

CS408 HW1

Bartu Sisman

00028038

1-)

This is the response packet that comes from the website

```
298 14.561384 10.2.1.88 159.20.91.209 DNS 239 Standard query response 0xeb1b A bsu.edu.az A 85.132.96.212
```

When we go into details of this packet we see:

```
Answers
  bsu.edu.az: type A, class IN, addr 85.132.96.212
```

This is the ip address of the domain bsu.edu.az, 85.132.96.212

2-)

This is the GET request package that we are interested in

```
387 14.596881 159.20.91.209 85.132.96.212 HTTP 741 GET /en/ HTTP/1.1
```

And in the details, we see:

```
Transmission Control Protocol, Src Port: 51997, Dst Port: 80, Seq: 1, Ack: 1, Len: 687
  Source Port: 51997
  Destination Port: 80
```

Source port is 51997 and Destination port is 80

3-)

These are the request and reply packages when we used the command

`ping unsam.edu.ar` we only need one pair to determine the ip address so:

```
109... 41.176740 159.20.91.209 172.67.75.100 ICMP 74 Echo (ping) request id=0x0001, seq=41/10496, ttl=128 (reply in 10950)
109... 41.222197 172.67.75.100 159.20.91.209 ICMP 74 Echo (ping) reply id=0x0001, seq=41/10496, ttl=55 (request in 10949)
```

As we can see request has been made by pc which has an ip address of 159.20.91.209

And reply was made by the website which has the ip address of 172.67.15.100

So this the ip address of the domain

4-)

For the Echo request:

```
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
```

Type number is 8

For the Echo reply

```
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
```

Type number is 0

5-)

When we open the details of this package:

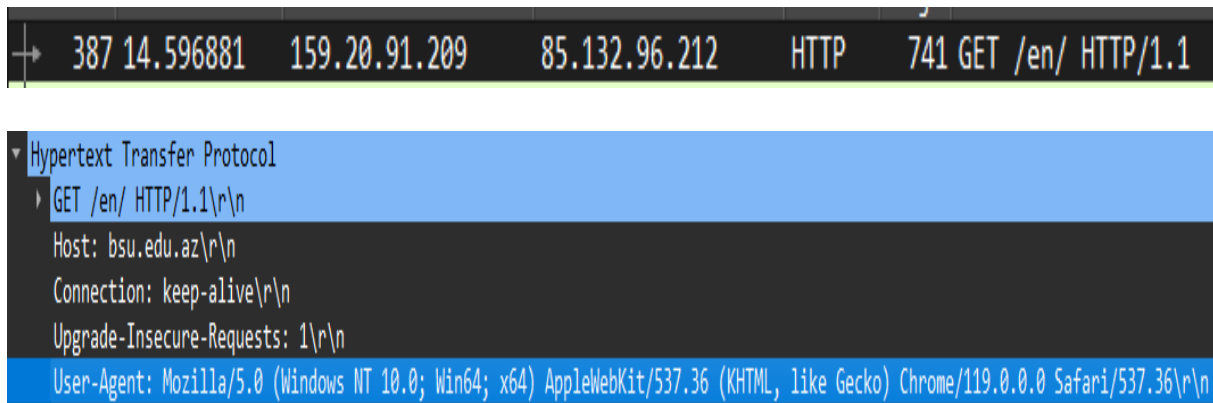
```
109... 41.222.197 172.67.75.100 159.20.91.209 ICMP 74 Echo (ping) reply id=0x0001, seq=41/10496, ttl=55 (request in 10949)
```

```
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x5532 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 41 (0x0029)
  Sequence Number (LE): 10496 (0x2900)
  [Request frame: 10949]
  [Response time: 45.457 ms]
  ▶ Data (32 bytes)
```

We can see that the data length is 32 bytes

6-)

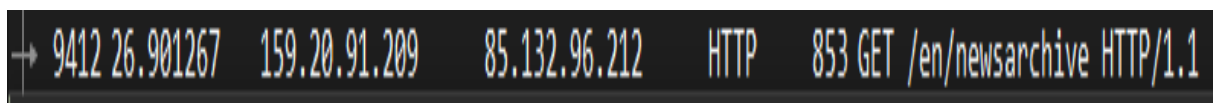
We can see when we get into the package details of this package:



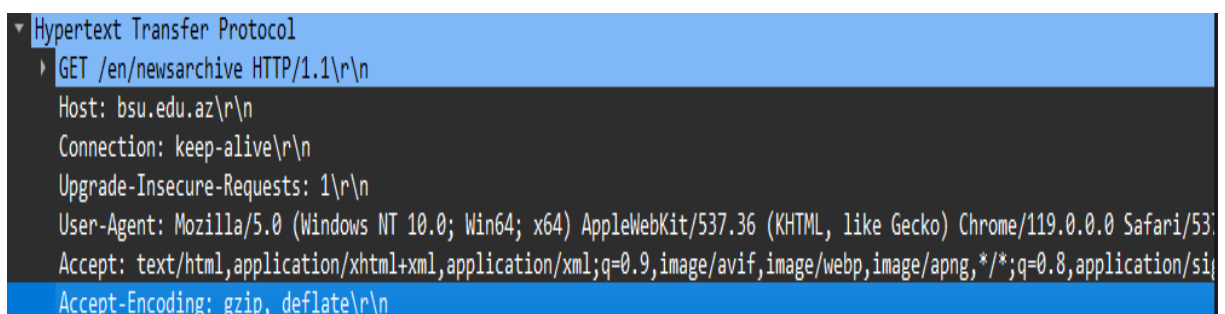
The user agent header's value is this string which identifies the versions of the browser and my operating system.

7-)

When we go into the details of this package:



We see:



The accept encoding part is show and its “gzip”

8-)

When we inspect the get package that was sent to the website:

```
▼ Hypertext Transfer Protocol
  ▶ GET /en/newsarchive HTTP/1.1\r\n
    Host: bsu.edu.az\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/5
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/s
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,tr-TR;q=0.8,tr;q=0.7\r\n
    ▶ [truncated]Cookie: __utzm=118507930.1700179795.1.1.utmcsr=(direct)|utmccn=(direct)|utmcid=(none); _ga=GA1.3.142100975
    \r\n
    [Full request URI: http://bsu.edu.az/en/newsarchive]
    [HTTP request 1/1]
    [Response in frame: 9529]
```

at the bottom line we see that Response in frame: 9529 which is the number of the message that was sent from the server which is this:

response package:

```
9529 28.214317 85.132.96.212 159.20.91.209 HTTP 188 HTTP/1.1 200 OK (text/html)
```

And we can see that http status code is 200 OK

9-)

These are ARP requests and replies:

45 3.220401	MicroStarINT_78:...	Broadcast	ARP	42 Who has 159.20.91.1? Tell 159.20.91.209
46 3.221418	Cisco_01:e9:fa	MicroStarINT_78:...	ARP	60 159.20.91.1 is at 70:01:b5:01:e9:fa
130 6.436723	RealtekSemic_68:...	Broadcast	ARP	60 Who has 169.254.187.211? (ARP Probe)
133 7.430977	RealtekSemic_68:...	Broadcast	ARP	60 Who has 169.254.187.211? (ARP Probe)
142 8.424814	RealtekSemic_68:...	Broadcast	ARP	60 Who has 169.254.187.211? (ARP Probe)
153 9.433055	RealtekSemic_68:...	Broadcast	ARP	60 ARP Announcement for 169.254.187.211
195 11.429283	RealtekSemic_68:...	Broadcast	ARP	60 ARP Announcement for 169.254.187.211
9441 27.898582	RealtekSemic_68:...	Broadcast	ARP	60 Who has 159.20.91.1? Tell 159.20.91.26
9504 28.174552	RealtekSemic_68:...	Broadcast	ARP	60 Who has 159.20.91.1? Tell 159.20.91.26
9536 28.235523	RealtekSemic_68:...	Broadcast	ARP	60 Who has 159.20.91.26? (ARP Probe)
9600 29.242893	RealtekSemic_68:...	Broadcast	ARP	60 Who has 159.20.91.26? (ARP Probe)
9618 30.238664	RealtekSemic_68:...	Broadcast	ARP	60 Who has 159.20.91.26? (ARP Probe)
9722 31.237344	RealtekSemic_68:...	Broadcast	ARP	60 ARP Announcement for 159.20.91.26
9929 33.238345	RealtekSemic_68:...	Broadcast	ARP	60 ARP Announcement for 159.20.91.26
109... 40.933339	RealtekSemic_68:...	Broadcast	ARP	60 Who has 169.254.187.211? (ARP Probe)
109... 41.928393	RealtekSemic_68:...	Broadcast	ARP	60 Who has 169.254.187.211? (ARP Probe)
109... 42.937744	RealtekSemic_68:...	Broadcast	ARP	60 Who has 169.254.187.211? (ARP Probe)
118... 43.936328	RealtekSemic_68:...	Broadcast	ARP	60 ARP Announcement for 169.254.187.211
119... 45.936872	RealtekSemic_68:...	Broadcast	ARP	60 ARP Announcement for 169.254.187.211

This is one of the ARP requests:

```
9536 28.235523 RealtekSemic_68:... Broadcast ARP 60 Who has 159.20.91.26? (ARP Probe)
```

And these are its s Sender, Target MAC addresses and Sender, Target IP addresses.

```
▼ Address Resolution Protocol (ARP Probe)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  [Is probe: True]
  Sender MAC address: RealtekSemic_68:37:ac (00:e0:4c:68:37:ac)
  Sender IP address: 0.0.0.0
  Target MAC address: Xerox_00:00:00 (00:00:00:00:00:00)
  Target IP address: 159.20.91.26
```

This is a ARP reply:

```
46 3.221418 Cisco_01:e9:fa MicroStarINT_78:... ARP 60 159.20.91.1 is at 70:01:b5:01:e9:fa
```

And these are its s Sender, Target MAC addresses and Sender, Target IP addresses.

```
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Cisco_01:e9:fa (70:01:b5:01:e9:fa)
  Sender IP address: 159.20.91.1
  Target MAC address: MicroStarINT_78:b0:f0 (2c:f0:5d:78:b0:f0)
  Target IP address: 159.20.91.209
```

10-)

ip.src == 192.105.59.24 && tcp.dstport == 1334

