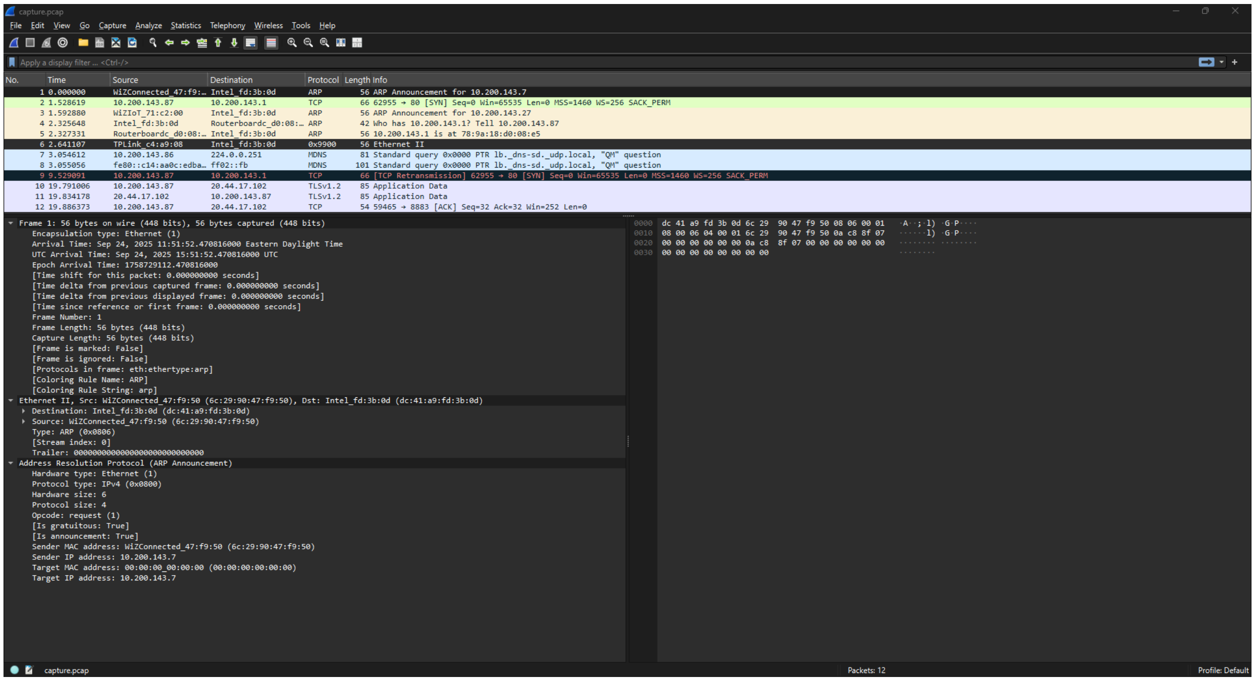
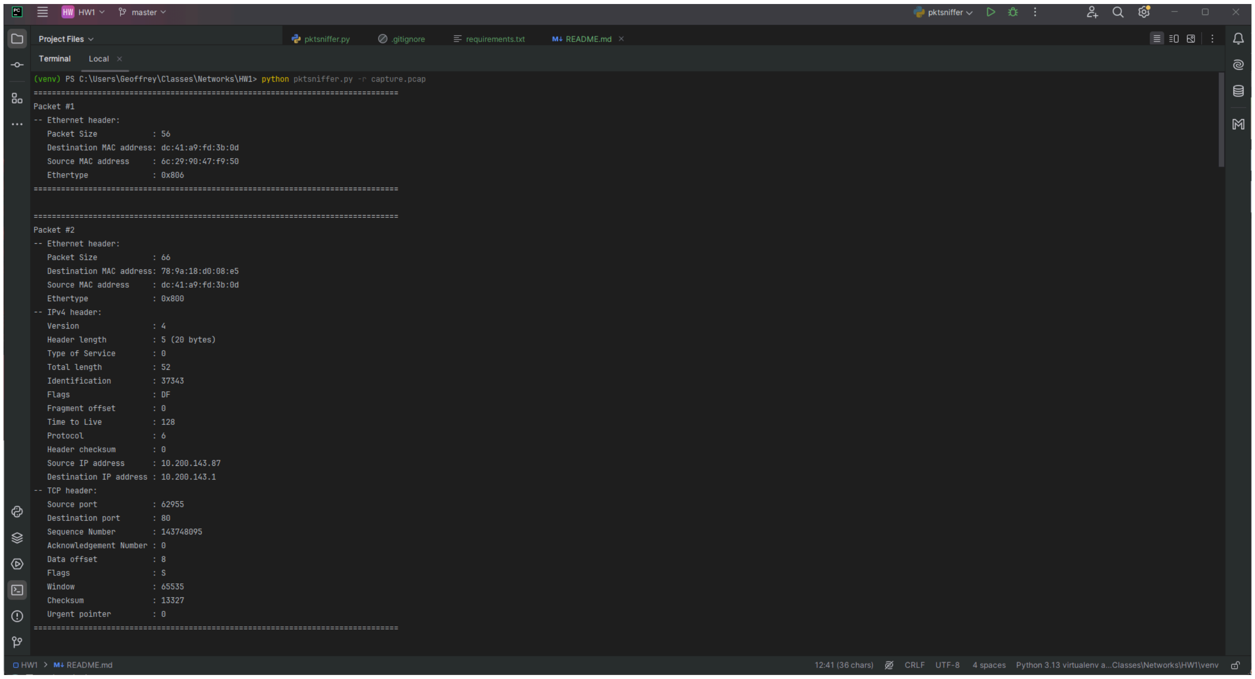
Packet 1:


capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source                Destination           Protocol Length Info
    1 0.000000   WiZConnected_47:f9:… Intel_fd:3b:0d        ARP        56 ARP Announcement for 10.200.143.7
    2 1.528619   10.200.143.87         10.200.143.1          TCP        66 62955 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
    3 1.592880   WiZIoT_71:c2:00       Intel_fd:3b:0d        ARP        56 ARP Announcement for 10.200.143.27
    4 2.325648   Intel_fd:3b:0d        Routerboardc_d0:08:… ARP        42 Who has 10.200.143.1? Tell 10.200.143.87
    5 2.327331   Routerboardc_d0:08:… Intel_fd:3b:0d        ARP        56 10.200.143.1 is at 78:9a:18:d0:08:e5
    6 2.641107   TPLink_c4:a9:08       Intel_fd:3b:0d        0x9900     56 Ethernet II
    7 3.054612   10.200.143.86         224.0.0.251           MDNS       81 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question
    8 3.055056   fe80::c14:aa0c:edba… ff02::fb              MDNS      101 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question
    9 9.529091   10.200.143.87         10.200.143.1          TCP        66 [TCP Retransmission] 62955 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   10 19.791006  10.200.143.87         20.44.17.102          TLSv1.2    85 Application Data
   11 19.834178  20.44.17.102          10.200.143.87         TLSv1.2    85 Application Data
   12 19.886373  10.200.143.87         20.44.17.102          TCP        54 59465 → 8883 [ACK] Seq=32 Ack=32 Win=252 Len=0
```

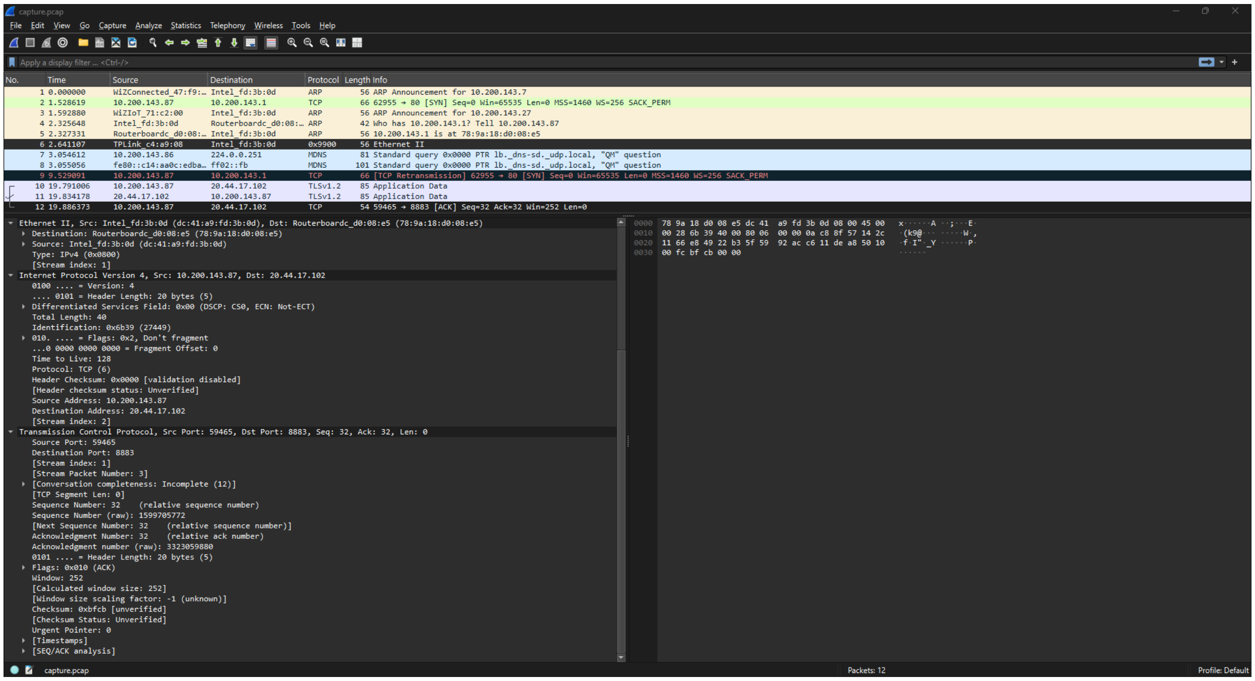
```
▾ Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 24, 2025 11:51:52.470816000 Eastern Daylight Time
    UTC Arrival Time: Sep 24, 2025 15:51:52.470816000 UTC
    Epoch Arrival Time: 1758729112.470816000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 56 bytes (448 bits)
    Capture Length: 56 bytes (448 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
▾ Ethernet II, Src: WiZConnected_47:f9:50 (6c:29:90:47:f9:50), Dst: Intel_fd:3b:0d (dc:41:a9:fd:3b:0d)
  ▸ Destination: Intel_fd:3b:0d (dc:41:a9:fd:3b:0d)
  ▸ Source: WiZConnected_47:f9:50 (6c:29:90:47:f9:50)
    Type: ARP (0x0806)
    [Stream index: 0]
    Trailer: 0000000000000000000000000000
▾ Address Resolution Protocol (ARP Announcement)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    [Is announcement: True]
    Sender MAC address: WiZConnected_47:f9:50 (6c:29:90:47:f9:50)
    Sender IP address: 10.200.143.7
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.200.143.7
```

```
0000  dc 41 a9 fd 3b 0d 6c 29  90 47 f9 50 08 06 00 01   ·A··;·l) ·G·P····
0010  08 00 06 04 00 01 6c 29  90 47 f9 50 0a c8 8f 07   ······l) ·G·P····
0020  00 00 00 00 00 00 0a c8  8f 07 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00                            ········
```



```
(venv) PS C:\Users\Geoffrey\Classes\Networks\HW1> python pktsniffer.py -r capture.pcap
================================================================================
Packet #1
-- Ethernet header:
   Packet Size            : 56
   Destination MAC address: dc:41:a9:fd:3b:0d
   Source MAC address     : 6c:29:90:47:f9:50
   Ethertype              : 0x806
================================================================================

================================================================================
Packet #2
-- Ethernet header:
   Packet Size            : 66
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
   Header length          : 5 (20 bytes)
   Type of Service        : 0
   Total length           : 52
   Identification         : 37343
   Flags                  : DF
   Fragment offset        : 0
   Time to Live           : 128
   Protocol               : 6
   Header checksum        : 0
   Source IP address      : 10.200.143.87
   Destination IP address : 10.200.143.1
-- TCP header:
   Source port            : 62955
   Destination port       : 80
   Sequence Number        : 143748095
   Acknowledgement Number : 0
   Data offset            : 8
   Flags                  : S
   Window                 : 65535
   Checksum               : 13327
   Urgent pointer         : 0
================================================================================
```

Packet 12:

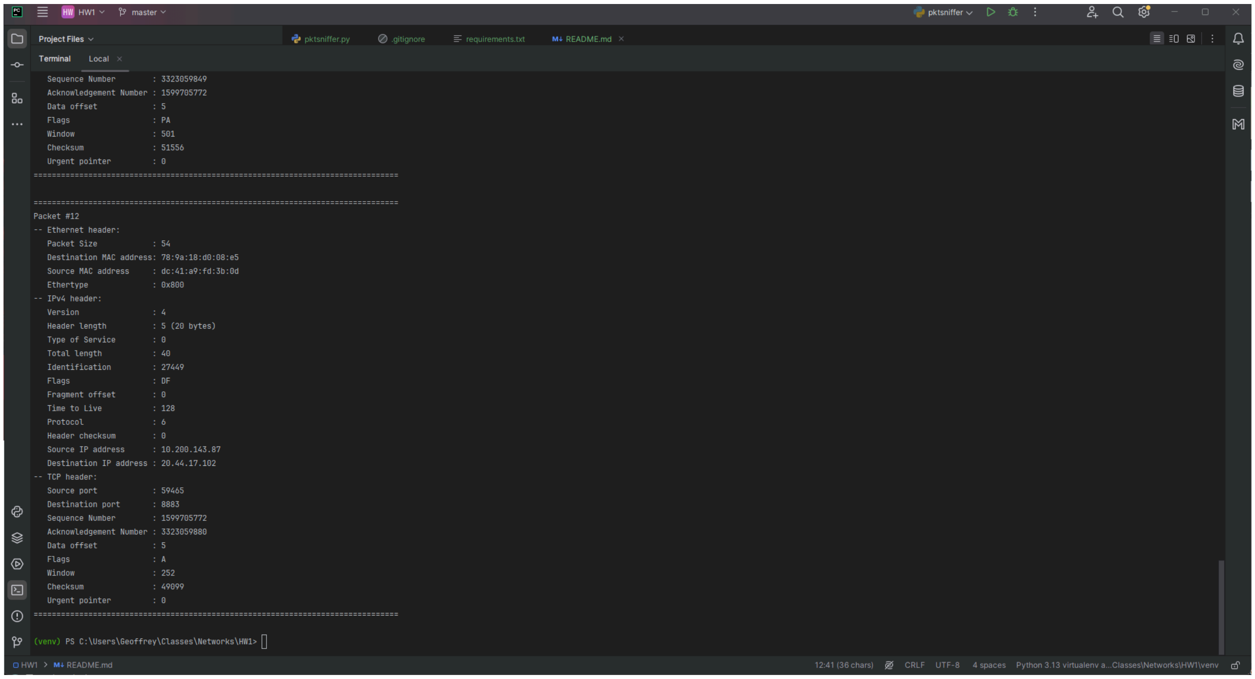

capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Packets: 12
Profile: Default

```
No.  Time       Source                 Destination          Protocol Length Info
   1 0.000000   WiZConnected_47:f9:…   Intel_fd:3b:0d       ARP        56 ARP Announcement for 10.200.143.7
   2 1.528619   10.200.143.87          10.200.143.1         TCP        66 62955 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   3 1.592880   WiZIoT_71:c2:00        Intel_fd:3b:0d       ARP        56 ARP Announcement for 10.200.143.27
   4 2.325648   Intel_fd:3b:0d         Routerboardc_d0:08:… ARP        42 Who has 10.200.143.1? Tell 10.200.143.87
   5 2.327331   Routerboardc_d0:08:…   Intel_fd:3b:0d       ARP        56 10.200.143.1 is at 78:9a:18:d0:08:e5
   6 2.641107   TPLink_c4:a9:08        Intel_fd:3b:0d       0x9900     56 Ethernet II
   7 3.054612   10.200.143.86          224.0.0.251          MDNS       81 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question
   8 3.055056   fe80::c14:aa0c:edba…   ff02::fb             MDNS      101 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question
   9 9.529091   10.200.143.87          10.200.143.1         TCP        66 [TCP Retransmission] 62955 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  10 19.791006  10.200.143.87          20.44.17.102         TLSv1.2    85 Application Data
  11 19.834178  20.44.17.102           10.200.143.87        TLSv1.2    85 Application Data
  12 19.886373  10.200.143.87          20.44.17.102         TCP        54 59465 → 8883 [ACK] Seq=32 Ack=32 Win=252 Len=0
```

```
Ethernet II, Src: Intel_fd:3b:0d (dc:41:a9:fd:3b:0d), Dst: Routerboardc_d0:08:e5 (78:9a:18:d0:08:e5)
  Destination: Routerboardc_d0:08:e5 (78:9a:18:d0:08:e5)
  Source: Intel_fd:3b:0d (dc:41:a9:fd:3b:0d)
  Type: IPv4 (0x0800)
  [Stream index: 1]
Internet Protocol Version 4, Src: 10.200.143.87, Dst: 20.44.17.102
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0x6b39 (27449)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.200.143.87
  Destination Address: 20.44.17.102
  [Stream index: 2]
Transmission Control Protocol, Src Port: 59465, Dst Port: 8883, Seq: 32, Ack: 32, Len: 0
  Source Port: 59465
  Destination Port: 8883
  [Stream index: 1]
  [Stream Packet Number: 3]
  [Conversation completeness: Incomplete (12)]
  [TCP Segment Len: 0]
  Sequence Number: 32    (relative sequence number)
  Sequence Number (raw): 1599705772
  [Next Sequence Number: 32    (relative sequence number)]
  Acknowledgment Number: 32    (relative ack number)
  Acknowledgment number (raw): 3323059880
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x010 (ACK)
  Window: 252
  [Calculated window size: 252]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0xbfcb [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
```

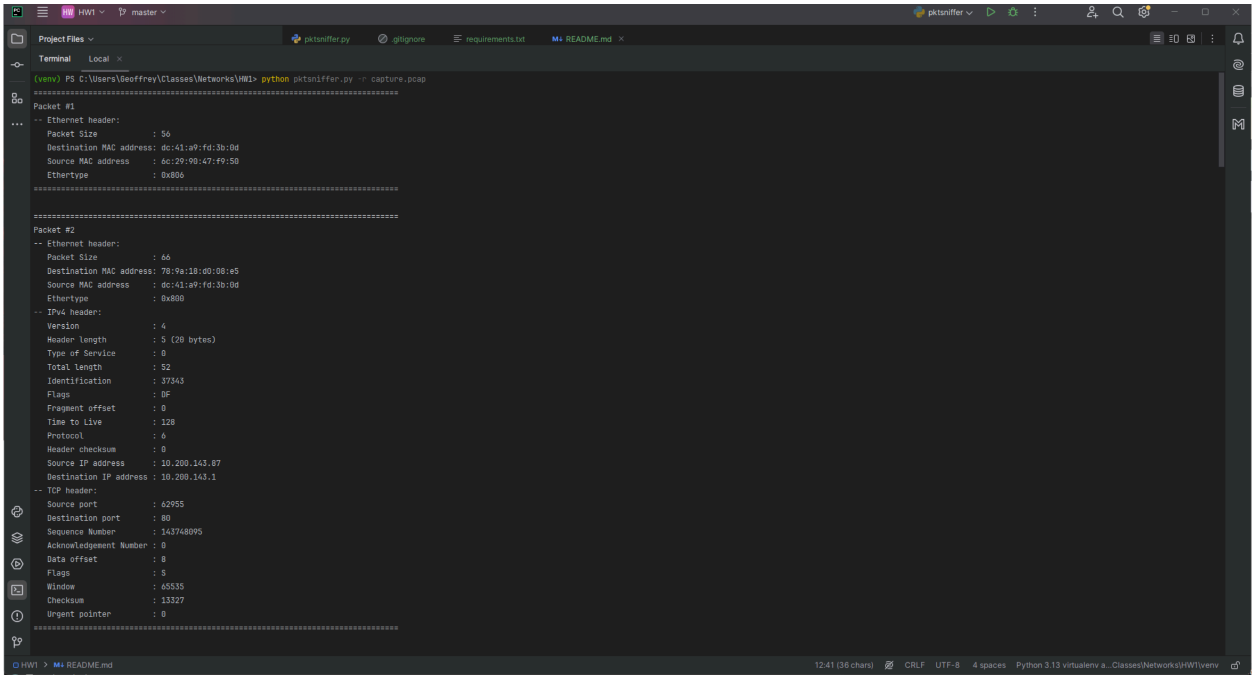
```
0000  78 9a 18 d0 08 e5 dc 41  a9 fd 3b 0d 08 00 45 00   x·····A ··;···E·
0010  00 28 6b 39 40 00 80 06  00 00 0a c8 8f 57 14 2c   ·(k9@··· ·····W·,
0020  11 66 e8 49 22 b3 5f 59  92 ac c6 11 de a8 50 10   ·f·I"·_Y ······P·
0030  00 fc bf cb 00 00                                  ······
```

capture.pcap



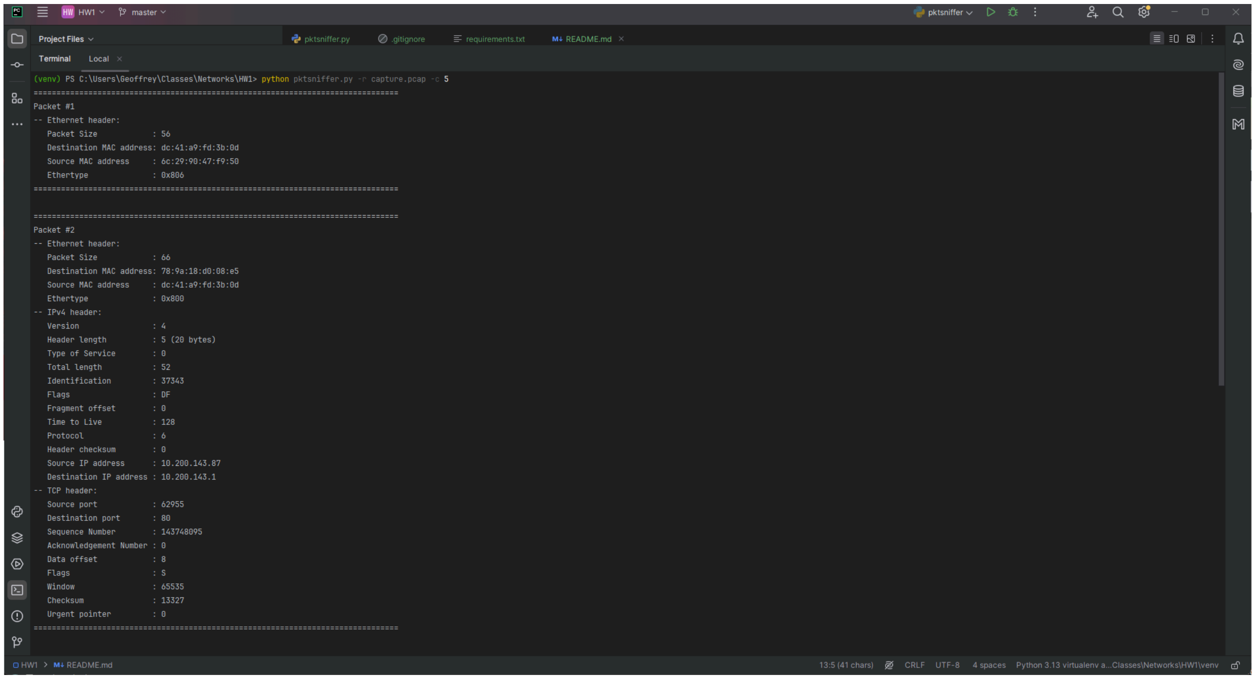
```
   Sequence Number        : 3323059849
   Acknowledgement Number : 1599705772
   Data offset            : 5
   Flags                  : PA
   Window                 : 501
   Checksum               : 51556
   Urgent pointer         : 0
================================================================================

================================================================================
Packet #12
-- Ethernet header:
   Packet Size            : 54
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
   Header length          : 5 (20 bytes)
   Type of Service        : 0
   Total length           : 40
   Identification         : 27449
   Flags                  : DF
   Fragment offset        : 0
   Time to Live           : 128
   Protocol               : 6
   Header checksum        : 0
   Source IP address      : 10.200.143.87
   Destination IP address : 20.44.17.102
-- TCP header:
   Source port            : 59465
   Destination port       : 8883
   Sequence Number        : 1599705772
   Acknowledgement Number : 3323059880
   Data offset            : 5
   Flags                  : A
   Window                 : 252
   Checksum               : 49099
   Urgent pointer         : 0
================================================================================

(venv) PS C:\Users\Geoffrey\Classes\Networks\HW1>
```

python pktsniffer.py -r capture.pcap



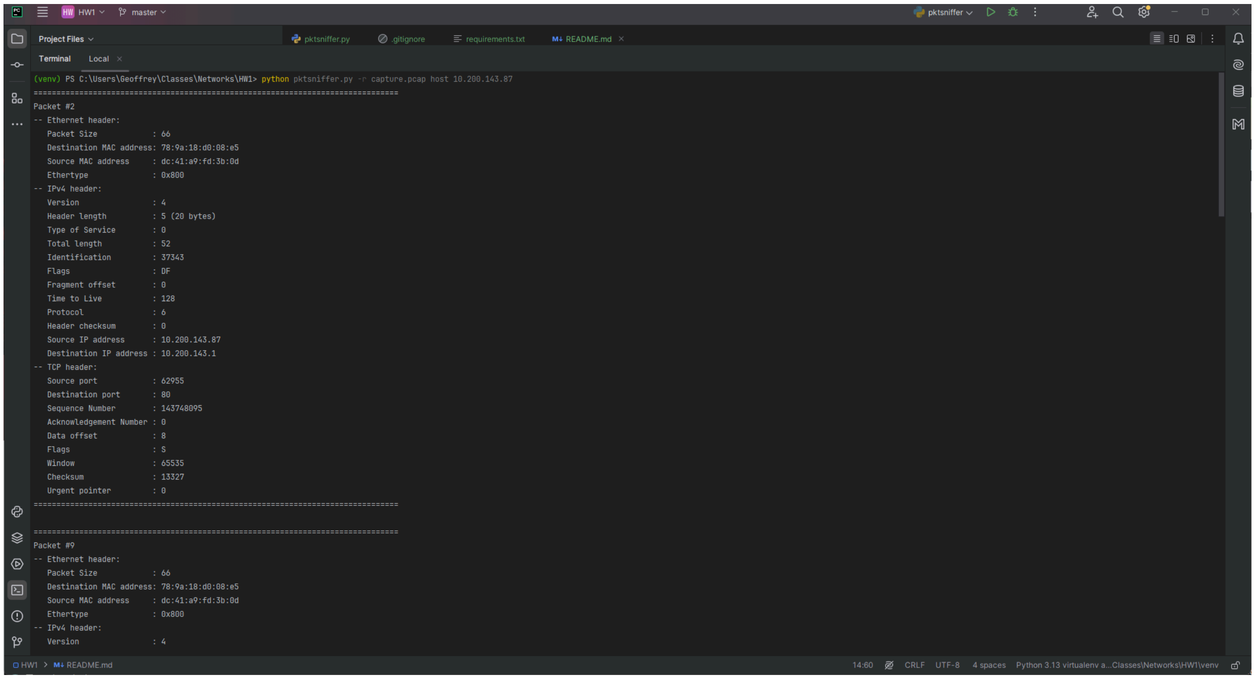
```
(venv) PS C:\Users\Geoffrey\Classes\Networks\HW1> python pktsniffer.py -r capture.pcap
================================================================================
Packet #1
-- Ethernet header:
   Packet Size            : 56
   Destination MAC address: dc:41:a9:fd:3b:0d
   Source MAC address     : 6c:29:90:47:f9:50
   Ethertype              : 0x806
================================================================================

================================================================================
Packet #2
-- Ethernet header:
   Packet Size            : 66
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
   Header length          : 5 (20 bytes)
   Type of Service        : 0
   Total length           : 52
   Identification         : 37343
   Flags                  : DF
   Fragment offset        : 0
   Time to Live           : 128
   Protocol               : 6
   Header checksum        : 0
   Source IP address      : 10.200.143.87
   Destination IP address : 10.200.143.1
-- TCP header:
   Source port            : 62955
   Destination port       : 80
   Sequence Number        : 143748095
   Acknowledgement Number : 0
   Data offset            : 8
   Flags                  : S
   Window                 : 65535
   Checksum               : 13327
   Urgent pointer         : 0
================================================================================
```

python pktsniffer.py -r capture.pcap -c 5



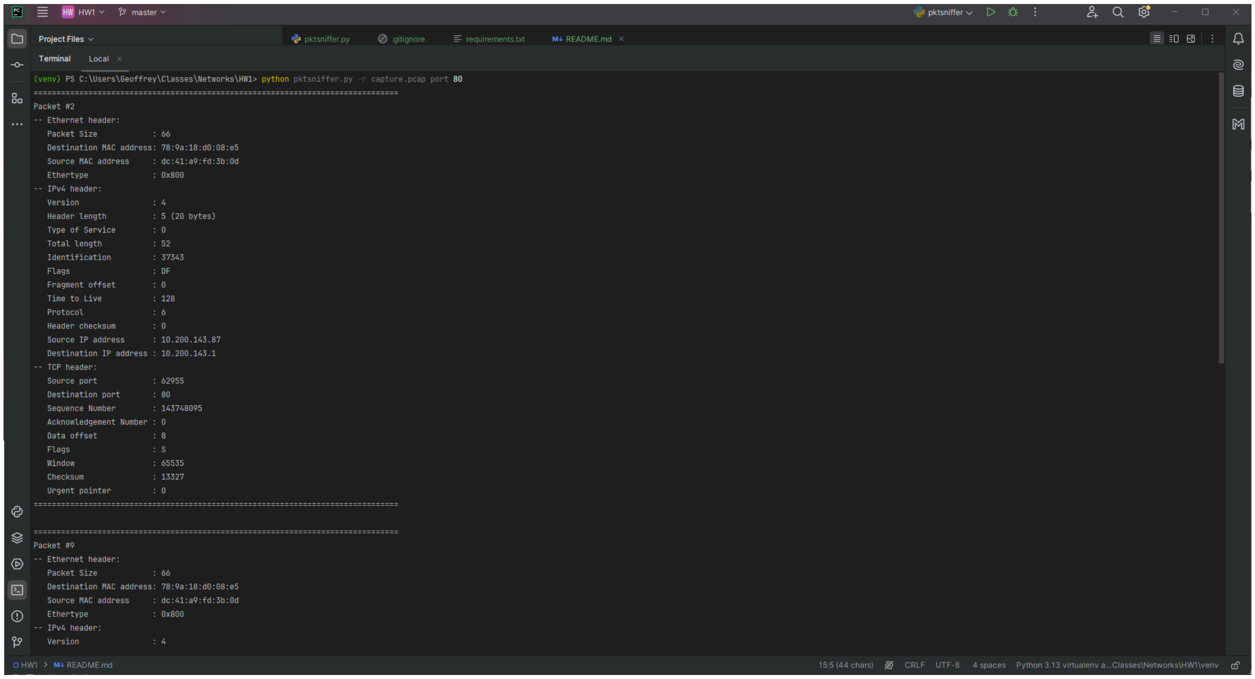
```
(venv) PS C:\Users\Geoffrey\Classes\Networks\HW1> python pktsniffer.py -r capture.pcap -c 5
================================================================================
Packet #1
-- Ethernet header:
   Packet Size            : 56
   Destination MAC address: dc:41:a9:fd:3b:0d
   Source MAC address     : 6c:29:90:47:f9:50
   Ethertype              : 0x806
================================================================================

================================================================================
Packet #2
-- Ethernet header:
   Packet Size            : 66
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
   Header length          : 5 (20 bytes)
   Type of Service        : 0
   Total length           : 52
   Identification         : 37343
   Flags                  : DF
   Fragment offset        : 0
   Time to Live           : 128
   Protocol               : 6
   Header checksum        : 0
   Source IP address      : 10.200.143.87
   Destination IP address : 10.200.143.1
-- TCP header:
   Source port            : 62955
   Destination port       : 80
   Sequence Number        : 143748095
   Acknowledgement Number : 0
   Data offset            : 8
   Flags                  : S
   Window                 : 65535
   Checksum               : 13327
   Urgent pointer         : 0
================================================================================
```

python pktsniffer.py -r capture.pcap host 10.200.143.87



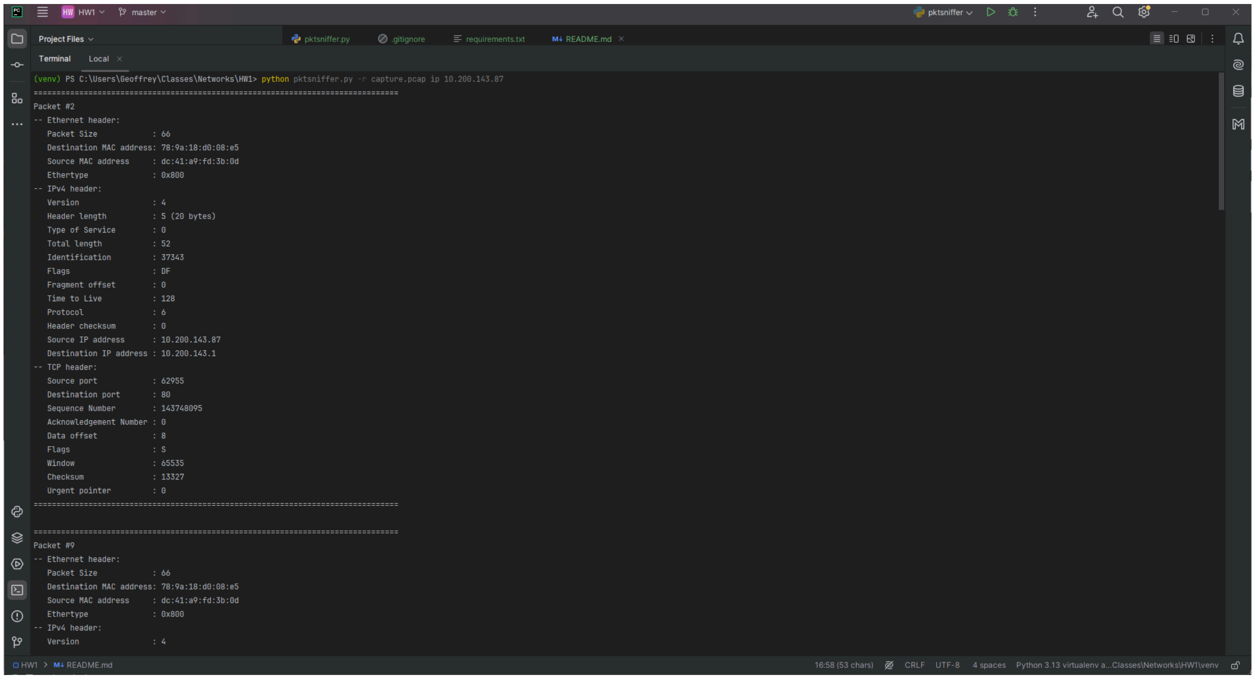
```
(venv) PS C:\Users\Geoffrey\Classes\Networks\HW1> python pktsniffer.py -r capture.pcap host 10.200.143.87
================================================================================
Packet #2
-- Ethernet header:
   Packet Size            : 66
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
   Header length          : 5 (20 bytes)
   Type of Service        : 0
   Total length           : 52
   Identification         : 37343
   Flags                  : DF
   Fragment offset        : 0
   Time to Live           : 128
   Protocol               : 6
   Header checksum        : 0
   Source IP address      : 10.200.143.87
   Destination IP address : 10.200.143.1
-- TCP header:
   Source port            : 62955
   Destination port       : 80
   Sequence Number        : 143748095
   Acknowledgement Number : 0
   Data offset            : 8
   Flags                  : S
   Window                 : 65535
   Checksum               : 13327
   Urgent pointer         : 0
================================================================================

================================================================================
Packet #9
-- Ethernet header:
   Packet Size            : 66
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
```

python pktsniffer.py -r capture.pcap port 80



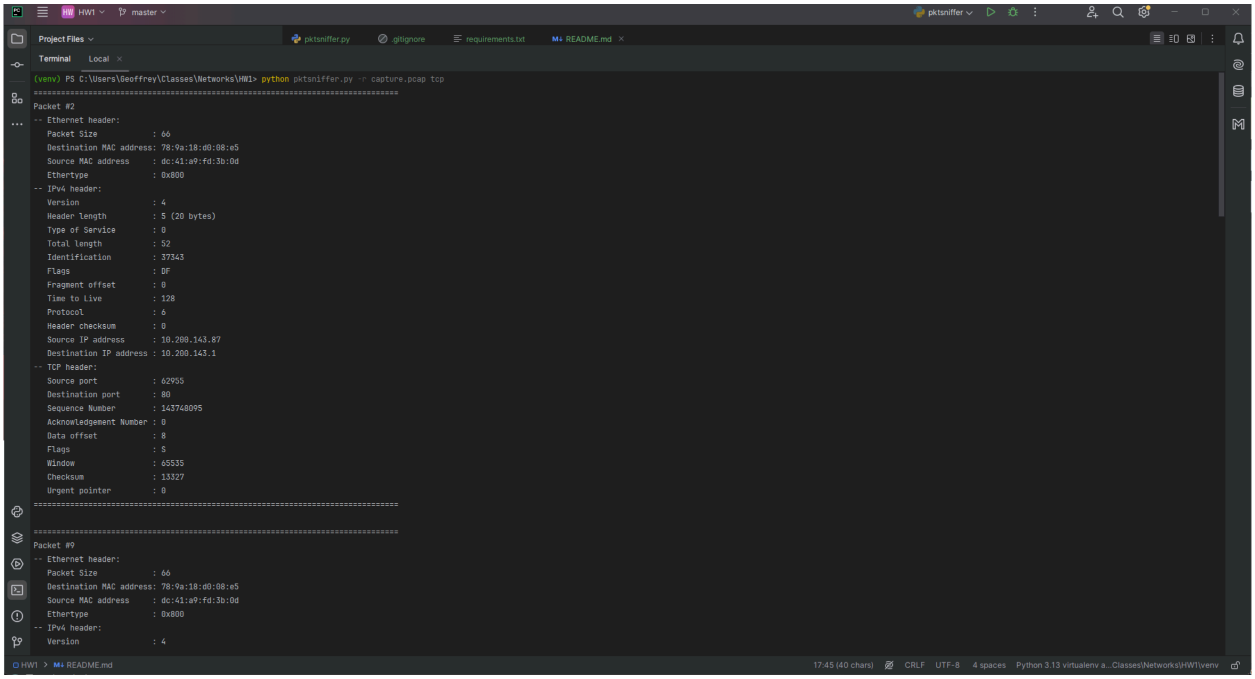
```
(venv) PS C:\Users\Geoffrey\Classes\Networks\HW1> python pktsniffer.py -r capture.pcap port 80
================================================================================
Packet #2
-- Ethernet header:
   Packet Size            : 66
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
   Header length          : 5 (20 bytes)
   Type of Service        : 0
   Total length           : 52
   Identification         : 37343
   Flags                  : DF
   Fragment offset        : 0
   Time to Live           : 128
   Protocol               : 6
   Header checksum        : 0
   Source IP address      : 10.200.143.87
   Destination IP address : 10.200.143.1
-- TCP header:
   Source port            : 62955
   Destination port       : 80
   Sequence Number        : 143748095
   Acknowledgement Number : 0
   Data offset            : 8
   Flags                  : S
   Window                 : 65535
   Checksum               : 13327
   Urgent pointer         : 0
================================================================================

================================================================================
Packet #9
-- Ethernet header:
   Packet Size            : 66
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
```

python pktsniffer.py -r capture.pcap ip 10.200.143.87



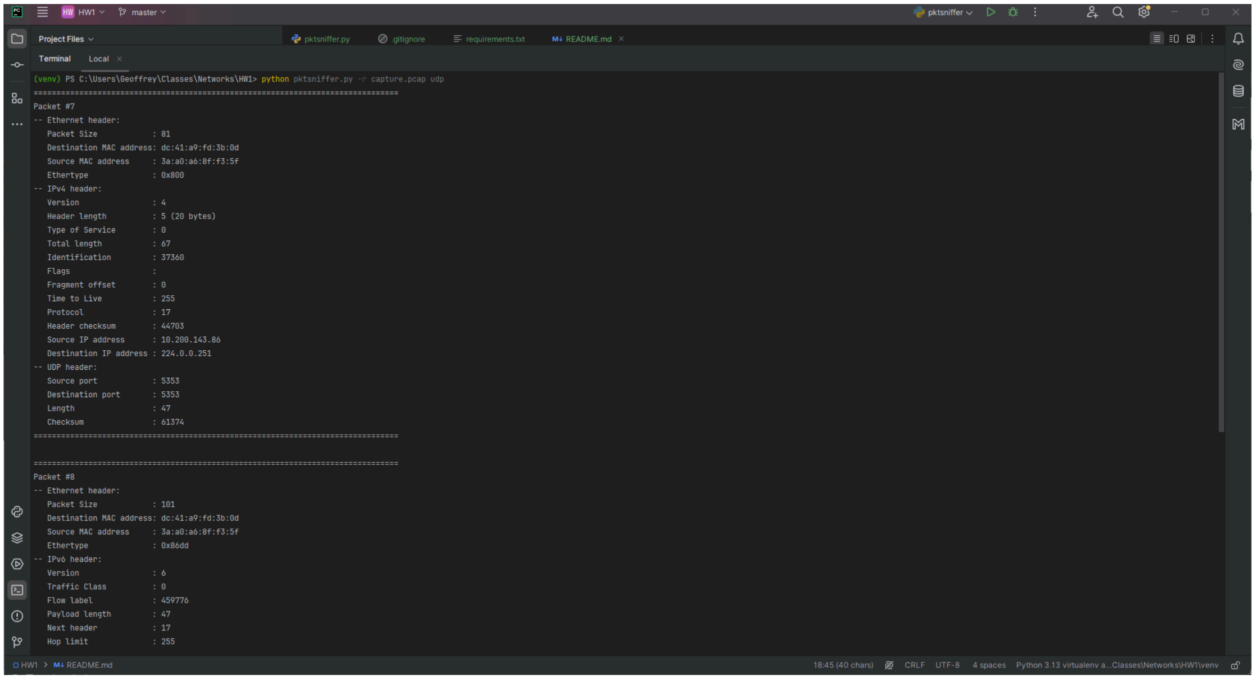
```
(venv) PS C:\Users\Geoffrey\Classes\Networks\HW1> python pktsniffer.py -r capture.pcap ip 10.200.143.87
================================================================================
Packet #2
-- Ethernet header:
   Packet Size           : 66
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
   Header length          : 5 (20 bytes)
   Type of Service        : 0
   Total length           : 52
   Identification         : 37343
   Flags                  : DF
   Fragment offset        : 0
   Time to Live           : 128
   Protocol               : 6
   Header checksum        : 0
   Source IP address      : 10.200.143.87
   Destination IP address : 10.200.143.1
-- TCP header:
   Source port            : 62955
   Destination port       : 80
   Sequence Number        : 143748095
   Acknowledgement Number : 0
   Data offset            : 8
   Flags                  : S
   Window                 : 65535
   Checksum               : 13327
   Urgent pointer         : 0
================================================================================

================================================================================
Packet #9
-- Ethernet header:
   Packet Size            : 66
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
```

python pktsniffer.py -r capture.pcap tcp



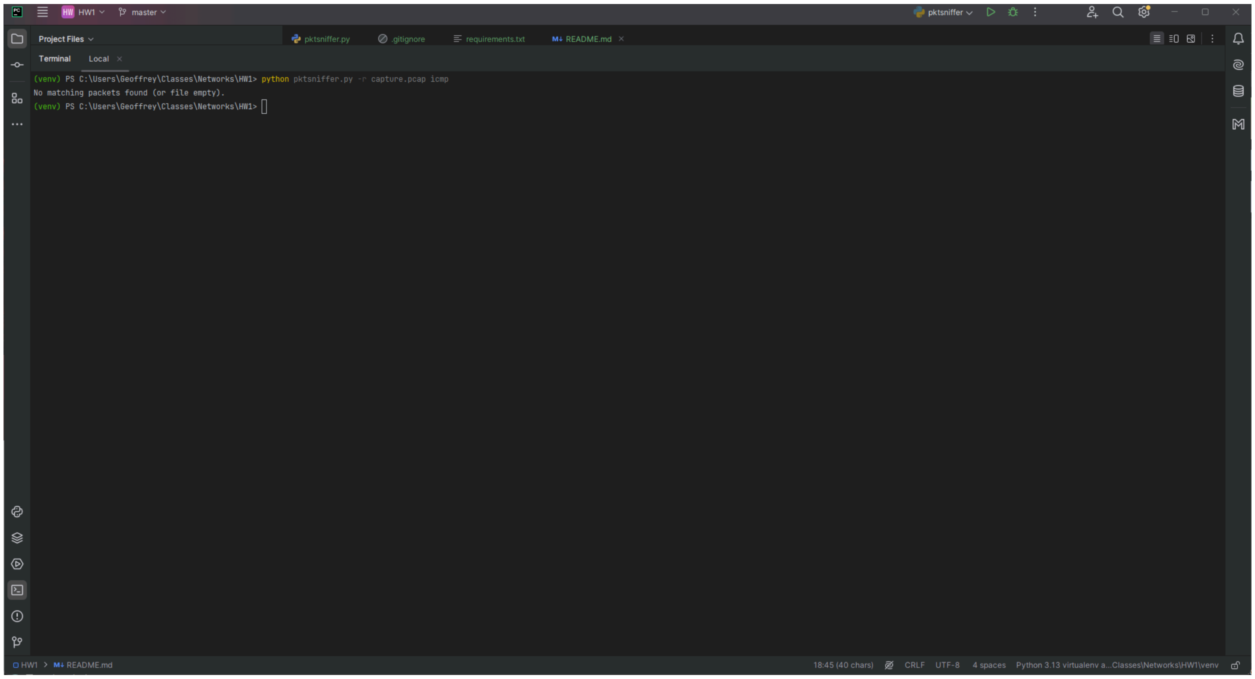
```
(venv) PS C:\Users\Geoffrey\Classes\Networks\HW1> python pktsniffer.py -r capture.pcap tcp
================================================================================
Packet #2
-- Ethernet header:
   Packet Size            : 66
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
   Header length          : 5 (20 bytes)
   Type of Service        : 0
   Total length           : 52
   Identification         : 37343
   Flags                  : DF
   Fragment offset        : 0
   Time to Live           : 128
   Protocol               : 6
   Header checksum        : 0
   Source IP address      : 10.200.143.87
   Destination IP address : 10.200.143.1
-- TCP header:
   Source port            : 62955
   Destination port       : 80
   Sequence Number        : 143748095
   Acknowledgement Number : 0
   Data offset            : 8
   Flags                  : S
   Window                 : 65535
   Checksum               : 13327
   Urgent pointer         : 0
================================================================================

================================================================================
Packet #9
-- Ethernet header:
   Packet Size            : 66
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
```

python pktsniffer.py -r capture.pcap udp



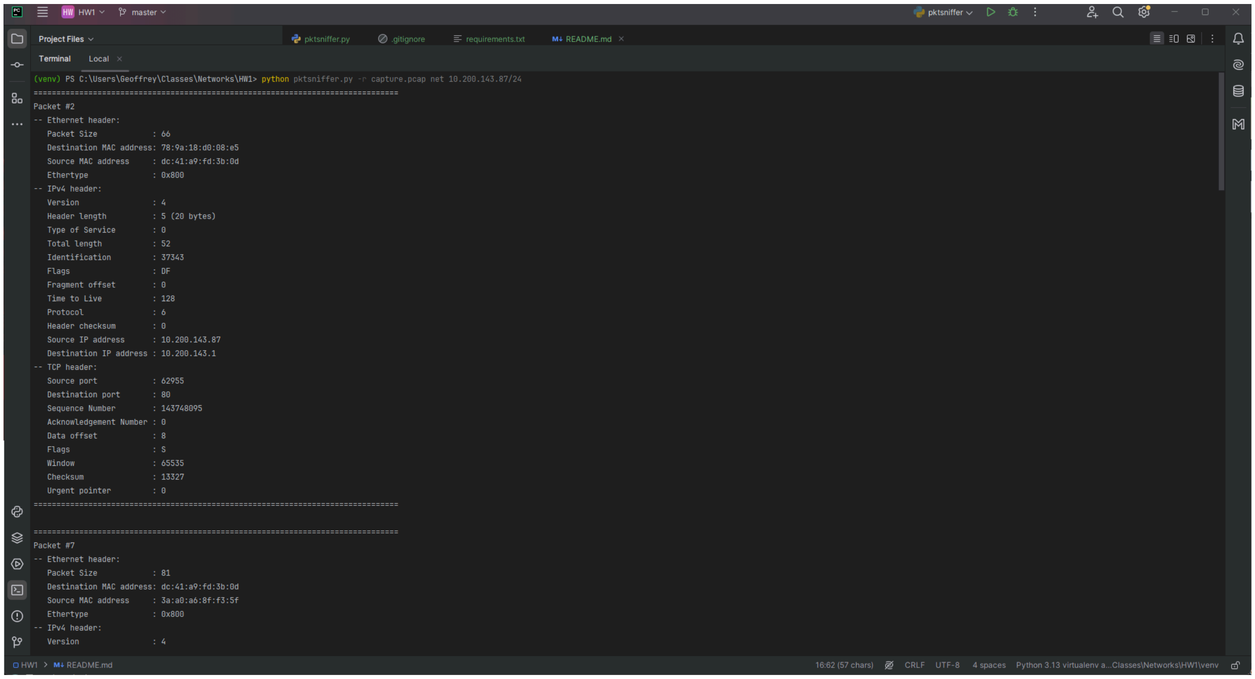
```
(venv) PS C:\Users\Geoffrey\Classes\Networks\HW1> python pktsniffer.py -r capture.pcap udp
================================================================================
Packet #7
-- Ethernet header:
   Packet Size            : 81
   Destination MAC address: dc:41:a9:fd:3b:0d
   Source MAC address     : 3a:a0:a6:8f:f3:5f
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
   Header length          : 5 (20 bytes)
   Type of Service        : 0
   Total length           : 67
   Identification         : 37360
   Flags                  :
   Fragment offset        : 0
   Time to Live           : 255
   Protocol               : 17
   Header checksum        : 44703
   Source IP address      : 10.200.143.86
   Destination IP address : 224.0.0.251
-- UDP header:
   Source port            : 5353
   Destination port       : 5353
   Length                 : 47
   Checksum               : 61374
================================================================================

================================================================================
Packet #8
-- Ethernet header:
   Packet Size            : 101
   Destination MAC address: dc:41:a9:fd:3b:0d
   Source MAC address     : 3a:a0:a6:8f:f3:5f
   Ethertype              : 0x86dd
-- IPv6 header:
   Version                : 6
   Traffic Class          : 0
   Flow label             : 459776
   Payload length         : 47
   Next header            : 17
   Hop limit              : 255
```

python pktsniffer.py -r capture.pcap icmp



```
(venv) PS C:\Users\Geoffrey\Classes\Networks\HW1> python pktsniffer.py -r capture.pcap icmp
No matching packets found (or file empty).
(venv) PS C:\Users\Geoffrey\Classes\Networks\HW1>
```

python pktsniffer.py -r capture.pcap net 10.200.143.87/24



```
(venv) PS C:\Users\Geoffrey\Classes\Networks\HW1> python pktsniffer.py -r capture.pcap net 10.200.143.87/24
==================================================================================
Packet #2
-- Ethernet header:
   Packet Size            : 66
   Destination MAC address: 78:9a:18:d0:08:e5
   Source MAC address     : dc:41:a9:fd:3b:0d
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
   Header length          : 5 (20 bytes)
   Type of Service        : 0
   Total length           : 52
   Identification         : 37343
   Flags                  : DF
   Fragment offset        : 0
   Time to Live           : 128
   Protocol               : 6
   Header checksum        : 0
   Source IP address      : 10.200.143.87
   Destination IP address : 10.200.143.1
-- TCP header:
   Source port            : 62955
   Destination port       : 80
   Sequence Number        : 143748095
   Acknowledgement Number : 0
   Data offset            : 8
   Flags                  : S
   Window                 : 65535
   Checksum               : 13327
   Urgent pointer         : 0
==================================================================================

==================================================================================
Packet #7
-- Ethernet header:
   Packet Size            : 81
   Destination MAC address: dc:41:a9:fd:3b:0d
   Source MAC address     : 3a:a0:a6:8f:f3:5f
   Ethertype              : 0x800
-- IPv4 header:
   Version                : 4
```