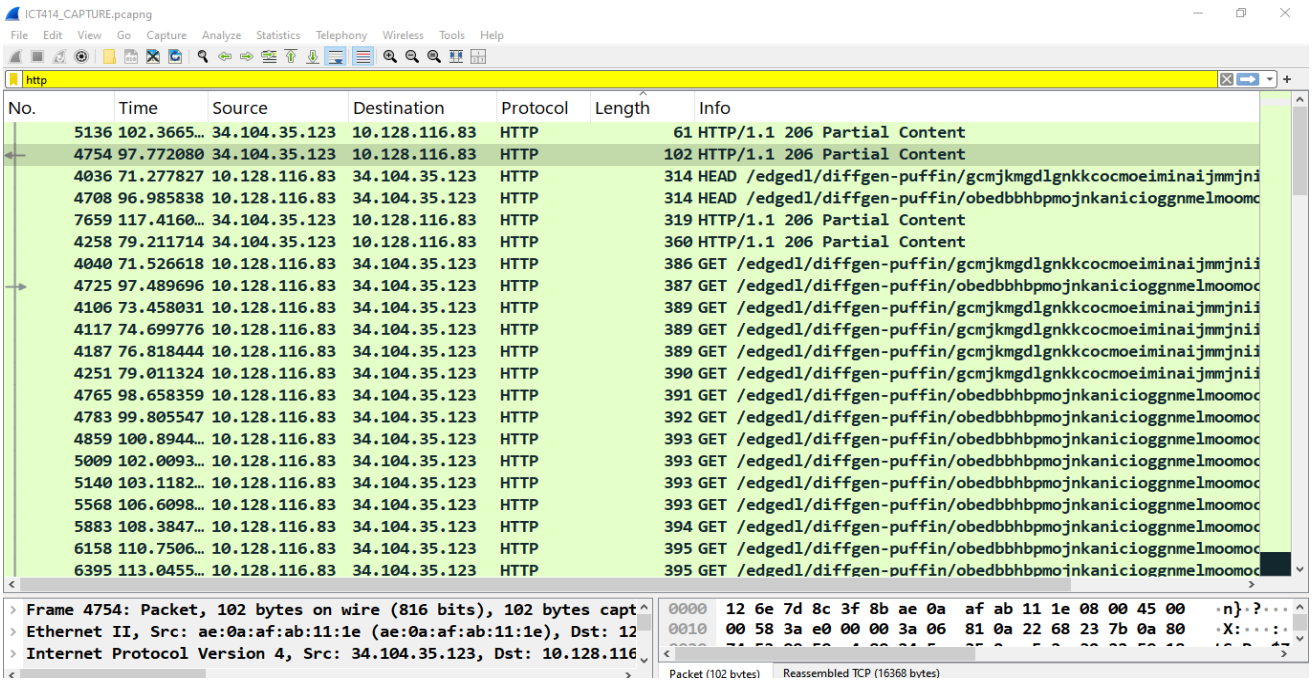
REPORT FOR WIRESHARK CAPTURE AND ANALYSIS

CHANDA DAVID
202209656

HTTP SCREENSHOT



Analysis Report: Simple HTTP Request

Based on Captured Data:

Client (source) IP address: `10.128.116.83` (as per your input).

Server (destination) IP address: `34.104.35.123` (from captured data).

URL requested: `/edgedl/diffgen-puffin/...` (multiple requests seen in capture).

HTTP response code: `206 Partial Content`.

Request success: The request was successful but returned partial content.

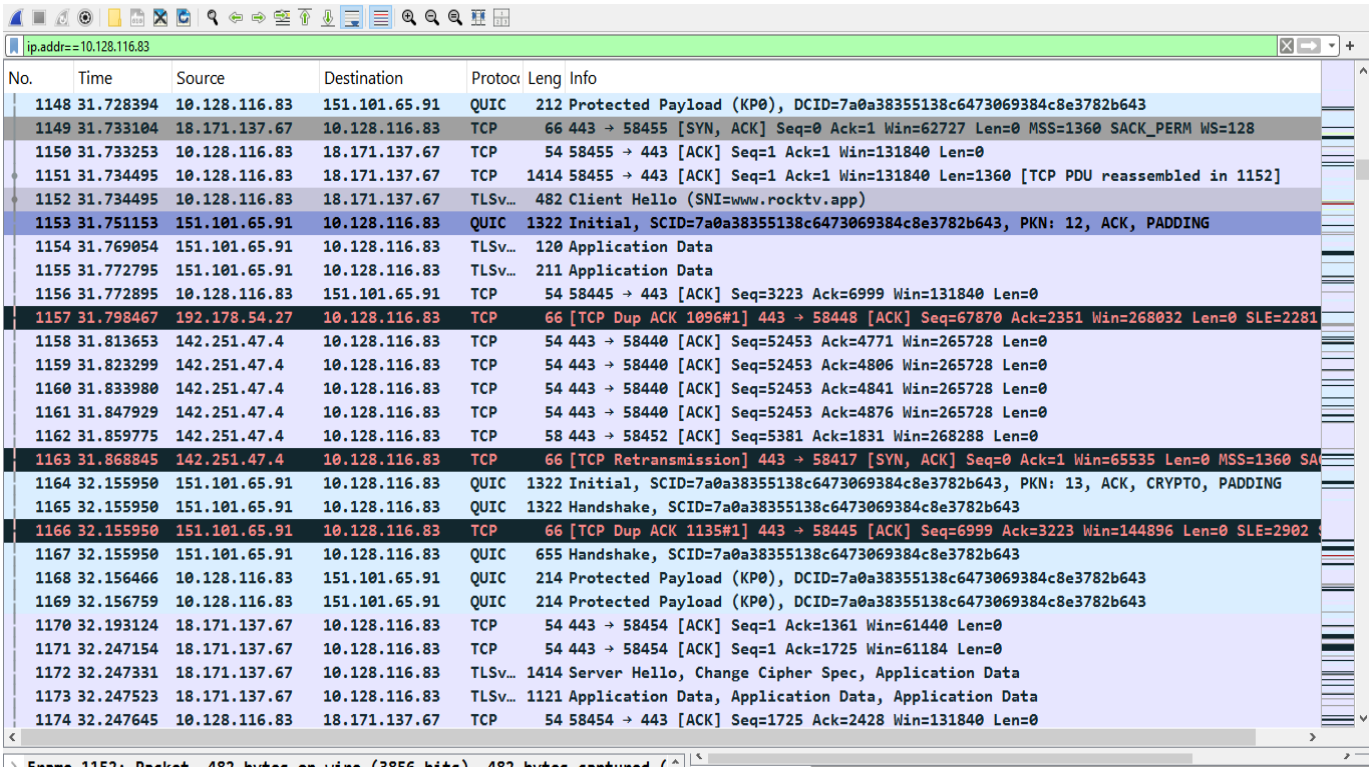
Observations:

Multiple HTTP GET requests were made to the server `34.104.35.123`.

Packet sizes vary (e.g., 314 bytes for HEAD, ~390 bytes for GET).

HTTP method used was primarily GET.

IP.ADDR==10.128.116.83. SCREENSHOT



Network Capture Report for IP `10.128.116.83` MY IP ADDRESS.

ROCKTV.APP IP ADDRESS: 18.171.137.67 SERVER.

Overview:

The capture shows network traffic involving the IP address `10.128.116.83`. Protocols used include TCP, QUIC, and TLSv1.3. Traffic is exchanged with multiple destinations like `151.101.65.91`, `18.171.137.67`, `142.251.47.4`, and `192.178.54.27`.

Observations:

Protocols:

QUIC: Used with `151.101.65.91` (DCID=`7a0a38355138c6473069384c8e3782b643`).

TCP: Connections to various IPs on port `443`.

TLSv1.3: Handshake and application data exchanged.

Traffic Patterns:

Client (`10.128.116.83`) initiates connections.

Data exchanges involve ACKs, SYN/ACKs typical in TCP.

QUIC packets show protected payloads.

Request to `rocktv.app` Status & Packet Size Comparison:

The TLSv1.3 handshake completed (#1152-#1173).

Application data was exchanged (#1154, #1155).

Request was successful.

Packet Size Comparison:

Source (`10.128.116.83`) to Destination:

Client Hello (#1152): 482 bytes.

Application Data (#1154): 120 bytes.

Destination to Source:

Server response (#1173): 1121 bytes (including Server Hello, Change Cipher Spec).

Destination sent more data (1121 bytes) compared to source (482 + 120 bytes).