AF-IAST
Skilling Pakistan

PAK-AUSTRIA FACHHOCHSCHULE:
INSTITUTE OF APPLIED SCIENCES AND TECHNOLOGY

Assignment : 01

Submitted by: Fatima Wajid

Registration no:B23F0155AI093

Instructor : Sir Adnan

Department: BSAI BLUE

PART 01 AND 04:

Task 4:

For the HTTP based website access, answer the following after analysing collected traces of HTTP:

Question :01:

What is the name of website?

Answer:

The name of the website is

Host: edgedl.me.gvt1.com

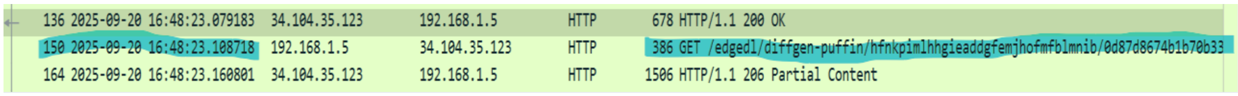
Question :02:

Find the packet that contains the first GET request for the website you have accessed.

Answer:

The packet that contains the first GET request for the website I have accessed is **packet 150**.

```
GET /edged1/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfb1lmnib/@d87d8674b1b70b3339
```



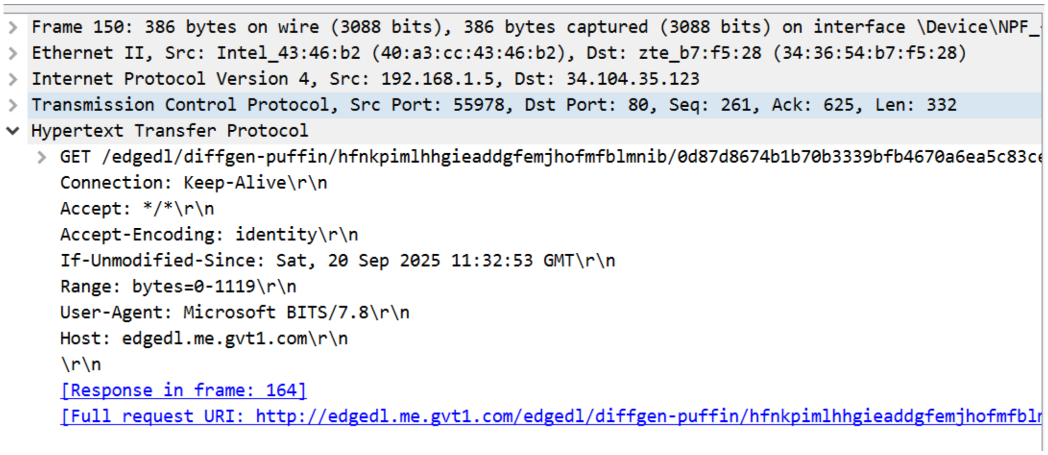
```
136 2025-09-20 16:48:23.079183  34.104.35.123   192.168.1.5     HTTP    678 HTTP/1.1 200 OK
150 2025-09-20 16:48:23.108718  192.168.1.5     34.104.35.123   HTTP    386 GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/0d87d8674b1b70b33
164 2025-09-20 16:48:23.160801  34.104.35.123   192.168.1.5     HTTP   1506 HTTP/1.1 206 Partial Content
```

Question :03:

Describe all headers and their values in this GET request message.

Answer:

- **Host:** edged1.me.gvt1.com
- **Connection:** keep-alive
- **Upgrade-Insecure-Requests:** 1
- **User-Agent:** Microsoft BITS/7.8\r\n
- **Accept:** */*
- **Accept-Encoding:** identity
- **If-Unmodified-Since:** Sat, 20 Sep 2025 11:32:53 GMT
- **Range:** bytes=0-1119



```
> Frame 150: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface \Device\NPF_
> Ethernet II, Src: Intel_43:46:b2 (40:a3:cc:43:46:b2), Dst: zte_b7:f5:28 (34:36:54:b7:f5:28)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 34.104.35.123
> Transmission Control Protocol, Src Port: 55978, Dst Port: 80, Seq: 261, Ack: 625, Len: 332
v Hypertext Transfer Protocol
  > GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/0d87d8674b1b70b3339bfb4670a6ea5c83c
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    Accept-Encoding: identity\r\n
    If-Unmodified-Since: Sat, 20 Sep 2025 11:32:53 GMT\r\n
    Range: bytes=0-1119\r\n
    User-Agent: Microsoft BITS/7.8\r\n
    Host: edgedl.me.gvt1.com\r\n
    \r\n
    [Response in frame: 164]
    [Full request URI: http://edgedl.me.gvt1.com/edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfbl
```

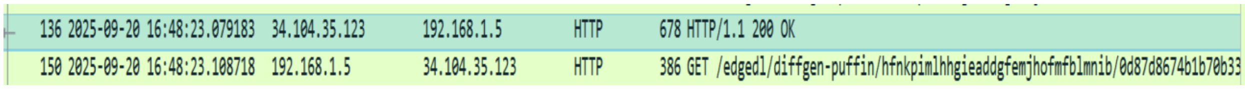
Question :04:

Identify the status code in the first server response.

Answer:

The status code : *200 OK*".

```
HTTP/1.1 200 OK
```



```
136 2025-09-20 16:48:23.079183  34.104.35.123  192.168.1.5    HTTP  678 HTTP/1.1 200 OK
150 2025-09-20 16:48:23.108718  192.168.1.5    34.104.35.123  HTTP  386 GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/0d87d8674b1b70b33
```

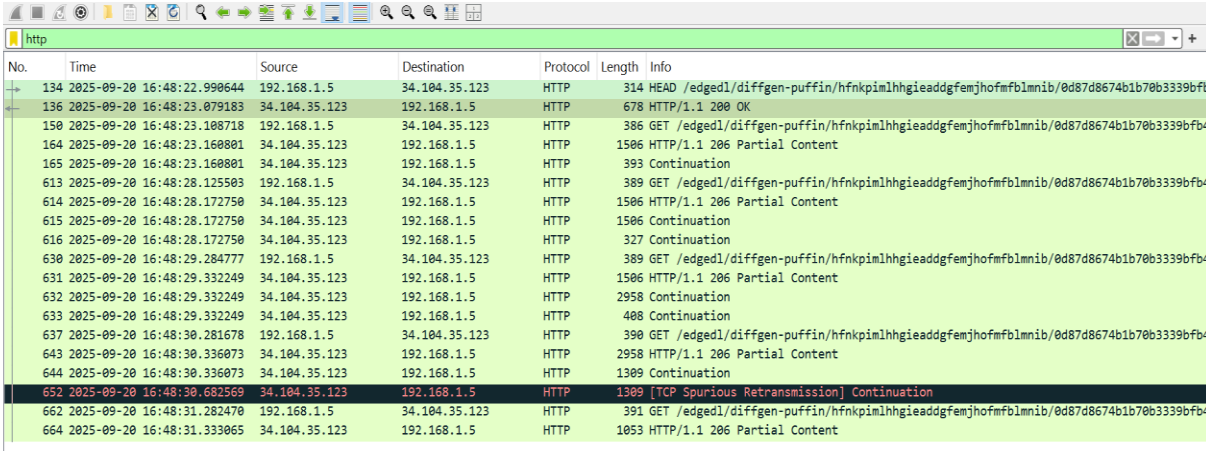
Question :05:

How many HTTP response messages are exchanged in total?

Answer:

There are the 11 response Messages .

1. Packet 135: `HTTP/1.1 200 OK` (Response to the HEAD request)
2. Packet 144: `HTTP/1.1 200 OK` (Response to the GET request)
3. Packet 158: `HTTP/1.1 206 Partial Content` (Response to a GET request)
4. Packet 614: `HTTP/1.1 206 Partial Content` (Response to a GET request)
5. Packet 616: `HTTP/1.1 206 Partial Content` (Response to a GET request)
6. Packet 631: `HTTP/1.1 206 Partial Content` (Response to a GET request)
7. Packet 633: `HTTP/1.1 206 Partial Content` (Response to a GET request)
8. Packet 643: `HTTP/1.1 206 Partial Content` (Response to a GET request)
9. Packet 644: `HTTP/1.1 206 Partial Content` (Response to a GET request)
10. Packet 652: `HTTP/1.1 206 Partial Content` (Response to a GET request)
11. Packet 664: `HTTP/1.1 206 Partial Content` (Response to a GET request)



http

No.	Time	Source	Destination	Protocol	Length	Info
134	2025-09-20 16:48:22.990644	192.168.1.5	34.104.35.123	HTTP	314	HEAD /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/0d87d8674b1b70b3339bf
136	2025-09-20 16:48:23.079183	34.104.35.123	192.168.1.5	HTTP	678	HTTP/1.1 200 OK
150	2025-09-20 16:48:23.108718	192.168.1.5	34.104.35.123	HTTP	386	GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/0d87d8674b1b70b3339bfb
164	2025-09-20 16:48:23.160801	34.104.35.123	192.168.1.5	HTTP	1506	HTTP/1.1 206 Partial Content
165	2025-09-20 16:48:23.160801	34.104.35.123	192.168.1.5	HTTP	393	Continuation
613	2025-09-20 16:48:28.125503	192.168.1.5	34.104.35.123	HTTP	389	GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/0d87d8674b1b70b3339bfb
614	2025-09-20 16:48:28.172750	34.104.35.123	192.168.1.5	HTTP	1506	HTTP/1.1 206 Partial Content
615	2025-09-20 16:48:28.172750	34.104.35.123	192.168.1.5	HTTP	1506	Continuation
616	2025-09-20 16:48:28.172750	34.104.35.123	192.168.1.5	HTTP	327	Continuation
630	2025-09-20 16:48:29.284777	192.168.1.5	34.104.35.123	HTTP	389	GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/0d87d8674b1b70b3339bfb
631	2025-09-20 16:48:29.332249	34.104.35.123	192.168.1.5	HTTP	1506	HTTP/1.1 206 Partial Content
632	2025-09-20 16:48:29.332249	34.104.35.123	192.168.1.5	HTTP	2958	Continuation
633	2025-09-20 16:48:29.332249	34.104.35.123	192.168.1.5	HTTP	408	Continuation
637	2025-09-20 16:48:30.281678	192.168.1.5	34.104.35.123	HTTP	390	GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/0d87d8674b1b70b3339bfb
643	2025-09-20 16:48:30.336073	34.104.35.123	192.168.1.5	HTTP	2958	HTTP/1.1 206 Partial Content
644	2025-09-20 16:48:30.336073	34.104.35.123	192.168.1.5	HTTP	1309	Continuation
652	2025-09-20 16:48:30.682569	34.104.35.123	192.168.1.5	HTTP	1309	[TCP Spurious Retransmission] Continuation
662	2025-09-20 16:48:31.282470	192.168.1.5	34.104.35.123	HTTP	391	GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/0d87d8674b1b70b3339bfb
664	2025-09-20 16:48:31.333065	34.104.35.123	192.168.1.5	HTTP	1053	HTTP/1.1 206 Partial Content

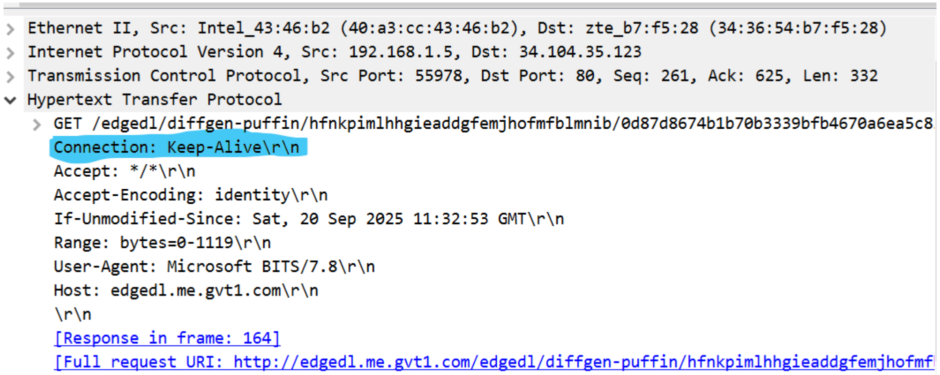
Question :06:

Determine whether the connection is persistent or not. Justify with evidence from packet captures.

Answer:

Yes, the connection is persistent. There is clear evidence in the capture:

1. **Client Request:** The client explicitly asks for a persistent connection with the header Connection : **Keep-Alive.**



```
> Ethernet II, Src: Intel_43:46:b2 (40:a3:cc:43:46:b2), Dst: zte_b7:f5:28 (34:36:54:b7:f5:28)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 34.104.35.123
> Transmission Control Protocol, Src Port: 55978, Dst Port: 80, Seq: 261, Ack: 625, Len: 332
v Hypertext Transfer Protocol
  > GET /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/0d87d8674b1b70b3339bfb4670a6ea5c8
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    Accept-Encoding: identity\r\n
    If-Unmodified-Since: Sat, 20 Sep 2025 11:32:53 GMT\r\n
    Range: bytes=0-1119\r\n
    User-Agent: Microsoft BITS/7.8\r\n
    Host: edgedl.me.gvt1.com\r\n
    \r\n
    [Response in frame: 164]
    [Full request URI: http://edgedl.me.gvt1.com/edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmf
```

2. **Server Action:** Multiple HTTP request/response transactions (e.g., the GET requests in packets 150, 164, 165) occur between the same IP addresses (**192.168.1.5** and **34.104.35.123**) over a very short time span (~7 seconds) without the TCP connection being torn down and re-established between them. This is the practical evidence of a persistent connection being used.

The use of the **Range** header and multiple **206 Partial Content** responses is a classic example of a single client using a single persistent connection to download different chunks of a file.