Questions

1)Start a Wireshark capture and browse to twitter.com . Use display filtering to reduce displayed packets to only those sent and received by your computer. How many sites are you actually interacting with when you interact with Twitter? What are they?

A capture filter limits packets that Wireshark receives from the kernel.Filter expressions are actually compiled down to bytecode blobs,these blobs are passed to the kernel, and the kernel filters thepackets it passes up to Wireshark. This is the same language thattcpdump uses; it is described in the tcpdump manpage ("man tcpdump",skip to EXAMPLES).

Useful capture filters:

"host 129.170.17.4" -- capture only packets to or from 129.170.17.4

"icmp" -- capture only ICMP packets

"arp" -- capture only ARP packets

"icmp or arp" -- capture ICMP packets or ARP packets

"not arp" -- capture all packets but arp "port 22" -- capture only packets from or to port 22 (TCP or UDP) "not port 22" -- capture all packets but those from or to port 22 (TCP or UDP)

"ip[9] == 0x6" -- capture all IP packets that have 0x06 as the 9th byte of their IP header (this is the same as "tcp", incidentally, because TCP's protocol # is 6)

"ether[12:2] == 0x0806" -- capture only those Ethernet packets that have 0x0806 as their 13th & 14th bytes (the two-byte word). This is the same as "arp", because 0x0806 is the protocol number of ARP in the Ethernet header. see EXAMPLES in "man tcpdump" for more3.

a) Write and test capture filters that capture only your machine's ARP requests. How often are they sent (i.e., how many ARP packets your machine sends per minute, on average?) This, of course, depends on your OS and network usage pattern.

b) Write and test capture filters that capture only ARP requests sent to your computer. Who sends them, and how often?

In this first part you will examine a packet capture for a web browsing operation. Open the capture file ‘http.cap’ (clear any display filters) and use WireShark to answer the following questions:

1. What is the IP address of the host?

2. What is the IP address of the router?

3. What protocol is used to resolve the website domain name?

4. What is the IP address of the HTTP server?

5. Which transport layer protocol is used by DNS?

6. Which well-known port is used when contacting the DNS server?

7. Which ephemeral port does the host initiating the DNS query use?

8. What is the Ethernet address of the host?

9. What is the Ethernet address of the router?

10. How long does the 3-way handshake take to complete?

11. Which website is the host machine trying to access?

12. What version of HTTP is the browser running?

13. In the filter box enter the following query: udp.dstport==53 and click apply. What does the query mean and what are the results?

14. Go to Statistics -> Protocol Hierarchy and answer: A. What percentage of frames are Ethernet frames? B. Which transport layer protocols were present and which one made up more of the traffic?

15. Now plot the UDP and TCP traffic as follows:

● Go to Statistics -> IO Graph (Adjust Interval as appropriate)

● Click + and add Display filter: tcp (Rest of the information can be default)

● Click + and add Display filter: udp (Rest of the information can be default)

● Click + and add Display filter: http and Y Axis: Bits (Rest of the information can be default)

Answer the following questions:

A. What is the highest number of TCP packets/sec observed? Around what time (second)?

B. What is the highest number of UDP packets/sec observed? Around what time (second)?

C. What is the highest number of HTTP bits/sec observed? Around what time (second)?