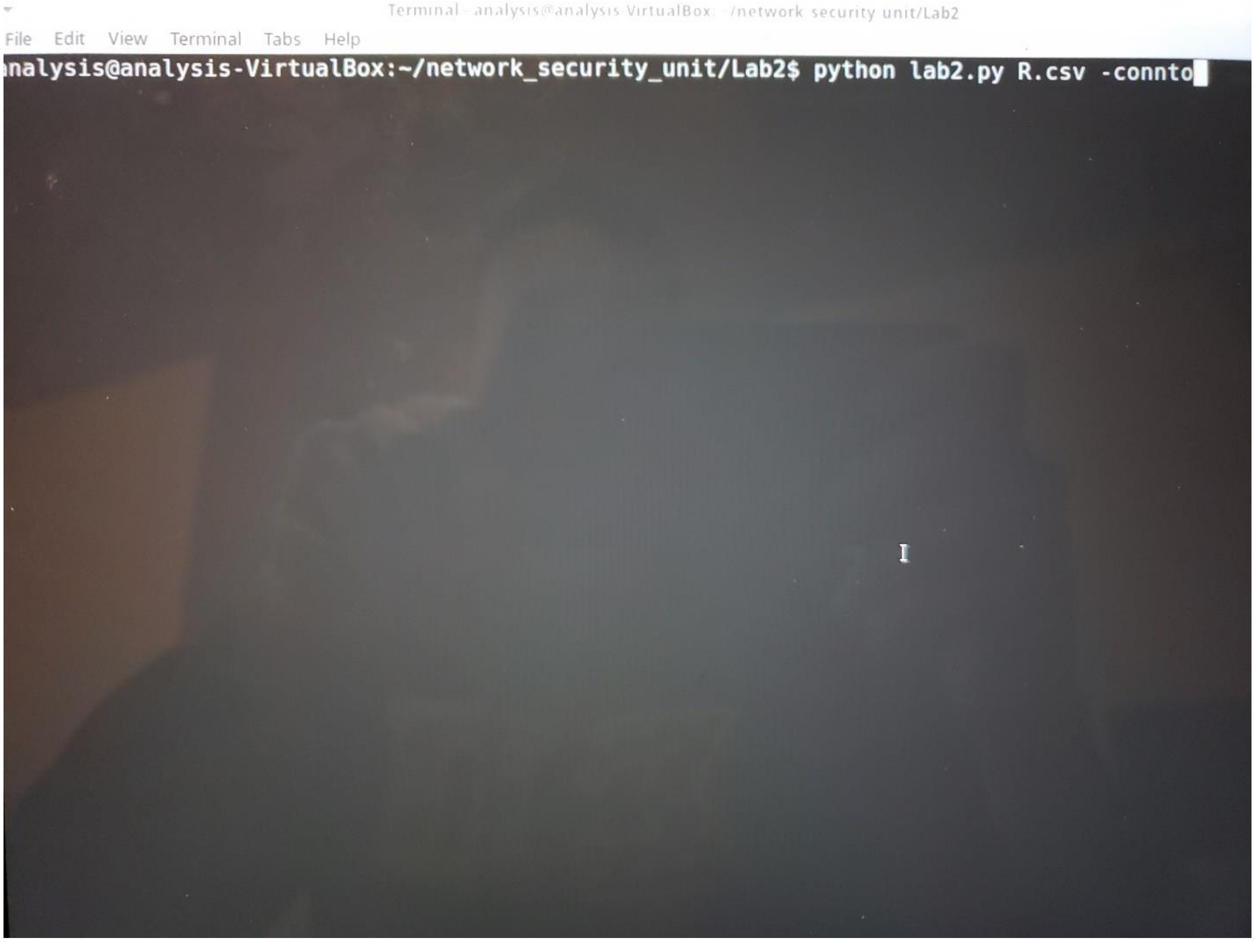
Lab 2

Commands are run using “python lab2.py R/O.csv -command” for final version.

Pictures are from different steps in development; labconnto.py assign.py and test.py

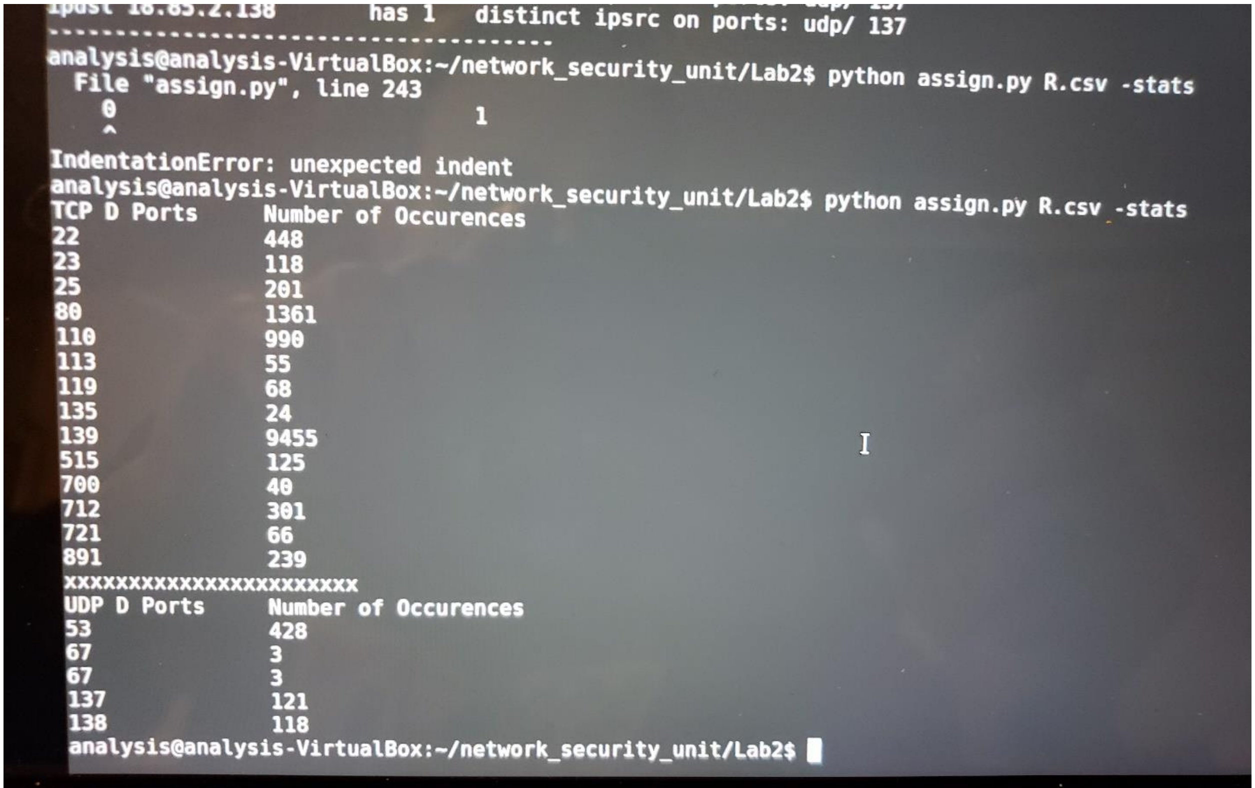


Terminal - analysis@analysis-VirtualBox: ~/network security unit/Lab2
File
Edit
View
Terminal
Tabs
Help

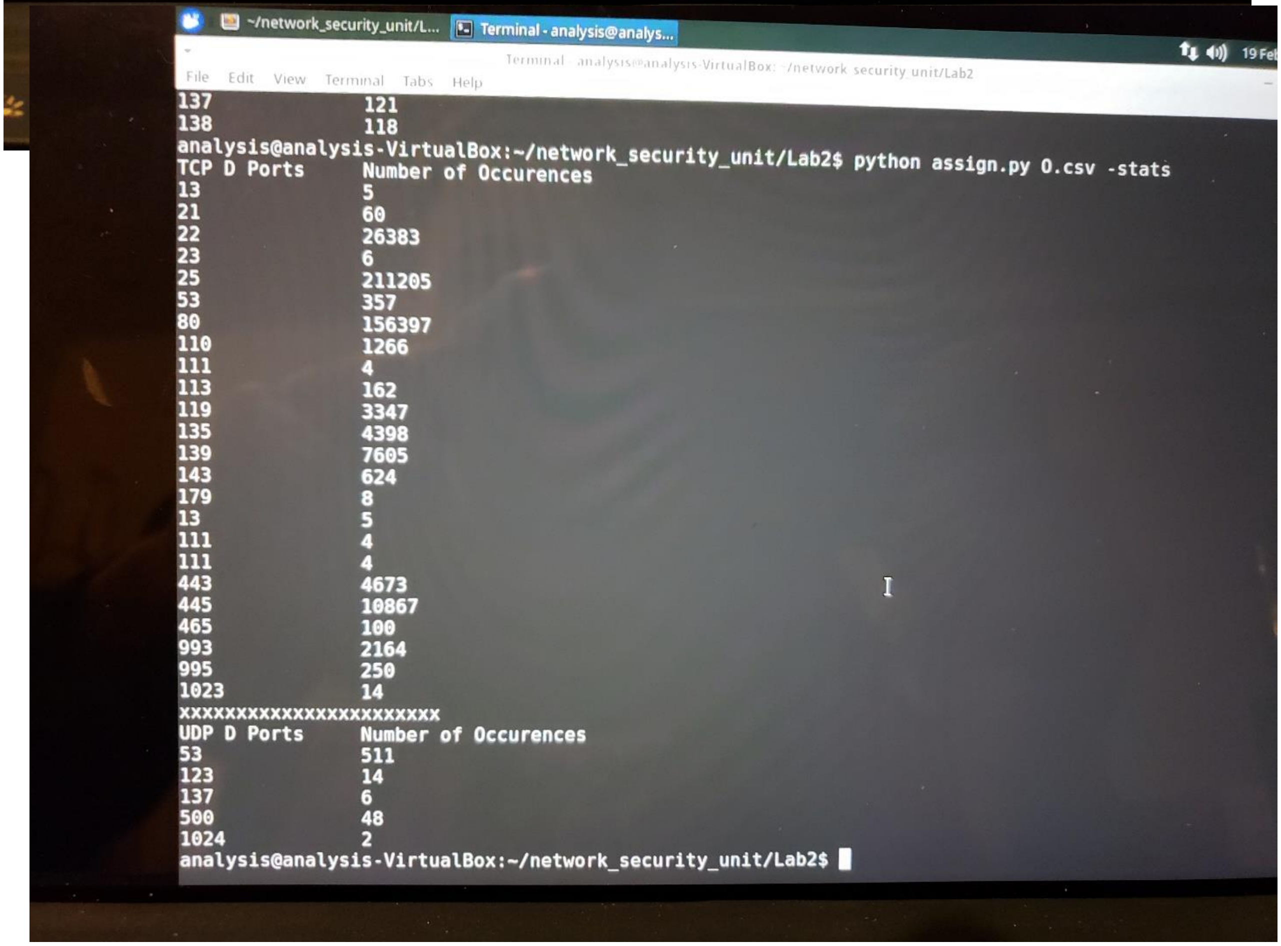
```
nalysis@analysis-VirtualBox:~/network_security_unit/Lab2$ python lab2.py R.csv -connto
```

Pictures of code (I couldn’t export it out of the vm) at the end of this writeup.

1.



```
ipdst 10.83.2.138       has 1   distinct ipsrc on ports: udp/ 137
---------------------------------------
analysis@analysis-VirtualBox:~/network_security_unit/Lab2$ python assign.py R.csv -stats
  File "assign.py", line 243
    0                        1
    ^
IndentationError: unexpected indent
analysis@analysis-VirtualBox:~/network_security_unit/Lab2$ python assign.py R.csv -stats
TCP D Ports     Number of Occurences
22              448
23              118
25              201
80              1361
110             990
113             55
119             68
135             24
139             9455
515             125
700             40
712             301
721             66
891             239
xxxxxxxxxxxxxxxxxxxxxx
UDP D Ports     Number of Occurences
53              428
67              3
67              3
137             121
138             118
analysis@analysis-VirtualBox:~/network_security_unit/Lab2$ █
```

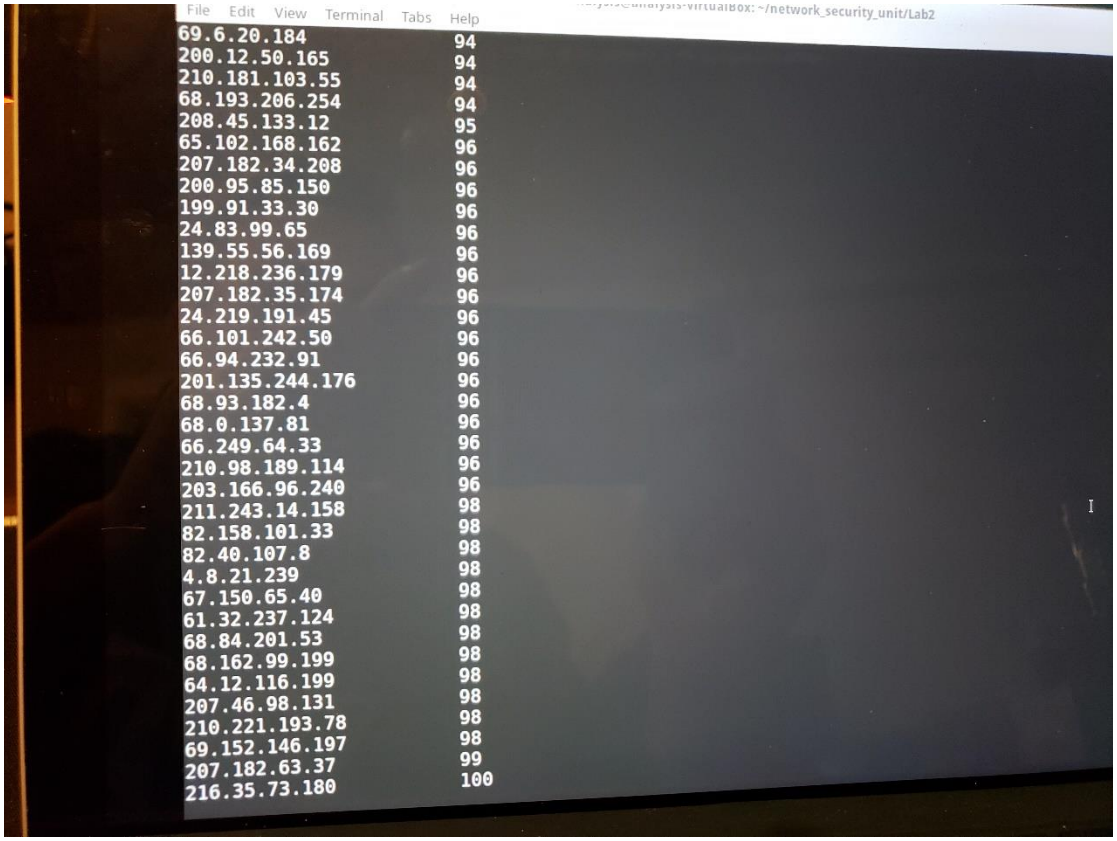

~/network_security_unit/L...
Terminal - analysis@analys...
19 Feb
Terminal - analysis@analysis-VirtualBox: ~/network_security_unit/Lab2
File Edit View Terminal Tabs Help

```
137             121
138             118
analysis@analysis-VirtualBox:~/network_security_unit/Lab2$ python assign.py O.csv -stats
TCP D Ports     Number of Occurences
13              5
21              60
22              26383
23              6
25              211205
53              357
80              156397
110             1266
111             4
113             162
119             3347
135             4398
139             7605
143             624
179             8
13              5
111             4
111             4
443             4673
445             10867
465             100
993             2164
995             250
1023            14
xxxxxxxxxxxxxxxxxxxxxx
UDP D Ports     Number of Occurences
53              511
123             14
137             6
500             48
1024            2
analysis@analysis-VirtualBox:~/network_security_unit/Lab2$ █
```

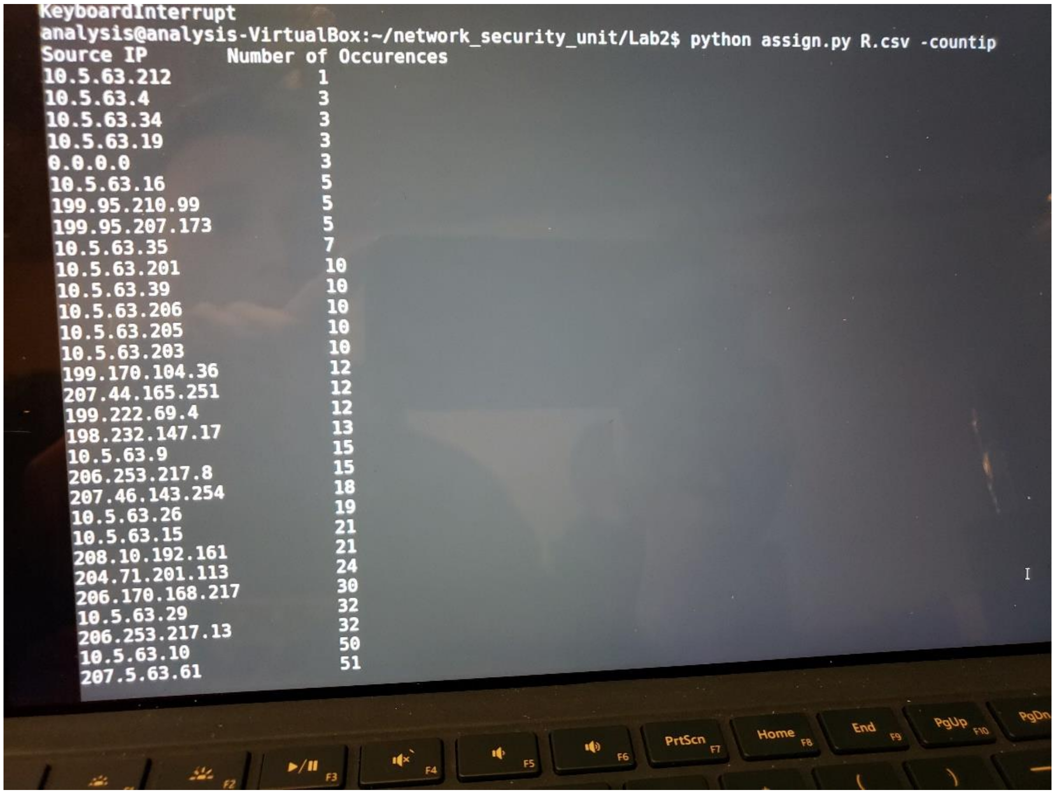
1. Judging by the large amount of IP addresses I would guess this is some kind of data center or work center.

    4 Yes it does inform my answer, there is a huge amount of occurrences of hundreds of source IPs so I would guess this is a data center or major server operation.

(O data, output was so large I couldn't scroll up enough)


File Edit View Terminal Tabs Help
VirtualBox: ~/network_security_unit/Lab2

```
69.6.20.184            94
200.12.50.165          94
210.181.103.55         94
68.193.206.254         94
208.45.133.12          95
65.102.168.162         96
207.182.34.208         96
200.95.85.150          96
199.91.33.30           96
24.83.99.65            96
139.55.56.169          96
12.218.236.179         96
207.182.35.174         96
24.219.191.45          96
66.101.242.50          96
66.94.232.91           96
201.135.244.176        96
68.93.182.4            96
68.0.137.81            96
66.249.64.33           96
210.98.189.114         96
203.166.96.240         96
211.243.14.158         98
82.158.101.33          98
82.40.107.8            98
4.8.21.239             98
67.150.65.40           98
61.32.237.124          98
68.84.201.53           98
68.162.99.199          98
64.12.116.199          98
207.46.98.131          98
210.221.193.78         98
69.152.146.197         98
207.182.63.37          99
216.35.73.180          100
```



```
KeyboardInterrupt
analysis@analysis-VirtualBox:~/network_security_unit/Lab2$ python assign.py R.csv -countip
Source IP        Number of Occurences
10.5.63.212             1
10.5.63.4               3
10.5.63.34              3
10.5.63.19              3
0.0.0.0                 3
10.5.63.16              5
199.95.210.99           5
199.95.207.173          5
10.5.63.35              7
10.5.63.201             10
10.5.63.39              10
10.5.63.206             10
10.5.63.205             10
10.5.63.203             10
199.170.104.36          12
207.44.165.251          12
199.222.69.4            12
198.232.147.17          13
10.5.63.9               15
206.253.217.8           15
207.46.143.254          18
10.5.63.26              19
10.5.63.15              21
208.10.192.161          21
204.71.201.113          24
206.170.168.217         30
10.5.63.29              32
206.253.217.13          32
10.5.63.10              50
207.5.63.61             51
```

5 it looks like the 10.5.63 prefix dominates with several tens of thousands of occurrences.

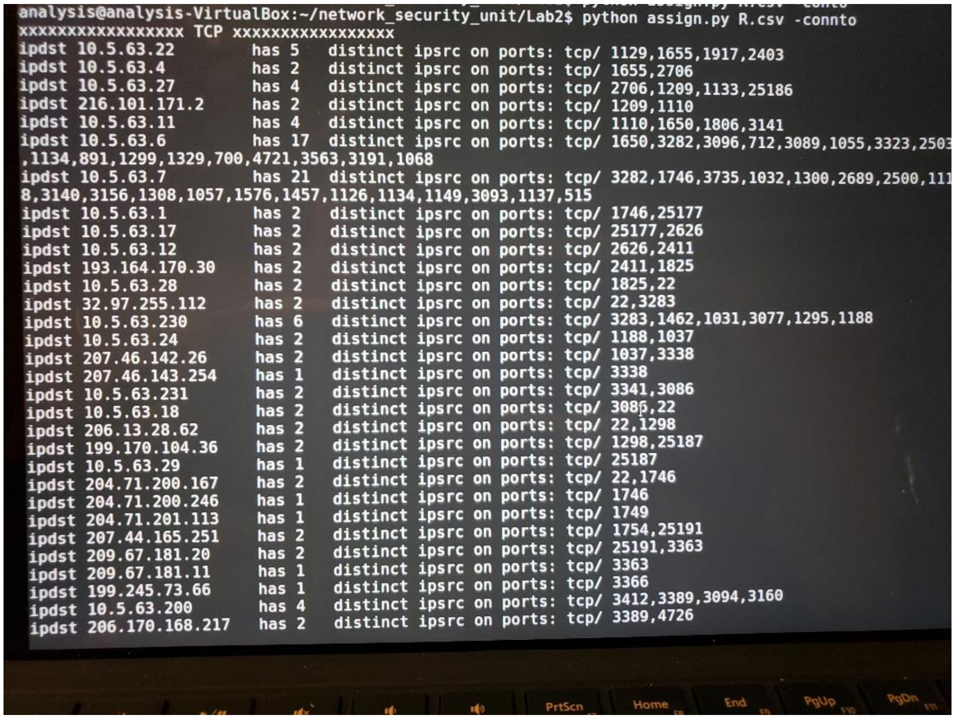
7 Perhaps the 234.142.142 prefix, it has a lot of occurrences as well.

8 Yes, it confirms my suspicions.

9. results below.

10. Yes if you analyze the data see below. The ipdst's with a large amount of distinct ipsources are likely to be the servers, the items with only a few distinct sources are likely to be user computers or printers.

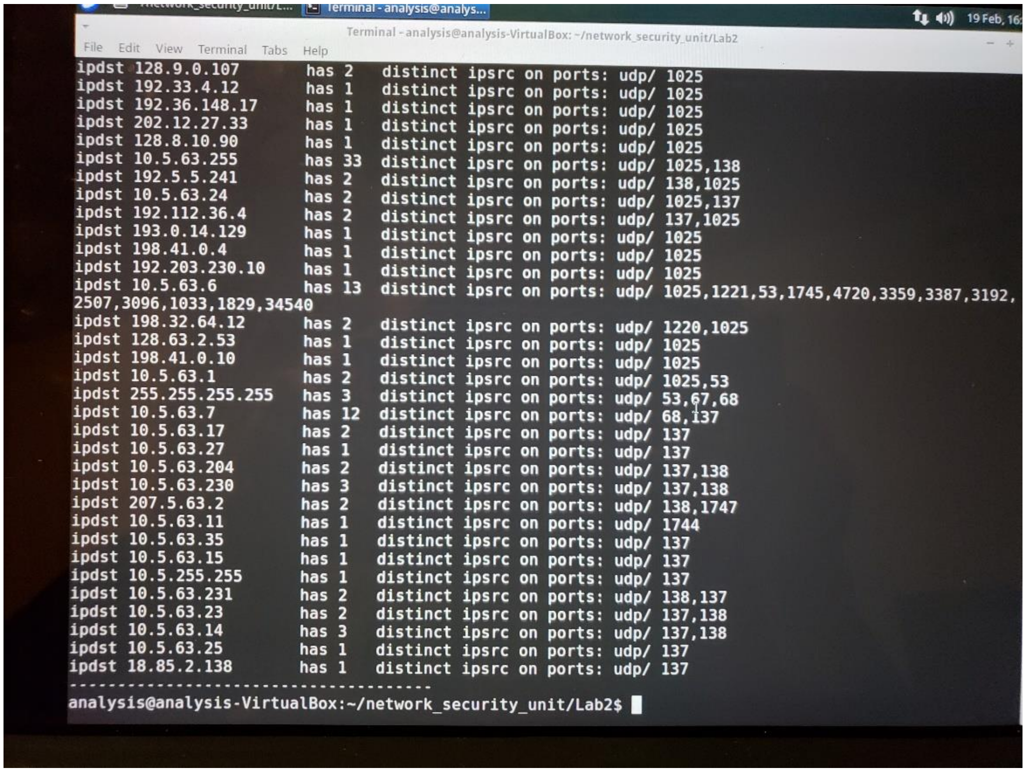
11. I suppose it is a major workplace then, with a multitude of different devices (printers, mail servers, dns servers, computers) involved.



```
analysis@analysis-VirtualBox:~/network_security_unit/Lab2$ python assign.py R.csv -connto
xxxxxxxxxxxxxxxxx TCP xxxxxxxxxxxxxxxxx
ipdst 10.5.63.22        has 5   distinct ipsrc on ports: tcp/ 1129,1655,1917,2403
ipdst 10.5.63.4         has 2   distinct ipsrc on ports: tcp/ 1655,2706
ipdst 10.5.63.27        has 4   distinct ipsrc on ports: tcp/ 2706,1209,1133,25186
ipdst 216.101.171.2     has 2   distinct ipsrc on ports: tcp/ 1209,1110
ipdst 10.5.63.11        has 4   distinct ipsrc on ports: tcp/ 1110,1650,1806,3141
ipdst 10.5.63.6         has 17  distinct ipsrc on ports: tcp/ 1650,3282,3096,712,3089,1055,3323,2503
,1134,891,1299,1329,700,4721,3563,3191,1068
ipdst 10.5.63.7         has 21  distinct ipsrc on ports: tcp/ 3282,1746,3735,1032,1300,2689,2500,111
8,3140,3156,1308,1057,1576,1457,1126,1134,1149,3093,1137,515
ipdst 10.5.63.1         has 2   distinct ipsrc on ports: tcp/ 1746,25177
ipdst 10.5.63.17        has 2   distinct ipsrc on ports: tcp/ 25177,2626
ipdst 10.5.63.12        has 2   distinct ipsrc on ports: tcp/ 2626,2411
ipdst 193.164.170.30    has 2   distinct ipsrc on ports: tcp/ 2411,1825
ipdst 10.5.63.28        has 2   distinct ipsrc on ports: tcp/ 1825,22
ipdst 32.97.255.112     has 2   distinct ipsrc on ports: tcp/ 22,3283
ipdst 10.5.63.230       has 6   distinct ipsrc on ports: tcp/ 3283,1462,1031,3077,1295,1188
ipdst 10.5.63.24        has 2   distinct ipsrc on ports: tcp/ 1188,1037
ipdst 207.46.142.26     has 2   distinct ipsrc on ports: tcp/ 1037,3338
ipdst 207.46.143.254    has 1   distinct ipsrc on ports: tcp/ 3338
ipdst 10.5.63.231       has 2   distinct ipsrc on ports: tcp/ 3341,3086
ipdst 10.5.63.18        has 2   distinct ipsrc on ports: tcp/ 3086,22
ipdst 206.13.28.62      has 2   distinct ipsrc on ports: tcp/ 22,1298
ipdst 199.170.104.36    has 2   distinct ipsrc on ports: tcp/ 1298,25187
ipdst 10.5.63.29        has 1   distinct ipsrc on ports: tcp/ 25187
ipdst 204.71.200.167    has 2   distinct ipsrc on ports: tcp/ 22,1746
ipdst 204.71.200.246    has 1   distinct ipsrc on ports: tcp/ 1746
ipdst 204.71.201.113    has 1   distinct ipsrc on ports: tcp/ 1749
ipdst 207.44.165.251    has 2   distinct ipsrc on ports: tcp/ 1754,25191
ipdst 209.67.181.20     has 2   distinct ipsrc on ports: tcp/ 25191,3363
ipdst 209.67.181.11     has 1   distinct ipsrc on ports: tcp/ 3363
ipdst 199.245.73.66     has 1   distinct ipsrc on ports: tcp/ 3366
ipdst 10.5.63.200       has 4   distinct ipsrc on ports: tcp/ 3412,3389,3094,3160
ipdst 206.170.168.217   has 2   distinct ipsrc on ports: tcp/ 3389,4726
```

-connto for R

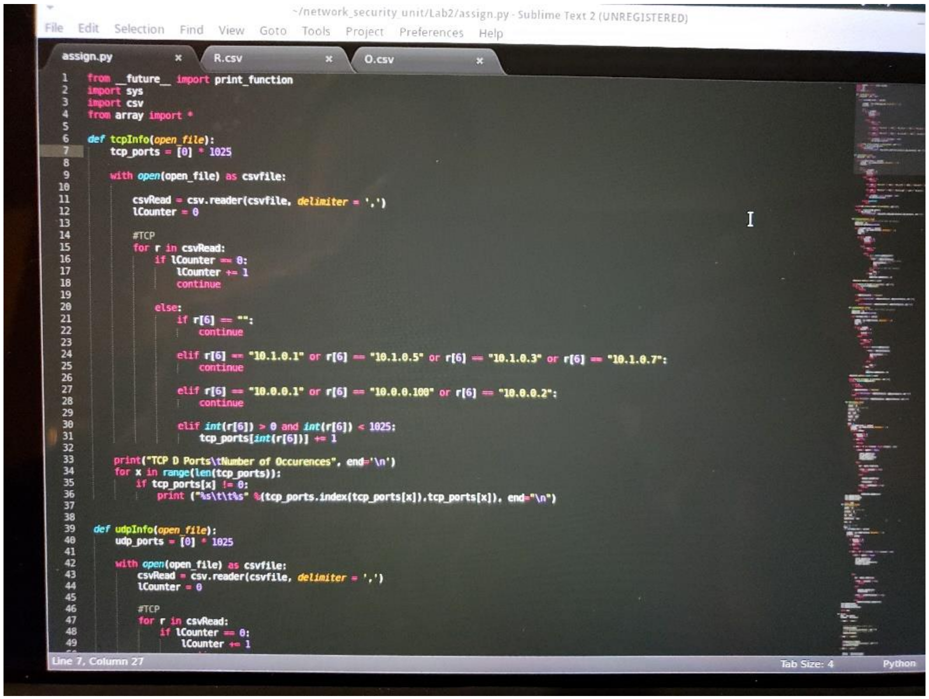
-connto for O



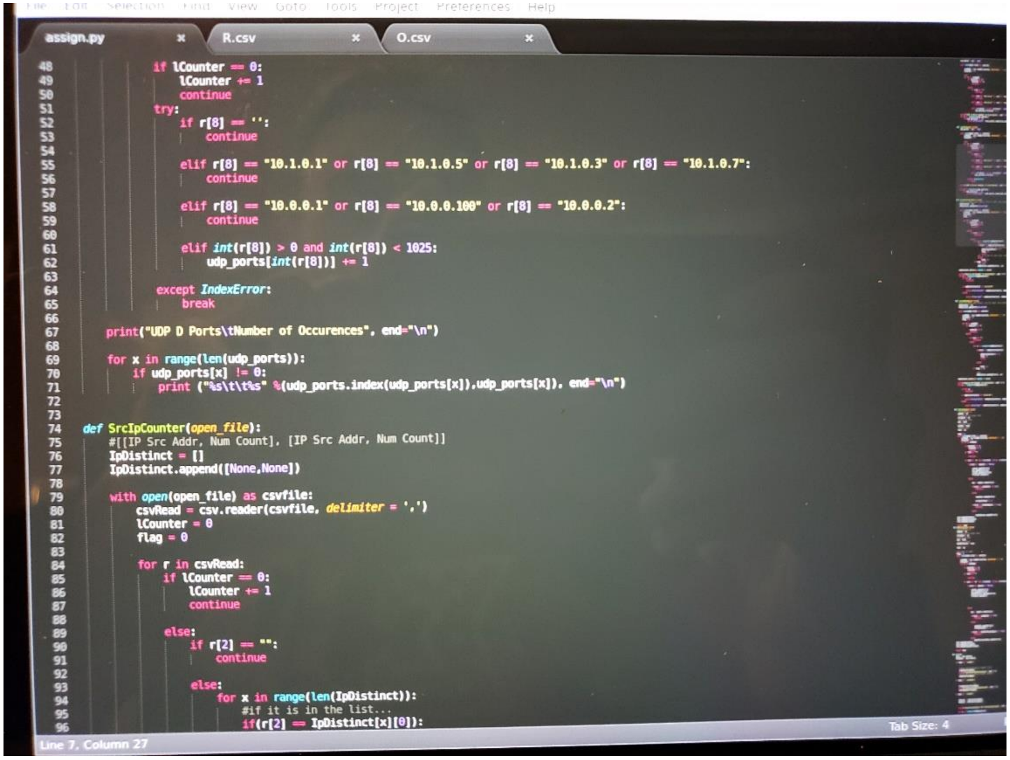
Terminal - analysis@analys...
19 Feb, 16
Terminal - analysis@analysis-VirtualBox: ~/network_security_unit/Lab2
File
Edit
View
Terminal
Tabs
Help

```
ipdst 128.9.0.107       has 2   distinct ipsrc on ports: udp/ 1025
ipdst 192.33.4.12       has 1   distinct ipsrc on ports: udp/ 1025
ipdst 192.36.148.17     has 1   distinct ipsrc on ports: udp/ 1025
ipdst 202.12.27.33      has 1   distinct ipsrc on ports: udp/ 1025
ipdst 128.8.10.90       has 1   distinct ipsrc on ports: udp/ 1025
ipdst 10.5.63.255       has 33  distinct ipsrc on ports: udp/ 1025,138
ipdst 192.5.5.241       has 2   distinct ipsrc on ports: udp/ 138,1025
ipdst 10.5.63.24        has 2   distinct ipsrc on ports: udp/ 1025,137
ipdst 192.112.36.4      has 2   distinct ipsrc on ports: udp/ 137,1025
ipdst 193.0.14.129      has 1   distinct ipsrc on ports: udp/ 1025
ipdst 198.41.0.4        has 1   distinct ipsrc on ports: udp/ 1025
ipdst 192.203.230.10    has 1   distinct ipsrc on ports: udp/ 1025
ipdst 10.5.63.6         has 13  distinct ipsrc on ports: udp/ 1025,1221,53,1745,4720,3359,3387,3192,
2507,3096,1033,1829,34540
ipdst 198.32.64.12      has 2   distinct ipsrc on ports: udp/ 1220,1025
ipdst 128.63.2.53       has 1   distinct ipsrc on ports: udp/ 1025
ipdst 198.41.0.10       has 1   distinct ipsrc on ports: udp/ 1025
ipdst 10.5.63.1         has 2   distinct ipsrc on ports: udp/ 1025,53
ipdst 255.255.255.255   has 3   distinct ipsrc on ports: udp/ 53,67,68
ipdst 10.5.63.7         has 12  distinct ipsrc on ports: udp/ 68,137
ipdst 10.5.63.17        has 2   distinct ipsrc on ports: udp/ 137
ipdst 10.5.63.27        has 1   distinct ipsrc on ports: udp/ 137
ipdst 10.5.63.204       has 2   distinct ipsrc on ports: udp/ 137,138
ipdst 10.5.63.230       has 3   distinct ipsrc on ports: udp/ 137,138
ipdst 207.5.63.2        has 2   distinct ipsrc on ports: udp/ 138,1747
ipdst 10.5.63.11        has 1   distinct ipsrc on ports: udp/ 1744
ipdst 10.5.63.35        has 1   distinct ipsrc on ports: udp/ 137
ipdst 10.5.63.15        has 1   distinct ipsrc on ports: udp/ 137
ipdst 10.5.255.255      has 1   distinct ipsrc on ports: udp/ 137
ipdst 10.5.63.231       has 2   distinct ipsrc on ports: udp/ 138,137
ipdst 10.5.63.23        has 2   distinct ipsrc on ports: udp/ 137,138
ipdst 10.5.63.14        has 3   distinct ipsrc on ports: udp/ 137,138
ipdst 10.5.63.25        has 1   distinct ipsrc on ports: udp/ 137
ipdst 18.85.2.138       has 1   distinct ipsrc on ports: udp/ 137
----------------------------------------
analysis@analysis-VirtualBox:~/network_security_unit/Lab2$ 
```

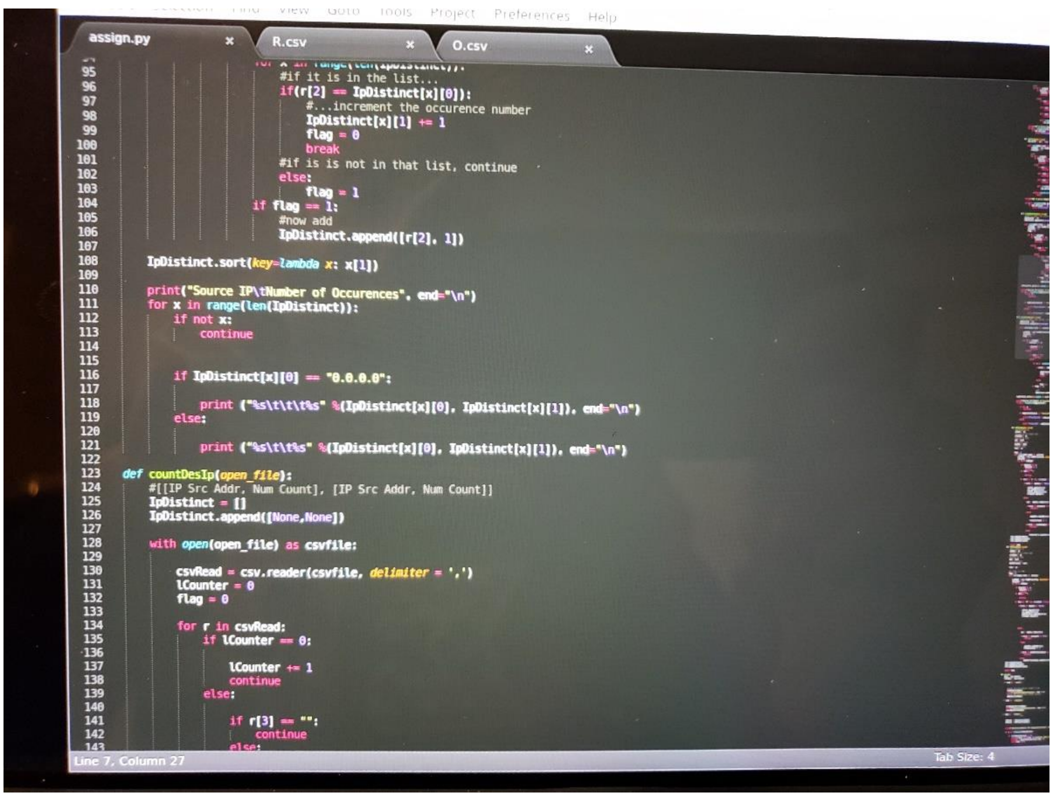
CODE:


~/network_security_unit/Lab2/assign.py - Sublime Text 2 (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
assign.py
R.csv
O.csv
Line 7, Column 27
Tab Size: 4
Python

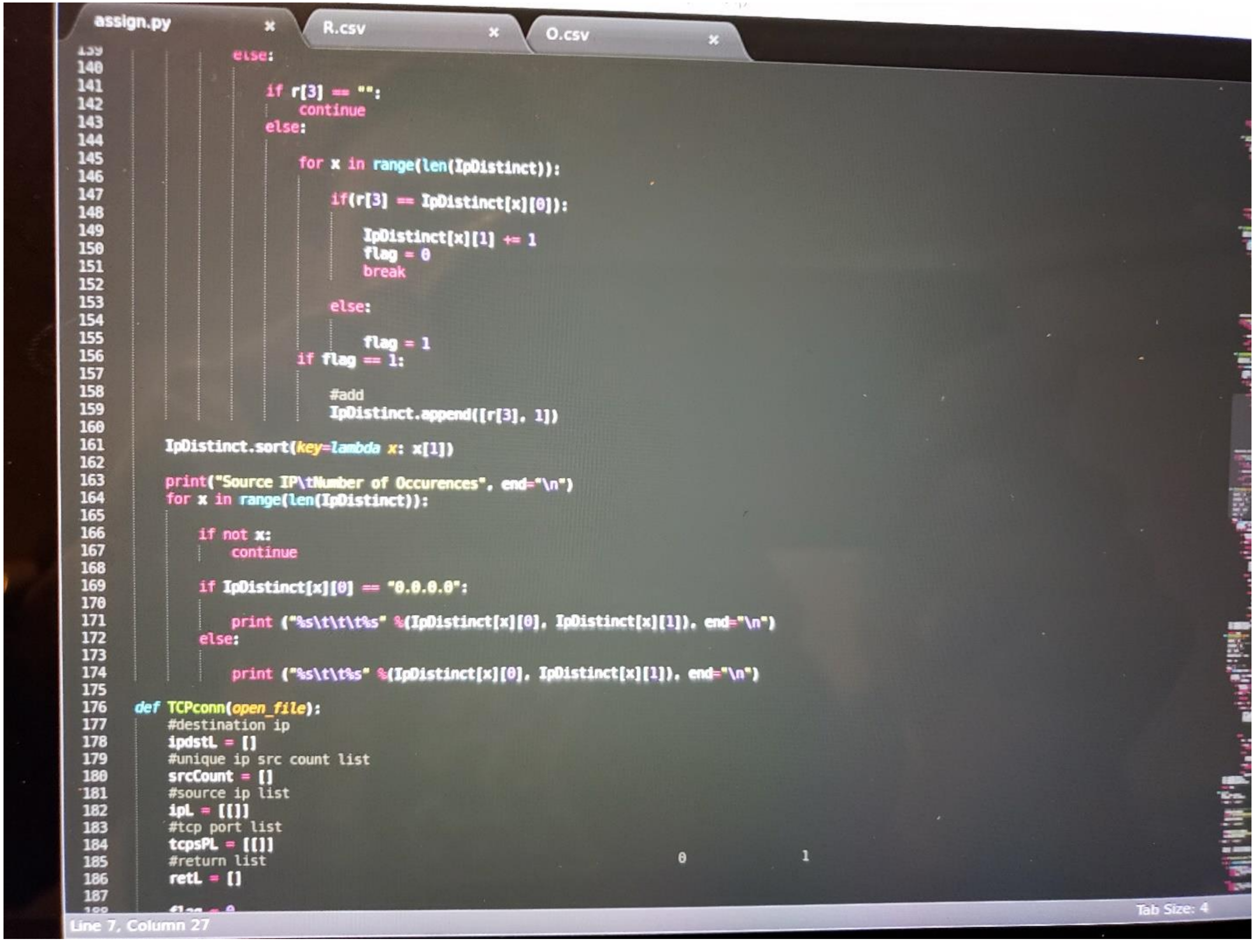
```
from __future__ import print_function
import sys
import csv
from array import *

def tcpInfo(open_file):
    tcp_ports = [0] * 1025

    with open(open_file) as csvfile:

        csvRead = csv.reader(csvfile, delimiter = ',')
        lCounter = 0

        #TCP
        for r in csvRead:
            if lCounter == 0:
                lCounter += 1
                continue

            else:
                if r[6] == "":
                    continue

                elif r[6] == "10.1.0.1" or r[6] == "10.1.0.5" or r[6] == "10.1.0.3" or r[6] == "10.1.0.7":
                    continue

                elif r[6] == "10.0.0.1" or r[6] == "10.0.0.100" or r[6] == "10.0.0.2":
                    continue

                elif int(r[6]) > 0 and int(r[6]) < 1025:
                    tcp_ports[int(r[6])] += 1

    print("TCP D Ports\tNumber of Occurences", end='\n')
    for x in range(len(tcp_ports)):
        if tcp_ports[x] != 0:
            print ("%s\t\t%s" %(tcp_ports.index(tcp_ports[x]),tcp_ports[x]), end="\n")


def udpInfo(open_file):
    udp_ports = [0] * 1025

    with open(open_file) as csvfile:
        csvRead = csv.reader(csvfile, delimiter = ',')
        lCounter = 0

        #TCP
        for r in csvRead:
            if lCounter == 0:
                lCounter += 1
```


File Edit Selection Find View Goto Tools Project Preferences Help
assign.py
R.csv
O.csv
Line 7, Column 27
Tab Size: 4

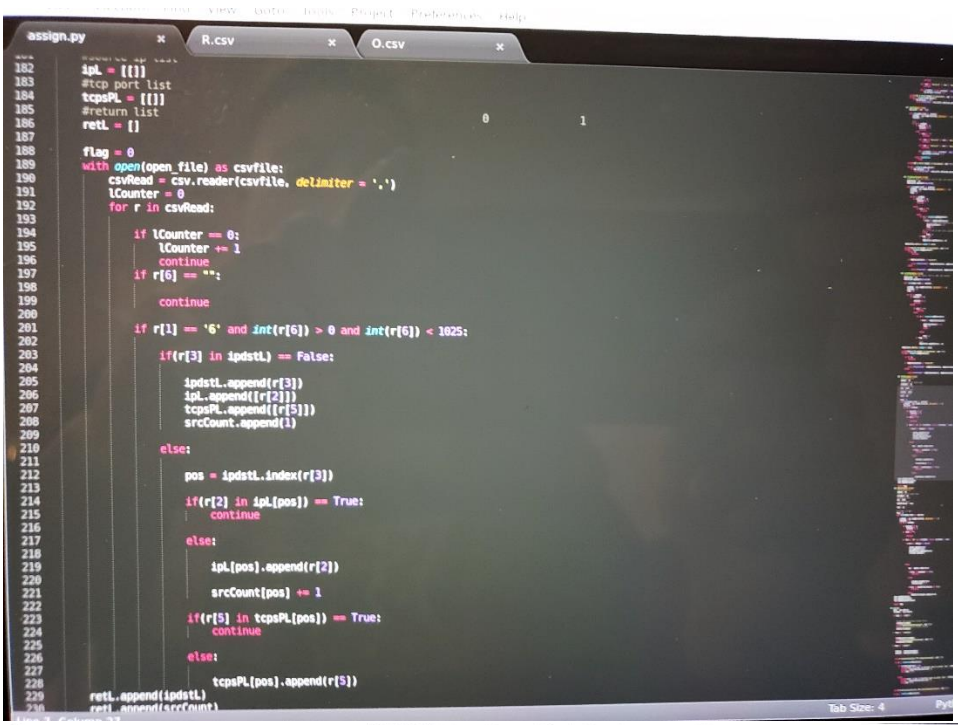
```
            if lCounter == 0:
                lCounter += 1
                continue
            try:
                if r[8] == '':
                    continue

                elif r[8] == "10.1.0.1" or r[8] == "10.1.0.5" or r[8] == "10.1.0.3" or r[8] == "10.1.0.7":
                    continue

                elif r[8] == "10.0.0.1" or r[8] == "10.0.0.100" or r[8] == "10.0.0.2":
                    continue

                elif int(r[8]) > 0 and int(r[8]) < 1025:
                    udp_ports[int(r[8])] += 1

            except IndexError:
                break

    print("UDP D Ports\tNumber of Occurences", end="\n")

    for x in range(len(udp_ports)):
        if udp_ports[x] != 0:
            print ("%s\t\t%s" %(udp_ports.index(udp_ports[x]),udp_ports[x]), end="\n")


def SrcIpCounter(open_file):
    #[[IP Src Addr, Num Count], [IP Src Addr, Num Count]]
    IpDistinct = []
    IpDistinct.append([None,None])

    with open(open_file) as csvfile:
        csvRead = csv.reader(csvfile, delimiter = ',')
        lCounter = 0
        flag = 0

        for r in csvRead:
            if lCounter == 0:
                lCounter += 1
                continue

            else:
                if r[2] == "":
                    continue

                else:
                    for x in range(len(IpDistinct)):
                        #if it is in the list...
                        if(r[2] == IpDistinct[x][0]):
```



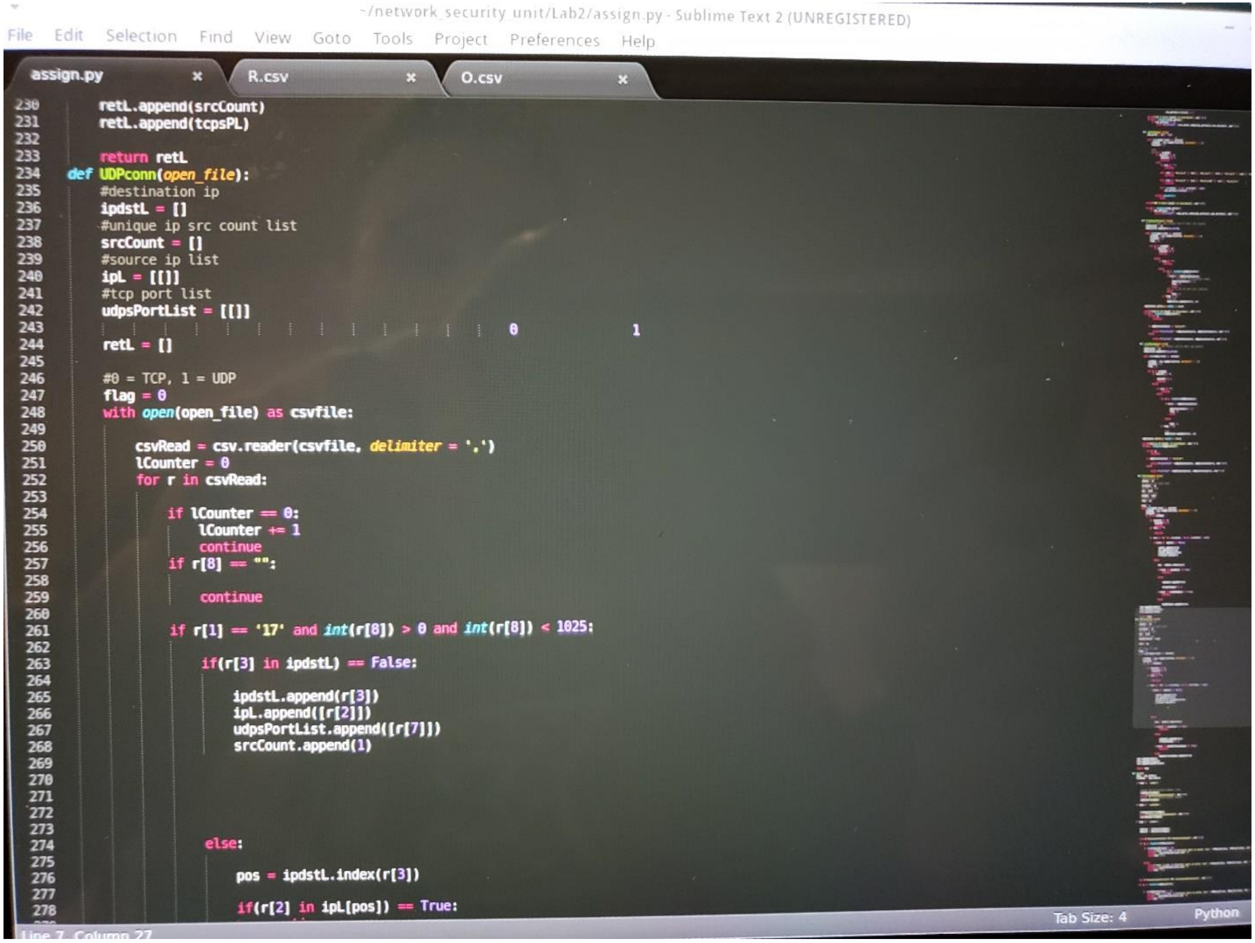
```python
                    for x in range(len(IpDistinct)):
                        #if it is in the list...
                        if(r[2] == IpDistinct[x][0]):
                            #...increment the occurence number
                            IpDistinct[x][1] += 1
                            flag = 0
                            break
                        #if is is not in that list, continue
                        else:
                            flag = 1
                    if flag == 1:
                        #now add
                        IpDistinct.append([r[2], 1])

    IpDistinct.sort(key=lambda x: x[1])

    print("Source IP\tNumber of Occurences", end="\n")
    for x in range(len(IpDistinct)):
        if not x:
            continue


        if IpDistinct[x][0] == "0.0.0.0":

            print ("%s\t\t\t%s" %(IpDistinct[x][0], IpDistinct[x][1]), end="\n")
        else:

            print ("%s\t\t%s" %(IpDistinct[x][0], IpDistinct[x][1]), end="\n")

def countDesIp(open_file):
    #[[IP Src Addr, Num Count], [IP Src Addr, Num Count]]
    IpDistinct = []
    IpDistinct.append([None,None])

    with open(open_file) as csvfile:

        csvRead = csv.reader(csvfile, delimiter = ',')
        lCounter = 0
        flag = 0

        for r in csvRead:
            if lCounter == 0:

                lCounter += 1
                continue
            else:

                if r[3] == "":
                    continue
                else:
```



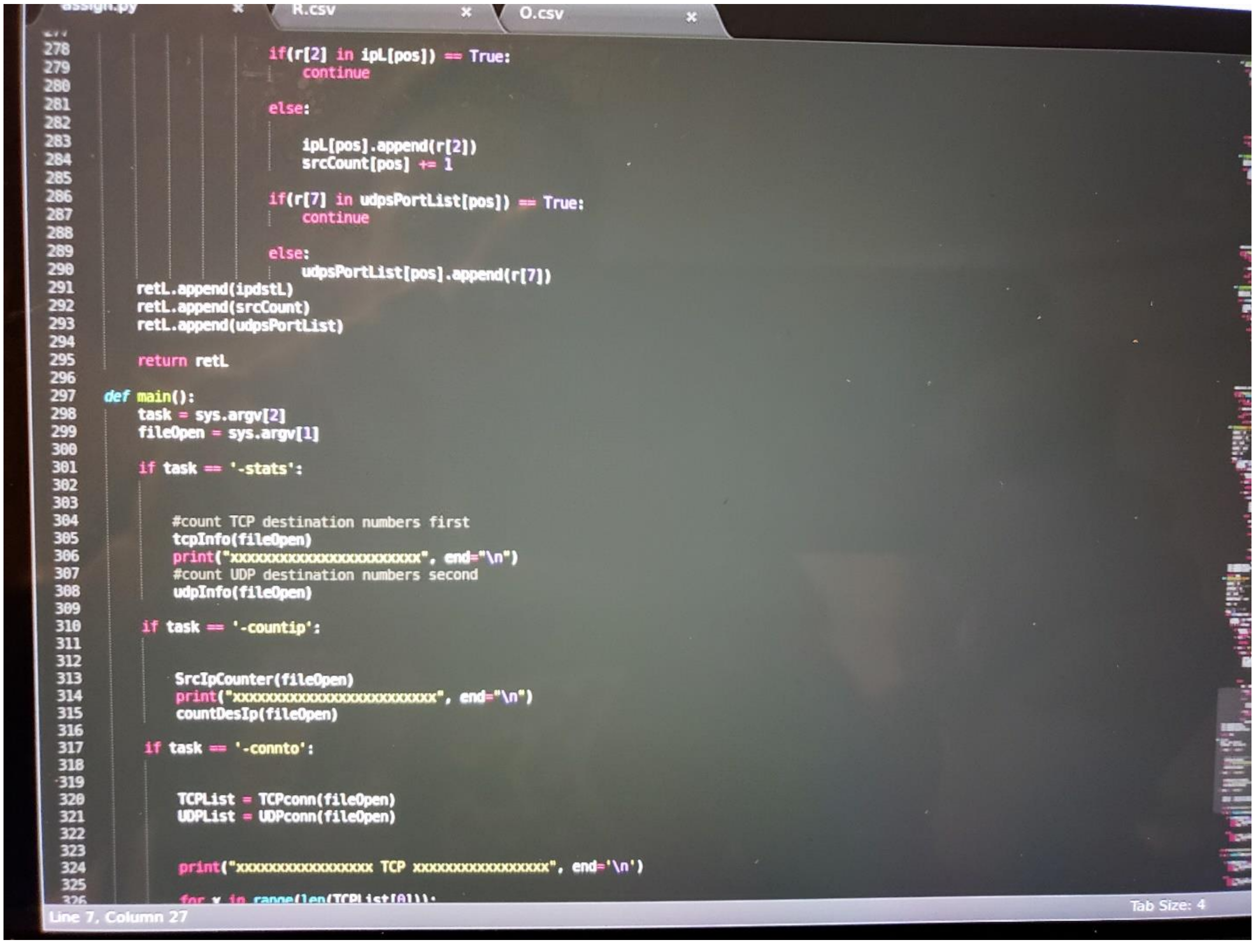
```python
            else:

                if r[3] == "":
                    continue
                else:

                    for x in range(len(IpDistinct)):

                        if(r[3] == IpDistinct[x][0]):

                            IpDistinct[x][1] += 1
                            flag = 0
                            break

                        else:

                            flag = 1
                    if flag == 1:

                        #add
                        IpDistinct.append([r[3], 1])

    IpDistinct.sort(key=lambda x: x[1])

    print("Source IP\tNumber of Occurences", end="\n")
    for x in range(len(IpDistinct)):

        if not x:
            continue

        if IpDistinct[x][0] == "0.0.0.0":

            print ("%s\t\t\t%s" %(IpDistinct[x][0], IpDistinct[x][1]), end="\n")
        else:

            print ("%s\t\t%s" %(IpDistinct[x][0], IpDistinct[x][1]), end="\n")

def TCPconn(open_file):
    #destination ip
    ipdstL = []
    #unique ip src count list
    srcCount = []
    #source ip list
    ipL = [[]]
    #tcp port list
    tcpsPL = [[]]
    #return list
    retL = []

    flag = 0
```


File Selection Find View Goto Tools Project Preferences Help
assign.py
R.csv
O.csv
Tab Size: 4
Python
Line 7, Column 27

```
    #source ip list
    ipL = [[]]
    #tcp port list
    tcpsPL = [[]]
    #return list
    retL = []                                          0            1

    flag = 0
    with open(open_file) as csvfile:
        csvRead = csv.reader(csvfile, delimiter = ',')
        lCounter = 0
        for r in csvRead:

            if lCounter == 0:
                lCounter += 1
                continue
            if r[6] == "":

                continue

            if r[1] == '6' and int(r[6]) > 0 and int(r[6]) < 1025:

                if(r[3] in ipdstL) == False:

                    ipdstL.append(r[3])
                    ipL.append([r[2]])
                    tcpsPL.append([r[5]])
                    srcCount.append(1)

                else:

                    pos = ipdstL.index(r[3])

                    if(r[2] in ipL[pos]) == True:
                        continue

                    else:

                        ipL[pos].append(r[2])

                        srcCount[pos] += 1

                    if(r[5] in tcpsPL[pos]) == True:
                        continue

                    else:

                        tcpsPL[pos].append(r[5])
    retL.append(ipdstL)
    retL.append(srcCount)
```


~/network_security_unit/Lab2/assign.py - Sublime Text 2 (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
assign.py
R.csv
O.csv
Tab Size: 4
Python
Line 7, Column 27

```
    retL.append(srcCount)
    retL.append(tcpsPL)

    return retL
def UDPconn(open_file):
    #destination ip
    ipdstL = []
    #unique ip src count list
    srcCount = []
    #source ip list
    ipL = [[]]
    #tcp port list
    udpsPortList = [[]]
                                                  0            1
    retL = []

    #0 = TCP, 1 = UDP
    flag = 0
    with open(open_file) as csvfile:

        csvRead = csv.reader(csvfile, delimiter = ',')
        lCounter = 0
        for r in csvRead:

            if lCounter == 0:
                lCounter += 1
                continue
            if r[8] == "":

                continue

            if r[1] == '17' and int(r[8]) > 0 and int(r[8]) < 1025:

                if(r[3] in ipdstL) == False:

                    ipdstL.append(r[3])
                    ipL.append([r[2]])
                    udpsPortList.append([r[7]])
                    srcCount.append(1)




                else:

                    pos = ipdstL.index(r[3])

                    if(r[2] in ipL[pos]) == True:
```



```python
                    if(r[2] in ipL[pos]) == True:
                        continue

                    else:

                        ipL[pos].append(r[2])
                        srcCount[pos] += 1

                    if(r[7] in udpsPortList[pos]) == True:
                        continue

                    else:
                        udpsPortList[pos].append(r[7])
    retL.append(ipdstL)
    retL.append(srcCount)
    retL.append(udpsPortList)

    return retL

def main():
    task = sys.argv[2]
    fileOpen = sys.argv[1]

    if task == '-stats':


        #count TCP destination numbers first
        tcpInfo(fileOpen)
        print("xxxxxxxxxxxxxxxxxxxxxxx", end="\n")
        #count UDP destination numbers second
        udpInfo(fileOpen)

    if task == '-countip':


        SrcIpCounter(fileOpen)
        print("xxxxxxxxxxxxxxxxxxxxxxxxxx", end="\n")
        countDesIp(fileOpen)

    if task == '-connto':


        TCPList = TCPconn(fileOpen)
        UDPList = UDPconn(fileOpen)


        print("xxxxxxxxxxxxxxxxx TCP xxxxxxxxxxxxxxxxx", end='\n')

        for x in range(len(TCPList[0])):
```