

Task 1 - Application Layer

Task 1a - Wireshark - HTTP

- 1 . (a) 104.24.6.6 and 104.24.7.6
(b) 192.168.178.1
(c) 86, DNS
- 2 . (a) 63
(b) `http.request.method == "GET" && ip.dst_host == 104.24.6.6 || ip.dst_host == 104.24.7.6`

Task 1b - Wireshark - Security

- 3 . (a) Tries to signup
(b) Signup info (email address etc)
(c) Yes, a cookie is set (and 200 OK is returned)

Task 1c - Command Line Tools: nmap, nc, curl, wget

- 4 . (a) Yes
(b) Yes
(c) 80/tcp, 443/tcp, 8080/tcp, 8443/tcp
(d) http, https, http-proxy, https-alt
- 5 . (a) `nc -zv -p 4040 www.reddit.com 80`
(b) the header of reddit.com and its source code
- 6 . (a) `nmap -sn 145.100.104.96/27`
(b) 32
- 7 . (a) `nc -l 6060`
(b) `nc localhost 6060`
(c) the terminals have a connection
- 8 . (a) `curl -l www.twitch.tv | perl -n -e '/^Location: (.*)$/ && print "$1\n"'`
(b) nginx

Task 2 - Network Layer

Task 2a - Wireshark - Investigate Traceroute

- 9 . (a) traceroute
(b) 6
(c) The first ICMP messages that does get a response has a TTL = 6

- 10 . (a) Ping requests
 (b) error messages with the ttl exceeded
 (c) it gets a response

Task 2b – Ping and Traceroute - Find availability and RTT

- 11 . (a) All, except bol and amazon
 (b) they disabled ping-requests to prevent DOS-attacks
- 12 . (a) uva: 4.015, ns: 5.828, yahoo: 101.605, alibaba: 160.306
 (b) No
 (c) Some packets have to travel a longer way to the host
 (d) propagation delay
- 13 . (a) translating the ip
 (b) most likely queueing

Task 2c – Traceroute - Find the network path

- 14 . (a) 3
 (b) 80.81.195.152, 54.239.106, 176.32.106.*
 (c) 178.236.0.189. This is in the datacenter of amazon which will have the most delay of congestions
- 15 . (a) 4
 (b) After they reach the Geant server they use the same path, but before they reach Geant they have to take different paths.