Q1

130.102.72.10

Q2

12.622

Graphical user interface, text, application

Description automatically generated

Q3

Number of routers (hops) determined by the difference between ttl for a fresh packet and the one you receive e.g. 64-49 = 15

Q4

ICMP request to 130.0.0.0 says “No response seen” in header indicating no packet was received in response to this one

Q5

Search “icmp && ip.src==192.168.122.129” in statbar at bottom it says Displayed: 102

Q6

Edit -> Find Packet -> change search to ‘string’ and enter the string to search for in the packet info.

Packet 28 is response from DNS containing 3 AAAA records (IPv6)

Q7

Find a DNS response continaing A records. Port is 53

Graphical user interface, application

Description automatically generated with medium confidence

Q8

Packet 745, 747 contains CNAME: youtube-ui.l.google.com

Q9

Packet 115 contains the DNS response. 142.250.167.103 is not there

Q10

Packet 86 is a UDP packet so Length = 42

Q11

Search for string “userinfo.php” packet says pass = Networks2

Q12

DNS query for [www.bom.gov.au](http://www.bom.gov.au) returns 23.48.157.36

Search “ip.dst==23.48.157.36 && http” displays 73 requests

Q13

Any request will show the user agent “Firefox/110.0”

Q14

Sort by length largest GET is 1272

Q15

Find GET request for the image, packet num = 1937. Below the TCP section of the packet tells us that 2 Reassembled TCP segments were used

Q16

<https://osqa-ask.wireshark.org/questions/35635/how-can-i-find-duplicate-ack-packets/>

search “tcp.analysis.duplicate\_ack” shows 53

Q17

“tcp.analysis.retransmission” 3

Q18

“ip.dst==192.168.122.129 && tcp.analysis.duplicate\_ack”

Packet number 217 relative ack = 1385

Q19

Search “dhcp”

Sandbox

Q20

In the last dhcp ACK packet te lease is listen in the Options at the bottom as 1 hour = 3600 sec