

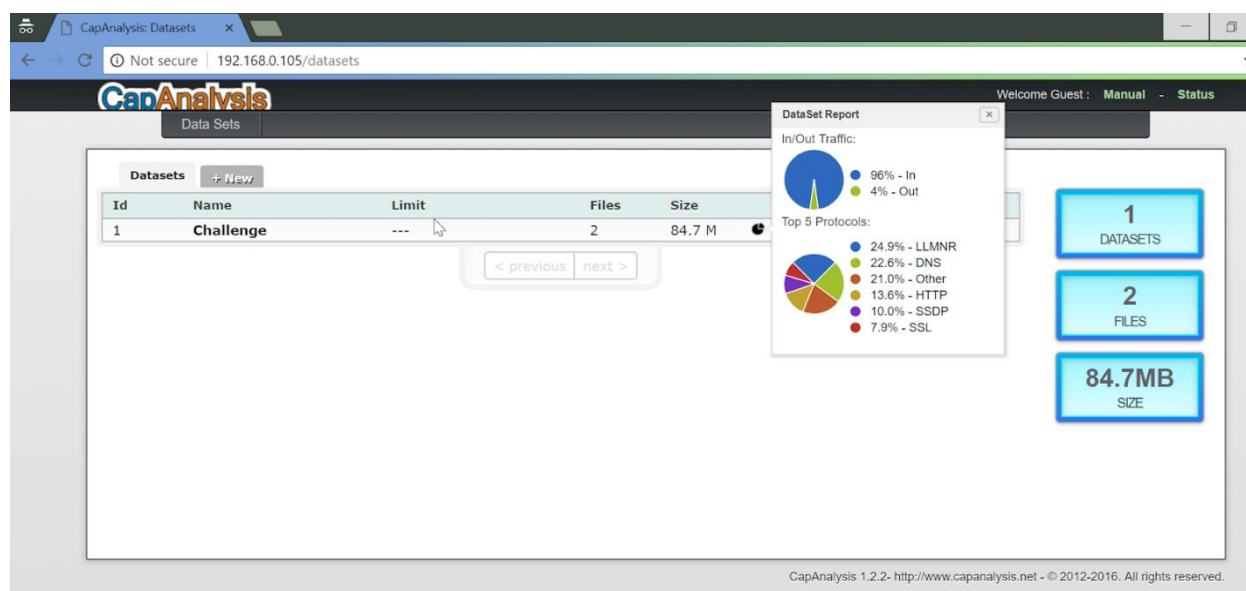
[illegible]

| | |
|-------------|---|
| Name | Capanalysis Basics |
| URL | https://www.attackdefense.com/challengedetails?cid=6 |
| Type | Traffic Analysis: Tshark Fu |

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

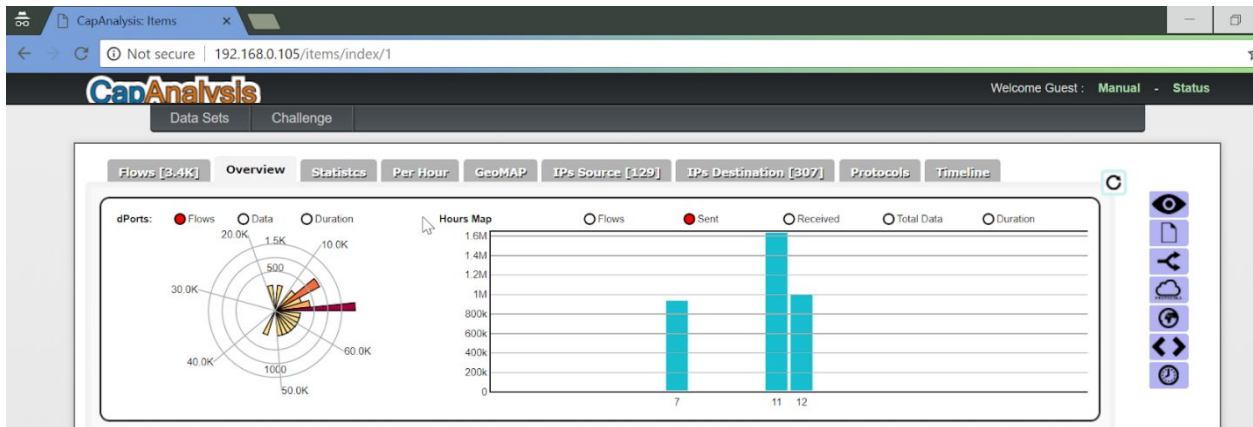
Q1. Out of total traffic, what is the percentage of outbound traffic?

Answer: 4%



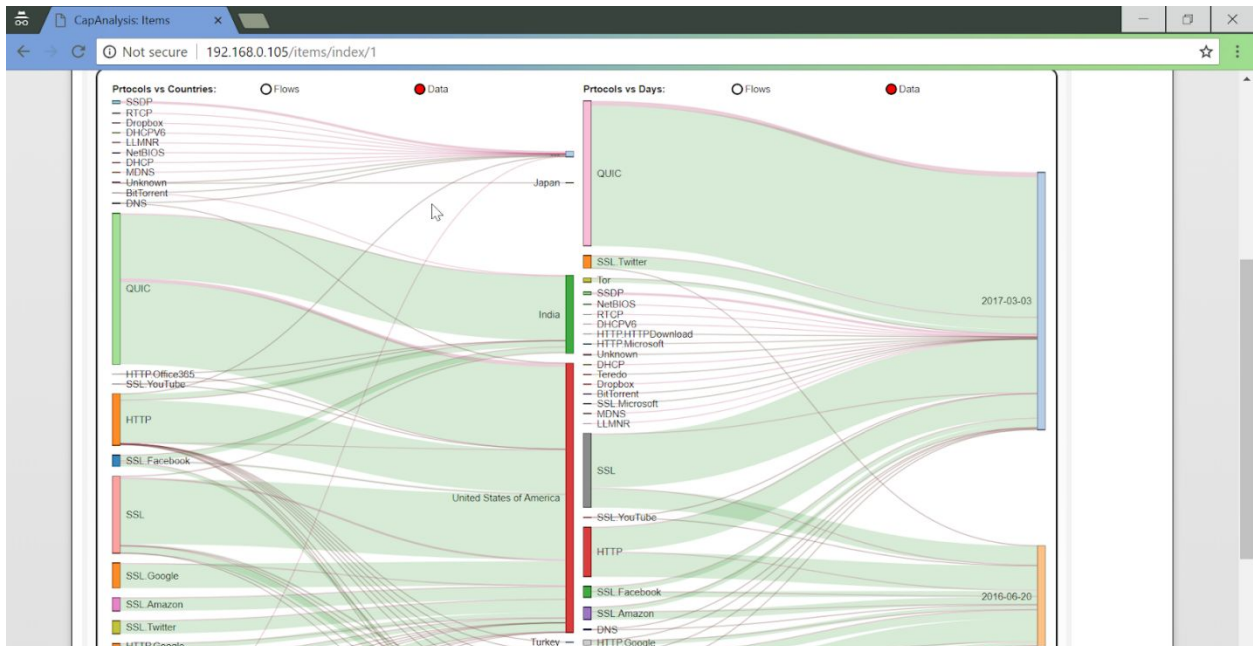
Q2. During which hour the outbound traffic volume was highest?

Answer: 11



Q3. Most of the traffic belongs to which protocol?

Answer: QUIC



Q4. Which IP address is responsible for highest data sent?

Answer: 192.168.10.9



Q5. How many bytes were sent from IP 192.168.0.102?

Answer: 24.5

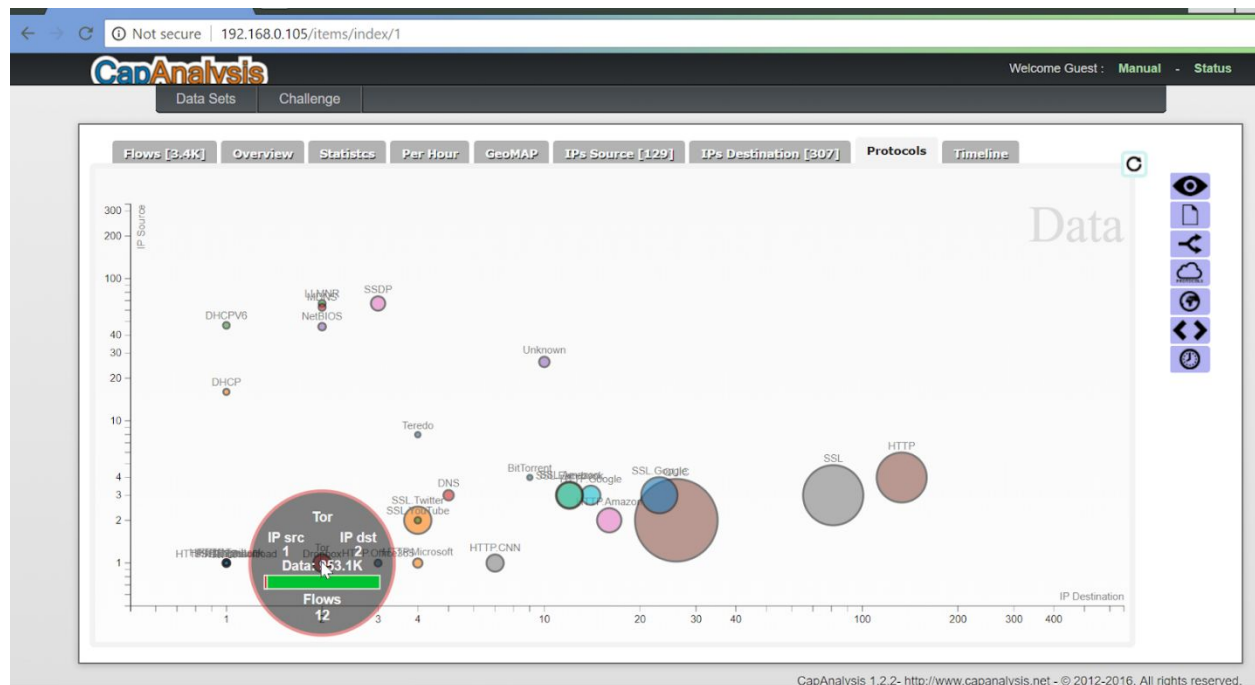
The figure displays a table of network flow statistics from the CapAnalysis interface. The table has five columns: IP, Flows, Bytes Sent, Bytes Received, and Pies %. The 'Overview' tab is selected.

| IP | Flows | Bytes Sent | Bytes Received | Pies % |
|---------------------------|-------|------------|----------------|--------|
| 192.168.252.128 | 1.2K | 930.4 K | 21 M | |
| 192.168.0.136 | 434 | 741.1 K | 18.9 M | |
| 192.168.10.9 | 411 | 969.2 K | 34.1 M | |
| fe80::79ca:ac8a:96e3:93d8 | 130 | 17.2 K | 0 | |
| 192.168.0.165 | 41 | 40.1 K | 0 | |
| 192.168.0.97 | 41 | 17 K | 0 | |
| 192.168.0.89 | 40 | 18.6 K | 0 | |
| 192.168.0.96 | 40 | 34.6 K | 0 | |
| 192.168.0.126 | 38 | 13.3 K | 0 | |
| 192.168.0.125 | 35 | 9.3 K | 0 | |
| fe80::d4cc:a7fd:340e:cde2 | 34 | 6.6 K | 0 | |
| 192.168.0.102 | 34 | 24.5 K | 0 | |
| fe80::903a:9266:7d9a:39f1 | 31 | 30.7 K | 0 | |

At the bottom of the table, there is a pagination control showing 'previous', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'next', and a 'Go' button.

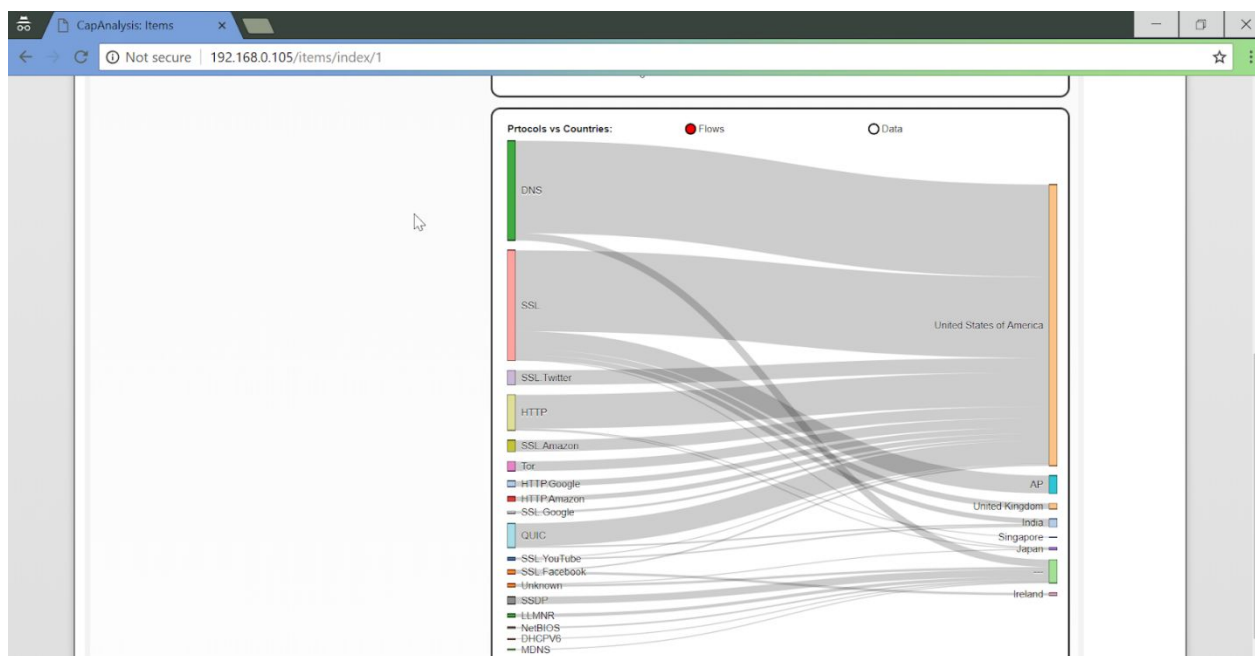
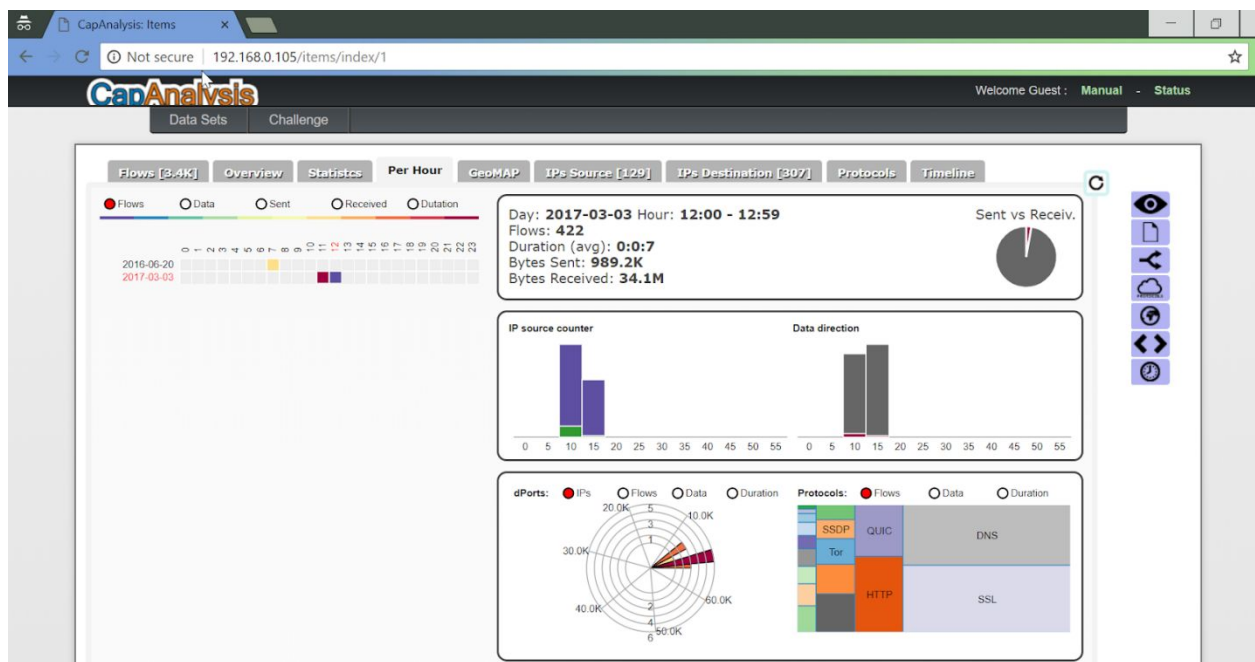
Q6. The traffic seems to contain some packets/flows from privacy protection technique (or anonymizer solution). Can you identify the technique/solution/tool?

Answer: TOR



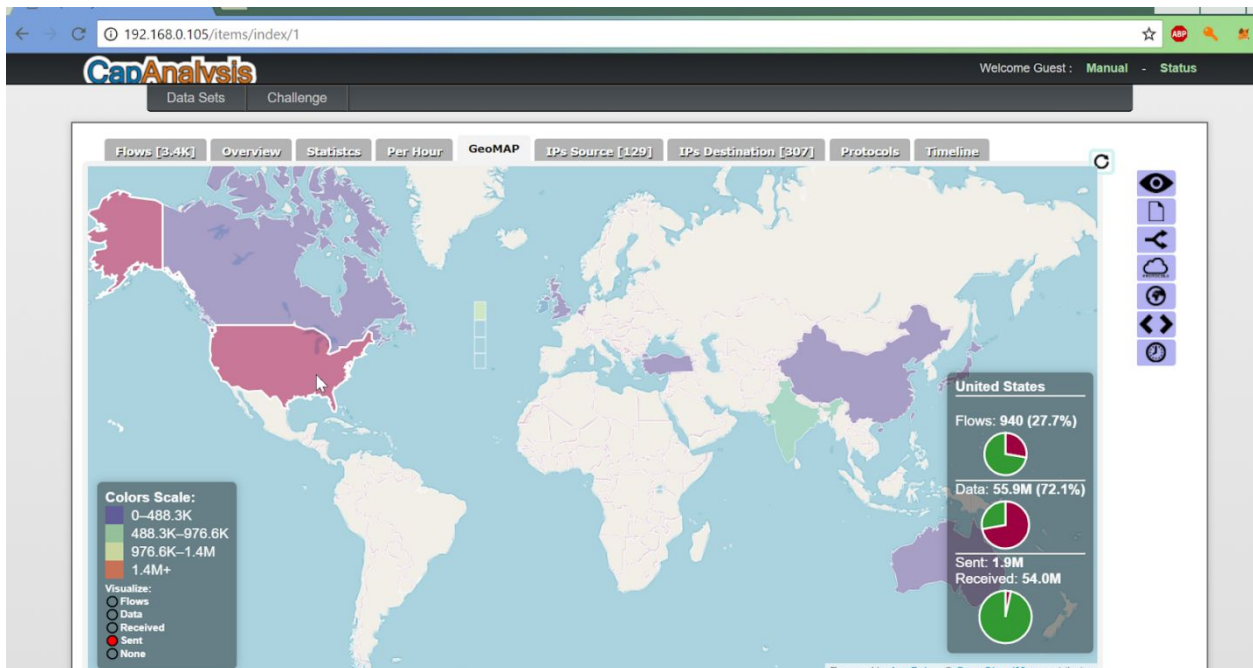
Q7. Between 12:00-12:59 on 3rd March 2017, traffic can be observed for an popular online shopping service. Can you name the service?

Answer: Amazon



Q8. Most of the traffic was destined to which country?

Answer: USA



Q9. There is also traffic from two file popular file sharing methods. What are their names?

Answer: BitTorrent and DropBox

Q10. Which social media platforms were used by the users during the traffic capture?

Answer: facebook, twitter

Answered from following screen

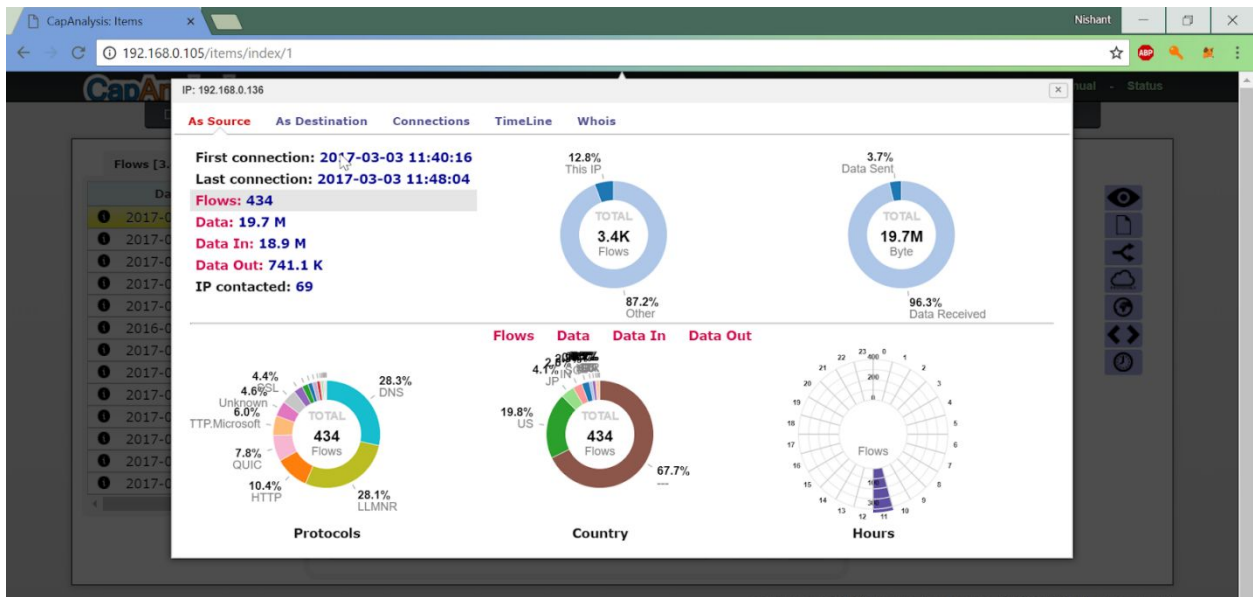


Q11. What is the total volume of the traffic given for analysis?

Answer: 77.5 MB

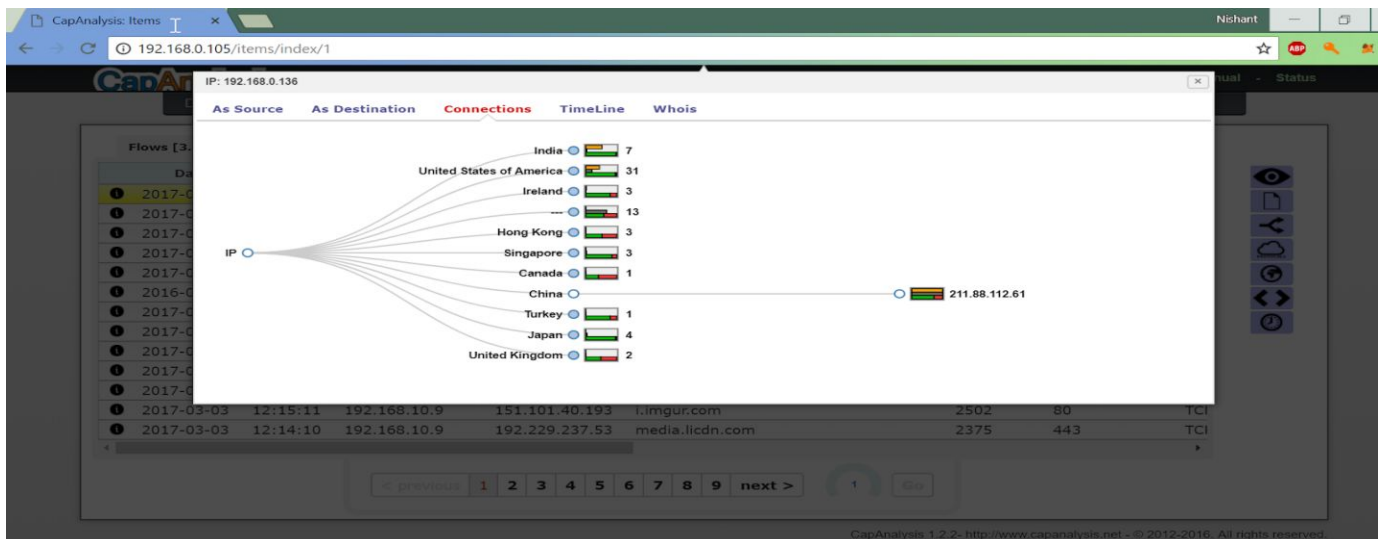
Q12. Which IP address is responsible for the largest chunk of traffic? What is the percentage share of this machine?

Answer: 192.168.0.136 25.4%



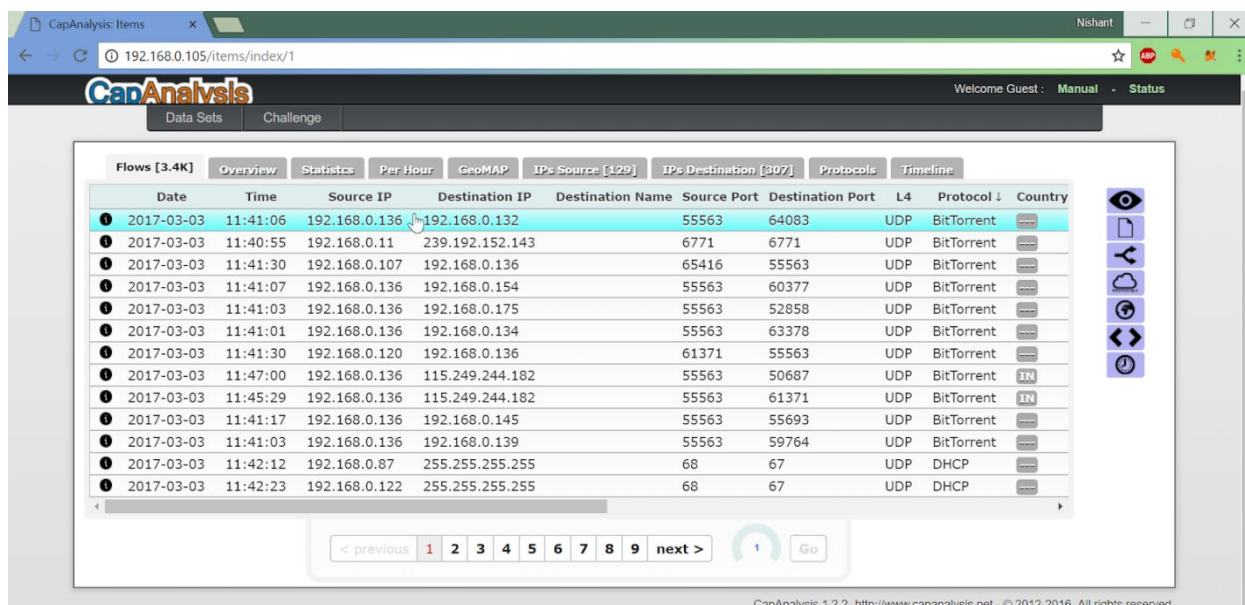
Q13. IP address 192.168.0.136 also exchanged som traffic with a machine in china. What is the IP of that machine?

Answer: 211.88.112.61



Q14. Which local machines (Private IP network) were using BitTorrent clients?

Answer: 192.168.0.136 192.168.0.120 192.168.0.11 192.168.0.107

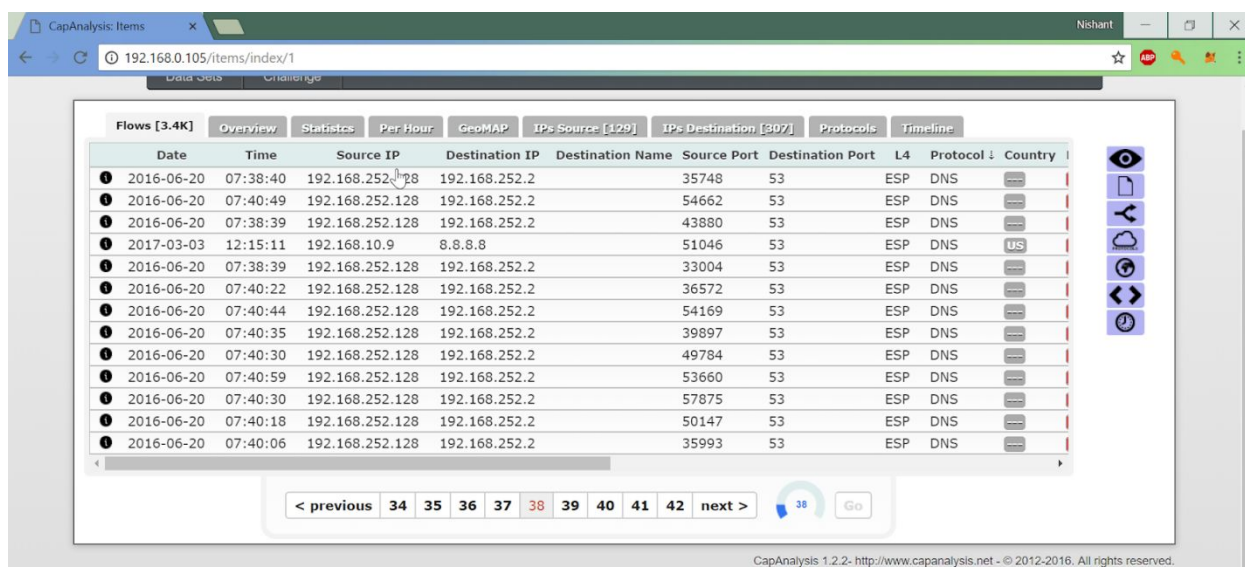


The screenshot shows the CapAnalysis web interface with a table of network flows. The table has columns for Date, Time, Source IP, Destination IP, Destination Name, Source Port, Destination Port, L4, Protocol, and Country. The flows are filtered by BitTorrent protocol. The following table represents the data shown in the screenshot:

| Date | Time | Source IP | Destination IP | Destination Name | Source Port | Destination Port | L4 | Protocol | Country |
|------------|----------|---------------|-----------------|------------------|-------------|------------------|-----|------------|---------|
| 2017-03-03 | 11:41:06 | 192.168.0.136 | 192.168.0.132 | | 55563 | 64083 | UDP | BitTorrent | |
| 2017-03-03 | 11:40:55 | 192.168.0.11 | 239.192.152.143 | | 6771 | 6771 | UDP | BitTorrent | |
| 2017-03-03 | 11:41:30 | 192.168.0.107 | 192.168.0.136 | | 65416 | 55563 | UDP | BitTorrent | |
| 2017-03-03 | 11:41:07 | 192.168.0.136 | 192.168.0.154 | | 55563 | 60377 | UDP | BitTorrent | |
| 2017-03-03 | 11:41:03 | 192.168.0.136 | 192.168.0.175 | | 55563 | 52858 | UDP | BitTorrent | |
| 2017-03-03 | 11:41:01 | 192.168.0.136 | 192.168.0.134 | | 55563 | 63378 | UDP | BitTorrent | |
| 2017-03-03 | 11:41:30 | 192.168.0.120 | 192.168.0.136 | | 61371 | 55563 | UDP | BitTorrent | |
| 2017-03-03 | 11:47:00 | 192.168.0.136 | 115.249.244.182 | | 55563 | 50687 | UDP | BitTorrent | IN |
| 2017-03-03 | 11:45:29 | 192.168.0.136 | 115.249.244.182 | | 55563 | 61371 | UDP | BitTorrent | IN |
| 2017-03-03 | 11:41:17 | 192.168.0.136 | 192.168.0.145 | | 55563 | 55693 | UDP | BitTorrent | |
| 2017-03-03 | 11:41:03 | 192.168.0.136 | 192.168.0.139 | | 55563 | 59764 | UDP | BitTorrent | |
| 2017-03-03 | 11:42:12 | 192.168.0.87 | 255.255.255.255 | | 68 | 67 | UDP | DHCP | |
| 2017-03-03 | 11:42:23 | 192.168.0.122 | 255.255.255.255 | | 68 | 67 | UDP | DHCP | |

Q15. What is the IP of local and public DNS server being used?

Answer: 192.168.252.2, 8.8.8.8



The screenshot shows the CapAnalysis web interface with a table of network flows. The table has columns for Date, Time, Source IP, Destination IP, Destination Name, Source Port, Destination Port, L4, Protocol, and Country. The flows are filtered by DNS protocol. The following table represents the data shown in the screenshot:

| Date | Time | Source IP | Destination IP | Destination Name | Source Port | Destination Port | L4 | Protocol | Country |
|------------|----------|-----------------|----------------|------------------|-------------|------------------|-----|----------|---------|
| 2016-06-20 | 07:38:40 | 192.168.252.128 | 192.168.252.2 | | 35748 | 53 | ESP | DNS | |
| 2016-06-20 | 07:40:49 | 192.168.252.128 | 192.168.252.2 | | 54662 | 53 | ESP | DNS | |
| 2016-06-20 | 07:38:39 | 192.168.252.128 | 192.168.252.2 | | 43880 | 53 | ESP | DNS | |
| 2017-03-03 | 12:15:11 | 192.168.10.9 | 8.8.8.8 | | 51046 | 53 | ESP | DNS | US |
| 2016-06-20 | 07:38:39 | 192.168.252.128 | 192.168.252.2 | | 33004 | 53 | ESP | DNS | |
| 2016-06-20 | 07:40:22 | 192.168.252.128 | 192.168.252.2 | | 36572 | 53 | ESP | DNS | |
| 2016-06-20 | 07:40:44 | 192.168.252.128 | 192.168.252.2 | | 54169 | 53 | ESP | DNS | |
| 2016-06-20 | 07:40:35 | 192.168.252.128 | 192.168.252.2 | | 39897 | 53 | ESP | DNS | |
| 2016-06-20 | 07:40:30 | 192.168.252.128 | 192.168.252.2 | | 49784 | 53 | ESP | DNS | |
| 2016-06-20 | 07:40:59 | 192.168.252.128 | 192.168.252.2 | | 53660 | 53 | ESP | DNS | |
| 2016-06-20 | 07:40:30 | 192.168.252.128 | 192.168.252.2 | | 57875 | 53 | ESP | DNS | |
| 2016-06-20 | 07:40:18 | 192.168.252.128 | 192.168.252.2 | | 50147 | 53 | ESP | DNS | |
| 2016-06-20 | 07:40:06 | 192.168.252.128 | 192.168.252.2 | | 35993 | 53 | ESP | DNS | |



References:

1. CapAnalysis (<https://www.capanalysis.net/ca/>)