

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

tcp.stream eq 6				
No.	Time	Source		Wire
1842	2023/299 00:06:36.746233	127.0.0.1		.D.F.L.A.B.{.F.T.P._e.x.p.o.r.t._s.u.5.}.
1843	2023/299 00:06:36.746316	127.0.0.1		
1844	2023/299 00:06:36.746345	127.0.0.1		
1845	2023/299 00:06:36.748951	127.0.0.1		
1846	2023/299 00:06:36.748981	127.0.0.1		
1847	2023/299 00:06:36.749051	127.0.0.1		
1848	2023/299 00:06:36.749066	127.0.0.1		
1851	2023/299 00:06:36.749284	127.0.0.1		
1852	2023/299 00:06:36.749300	127.0.0.1		

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

```
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf7a2 [correct]
  [Checksum Status: Good]
  Identifier (BE): 38212 (0x9544)
  Identifier (LE): 17557 (0x4495)
  Sequence Number (BE): 0 (0x0000)
  Sequence Number (LE): 0 (0x0000)
  [Response frame: 58]
▼ Data (1500 bytes)
  Data [truncated]: 3839353034653437306430613161306130303030303064343934383434353230303030306139303030303030316130383032
0020 00 01 08 00 f7 a2 95 44 00 00 38 39 35 30 34 65 .....D ..89504e
0030 34 37 30 64 30 61 31 61 30 61 30 30 30 30 30 30 470d0a1a 0a000000
0040 30 64 34 39 34 38 34 34 35 32 30 30 30 30 30 30 0d49484d 52000000
0050 61 39 30 30 30 30 30 30 31 61 30 38 30 32 30 30 a9000000 1a000200
0060 30 30 30 30 34 33 65 39 65 62 61 33 30 30 30 30 000043e9 eba30000
0070 30 30 30 31 37 33 35 32 34 37 34 32 30 30 61 65 00017352 474200ae
0080 63 65 31 63 65 39 30 30 30 30 30 30 34 36 37 ce1ce900 00000467
0090 34 31 34 64 34 31 30 30 30 30 62 31 38 66 30 62 414d4100 00b18f0b
00a0 66 63 36 31 30 35 30 30 30 30 30 30 39 37 30 fc610500 00000970
00b0 34 38 35 39 37 33 30 30 30 30 30 65 63 33 30 30 48597309 000ec300
00c0 30 30 30 65 63 33 30 31 63 37 36 66 61 38 36 34 000ec301 c76fa864
00d0 30 30 30 30 30 32 38 63 34 39 34 34 34 31 35 34 0000028c 49444154
00e0 36 38 34 33 65 64 39 36 65 39 37 35 30 32 33 31 6843ed96 e9750231
00f0 30 63 38 34 65 39 38 37 37 61 62 36 31 66 65 61 0c84e987 7ab61fea
0100 64 39 37 61 65 38 38 37 34 38 33 65 34 36 32 33 d97ae887 483e4623
0110 31 66 63 62 66 32 34 38 34 38 35 65 61 63 65 66 1fcbf248 485eacef
0120 34 66 36 34 39 64 36 33 38 62 32 34 35 63 31 65 4f649d63 8b245c1e
0130 63 31 61 61 63 34 65 65 64 37 32 35 37 36 62 66 c1aac4ee d72576bf
0140 32 65 62 31 66 62 37 35 38 39 64 64 61 66 34 62 2eb1fb75 89ddaf4b
0150 65 63 37 65 35 64 39 65 65 65 66 65 37 65 62 62 ec7e5d9e eefe7ebb
0160 35 65 38 63 36 64 32 66 36 65 65 37 62 66 64 65 5e8c6d2f 6ee7b7de
0170 65 65 65 32 64 39 33 37 30 61 31 37 63 34 35 37 eee2d937 0a17c457
0180 61 32 31 39 64 37 61 64 36 39 39 36 38 66 36 32 a219d7ad 69968f62
0190 35 32 38 31 64 36 32 37 33 30 63 32 66 37 32 62 5281d627 30c2f72b
01a0 30 64 37 33 32 39 39 32 62 39 37 35 63 33 34 38 0d732992 b975c348
01b0 65 34 30 34 61 66 30 34 31 63 37 35 36 38 65 34 e404af04 1c7568e4
01c0 30 65 33 64 30 37 62 63 39 34 39 63 62 33 63 66 0e3d07bc 949cb3cf
01d0 35 65 36 36 63 34 39 39 64 64 34 33 30 39 61 64 5e66c499 dd4309ad
```

Recipe

From Hex

Delimiter

None

From Hex

Delimiter

None

Render Image

Input format

Raw

Input

```

30346166303431633735363865343065336430376236393439636236366356536366334392964643433039616436386630332328333437
3531643763363665616139323538333539623139653461363639366136393864363837333335666235616233232308303861356230362232
363739303132363664653831366562343666323965377376564626232653334303113133832343466323438303764333623063336665316135
6464386262383566326661623766393465633631336635353931396237623939386435313836643664633763663262366133393137355653
6335353534613837666365623035353935613930356465343734346461346165383446446367643932313339393361396463636234363439
31623339363433393653353839323264333130663834303464336638643964646137637376433633961346163343861393131353031643134
653032616362653634616363366230373262323964313032363236343931646161363165383134333466343438346537643637656232333465
386333323962303433383237303936666431656537653866643936333235386433433643561376139626463343865386637306539646137
373936376637636564663062623162333539356332353565623563356335633638653830376130643166303437332361356432313430
33326439656361333933303937303830393653762383436346234313261343537626461633662386332653839363431663465356466623962
33643937333365356537666565363637616461303764346630313035356336393139346433666135626164323466373765306538313313963
6433333534386530333435316532623327676363356561376635663773938393631613330663862323738663392643366633936626262
313734643735666536664363366386133626139653265653323932353136636636393234646436336343563363662346433543833653
6163653935333338383730626562346332303635323564653639613233633122366135623937616637636439393139613531326263353636
3838393235646438383036656231303665316433396364396264336537336331363466376232343431323836626631316435316262623665
6138653735656165616661356373166646663161653537303561373430656537393832643636633130643637353533562636662666331
3863373532313939303539653561313039376262656432306239636334643566373235323234343416264616366613735965656566653133
6238313730386365663306637363966366646658333437663133663435623538663863630393966646166633136343963323632533
666663366565383364663230373662663265623166623735383964646166346265633765356436326637656231326232656393764386664
6261633465656437323537366266326138666337313738643966346262373939626537336334303030303030

```

Output

DLFAB(ICMP_hold_ScRsts)