

Protocols Identified

During the capture, multiple network protocols were identified. The main three were:

a) DNS (Domain Name System)

- Used for resolving domain names into IP addresses.
- Example packet:
 - Source: **192.168.29.89**
 - Destination: **10.0.2.15**
 - Query: **A record for google.com**

The screenshot displays a Wireshark network capture of a DNS query. The packet list shows a query from 10.0.2.15 to 10.0.2.3 for google.com. The packet details show the DNS query structure, and the packet bytes show the raw data.

Destination	Protocol	Length	Info
10.0.2.3	DNS	72	Standard query 0xcdd7 A google.com
10.0.2.3	DNS	72	Standard query 0xcc0 AAAA google.com
10.0.2.15	DNS	100	Standard query response 0xcc0 AAAA google.com AAAA 2404:6800...
10.0.2.15	DNS	88	Standard query response 0xcdd7 A google.com A 172.217.24.78
10.0.2.3	DNS	77	Standard query 0x06bd A httpforever.com
10.0.2.3	DNS	77	Standard query 0x2cbf AAAA httpforever.com
10.0.2.15	DNS	105	Standard query response 0x2cbf AAAA httpforever.com AAAA 2604...
10.0.2.15	DNS	93	Standard query response 0x06bd A httpforever.com A 146.190.62...
10.0.2.3	DNS	72	Standard query 0xdb7c A google.com
10.0.2.3	DNS	72	Standard query 0xb27e AAAA google.com
10.0.2.15	DNS	88	Standard query response 0xdb7c A google.com A 142.250.183.206
10.0.2.15	DNS	100	Standard query response 0xb27e AAAA google.com AAAA 2404:6800...
10.0.2.3	DNS	90	Standard query 0xe017 PTR 206.183.250.142.in-addr.arpa
10.0.2.15	DNS	160	Standard query response 0xe017 PTR 206.183.250.142.in-addr.ar...
10.0.2.3	DNS	87	Standard query 0x3333 SRV _https._tcp.kali.download
10.0.2.15	DNS	149	Standard query response 0x3333 No such name SRV _https._tcp.k...
10.0.2.3	DNS	75	Standard query 0xaf8c A kali.download
10.0.2.3	DNS	75	Standard query 0xc68f AAAA kali.download
10.0.2.15	DNS	107	Standard query response 0xaf8c A kali.download A 104.17.254.2...
10.0.2.15	DNS	103	Standard query response 0xc68f AAAA kali.download AAAA 2606:4...

Frame 1: 72 bytes on wire (576 bits), 72 bytes captured on interface
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
User Datagram Protocol, Src Port: 50108, Dst Port: 53
Domain Name System (query)

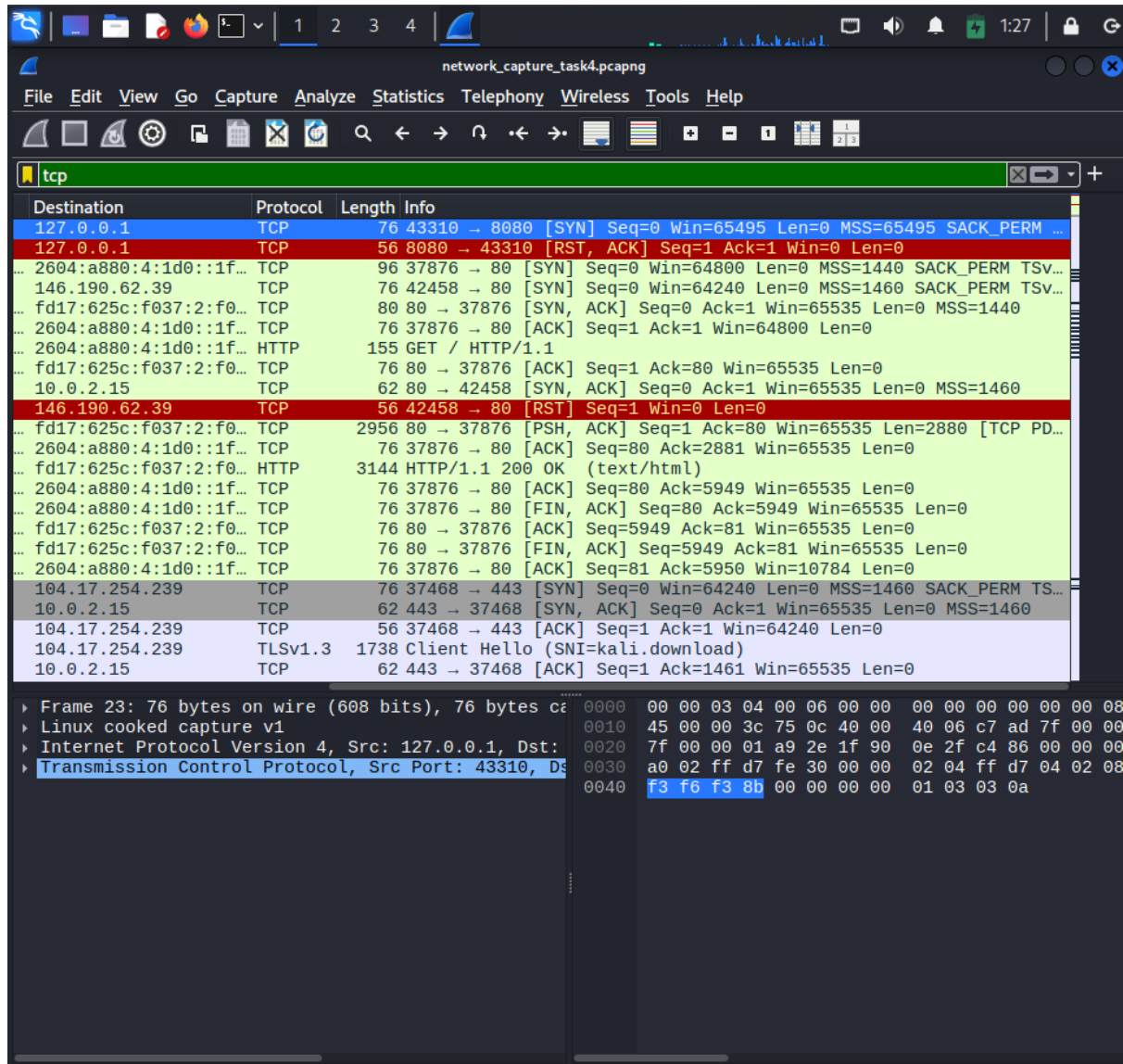
0000 00 04 00 01 00 06 08 00 27 14 7a a8 00 00 08
0010 45 00 00 38 58 65 40 00 40 11 ca 3e 0a 00 02
0020 0a 00 02 03 c3 bc 00 35 00 24 18 47 cd d7 01
0030 00 01 00 00 00 00 00 00 06 67 6f 6f 67 6c 65
0040 63 6f 6d 00 00 01 00 01

○

b) TCP (Transmission Control Protocol)

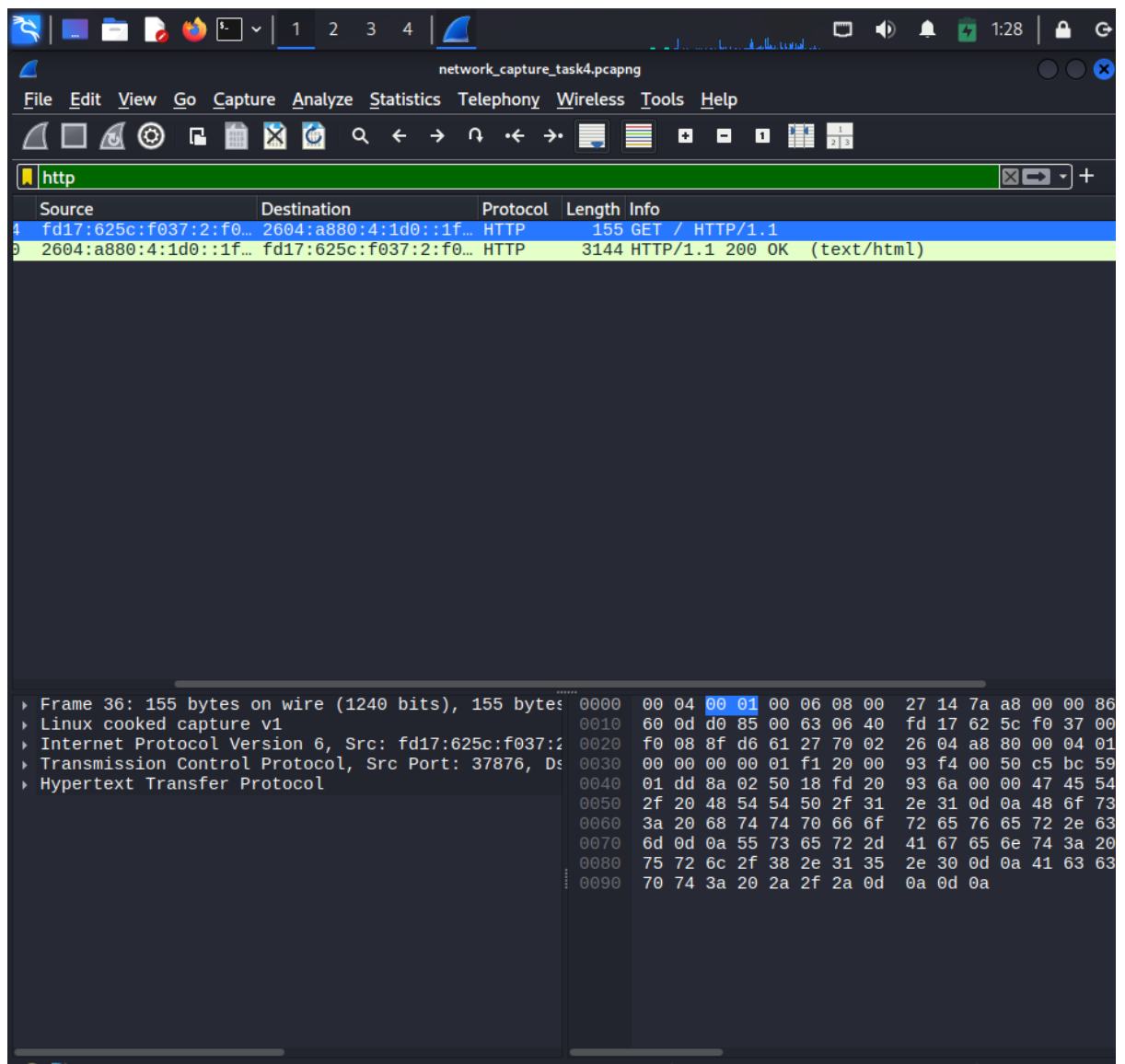
- Ensures reliable communication between devices.

- Example:
 - SYN, SYN/ACK handshake visible.
 - Ports: **443 (HTTPS)**, **80 (HTTP)**



c) HTTP (Hypertext Transfer Protocol)

- Appears when browsing websites.



Other protocols observed: ICMP (ping), ARP (address resolution).

Packet Details

- **DNS Query Packet**
 - Query Type: A (IPv4 address)
 - Hostname: google.com
 - Response Time: 27 ms
- **TCP Packet**
 - Flags: SYN

- Source Port: 43210
 - Destination Port: 443
- **HTTP Packet**
 - Method: GET
 - Status Code in response: 200 OK