14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A? yummyrecipesforme.com. (24)

14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A 203.0.113.22 (40)

14:18:32.192571  
The timestamp indicates precisely 2:18 PM and 32 seconds, with an added precision of one-twentieth of a millisecond, offering meticulous detail regarding the temporal aspect of the captured network activity.  
  
IP your.machine.52444  
The designation "IP your.machine.52444" delineates the origin of the packet, pinpointing the source as the machine identified as "your.machine" operating on port 52444, facilitating precise tracing of network traffic back to its originating endpoint.  
  
>  
The ">" symbol serves as an indicator of directionality, denoting that the packet is emanating from the specified IP address, "your.machine," and directed towards the destination entity in the communication exchange.  
  
dns.google.domain  
The notation "dns.google.domain" signifies the target destination of the packet, indicating that the communication is directed towards the DNS server operated by Google, illustrating the intricate interplay between network entities in the quest for information retrieval.  
  
35084  
The numerical identifier "35084" corresponds to a unique transactional event generated within the networking context, enabling the systematic tracking and analysis of individual interactions within the network communication framework.  
  
+  
The presence of the symbol "+" within the context of the DNS query signifies a forward lookup operation, indicative of the system's quest for domain name resolution, seeking to translate human-readable domain names into their corresponding IP addresses to facilitate seamless connectivity and communication.  
  
A?  
The inclusion of an "A" record within the DNS query elucidates the nature of the request, delineating it as an inquiry pertaining specifically to Address records, instrumental in mapping domain names to   
yummyrecipesforme.com.  
The fully qualified domain name of the A record translated from IP into words humans can understand.   
  
(24)  
The number of packets sent  
  
  
  
14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859 ecr 0,nop,wscale 7], length 0

14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags [S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS val 3302576859 ecr 3302576859,nop,wscale 7], length 0

14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [.], ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0

14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1

14:18:36.786595 IP yummyrecipesforme.com.http > your.machine.36086: Flags [.], ack 74, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0

…<a lot of traffic on the port 80>...   
  
  
Flags [S]  
SYN stands for synchronize and it is used during the TCP three-way handshake process to establish a connection between two devices (e.g a client and a server)   
  
  
seq 2873951608   
seq 2873951608" indicates the sequence number assigned to the first byte of data in the TCP segment sent from "your.machine" to "yummyrecipesforme.com" on port 80 (HTTP).  
  
ack 2873951609   
In a TCP/IP network communication, "ack 2873951609" indicates that the acknowledgment number (ack) in the TCP segment is set to 2873951609.  
  
  
win 65483  
The window is a buffer space maintained by the receiving party e.g., client or server to indicate the amount of data it can receive and process without overflowing its buffers or overwhelming its processing capabilities. So 65483 is the max packet size that is can accept and process.  
  
mss 65495  
Mss stands for the ma segment size, indicating the max amount of data in bytes that can be sent in a sigle TCP segment without fragmentation.   
  
sackOK,TS  
Selective Achknowledgment, enables the receiver to acknowledge individual segments of data. This allows for increased performance and reliability in cases where packets are lost or reordered.   
  
val 3302576859  
This stands for timestamp and is used for calculating round trip time (RTT) between the sender and receiver.   
  
ecr 0  
This value is apart of the timestamp feature that helps measure the network latency and congestion. Sometimes this feature is not enabled or supported so this value is set to zero.   
  
.  
ACK flag. ACK stands for "acknowledgment." The ACK flag is used to acknowledge the receipt of data from the sender. In the context of the TCP three-way handshake, the ACK flag acknowledges the receipt of the SYN segment from the sender and indicates the readiness of the receiving device to establish the connection.  
  
"[P.]"   
indicates that the TCP segment contains data from the sender (Push flag), and it also acknowledges the receipt of data from the recipient (ACK flag). This combination is commonly used in TCP communication to transmit data and acknowledge its receipt simultaneously, without waiting for additional data to be sent or received.  
  
HTTP: GET / HTTP/1.1  
HTTP: GET / HTTP/1.1" is a standard HTTP GET request asking the server to retrieve the main page (or root directory) of the website using the HTTP/1.1 protocol. It's the most common type of request made by web browsers when a user enters a URL into the address bar or clicks on a link.  
  
If the server has malicious code this is a potential site of infection.