

No.	Time	Source	Destination	Protocol	Length	Info
<div><div></div><div></div></div>						

departmental network

0000	ff ff ff ff ff ff 50 9a 4c 02 e3 74 08 00 45 00	.....P. L...t...E.
0010	00 24 c4 d4 00 00 80 11 5b 31 0a c8 10 83 ff ff	..\$.M.....[1.....
0020	ff ff c3 2d 0f 74 00 10 cf dd 42 01 00 02 00 00	.....t.....B.....
0030	00 01 00 00 00 00 00 00 00 00 00 00	.....

http network – I had to open a new page on the internet for packets to be sent.

The image shows a Wireshark packet capture of an HTTP transaction. The top pane displays a list of packets, with packet 9171 (499 bytes, OCSP Request) and packet 9474 (1012 bytes, OCSP Response) highlighted. The middle pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
9171	72.817721438	10.200.17.126	143.204.72.5	OCSP	499	Request
9474	72.900415508	143.204.72.5	10.200.17.126	OCSP	1012	Response

Frame 9171: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits) on interface enp0s31f6, id 0  
Ethernet II, Src: Dell\_02:66:f9 (50:9a:4c:02:66:f9), Dst: Cisco\_a2:1a:f1 (00:9a:d2:a2:1a:f1)  
Internet Protocol Version 4, Src: 10.200.17.126, Dst: 143.204.72.5  
Transmission Control Protocol, Src Port: 44452, Dst Port: 80, Seq: 1, Ack: 1, Len: 433  
Hypertext Transfer Protocol  
Online Certificate Status Protocol

0000 00 9a d2 a2 1a f1 50 9a 4c 02 66 f9 08 00 45 00 .....P..L.f...E..  
0010 01 e5 eb 8d 40 00 40 06 59 6e 0a c8 11 7e 8f cc ....@..Yn...~..  
0020 48 05 ad a4 00 50 5d 61 20 f9 58 54 ab 6c 80 18 H...P]a XT.l..  
0030 01 f6 f5 ee 00 00 01 01 08 0a de 16 70 b6 59 fa .....p.Y..  
0040 91 36 50 4f 53 54 20 2f 20 48 54 54 50 2f 31 2e .6POST / HTTP/1..  
0050 31 0d 0a 48 6f 73 74 3a 20 6f 63 73 70 2e 72 32 1..Host: ocsp.r2..  
0060 6d 30 31 2e 61 6d 61 7a 6f 6e 74 72 75 73 74 2e m01.amaz ontrust..  
0070 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a com..Use r-Agent:..  
0080 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 Mozilla /5.0 (X1..  
0090 31 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 1; Ubuntu; Linux..  
00a0 20 78 38 36 5f 36 34 3b 20 72 76 3a 31 30 39 2e x86\_64; rv:109..  
00b0 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 0) Gecko /2010010

## Raspberry Pi tcpdump

The image shows a Wireshark packet capture of network traffic on a Raspberry Pi. The top pane displays a list of packets, with packets 752 through 760 highlighted. The middle pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and SSH Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
752	58.279300127	192.168.10.1	192.168.10.2	TCP	66	50960 → 22 [ACK] Seq=
753	58.382989054	192.168.10.2	192.168.10.1	SSH	422	Server: Encrypted pac
754	58.383069320	192.168.10.1	192.168.10.2	TCP	66	50960 → 22 [ACK] Seq=
755	58.487149955	192.168.10.2	192.168.10.1	SSH	422	Server: Encrypted pac
756	58.487200793	192.168.10.1	192.168.10.2	TCP	66	50960 → 22 [ACK] Seq=
757	58.590970108	192.168.10.2	192.168.10.1	SSH	422	Server: Encrypted pac
758	58.591132844	192.168.10.1	192.168.10.2	TCP	66	50960 → 22 [ACK] Seq=
759	58.694959035	192.168.10.2	192.168.10.1	SSH	422	Server: Encrypted pac
760	58.695017001	192.168.10.1	192.168.10.2	TCP	66	50960 → 22 [ACK] Seq=

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface enx0c37965f8a27, id 0  
Ethernet II, Src: BizlinkT\_5f:8a:27 (0c:37:96:5f:8a:27), Dst: Raspberr\_8b:b3:71 (e4:5f:01:8b:b3:71)  
Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.2  
Transmission Control Protocol, Src Port: 50960, Dst Port: 22, Seq: 1, Ack: 1, Len: 36  
SSH Protocol

0000 e4 5f 01 8b b3 71 0c 37 96 5f 8a 27 08 00 45 10 ..\_..q.7 ..\_'.E..  
0010 00 58 77 83 40 00 40 06 2d b9 c0 a8 0a 01 c0 a8 .Xw.@.@. ....  
0020 0a 02 c7 10 00 16 e4 ec 30 1e 9a 20 f8 4c 80 18 .....0...L..  
0030 03 7d 95 9e 00 00 01 01 08 0a 23 03 19 f3 e2 4d .}.....#...M..  
0040 ee 93 d7 e0 d9 80 fa 1c 0f c2 ee b0 fb 80 13 54 .....T..  
0050 46 cb 63 f9 f9 ae 8c 18 2c 3d 74 b8 a4 e4 8a cf F.c.....,=t....  
0060 3c 86 8d 95 cc 5e <.....^

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	192.168.10.2	192.168.10.1	SSH	286	Server: Encrypted packet (
2	0.000000325	192.168.10.2	192.168.10.1	SSH	254	Server: Encrypted packet (
3	0.000047517	192.168.10.1	192.168.10.2	TCP	66	50960 → 22 [ACK] Seq=1 Ack:
4	0.000060215	192.168.10.1	192.168.10.2	TCP	66	50960 → 22 [ACK] Seq=1 Ack:
5	0.001358244	192.168.10.2	192.168.10.1	SSH	166	Server: Encrypted packet (
6	0.001385238	192.168.10.1	192.168.10.2	TCP	66	50960 → 22 [ACK] Seq=1 Ack:

sending Traffic

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
408	1575.3374803...	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
409	1575.4294675...	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
410	1575.5014646...	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
411	1575.5575314...	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
412	1575.6254120...	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
413	1575.7058662...	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
414	1575.7814281...	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
415	1575.8373737...	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
416	1578.2149015...	fe80::f143:9634:fdd...	ff02::2	ICMPv6	62	Router Solicitation

▶ Frame 411: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface enx0c37965f8a27, id 0 ▶ Ethernet II, Src: 00:00:00_00:00:02 (00:00:00:00:00:02), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01) ▶ Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.2 ▶ User Datagram Protocol, Src Port: 50000, Dst Port: 1024 ▶ Data (22 bytes) Data: 78657575766a6f766c666a6c72657a6475666777657a [Length: 22]
---

this is running the original code

you could use a UDP filter

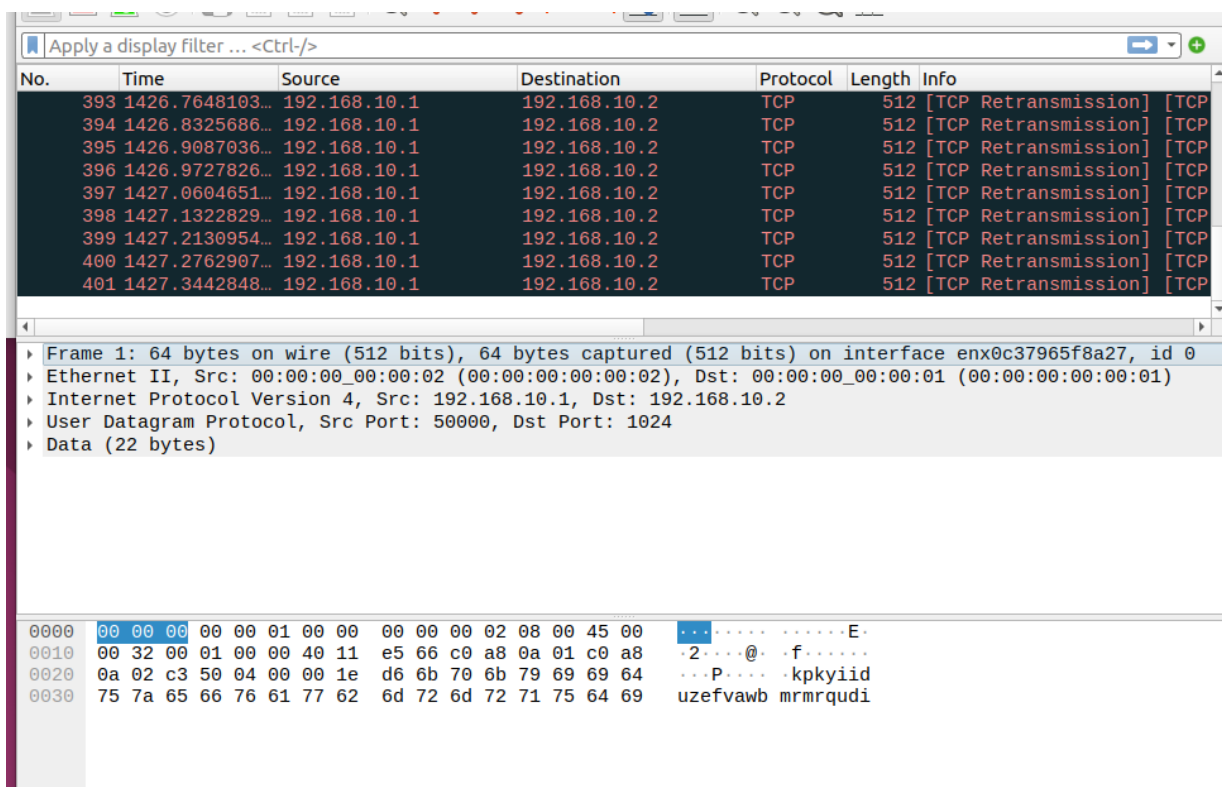
the length o data is 22 bytes but the packet itself is 64 bytes

protocol used is UDP

edited code

```
1#!/usr/bin/python
2
3from scapy.all import Ether, IP, sendp, get_if_hwaddr, get_if_list, TCP, Raw, UDP
4import sys
5import random, string
6
7
8def randomword(length):
9    return ''.join(random.choice(string.ascii_lowercase) for i in range(length))
10
11def send_random_traffic(num_packets, interface, src_ip, dst_ip):
12    dst_mac = "00:00:00:00:00:01"
13    src_mac= "CA:FE:CA:FE:CA:FE"
14    total_pkts = 0
15    port = 1024
16    for i in range(num_packets):
17        data = randomword(458)
18        p = Ether(dst=dst_mac,src=src_mac)/IP(dst=dst_ip,src=src_ip)
19        p = p/TCP(sport= 5555, dport=port)/Raw(load=data)
20        sendp(p, iface = interface, inter = 0.01)
21        # If you want to see the contents of the packet, uncomment the line below
22        # print(p.show())
23        total_pkts += 1
24    print("Sent %s packets in total" % total_pkts)
25
26if __name__ == '__main__':
27    if len(sys.argv) < 5:
28        print("Usage: python send.py number_of_packets interface_name src_ip_address dst_ip_address")
29        sys.exit(1)
30    else:
31        num_packets = sys.argv[1]
32        interface = sys.argv[2]
33        src_ip = sys.argv[3]
34        dst_ip = sys.argv[4]
35        send_random_traffic(int(num_packets), interface, src_ip, dst_ip)
```

result



No.	Time	Source	Destination	Protocol	Length	Info
393	1426.7648103...	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP
394	1426.8325686...	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP
395	1426.9087036...	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP
396	1426.9727826...	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP
397	1427.0604651...	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP
398	1427.1322829...	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP
399	1427.2130954...	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP
400	1427.2762907...	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP
401	1427.3442848...	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP

Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface enx0c37965f8a27, id 0	
Ethernet II, Src: 00:00:00:00:00:02 (00:00:00:00:00:02), Dst: 00:00:00:00:00:01 (00:00:00:00:00:01)	
Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.2	
User Datagram Protocol, Src Port: 50000, Dst Port: 1024	
Data (22 bytes)	
0000	00 00 00 00 00 01 00 00 00 00 02 08 00 45 00 .....
0010	00 32 00 01 00 00 40 11 e5 66 c0 a8 0a 01 c0 a8 .2....@. .f.....
0020	0a 02 c3 50 04 00 00 1e d6 b7 70 b7 79 69 69 64 ...P.... .kpyiid
0030	75 7a 65 66 76 61 77 62 6d 72 6d 72 71 75 64 69 uzefvawb mrmrqudi