

udp.port == 53						
No.	Time	Source	Destination	Protocol	Length	Info
3	46.423582	10.0.2.15	192.168.20.1	DNS	85	Standard query 0x0001 PTR 1.20.168.192.in-addr.arpa
4	46.424810	192.168.20.1	10.0.2.15	DNS	85	Standard query response 0x0001 No such name PTR 1.20.168.192.in-addr...
7	55.543698	10.0.2.15	192.168.20.1	DNS	91	Standard query 0x0002 A www.tuttomercatoweb.com.station
8	55.545154	192.168.20.1	10.0.2.15	DNS	91	Standard query response 0x0002 No such name A www.tuttomercatoweb.co...
9	55.545513	10.0.2.15	192.168.20.1	DNS	91	Standard query 0x0003 AAAA www.tuttomercatoweb.com.station
10	55.546943	192.168.20.1	10.0.2.15	DNS	91	Standard query response 0x0003 No such name AAAA www.tuttomercatoweb...
11	55.547431	10.0.2.15	192.168.20.1	DNS	83	Standard query 0x0004 A www.tuttomercatoweb.com
12	55.555478	192.168.20.1	10.0.2.15	DNS	113	Standard query response 0x0004 A www.tuttomercatoweb.com CNAME tutto...
13	55.561752	10.0.2.15	192.168.20.1	DNS	83	Standard query 0x0005 AAAA www.tuttomercatoweb.com
14	55.571201	192.168.20.1	10.0.2.15	DNS	157	Standard query response 0x0005 AAAA www.tuttomercatoweb.com CNAME tu...

> Frame 7: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{87EA3378-285... > Ethernet II, Src: PCSSystemtec_96:c2:10 (08:00:27:96:c2:10), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02) > Destination: 52:55:0a:00:02:02 (52:55:0a:00:02:02) > Source: PCSSystemtec_96:c2:10 (08:00:27:96:c2:10) Type: IPv4 (0x0800) [Stream index: 0] > Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.20.1 > User Datagram Protocol, Src Port: 51835, Dst Port: 53 > Domain Name System (query)		0000 52 55 0a 00 02 02 08 00 27 96 c2 0010 00 4d 9c e9 00 00 80 11 00 00 0a 0020 14 01 ca 7b 00 35 00 39 e1 02 06 0030 00 00 00 00 00 00 03 77 77 77 0f 0040 6d 65 72 63 61 74 6f 77 65 62 03 0050 74 61 74 69 6f 6e 00 00 01 00 01
---	--	--

wireshark_EthernetHVZL72.pcapng Pacchetti: 14- visualizzati: 10 (71.4%) - scartati: 0 (0.0%) Profilo: Default

- Quali sono gli indirizzi MAC di origine e destinazione?

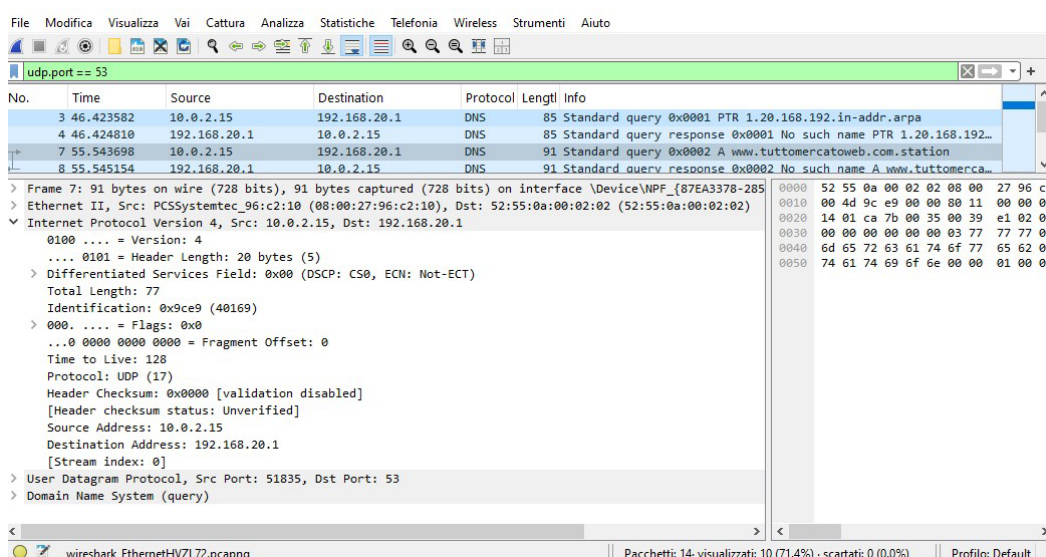
MAC di origine: 08:00:27:96:c2:10

MAC di destinazione: 52:55:00:0a:02:02

- A quali interfacce di rete sono associati questi indirizzi MAC?

08:00:27:96:c2:10 è associato all'interfaccia di rete della macchina virtuale

52:55:00:0a:02:02 è l'interfaccia del gateway virtuale o della rete NAT



- **Quali sono gli indirizzi IP di origine e destinazione?**

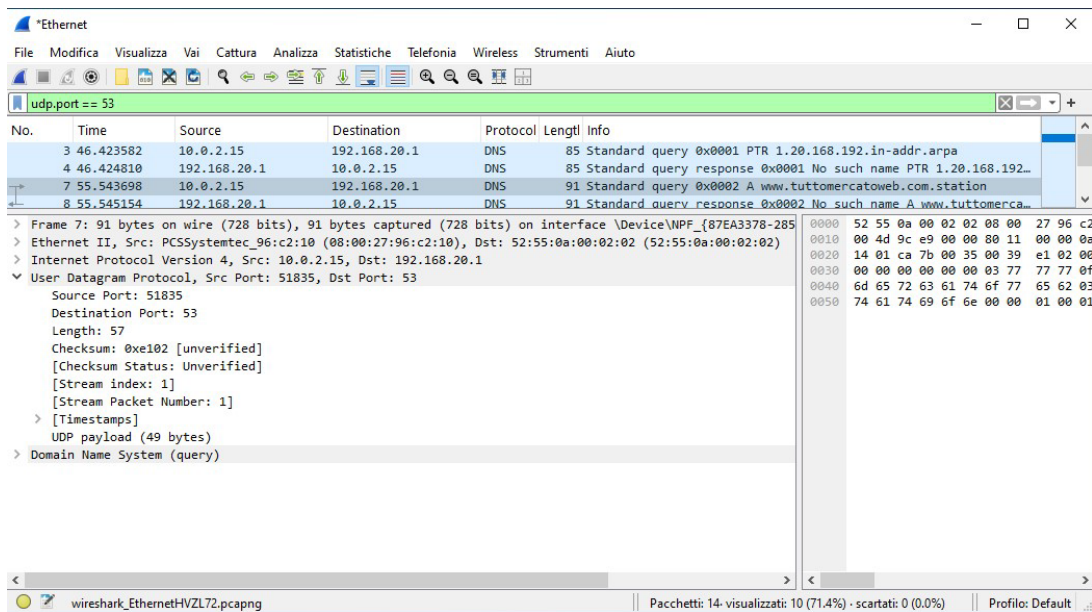
Indirizzo IP di origine: 10.0.2.15

Indirizzo IP di destinazione: 192.168.20.1

- **A quali interfacce di rete sono associati questi indirizzi IP?**

10.0.2.15 è associato all'interfaccia di rete della macchina virtuale

192.168.20.1 è associato al DNS server nella rete NAT



- **Quali sono le porte di origine e destinazione?**

Porta di origine: 51835 → Porta effimera usata dalla tua macchina per la richiesta

Porta di destinazione: 53 → Porta standard del servizio DNS

- **Qual è il numero di porta DNS predefinito?**

Porta 53 → Porta standard usata dai server DNS per ricevere le richieste.

- **Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC. Qual è la tua osservazione?**

Tutti gli indirizzi IP e MAC visualizzati in Wireshark sono coerenti con quelli configurati

La cattura dei pacchetti funziona correttamente

Il traffico DNS analizzato proviene dall' interfaccia di rete attiva

```
C:\Users\User>arp -a

Interfaccia: 10.0.2.15 --- 0x8
Indirizzo Internet    Indirizzo fisico      Tipo
10.0.2.2              52-55-0a-00-02-02   dinamico
10.0.2.3              52-55-0a-00-02-03   dinamico
10.0.2.255            ff-ff-ff-ff-ff-ff   statico
224.0.0.22            01-00-5e-00-00-16   statico
224.0.0.251           01-00-5e-00-00-fb   statico
224.0.0.252           01-00-5e-00-00-fc   statico
239.255.255.250       01-00-5e-7f-ff-fa   statico
255.255.255.255       ff-ff-ff-ff-ff-ff   statico
```

```
C:\Users\User>ipconfig /all

Configurazione IP di Windows

Nome host . . . . . : DESKTOP-8CAJRTO
Suffisso DNS primario . . . . . :
Tipo nodo . . . . . : Ibrido
Routing IP abilitato. . . . . : No
Proxy WINS abilitato . . . . . : No
Elenco di ricerca suffissi DNS. . . . : station

Scheda Ethernet Ethernet:

Suffisso DNS specifico per connessione: station
Descrizione . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Indirizzo fisico. . . . . : 08-00-27-96-C2-10
DHCP abilitato. . . . . : Si
Configurazione automatica abilitata : Si
Indirizzo IPv6 . . . . . : fd00::f1b3:4604:1737:425e(Preferenziale)
Indirizzo IPv6 temporaneo. . . . . : fd00::810f:8bef:c176:f54f(Preferenziale)
Indirizzo IPv6 locale rispetto al collegamento : fe80::7de5:ce64:b266:fed3%8(Preferenziale)
Indirizzo IPv4. . . . . : 10.0.2.15(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Lease ottenuto. . . . . : mercoledì 11 giugno 2025 14:19:19
Scadenza lease . . . . . : giovedì 12 giugno 2025 14:19:19
Gateway predefinito . . . . . : fe80::2%8
                               10.0.2.2
Server DHCP . . . . . : 10.0.2.2
IAID DHCPv6 . . . . . : 101187623
DUID Client DHCPv6. . . . . : 00-01-00-01-2E-6F-C9-F0-08-00-27-96-C2-10
Server DNS . . . . . : 192.168.20.1
NetBIOS su TCP/IP . . . . . : Attivato
```

Wireshark NetworkMiner - Ethernet

File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto

udp.port == 53

No.	Time	Source	Destination	Protocol	Length	Info
3	46.423582	10.0.2.15	192.168.20.1	DNS	85	Standard query 0x0001 PTR 1.20.168.192.in-addr.arpa
4	46.424810	192.168.20.1	10.0.2.15	DNS	85	Standard query response 0x0001 No such name PTR 1.20.168.192.in-addr.arpa
7	55.543698	10.0.2.15	192.168.20.1	DNS	91	Standard query 0x0002 A www.tuttomercatoweb.com.station
8	55.545154	192.168.20.1	10.0.2.15	DNS	91	Standard query response 0x0002 No such name A www.tuttomercatoweb.com.station

> Frame 8: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{87EA3378-285C-48E1-8967-A...} (08:00:27:96:C2:10)
 > Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_96:c2:10 (08:00:27:96:c2:10)
 > Internet Protocol Version 4, Src: 192.168.20.1, Dst: 10.0.2.15
 > User Datagram Protocol, Src Port: 53, Dst Port: 51835
 > Domain Name System (response)

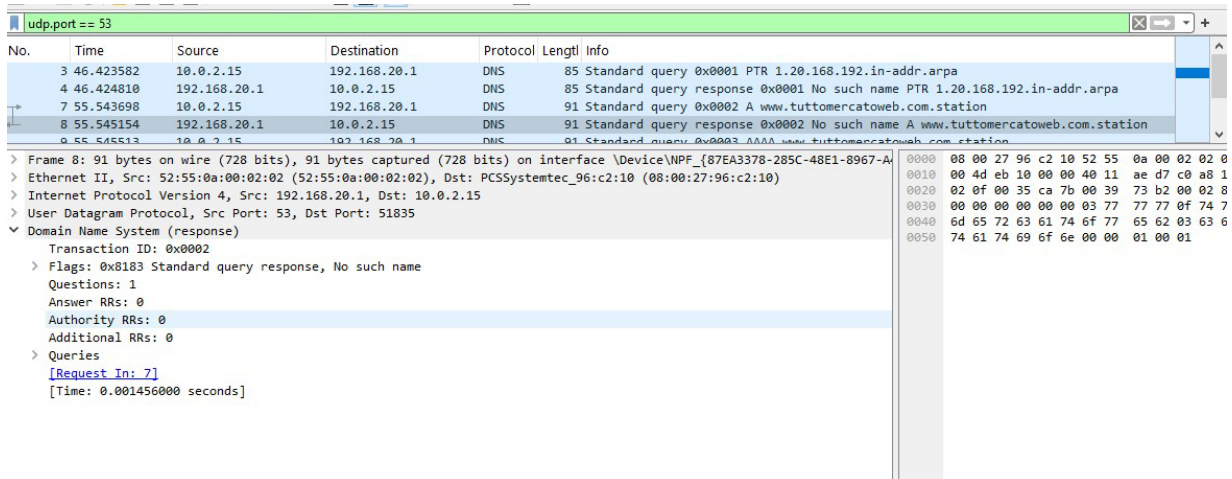
0000 08 00 27 96 c2 10 52 55 0a 00 02
 0010 00 4d eb 10 00 00 40 11 ae d7 c0
 0020 02 0f 00 35 ca 7b 00 39 73 b2 00
 0030 00 00 00 00 00 03 77 77 7f 0f
 0040 6d 65 72 63 61 74 6f 77 65 62 03
 0050 74 61 74 69 6f 6e 00 00 01 00 01

- Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione?

	Origine	Destinazione
Indirizzo MAC	52:55:00:00:02:02	08:00:27:96:c2:10
Indirizzo IP	192.168.20.1	10.0.2.15
Porta UDP	53	51835

- Come si confrontano con gli indirizzi nei pacchetti di query DNS

Analizzando il pacchetto di risposta DNS, si osserva che gli indirizzi MAC, IP e le porte sono l'esatto inverso rispetto a quelli utilizzati nella query DNS corrispondente.



No.	Time	Source	Destination	Protocol	Length	Info
3	46.423582	10.0.2.15	192.168.20.1	DNS	85	Standard query 0x0001 PTR 1.20.168.192.in-addr.arpa
4	46.424810	192.168.20.1	10.0.2.15	DNS	85	Standard query response 0x0001 No such name PTR 1.20.168.192.in-addr.arpa
7	55.543698	10.0.2.15	192.168.20.1	DNS	91	Standard query 0x0002 A www.tuttomercatoweb.com.station
8	55.545154	192.168.20.1	10.0.2.15	DNS	91	Standard query response 0x0002 No such name A www.tuttomercatoweb.com.station
9	55.545512	10.0.2.15	192.168.20.1	DNS	91	Standard query 0x0003 AAAA www.tuttomercatoweb.com.station

Frame 8: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{87EA3378-285C-48E1-8967-A...}

Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_96:c2:10 (08:00:27:96:c2:10)

Internet Protocol Version 4, Src: 192.168.20.1, Dst: 10.0.2.15

User Datagram Protocol, Src Port: 53, Dst Port: 51835

Domain Name System (response)

Transaction ID: 0x0002

Flags: 0x8183 Standard query response, No such name

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

[Request In: 7]

[Time: 0.001456000 seconds]

- Il server DNS può fare query ricorsive?

Sì, il server DNS può effettuare query ricorsive.

Analizzando il pacchetto di **risposta DNS**, dove nei **Flags** è impostato il bit **RA (Recursion Available)** a **1**. Questo significa che il server è in grado di ricevere richieste ricorsive da parte dei client e, se necessario, inoltrarle ad altri server DNS per ottenere la risposta finale.

- Come si confrontano i risultati con quelli di nslookup

I risultati mostrati in Wireshark coincidono con quelli che si ottengono tramite il comando nslookup, ma forniscono molte più informazioni, come il numero esatto di risposte ricevute, il tempo di risposta, la struttura del pacchetto dns, I dettagli di TTL, autorità, query inviate e porte utilizzate.

RIFLESSIONE

- Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?

Rimuovendo il filtro impostato possiamo osservare tutto il traffico della rete, non solo DNS. Possiamo vedere quali protocolli sono utilizzati, porte utilizzate, individuare eventuali tentativi di connessione sospetti o capire quali dispositivi stanno comunicando tra loro.

- **Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?**

Un attaccante può utilizzare Wireshark per intercettare credenziali se trasmesse in chiaro, mappare la rete identificando host attivi, DNS, gateway, e servizi in uso oppure lanciare attacchi più mirati come ARP spoofing o DNS spoofing per reindirizzare gli utenti verso siti malevoli