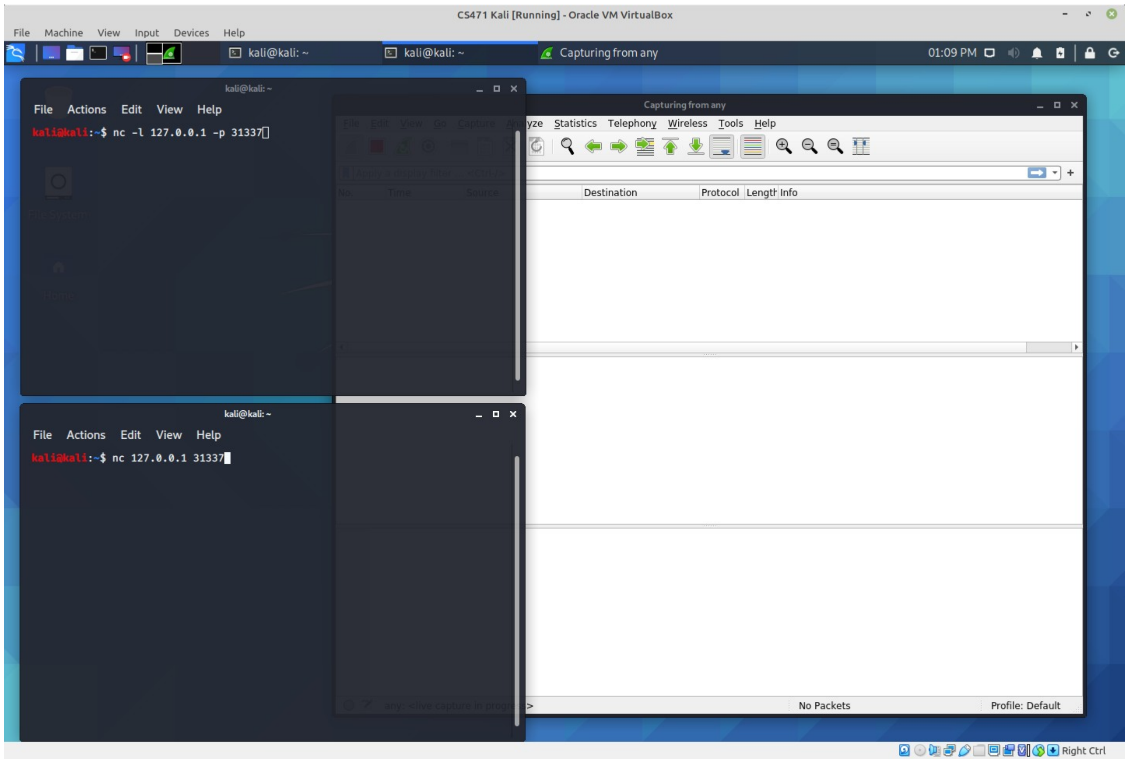
You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).

Ready to load or capture   No Packets   Profile: Default

Now Wireshark is listening. No packets heard.


CS471 Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Capturing from any
01:03 PM
Trash
File System
Home
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
any: <live capture in progress>
No Packets
Profile: Default
Right Ctrl

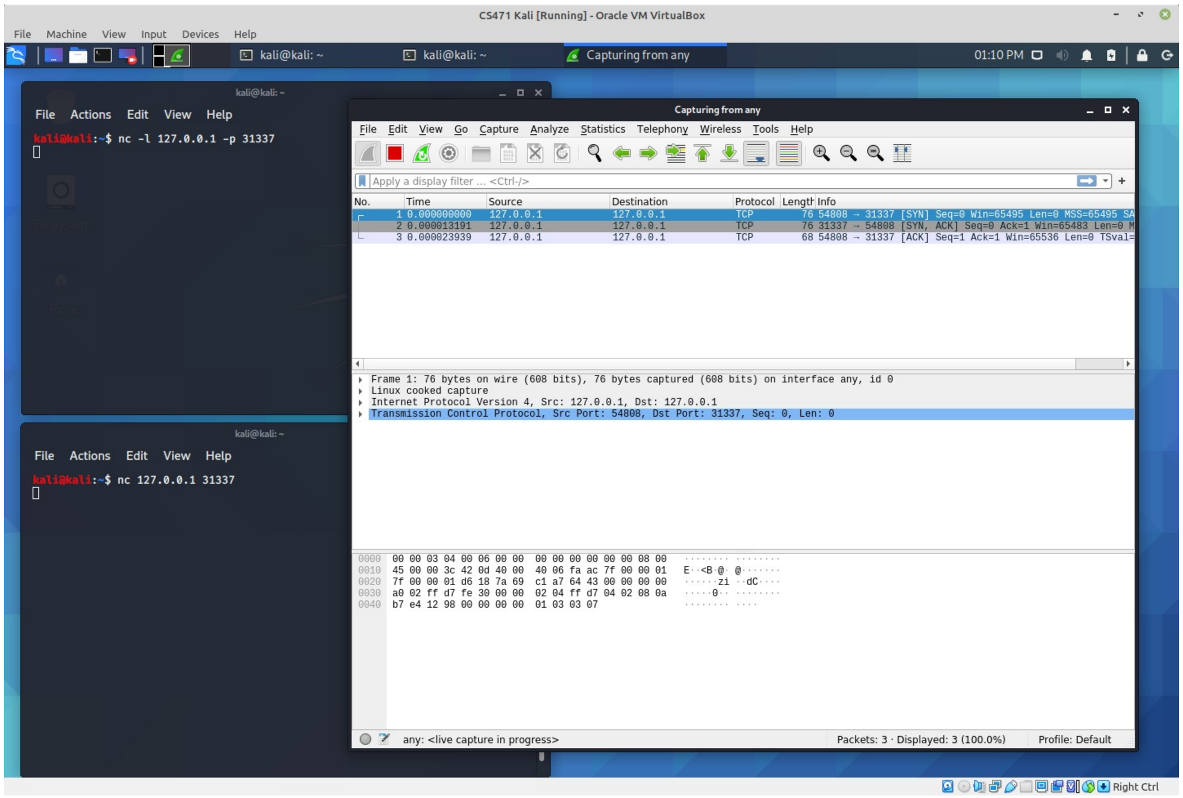
Next open two terminals. One as a netcat listener first, then another as a Netcat sender.


CS471 Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
Capturing from any
01:09 PM
kali@kali: ~
File Actions Edit View Help
Capturing from any
Statistics Telephony Wireless Tools Help
Destination Protocol Length Info
No Packets
Profile: Default
Right Ctrl

```
kali@kali:~$ nc -l 127.0.0.1 -p 31337
```

```
kali@kali:~$ nc 127.0.0.1 31337
```

This reveals the TCP setup connection packets, but no intentional data has been sent.



```
kali@kali:~$ nc -l 127.0.0.1 -p 31337
```

```
kali@kali:~$ nc 127.0.0.1 31337
```

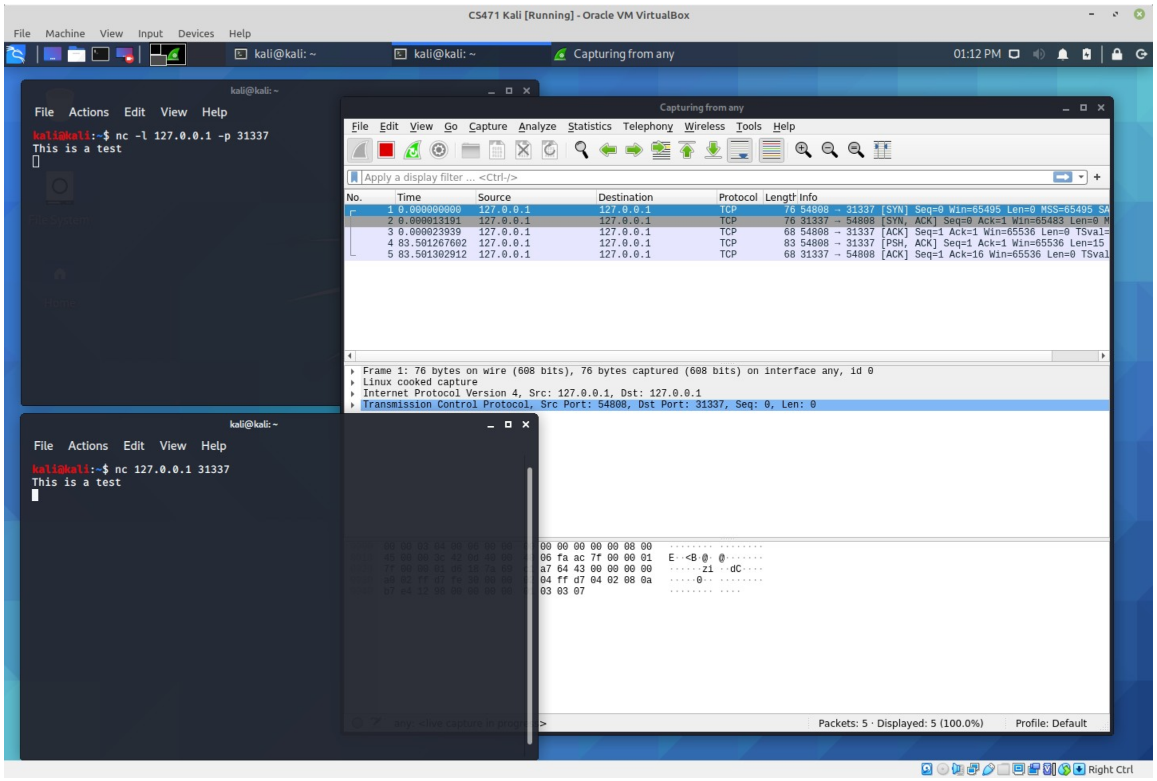
```
No.  Time         Source     Destination  Protocol Length Info
   1 0.000000000  127.0.0.1  127.0.0.1    TCP        76 54808 → 31337 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SA
   2 0.000013191  127.0.0.1  127.0.0.1    TCP        76 31337 → 54808 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 M
   3 0.000023939  127.0.0.1  127.0.0.1    TCP        68 54808 → 31337 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=
```

```
Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 54808, Dst Port: 31337, Seq: 0, Len: 0
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 00 3c 42 0d 40 00  40 06 fa ac 7f 00 00 01   E··<B·@· @·······
0020  7f 00 00 01 d6 18 7a 69  c1 a7 64 43 00 00 00 00   ······zi ··dC····
0030  a0 02 ff d7 fe 30 00 00  02 04 ff d7 04 02 08 0a   ·····0·· ········
0040  b7 e4 12 98 00 00 00 00  01 03 03 07               ········ ····
```

any: <live capture in progress>   Packets: 3 · Displayed: 3 (100.0%)   Profile: Default

Type some text into the sender terminal. Netcat sends this text to the listener over the network. Wireshark captures these packets also.



```
kali@kali:~$ nc -l 127.0.0.1 -p 31337
This is a test
```

```
kali@kali:~$ nc 127.0.0.1 31337
This is a test
```

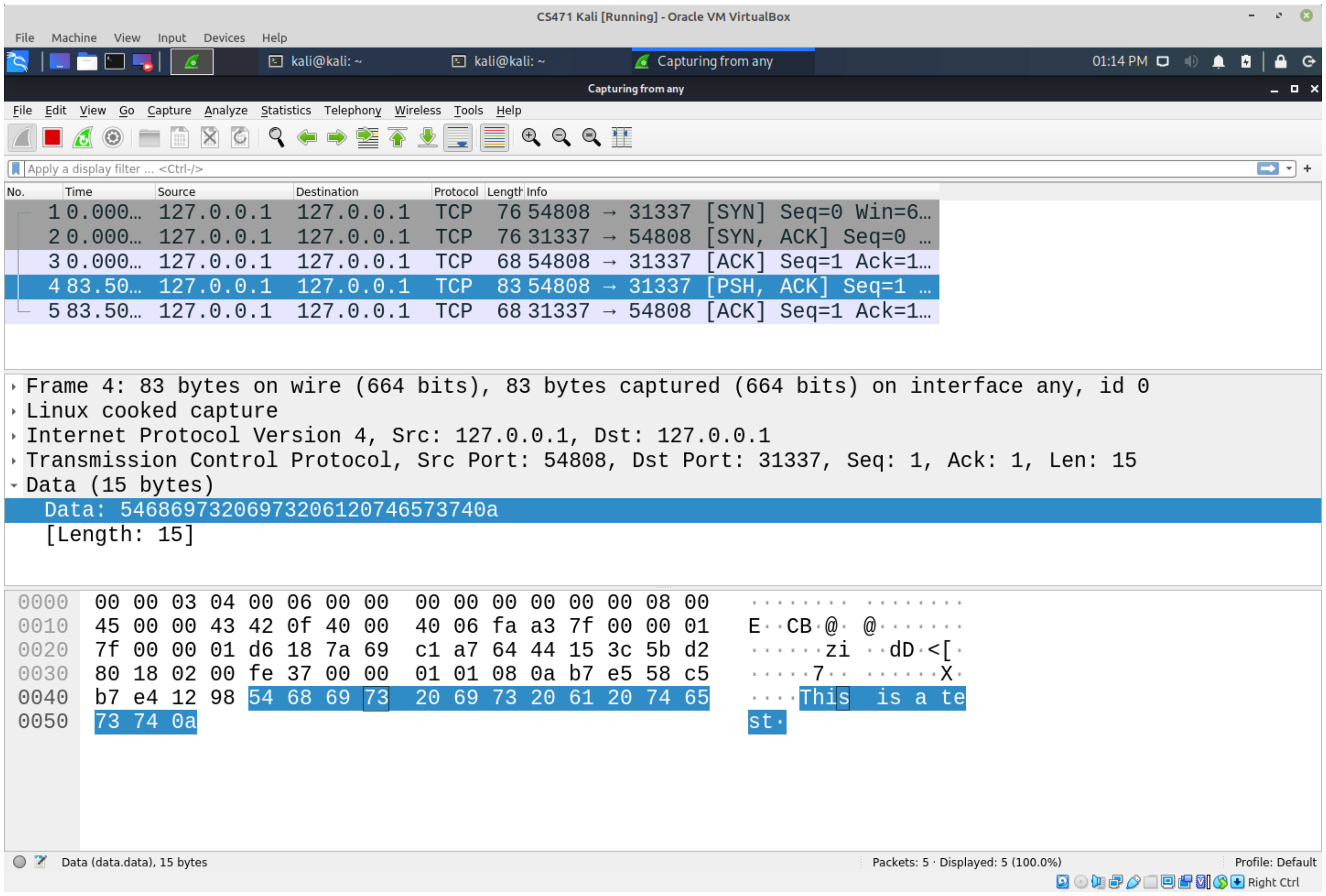
```
No.  Time          Source     Destination  Protocol Length Info
   1 0.000000000   127.0.0.1  127.0.0.1    TCP        76 54808 → 31337 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SA
   2 0.000013191   127.0.0.1  127.0.0.1    TCP        76 31337 → 54808 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 M
   3 0.000023939   127.0.0.1  127.0.0.1    TCP        68 54808 → 31337 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=
   4 83.501267602  127.0.0.1  127.0.0.1    TCP        83 54808 → 31337 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=15
   5 83.501302912  127.0.0.1  127.0.0.1    TCP        68 31337 → 54808 [ACK] Seq=1 Ack=16 Win=65536 Len=0 TSval
```

```
Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 54808, Dst Port: 31337, Seq: 0, Len: 0
```

```
00 00 00 00 08 00   ········ ········
06 fa ac 7f 00 00 01   E··<B·@· @·······
a7 64 43 00 00 00 00   ······zi ··dC····
04 ff d7 04 02 08 0a   ·····0·· ········
03 03 07               ········ ····
```

Packets: 5 · Displayed: 5 (100.0%)   Profile: Default

Notice the text sent over the network was found in the Wireshark capture. The text was easily intercepted and revealed.


CS471 Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
Capturing from any
01:14 PM
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Right Ctrl

```
No. Time     Source     Destination Protocol Length Info
  1 0.000... 127.0.0.1  127.0.0.1   TCP      76 54808 → 31337 [SYN] Seq=0 Win=6…
  2 0.000... 127.0.0.1  127.0.0.1   TCP      76 31337 → 54808 [SYN, ACK] Seq=0 …
  3 0.000... 127.0.0.1  127.0.0.1   TCP      68 54808 → 31337 [ACK] Seq=1 Ack=1…
  4 83.50... 127.0.0.1  127.0.0.1   TCP      83 54808 → 31337 [PSH, ACK] Seq=1 …
  5 83.50... 127.0.0.1  127.0.0.1   TCP      68 31337 → 54808 [ACK] Seq=1 Ack=1…
```

```
› Frame 4: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface any, id 0
› Linux cooked capture
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
› Transmission Control Protocol, Src Port: 54808, Dst Port: 31337, Seq: 1, Ack: 1, Len: 15
⌄ Data (15 bytes)
    Data: 54686973206973206120746573740a
    [Length: 15]
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 00 43 42 0f 40 00  40 06 fa a3 7f 00 00 01   E··CB·@· @·······
0020  7f 00 00 01 d6 18 7a 69  c1 a7 64 44 15 3c 5b d2   ······zi ··dD·<[·
0030  80 18 02 00 fe 37 00 00  01 01 08 0a b7 e5 58 c5   ·····7·· ······X·
0040  b7 e4 12 98 54 68 69 73  20 69 73 20 61 20 74 65   ····This  is a te
0050  73 74 0a                                           st·
```

Data (data.data), 15 bytes   Packets: 5 · Displayed: 5 (100.0%)   Profile: Default

Conclusion

Packets sent over the network are clear to read by any device that intercepts them. Additional measures are required to secure private information.

Note to students:

This sample report is an example of the *format* to use for assignment submission; it lacks sufficent details for a full credit submission. Be sure to include more substance than this example. For each submitted screenshot, be sure to provide a short paragraph explaining the activity shown.

The report should speak to a technical audience and provide enough details so your work is reproducible by following the documented steps. The body of your report should clearly demonstrate your progress when completing the assignment. This includes any difficulties you may have experienced along the way.

Be sure to document your results. Use the conclusion section to explain your results.

Abstract: The abstract is a very short executive summary of the entire document. This includes result. 3-4 sentences only.

Introduction: This includes the tools used and any background information needed to understand your report.

Summary of Results: This includes your work in a *reproducible* way. Explain all of your work here. Include screenshots with descriptions. There should be more words here than pictures….

Conclusion: This should be a cogent explanation of the results. This should explain what the results imply and what the importance of this is. If prompted for a specific conclusion topic, include this, but do not exclude your explanation of results.

Last, try to avoid editorializing and using marketing jargon. Be clear and support your claims with results.