COMP 9121 Week 10 Lab

1. Wireshark DNS

1.1. Open dns_tut1.pcap. This is a DNS lookup from a computer in a home. Answer the following questions:
• Which one is the name server here? 192.168.178.1
• How is the client doing the lookup? Is this a recursive query? How do you know? yes
• What is queried here? Give resource record and domain name. independent.ie
• Does the server support recursive queries? How do you know? yes
• Was the reply received from a server that is authoritative for the zone? No

1.2. Open dns_tut2.pcap. This is another query, within the same setting.
• What is being queried? www.independent.ie
• Explain the reply to the query, based on the two types of received records! How many 'A results' are received? 8
• Investigate more closely: what is Cloudfront (Google it)? What kind of hosting of the web server is this?

1.3Open dns_tut3.pcap. Then answer:
• What happened here? query a domain does not exist

2. Wireshark HTTP

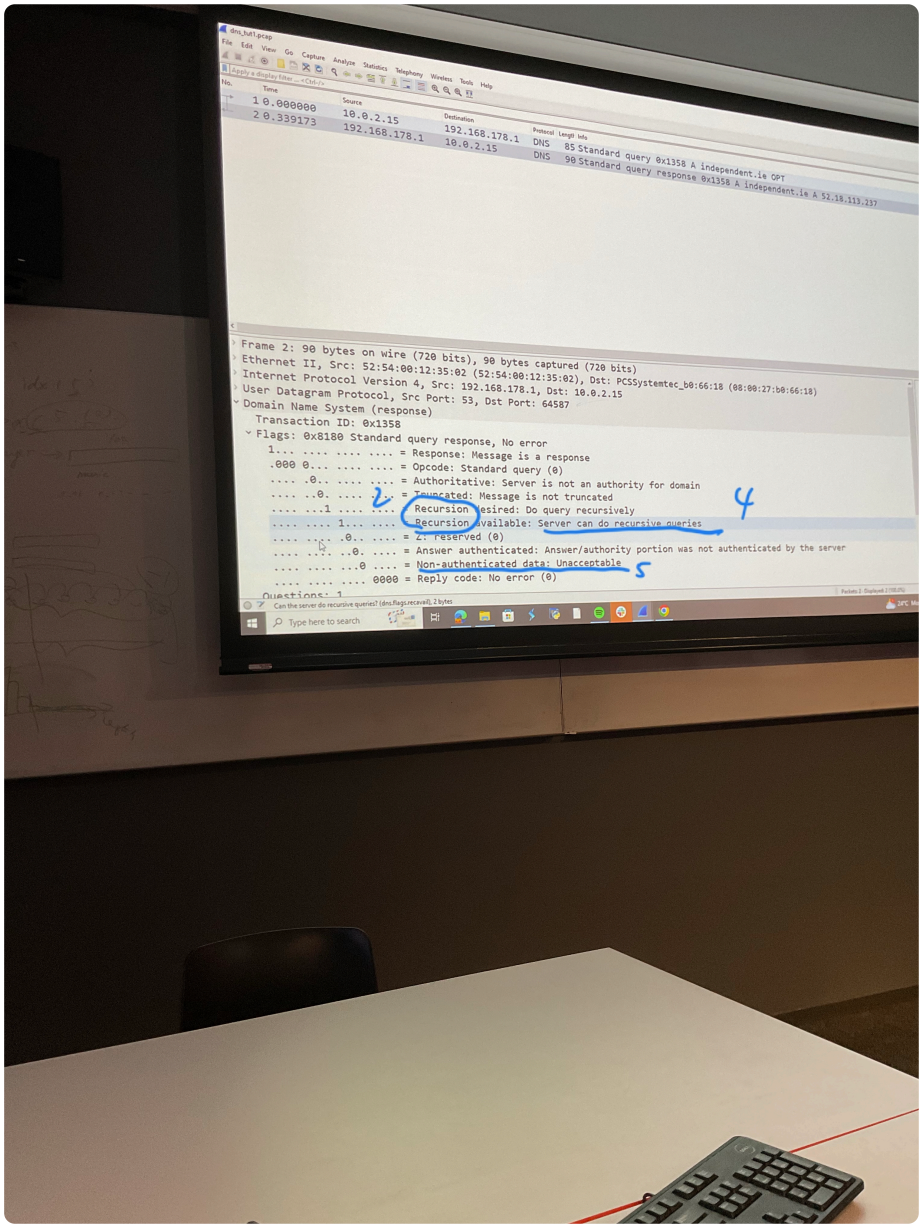
1. Open http_tut1.pcap. Then answer:
• What site is being accessed?
• Does the site set a cookie? How many? How do you know?
• What browser was used? How do you know?
• What does the first HTTP response code mean? → 大于400 的回答
• Is there a failed HTTP request? What did you look for?
• Why is there more than one HTTP GET? How are elements of the website loaded?
• Is non-persistent or persistent HTTP used? → connection: keep-alive persistent
• Why are there so many TCP connections?

2. Did you ever wonder how sites such as Ebay 'recognise' you and have the items in your shopping cart ready for you to order? Open http_tut2.pcap. **This capture was taken after closing and then opening the browser again, and then surfing to the site.** Answer:
• How is the server able to recognise the browser? Give the frame that contains the solution and explain. cookies
• Can the server distinguish between different people using the same browser?

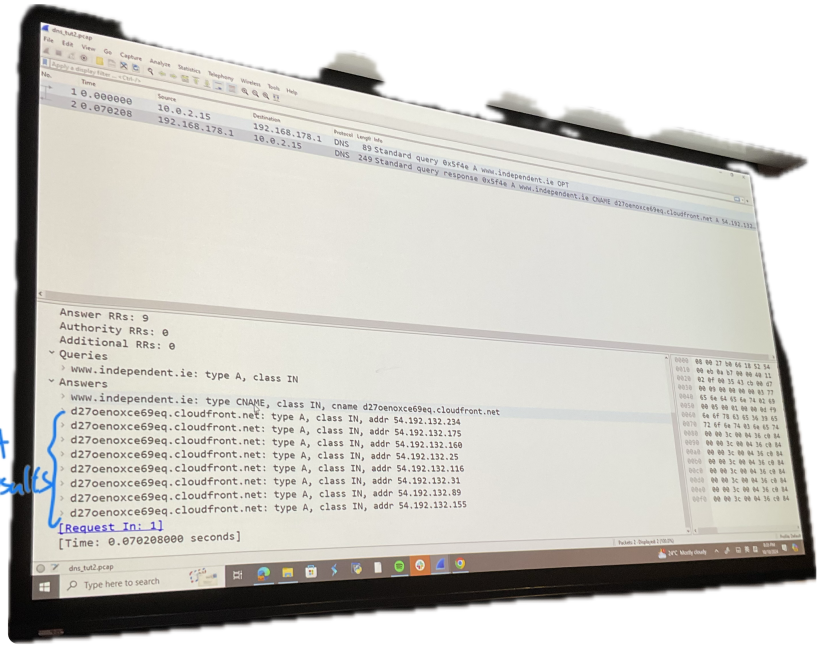
1.1

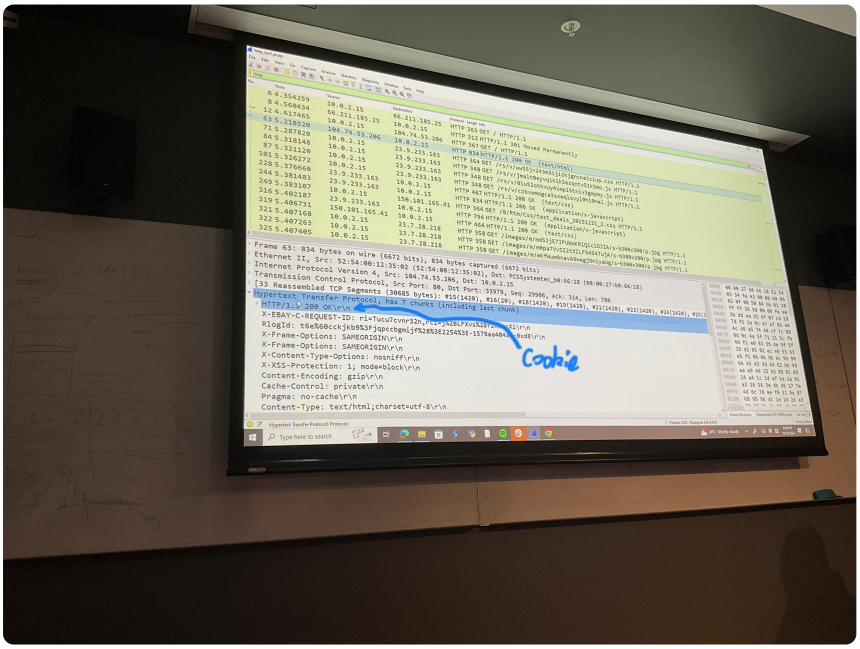
(٢)

(٤)


1 0.000000 10.0.2.15 192.168.178.1 DNS 85 Standard query 0x1358 A independent.ie OPT
2 0.339173 192.168.178.1 10.0.2.15 DNS 90 Standard query response 0x1358 A independent.ie A 52.18.113.237
Frame 2: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_b0:66:18 (08:00:27:b0:66:18)
Internet Protocol Version 4, Src: 192.168.178.1, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 64587
Domain Name System (response)
Transaction ID: 0x1358
Flags: 0x8180 Standard query response, No error
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not an authority for domain
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available: Server can do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 .... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Type here to search

1.2


1 0.000000 10.0.2.15 192.168.178.1 DNS 89 Standard query 0x5f4e A www.independent.ie OPT
2 0.070208 192.168.178.1 10.0.2.15 DNS 249 Standard query response 0x5f4e A www.independent.ie CNAME d27oenoxce69eq.cloudfront.net A 54.192.132.
Answer RRs: 9
Authority RRs: 0
Additional RRs: 0
Queries
www.independent.ie: type A, class IN
Answers
www.independent.ie: type CNAME, class IN, cname d27oenoxce69eq.cloudfront.net
d27oenoxce69eq.cloudfront.net: type A, class IN, addr 54.192.132.234
d27oenoxce69eq.cloudfront.net: type A, class IN, addr 54.192.132.175
d27oenoxce69eq.cloudfront.net: type A, class IN, addr 54.192.132.160
d27oenoxce69eq.cloudfront.net: type A, class IN, addr 54.192.132.25
d27oenoxce69eq.cloudfront.net: type A, class IN, addr 54.192.132.116
d27oenoxce69eq.cloudfront.net: type A, class IN, addr 54.192.132.31
d27oenoxce69eq.cloudfront.net: type A, class IN, addr 54.192.132.89
d27oenoxce69eq.cloudfront.net: type A, class IN, addr 54.192.132.155
[Request In: 1]
[Time: 0.070208000 seconds]
8 A results


Cookie