

COMP 7003

Assignment 2

Testing

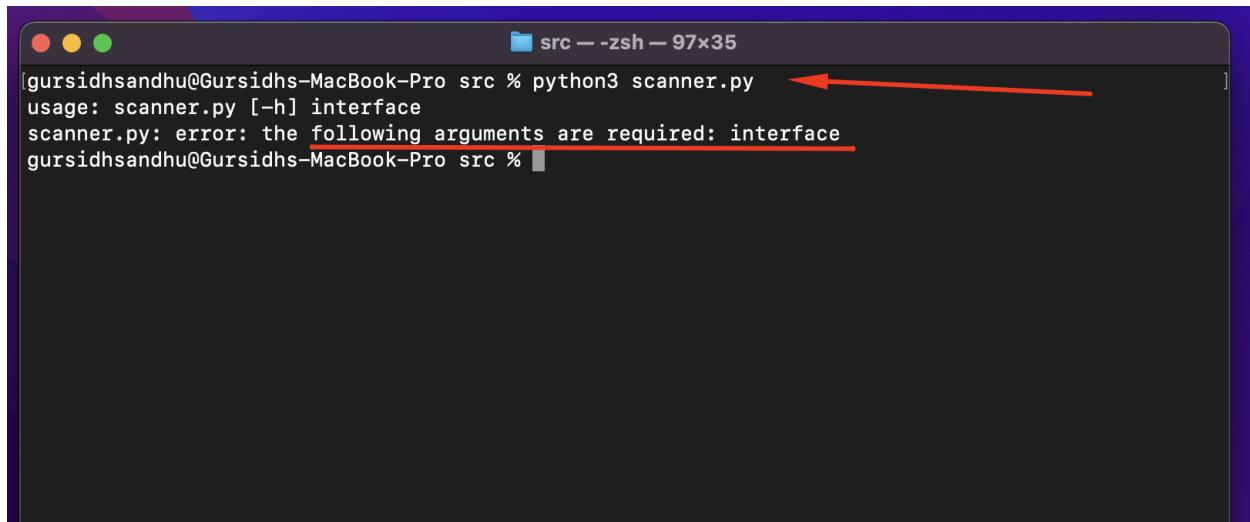
Gursidh Sandhu
A01319563
Oct 4,2024

Tests	4
Test 1	4
Test 2	5
Test 3	5
Test 4	6
Test 5	7
Test 6	7
Test 7	8
Test 8	8
Test 9	9
Test 10	10
Test 11	10
Test 12	11
Test 13	12
Test 14	12
Test 15	13

Test	Expected	Actual	Screenshot
No arguments	fail	fail	Test 1
More than one argument	fail	fail	Test 2
Invalid interface string provided	fail	fail	Test 3
Interface argument provided, but not a string	fail	fail	Test 4
Interface argument provided, but empty string	pass	pass	Test 5
Interface argument provided, but contains special characters	fail	fail	Test 6
Run multiple instances of program in different terminals using same interface	pass	pass	Test 7
Run multiple instances of program in different terminals using different network interface	pass	pass	Test 8
Command+C to skip current packet capture and move on to next packet capture	pass	pass	Test 9
Command+C to exit program	pass	pass	Test 10
Run one instance of program, start a new instance and shut down the first instance while second is running	pass	pass	Test 11
Run program on a network interface that currently has no traffic	pass	pass	Test 12
Run program on valid interface, but shut down connection to network after connecting	fail	fail	Test 13
Run program on valid interface without being connected to a network	fail	fail	Test 14
Run program while not being connected to network, then connect to network while it's being run	pass	pass	Test 15

Tests

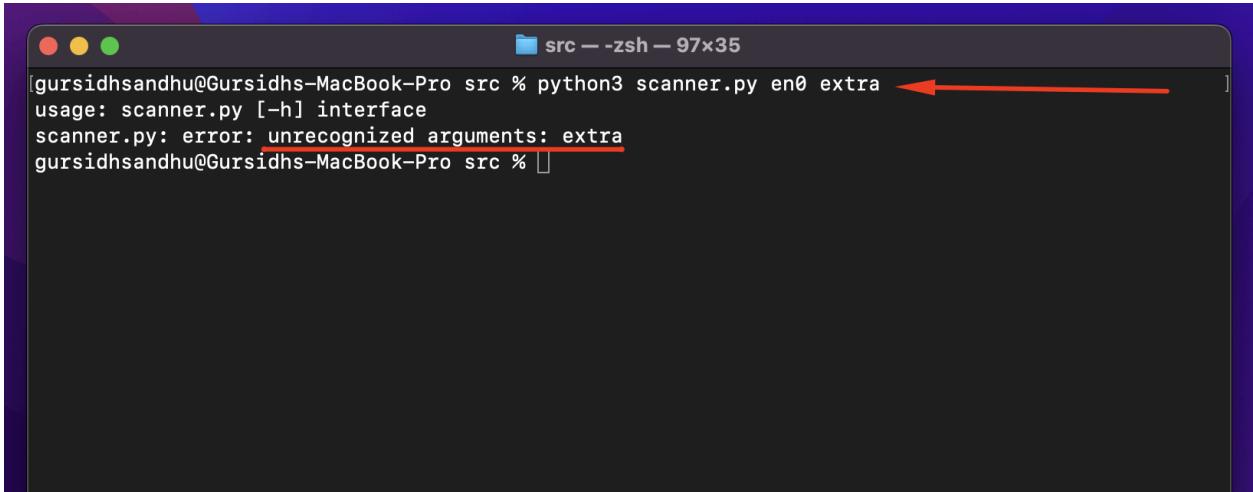
Test 1



A screenshot of a macOS terminal window titled "src — -zsh — 97x35". The window shows the command "python3 scanner.py" being run, followed by an error message: "usage: scanner.py [-h] interface" and "scanner.py: error: the following arguments are required: interface". A red arrow points to the word "interface" in the error message.

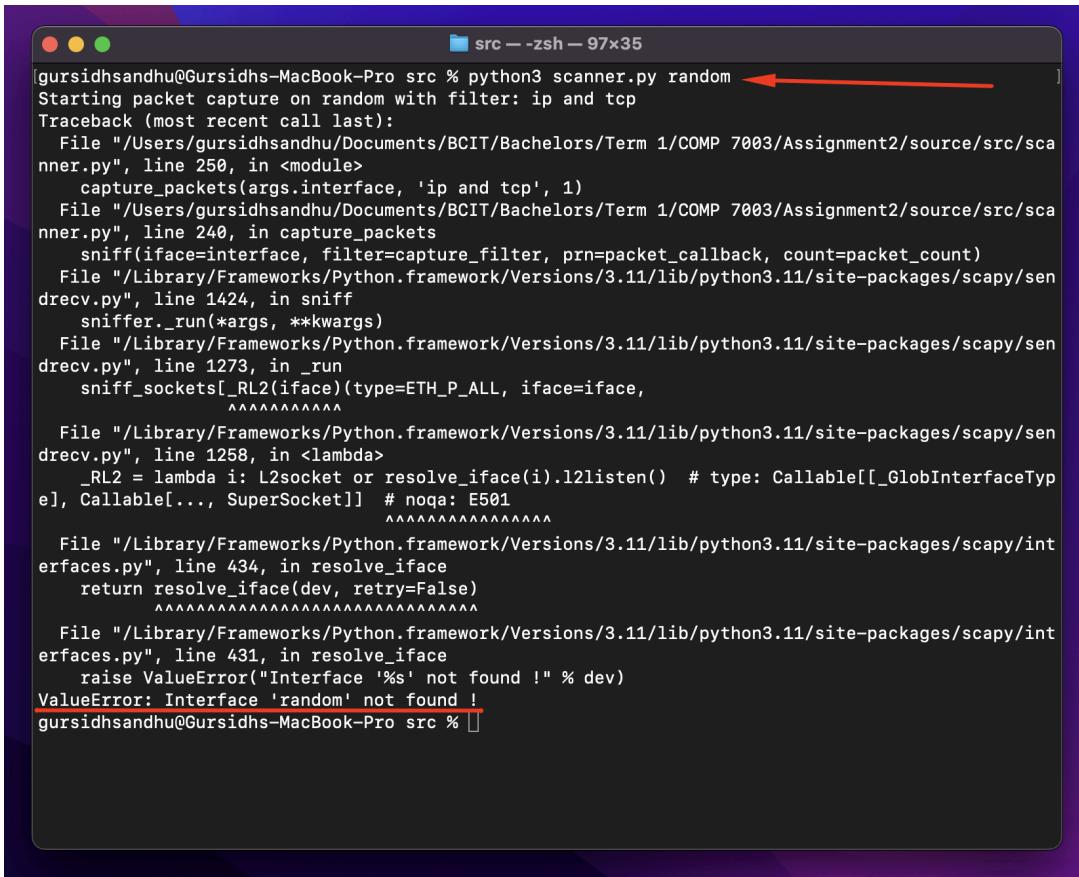
```
gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py
usage: scanner.py [-h] interface
scanner.py: error: the following arguments are required: interface
gursidhsandhu@Gursidhs-MacBook-Pro src %
```

Test 2



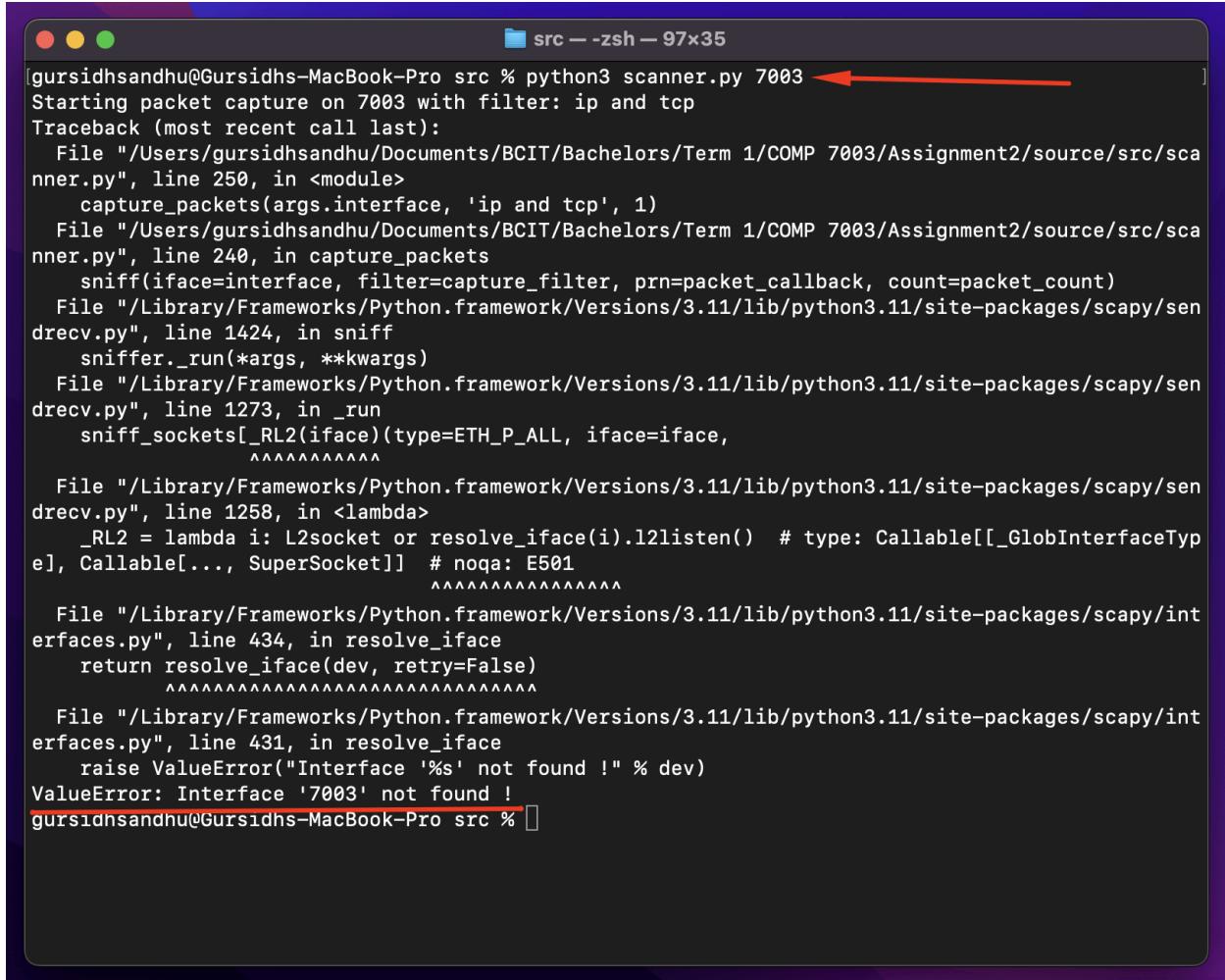
```
[gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py en0 extra
usage: scanner.py [-h] interface
scanner.py: error: unrecognized arguments: extra
gursidhsandhu@Gursidhs-MacBook-Pro src % ]
```

Test 3



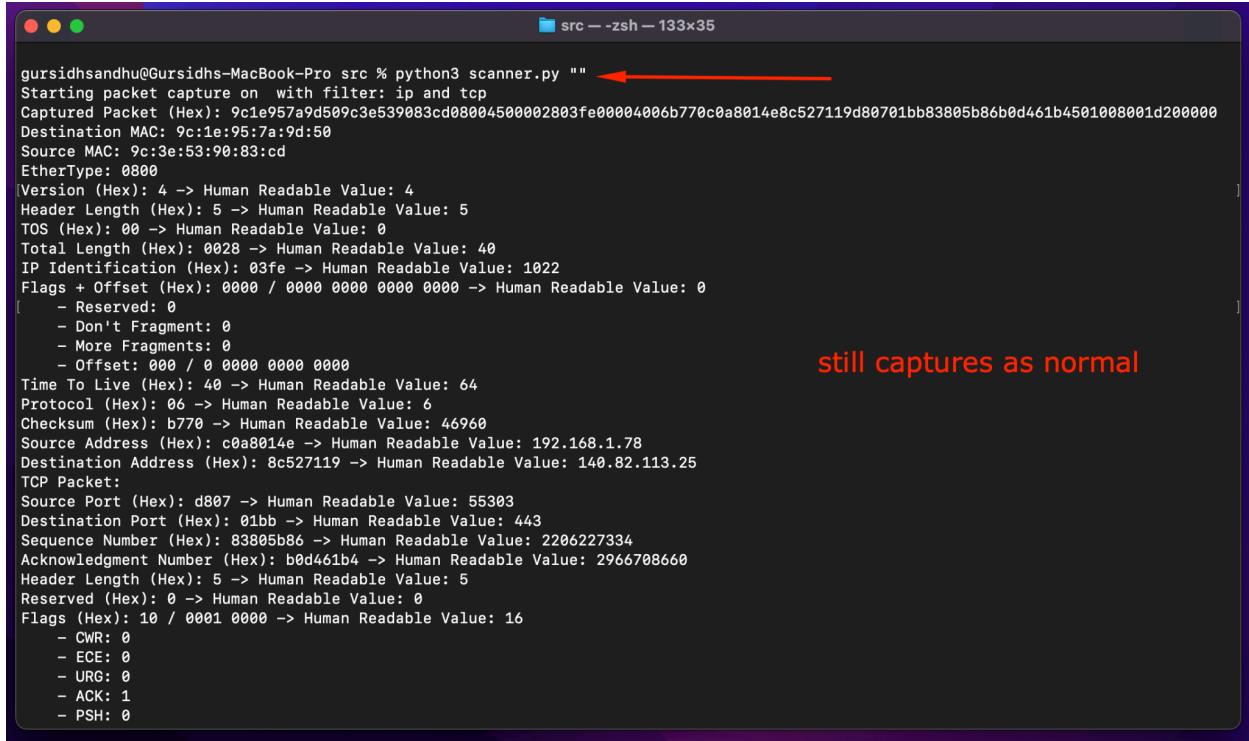
```
[gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py random
Starting packet capture on random with filter: ip and tcp
Traceback (most recent call last):
  File "/Users/gursidhsandhu/Documents/BCIT/Bachelors/Term 1/COMP 7003/Assignment2/source/src/scanner.py", line 250, in <module>
    capture_packets(args.interface, 'ip and tcp', 1)
  File "/Users/gursidhsandhu/Documents/BCIT/Bachelors/Term 1/COMP 7003/Assignment2/source/src/scanner.py", line 240, in capture_packets
    sniff(iface=args.interface, filter=capture_filter, prn=packet_callback, count=packet_count)
  File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/sendrecv.py", line 1424, in sniff
    sniffer._run(*args, **kwargs)
  File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/sendrecv.py", line 1273, in _run
    sniff_packets[_RL2(iface)](type=ETH_P_ALL, iface=iface,
                                ^^^^^^^^^^
  File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/sendrecv.py", line 1258, in <lambda>
    _RL2 = lambda i: L2socket or resolve_iface(i).l2listen() # type: Callable[[_GlobInterfaceType], Callable[..., SuperSocket]] # noqa: E501
                                ^^^^^^^^^^
  File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/intefaces.py", line 434, in resolve_iface
    return resolve_iface(dev, retry=False)
                                ^^^^^^^^^^
  File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/intefaces.py", line 431, in resolve_iface
    raise ValueError("Interface '%s' not found !" % dev)
ValueError: Interface 'random' not found !
gursidhsandhu@Gursidhs-MacBook-Pro src % ]
```

Test 4



```
gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py 7003 ←
Starting packet capture on 7003 with filter: ip and tcp
Traceback (most recent call last):
  File "/Users/gursidhsandhu/Documents/BCIT/Bachelors/Term 1/COMP 7003/Assignment2/source/src/scanner.py", line 250, in <module>
    capture_packets(args.interface, 'ip and tcp', 1)
  File "/Users/gursidhsandhu/Documents/BCIT/Bachelors/Term 1/COMP 7003/Assignment2/source/src/scanner.py", line 240, in capture_packets
    sniff(iface=interface, filter=capture_filter, prn=packet_callback, count=packet_count)
  File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/sendrecv.py", line 1424, in sniff
    sniffer._run(*args, **kwargs)
  File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/sendrecv.py", line 1273, in _run
    sniff_sockets[_RL2(iface)](type=ETH_P_ALL, iface=iface,
                                ^^^^^^^^^^
  File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/sendrecv.py", line 1258, in <lambda>
    _RL2 = lambda i: L2socket or resolve_iface(i).l2listen() # type: Callable[[_GlobInterfaceType], Callable[..., SuperSocket]] # noqa: E501
                                ^^^^^^^^^^^^^^
  File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/interfaces.py", line 434, in resolve_iface
    return resolve_iface(dev, retry=False)
                                ^^^^^^^^^^
  File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/interfaces.py", line 431, in resolve_iface
    raise ValueError("Interface '%s' not found !" % dev)
ValueError: Interface '7003' not found !
gursidhsandhu@Gursidhs-MacBook-Pro src %
```

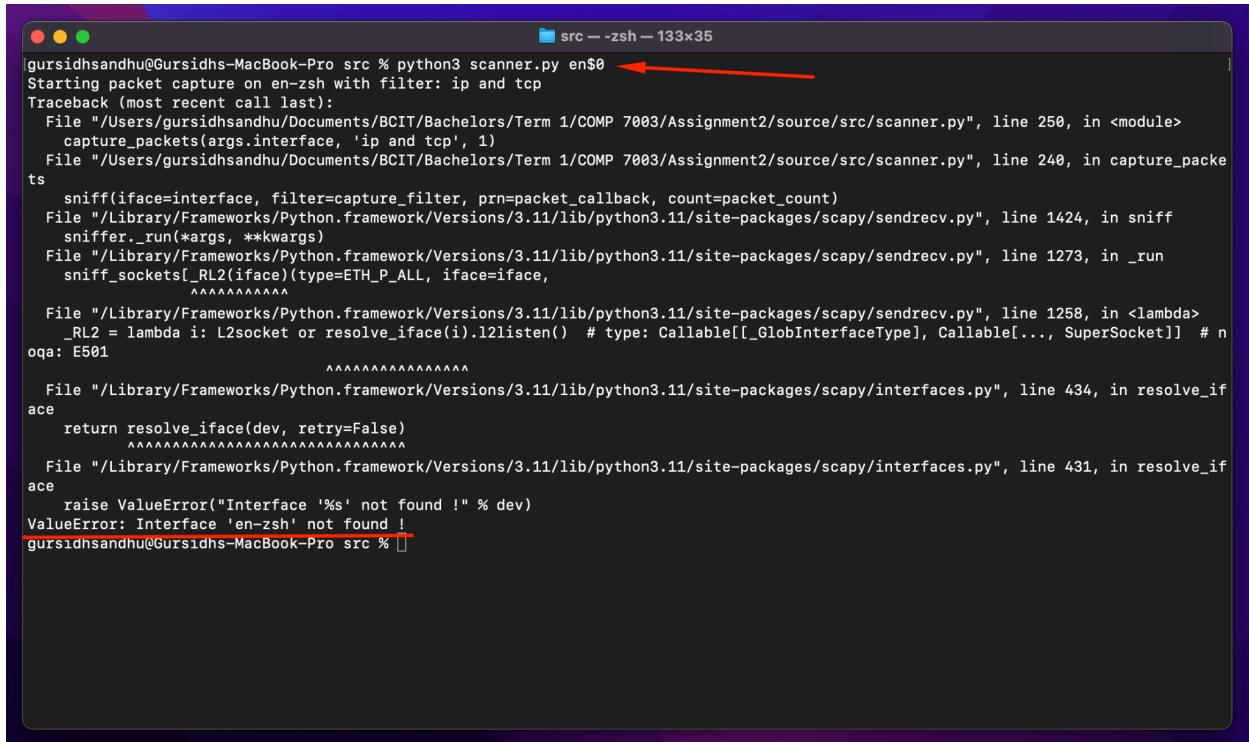
Test 5



gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py ""
Starting packet capture on with filter: ip and tcp
Captured Packet (Hex): 9c1e957a9d509c3e539083cd08004500002803fe00004006b770c0a8014e8c527119d80701bb83805b86b0d461b4501008001d200000
Destination MAC: 9c:1e:95:7a:9d:50
Source MAC: 9c:3e:53:90:83:cd
EtherType: 0800
Version (Hex): 4 -> Human Readable Value: 4
Header Length (Hex): 5 -> Human Readable Value: 5
TOS (Hex): 00 -> Human Readable Value: 0
Total Length (Hex): 0028 -> Human Readable Value: 40
IP Identification (Hex): 03fe -> Human Readable Value: 1022
Flags + Offset (Hex): 0000 / 0000 0000 0000 0000 -> Human Readable Value: 0
| - Reserved: 0
| - Don't Fragment: 0
| - More Fragments: 0
| - Offset: 000 / 0 0000 0000 0000
Time To Live (Hex): 40 -> Human Readable Value: 64
Protocol (Hex): 06 -> Human Readable Value: 6
Checksum (Hex): b770 -> Human Readable Value: 46960
Source Address (Hex): c0a8014e -> Human Readable Value: 192.168.1.78
Destination Address (Hex): 8c527119 -> Human Readable Value: 140.82.113.25
TCP Packet:
Source Port (Hex): d807 -> Human Readable Value: 55303
Destination Port (Hex): 01bb -> Human Readable Value: 443
Sequence Number (Hex): 83805b86 -> Human Readable Value: 2206227334
Acknowledgment Number (Hex): b0d461b4 -> Human Readable Value: 2966708660
Header Length (Hex): 5 -> Human Readable Value: 5
Reserved (Hex): 0 -> Human Readable Value: 0
Flags (Hex): 10 / 0001 0000 -> Human Readable Value: 16
| - CWR: 0
| - ECE: 0
| - URG: 0
| - ACK: 1
| - PSH: 0

still captures as normal

Test 6



gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py en\$0
Starting packet capture on en-zsh with filter: ip and tcp
Traceback (most recent call last):
 File "/Users/gursidhsandhu/Documents/BCIT/Bachelors/Term 1/COMP 7003/Assignment2/source/src/scanner.py", line 250, in <module>
 capture_packets(args.interface, 'ip and tcp', 1)
 File "/Users/gursidhsandhu/Documents/BCIT/Bachelors/Term 1/COMP 7003/Assignment2/source/src/scanner.py", line 240, in capture_packets
 sniff(iface=interface, filter=capture_filter, prn=packet_callback, count=packet_count)
 File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/sendrecv.py", line 1424, in sniff
 sniffer._run(*args, **kwargs)
 File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/sendrecv.py", line 1273, in _run
 sniff_sockets[_RL2(iface)](type=ETH_P_ALL, iface=iface,
 ^^^^^^^^^^
 File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/sendrecv.py", line 1258, in <lambda>
 _RL2 = lambda i: L2socket or resolve_iface(i).l2listen() # type: Callable[[_GlobInterfaceType], Callable[..., SuperSocket]] # noqa: E501
 ^^^^^^^^^^
 File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/interfaces.py", line 434, in resolve_iface
 return resolve_iface(dev, retry=False)
 ^^^^^^
 File "/Library/Frameworks/Python.framework/Versions/3.11/lib/python3.11/site-packages/scapy/interfaces.py", line 431, in resolve_iface
 raise ValueError("Interface '%s' not found !" % dev)
ValueError: Interface 'en-zsh' not found!
gursidhsandhu@Gursidhs-MacBook-Pro src %

Test 7

The image shows two terminal windows side-by-side. Both windows have a red arrow pointing to the command line at the top, which reads: `[src -- zsh - 83x23] gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py en0`. Below the command, both windows display identical captured packet details. A red box highlights the first few lines of the output:

```
Captured Packet (Hex): 9c1e957a9d509c3e539083cd080045000028375b00004006955fc0a8014e  
2275c9aa81301bb1e6f65af97cbf4c501008000db90000
```

Both windows also show the same detailed packet analysis below the hex dump.

both instances capture same packet

Test 8

The image shows two terminal windows side-by-side. The left window has a red arrow pointing to the command line at the top, which reads: `[src -- zsh - 83x23] gursidhsandhu@Gursidhs-MacBook-Pro src % clear`. Below it, another red arrow points to the command line: `[src -- zsh - 83x23] gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py en0`. A red box highlights the first few lines of the output:

```
Captured Packet (Hex): 9c1e957a9d509c3e539083cd080045000028a8ec0000400623cec0a8014e  
2275c9aa81301bb1e6f672d97cbf76b581008000b1c0000
```

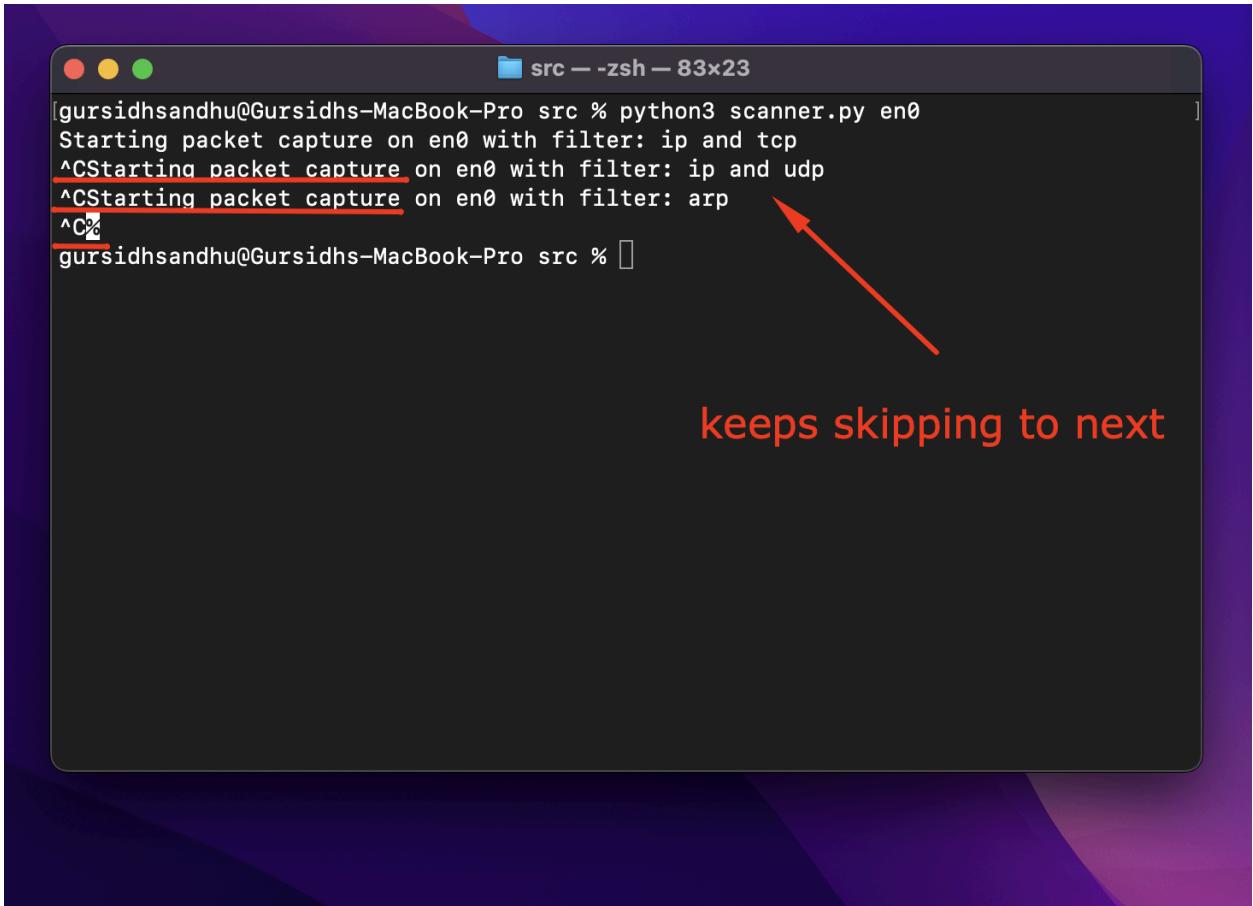
A red arrow points from the right side of the left window to the right side of the right window, with the text "gets packet" written above it.

The right window has a red arrow pointing to the command line at the top, which reads: `[src -- Python scanner.py en1 - 80x24] gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py en1`. Below it, a red box highlights the first few lines of the output:

```
Starting packet capture on en1 with filter: ip and tcp
```

A red arrow points from the right side of the left window to the right side of the right window, with the text "still waits here" written above it.

Test 9



A screenshot of a macOS terminal window titled "src — -zsh — 83x23". The window shows the command "python3 scanner.py en0" being run. The output indicates that the script is attempting to start packet capture on interface "en0" with filters for IP/TCP, UDP, and ARP. However, it is stuck in a loop, with each attempt being terminated by a Ctrl-C interrupt (indicated by the '^C' prefix). A red arrow points from the text "keeps skipping to next" to the final '^C%' entry in the log.

```
[gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py en0
Starting packet capture on en0 with filter: ip and tcp
^CStarting packet capture on en0 with filter: ip and udp
^CStarting packet capture on en0 with filter: arp
^C%
gursidhsandhu@Gursidhs-MacBook-Pro src % ]
```

keeps skipping to next

Test 10

```
[gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py en0
Starting packet capture on en0 with filter: ip and tcp
^CStarting packet capture on en0 with filter: ip and udp
^CStarting packet capture on en0 with filter: arp
^C%]
```

The terminal window shows the command `python3 scanner.py en0` running. It captures three types of packets: IP and TCP, IP and UDP, and ARP. The user then presses `^C` (Control-C) to stop the capture. A red arrow points from the `^C` character in the command line to the text "last one ends program". Another red arrow points from the command line to the text "no more capture calls are left".

last one ends program

no more capture calls
are left

Test 11

```
Version (Hex): 4 -> Human Readable Value: 4
Header Length (Hex): 5 -> Human Readable Value: 5
TOS (Hex): 00 -> Human Readable Value: 0
Total Length (Hex): 0044 -> Human Readable Value: 68
IP Identification (Hex): b67c -> Human Readable Value: 46716
Flags + Offset (Hex): 0000 / 0000 0000 0000 0000 -> Human Readable Value: 0
- Reserved: 0
- Don't Fragment: 0
- More Fragments: 0
- Offset: 000 / 0 0000 0000 0000
Time To Live (Hex): 40 -> Human Readable Value: 64
Protocol (Hex): 11 -> Human Readable Value: 17
Checksum (Hex): 3f90 -> Human Readable Value: 16272
Source Address (Hex): c0a8014e -> Human Readable Value: 192.168.1.78
Destination Address (Hex): c0a801fe -> Human Readable Value: 192.168.1.254
UDP Packet:
Source Port (Hex): e686 -> Human Readable Value: 59014
Destination Port (Hex): 0035 -> Human Readable Value: 53
Length (Hex): 0030 -> Human Readable Value: 48
Checksum (Hex): ec6d -> Human Readable Value: 60525
Starting packet capture on en0 with filter: arp
^C%
```

The first terminal window (left) shows the configuration of the scanner with various filters (ip and tcp, ip and udp, arp) and then stops with a `^C` interrupt. A red arrow points from the `^C` character to the text "skips arp capture".

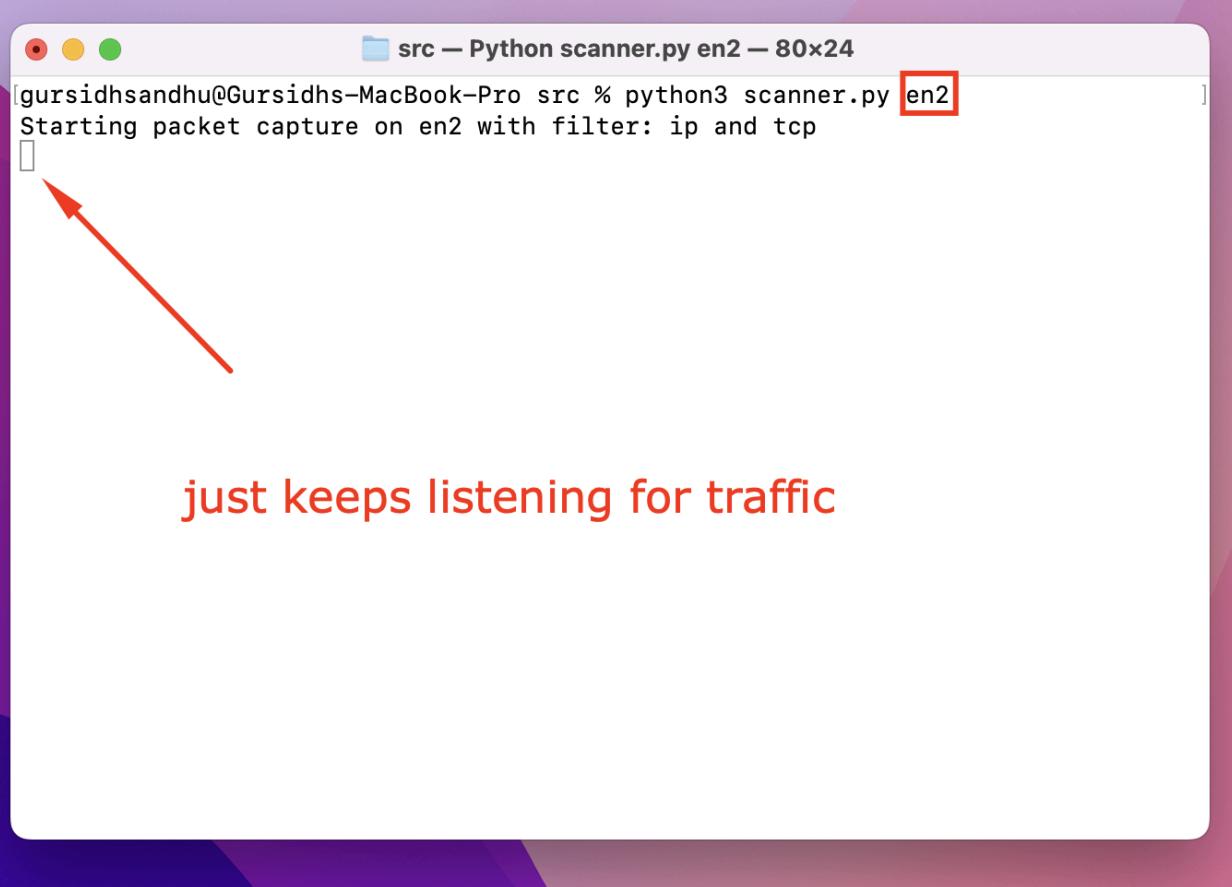
```
Destination Address (Hex): c0a801fe -> Human Readable Value: 192.168.1.254
Source Port (Hex): e686 -> Human Readable Value: 59014
Destination Port (Hex): 0035 -> Human Readable Value: 53
Length (Hex): 0030 -> Human Readable Value: 48
Checksum (Hex): ec6d -> Human Readable Value: 60525
Starting packet capture on en0 with filter: arp
Captured Packet (Hex): 3a12b8ea591f9c3e539083cd080060010800060400019c3e539083cdc0a8014e3a12b8ea591fc0a80157
Destination MAC: 3a:12:b8:ea:59:1f
Source MAC: 9c:3e:53:90:83:cd
EtherType: 0806
Hardware Address Type (Hex): 0001 -> Human Readable Value: 1
Protocol Address Type (Hex): 0800 -> Human Readable Value: 2048
Hardware Address Length (Hex): 06 -> Human Readable Value: 6
Protocol Address Length (Hex): 04 -> Human Readable Value: 4
Opcode (Hex): 0001 -> Human Readable Value: 1
Source Hardware Address (Hex): 9c:3e:53:90:83:cd -> Human Readable Value: 9c:3e:53:90:83:cd
Source Protocol Address (Hex): c0a8014e -> Human Readable Value: 192.168.1.78
Target Hardware Address (Hex): 3a12b8ea591f -> Human Readable Value: 3a:12:b8:ea:59:1f
Target Protocol Address (Hex): c0a80157 -> Human Readable Value: 192.168.1.87
gursidhsandhu@Gursidhs-MacBook-Pro src %
```

The second terminal window (right) shows the scanner capturing a single UDP packet (highlighted by a red box) and then continuing to capture ARP packets (also highlighted by a red box). A red arrow points from the text "this instance still captures arp" to the second window.

skips arp capture

this instance still captures arp

Test 12

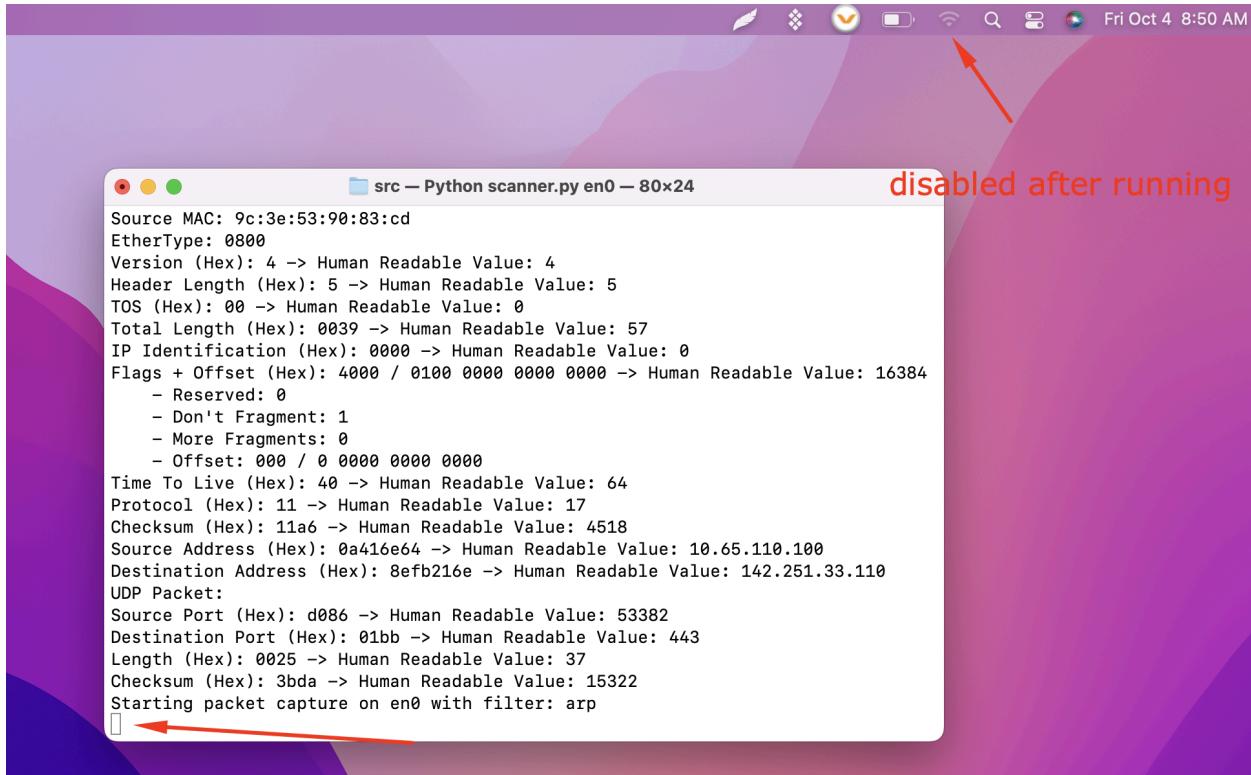


A screenshot of a terminal window titled "src — Python scanner.py en2 — 80x24". The window shows the command "python3 scanner.py en2" being run. A red arrow points from the text "just keeps listening for traffic" down towards the terminal window. The terminal output includes the message "Starting packet capture on en2 with filter: ip and tcp".

```
[gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py en2
Starting packet capture on en2 with filter: ip and tcp]
```

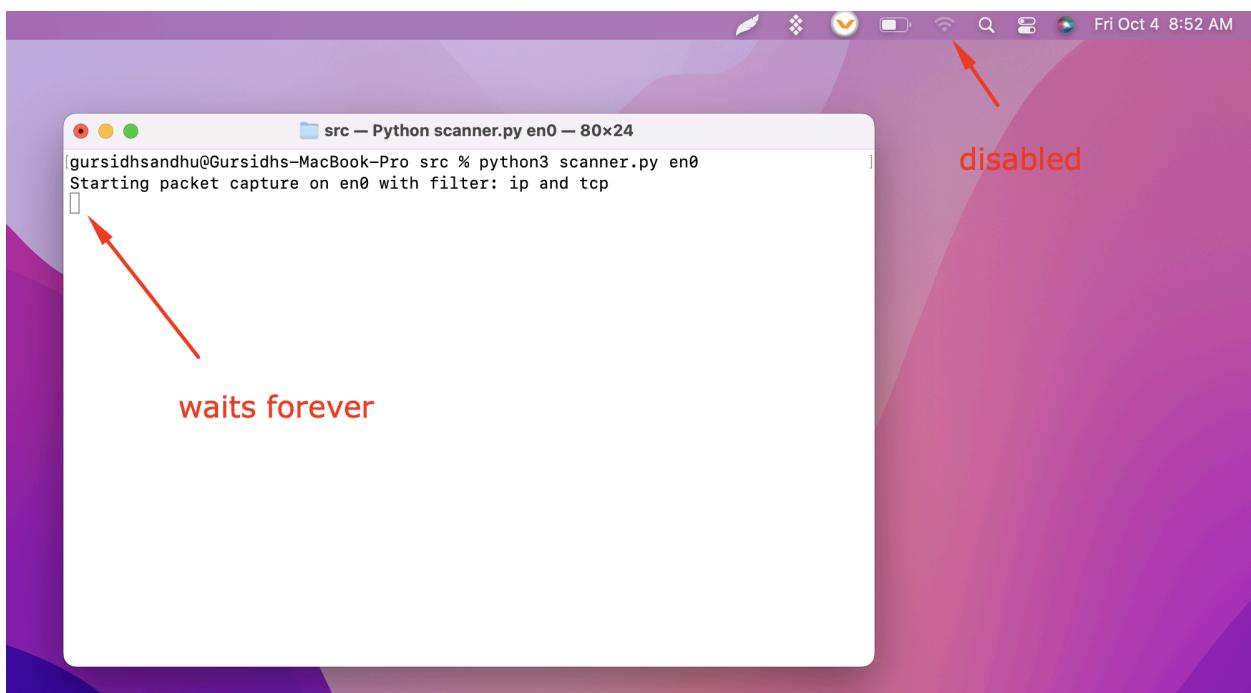
just keeps listening for traffic

Test 13



```
Source MAC: 9c:3e:53:90:83:cd
EtherType: 0800
Version (Hex): 4 -> Human Readable Value: 4
Header Length (Hex): 5 -> Human Readable Value: 5
TOS (Hex): 00 -> Human Readable Value: 0
Total Length (Hex): 0039 -> Human Readable Value: 57
IP Identification (Hex): 0000 -> Human Readable Value: 0
Flags + Offset (Hex): 4000 / 0100 0000 0000 0000 -> Human Readable Value: 16384
    - Reserved: 0
    - Don't Fragment: 1
    - More Fragments: 0
    - Offset: 000 / 0 0000 0000 0000
Time To Live (Hex): 40 -> Human Readable Value: 64
Protocol (Hex): 11 -> Human Readable Value: 17
Checksum (Hex): 11a6 -> Human Readable Value: 4518
Source Address (Hex): 0a416e64 -> Human Readable Value: 10.65.110.100
Destination Address (Hex): 8efb216e -> Human Readable Value: 142.251.33.110
UDP Packet:
Source Port (Hex): d086 -> Human Readable Value: 53382
Destination Port (Hex): 01bb -> Human Readable Value: 443
Length (Hex): 0025 -> Human Readable Value: 37
Checksum (Hex): 3bda -> Human Readable Value: 15322
Starting packet capture on en0 with filter: arp
```

Test 14



```
[gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py en0
Starting packet capture on en0 with filter: ip and tcp
```

waits forever

Test 15

gursidhsandhu@Gursidhs-MacBook-Pro src % python3 scanner.py en0
Starting packet capture on en0 with filter: ip and tcp

not connected, so just waits

This screenshot shows a terminal window titled "src — Python scanner.py en0 — 80x24". The command "python3 scanner.py en0" was run, followed by the message "Starting packet capture on en0 with filter: ip and tcp". A red arrow points to the top-left corner of the terminal window, and another red arrow points to the top-right corner of the desktop.

Destination Address (Hex): 8ee84cbf -> Human Readable Value: 142.232.76.191
UDP Packet:
Source Port (Hex): fac8 -> Human Readable Value: 64200
Destination Port (Hex): 0035 -> Human Readable Value: 53
Length (Hex): 0030 -> Human Readable Value: 48
Checksum (Hex): fd27 -> Human Readable Value: 64807
Starting packet capture on en0 with filter: arp
Captured Packet (Hex): ffffffffffffff9c3e539083cd080060010800060400019c3e539083cd0a416e6400000000000000a417ffe
Destination MAC: ff:ff:ff:ff:ff:ff
Source MAC: 9c:3e:53:90:83:cd
EtherType: 0806
Hardware Address Type (Hex): 0001 -> Human Readable Value: 1
Protocol Address Type (Hex): 0800 -> Human Readable Value: 2048
Hardware Address Length (Hex): 06 -> Human Readable Value: 6
Protocol Address Length (Hex): 04 -> Human Readable Value: 4
Opcode (Hex): 0001 -> Human Readable Value: 1
Source Hardware Address (Hex): 9c3e539083cd -> Human Readable Value: 9c:3e:53:90:83:cd
Source Protocol Address (Hex): 0a416e64 -> Human Readable Value: 10.65.110.100
Target Hardware Address (Hex): 000000000000 -> Human Readable Value: 00:00:00:00:00:00
Target Protocol Address (Hex): 0a417ffe -> Human Readable Value: 10.65.127.254
gursidhsandhu@Gursidhs-MacBook-Pro src %

gets connection

now captures packet

This screenshot shows a terminal window titled "src — -zsh — 80x24". The command "arp" was used as a filter for packet capture. The output shows a captured ARP packet. A red box highlights the line "Starting packet capture on en0 with filter: arp". Red arrows point from this box to the top-right corner of the desktop and to the line "now captures packet" in the text below. Another red arrow points to the bottom-right corner of the terminal window.