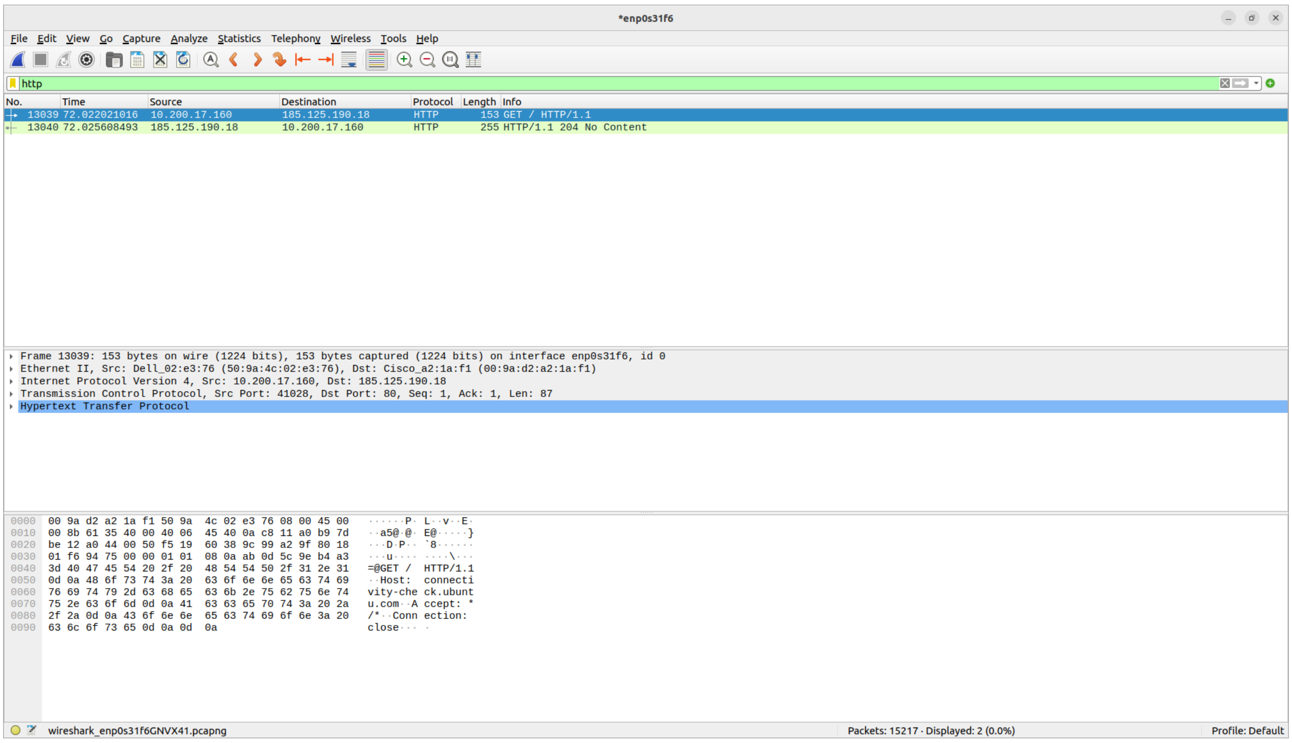
Traffic capture – assignment 1

connection to 192.168.10.1:
no packets captured

connecting to the departmental network:
Many packets captured.
Many were sent to 10.200.xx.xx as these are departmental addresses.
Many were also sent to 255.255.255.255 – broadband
The most common protocol was GVCP
no of packets increased as I searched the web – this produced http traffic which could be viewed after I placed a http filer on


*enp0s31f6
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

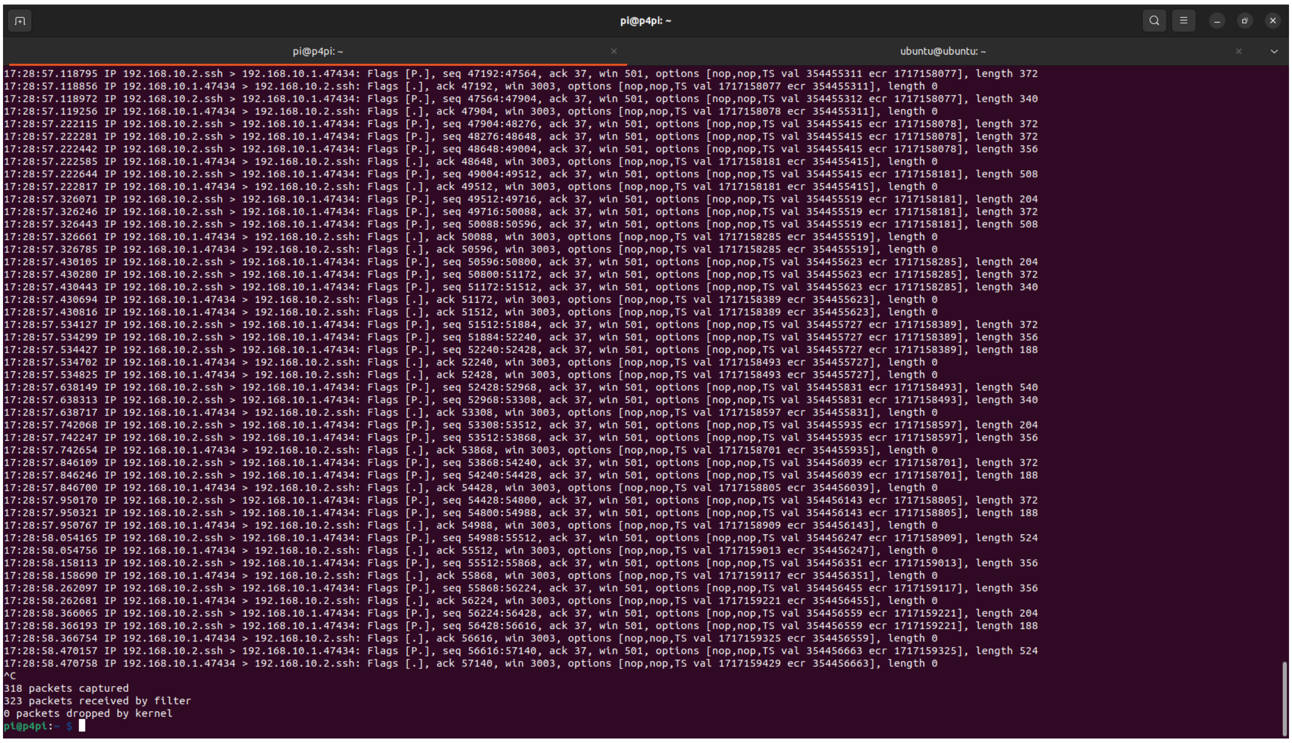
```
No.    Time          Source          Destination     Protocol  Length Info
13039 72.022021016  10.200.17.160   185.125.190.18  HTTP         153 GET / HTTP/1.1
13040 72.025608493  185.125.190.18  10.200.17.160   HTTP         255 HTTP/1.1 204 No Content
```

```
Frame 13039: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface enp0s31f6, id 0
Ethernet II, Src: Dell_02:e3:76 (50:9a:4c:02:e3:76), Dst: Cisco_a2:1a:f1 (00:9a:d2:a2:1a:f1)
Internet Protocol Version 4, Src: 10.200.17.160, Dst: 185.125.190.18
Transmission Control Protocol, Src Port: 41028, Dst Port: 80, Seq: 1, Ack: 1, Len: 87
Hypertext Transfer Protocol
```

```
0000  00 9a d2 a2 1a f1 50 9a  4c 02 e3 76 08 00 45 00   ······P· L··v··E·
0010  00 8b 61 35 40 00 40 06  45 40 0a c8 11 a0 b9 7d   ··a5@·@· E@·····}
0020  be 12 a0 44 00 50 f5 19  60 38 9c 99 a2 9f 80 18   ···D·P·· `8······
0030  01 f6 94 75 00 00 01 01  08 0a ab 0d 5c 9e b4 a3   ···u···· ····\···
0040  3d 40 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   =@GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  63 6f 6e 6e 65 63 74 69   ··Host:  connecti
0060  76 69 74 79 2d 63 68 65  63 6b 2e 75 62 75 6e 74   vity-che ck.ubunt
0070  75 2e 63 6f 6d 0d 0a 41  63 63 65 70 74 3a 20 2a   u.com··A ccept: *
0080  2f 2a 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   /*··Conn ection: 
0090  63 6c 6f 73 65 0d 0a 0d  0a                        close··· ·
```

wireshark_enp0s31f6GNVX41.pcapng   Packets: 15217 · Displayed: 2 (0.0%)   Profile: Default

Packet capture on raspberry pi:

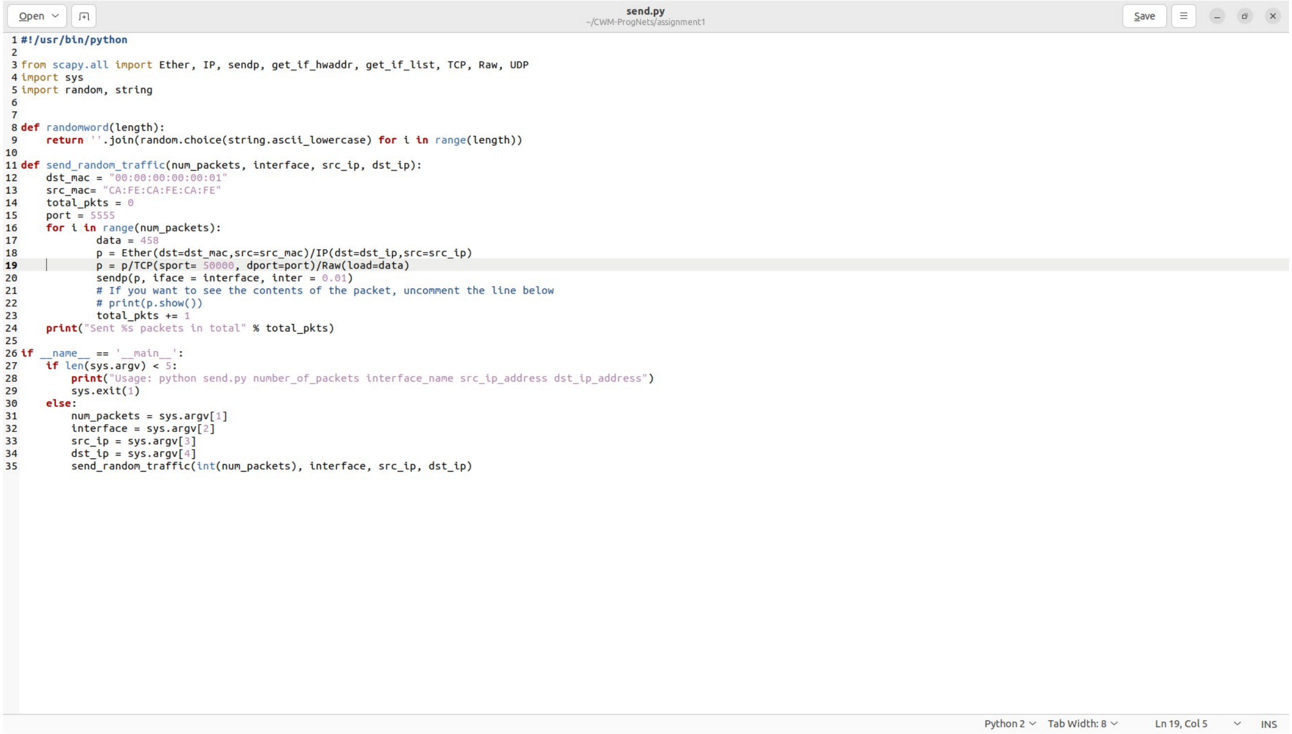


```
17:28:57.118795 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 47192:47564, ack 37, win 501, options [nop,nop,TS val 354455311 ecr 1717158077], length 372
17:28:57.118856 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 47192, win 3003, options [nop,nop,TS val 1717158077 ecr 354455311], length 0
17:28:57.118972 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 47564:47904, ack 37, win 501, options [nop,nop,TS val 354455312 ecr 1717158077], length 340
17:28:57.119256 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 47904, win 3003, options [nop,nop,TS val 1717158078 ecr 354455311], length 0
17:28:57.222115 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 47904:48276, ack 37, win 501, options [nop,nop,TS val 354455415 ecr 1717158078], length 372
17:28:57.222281 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 48276:48648, ack 37, win 501, options [nop,nop,TS val 354455415 ecr 1717158078], length 372
17:28:57.222442 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 48648:49004, ack 37, win 501, options [nop,nop,TS val 354455415 ecr 1717158078], length 356
17:28:57.222585 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 48648, win 3003, options [nop,nop,TS val 1717158181 ecr 354455415], length 0
17:28:57.222644 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 49004:49512, ack 37, win 501, options [nop,nop,TS val 354455415 ecr 1717158181], length 508
17:28:57.222817 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 49512, win 3003, options [nop,nop,TS val 1717158181 ecr 354455415], length 0
17:28:57.326071 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 49512:49716, ack 37, win 501, options [nop,nop,TS val 354455519 ecr 1717158181], length 204
17:28:57.326246 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 49716:50088, ack 37, win 501, options [nop,nop,TS val 354455519 ecr 1717158181], length 372
17:28:57.326443 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 50088:50596, ack 37, win 501, options [nop,nop,TS val 354455519 ecr 1717158181], length 508
17:28:57.326661 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 50088, win 3003, options [nop,nop,TS val 1717158285 ecr 354455519], length 0
17:28:57.326785 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 50596, win 3003, options [nop,nop,TS val 1717158285 ecr 354455519], length 0
17:28:57.430105 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 50596:50800, ack 37, win 501, options [nop,nop,TS val 354455623 ecr 1717158285], length 204
17:28:57.430280 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 50800:51172, ack 37, win 501, options [nop,nop,TS val 354455623 ecr 1717158285], length 372
17:28:57.430443 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 51172:51512, ack 37, win 501, options [nop,nop,TS val 354455623 ecr 1717158285], length 340
17:28:57.430694 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 51172, win 3003, options [nop,nop,TS val 1717158389 ecr 354455623], length 0
17:28:57.430816 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 51512, win 3003, options [nop,nop,TS val 1717158389 ecr 354455623], length 0
17:28:57.534127 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 51512:51884, ack 37, win 501, options [nop,nop,TS val 354455727 ecr 1717158389], length 372
17:28:57.534299 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 51884:52240, ack 37, win 501, options [nop,nop,TS val 354455727 ecr 1717158389], length 356
17:28:57.534427 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 52240:52428, ack 37, win 501, options [nop,nop,TS val 354455727 ecr 1717158389], length 188
17:28:57.534702 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 52240, win 3003, options [nop,nop,TS val 1717158493 ecr 354455727], length 0
17:28:57.534825 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 52428, win 3003, options [nop,nop,TS val 1717158493 ecr 354455727], length 0
17:28:57.638149 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 52428:52968, ack 37, win 501, options [nop,nop,TS val 354455831 ecr 1717158493], length 540
17:28:57.638313 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 52968:53308, ack 37, win 501, options [nop,nop,TS val 354455831 ecr 1717158493], length 340
17:28:57.638717 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 53308, win 3003, options [nop,nop,TS val 1717158597 ecr 354455831], length 0
17:28:57.742068 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 53308:53512, ack 37, win 501, options [nop,nop,TS val 354455935 ecr 1717158597], length 204
17:28:57.742247 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 53512:53868, ack 37, win 501, options [nop,nop,TS val 354455935 ecr 1717158597], length 356
17:28:57.742654 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 53868, win 3003, options [nop,nop,TS val 1717158701 ecr 354455935], length 0
17:28:57.846109 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 53868:54240, ack 37, win 501, options [nop,nop,TS val 354456039 ecr 1717158701], length 372
17:28:57.846246 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 54240:54428, ack 37, win 501, options [nop,nop,TS val 354456039 ecr 1717158701], length 188
17:28:57.846700 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 54428, win 3003, options [nop,nop,TS val 1717158805 ecr 354456039], length 0
17:28:57.950170 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 54428:54800, ack 37, win 501, options [nop,nop,TS val 354456143 ecr 1717158805], length 372
17:28:57.950321 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 54800:54988, ack 37, win 501, options [nop,nop,TS val 354456143 ecr 1717158805], length 188
17:28:57.950767 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 54988, win 3003, options [nop,nop,TS val 1717158909 ecr 354456143], length 0
17:28:58.054165 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 54988:55512, ack 37, win 501, options [nop,nop,TS val 354456247 ecr 1717158909], length 524
17:28:58.054756 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 55512, win 3003, options [nop,nop,TS val 1717159013 ecr 354456247], length 0
17:28:58.158113 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 55512:55868, ack 37, win 501, options [nop,nop,TS val 354456351 ecr 1717159013], length 356
17:28:58.158690 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 55868, win 3003, options [nop,nop,TS val 1717159117 ecr 354456351], length 0
17:28:58.262097 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 55868:56224, ack 37, win 501, options [nop,nop,TS val 354456455 ecr 1717159117], length 356
17:28:58.262681 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 56224, win 3003, options [nop,nop,TS val 1717159221 ecr 354456455], length 0
17:28:58.366065 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 56224:56428, ack 37, win 501, options [nop,nop,TS val 354456559 ecr 1717159221], length 204
17:28:58.366193 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 56428:56616, ack 37, win 501, options [nop,nop,TS val 354456559 ecr 1717159221], length 188
17:28:58.366754 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 56616, win 3003, options [nop,nop,TS val 1717159325 ecr 354456559], length 0
17:28:58.470157 IP 192.168.10.2.ssh > 192.168.10.1.47434: Flags [P.], seq 56616:57140, ack 37, win 501, options [nop,nop,TS val 354456663 ecr 1717159325], length 524
17:28:58.470758 IP 192.168.10.1.47434 > 192.168.10.2.ssh: Flags [.], ack 57140, win 3003, options [nop,nop,TS val 1717159429 ecr 354456663], length 0
^C
318 packets captured
323 packets received by filter
0 packets dropped by kernel
pi@p4pi:~ $
```

Sending Traffic

1. a filter to only capture the packets I sent is UDP only
2. the packet size is 512 bits or 64B
3. the protocol is UDP

Modified send.py for TCP protocol and length of 512B:



```python
#!/usr/bin/python

from scapy.all import Ether, IP, sendp, get_if_hwaddr, get_if_list, TCP, Raw, UDP
import sys
import random, string


def randomword(length):
    return ''.join(random.choice(string.ascii_lowercase) for i in range(length))

def send_random_traffic(num_packets, interface, src_ip, dst_ip):
    dst_mac = "00:00:00:00:00:01"
    src_mac= "CA:FE:CA:FE:CA:FE"
    total_pkts = 0
    port = 5555
    for i in range(num_packets):
            data = 458
            p = Ether(dst=dst_mac,src=src_mac)/IP(dst=dst_ip,src=src_ip)
            p = p/TCP(sport= 50000, dport=port)/Raw(load=data)
            sendp(p, iface = interface, inter = 0.01)
            # If you want to see the contents of the packet, uncomment the line below
            # print(p.show())
            total_pkts += 1
    print("Sent %s packets in total" % total_pkts)

if __name__ == '__main__':
    if len(sys.argv) < 5:
        print("Usage: python send.py number_of_packets interface_name src_ip_address dst_ip_address")
        sys.exit(1)
    else:
        num_packets = sys.argv[1]
        interface = sys.argv[2]
        src_ip = sys.argv[3]
        dst_ip = sys.argv[4]
        send_random_traffic(int(num_packets), interface, src_ip, dst_ip)
```