CS373 Defense Against the Dark Arts

Lab 2

By

Garrett Haley

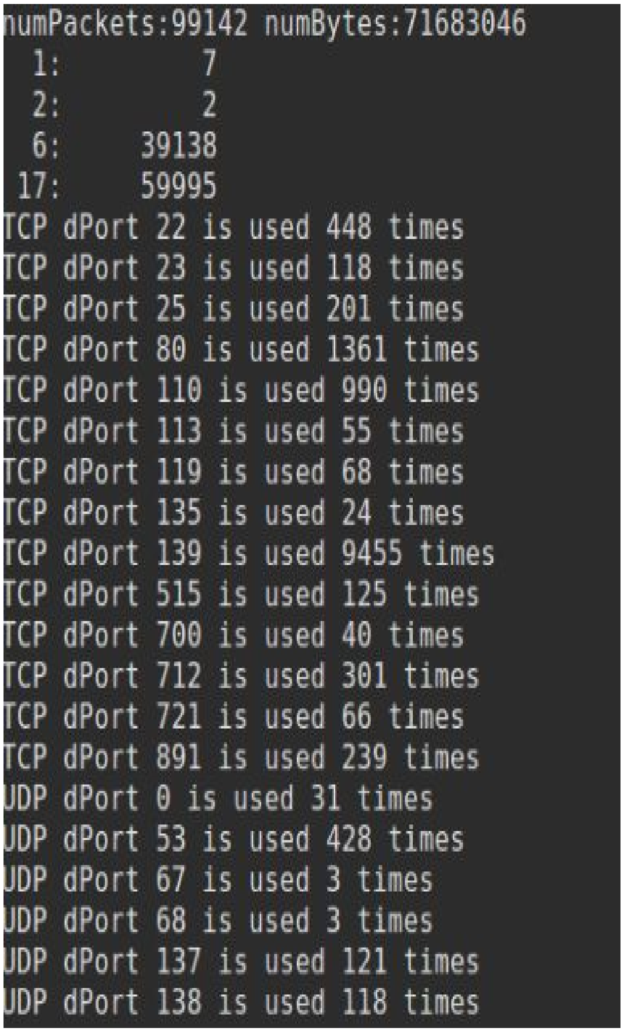
College of Electrical Engineering and Computer Science

Oregon State University

February 14 2019

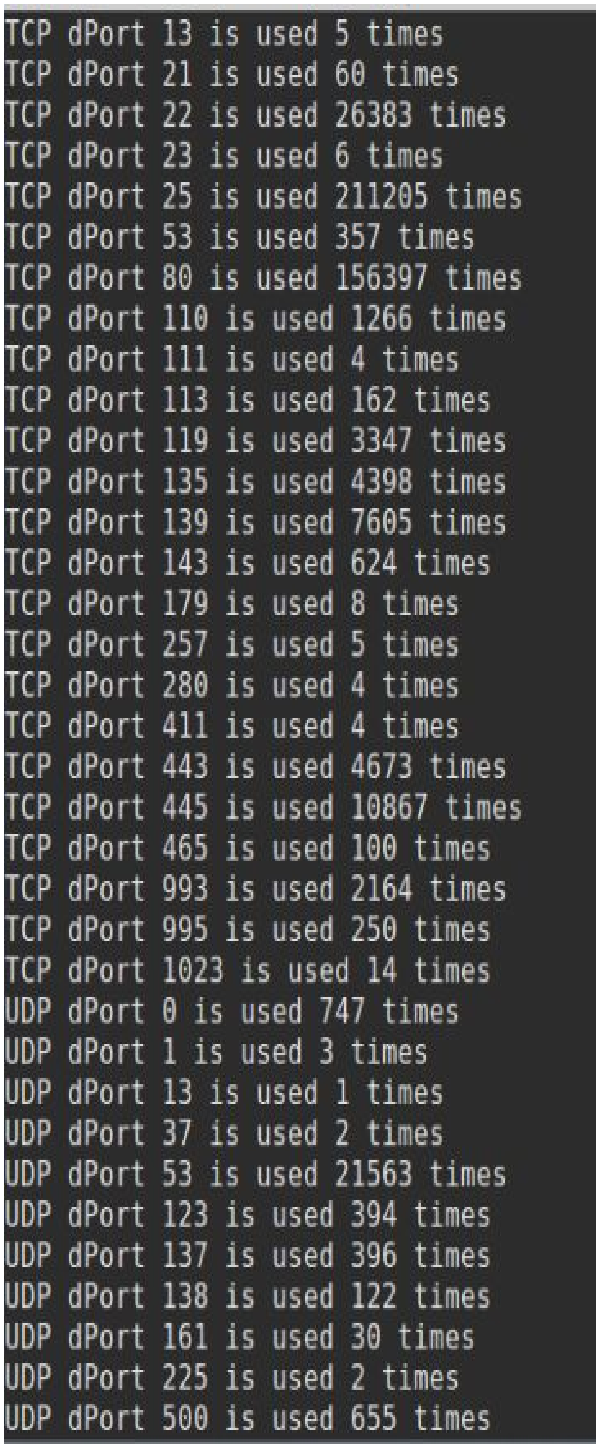
I. First, I extended script statistics to find TCP and UDP destination ports 1-1024. Below are my Results:

R-Dataset:



```
numPackets:99142 numBytes:71683046
  1:        7
  2:        2
  6:    39138
 17:    59995
TCP dPort 22 is used 448 times
TCP dPort 23 is used 118 times
TCP dPort 25 is used 201 times
TCP dPort 80 is used 1361 times
TCP dPort 110 is used 990 times
TCP dPort 113 is used 55 times
TCP dPort 119 is used 68 times
TCP dPort 135 is used 24 times
TCP dPort 139 is used 9455 times
TCP dPort 515 is used 125 times
TCP dPort 700 is used 40 times
TCP dPort 712 is used 301 times
TCP dPort 721 is used 66 times
TCP dPort 891 is used 239 times
UDP dPort 0 is used 31 times
UDP dPort 53 is used 428 times
UDP dPort 67 is used 3 times
UDP dPort 68 is used 3 times
UDP dPort 137 is used 121 times
UDP dPort 138 is used 118 times
```

O-Dataset



```
TCP dPort 13 is used 5 times
TCP dPort 21 is used 60 times
TCP dPort 22 is used 26383 times
TCP dPort 23 is used 6 times
TCP dPort 25 is used 211205 times
TCP dPort 53 is used 357 times
TCP dPort 80 is used 156397 times
TCP dPort 110 is used 1266 times
TCP dPort 111 is used 4 times
TCP dPort 113 is used 162 times
TCP dPort 119 is used 3347 times
TCP dPort 135 is used 4398 times
TCP dPort 139 is used 7605 times
TCP dPort 143 is used 624 times
TCP dPort 179 is used 8 times
TCP dPort 257 is used 5 times
TCP dPort 280 is used 4 times
TCP dPort 411 is used 4 times
TCP dPort 443 is used 4673 times
TCP dPort 445 is used 10867 times
TCP dPort 465 is used 100 times
TCP dPort 993 is used 2164 times
TCP dPort 995 is used 250 times
TCP dPort 1023 is used 14 times
UDP dPort 0 is used 747 times
UDP dPort 1 is used 3 times
UDP dPort 13 is used 1 times
UDP dPort 37 is used 2 times
UDP dPort 53 is used 21563 times
UDP dPort 123 is used 394 times
UDP dPort 137 is used 396 times
UDP dPort 138 is used 122 times
UDP dPort 161 is used 30 times
UDP dPort 225 is used 2 times
UDP dPort 500 is used 655 times
```

Identifying prominent ports from R-dataset:

1. TCP dport 139: 9,455

“TCP NetBIOS connections are made over this port, usually with Windows machines but also with any other system running Samba (SMB). These TCP connections form "NetBIOS sessions" to support connection oriented file sharing activities”[1].

2. TCP dport 80: 1,361

“This is the primary port used by the world wide web (www) system. Web servers open this port then listen for incoming connections from web browsers. Similarly, when a web browser is given a remote address (like grc.com or amazon.com), it assumes that a remote web server will be listening for connections on port 80 at that location”[1].

3. TCP dport 110: 990

“Pop3 "post office protocol" is used by eMail clients for the retrieval of their eMail from designated eMail "post office" servers. Email Clients such as Microsoft Outlook, Netscape, Eudora, and many others, connect to port 110 of a remote eMail server, then use the pop3 protocol to retrieve their eMail”[1].

4. TCP dport 22: 448

“SSH Remote Login Protocol”[1].

5. UDP dport 53: 428

Domain name service (DNS)

Identifying prominent ports from O-dataset:

1. TCP dport 25: 211,205

“SMTP is the protocol used to shuttle eMail across the Internet from one mail server to another. Over its years of use, the protocol has evolved significantly to become much more capable, and much less "simple" than it was in the beginning”[1].

2. TCP dport 80: 156,397

See part two above for port description.

3. TCP dport 22: 26,383

See part four above for port description.

4. UDP dport 53: 21,563

See part five above for port description.

5. TCP dport 445: 10, 867

“Preferred port for carrying Windows file sharing and numerous other services”[1].

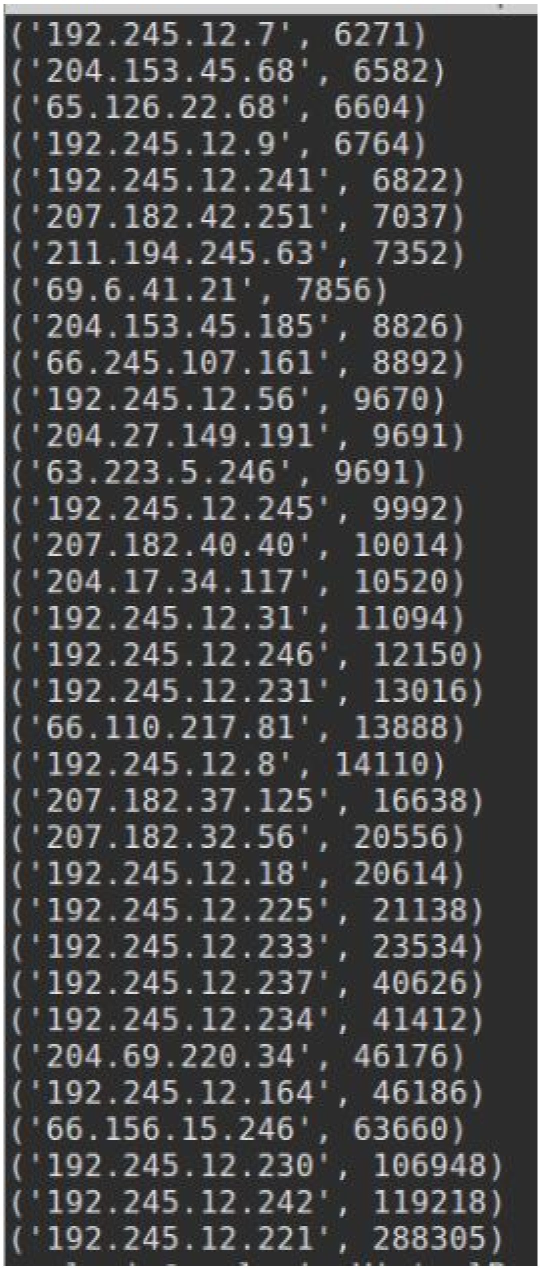
II. Characterizing the main functions of each network

R-dataset Network: From the data gathered above, we can extrapolate that this network is most likely a workplace network. The primary service destinations are ports 139, 80, 110, 22, and 53. The services are most likely SMB, HTTP, Pop3, SSH, and OCS_CMU . Pop3 is used by eMail clients for the retrieval of their eMail from designated eMail "post office" servers. SMB is an application-layer network protocol primarily used for offering shared access to files, printers, serial ports, and other sorts of communications between nodes on a network. Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network [1]. These three services seem to be the biggest clue this network is a workplace network. Checking emails, sharing files, and remotely accessing computers from a distance are common workplace activities.

O-dataset Network: From the data gathered above, we can extrapolate that this network is most likely a data center, ISP, or some kind of corporate mail network.The primary service destinations are ports 25, 80, 22, 53, and 445. Port 25 is most likely running SMTP which is the service used to shuttle eMail across the Internet from one mail server to another. Port 25 is often blocked by service providers from outgoing traffic to prevent unwanted email/spamming to clients (Therefore, this is most likely not a client network). Port 80 is typically reserved for http/https, port 53 is for DNS, and 445 for microsoft directory services (MDS).

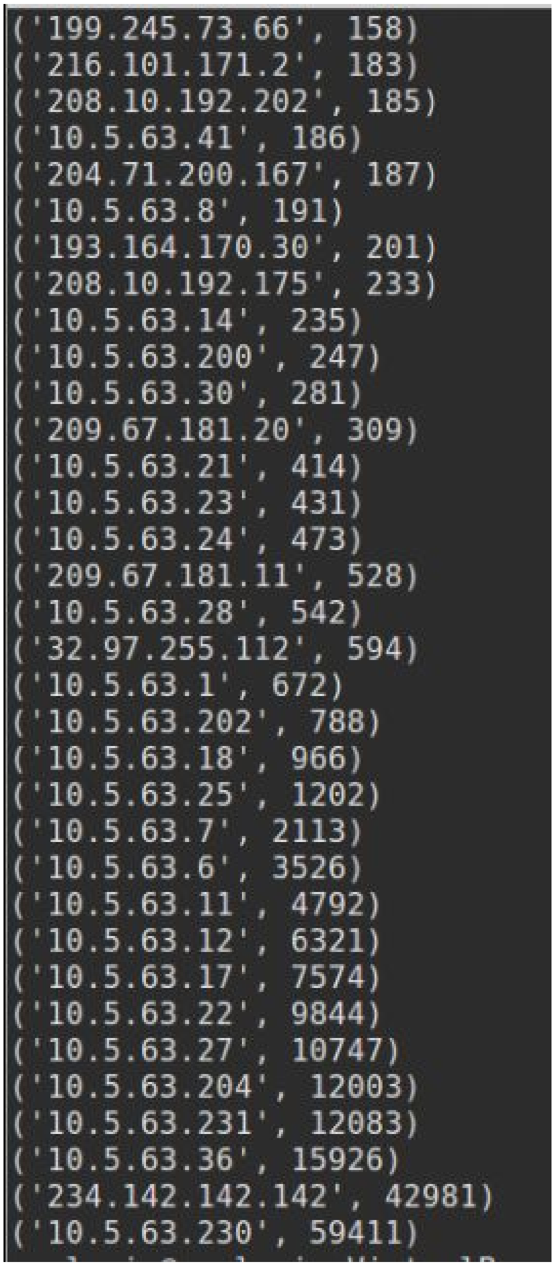
III. List of Distinct IP Addresses with Their Usage Counts.

O-Dataset IP’s



```
('192.245.12.7', 6271)
('204.153.45.68', 6582)
('65.126.22.68', 6604)
('192.245.12.9', 6764)
('192.245.12.241', 6822)
('207.182.42.251', 7037)
('211.194.245.63', 7352)
('69.6.41.21', 7856)
('204.153.45.185', 8826)
('66.245.107.161', 8892)
('192.245.12.56', 9670)
('204.27.149.191', 9691)
('63.223.5.246', 9691)
('192.245.12.245', 9992)
('207.182.40.40', 10014)
('204.17.34.117', 10520)
('192.245.12.31', 11094)
('192.245.12.246', 12150)
('192.245.12.231', 13016)
('66.110.217.81', 13888)
('192.245.12.8', 14110)
('207.182.37.125', 16638)
('207.182.32.56', 20556)
('192.245.12.18', 20614)
('192.245.12.225', 21138)
('192.245.12.233', 23534)
('192.245.12.237', 40626)
('192.245.12.234', 41412)
('204.69.220.34', 46176)
('192.245.12.164', 46186)
('66.156.15.246', 63660)
('192.245.12.230', 106948)
('192.245.12.242', 119218)
('192.245.12.221', 288305)
```

R-Dataset IP’s



```
('199.245.73.66', 158)
('216.101.171.2', 183)
('208.10.192.202', 185)
('10.5.63.41', 186)
('204.71.200.167', 187)
('10.5.63.8', 191)
('193.164.170.30', 201)
('208.10.192.175', 233)
('10.5.63.14', 235)
('10.5.63.200', 247)
('10.5.63.30', 281)
('209.67.181.20', 309)
('10.5.63.21', 414)
('10.5.63.23', 431)
('10.5.63.24', 473)
('209.67.181.11', 528)
('10.5.63.28', 542)
('32.97.255.112', 594)
('10.5.63.1', 672)
('10.5.63.202', 788)
('10.5.63.18', 966)
('10.5.63.25', 1202)
('10.5.63.7', 2113)
('10.5.63.6', 3526)
('10.5.63.11', 4792)
('10.5.63.12', 6321)
('10.5.63.17', 7574)
('10.5.63.22', 9844)
('10.5.63.27', 10747)
('10.5.63.204', 12003)
('10.5.63.231', 12083)
('10.5.63.36', 15926)
('234.142.142.142', 42981)
('10.5.63.230', 59411)
```

IV Confirmation

Yes, these prefixes (192.245 and 10.5.63) can be used to aid in the IP network classification based on the A, B, C, and D network classifications.

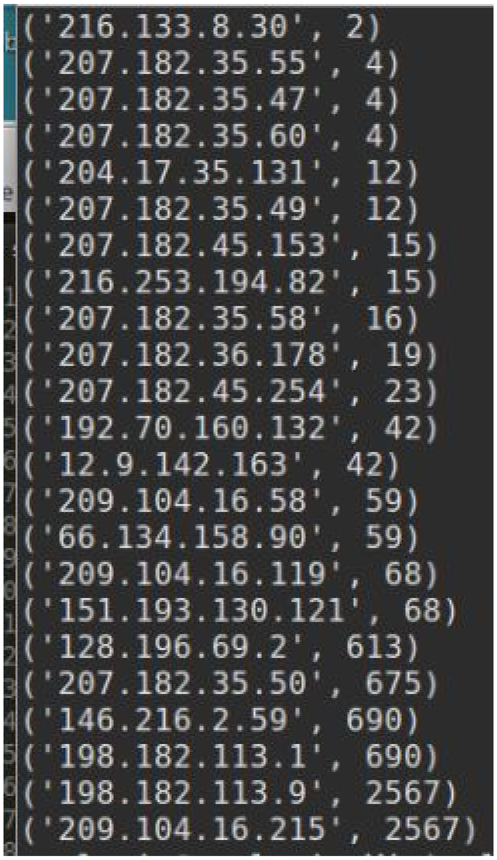
V Network Number (Network Prefix) that Seems to Dominate the Traffic

O-dataset: 192.245.12
R-dataset**:** 10.5.63

VI. GRE, IPSEC, OSPF Sorted IP Count Output

R-dataset: no results (0)

O-dataset:



```
('216.133.8.30', 2)
('207.182.35.55', 4)
('207.182.35.47', 4)
('207.182.35.60', 4)
('204.17.35.131', 12)
('207.182.35.49', 12)
('207.182.45.153', 15)
('216.253.194.82', 15)
('207.182.35.58', 16)
('207.182.36.178', 19)
('207.182.45.254', 23)
('192.70.160.132', 42)
('12.9.142.163', 42)
('209.104.16.58', 59)
('66.134.158.90', 59)
('209.104.16.119', 68)
('151.193.130.121', 68)
('128.196.69.2', 613)
('207.182.35.50', 675)
('146.216.2.59', 690)
('198.182.113.1', 690)
('198.182.113.9', 2567)
('209.104.16.215', 2567)
```

VII. Network Number (Network Prefix) that Seems to Dominate the Traffic

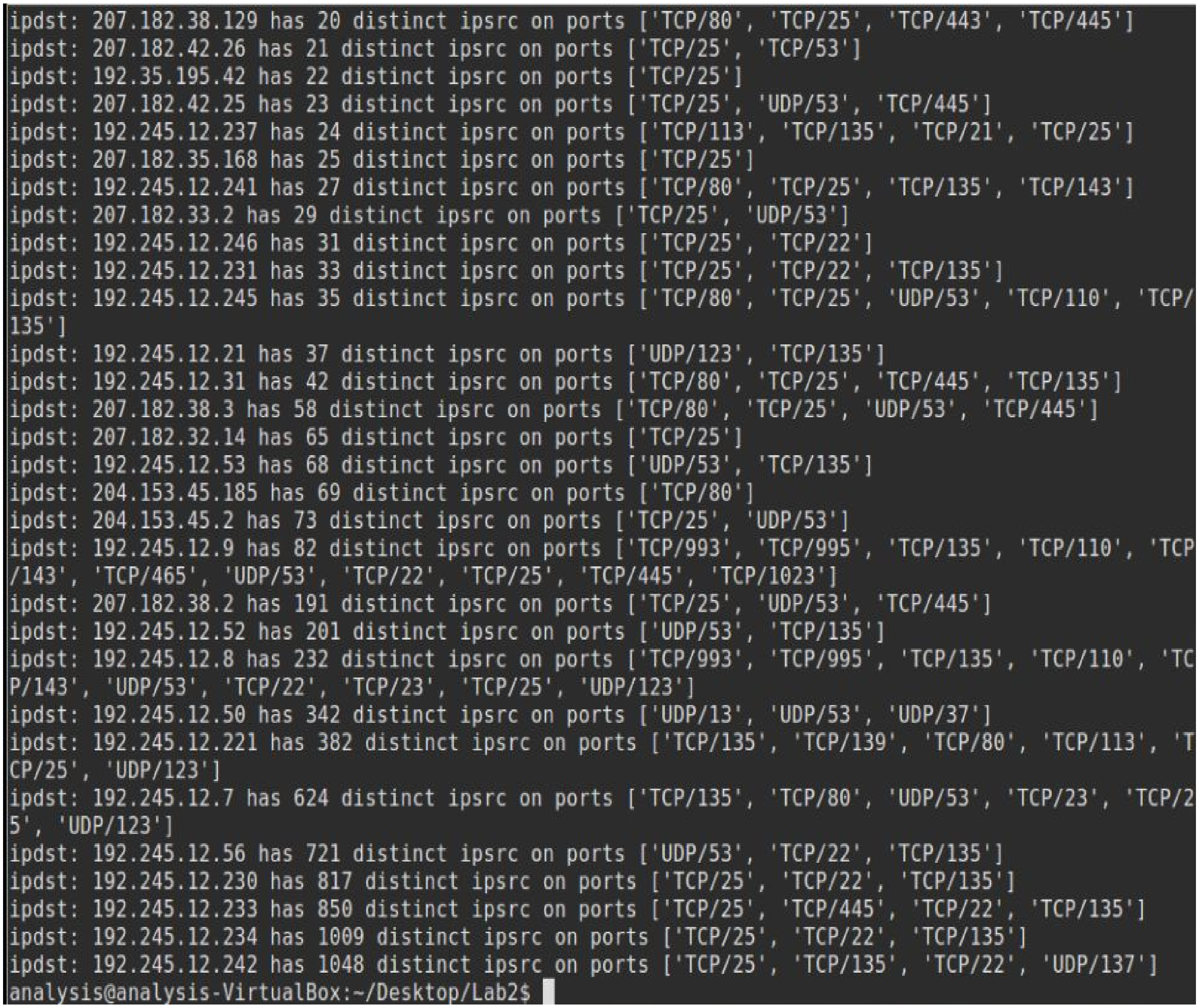
O-dataset: 198.182.113

VIII Confirmation.

Yes, the OSPF is the open shortest path first routing protocol. With the R dataset failing to produce packets using this protocol while the O dataset producing packets using this protocol can indicate one of these networks is able to discover the topology and choose the best routing paths as connections between routers appear and disappear. Therefore R cannot be an ISP without those protocols.

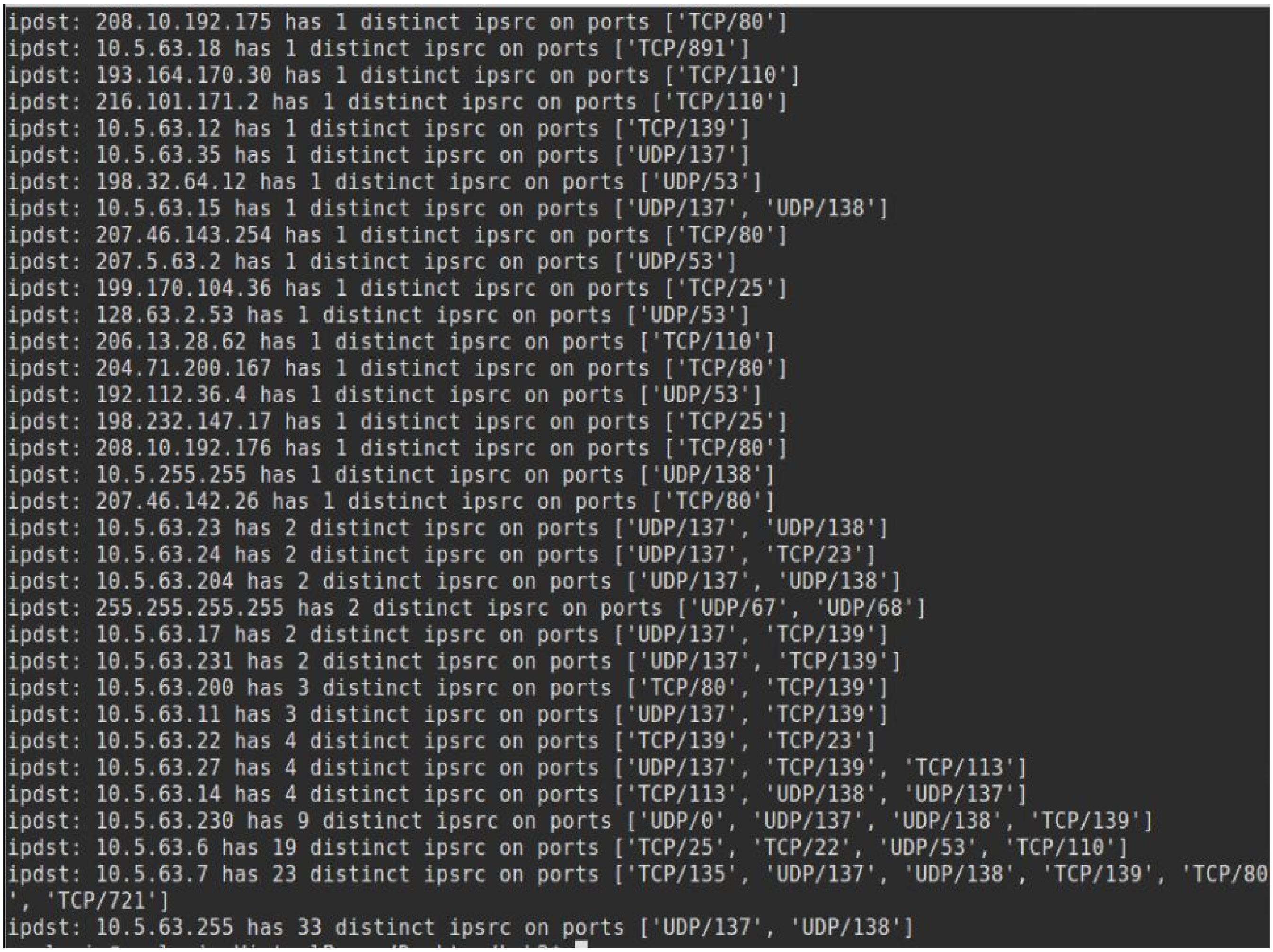
IX Finding the Servers

O-dataset “connto” Results:



```
ipdst: 207.182.38.129 has 20 distinct ipsrc on ports ['TCP/80', 'TCP/25', 'TCP/443', 'TCP/445']
ipdst: 207.182.42.26 has 21 distinct ipsrc on ports ['TCP/25', 'TCP/53']
ipdst: 192.35.195.42 has 22 distinct ipsrc on ports ['TCP/25']
ipdst: 207.182.42.25 has 23 distinct ipsrc on ports ['TCP/25', 'UDP/53', 'TCP/445']
ipdst: 192.245.12.237 has 24 distinct ipsrc on ports ['TCP/113', 'TCP/135', 'TCP/21', 'TCP/25']
ipdst: 207.182.35.168 has 25 distinct ipsrc on ports ['TCP/25']
ipdst: 192.245.12.241 has 27 distinct ipsrc on ports ['TCP/80', 'TCP/25', 'TCP/135', 'TCP/143']
ipdst: 207.182.33.2 has 29 distinct ipsrc on ports ['TCP/25', 'UDP/53']
ipdst: 192.245.12.246 has 31 distinct ipsrc on ports ['TCP/25', 'TCP/22']
ipdst: 192.245.12.231 has 33 distinct ipsrc on ports ['TCP/25', 'TCP/22', 'TCP/135']
ipdst: 192.245.12.245 has 35 distinct ipsrc on ports ['TCP/80', 'TCP/25', 'UDP/53', 'TCP/110', 'TCP/
135']
ipdst: 192.245.12.21 has 37 distinct ipsrc on ports ['UDP/123', 'TCP/135']
ipdst: 192.245.12.31 has 42 distinct ipsrc on ports ['TCP/80', 'TCP/25', 'TCP/445', 'TCP/135']
ipdst: 207.182.38.3 has 58 distinct ipsrc on ports ['TCP/80', 'TCP/25', 'UDP/53', 'TCP/445']
ipdst: 207.182.32.14 has 65 distinct ipsrc on ports ['TCP/25']
ipdst: 192.245.12.53 has 68 distinct ipsrc on ports ['UDP/53', 'TCP/135']
ipdst: 204.153.45.185 has 69 distinct ipsrc on ports ['TCP/80']
ipdst: 204.153.45.2 has 73 distinct ipsrc on ports ['TCP/25', 'UDP/53']
ipdst: 192.245.12.9 has 82 distinct ipsrc on ports ['TCP/993', 'TCP/995', 'TCP/135', 'TCP/110', 'TCP
/143', 'TCP/465', 'UDP/53', 'TCP/22', 'TCP/25', 'TCP/445', 'TCP/1023']
ipdst: 207.182.38.2 has 191 distinct ipsrc on ports ['TCP/25', 'UDP/53', 'TCP/445']
ipdst: 192.245.12.52 has 201 distinct ipsrc on ports ['UDP/53', 'TCP/135']
ipdst: 192.245.12.8 has 232 distinct ipsrc on ports ['TCP/993', 'TCP/995', 'TCP/135', 'TCP/110', 'TC
P/143', 'UDP/53', 'TCP/22', 'TCP/23', 'TCP/25', 'UDP/123']
ipdst: 192.245.12.50 has 342 distinct ipsrc on ports ['UDP/13', 'UDP/53', 'UDP/37']
ipdst: 192.245.12.221 has 382 distinct ipsrc on ports ['TCP/135', 'TCP/139', 'TCP/80', 'TCP/113', 'T
CP/25', 'UDP/123']
ipdst: 192.245.12.7 has 624 distinct ipsrc on ports ['TCP/135', 'TCP/80', 'UDP/53', 'TCP/23', 'TCP/2
5', 'UDP/123']
ipdst: 192.245.12.56 has 721 distinct ipsrc on ports ['UDP/53', 'TCP/22', 'TCP/135']
ipdst: 192.245.12.230 has 817 distinct ipsrc on ports ['TCP/25', 'TCP/22', 'TCP/135']
ipdst: 192.245.12.233 has 850 distinct ipsrc on ports ['TCP/25', 'TCP/445', 'TCP/22', 'TCP/135']
ipdst: 192.245.12.234 has 1009 distinct ipsrc on ports ['TCP/25', 'TCP/22', 'TCP/135']
ipdst: 192.245.12.242 has 1048 distinct ipsrc on ports ['TCP/25', 'TCP/135', 'TCP/22', 'UDP/137']
analysis@analysis-VirtualBox:~/Desktop/Lab2$
```

R-dataset “connto” Results:



```
ipdst: 208.10.192.175 has 1 distinct ipsrc on ports ['TCP/80']
ipdst: 10.5.63.18 has 1 distinct ipsrc on ports ['TCP/891']
ipdst: 193.164.170.30 has 1 distinct ipsrc on ports ['TCP/110']
ipdst: 216.101.171.2 has 1 distinct ipsrc on ports ['TCP/110']
ipdst: 10.5.63.12 has 1 distinct ipsrc on ports ['TCP/139']
ipdst: 10.5.63.35 has 1 distinct ipsrc on ports ['UDP/137']
ipdst: 198.32.64.12 has 1 distinct ipsrc on ports ['UDP/53']
ipdst: 10.5.63.15 has 1 distinct ipsrc on ports ['UDP/137', 'UDP/138']
ipdst: 207.46.143.254 has 1 distinct ipsrc on ports ['TCP/80']
ipdst: 207.5.63.2 has 1 distinct ipsrc on ports ['UDP/53']
ipdst: 199.170.104.36 has 1 distinct ipsrc on ports ['TCP/25']
ipdst: 128.63.2.53 has 1 distinct ipsrc on ports ['UDP/53']
ipdst: 206.13.28.62 has 1 distinct ipsrc on ports ['TCP/110']
ipdst: 204.71.200.167 has 1 distinct ipsrc on ports ['TCP/80']
ipdst: 192.112.36.4 has 1 distinct ipsrc on ports ['UDP/53']
ipdst: 198.232.147.17 has 1 distinct ipsrc on ports ['TCP/25']
ipdst: 208.10.192.176 has 1 distinct ipsrc on ports ['TCP/80']
ipdst: 10.5.255.255 has 1 distinct ipsrc on ports ['UDP/138']
ipdst: 207.46.142.26 has 1 distinct ipsrc on ports ['TCP/80']
ipdst: 10.5.63.23 has 2 distinct ipsrc on ports ['UDP/137', 'UDP/138']
ipdst: 10.5.63.24 has 2 distinct ipsrc on ports ['UDP/137', 'TCP/23']
ipdst: 10.5.63.204 has 2 distinct ipsrc on ports ['UDP/137', 'UDP/138']
ipdst: 255.255.255.255 has 2 distinct ipsrc on ports ['UDP/67', 'UDP/68']
ipdst: 10.5.63.17 has 2 distinct ipsrc on ports ['UDP/137', 'TCP/139']
ipdst: 10.5.63.231 has 2 distinct ipsrc on ports ['UDP/137', 'TCP/139']
ipdst: 10.5.63.200 has 3 distinct ipsrc on ports ['TCP/80', 'TCP/139']
ipdst: 10.5.63.11 has 3 distinct ipsrc on ports ['UDP/137', 'TCP/139']
ipdst: 10.5.63.22 has 4 distinct ipsrc on ports ['TCP/139', 'TCP/23']
ipdst: 10.5.63.27 has 4 distinct ipsrc on ports ['UDP/137', 'TCP/139', 'TCP/113']
ipdst: 10.5.63.14 has 4 distinct ipsrc on ports ['TCP/113', 'UDP/138', 'UDP/137']
ipdst: 10.5.63.230 has 9 distinct ipsrc on ports ['UDP/0', 'UDP/137', 'UDP/138', 'TCP/139']
ipdst: 10.5.63.6 has 19 distinct ipsrc on ports ['TCP/25', 'TCP/22', 'UDP/53', 'TCP/110']
ipdst: 10.5.63.7 has 23 distinct ipsrc on ports ['TCP/135', 'UDP/137', 'UDP/138', 'TCP/139', 'TCP/80
', 'TCP/721']
ipdst: 10.5.63.255 has 33 distinct ipsrc on ports ['UDP/137', 'UDP/138']
```

X. Server Set

A. R-dataset top 20: Seen in R-dataset photo above.
   O-dataset top 20: Seen in O-dataset photo above.

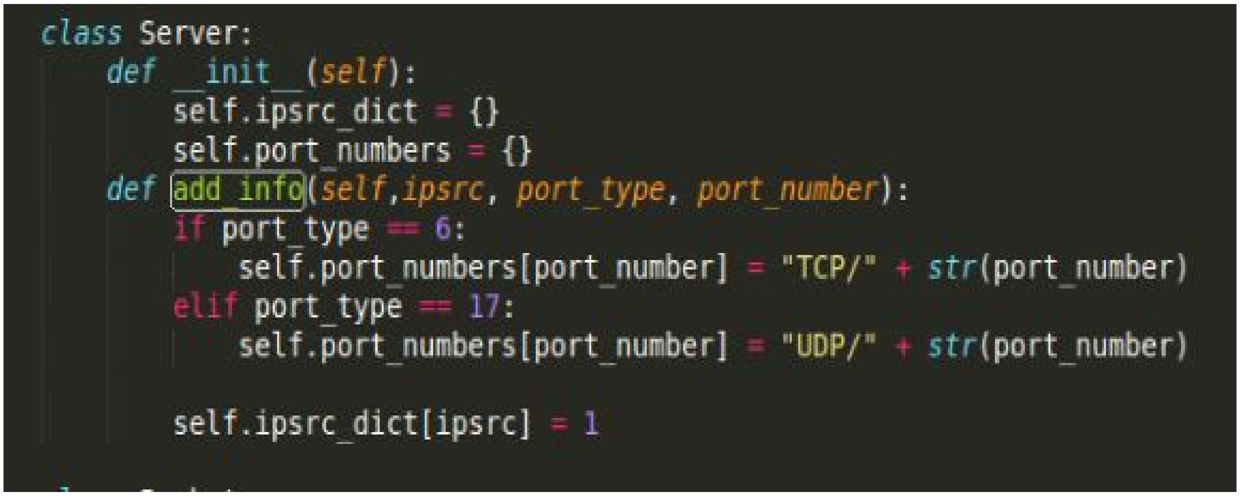
B. R-dataset servers:
   - Mail servers: 10.5.63.6, 198.232.147.17, 199.170.104.36.
   - Web servers: 10.5.63.200, 207.46.142.26, 208.10.192.176, 204.71.200.167, 207.46.143.254, 208.10.192.175.
   - Printers: 10.5.63.7, 10.5.63.230, 10.5.63.14, 10.5.63.27, 10.5.6.22, 10.5.63.11, 10.5.63.17, 10.5.63.204, 10.5.63.
   - DNS servers: 192.112.36.4, 128.63.2.53, 207.5.63.2, 198.32.64.12.

C. O-dataset servers:
   - Mail servers: 207.182.38.129, 192.35.195.42, 192.245.12.231, 207.182.32.14, 192.245.12.230, 192.245.12.233, 192.245.12.234, 192.245.12.242, 207.182.35.168.
   - Web servers: 192.245.12.241, 192.245.12.245, 192.245.12.31, 207.182.38.3, 204.153.45.185.
   - Pop/imap servers: 192.245.12.9, 192.245.12.8.
   - DNS servers: 192.245.12.52, 192.245.12.50, 192.245.12.56, 192.245.12.53

XI. Updated Information

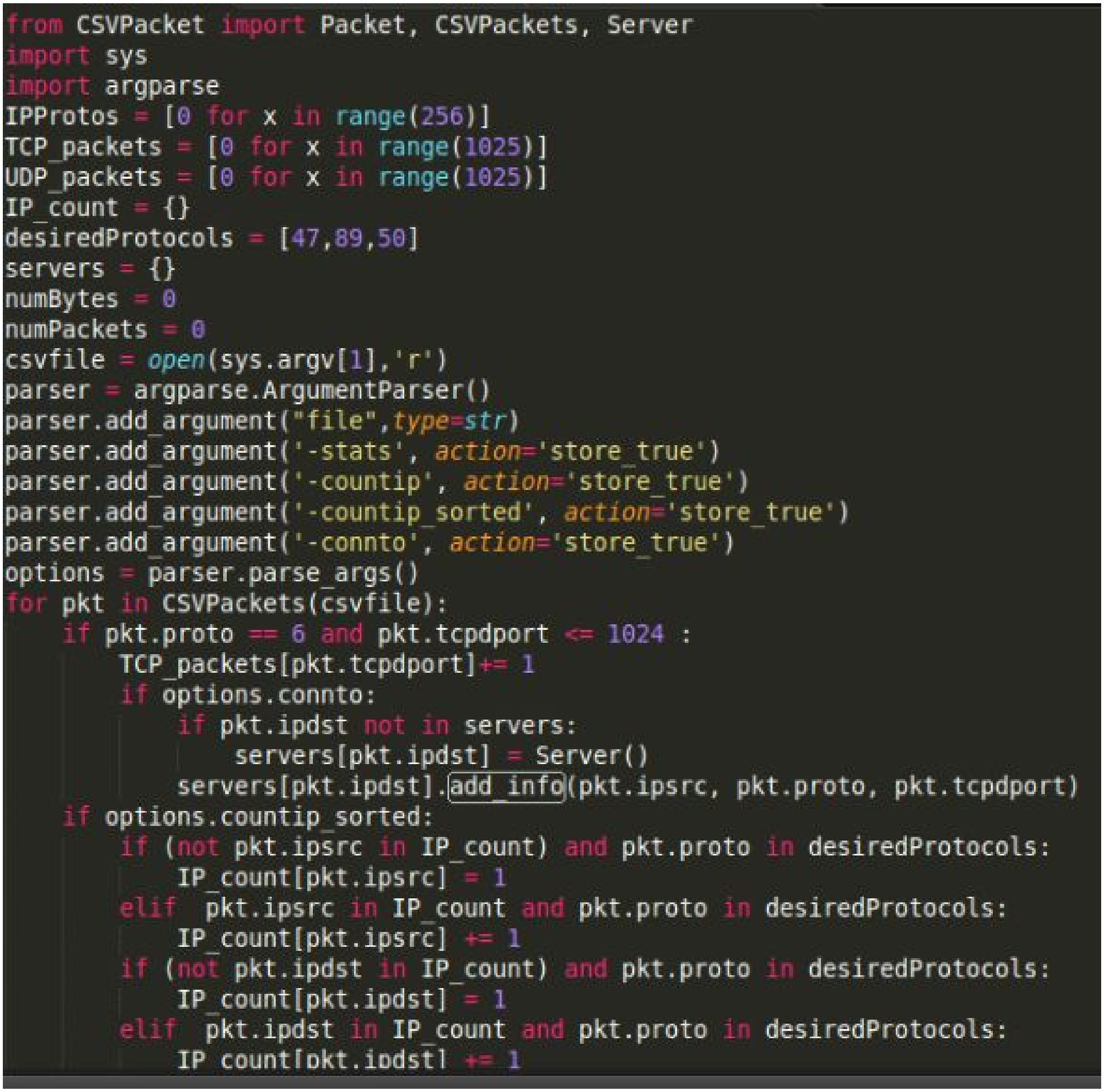
Based on the information I have gathered, the network from dataset R is most likely a workplace environment due to the large amount of traffic related to printing services and file transfers. The network from dataset O is most likely a small ISP due to the large usage of SMTP and HTTP/HTTPS services as well as the Open Shortest Path First protocol packets found in the dataset.

Source Code Below:

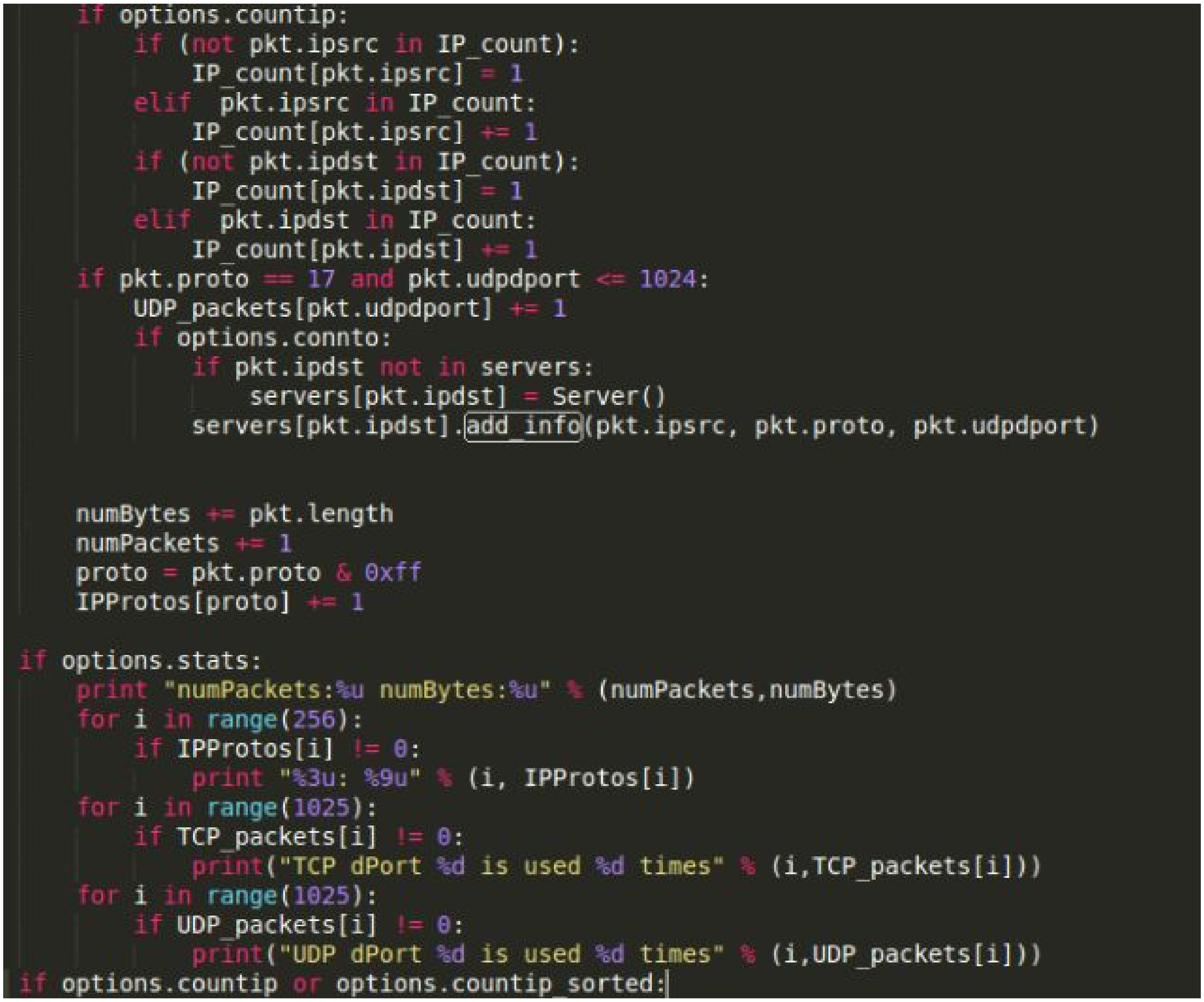


```
class Server:
    def __init__(self):
        self.ipsrc_dict = {}
        self.port_numbers = {}
    def add_info(self,ipsrc, port_type, port_number):
        if port_type == 6:
            self.port_numbers[port_number] = "TCP/" + str(port_number)
        elif port_type == 17:
            self.port_numbers[port_number] = "UDP/" + str(port_number)

        self.ipsrc_dict[ipsrc] = 1
```



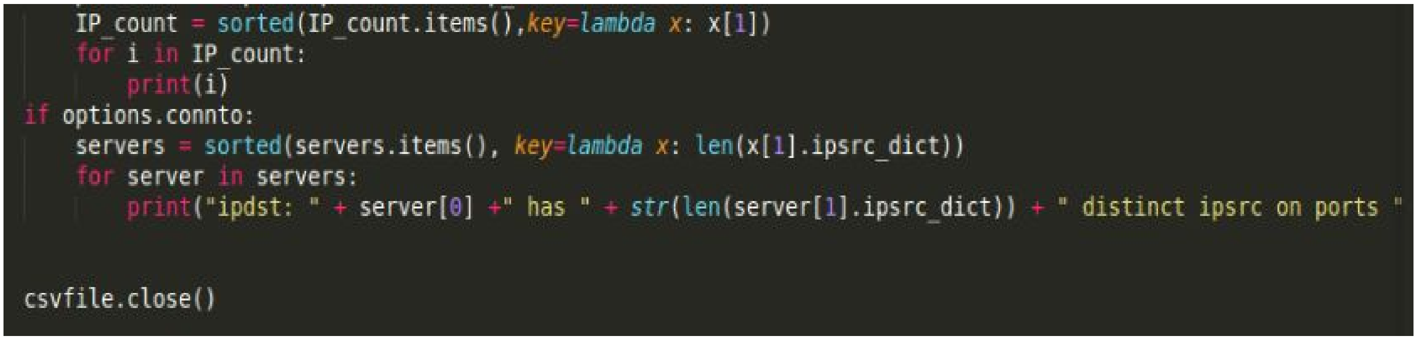
```
from CSVPacket import Packet, CSVPackets, Server
import sys
import argparse
IPProtos = [0 for x in range(256)]
TCP_packets = [0 for x in range(1025)]
UDP_packets = [0 for x in range(1025)]
IP_count = {}
desiredProtocols = [47,89,50]
servers = {}
numBytes = 0
numPackets = 0
csvfile = open(sys.argv[1],'r')
parser = argparse.ArgumentParser()
parser.add_argument("file",type=str)
parser.add_argument('-stats', action='store_true')
parser.add_argument('-countip', action='store_true')
parser.add_argument('-countip_sorted', action='store_true')
parser.add_argument('-connto', action='store_true')
options = parser.parse_args()
for pkt in CSVPackets(csvfile):
    if pkt.proto == 6 and pkt.tcpdport <= 1024 :
        TCP_packets[pkt.tcpdport]+= 1
        if options.connto:
            if pkt.ipdst not in servers:
                servers[pkt.ipdst] = Server()
            servers[pkt.ipdst].add_info(pkt.ipsrc, pkt.proto, pkt.tcpdport)
    if options.countip_sorted:
        if (not pkt.ipsrc in IP_count) and pkt.proto in desiredProtocols:
            IP_count[pkt.ipsrc] = 1
        elif  pkt.ipsrc in IP_count and pkt.proto in desiredProtocols:
            IP_count[pkt.ipsrc] += 1
        if (not pkt.ipdst in IP_count) and pkt.proto in desiredProtocols:
            IP_count[pkt.ipdst] = 1
        elif  pkt.ipdst in IP_count and pkt.proto in desiredProtocols:
            IP_count[pkt.ipdst] += 1
```



```
    if options.countip:
        if (not pkt.ipsrc in IP_count):
            IP_count[pkt.ipsrc] = 1
        elif  pkt.ipsrc in IP_count:
            IP_count[pkt.ipsrc] += 1
        if (not pkt.ipdst in IP_count):
            IP_count[pkt.ipdst] = 1
        elif  pkt.ipdst in IP_count:
            IP_count[pkt.ipdst] += 1
    if pkt.proto == 17 and pkt.udpdport <= 1024:
        UDP_packets[pkt.udpdport] += 1
        if options.connto:
            if pkt.ipdst not in servers:
                servers[pkt.ipdst] = Server()
            servers[pkt.ipdst].add_info(pkt.ipsrc, pkt.proto, pkt.udpdport)


    numBytes += pkt.length
    numPackets += 1
    proto = pkt.proto & 0xff
    IPProtos[proto] += 1

if options.stats:
    print "numPackets:%u numBytes:%u" % (numPackets,numBytes)
    for i in range(256):
        if IPProtos[i] != 0:
            print "%3u: %9u" % (i, IPProtos[i])
    for i in range(1025):
        if TCP_packets[i] != 0:
            print("TCP dPort %d is used %d times" % (i,TCP_packets[i]))
    for i in range(1025):
        if UDP_packets[i] != 0:
            print("UDP dPort %d is used %d times" % (i,UDP_packets[i]))
if options.countip or options.countip_sorted:
```



```
    IP_count = sorted(IP_count.items(),key=lambda x: x[1])
    for i in IP_count:
        print(i)
if options.connto:
    servers = sorted(servers.items(), key=lambda x: len(x[1].ipsrc_dict))
    for server in servers:
        print("ipdst: " + server[0] +" has " + str(len(server[1].ipsrc_dict)) + " distinct ipsrc on ports "


csvfile.close()
```

Citations

[1] S. Gibson and Gibson, *GRC | Port Authority, for Port {port}* . [Online]. Available: https://www.grc.com/port_{port}.htm. [Accessed: 14-Feb-2019].