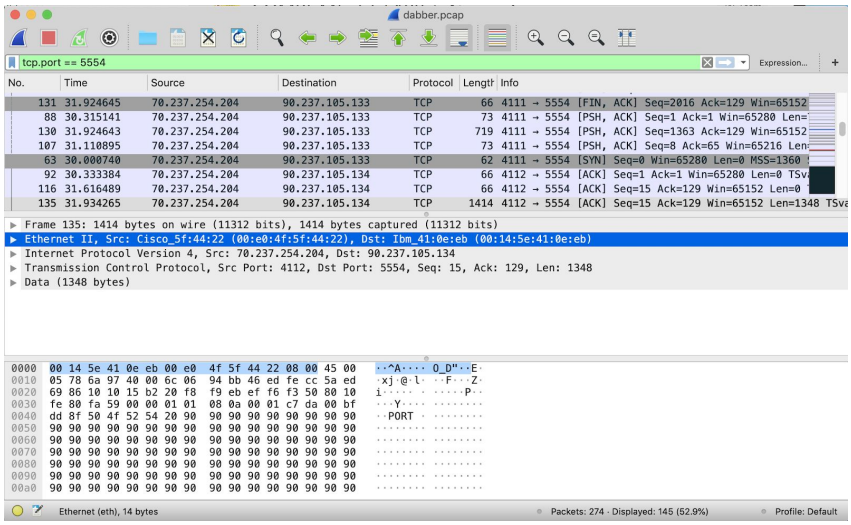
Week 6

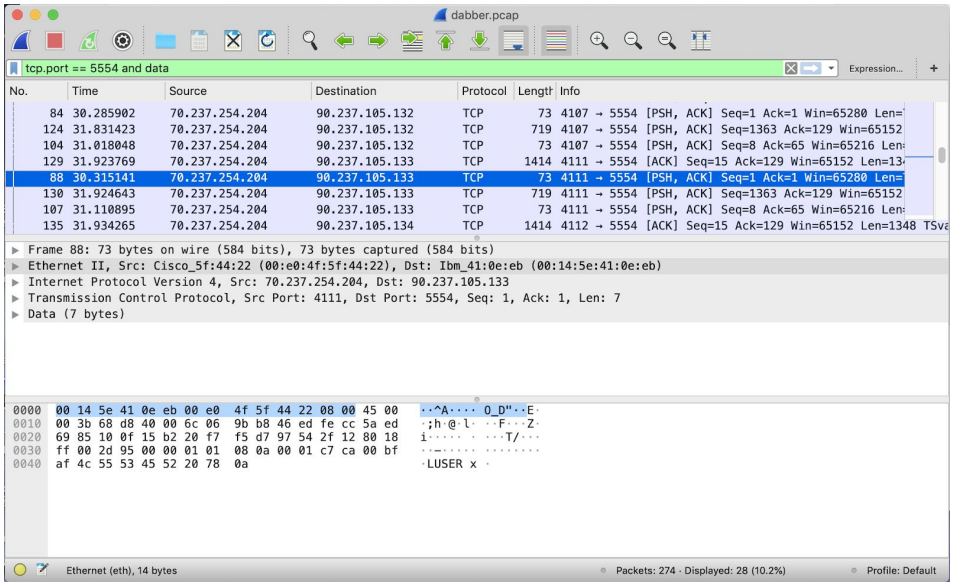
0. First we should hash the evidence file using an md5 hash.

```
Claires-MBP:Desktop claire.fei$ md5sum dabber.pcap
78f36ff84d63fc7da70c1b5052175e96  dabber.pcap
```

1. Inspect Ports 5554 by applying the filter “tcp.port == 5554”. This allows us to see anything interacting with that port which would be useful due to the nature of the dabber malware which was given to us to target that port first.

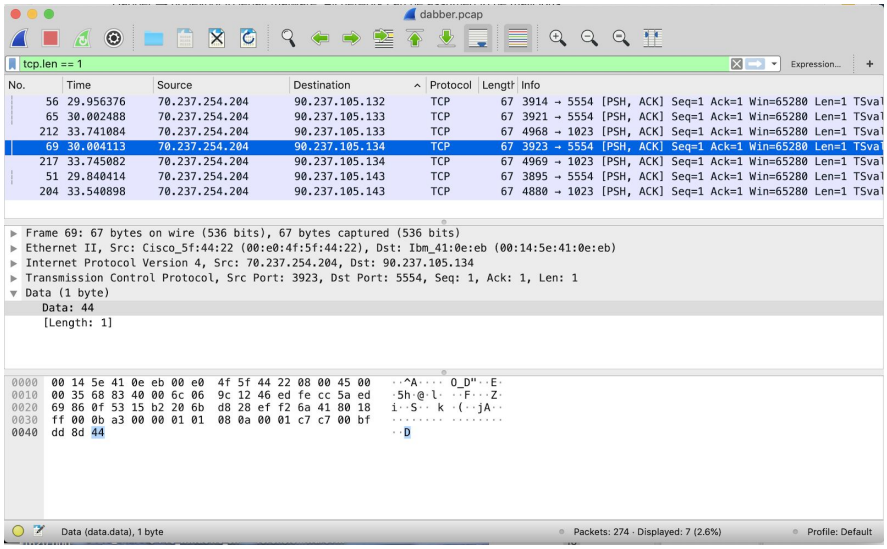


2. As there is a lot of data shown, we want to further filter down more tightly. As such, we apply the filter “tcp.port == 5554 and data” to only capture those transmitting data as those would be the ones that contain useful information to us.

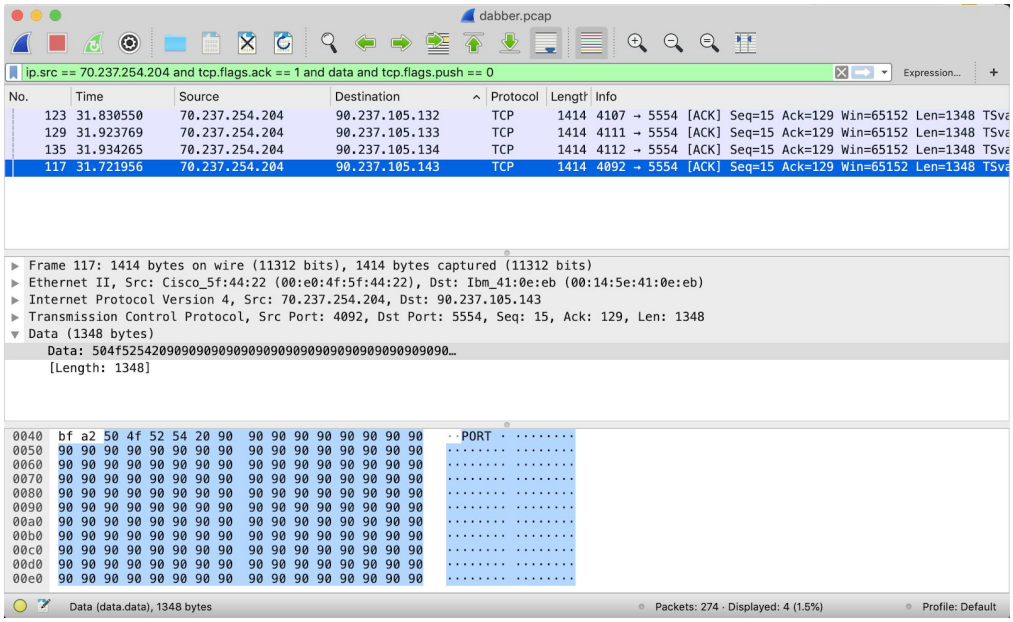


We can see that the source ip is the same, however the destination ip varies. This implies that ip 70.237.254.204 is the attacking source who is trying different computers (as seen by the varying destination ips).

3. Changing the filter to “tcp.len == 1” we can see all the packets that had a packet length of 1, and viewing each of these we can see that it sent a “D“ which lines up with the report on how dabber works, sending a “D” to test whether a computer has already been infected with Sasser. (This can be seen at the bottom where the D is highlighted in blue with hex 44).

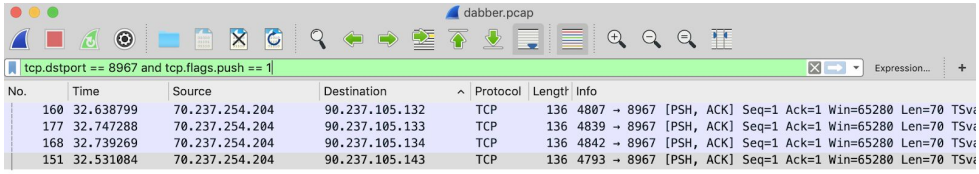


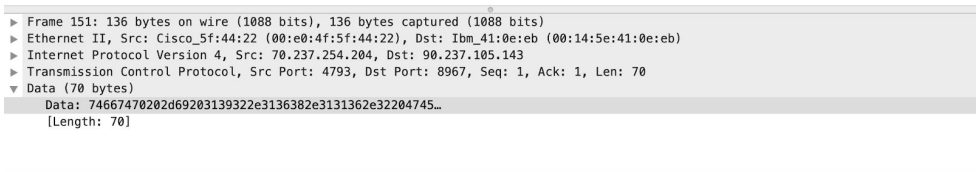
4. Next we can imply the filter “ip.src == 70.237.254.204 and tcp.flags.ack == 1 and data and tcp.flags.push == 0” to filter by the attacking IP with packets that acknowledge the receipt of data and packets that have data. This allows us to find packets that may be of use as they contain data.

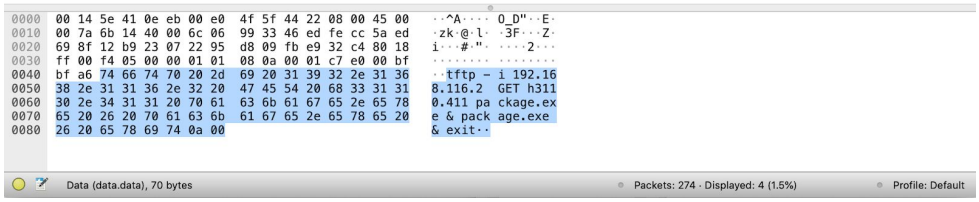


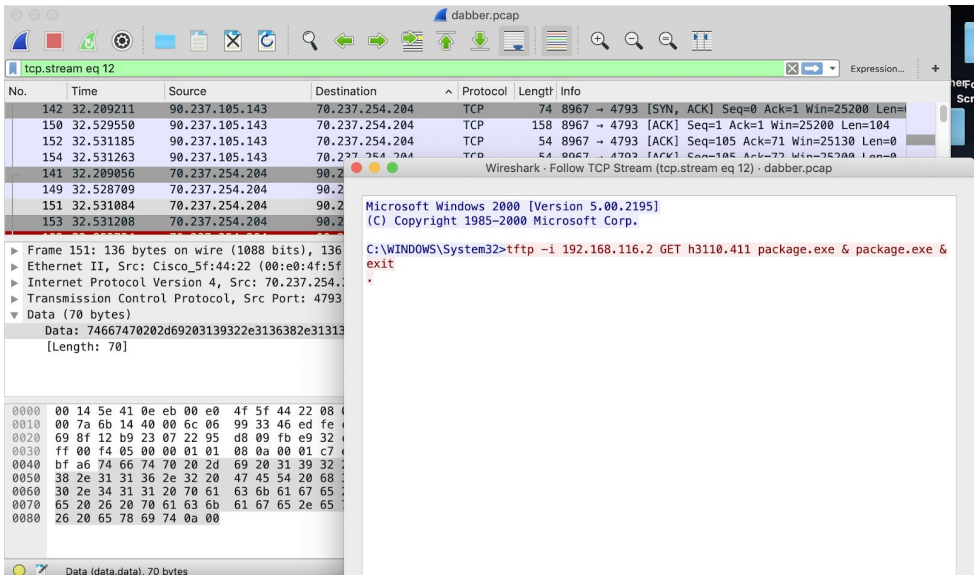
It is quite obvious that there is something suspicious occurring in these packets as we can see the data contains a lot of hex “90”s which is indicative of a nopsled, a common technique that often leads into shell code to exploit a computer.

5. Given we know the way dabber works in opening a port on 8967, we can filter by these specific ports and investigate. In the second photo below, we can see the command that was viciously executed.



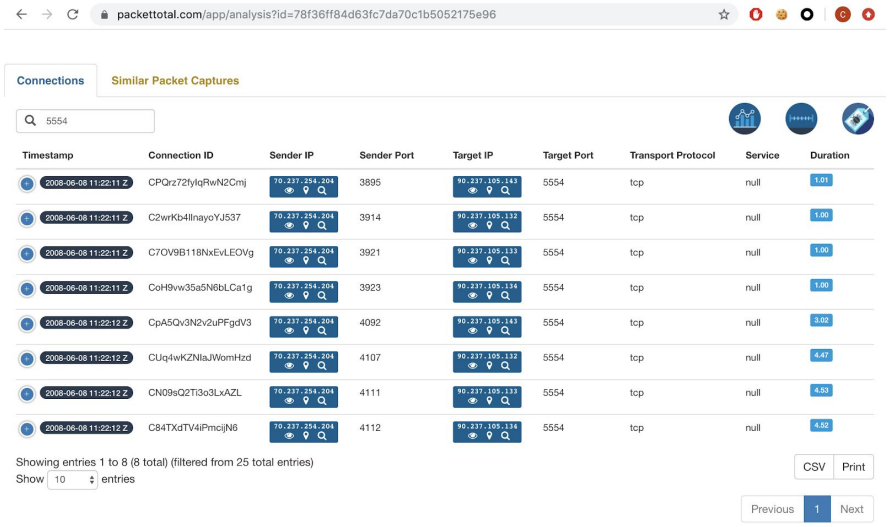




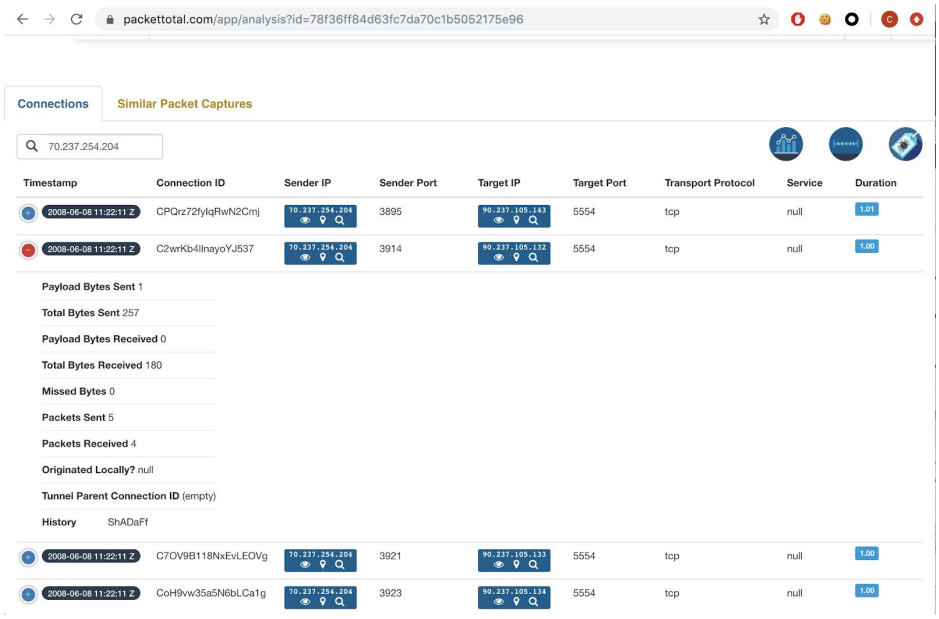


The procedure will now be repeated using a different tool to verify the process and results. The chosen tool is an online tool called “PacketTotal”. This will be a briefer version of the same investigation above to see if we can get the same results. First we hash it similarly as above. Then we filter by the known port that dabber attacks to check if sasser has already infected the

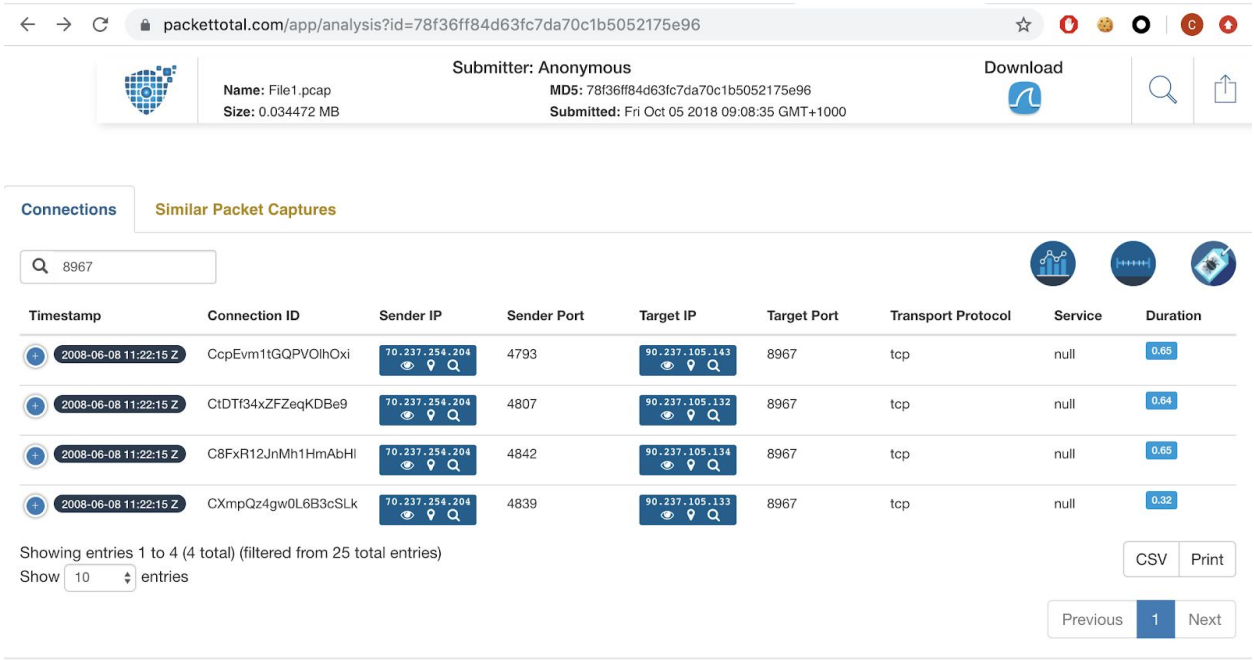
device. We can see below that a lot of results have been returned, all originating from the same IP with differing destination IPs, similar to the wireshark analysis.



Then, filtering by that IP as a sender IP, we can see that it is indeed sending the 1 byte of test packets to test the Sasser infection. This can be seen in the information “Payload Bytes Sent 1”



Next we investigate the port that we know that Dabber opens when infecting the computer, we receive the same four results from the wireshark analysis. Hence confirming the same results as the more thorough and detailed investigation as above that four computers were infected with Dabber.



Hence the answer to the question "how many computers were infected" is 4 as seen through the investigation above.