RAO ALI NAWAZ
FA22A-222666
DIGITAL FORENSICS LAB 4

**TASK 1**

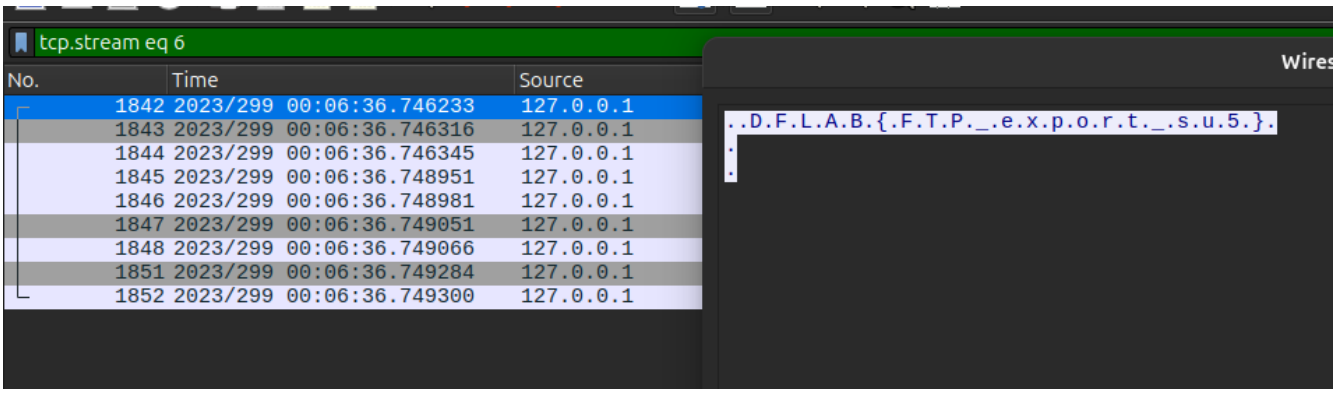
**1. Which File Transfer Service is used in the captured traffic?**
**FTP**

| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | End Bits/s | PDUs |
|---|---|---|---|---|---|---|---|---|---|
| Frame | 100.0 | 2019 | 100.0 | 100616 | 6,966 | 0 | 0 | 0 | 2019 |
| Null/Loopback | 100.0 | 2019 | 8.0 | 8076 | 559 | 0 | 0 | 0 | 2019 |
| Internet Protocol Version 4 | 100.0 | 2019 | 40.1 | 40392 | 2,796 | 0 | 0 | 0 | 2019 |
| User Datagram Protocol | 1.0 | 21 | 0.2 | 168 | 11 | 0 | 0 | 0 | 21 |
| Simple Service Discovery Protocol | 1.0 | 21 | 3.7 | 3675 | 254 | 21 | 3675 | 254 | 21 |
| Transmission Control Protocol | 98.4 | 1987 | 47.2 | 47449 | 3,285 | 1009 | 20276 | 1,403 | 1987 |
| Transport Layer Security | 1.9 | 39 | 5.5 | 5539 | 383 | 39 | 5539 | 383 | 39 |
| File Transfer Protocol (FTP) | 2.2 | 44 | 1.1 | 1132 | 78 | 44 | 1132 | 78 | 44 |
| Data | 44.3 | 895 | 0.9 | 942 | 65 | 895 | 942 | 65 | 895 |
| Internet Group Management Protocol | 0.1 | 3 | 0.0 | 24 | 1 | 3 | 24 | 1 | 3 |
| Internet Control Message Protocol | 0.4 | 8 | 0.8 | 832 | 57 | 0 | 0 | 0 | 8 |
| NetBIOS Name Service | 0.4 | 8 | 0.5 | 544 | 37 | 8 | 544 | 37 | 8 |

**2. What was the name of the file that was transferred?**
**`important.txt`**

```
220-FileZilla Server 1.7.3
220 Please visit https://filezilla-project.org/
OPTS UTF8 ON
202 UTF8 mode is always enabled. No need to send this command
USER test
331 Please, specify the password.
PASS
230 Login successful.
PORT 127,0,0,1,208,142
200 PORT command successful.
STOR important.txt
150 Starting data transfer.
226 Operation successful
QUIT
221 Goodbye.
```

**3. What was the packet number and timestamp? 1842, Oct 26, 2023 00:06:36.746233000 PKT**




**4. In which packet number data (flag) was found? D.F.L.A.B.{.F.T.P._.e.x.p.o.r.t._.s.u.5.}.**

**5. What was the DATA?**

**D.F.L.A.B.{.F.T.P._.e.x.p.o.r.t._.s.u.5.}.**

**TASK 2**

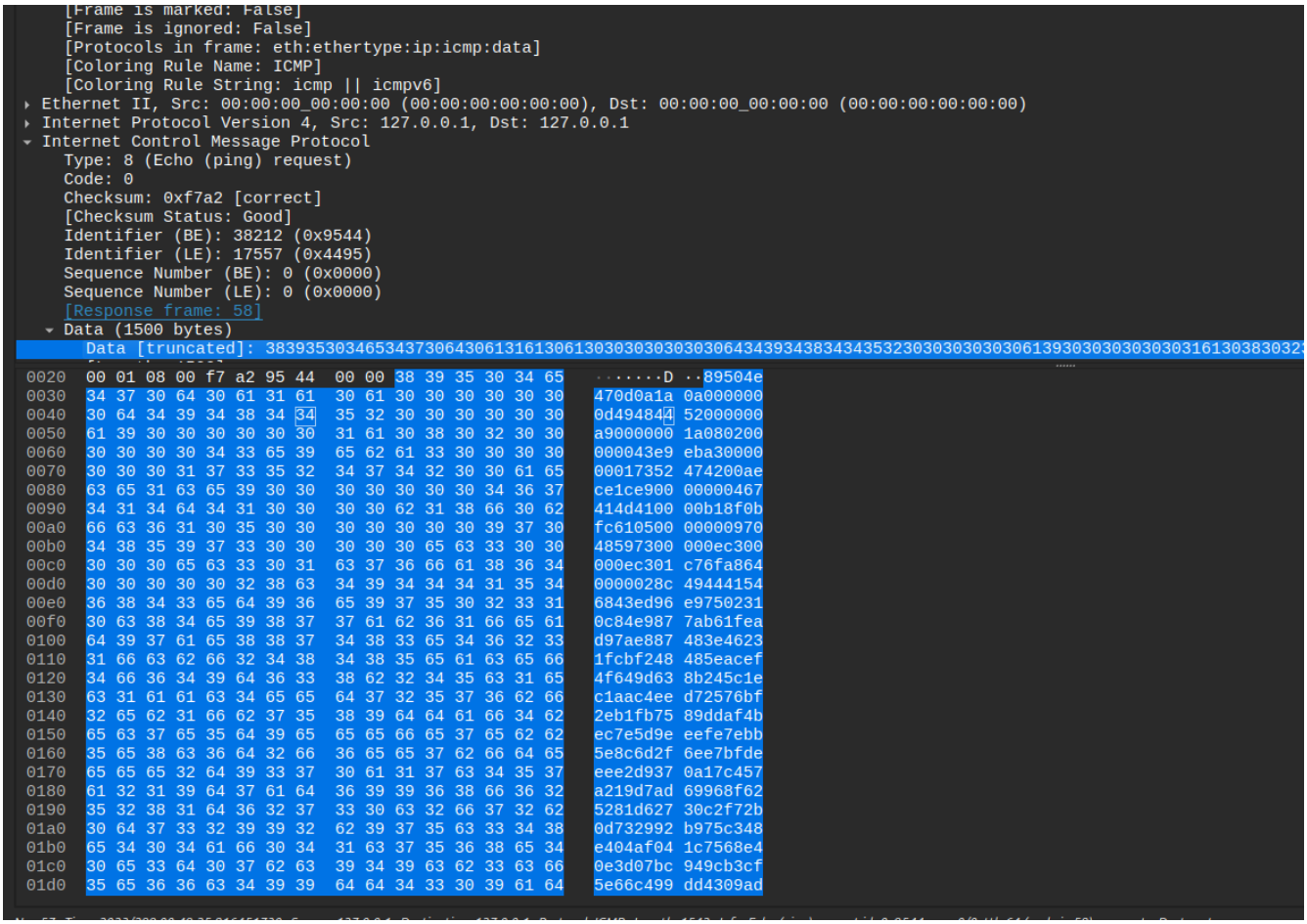
**Analyze the file named icmp.pcap. Answer these questions:**

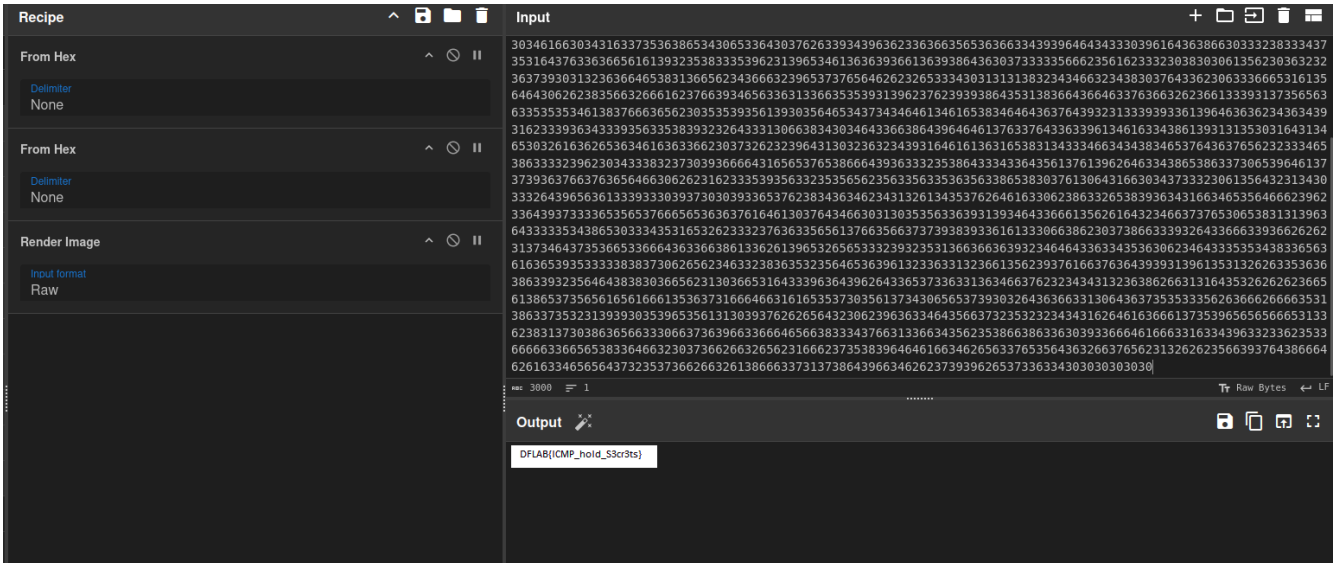
**1. What was the timestamp of the first packet sent? Oct 26, 2023 00:48:18.077216790 PKT**

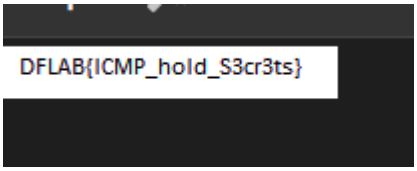
**2. What is the ICMP type number of the request packet? 8**

**3. What is the recovered DATA?**

**57 packet**




Recipe
From Hex
Delimiter
None
From Hex
Delimiter
None
Render Image
Input format
Raw
Input
Output
DFLAB{ICMP_hold_S3cr3ts}


DFLAB{ICMP_hold_S3cr3ts}