

# REPORT FOR WIRESHARK CAPTURE AND ANALYSIS

CHANDA DAVID

202209656

## HTTP SCREENSHOT

No.	Time	Source	Destination	Protocol	Length	Info
5136	102.3665...	34.104.35.123	10.128.116.83	HTTP	61	HTTP/1.1 206 Partial Content
4754	97.772080	34.104.35.123	10.128.116.83	HTTP	102	HTTP/1.1 206 Partial Content
4036	71.277827	10.128.116.83	34.104.35.123	HTTP	314	HEAD /edgedl/diffgen-puffin/gcmjkmhdlgnkkcocoeimainajmmjni
4708	96.985838	10.128.116.83	34.104.35.123	HTTP	314	HEAD /edgedl/diffgen-puffin/obedbbhbpmojnkanicioggnmelmooc
7659	117.4160...	34.104.35.123	10.128.116.83	HTTP	319	HTTP/1.1 206 Partial Content
4258	79.211714	34.104.35.123	10.128.116.83	HTTP	360	HTTP/1.1 206 Partial Content
4040	71.526618	10.128.116.83	34.104.35.123	HTTP	386	GET /edgedl/diffgen-puffin/gcmjkmhdlgnkkcocoeimainajmmjni
4725	97.489696	10.128.116.83	34.104.35.123	HTTP	387	GET /edgedl/diffgen-puffin/obedbbhbpmojnkanicioggnmelmooc
4106	73.458031	10.128.116.83	34.104.35.123	HTTP	389	GET /edgedl/diffgen-puffin/gcmjkmhdlgnkkcocoeimainajmmjni
4117	74.699776	10.128.116.83	34.104.35.123	HTTP	389	GET /edgedl/diffgen-puffin/gcmjkmhdlgnkkcocoeimainajmmjni
4187	76.818444	10.128.116.83	34.104.35.123	HTTP	389	GET /edgedl/diffgen-puffin/gcmjkmhdlgnkkcocoeimainajmmjni
4251	79.011324	10.128.116.83	34.104.35.123	HTTP	390	GET /edgedl/diffgen-puffin/gcmjkmhdlgnkkcocoeimainajmmjni
4765	98.658359	10.128.116.83	34.104.35.123	HTTP	391	GET /edgedl/diffgen-puffin/obedbbhbpmojnkanicioggnmelmooc
4783	99.805547	10.128.116.83	34.104.35.123	HTTP	392	GET /edgedl/diffgen-puffin/obedbbhbpmojnkanicioggnmelmooc
4859	100.8944...	10.128.116.83	34.104.35.123	HTTP	393	GET /edgedl/diffgen-puffin/obedbbhbpmojnkanicioggnmelmooc
5009	102.0093...	10.128.116.83	34.104.35.123	HTTP	393	GET /edgedl/diffgen-puffin/obedbbhbpmojnkanicioggnmelmooc
5140	103.1182...	10.128.116.83	34.104.35.123	HTTP	393	GET /edgedl/diffgen-puffin/obedbbhbpmojnkanicioggnmelmooc
5568	106.6098...	10.128.116.83	34.104.35.123	HTTP	393	GET /edgedl/diffgen-puffin/obedbbhbpmojnkanicioggnmelmooc
5883	108.3847...	10.128.116.83	34.104.35.123	HTTP	394	GET /edgedl/diffgen-puffin/obedbbhbpmojnkanicioggnmelmooc
6158	110.7506...	10.128.116.83	34.104.35.123	HTTP	395	GET /edgedl/diffgen-puffin/obedbbhbpmojnkanicioggnmelmooc
6395	113.0455...	10.128.116.83	34.104.35.123	HTTP	395	GET /edgedl/diffgen-puffin/obedbbhbpmojnkanicioggnmelmooc

> Frame 4754: Packet, 102 bytes on wire (816 bits), 102 bytes captured on interface eth0  
> Ethernet II, Src: ae:0a:af:ab:11:1e (ae:0a:af:ab:11:1e), Dst: 10:00:00:00:00:00  
> Internet Protocol Version 4, Src: 34.104.35.123, Dst: 10.128.116.83  
> Hypertext Transfer Protocol, Method: GET, Path: /edgedl/diffgen-puffin/obedbbhbpmojnkanicioggnmelmooc, Status: 206 Partial Content

### 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

No.	Time	Source	Destination	Protocol	Length	Info
1148	31.728394	10.128.116.83	151.101.65.91	QUIC	212	Protected Payload (KP0), DCID=7a0a38355138c6473069384c8e3782b643
1149	31.733104	18.171.137.67	10.128.116.83	TCP	66	443 → 58455 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1360 SACK_PERM WS=128
1150	31.733253	10.128.116.83	18.171.137.67	TCP	54	58455 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
1151	31.734495	10.128.116.83	18.171.137.67	TCP	1414	58455 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=1360 [TCP PDU reassembled in 1152]
1152	31.734495	10.128.116.83	18.171.137.67	TLSv1.3	482	Client Hello (SNI=www.rocktv.app)
1153	31.751153	151.101.65.91	10.128.116.83	QUIC	1322	Initial, SCID=7a0a38355138c6473069384c8e3782b643, PKN: 12, ACK, PADDING
1154	31.769054	151.101.65.91	10.128.116.83	TLSv1.3	120	Application Data
1155	31.772795	151.101.65.91	10.128.116.83	TLSv1.3	211	Application Data
1156	31.772895	10.128.116.83	151.101.65.91	TCP	54	58445 → 443 [ACK] Seq=3223 Ack=6999 Win=131840 Len=0
1157	31.798467	192.178.54.27	10.128.116.83	TCP	66	[TCP Dup ACK 1096#1] 443 → 58448 [ACK] Seq=67870 Ack=2351 Win=268032 Len=0 SLE=2281
1158	31.813653	142.251.47.4	10.128.116.83	TCP	54	443 → 58440 [ACK] Seq=52453 Ack=4771 Win=265728 Len=0
1159	31.823299	142.251.47.4	10.128.116.83	TCP	54	443 → 58440 [ACK] Seq=52453 Ack=4806 Win=265728 Len=0
1160	31.833980	142.251.47.4	10.128.116.83	TCP	54	443 → 58440 [ACK] Seq=52453 Ack=4841 Win=265728 Len=0
1161	31.847929	142.251.47.4	10.128.116.83	TCP	54	443 → 58440 [ACK] Seq=52453 Ack=4876 Win=265728 Len=0
1162	31.859775	142.251.47.4	10.128.116.83	TCP	58	443 → 58452 [ACK] Seq=5381 Ack=1831 Win=268288 Len=0
1163	31.868845	142.251.47.4	10.128.116.83	TCP	66	[TCP Retransmission] 443 → 58417 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SA
1164	32.155950	151.101.65.91	10.128.116.83	QUIC	1322	Initial, SCID=7a0a38355138c6473069384c8e3782b643, PKN: 13, ACK, CRYPTO, PADDING
1165	32.155950	151.101.65.91	10.128.116.83	QUIC	1322	Handshake, SCID=7a0a38355138c6473069384c8e3782b643
1166	32.155950	151.101.65.91	10.128.116.83	TCP	66	[TCP Dup ACK 1135#1] 443 → 58445 [ACK] Seq=6999 Ack=3223 Win=144896 Len=0 SLE=2902
1167	32.155950	151.101.65.91	10.128.116.83	QUIC	655	Handshake, SCID=7a0a38355138c6473069384c8e3782b643
1168	32.156466	10.128.116.83	151.101.65.91	QUIC	214	Protected Payload (KP0), DCID=7a0a38355138c6473069384c8e3782b643
1169	32.156759	10.128.116.83	151.101.65.91	QUIC	214	Protected Payload (KP0), DCID=7a0a38355138c6473069384c8e3782b643
1170	32.193124	18.171.137.67	10.128.116.83	TCP	54	443 → 58454 [ACK] Seq=1 Ack=1361 Win=61440 Len=0
1171	32.247154	18.171.137.67	10.128.116.83	TCP	54	443 → 58454 [ACK] Seq=1 Ack=1725 Win=61184 Len=0
1172	32.247331	18.171.137.67	10.128.116.83	TLSv1.3	1414	Server Hello, Change Cipher Spec, Application Data
1173	32.247523	18.171.137.67	10.128.116.83	TLSv1.3	1121	Application Data, Application Data, Application Data
1174	32.247645	10.128.116.83	18.171.137.67	TCP	54	58454 → 443 [ACK] Seq=1725 Ack=2428 Win=131840 Len=0

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).