

# DIGITAL FORENSICS PROJECT – QUESTION 1

As a forensic examiner, you are required to analyze the given capture file using Wireshark and answer the following questions in your report:

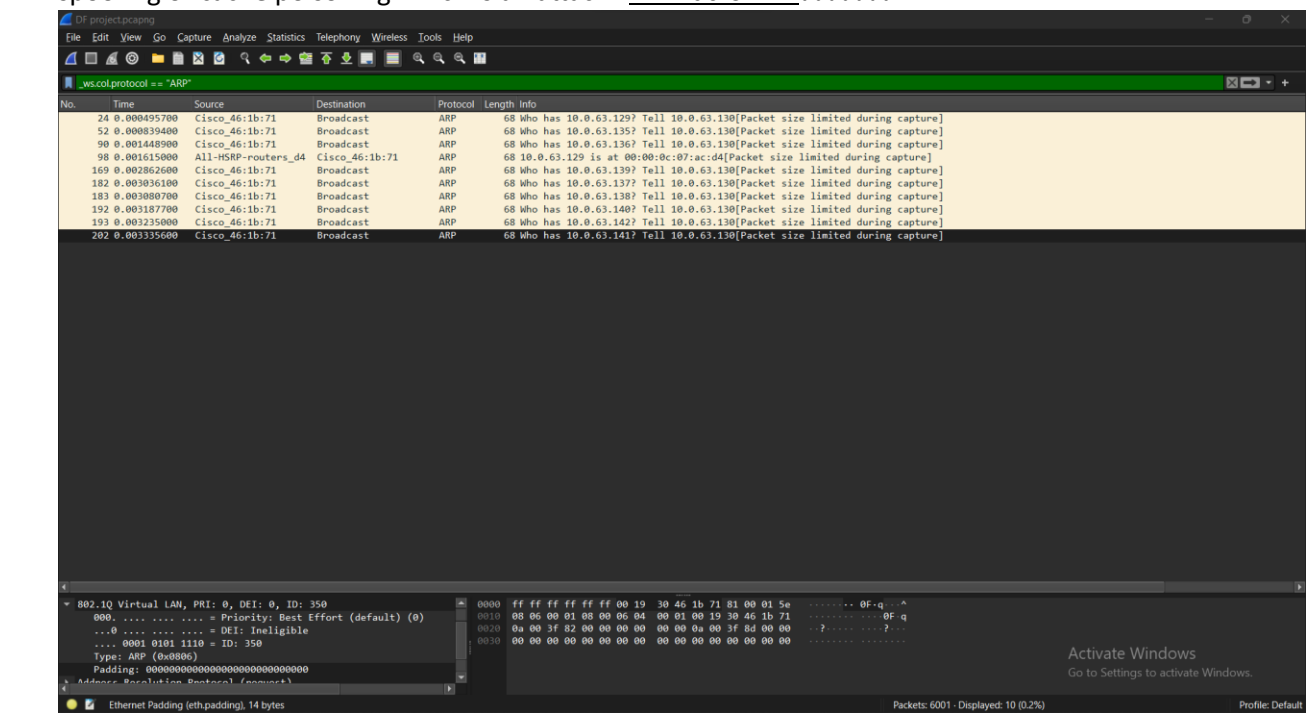
<https://drive.google.com/file/d/16GR5hpLa-Jlo7HcJiN2BFAIMLO0I3IG5/view?usp=sharing>

## 1.1 Is this an Attack? Justify your answer.

**Yes, it is a Distributed Denial of Service attack (DDoS)**

**Justification:**

- Different source IPs are sending to the same destination IP (attempt to overwhelm a target system or network with a flood of traffic).
- [Packet size limited during capture] -- Was repeated multiple times which indicates a big traffic of data was being forced into transmission.
- Distinct/unexpected protocol (ARP) repeated multiple times which might indicate for ARP spoofing or cache poisoning which is an attack. – **What is ARP???????**



- Unusual source/destination ports (Greater than 1024)

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a TCP capture with the filter 'tcp.port > 1024'. The packet list shows multiple SYN packets from various source IP addresses to destination 10.0.64.129 on ports ranging from 16384 to 1986. The packet details pane shows the structure of a TCP segment, including the Virtual LAN (VLAN) tag and the Ethernet II header. The bottom screenshot shows a UDP capture with the filter 'udp.port > 1024'. The packet list shows three UDP packets from source IP 0.0.0.0 to destination 172.16.104.0 on ports 8116, 8116, and 22472. The packet details pane shows the structure of a UDP segment, including the Ethernet II header and the IP header.

## 1.2 Discover the source geo IP country? (do your own research)

Argentina.

Sorting by "Bytes" displayed IP addresses based on the number of Bytes sent:

Wireshark - Endpoints - DF project.pcapng

Endpoint Settings

- Name resolution
- Limit to display filter

Copy

Map

Protocol

- Bluetooth
- BPv7
- DCCP
- ✓ Ethernet
- FC
- FDI
- IEEE 802.11
- IEEE 802.15.4
- ✓ IPv4
- ✓ IPv6
- IPX
- JXTA
- LTP
- MPICP
- NCP
- OpenSAFETY
- RSVP
- SCTP
- SLL
- TCP
- Token-Ring
- ✓ UDP

Filter list for specific type

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
mail-mail-mov.net	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
46.19.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
233.19.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
144.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
148.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
149.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
157.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
160.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
161.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
169.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
174.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
183.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
189.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
191.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
192.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
193.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
199.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
201.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
205.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
206.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
208.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
209.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
212.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
214.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
215.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
231.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
251.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
252.27.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
6.28.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
7.28.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
18.28.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
19.28.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
24.28.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
200.80.28.26	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
200.80.28.27	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
200.80.28.30	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
200.80.28.31	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
33.28.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
200.80.28.47	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
70.28.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
71.28.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
82.28.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
83.28.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
200.80.28.84	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
200.80.28.85	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					
92.28.80.200.static.host.ifmw.com.ar	1	64 bytes	1	64 bytes	0	0 bytes	Argentina					

Activate Windows  
Go to Settings to activate Windows.

Close Help

### 1.3 How many countries are involved?

19 countries.

➔ Argentina, Canada, China, Germany, India, Japan, Mexico, Russia, Turkey, UK, US, Belgium, Australia, Sweden, Switzerland, Colombia, Slovenia, Netherlands

### 1.4 Choose any of the identified locations in Question 2, how many packets come from the location you choose? Mention the location and the number of packets.

I choose the **United States (US)**.

Number of packets: **569**

Wireshark - DF project.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==10.0.0.0/8

No.	Time	Source	Destination	Protocol	Length	Info
51	0.000825880	10.0.63.131	95.173.168.10	TCP	68	1986 → 2938 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 [Packet size limited during capture]
99	0.001782280	1.147.61.208	10.0.64.129	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit) [Packet size limited during capture]
228	0.004048480	7.147.61.208	10.0.64.129	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit) [Packet size limited during capture]
285	0.004945300	10.0.64.129	214.174.37.159	TCP	68	80 → 19920 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
286	0.004973400	10.0.64.129	61.181.39.27	TCP	68	80 → 19907 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
287	0.005023300	10.0.64.129	161.39.195.35.bc.go...	TCP	68	80 → 20255 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
288	0.005037400	10.0.64.129	194.74.23.131	TCP	68	80 → 18188 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
289	0.005071600	10.0.64.129	194.74.22.221	TCP	68	80 → 18042 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
290	0.005104000	10.0.64.129	61.181.39.144	TCP	68	80 → 20024 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
291	0.005132100	10.0.64.129	34.39.195.35.bc.go...	TCP	68	80 → 20128 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
297	0.005201200	10.0.64.129	194.74.23.108	TCP	68	80 → 18185 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
301	0.005274700	10.0.64.129	142.142.23.122	TCP	68	80 → 15267 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
310	0.005315700	10.0.64.129	206.126.31.67	TCP	68	80 → 18044 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
311	0.005357100	10.0.64.129	142.142.23.133	TCP	68	80 → 15278 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
312	0.005403600	10.0.64.129	63.39.195.35.bc.go...	TCP	68	80 → 20157 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
313	0.005437600	10.0.64.129	99.99.27.87.1lightsp...	TCP	68	80 → 18613 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
314	0.005457700	10.0.64.129	99.99.27.85.1lightsp...	TCP	68	80 → 18611 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
323	0.005585800	10.0.64.129	142.142.23.119	TCP	68	80 → 15264 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
324	0.005618000	10.0.64.129	206.126.30.239	TCP	68	80 → 17960 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
324	0.005621400	10.0.64.129	10.0.64.129	TCP	68	Time-to-live exceeded (Time to live exceeded in transit) [Packet size limited during capture]
351	0.006363000	10.0.64.129	93.173.34.255	TCP	68	80 → 19847 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
352	0.006369400	10.0.64.129	142.142.23.97	TCP	68	80 → 15242 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
353	0.006376500	10.0.64.129	ec2-44-204-9-135.co...	TCP	68	80 → 14958 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
354	0.006383700	10.0.64.129	host-232-252-14-15...	TCP	68	80 → 16766 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
355	0.006390200	10.0.64.129	206.126.31.7	TCP	68	80 → 17984 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
356	0.006397100	10.0.64.129	142.142.23.64	TCP	68	80 → 15209 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
357	0.006404600	10.0.64.129	206.126.30.242	TCP	68	80 → 17963 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
358	0.006411500	10.0.64.129	142.142.23.135	TCP	68	80 → 15280 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
359	0.006418000	10.0.64.129	206.126.31.110	TCP	68	80 → 18087 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
360	0.006424900	10.0.64.129	ec2-44-204-9-24.co...	TCP	68	80 → 14847 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
361	0.006431800	10.0.64.129	61.181.39.24	TCP	68	80 → 19904 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
362	0.006438900	10.0.64.129	206.126.31.55	TCP	68	80 → 18032 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
363	0.006445300	10.0.64.129	194.74.22.235	TCP	68	80 → 18056 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
364	0.006451800	10.0.64.129	206.126.31.127	TCP	68	80 → 18104 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
365	0.006458800	10.0.64.129	dsl-187-147-14-7-dy...	TCP	68	80 → 16253 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
366	0.006465300	10.0.64.129	172.212.12.97	TCP	68	80 → 16296 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
367	0.006471700	10.0.64.129	ec2-44-204-9-31.co...	TCP	68	80 → 14854 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
368	0.006478700	10.0.64.129	206.126.31.22	TCP	68	80 → 17999 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
369	0.006485600	10.0.64.129	93.173.34.252.bb.ne...	TCP	68	80 → 19844 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
373	0.006492100	10.0.64.129	61.181.38.220	TCP	68	80 → 19844 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
378	0.006498800	10.0.64.129	61.181.39.36	TCP	68	80 → 19916 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460
381	0.006505600	10.0.64.129	206.126.31.42	TCP	68	80 → 18019 [SYN, ACK] Seq=0 Ack=1 Win=1608 Len=0 MSS=1460

Activate Windows  
Go to Settings to activate Windows.

Close Help

Source Address: IPv4 address

Packets: 6001. Displayed: 569 (9.5%)

Profile: Default

### 1.5 Are these packets made by a bot or normal devices?

Packets are made by normal devices.

- (Most of them are with source /destination MAC addresses from Cisco.
- No environmental metrics were shown.
- Looked for protocols that might indicate IoT devices communication and there were none.

### 1.6 Extract the TTL of the packets and show how it can be used in discovering attacks.

**TTLs of the US packets:**

- **255** – “The maximum TTL value”. It could suggest potential packet spoofing, as the packet might have originated from nearby or directly from the source rather than going through multiple network hops.
- **254** – “A common initial TTL value set by many operating systems”. Might indicate altered routing paths or attempts to blend in with normal traffic by setting TTL to a commonly expected value.
- **248, 247, 246, 245 and 243** – Might indicate a typical number of hops for certain types of traffic. Could indicate route manipulation, altered traffic paths, or potential attacks like packet injection.
- **127, 126, 63 and 62** – “Intermediate TTL values”. Sudden changes in TTL values compared to the normal for specific traffic could indicate anomalies, route manipulation, or traffic redirection attempts.
- **52 and 47** - Unexpectedly low TTL values for specific traffic might suggest potential spoofing or route alteration.