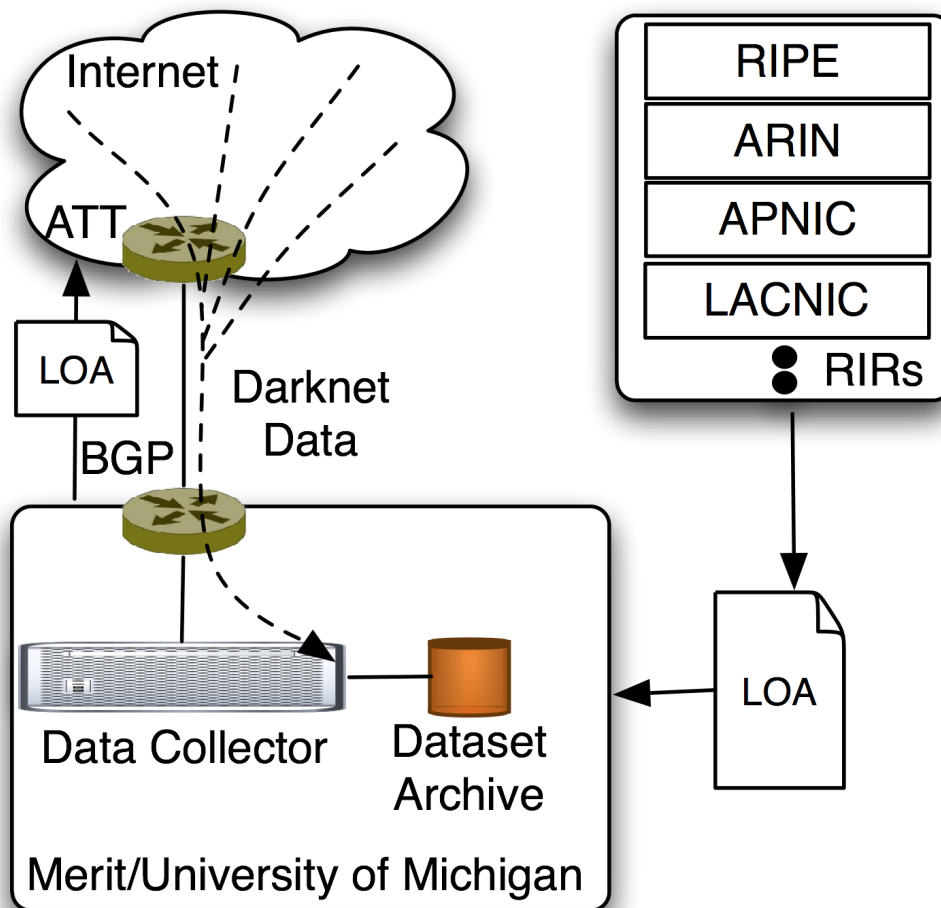


# Internet Pollution – Part 2

Scott Walls, Manish Karir  
Merit Network Inc.

# A Framework for Internet Pollution Analysis

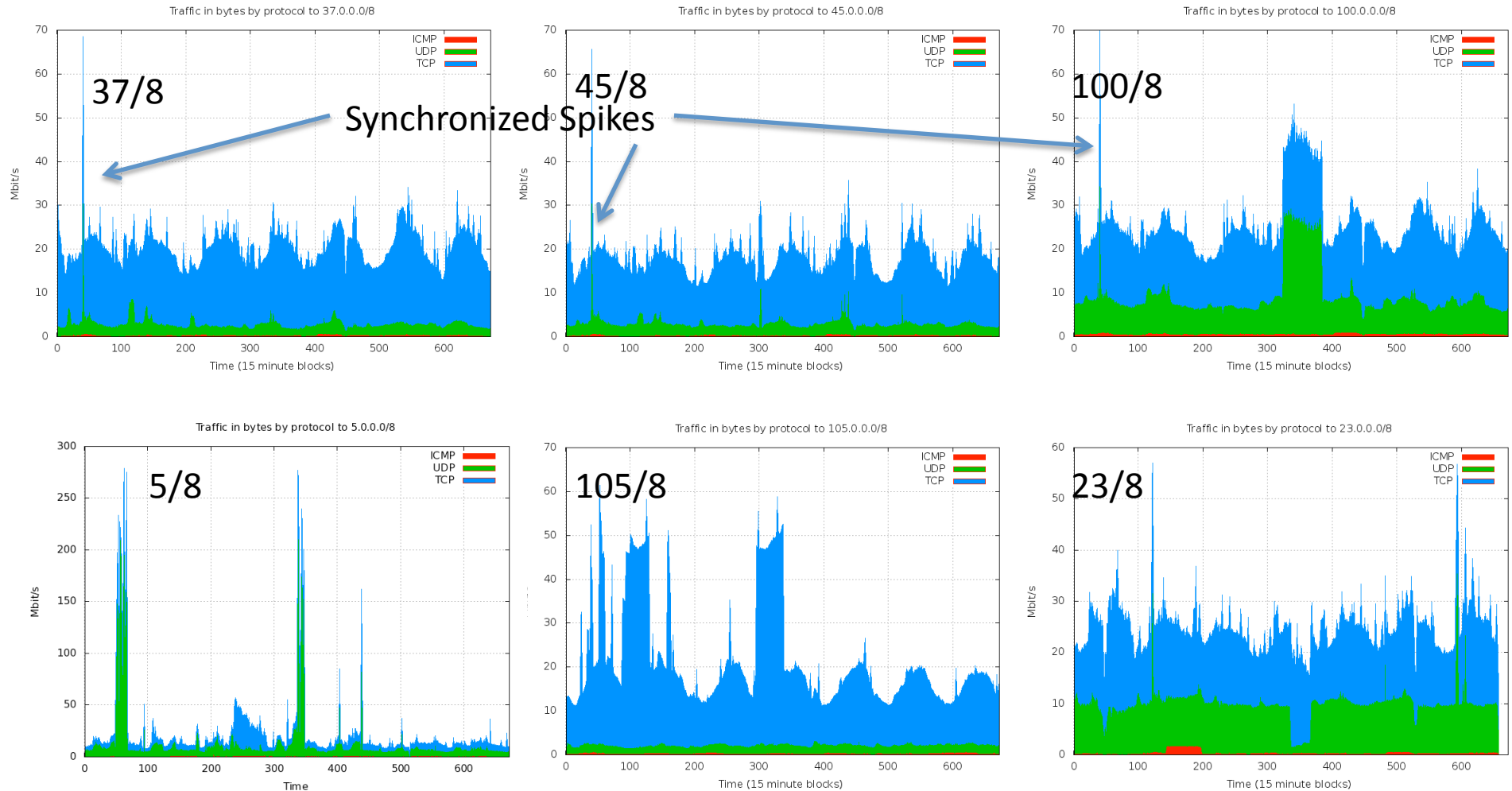


- Work with RIRs to identify upcoming allocation
- Obtain LOA
- Advertise, Collect, Analyze, Archive, Provide to research community
- Cleanup/Quarantine recommendations
- Support from DHS via PREDICT Project

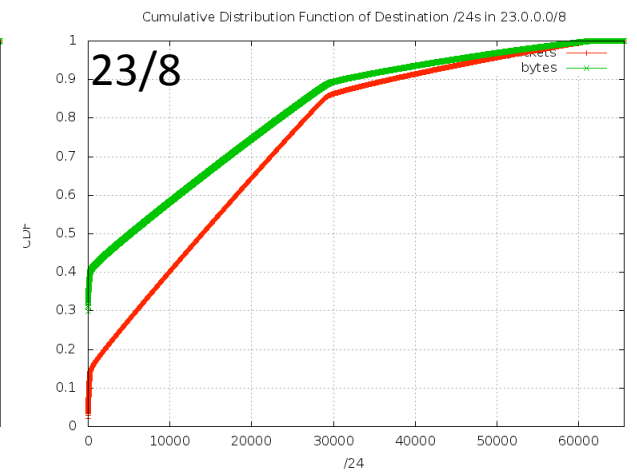
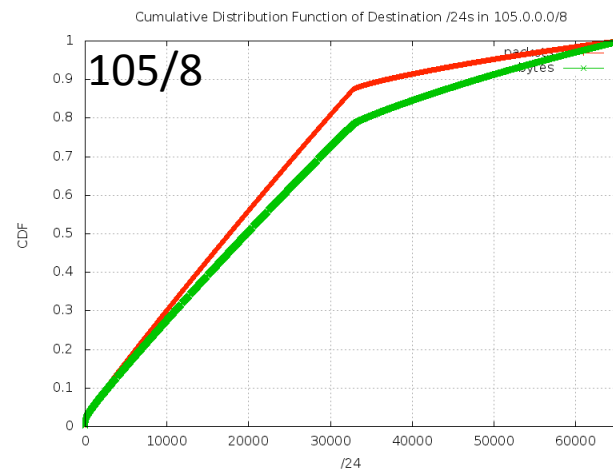
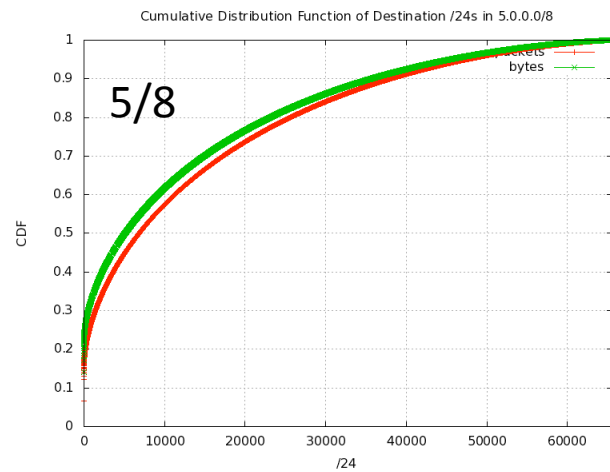
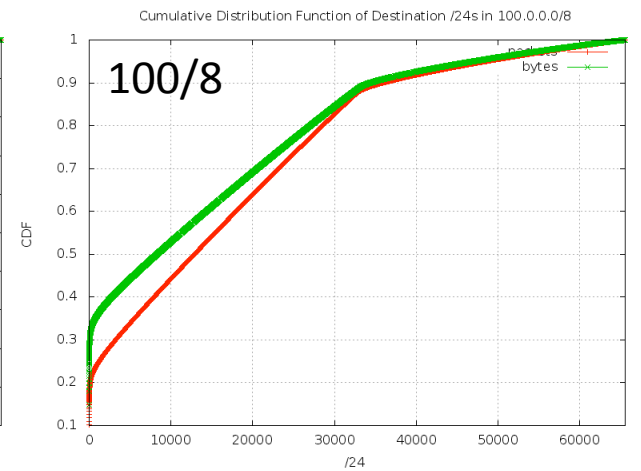
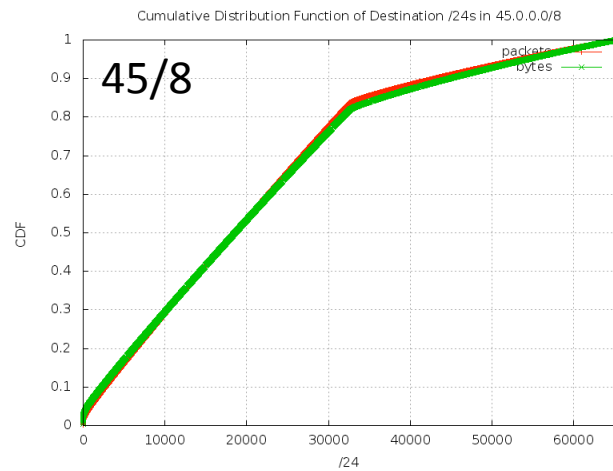
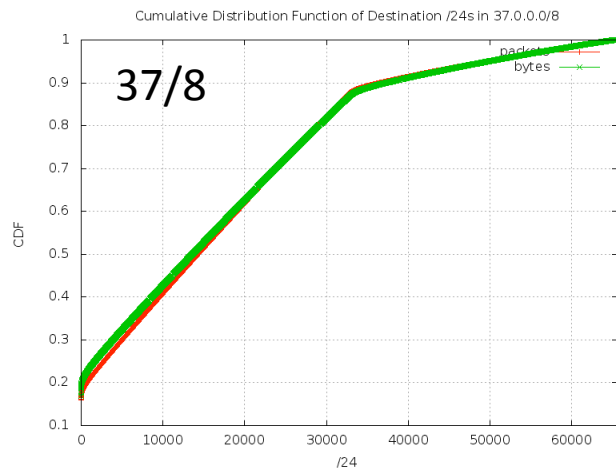
# Cross RIR Darknet Traffic Analysis

- Goal: Analyze darknet traffic to determine how much and what kinds of pollution were present in each block and determine whether cleanup/quarantine were viable options
- 23/8, 100/8, 45/8 - ARIN
- 5/8, 37/8 - RIPE
- 105/8 – AfriNIC
- Several 7 day long datasets were collected – here we are presenting results from a 6 /8 collection with 3 simultaneous announcements (37, 45, 100)
- Alternate dataset has all 6 /8 announcements at the same time

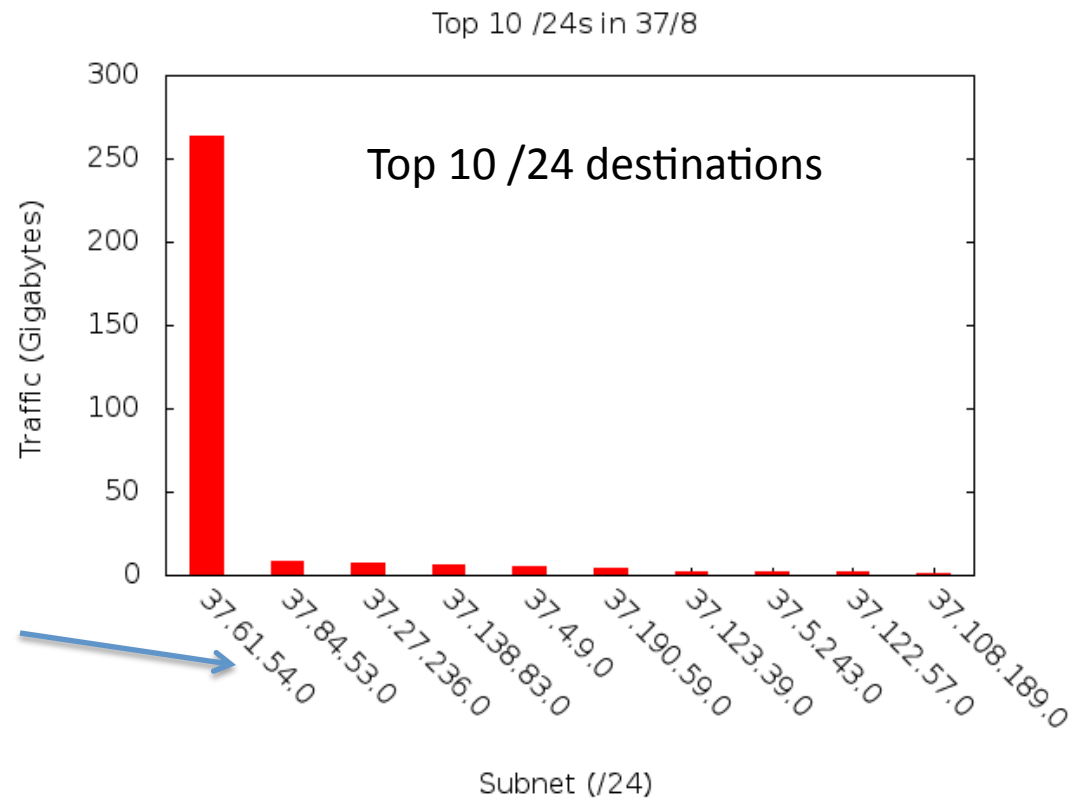
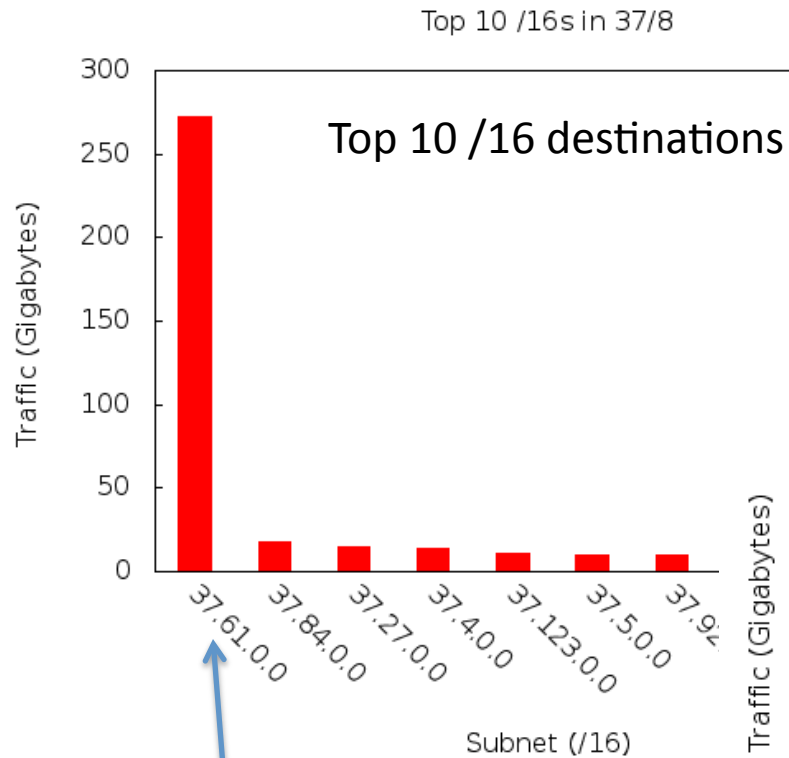
# Comparing Traffic Volumes



# Comparing Hotspot Activity



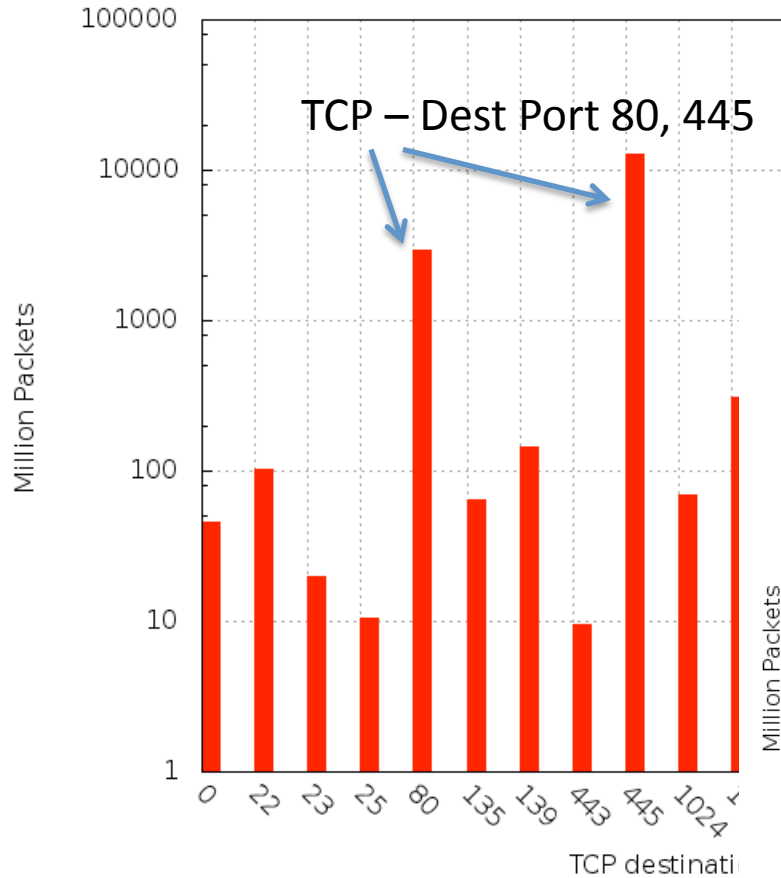
# 37/8



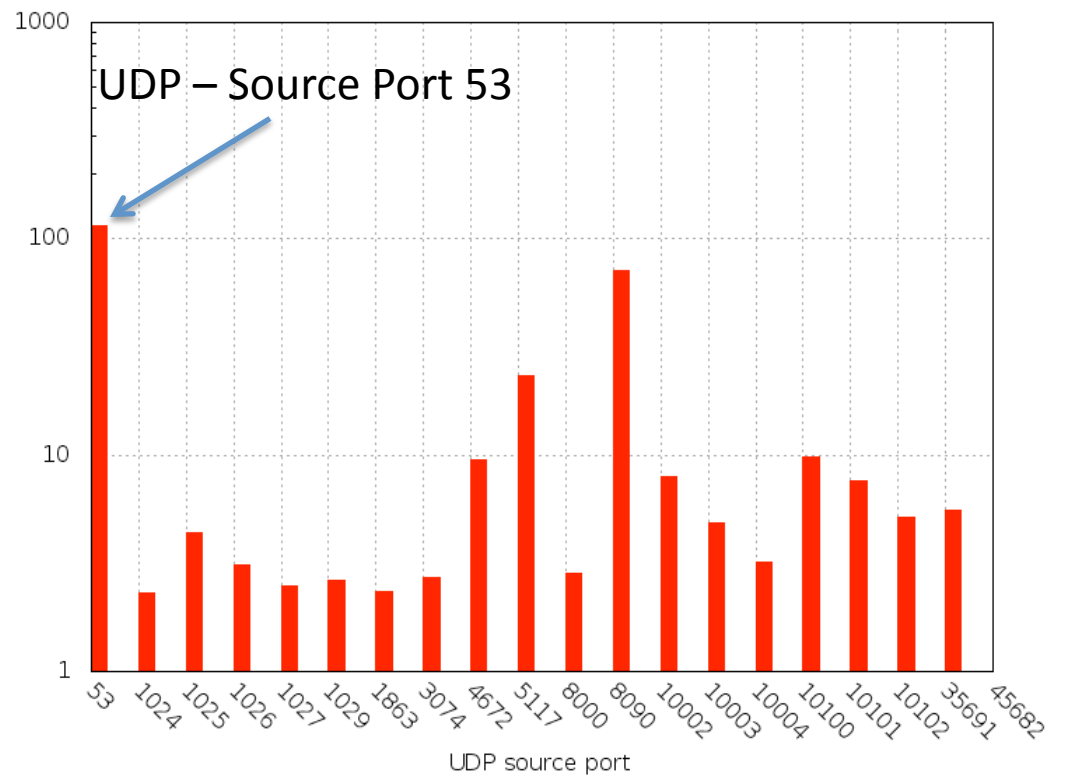
Single /16 and single /24 account for majority of the captured traffic by byte count

# 37/8

Top 20 TCP destination ports (by packets) to 37.0.0.0/8



Top 20 UDP source ports (by packets) to 37.0.0.0/8



# 37/8

- Port 80 TCP traffic all appears to be directed at single IP address and appears to be related with facebook blocking in china

<http://www.renesys.com/blog/2010/06/two-strikes-i-root.shtml>

```
dig @dns1.chinatelecom.com.cn. www.facebook.com.
```

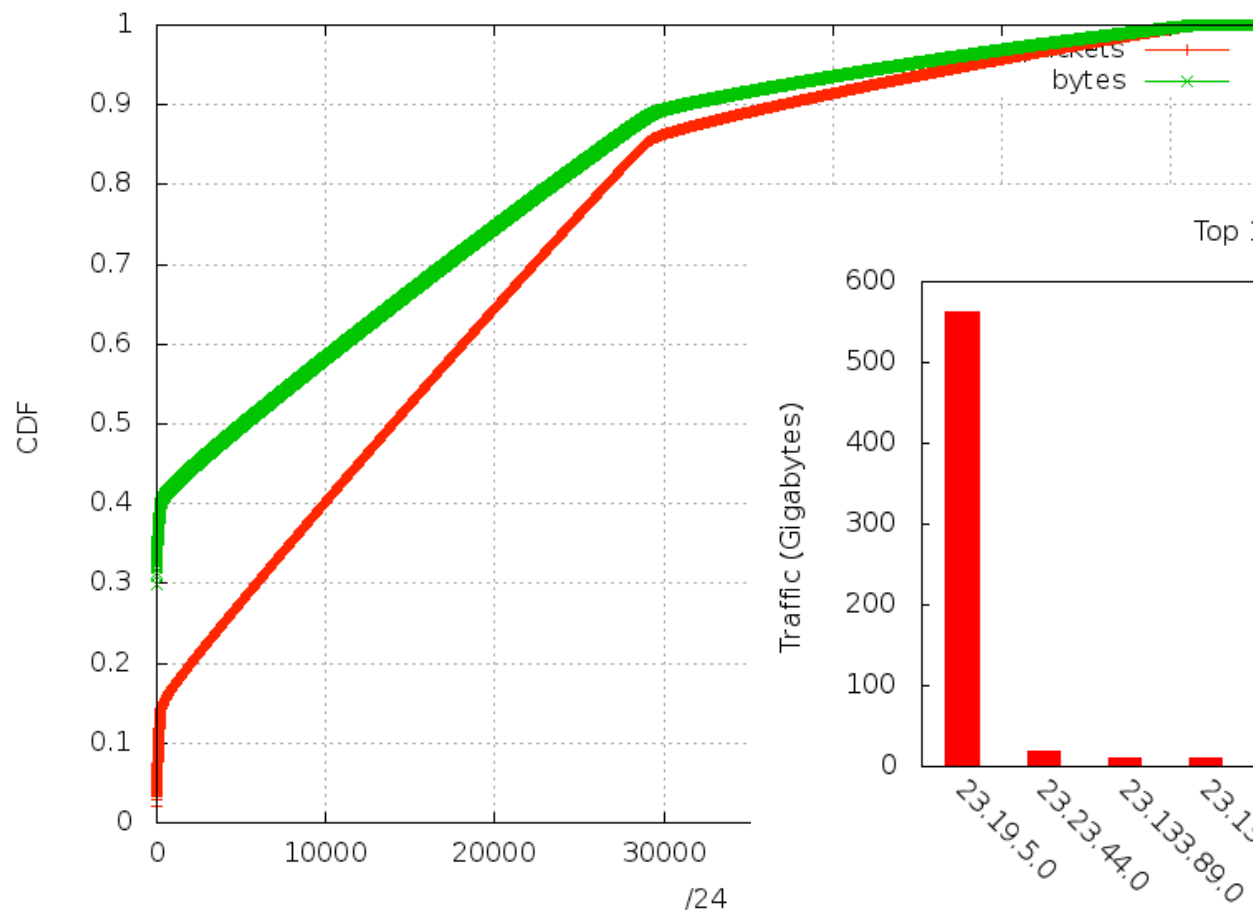
```
...
```

```
www.facebook.com. 11556 IN A 37.61.54.158  
www.facebook.com. 24055 IN A 78.16.49.15  
www.facebook.com. 38730 IN A 203.98.7.65
```

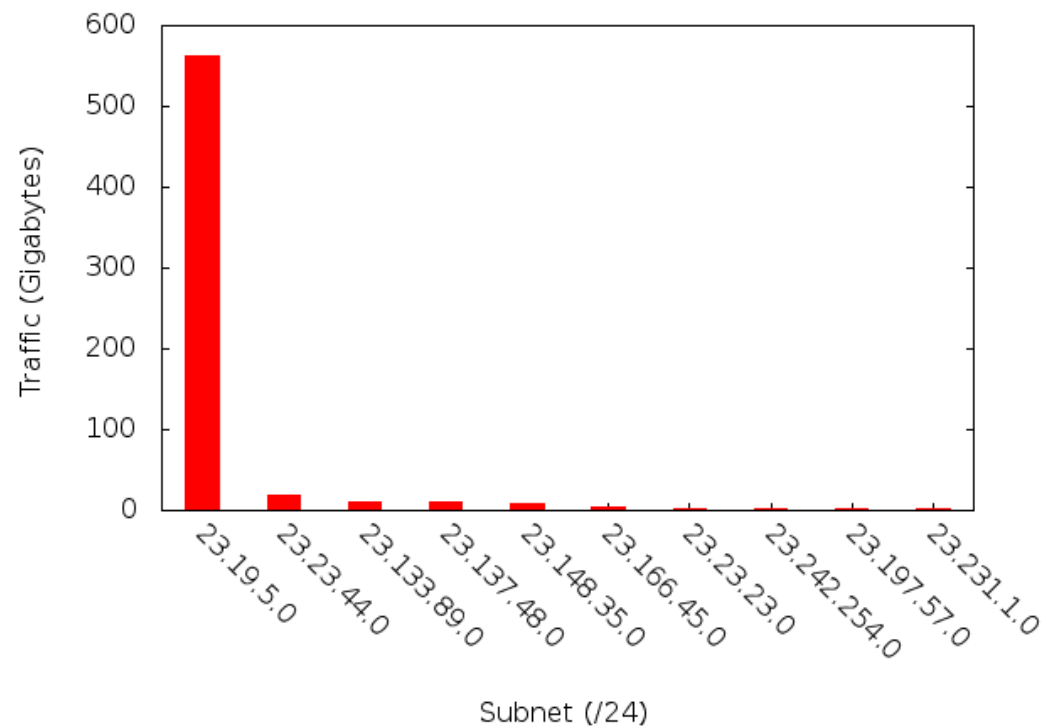


# 23/8

Cumulative Distribution Function of Destination /24s in 23.0.0.0/8

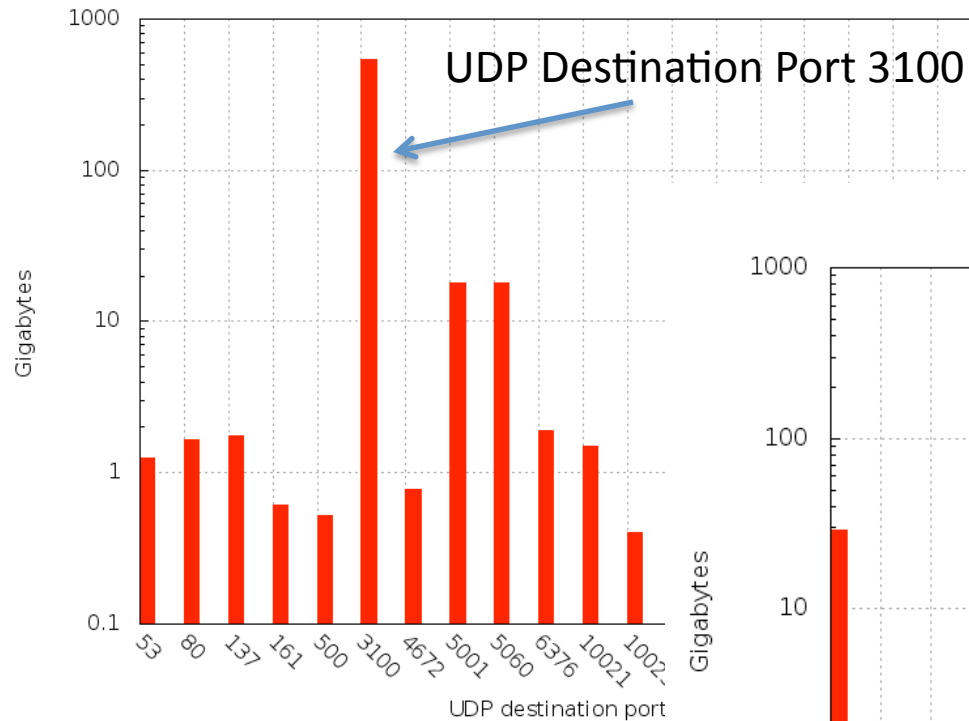


Top 10 /24s in 23/8

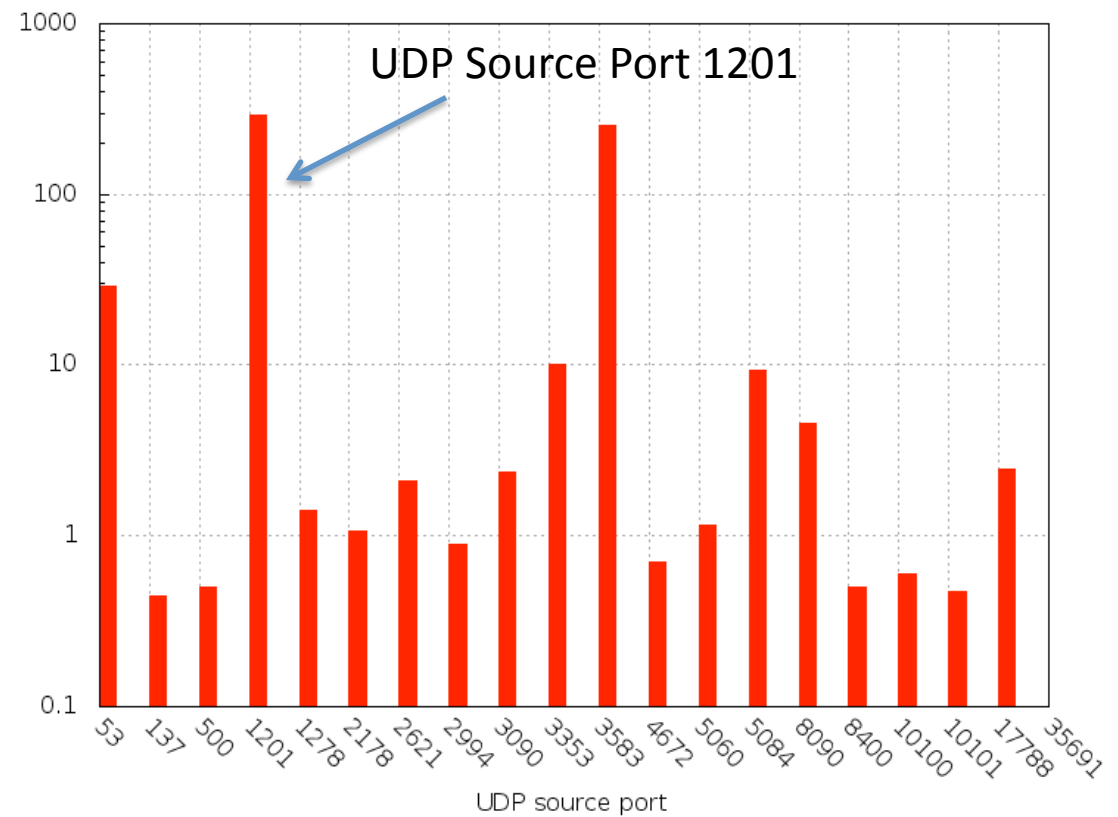


# 23/8

Top 20 UDP destination ports (by bytes) to 23.0.0.0/8



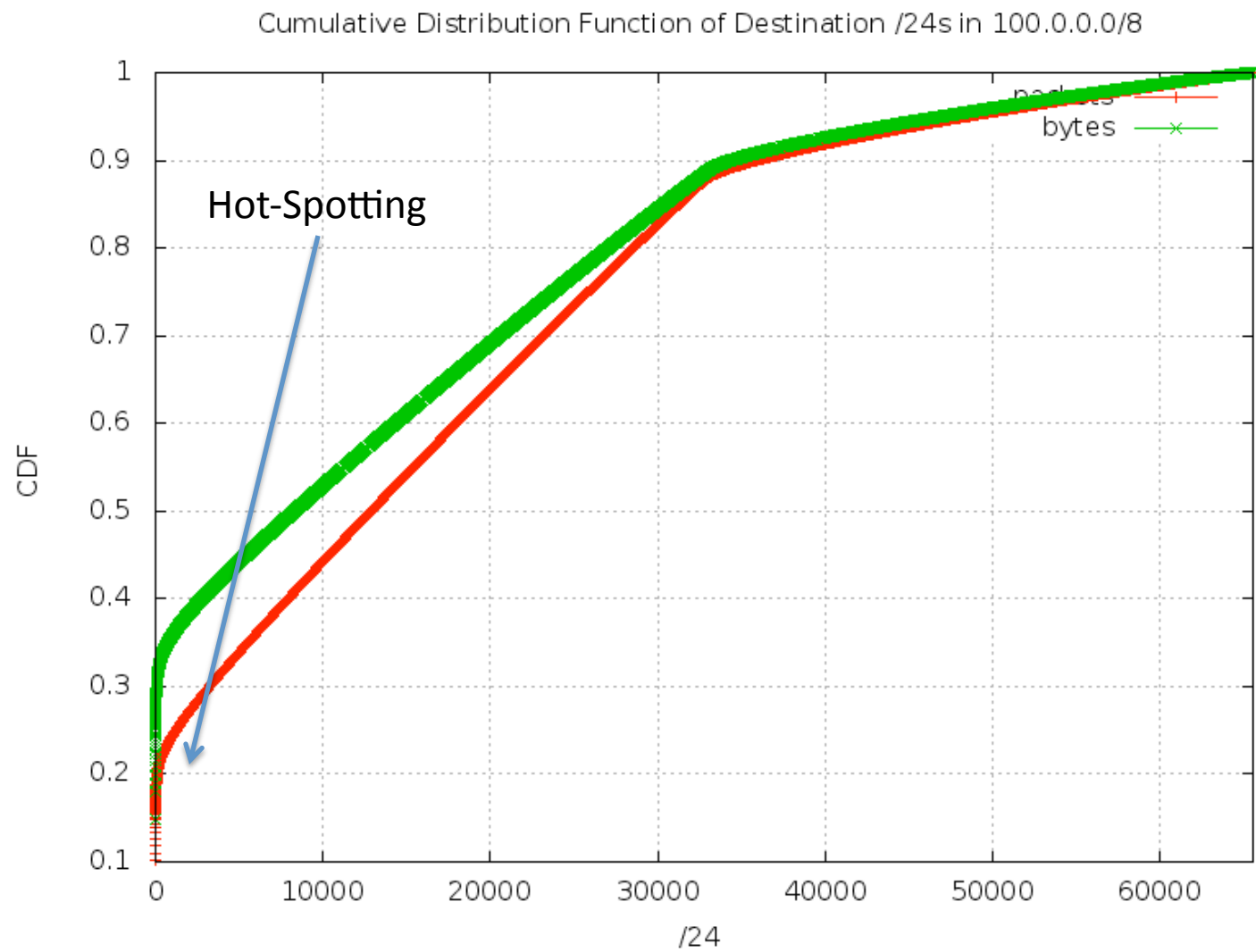
Top 20 UDP source ports (by bytes) to 23.0.0.0/8



# 23/8

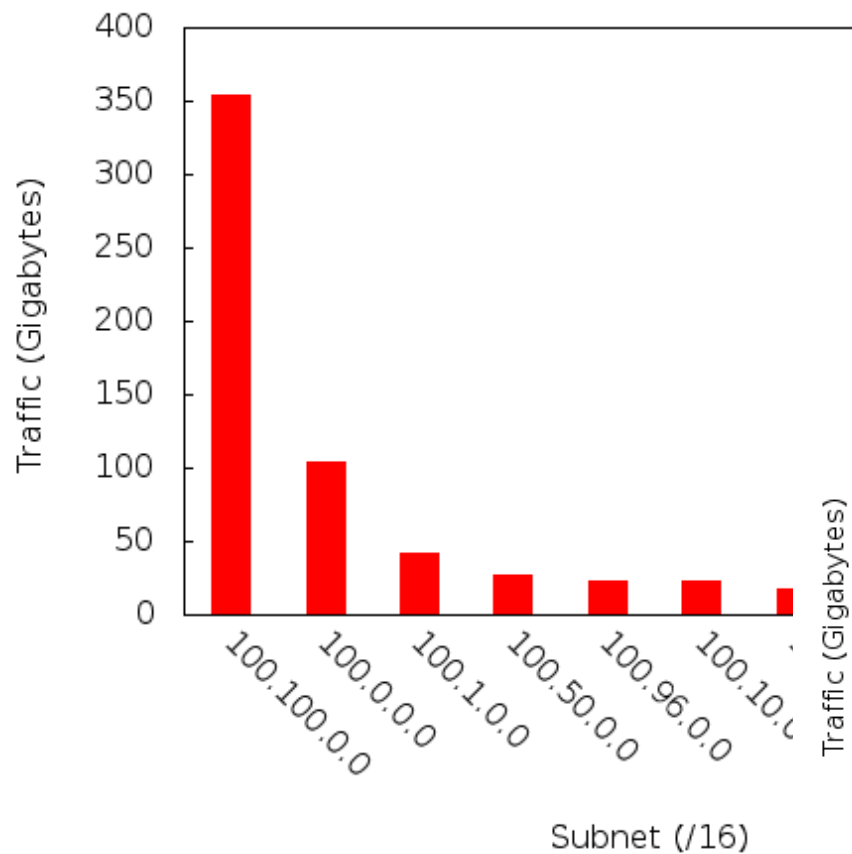
- Traffic from source port 1201 to dest port 3100 from single source to single destination
- Video stream – decoded to 1080p video!

# 100/8

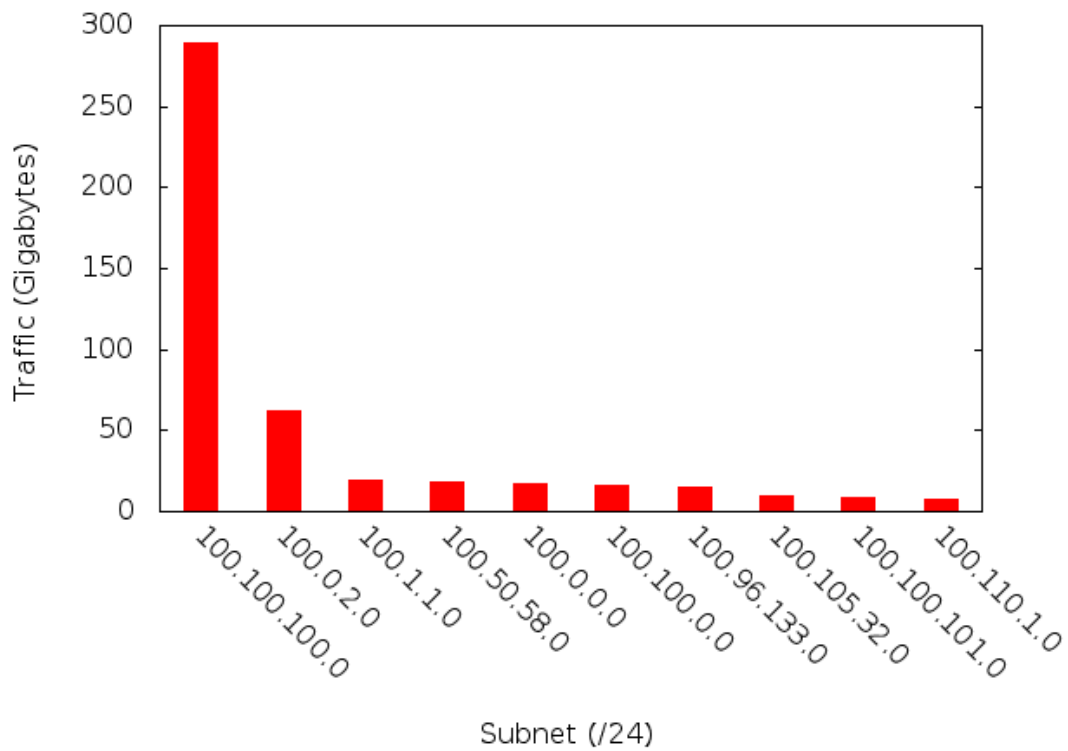


# 100/8

Top 10 /16s in 100/8

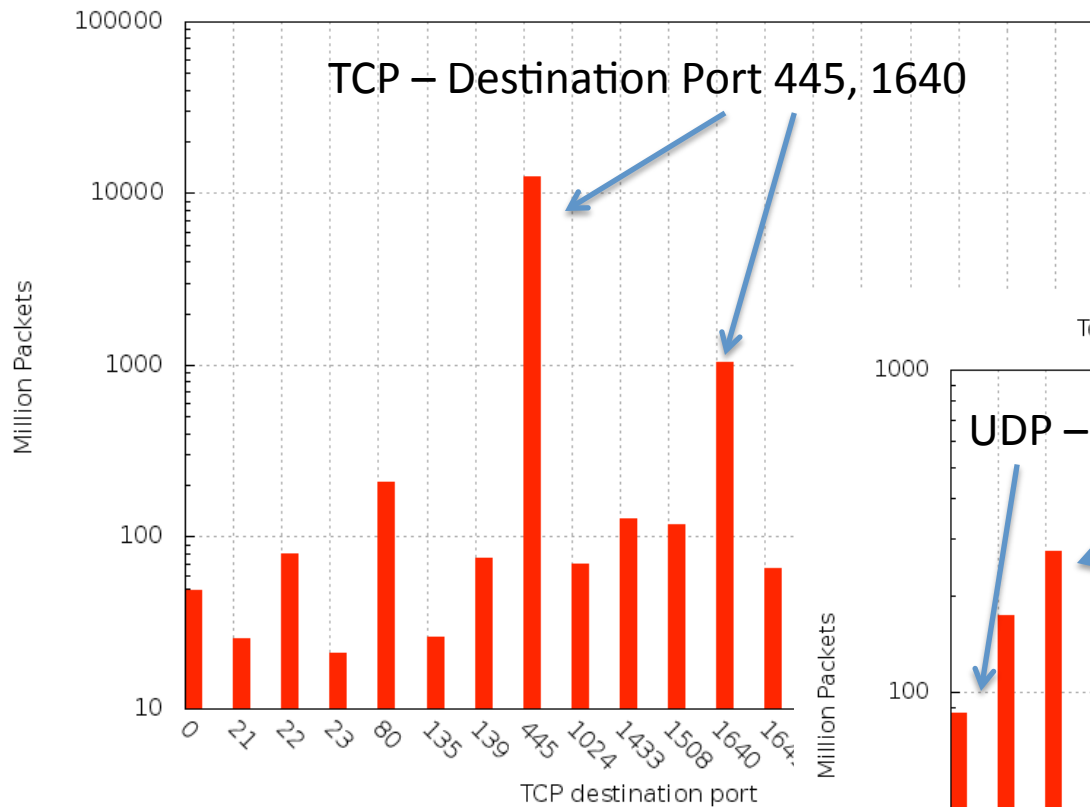


Top 10 /24s in 100/8

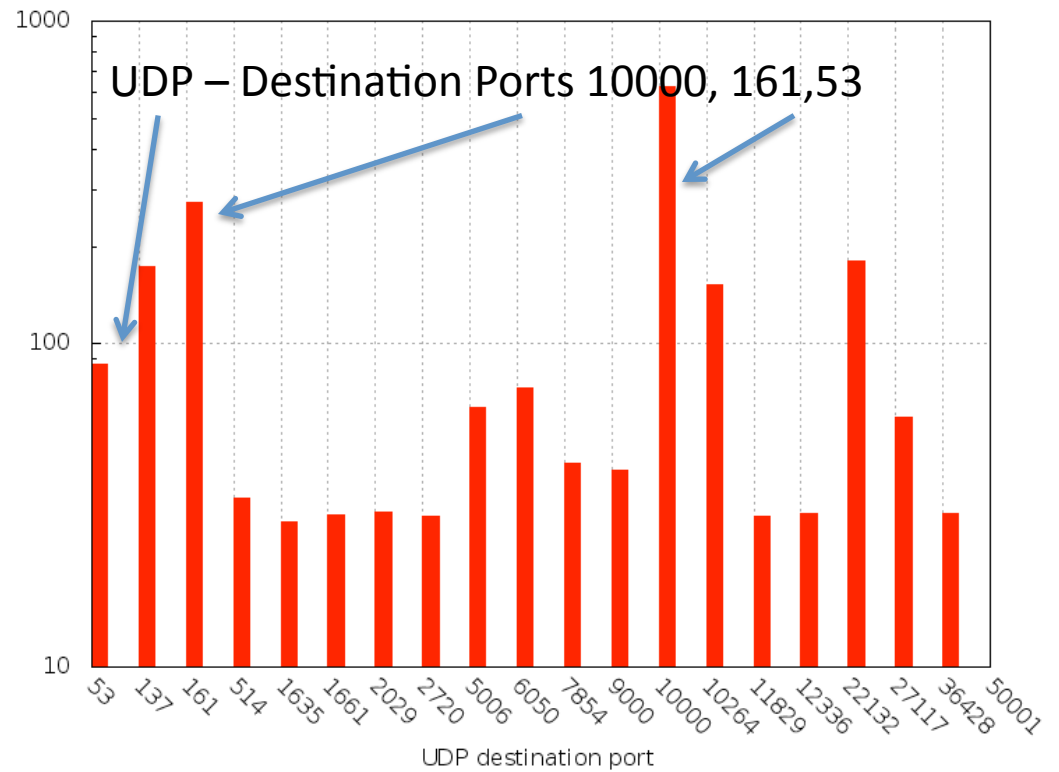


# 100/8

Top 20 TCP destination ports (by packets) to 100.0.0.0/8



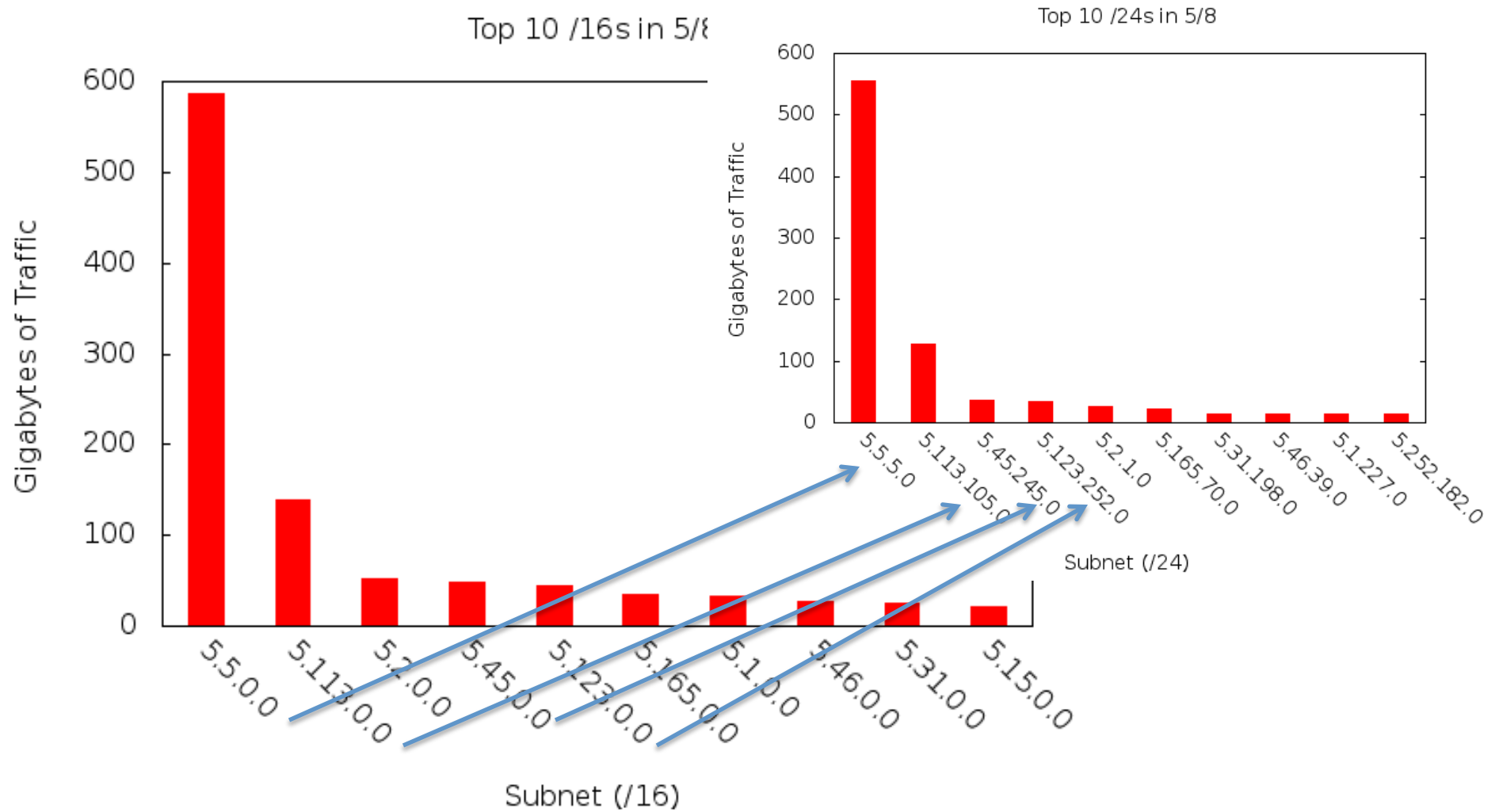
Top 20 UDP destination ports (by packets) to 100.0.0.0/8



# 100/8

- UDP port 161 – SNMP traffic – default settings in manuals
- UDP source port 10000 – 33 byte packets – micro-torrent some SNMP etc.

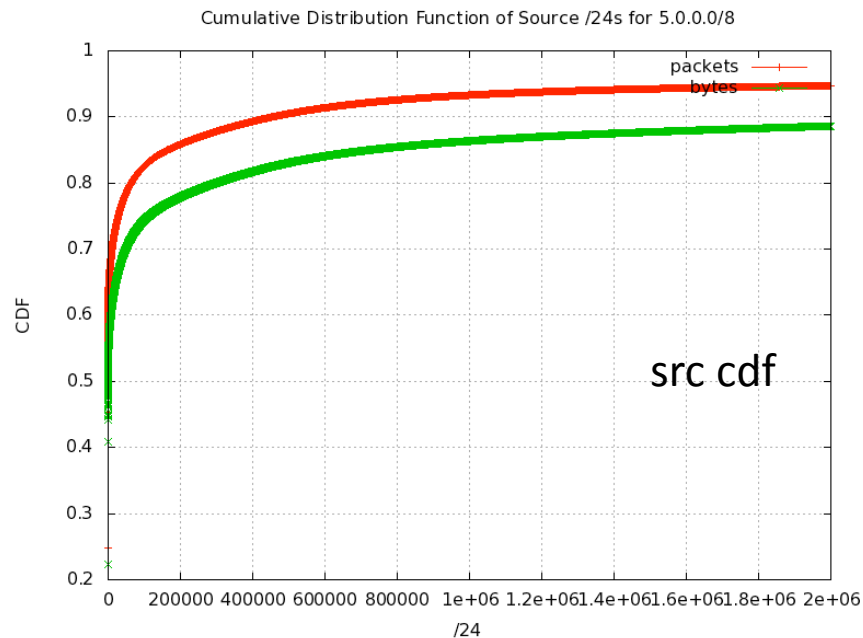
# 5/8





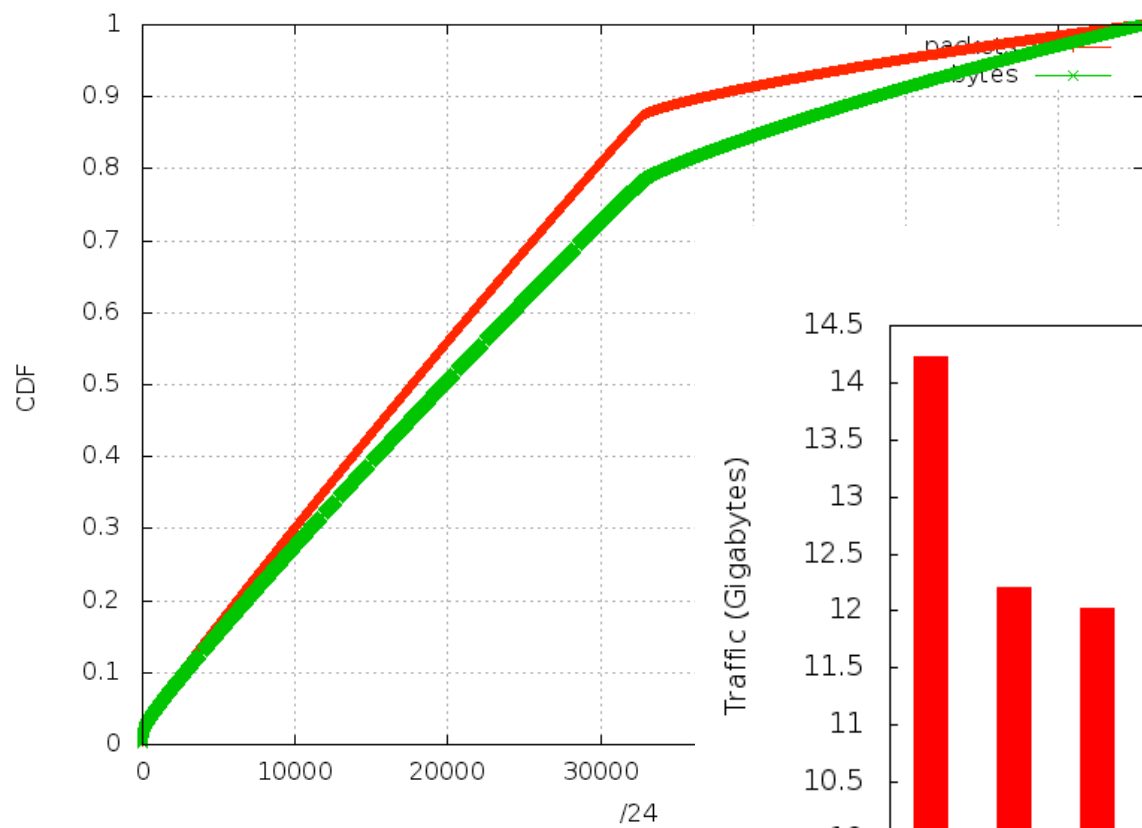
# 5/8

- Traffic spikes of upto 250Mbps
  - 5.5.5.5 – UDP – 250Byte pkts random ports/srcip
- ICMP6! 5.113.105.0/24
- Flash video – 5.45.245.0/24

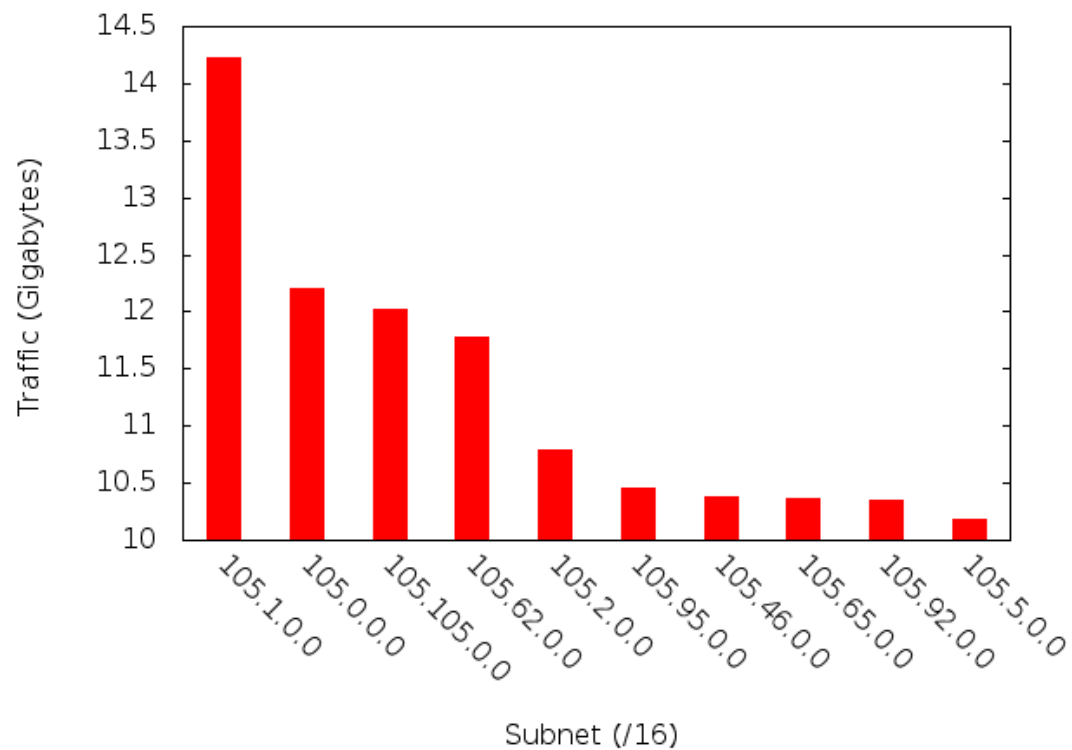


# 105/8

Cumulative Distribution Function of Destination /24s in 105.0.0.0/8

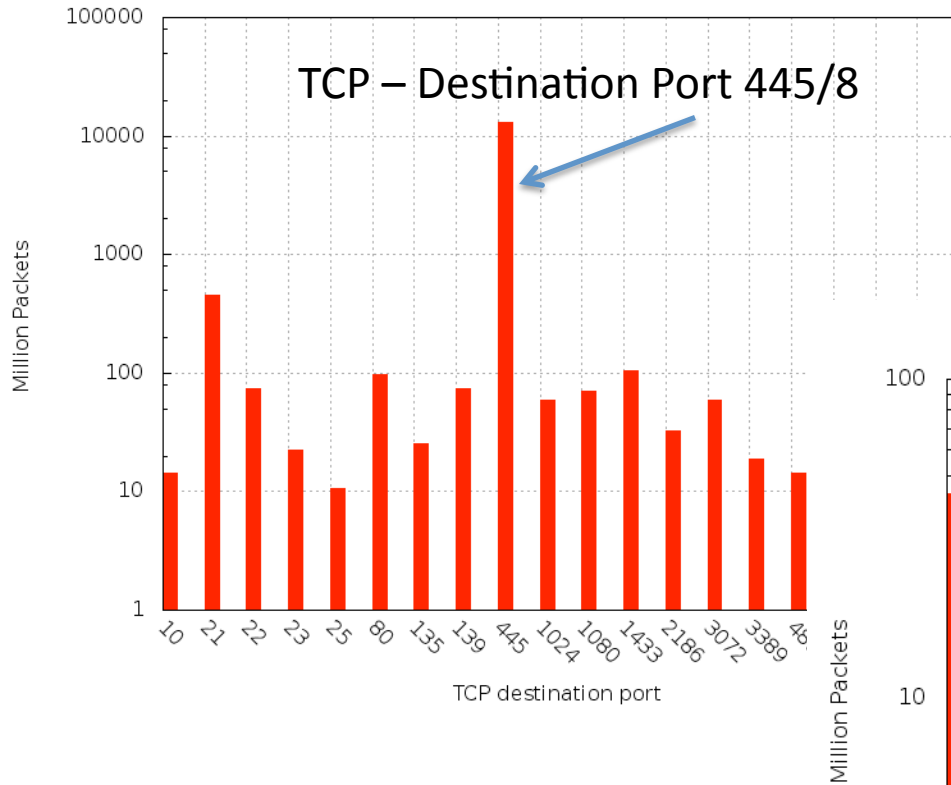


Top 10 /16s in 105/8

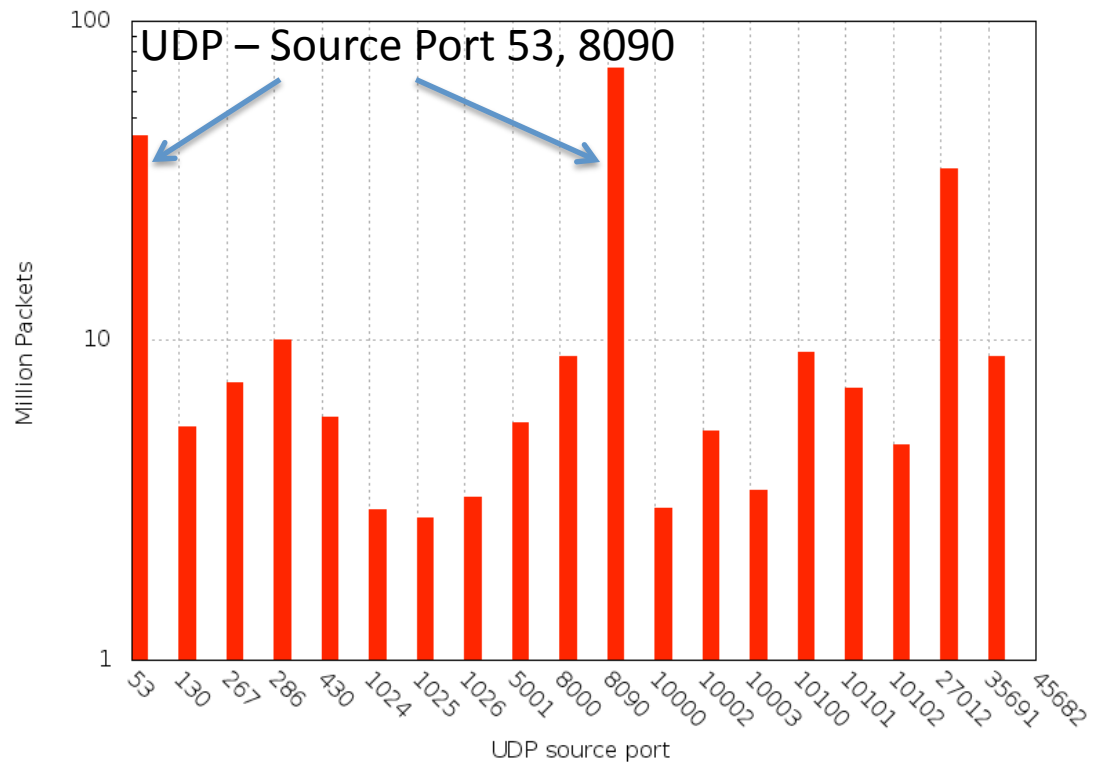


# 105/8

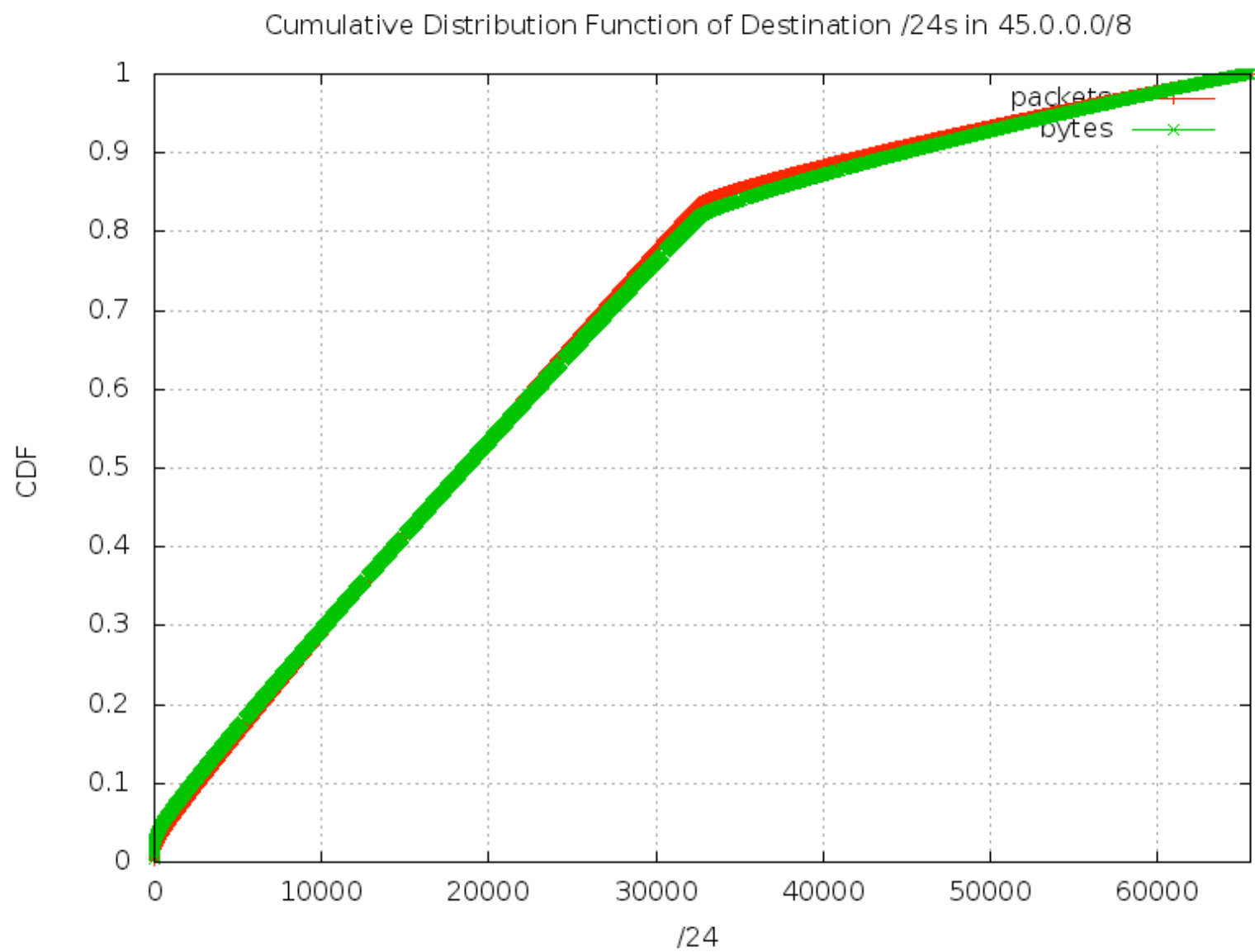
Top 20 TCP destination ports (by packets) to 105.0.0.0/8



Top 20 UDP source ports (by packets) to 105.0.0.0/8

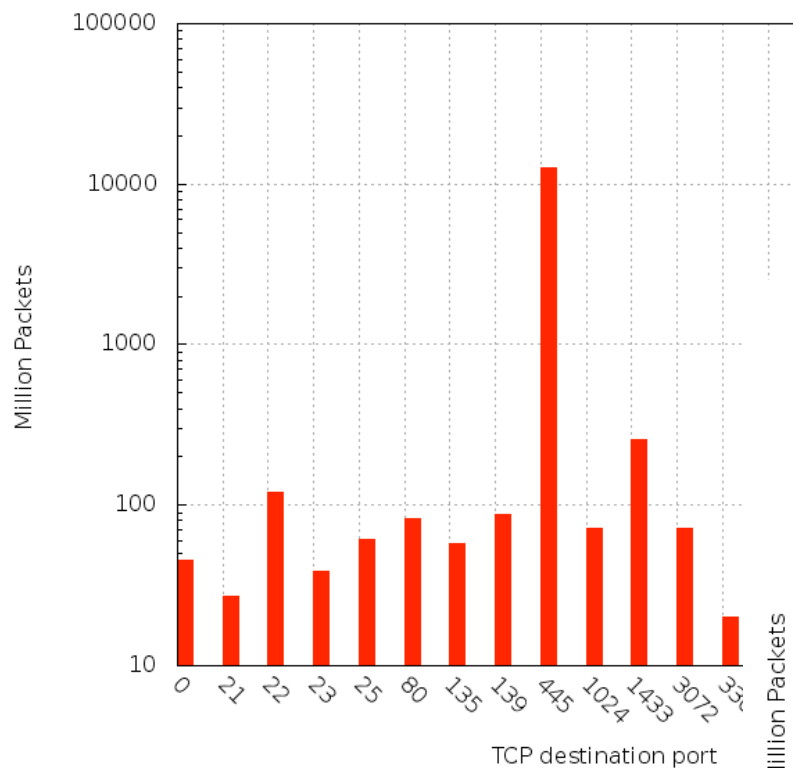


# 45/8

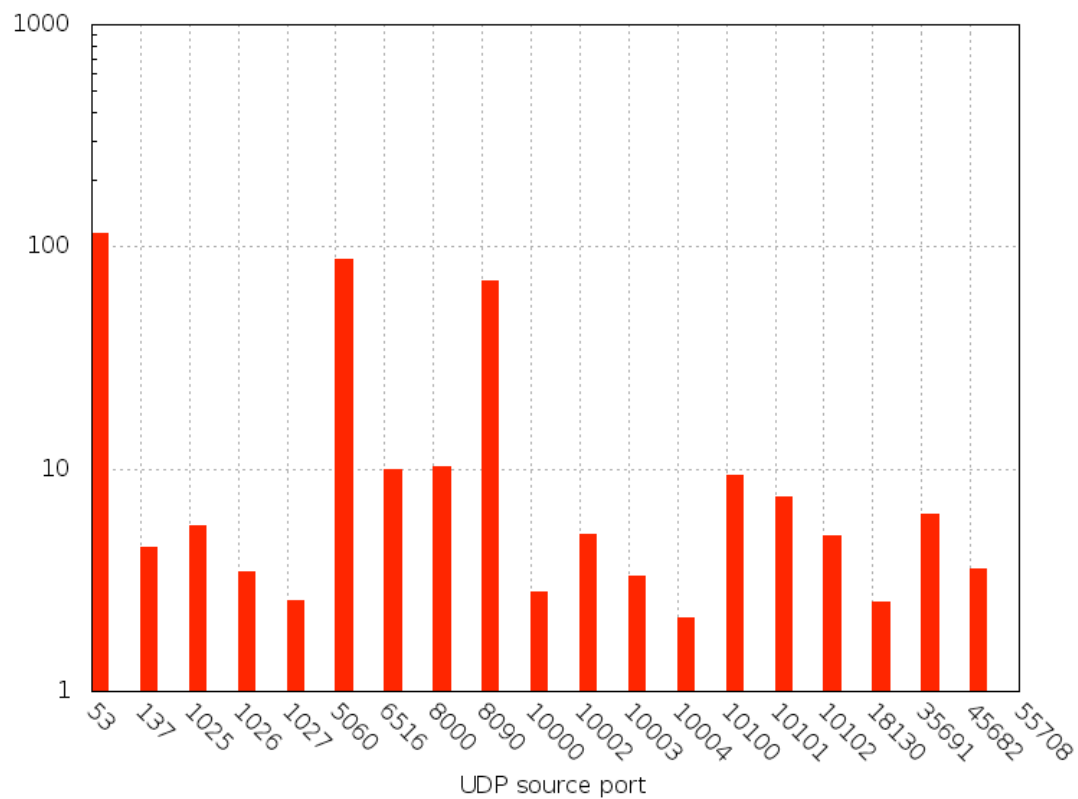


# 45/8

Top 20 TCP destination ports (by packets) to 45.0.0.0/8

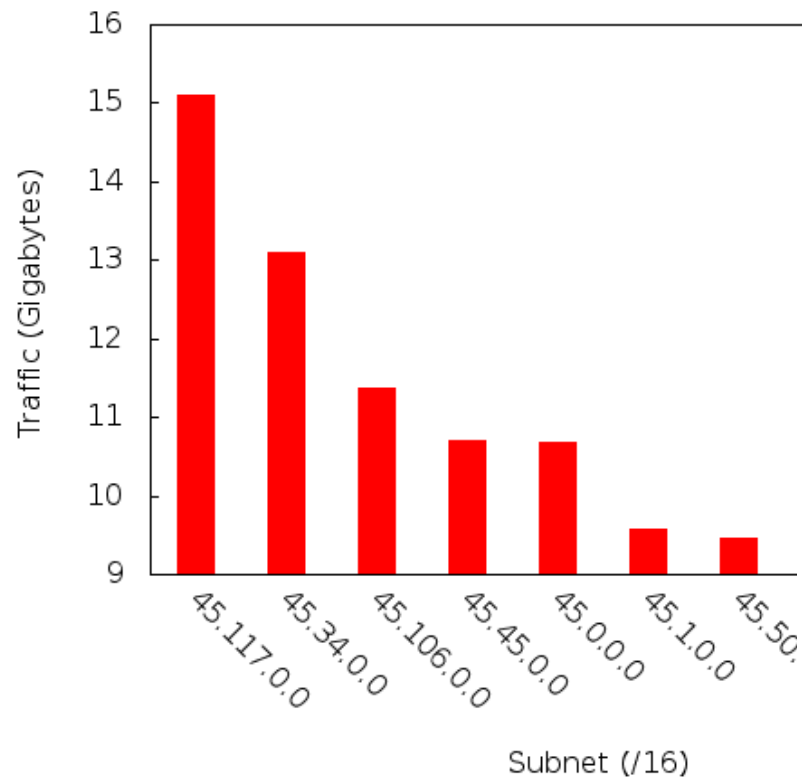


Top 20 UDP source ports (by packets) to 45.0.0.0/8

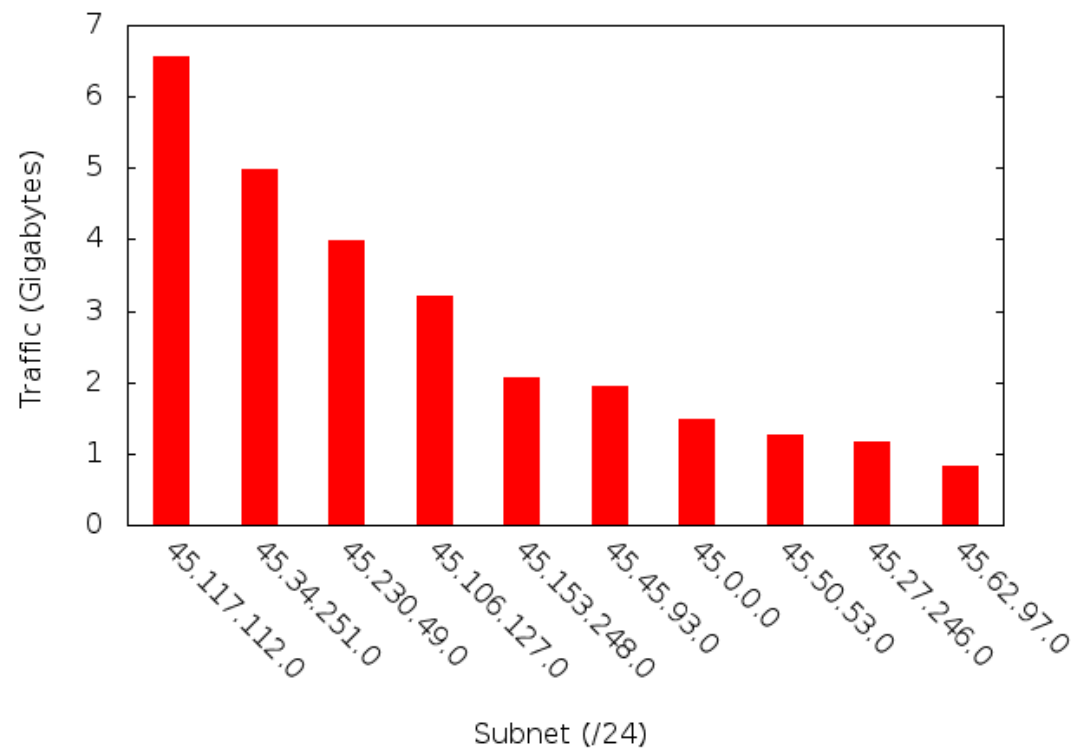


# 45/8

Top 10 /16s in 45/8



Top 10 /24s in 45/8



# Conclusions

- Pollution tends to greatly skew darknet traffic
  - Diverse darknets – diverse reasons for pollution
- General characteristics of background radiation:
  - 15-30Mbps of base traffic for /8 spikes upto 70Mbps
  - Heavily dominated by conficker for TCP traffic
  - DNS for UDP traffic from small set of servers (\*)
- Sharing results with relevant RIRs so that they can determine appropriate action regarding cleanup/quarantine

# Conclusions

- 100/8, 5/8, 23/8 show relatively abnormal amounts of traffic to portions of the address space
  - Special consideration for:
    - 37.61.54.0/24
    - 23.19.5/24
    - 100.100.100.0/24, 100.0.2.0/24, 100.1.1.0/24
    - 5.5.5.0/24, 5.13.105/24, 5.45.245.0/24, 5.123.252.0/24
  - 45/8, 105/8 relatively clean