

S11L4



Data: 12/12/24

INFORMAZIONI PRINCIPALI

Laboratorio - Esplorazione del Traffico DNS

In questo laboratorio, completa i seguenti obiettivi:

1. Catturare il traffico DNS

- Avvia uno strumento come Wireshark per monitorare il traffico di rete.
- Filtra il traffico per il protocollo DNS (dns O porta UDP 53 standard).

2. Esplorare il traffico delle query DNS

- Identifica le richieste DNS effettuate dai dispositivi verso i server DNS.
- Analizza i dettagli delle query, come il nome del dominio richiesto e il tipo di record (es. A).

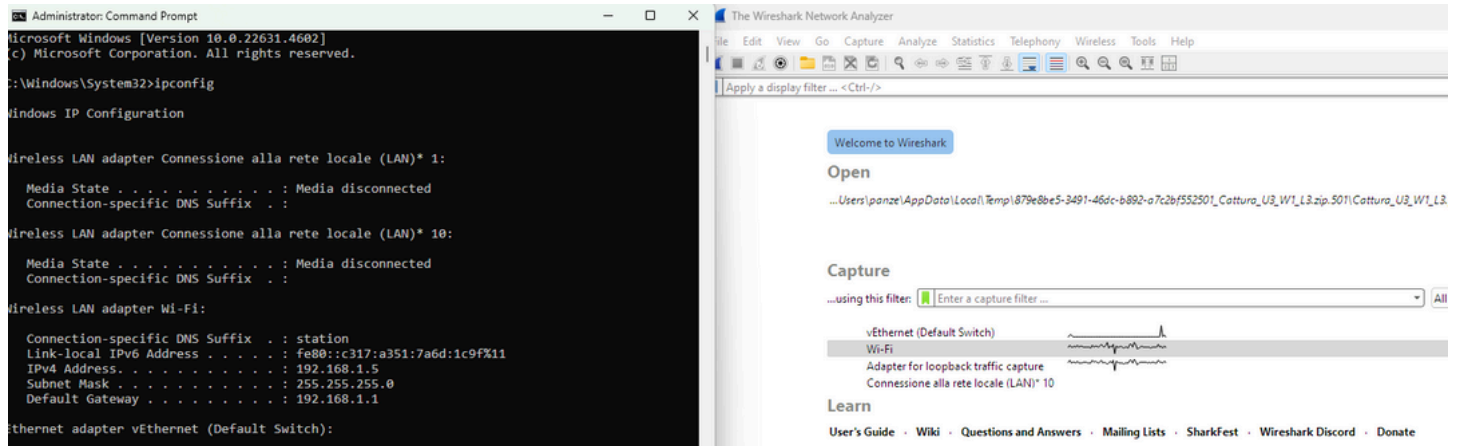
3. Esplorare il traffico delle risposte DNS

- Individua le risposte DNS inviate dai server ai dispositivi.
- Analizza le informazioni fornite, come l'indirizzo IP associato al dominio o eventuali errori di risoluzione.

Premessa: Invece di andagare su “cisco” ho analizzato discord.com (the point of the exercise remains the same and the completion equal (if not better-going over as always.) it's just to make it different.

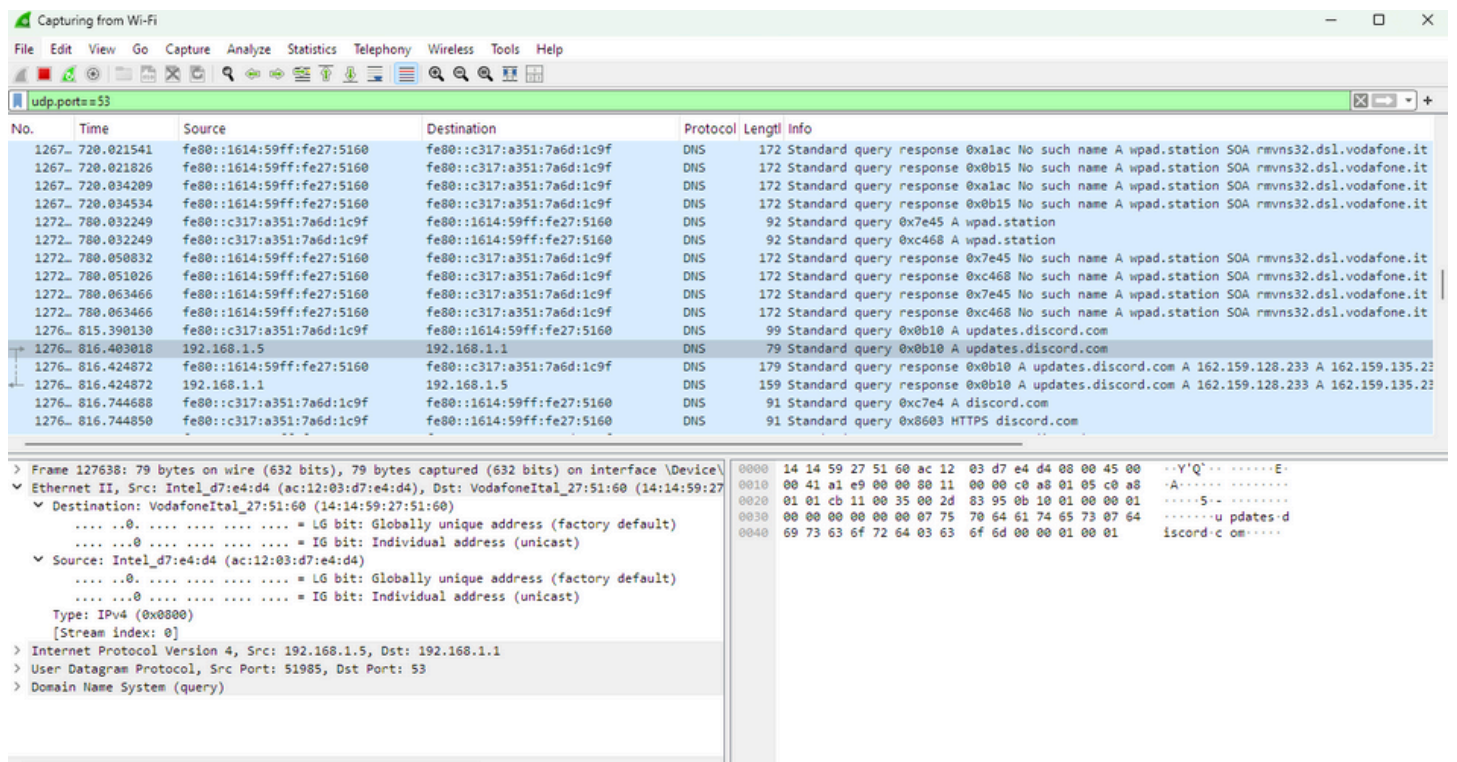
INIZIO ESERCIZIO

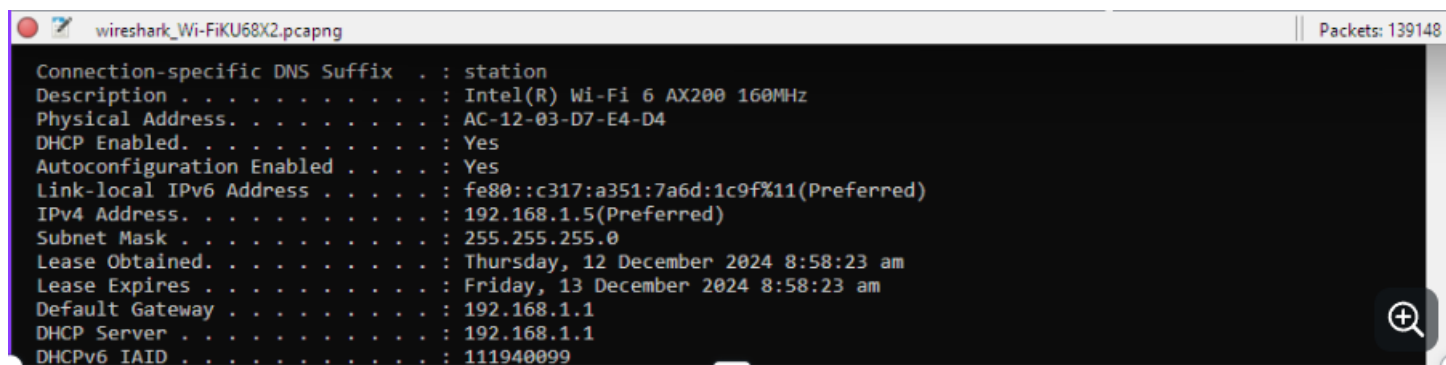
Apriamo wireshark e selezioname la nostra rete (for showcase i just also did an ipconfig showing that it's associated with a wireless adapter)



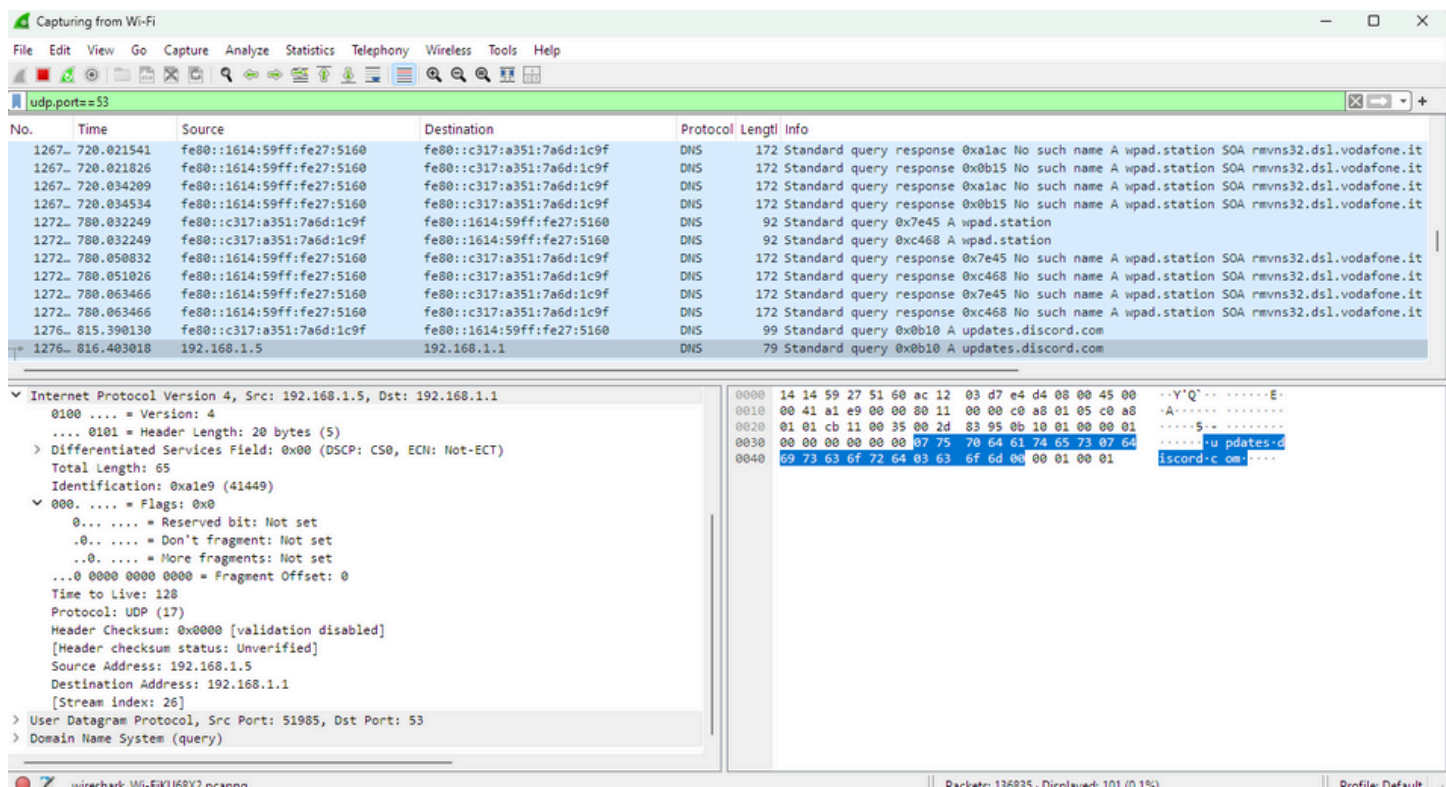
Eseguiamo un ipflush su windows mentre wireshark è in “mezzo” e andremo ad osservare le richieste. Nel filtro possiamo specificare il protocollo UDP (totale) o restringere la ricerca alla porta 53, specifica per il DNS. Poi apriamo il pannello dettagliato e espandiamo l'opzione ethernet2 che contiene l'intestazione i dati/payload e il CRC. (((Crc per il controllo di errori di trasmissione (check) dati e payload es. pacchetti ip* (intestazione: time to live, ipv4 o 6 etc payload richieste http.)))

Vediamo che “source” è associato a alla mia scheda di rete “intel” con indirizzo mac fisico AC120307 e la destinazione è il gateway o il mio router.





Estendiamo internet protocol e vediamo che l'indirizzo ip del source è associata alla nostra scheda di rete mentre alla destinazione riconfermiamo che è il gateway.



La porta da parte della “sorgente” (in questo caso noi 1.5) è 51985 (casuale/random every time just for this part is entire connection is set to 51985, next time it may be something else). E la destinazione (1.1) sulla porta 53 (DNS) (Standard DNS)

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
1267...	720.021541	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0xalac No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1267...	720.021826	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x0b15 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1267...	720.034209	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0xalac No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1267...	720.034534	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x0b15 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272...	780.032249	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	92	Standard query 0x7e45 A wpad.station
1272...	780.032249	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	92	Standard query 0xc468 A wpad.station
1272...	780.050832	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x7e45 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272...	780.051026	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0xc468 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272...	780.063466	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x7e45 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272...	780.063466	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0xc468 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1276...	815.390130	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	99	Standard query 0x0b10 A updates.discord.com
1276...	816.403018	192.168.1.5	192.168.1.1	DNS	79	Standard query 0x0b10 A updates.discord.com

> Frame 127638: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF...
 > Ethernet II, Src: Intel_d7:e4:d4 (ac:12:03:d7:e4:d4), Dst: VodafoneItalia_27:51:60 (14:14:59:27:51:60)
 > Internet Protocol Version 4, Src: 192.168.1.5, Dst: 192.168.1.1
 > User Datagram Protocol, Src Port: 51985, Dst Port: 53
 > Source Port: 51985
 > Destination Port: 53
 > Length: 45
 > Checksum: 0x8395 [unverified]
 > [Checksum Status: Unverified]
 > [Stream index: 119]
 > [Stream Packet Number: 1]
 > [Timestamps]
 > UDP payload (37 bytes)
 > Domain Name System (query)

Adesso espandiamo domain system e troviamo il tipo di risposta (il messaggio è una query) il tipo (standard) se è stato “truncated” o se ha dei “byte” riservati e sei dati non autenticati sono “accettabili”. A noi interessa per l’esercizio la recursion, ed è impostata su “do query”. In caso della risoluzione ricorsiva, il server DNS interroga altri server DNS fino a ottenere una risposta completa da restituire al client. altrimenti se sarebbe impostato su do not query recursively Il server DNS non esegue la risoluzione completa, ma risponde con un riferimento al prossimo server DNS da interrogare (modalità iterativa). il server dns risponderà al client u chi dovrà dopo interrogare per ottenere gli indirizzi ip associati ai nomi di dominio.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
1267...	720.021541	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0xalac No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1267...	720.021826	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x0b15 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1267...	720.034209	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0xalac No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1267...	720.034534	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x0b15 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272...	780.032249	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	92	Standard query 0x7e45 A wpad.station
1272...	780.032249	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	92	Standard query 0xc468 A wpad.station
1272...	780.050832	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x7e45 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272...	780.051026	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0xc468 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272...	780.063466	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x7e45 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272...	780.063466	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0xc468 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1276...	815.390130	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	99	Standard query 0x0b10 A updates.discord.com
1276...	816.403018	192.168.1.5	192.168.1.1	DNS	79	Standard query 0x0b10 A updates.discord.com

Type: IPv4 (0x0800)
 [Stream index: 0]
 > Internet Protocol Version 4, Src: 192.168.1.5, Dst: 192.168.1.1
 > User Datagram Protocol, Src Port: 51985, Dst Port: 53
 > Domain Name System (query)
 > Transaction ID: 0x0b10
 > Flags: 0x0100 Standard query
 > 0... .. = Response: Message is a query
 > .000 0... .. = Opcode: Standard query (0)
 > = Truncated: Message is not truncated
 > = Recursion desired: Do query recursively
 > = Z: reserved (0)
 > = Non-authenticated data: Unacceptable
 > Questions: 1
 > Answer RRs: 0
 > Authority RRs: 0
 > Additional RRs: 0
 > Queries
 > updates.discord.com: type A, class IN
 > [Response In: 127642]

Do query recursively? (dns.flags.recdesired). 1 bit

Packets: 140913 - Displayed: 101 (0.1%) Profile: Default

Procediamo con la risposta (ipv4 for showing purposes, you can clearly see there is both ipv4/ipv6 “calls” and answers.) Adesso si sono invertiti i ruoli. la precedente "destinazione" è adesso diventata "sorgente" e Sorgente ora è destinazione <>. Lo confermiamo sia a primo impatto da l'indirizzo ip 1.1 su source ma lo confermiamo con il mac nella sezione ethernet2 (execeise has to be this way) lui sta rispondendo a noi 1.1>1.5 con le liste DNS (per poter associare i nomi di dominio ad indirizzi ip 233 e 232) La porta si è invertita in equalmodo. Porta 53>51985e anche lui in modo recursivo

Wireshark packet capture showing DNS traffic. The packet list shows a series of DNS queries and responses. The packet details pane shows the structure of a DNS response packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (response). The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1267	720.034534	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x0b15 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272	780.032249	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	92	Standard query 0x7e45 A wpad.station
1272	780.032249	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	92	Standard query 0xc468 A wpad.station
1272	780.050832	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x7e45 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272	780.051026	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0xc468 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272	780.063466	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x7e45 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272	780.063466	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0xc468 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1276	815.390130	fe80::1614:59ff:fe27:5160	fe80::1614:59ff:fe27:5160	DNS	99	Standard query 0x0b10 A updates.discord.com
1276	816.403018	192.168.1.5	192.168.1.1	DNS	79	Standard query 0x0b10 A updates.discord.com
1276	816.424072	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	179	Standard query response 0x0b10 A updates.discord.com A 162.159.128.233 A 162.159.135.232
1276	816.424872	192.168.1.1	192.168.1.5	DNS	159	Standard query response 0x0b10 A updates.discord.com A 162.159.128.233 A 162.159.135.232
1276	816.744688	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	91	Standard query 0xc7e4 A discord.com

Frame 127642: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface \Device\NPF...
 Ethernet II, Src: VodafoneItal_27:51:60 (14:14:59:27:51:60), Dst: Intel_d7:e4:d4 (ac:12:03:d7:e4:d4)
 Destination: Intel_d7:e4:d4 (ac:12:03:d7:e4:d4)
 Source: VodafoneItal_27:51:60 (14:14:59:27:51:60)
 Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.5
 User Datagram Protocol, Src Port: 53, Dst Port: 51985
 Domain Name System (response)

Stiamo chiedendo al server di fare il "lavoro completo" e lui ci risponde si ok va bene con do recursive. Se il server non supporta la risoluzione ricorsiva, invierà una risposta parziale o iterativa, con informazioni sul server successivo da interrogare.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
1267	720.034534	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x0b15 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272	780.032249	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	92	Standard query 0x7e45 A wpad.station
1272	780.032249	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	92	Standard query 0xc468 A wpad.station
1272	780.050832	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x7e45 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272	780.051026	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0xc468 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272	780.063466	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0x7e45 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1272	780.063466	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	172	Standard query response 0xc468 No such name A wpad.station SOA rmvns32.dsl.vodafone.it
1276	815.390130	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	99	Standard query 0x0b10 A updates.discord.com
1276	816.403018	192.168.1.5	192.168.1.1	DNS	79	Standard query 0x0b10 A updates.discord.com
1276	816.424872	fe80::1614:59ff:fe27:5160	fe80::c317:a351:7a6d:1c9f	DNS	179	Standard query response 0x0b10 A updates.discord.com A 162.159.128.233 A 162.159.135.232
1276	816.424872	192.168.1.1	192.168.1.5	DNS	159	Standard query response 0x0b10 A updates.discord.com A 162.159.128.233 A 162.159.135.232
1276	816.744688	fe80::c317:a351:7a6d:1c9f	fe80::1614:59ff:fe27:5160	DNS	91	Standard query 0xc7e4 A discord.com

Type: IPv4 (0x0800)
[Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.5
> User Datagram Protocol, Src Port: 53, Dst Port: 51985
▼ Domain Name System (response)
Transaction ID: 0x0b10
▼ 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
... ..0... .. = Non-authenticated data: Unacceptable
... ..0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 5
Authority RRs: 0
... ..

0000 ac 12 03 d7 e4 d4 14 14 59 27 51 60 08 00 45 00 Y'Q'...E:
0010 00 91 4a 55 00 00 40 11 ac b0 c0 a8 01 01 c0 a8 ...JU...@
0020 01 05 00 35 cb 11 00 7d 5b ec 0b 10 81 80 00 01 ...5...} [.....
0030 00 05 00 00 00 00 07 75 70 64 61 74 65 73 07 64u pdates: d
0040 69 73 63 6f 72 64 03 63 6f 6d 00 00 01 00 01 c0 iscord-c om.....
0050 0c 00 01 00 01 00 00 00 8e 00 04 a2 9f 80 e9 c0
0060 0c 00 01 00 01 00 00 00 8e 00 04 a2 9f 87 e8 c0
0070 0c 00 01 00 01 00 00 00 8e 00 04 a2 9f 88 e8 c0
0080 0c 00 01 00 01 00 00 00 8e 00 04 a2 9f 89 e8 c0
0090 0c 00 01 00 01 00 00 00 8e 00 04 a2 9f 8a e8
.....

wireshark: Wi-FiK16RX7.ncannn

Packets: 143330 · Displayed: 132 (0.1%)

Profile: Default

Scorriamo in basso e controlliamo con nslookup (il nostro server DNS impostato e indirizzo) e con nslookup discord.com tutti gli indirizzi ip associato al dominio discord.com e vediamo che le richieste sono corrette e coincidono, completando l'esercizio. (Type A-ANSWER risponde con la richiesta a Chi è discord.com? discord è 162.x.x.232 e 162.x.x.233 associando nome di dominio a indirizzi ip.)

```

C:\Windows\System32>nslookup
Default Server: vodafone.station
Address: fe80::1614:59ff:fe27:5160

> nslookup discord.com
Server: discord.com
Addresses: 162.159.128.233
          162.159.135.232
          162.159.137.232
          162.159.138.232
          162.159.136.232

*** discord.com can't find nslookup: Non-existent domain

```

Class: IN (0x0001)
Time to live: 142 (2 minutes, 22 seconds)
Data length: 4
Address: 162.159.128.233
▼ updates.discord.com: type A, class IN, addr 162.159.135.232
Name: updates.discord.com
Type: A (1) (Host Address)
Class: IN (0x0001)
Time to live: 142 (2 minutes, 22 seconds)
Data length: 4
Address: 162.159.135.232
▼ updates.discord.com: type A, class IN, addr 162.159.136.232
Name: updates.discord.com

0000 ac 12 03 d7 e4 d4 14 14 59 27 51 60 08 00 45 00 Y'Q'...E:
0010 00 91 4a 55 00 00 40 11 ac b0 c0 a8 01 01 c0 a8 ...JU...@
0020 01 05 00 35 cb 11 00 7d 5b ec 0b 10 81 80 00 01 ...5...} [.....
0030 00 05 00 00 00 00 07 75 70 64 61 74 65 73 07 64u pdates: d
0040 69 73 63 6f 72 64 03 63 6f 6d 00 00 01 00 01 c0 iscord-c om.....
0050 0c 00 01 00 01 00 00 00 8e 00 04 a2 9f 80 e9 c0
0060 0c 00 01 00 01 00 00 00 8e 00 04 a2 9f 87 e8 c0
0070 0c 00 01 00 01 00 00 00 8e 00 04 a2 9f 88 e8 c0
0080 0c 00 01 00 01 00 00 00 8e 00 04 a2 9f 89 e8 c0
0090 0c 00 01 00 01 00 00 00 8e 00 04 a2 9f 8a e8
.....

Response IPv4 Address (dns.a). 4 bytes

Packets: 147057 · Display

RECAP

1. Dopo aver avviato Wireshark, filtriamo il traffico DNS utilizzando il filtro `udp.port==53`. Questo ci permette di osservare sia le query che le risposte DNS.
2. Espandendo l'opzione Ethernet nel pannello dettagliato, vediamo che l'indirizzo MAC sorgente appartiene alla nostra scheda di rete (Intel, MAC AC:12:03:07). La destinazione iniziale è il gateway (1.1).
3. Analizzando il protocollo IP, notiamo che la sorgente è l'indirizzo del nostro dispositivo (1.5), mentre la destinazione è il server DNS del gateway (1.1). La porta UDP sorgente è casuale (51985), mentre la destinazione utilizza la porta standard 53.
4. All'interno del protocollo DNS, analizziamo i dettagli della richiesta:
 - Tipo di messaggio: Query.
 - Tipo di record richiesto: A (per IPv4).
 - Flag di ricorsione: *Recursion Desired* impostato su 1 (richiesta ricorsiva).

Answer analysis:

- Nella risposta, i ruoli di sorgente e destinazione si invertono. Il server DNS (1.1) risponde al client (1.5) fornendo gli indirizzi IP associati al dominio richiesto. La porta sorgente diventa 53, mentre la destinazione utilizza la porta 51985.
- Il flag *Recursion Available* nella risposta indica che il server DNS ha completato la risoluzione ricorsiva, interrogando altri server DNS e restituendo una risposta completa.

Il server DNS del gateway supporta richieste ricorsive, completando la risoluzione dei nomi di dominio (es. discord.com → 162.x.x.232, 162.x.x.233). Se la ricorsione non fosse supportata, il server avrebbe restituito una risposta iterativa con l'indirizzo del server successivo da interrogare. Nlookup per la corretta associazione di nomi di dominio agli indirizzi IP.