Networking Presentation

ITMS 448

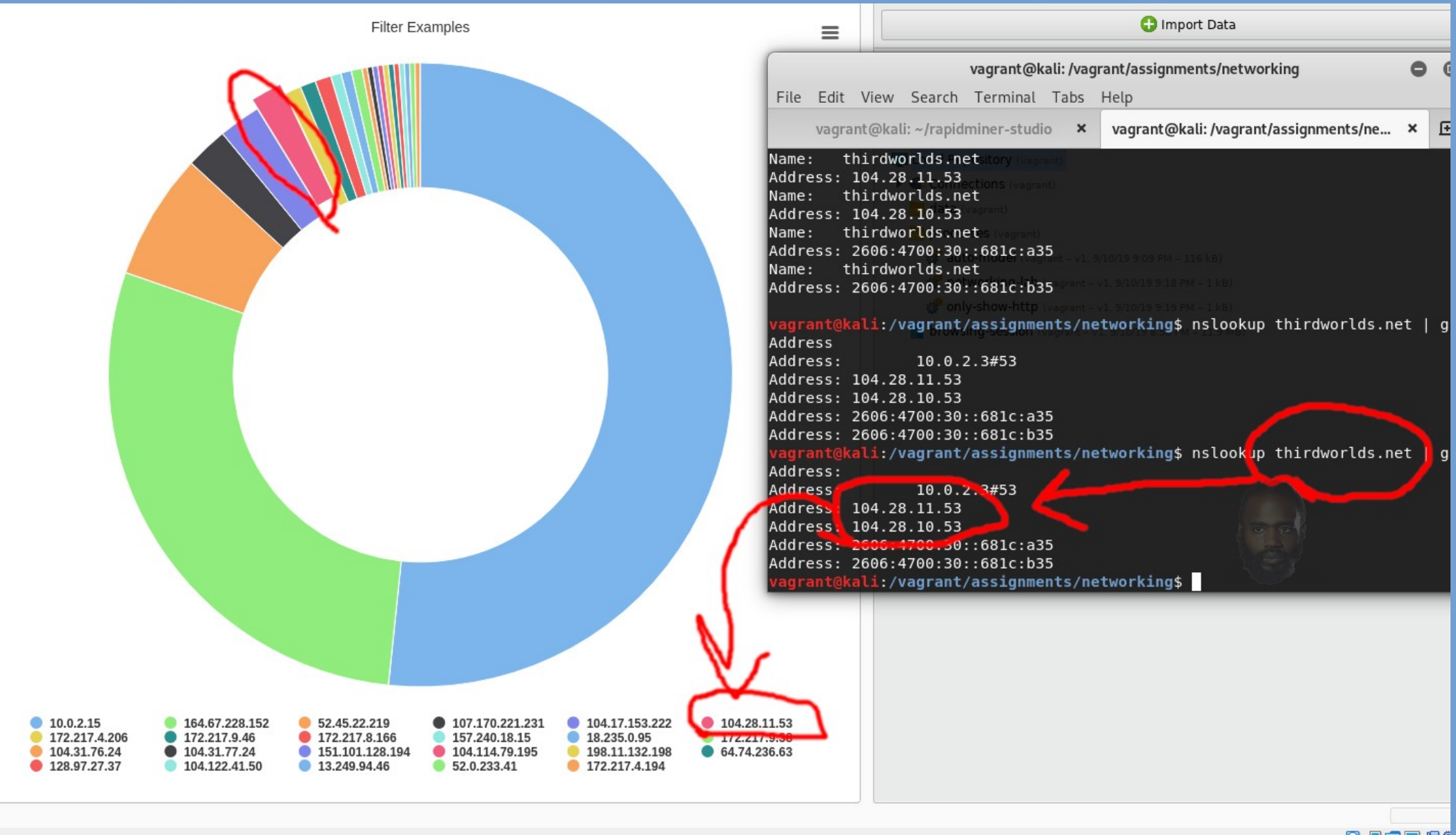
Henry Post

There is no formatting because LibreOffice Impress themes are broken for flat ODP files :)

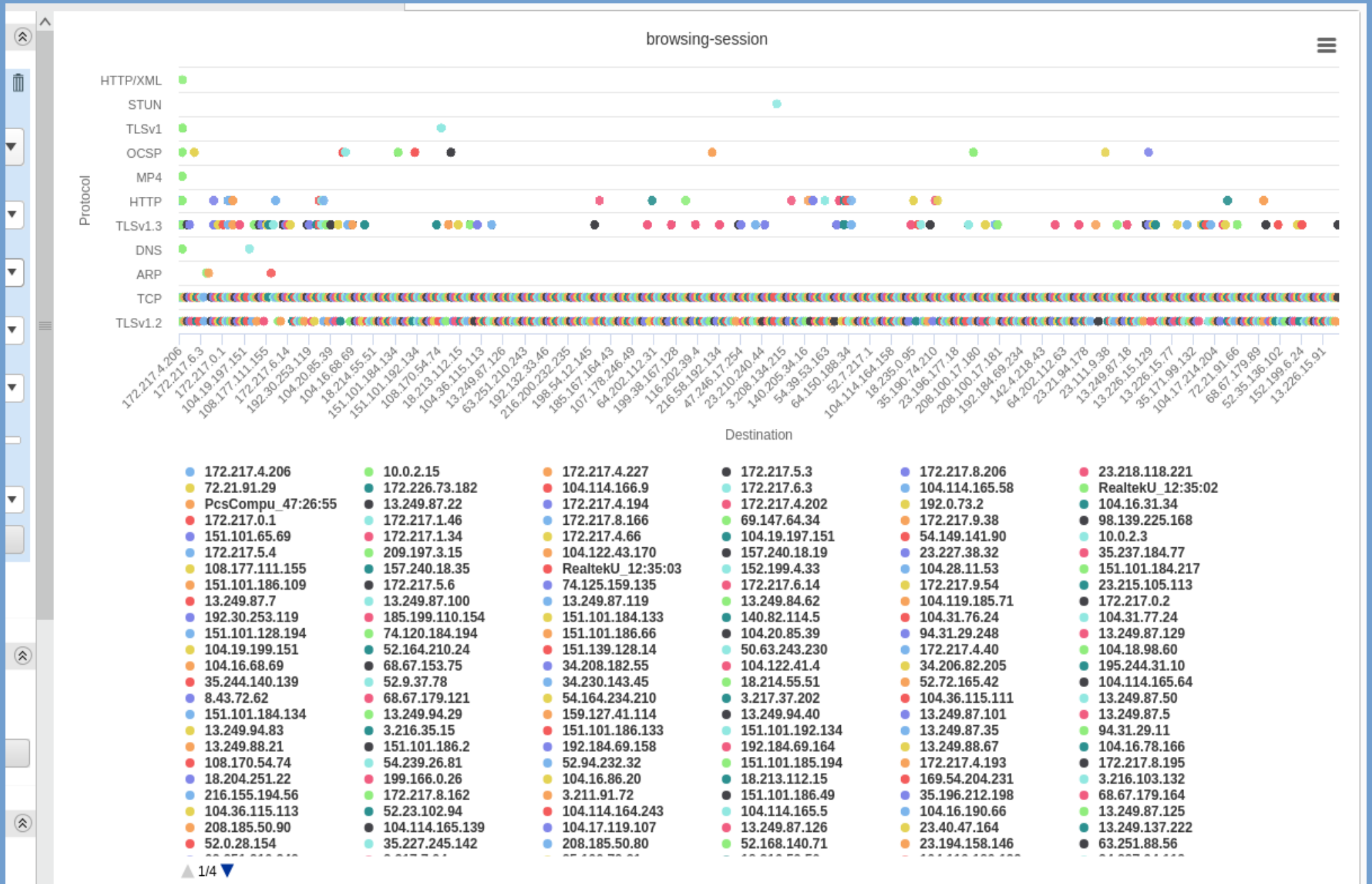
Analysis of Wireshark

- I browsed news sites, music sites, and watched videos while capturing my packets.
- Some was on HTTPS, some on HTTP, and some was other protocols.
- I mainly focused on seeing what I could find out from the HTTP/S traffic because that's web browsing activity, which is often *interesting*.

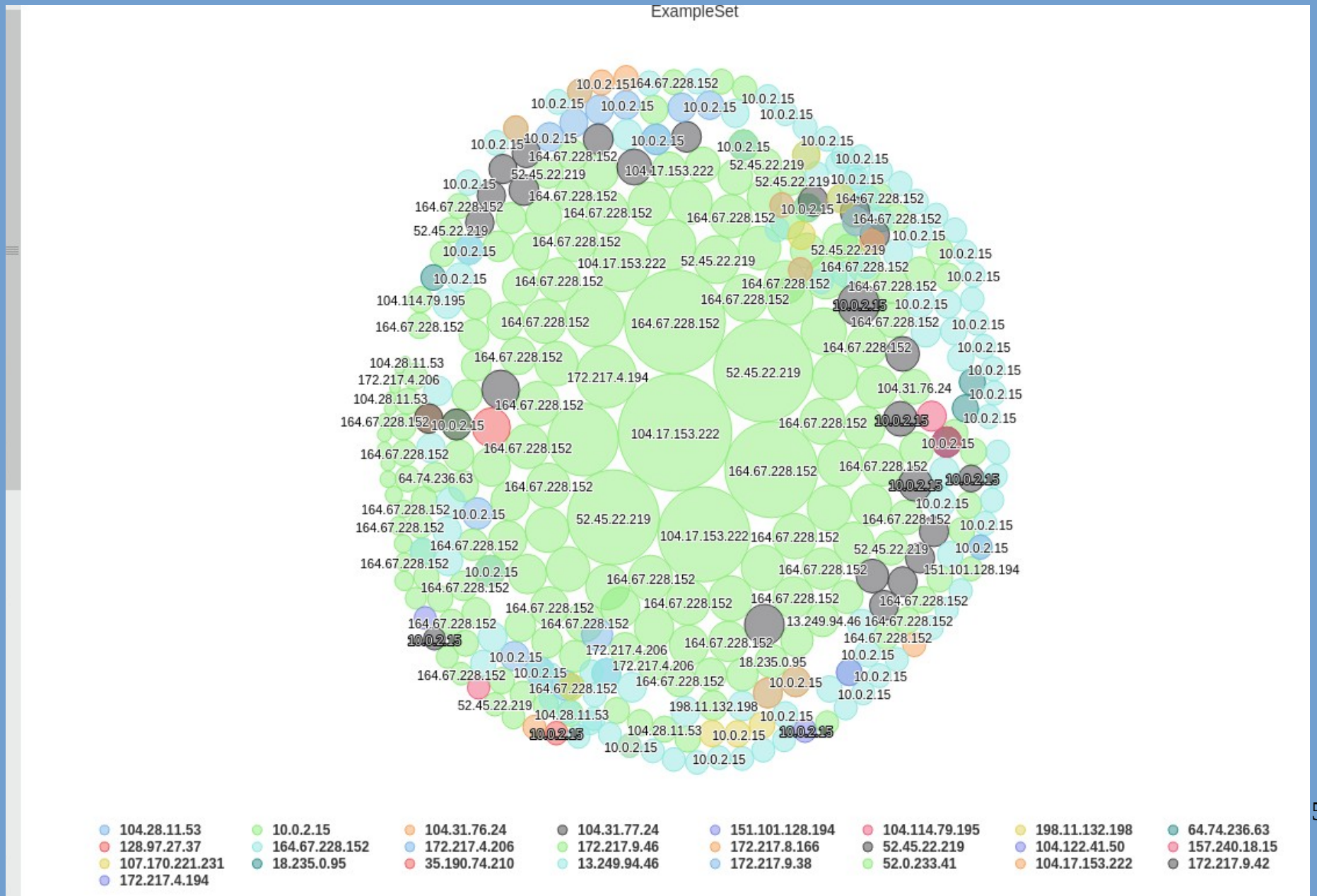
Most HTTP packets tx/rx by IP



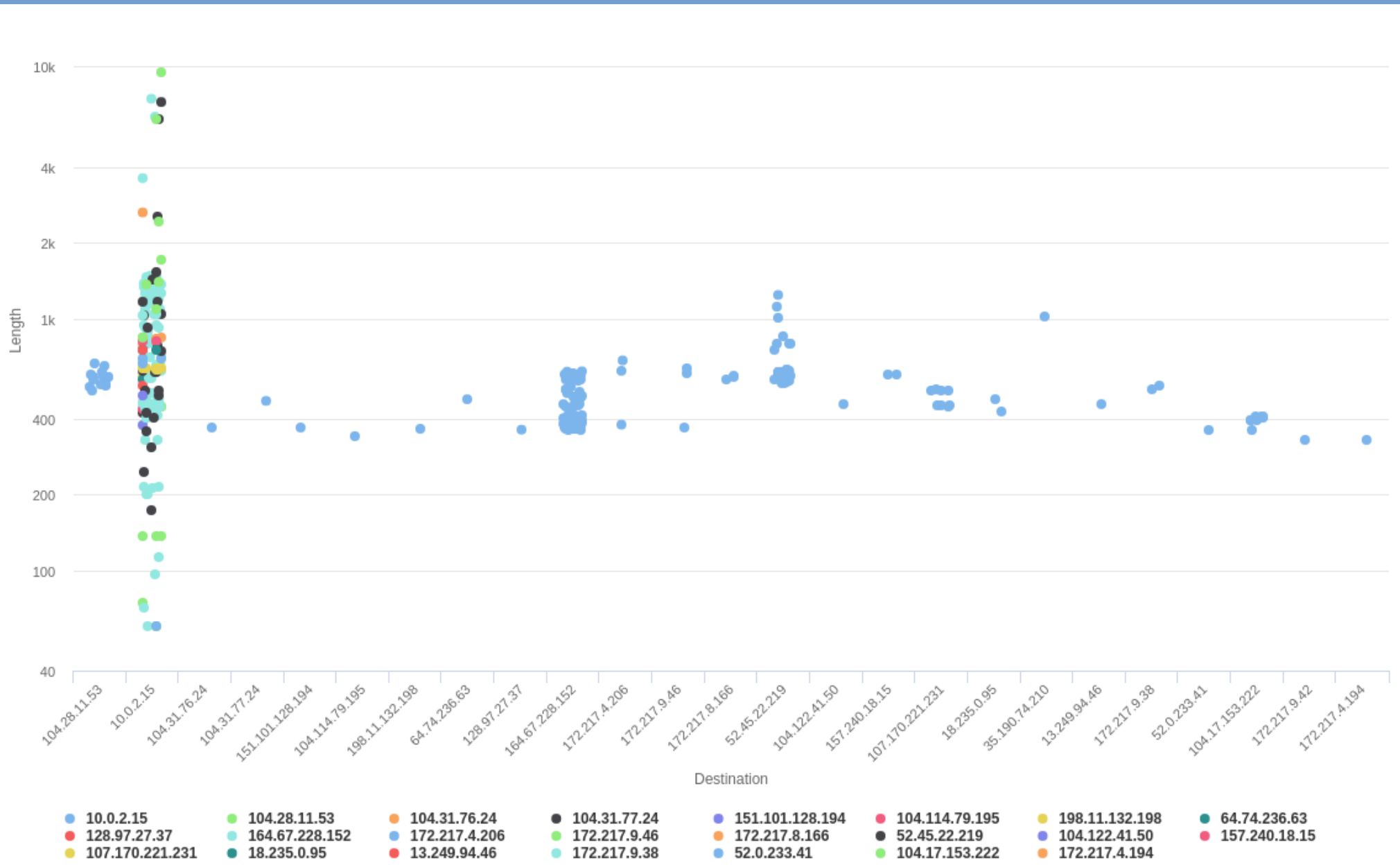
Popular protocols per host



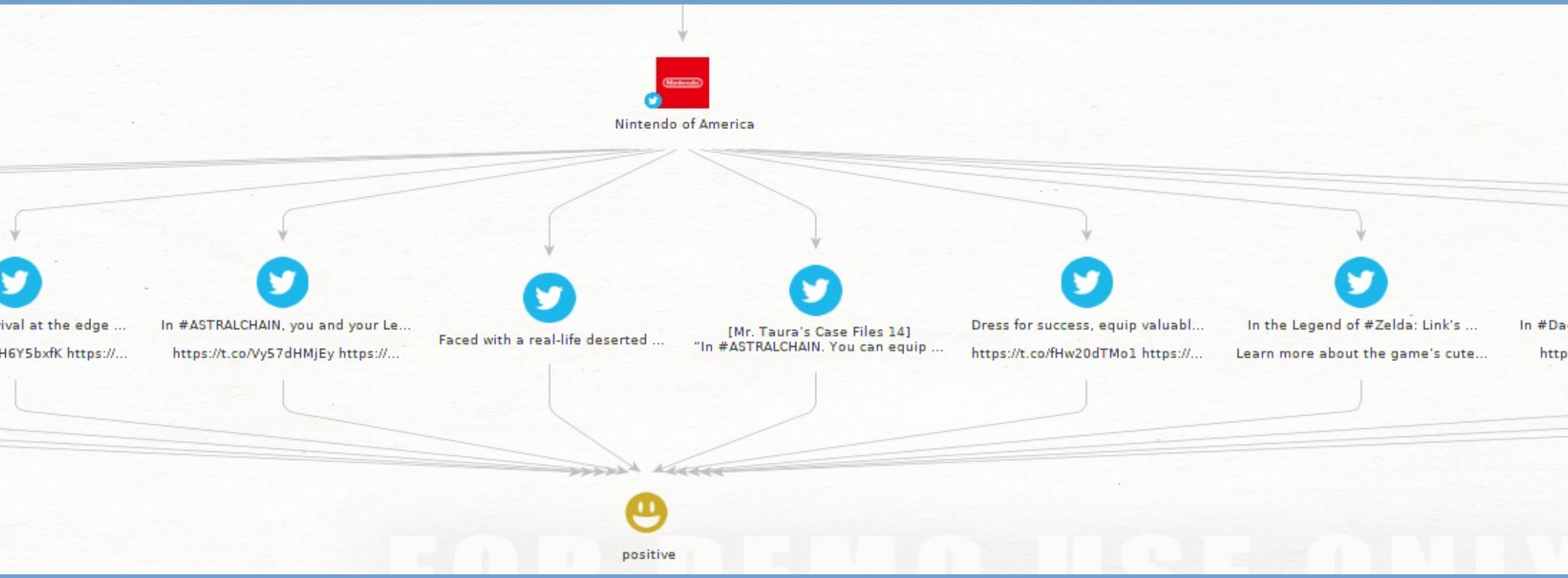
Most HTTP packets, bubble graph



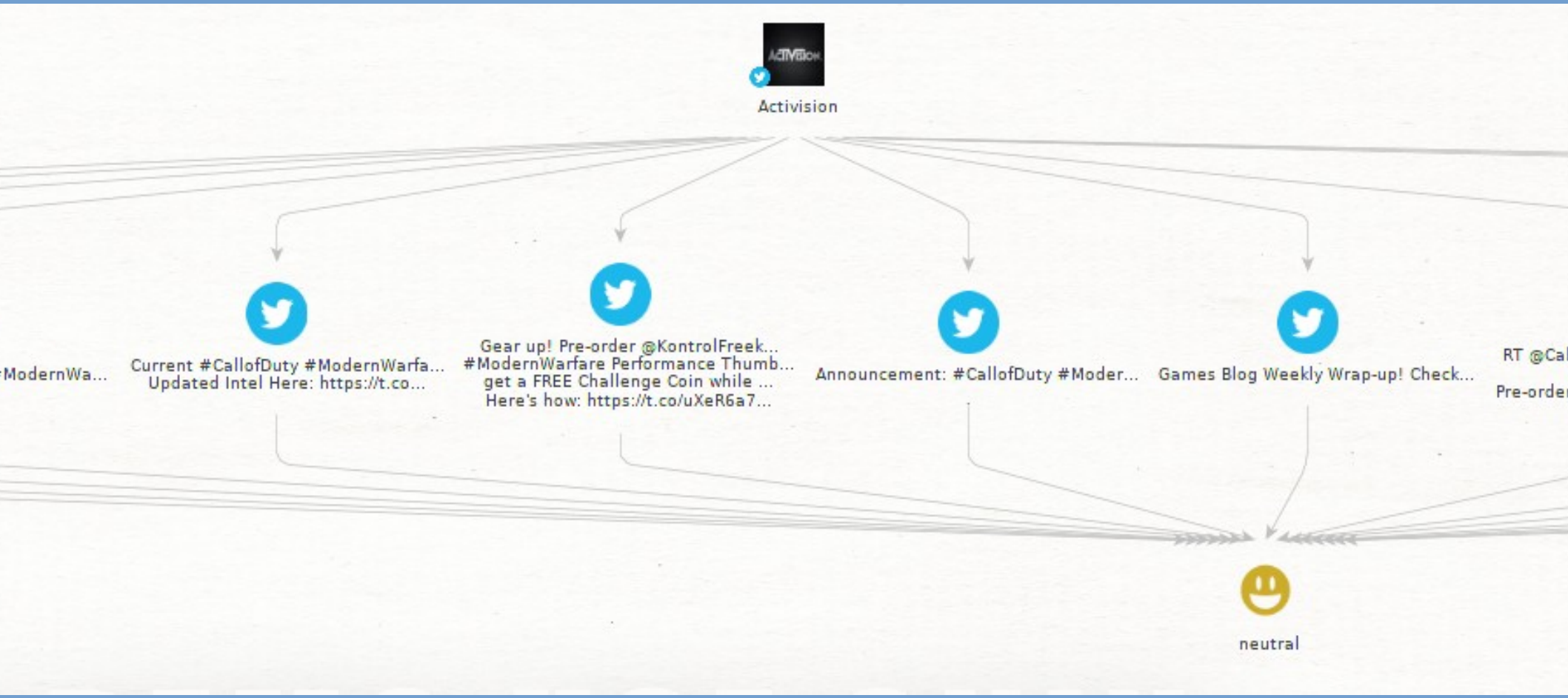
Longest packet sequences per host



Game Retail Twitter Sentiments



Game Retail Twitter Sentiments



nmap and traceroute

Target: scanme.nmap.com ▼ Profile: Intense scan

Command: nmap -T4 -A -v scanme.nmap.com

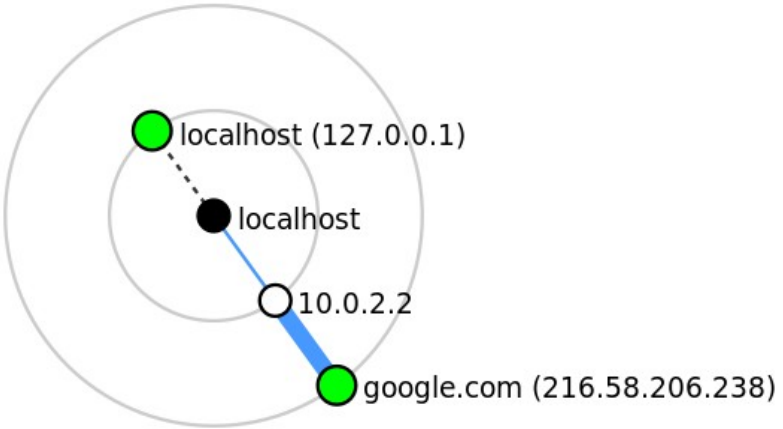
Hosts | Services

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

OS | Host

scanme.nmap

Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25	tcp	filtered	smtp	
80	tcp	open	http	Apache httpd 2.4.7 ((Ubuntu))
139	tcp	filtered	netbios-ssn	
445	tcp	filtered	microsoft-ds	
465	tcp	filtered	smtps	
587	tcp	filtered	submission	
9929	tcp	open	nping-echo	Nping echo
31337	tcp	open	tcpwrapped	



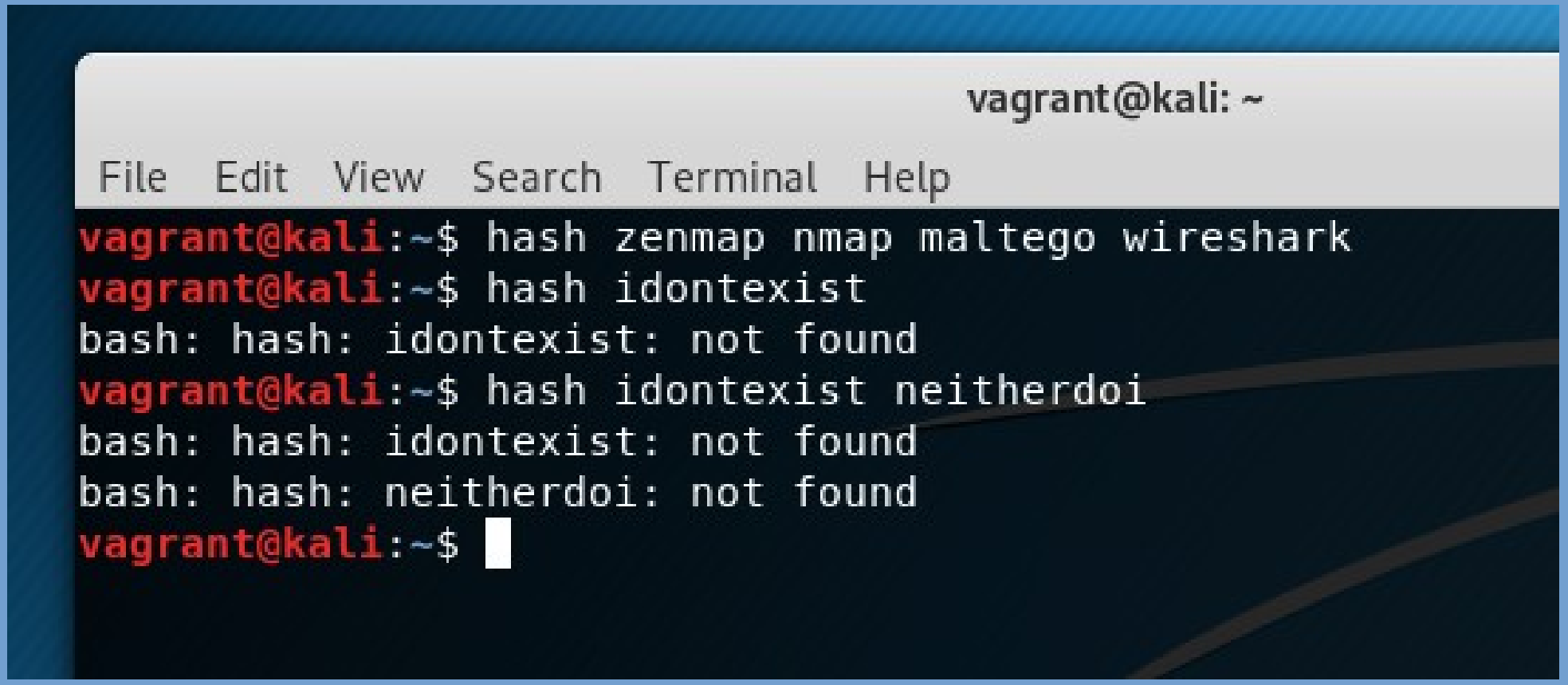
(Don't worry, I only ran traceroute on google.)

Thank you!

Questions?

(Prof. Dawson, go past this slide for other deliverables.)

Installed Programs Proof



UFW config proof

```
Rules updated
Firewall is active and enabled on system startup
Status: active

To                         Action      From
--                         ------      ----
SSH                        ALLOW       Anywhere
224.0.0.251 mDNS           ALLOW       Anywhere
443                        ALLOW       Anywhere
80                         ALLOW       Anywhere
21                         ALLOW       Anywhere
Anywhere                   ALLOW       10.0.0.0/24
5000:5100/udp              ALLOW       Anywhere
22                         ALLOW       192.0.2.0
SSH (v6)                   ALLOW       Anywhere (v6)
ff02::fb mDNS              ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)
21 (v6)                    ALLOW       Anywhere (v6)
5000:5100/udp (v6)         ALLOW       Anywhere (v6)
```

Raw data/graphs/CSV

- See other files in the ZIP file for raw data/graphs/CSV files