

Analisi del protocollo TCP/IP

Nicolò Penserini 0001080348

Dicembre 2024

Indice

1	Introduzione e richieste DNS	2
1.1	Introduzione	2
1.2	Richieste DNS	2
2	Handshake TCP e frammentazione dei pacchetti	3
2.1	Handshake TCP	3
2.2	Frammentazione dei pacchetti	3
3	Ritrasmissioni	5
4	Statistiche	6
4.1	Pacchetti	6
4.2	Tempi di latenza	7

Capitolo 1

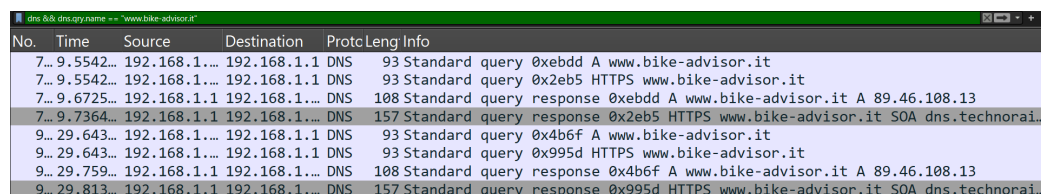
Introduzione e richieste DNS

1.1 Introduzione

Per l'analisi del traffico di rete durante una sessione di trasferimento file ho deciso di avviare una cattura Wireshark e di iniziare la navigazione su un sito web. Dato che il sito utilizza una connessione sicura, il protocollo utilizzato è il protocollo https.

1.2 Richieste DNS

Per poter trovare l'indirizzo da cui provengono i pacchetti e poterli successivamente filtrare, ho deciso di applicare un filtro sulla cattura che ritornasse solo i pacchetti dns corrispondenti al sito selezionato in modo da poter visualizzare la risposta DNS alla query di tipo A.



The image shows a Wireshark packet capture window with a filter set to 'dns && dns.qry.name == "www.bike-advisor.it"'. The packet list shows several DNS queries and responses. The packet details pane shows the structure of a DNS Standard query response, including the question section with the query name and type.

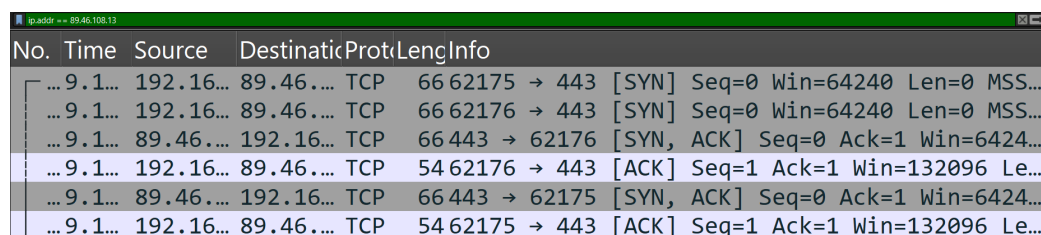
No.	Time	Source	Destination	Proto	Leng	Info
7...	9.5542...	192.168.1.1...	192.168.1.1	DNS	93	Standard query 0xebdd A www.bike-advisor.it
7...	9.5542...	192.168.1.1...	192.168.1.1	DNS	93	Standard query 0x2eb5 HTTPS www.bike-advisor.it
7...	9.6725...	192.168.1.1	192.168.1.1...	DNS	108	Standard query response 0xebdd A www.bike-advisor.it A 89.46.108.13
7...	9.7364...	192.168.1.1	192.168.1.1...	DNS	157	Standard query response 0x2eb5 HTTPS www.bike-advisor.it SOA dns.technorai...
9...	29.643...	192.168.1.1...	192.168.1.1	DNS	93	Standard query 0x4b6f A www.bike-advisor.it
9...	29.643...	192.168.1.1...	192.168.1.1	DNS	93	Standard query 0x995d HTTPS www.bike-advisor.it
9...	29.759...	192.168.1.1	192.168.1.1...	DNS	108	Standard query response 0x4b6f A www.bike-advisor.it A 89.46.108.13
9...	29.813...	192.168.1.1	192.168.1.1...	DNS	157	Standard query response 0x995d HTTPS www.bike-advisor.it SOA dns.technorai...

Capitolo 2

Handshake TCP e frammentazione dei pacchetti

2.1 Handshake TCP

Una volta scoperto l'indirizzo di cui ci vogliamo interessare, possiamo applicare un filtro sull'indirizzo IP in modo da vedere solo i pacchetti che riguardano l'indirizzo specificato. Si può notare che i primi pacchetti che si vedono sono quelli che riguardano l'Handshake TCP. Il primo pacchetto è un pacchetto con flag SYN dal client verso il server, a cui il server risponde con un pacchetto con i flag SYN e ACK. La fase di Handshake TCP si conclude con un pacchetto con il flag ACK dal server verso il client.



No.	Time	Source	Destination	Protocol	Length	Info
...	9.1...	192.16...	89.46...	TCP	66	62175 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS...
...	9.1...	192.16...	89.46...	TCP	66	62176 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS...
...	9.1...	89.46...	192.16...	TCP	66	443 → 62176 [SYN, ACK] Seq=0 Ack=1 Win=6424...
...	9.1...	192.16...	89.46...	TCP	54	62176 → 443 [ACK] Seq=1 Ack=1 Win=132096 Le...
...	9.1...	89.46...	192.16...	TCP	66	443 → 62175 [SYN, ACK] Seq=0 Ack=1 Win=6424...
...	9.1...	192.16...	89.46...	TCP	54	62175 → 443 [ACK] Seq=1 Ack=1 Win=132096 Le...

2.2 Frammentazione dei pacchetti

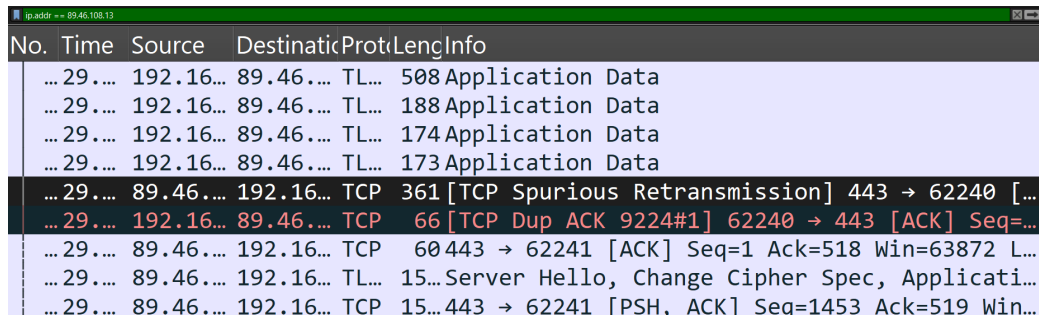
Applicando un ulteriore filtro (`ip.flags.mf == 1`) possiamo controllare il flag MF, More Fragment, dei pacchetti e visualizzare quindi i pacchetti che sono frammenti intermedi di un pacchetto frammentato. Poichè non ci sono frammenti intermedi, possiamo dedurre che nessuno dei pacchetti è stato frammentato, e questo ci può dare alcune informazioni sull'MTU, Maximum

Transmission Unit, che sarà sicuramente maggiore della dimensione di tutti i pacchetti analizzati in questa cattura.

Capitolo 3

Ritrasmissioni

Applicando il filtro "tcp.analysis.retransmission" possiamo vedere i pacchetti che sono una ritrasmissione di un pacchetto già inviato, infatti Wireshark marca i pacchetti ritrasmessi. Possiamo notare che c'è stata una ritrasmissione di un pacchetto e, analizzandola, possiamo vedere che si tratta di una ritrasmissione spuria, cioè inviata senza che ce ne fosse una reale necessità e quindi senza che il pacchetto originario fosse stato perso o danneggiato; questo si verifica solitamente a causa di ACK ritardati o perdita di pacchetti nell'ACK. Il fatto che questa ritrasmissione sia spuria ci viene confermato dal pacchetto immediatamente successivo, che è infatti un ACK duplicato.



The image shows a Wireshark packet capture window with the filter "ip.addr == 89.46.108.13". The packet list shows several application data packets followed by a spurious retransmission and a duplicate ACK.

No.	Time	Source	Destination	Protocol	Length	Info
...	29....	192.16...	89.46....	TLS	508	Application Data
...	29....	192.16...	89.46....	TLS	188	Application Data
...	29....	192.16...	89.46....	TLS	174	Application Data
...	29....	192.16...	89.46....	TLS	173	Application Data
...	29....	89.46....	192.16...	TCP	361	[TCP Spurious Retransmission] 443 → 62240 [...
...	29....	192.16...	89.46....	TCP	66	[TCP Dup ACK 9224#1] 62240 → 443 [ACK] Seq=...
...	29....	89.46....	192.16...	TCP	60	443 → 62241 [ACK] Seq=1 Ack=518 Win=63872 L...
...	29....	89.46....	192.16...	TLS	15	Server Hello, Change Cipher Spec, Applicati...
...	29....	89.46....	192.16...	TCP	15	443 → 62241 [PSH, ACK] Seq=1453 Ack=519 Win...

Capitolo 4

Statistiche

4.1 Pacchetti

Si riporta di seguito un'immagine con le caratteristiche dei pacchetti catturati, quelli visualizzati riguardano solo i pacchetti che coinvolgono l'indirizzo IP individuato dalle catture DNS.

Statistiche			
<u>Misure</u>	<u>Catturati</u>	<u>Visualizzati</u>	<u>Marcati</u>
Pacchetti	12010	5513 (45.9%)	—
Tempo, s	56.385	45.180	—
PPS medi	213.0	122.0	—
Dimensione media dei pacchetti, B	861	1016	—
Byte	10339163	5598470 (54.1%)	0
Byte/s medi	183 k	123 k	—
Bit/s medi	1466 k	991 k	—

4.2 Tempi di latenza

SI riporta in seguito un'immagine che riporta l'RTT, Round Trip Time, in funzione del tempo per un flusso che va dal server al client.

