# Comunicações por Computador

# Trabalho Prático $N^{\circ}$ .1 - Protocolos da Camada de Transporte

Eduardo Coelho, Henrique Neto, Júlio Alves e-mail: {a89616,a89618,a89468}@alunos.uminho.pt

16 de março de 2021

## Questões e Respostas

1. Identifique, para cada comando executado, qual o protocolo de aplicação, o protocolo de transporte, porta de atendimento e *overhead* de transporte.

Comando usado   Protocolo de Aplicação		Protocolo de transporte	Porta de atendimento	Overhead de transporte
(aplicação)	(se aplicável)	(se aplicável)	(se aplicável)	em bytes (se aplicável)
Ping	_	_	_	_
traceroute	_	UDP	33447	8
telnet	TELNET	TCP	23	20
ftp	FTP	TCP	58788	20
Tftp	TFTP	UDP	69	8
browser/http	HTTP	TCP	80	20
nslookup	DNS	UDP	60615	8
ssh	SSHv2	TCP	34980	20

No.	Time	Source	Destination	Protocol	
					Length Info
	1 0.000000000	10.0.2.15	192.168.1.1	DNS	89 Standard query 0xbd5b AAAA cisco.di.uminho.pt OPT
	2 0.003024052	192.168.1.1	10.0.2.15	DNS	89 Standard query response 0xbd5b AAAA cisco.di.uminho.pt OPT
	3 0.003901116	10.0.2.15	193.136.19.254	UDP	74 53240 → 33434 Len=32
	4 0.003988276	10.0.2.15	193.136.19.254	UDP	74 34172 → 33435 Len=32
	5 0.004048165	10.0.2.15	193.136.19.254	UDP	74 45309 → 33436 Len=32
	6 0.004389482	10.0.2.15	193.136.19.254	UDP	74 47991 → 33437 Len=32
	7 0.004416754	10.0.2.2	10.0.2.15	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
	8 0.004451081	10.0.2.15	193.136.19.254	UDP	74 38824 → 33438 Len=32
	9 0.004416867	10.0.2.2	10.0.2.15	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
	10 0.004416896	10.0.2.2	10.0.2.15	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
	11 0.004511339	10.0.2.15	193.136.19.254	UDP	74 32936 → 33439 Len=32
	12 0.004568916	10.0.2.15	193.136.19.254	UDP	74 55439 → 33440 Len=32
	13 0.004638589	10.0.2.15	193.136.19.254	UDP	74 36044 → 33441 Len=32
	14 0.004708286	10.0.2.15	193.136.19.254	UDP	74 54936 → 33442 Len=32
	15 0.004796737	10.0.2.15	193.136.19.254	UDP	74 38847 → 33443 Len=32
	16 0.004856495	10.0.2.15	193.136.19.254	UDP	74 40485 → 33444 Len=32
	17 0.004913822	10.0.2.15	193.136.19.254	UDP	74 58402 → 33445 Len=32
	18 0.004971786	10.0.2.15	193.136.19.254	UDP	74 59120 → 33446 Len=32
Г	19 0.005039551	10.0.2.15	193.136.19.254	UDP	74 49629 → 33447 Len=32
	20 0.005097270	10.0.2.15	193.136.19.254	UDP	74 34871 → 33448 Len=32
	21 0.005155593	10.0.2.15	193.136.19.254	UDP	74 52579 → 33449 Len=32
	22 0.005705004	10.0.2.15	192.168.1.1	DNS	■ Wireshark - Packet 19 - traceroute.pcapng
	23 0.006676381	10.0.2.2	10.0.2.15	ICMP	wirestank racket 13 traceroute, peaping
	24 0.008379750	10.0.2.2	10.0.2.15	ICMP	> Frame 19: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
	25 0.008380130	10.0.2.2	10.0.2.15	ICMP	> Ethernet II, Src: PcsCompu d1:8b:d0 (08:00:27:d1:8b:d0), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)
	26 0.009421706	192.168.1.1	10.0.2.15	DNS	> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 193.136.19.254
	27 0.009781524	10.0.2.15	192.168.1.1	DNS	✓ User Datagram Protocol, Src Port: 49629, Dst Port: 33447
	28 0.011569612	192.168.1.1	10.0.2.15	DNS	Source Port: 49629
	29 0.012222185	10.0.2.15	193.136.19.254	UDP	Destination Port: 33447
	30 0.012293674	10.0.2.15	193.136.19.254	UDP	Length: 40
	31 0.012492057	10.0.2.15	193.136.19.254	UDP	Checksum: 0xe1ce [unverified]
	32 0.012706310	10.0.2.15	192.168.1.1	DNS	[Checksum: oxeice [unverified]
	33 0.015734706	10.0.2.2	10.0.2.15	ICMP	[Stream index: 14]
	34 0.015734865	10.0.2.2	10.0.2.15	ICMP	[Stream index: 14] > [Timestamps]
	35 0.015735215	10.0.2.2	10.0.2.15	ICMP	UDP payload (32 bytes)
	36 0.015735248	10.0.2.2	10.0.2.15	ICMP	DDP payload (32 bytes)  Data (32 bytes)
	1// /21 /11 7 //	20.000	20 0 3 21	17.881	v Data (32 Dytes)

Figura 1: Traceroute

```
Length Info

86 Standard query 0x215c A cc2021.ddns.net OPT

86 Standard query 0x7243 AAAA cc2021.ddns.net OPT

86 Standard query response 0x7243 AAAA cc2021.ddns.net OPT

86 Standard query response 0x215c A cc2021.ddns.net OPT

87 Standard query response 0x215c A cc2021.ddns.net A 193.136.9.183 NS nf3.no-ip.com NS nf1.no-ip.com

87 S8928 + 23 [SVN] Seq=0 Win-62240 Len-0 MSS=1460 SACK_PERM=1 TSval=4142914872 TSecr=0 WS=128

88 S8928 + 23 [ACK] Seq=1 Ack=1 Win-65235 Len-0 MSS=1460

89 S8928 + 23 [ACK] Seq=1 Ack=2 Win-65240 Len-0

80 S81 Telnet Data ...

80 23 + S8928 [ACK] Seq=1 Ack=28 Win-65535 Len-0

80 Application Data

80 Application Data

80 A43 + 48702 [ACK] Seq=32 Ack=36 Win-65535 Len-0

81 Telnet Data ...
  Time
1 0.00000000
2 0.000167681
3 0.004317128
4 0.056743114
5 0.05726953
6 0.07788630
7 0.077988206
8 0.078685943
9 0.079043123
10 1.206416279
11 1.206649156
                                                                                                                                            10.0.2.15
10.0.2.15
192.168.1.1
192.168.1.1
                                                                                                                                                                                                                                                                                                                      192.168.1.1
192.168.1.1
192.168.1.1
10.0.2.15
10.0.2.15
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             DNS
DNS
DNS
DNS
                                                                                                                                     192.168.1.1
10.0.2.15
193.136.9.183
10.0.2.15
10.0.2.15
193.136.9.183
52.35.247.112
10.0.2.15
52.35.247.112
10.0.2.15
                                                                                                                                                                                                                                                                                                                   10.0.2.15
193.136.9.183
10.0.2.15
193.136.9.183
193.136.9.183
10.0.2.15
10.0.2.15
52.35.247.112
10.0.2.15
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             TCP
TCP
TELNET
TCP
TLSv1.2
TLSv1.2
10 1.206416279 52.35.247.112
11 1.206649156 10.0.2.15
12 1.207269054 52.35.247.112
13 4.001138130 10.0.2.15
16 14.286683958 193.136.9.183
18 15.127613457 10.0.2.15
19 15.186888622 193.136.9.183
18 15.127613457 10.0.2.15
19 15.186980364 10.0.2.15
21 15.187386422 10.0.2.15
21 15.187386422 10.0.2.15
21 5.207774768 10.0.2.15
25 15.208174538 10.0.2.15
25 15.208174538 10.0.2.15
26 15.208541368 193.136.9.183
27 15.227697723 193.136.9.183
27 15.227697723 193.136.9.183
15.247511454 10.0.2.15
29 15.228129653 10.0.2.15
29 15.228129653 10.0.2.15
30 15.228506058 193.136.9.183
31 15.247511540 193.136.9.183
31 15.2475196841 10.0.2.15
33 15.617379522 193.136.9.183
32 15.290566941 10.0.2.15
33 15.617379522 193.136.9.183
34 15.617399724 193.136.9.183
35 15.6173799729 193.136.9.183
36 15.658575010 10.0.2.15
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             TCP
TELNET
                                                                                                                                                                                                                                                                                                                      193.136.9.183
                                                                                                                                                                                                                                                                                                                      10.0.2.15
193.136.9.183
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               TCP
TELNET
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Wireshark-Packet 13·telnet.pcapng

> Frame 13: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface enp0s3, id 0

> Ethernet II, Src: PcsCompu_dl:8b:d0 (08:00:27:dl:8b:d0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 193.136.9.183

> Transmission Control Protocol, Src Port: 58928, Dst Port: 23, Seq: 28, Ack: 1, Len: 4

Source Port: 58928

Destination Port: 23

[Stream index: 0]

[TCP Segment Len: 4]

Sequence Number: 28 (relative sequence number)

Sequence Number (raw): 3108726961

[Next Sequence Number (raw): 3108726961

[Next Sequence Number: 1 (relative ack number)

Acknowledgment number (raw): 115328002

0101 ... = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Mindow: 64240

[Calculated window size: 64240]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0xd76c [unverified]

[Checksum: 8xd76c [unverified]

Urgent Pointer: 0

> [SEQ/ACK analysis]

| Timestamps]

| TCP payload (4 bytes)

Telnet

■ Wireshark · Packet 13 · telnet.pcapng

                                                                                                                                                                                                                                                                                                                 10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.136.9.183
10.0.2.15
10.136.9.183
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               TCP
TELNET
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               TCP
TELNET
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               TCP
TELNET
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             TCP
TELNET
TCP
TELNET
TCP
TELNET
TCP
TELNET
TCP
TELNET
TCP
TELNET
TCP
TELNET
```

Figura 2: Telnet

No.	Time	Source	Destination	Protocol	Length Info
	1 0.000000000	10.0.2.15	192.168.1.1	DNS	86 Standard query 0x268d A cc2021.ddns.net OPT
	2 0.000322862	10.0.2.15	192.168.1.1	DNS	86 Standard query 0x7fda AAAA cc2021.ddns.net OPT
	3 0.007920147	192.168.1.1	10.0.2.15	DNS	86 Standard query response 0x7fda AAAA cc2021.ddns.net OPT
	4 0.049535143	192.168.1.1	10.0.2.15	DNS	359 Standard query response 0x268d A cc2021.ddns.net A 193.136.9.183 NS nf4.no-ip.com NS nf1.no-ip.com
	5 0.050125741	10.0.2.15	193.136.9.183	TCP	74 58788 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4142624843 TSecr=0 WS=128
	6 0.070745821	193.136.9.183	10.0.2.15	TCP	60 21 → 58788 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
	7 0.070835184	10.0.2.15	193.136.9.183	TCP	54 58788 → 21 [ACK] Seq=1 Ack=1 Win=64240 Len=0
	8 0.109625933	193.136.9.183	10.0.2.15	FTP	74 Response: 220 (vsFTPd 2.3.5)
	9 0.109646294	10.0.2.15	193.136.9.183	TCP	54 58788 → 21 [ACK] Seq=1 Ack=21 Win=64220 Len=0
	10 1.950492932	10.0.2.15	193.136.9.183	FTP	63 Request: USER cc
	11 1.950868011	193.136.9.183	10.0.2.15	TCP	60 21 → 58788 [ACK] Seq=21 Ack=10 Win=65535 Len=0
	12 1.971303687	193.136.9.183	10.0.2.15	FTP	88 Response: 331 Please specify the password.
	13 1.971319025	10.0.2.15	193.136.9.183	TCP	54 58788 → 21 [ACK] Seq=10 Ack=55 Win=64186 Len=0
	14 2.431221973	10.0.2.15	157.131.143.13	TCP	■ Wireshark - Packet 8 - ftp.pcapng
	15 2.431916075	157.131.143.13	10.0.2.15	TCP	The state of the s
	16 2.601954977	157.131.143.13	10.0.2.15	TCP	> Ethernet II. Src: RealtekU 12:35:02 (52:54:00:12:35:02), Dst: PcsCompu d1:8b:d0 (08:00:27:d1:8b:d0)
	17 2.601973795	10.0.2.15	157.131.143.13	TCP	> Internet Protocol Version 4, Src: 193.136.9.183, Dst: 10.0.2.15
	18 2.601955231	157.131.143.13	10.0.2.15	TCP	Transmission Control Protocol, Src Port: 21, Dst Port: 58788, Seq: 1, Ack: 1, Len: 20
	19 2.602030383	10.0.2.15	157.131.143.13	TCP	Source Port: 21
	20 2.602500351	157.131.143.13	10.0.2.15	TCP	Destination Port: 58788
	21 5.368972911	10.0.2.15	193.136.9.183	FTP	[Stream index: 0]
	22 5.369311059	193.136.9.183	10.0.2.15	TCP	[TCP Segment Len: 20]
	23 5.467483743	193.136.9.183	10.0.2.15	FTP	Sequence Number: 1 (relative sequence number)
	24 5.467508716	10.0.2.15	193.136.9.183	TCP	Sequence Number (raw): 78912002
	25 5.469224687	10.0.2.15	193.136.9.183	FTP	[Next Sequence Number: 21 (relative sequence number)]
	26 5.469617406	193.136.9.183	10.0.2.15	TCP	Acknowledgment Number: 1 (relative ack number)
	27 5.488097516	193.136.9.183	10.0.2.15	FTP	Acknowledgment number (raw): 42479950
L	28 5.488119081	10.0.2.15	193.136.9.183	TCP	0101 = Header Length: 20 bytes (5)
					> Flags: 0x018 (PSH, ACK)
					Window: 65535
					[Calculated window size: 65535]
					[Window size scaling factor: -2 (no window scaling used)]
					Checksum: 0x4215 [unverified]
					[Checksum Status: Unverified]
					Urgent Pointer: 0
					> [SEO/ACK analysis]
					> [Timestamps]
					TCP payload (20 bytes)
					> File Transfer Protocol (FTP)
- 1					

Figura 3: FTP

No.	Time	Source	Destination	Protocol	Length Info
	1 0.000000000	10.0.2.15	192.168.1.1	DNS	86 Standard query 0xfe43 A cc2021.ddns.net OPT
	2 0.000375471	10.0.2.15	192.168.1.1	DNS	86 Standard query 0xacfd AAAA cc2021.ddns.net OPT
	3 0.016745643	192.168.1.1	10.0.2.15	DNS	146 Standard query response 0xacfd AAAA cc2021.ddns.net SOA nf1.no-ip.com OPT
	4 0.055234742	192.168.1.1	10.0.2.15	DNS	359 Standard query response 0xfe43 A cc2021.ddns.net A 193.136.9.183 NS nf2.no-ip.com NS nf3.no-ip.co
Г	5 0.055909101	10.0.2.15	193.136.9.183	TFTP	86 Read Request, File: file1, Transfer type: octet, tsize=0, blksize=512, timeout=6
	6 4.694101037	10.0.2.15	13.225.242.80	TCP	54 39342 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
	7 4.694486231	13.225.242.80	10.0.2.15	TCP	60 [TCP ACKed unseen segment] 443 → 39342 [ACK] Seq=1 Ack=2 Win=65535 Len=0
	8 4.959105880	10.0.2.15	13.225.242.34	TCP	54 36386 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
	9 4.959359056	10.0.2.15	13.225.242.80	TCP	54 39346 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
	10 4.959405844	10.0.2.15	13.225.242.80	TCP	54 39344 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
	11 4.959449209	10.0.2.15	13.225.242.80	TCP	54 39348 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
	12 4.959494238	10.0.2.15	13.225.242.80	TCP	54 39350 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
	13 4.959537321	10.0.2.15	13.225.242.80	TCP	54 39352 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
	14 4.959624598	13.225.242.34	10.0.2.15	TCP	60 [TCP ACKed unseen segment] 443 → 36386 [ACK] Seq=1 Ack=2 Win=65535 Len=0
		13.225.242.80	10.0.2.15	TCP	60 [TCP ACKed unseen segment] 443 → 39346 [ACK] Seq=1 Ack=2 Win=65535 Len=0
	16 4.959624728	13.225.242.80	10.0.2.15	TCP	60[TCP ACKed unseen segment] 443 → 39344 [ACK] Seq=1 Ack=2 Win=65535 Len=0
		13.225.242.80	10.0.2.15	TCP	60 [TCP ACKed unseen segment] 443 → 39348 [ACK] Seq=1 Ack=2 Win=65535 Len=0
	18 4.959624779	13.225.242.80	10.0.2.15	TCP	60 [TCP ACKed unseen segment] 443 → 39350 [ACK] Seq=1 Ack=2 Win=65535 Len=0
	19 4.959908043	13.225.242.80	10.0.2.15		60 [TCP ACKed unseen segment] 443 → 39352 [ACK] Seq=1 Ack=2 Win=65535 Len=0
	20 5.205301365	10.0.2.15	13.225.242.34	TCP	54 36396 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
	21 5.205360568	10.0.2.15	13.225.242.34	TCP	54 36394 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
	22 5.205362191	10.0.2.15	13.225.242.34	TCP	Wireshark - Packet 5 - tftp.pcapng
	23 5.205362555	10.0.2.15	13.225.242.34	TCP	Wilder Guerry
	24 5.205362883	10.0.2.15	13.225.242.34	TCP	> Frame 5: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface enp0s3, id 0
			10.0.2.15	TCP	> Ethernet II. Src: PcsCompu d1:8b:d0 (08:00:27:d1:8b:d0). Dst: RealtekU 12:35:02 (52:54:00:12:35:02)
			10.0.2.15	TCP	> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 193.136.9.183
			10.0.2.15	TCP	V User Datagram Protocol, Src Port: 53852, Dst Port: 69
	28 5.205557540		10.0.2.15	TCP	Source Port: 53852
	29 5.205557567	13.225.242.34	10.0.2.15	TCP	Destination Port: 69
	30 7.292692428	10.0.2.15	193.136.9.183	TFTP	Length: 52
	31 14.306717183	10.0.2.15	193.136.9.183	TFTP	Checksum: 0xd793 [unverified]
	32 14.934302641	10.0.2.15	13.225.242.80	TCP	[Checksum Status: Unverified]
	33 14.934603305	13.225.242.80	10.0.2.15	TCP	[Stream index: 2]
	34 15.189707642	10.0.2.15		TCP	> [Timestamps]
	35 15.190005102	10.0.2.15	13.225.242.80	TCP	UDP payload (44 bytes)
	36 15.190059643	10.0.2.15	13.225.242.80	TCP	> Trivial File Transfer Protocol
	37 45 400405055	40 0 0 45			/ II IVIAI   IIC   I Alisici Fiotocoi

Figura 4: TFTP

No.	Time	Source	Destination	Protocol	Length Info
	1 0.0000000000	10.0.2.15	13.225.242.68	TCP	54 36700 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
	2 0.000459208	13.225.242.68	10.0.2.15	TCP	60 [TCP ACKed unseen segment] 443 → 36700 [ACK] Seq=1 Ack=2 Win=65535 Len=0
	3 4.708202499	10.0.2.15	35.244.181.201	TLSv1.2	100 Application Data
	4 4.708826958	35.244.181.201	10.0.2.15	TCP	60 443 → 38730 [ACK] Seq=1 Ack=47 Win=65535 Len=0
	5 4.725858075	10.0.2.15	192.168.1.1	DNS	86 Standard query 0x7cd9 AAAA marco.uminho.pt OPT
	6 4.730908728	35.244.181.201	10.0.2.15	TLSv1.2	100 Application Data
	7 4.730908983	192.168.1.1	10.0.2.15	DNS	86 Standard query response 0x7cd9 AAAA marco.uminho.pt OPT
г	8 4.731376385	10.0.2.15	193.136.9.240	TCP	74 58072 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2608126961 TSecr=0 WS=128
	9 4.772128711	10.0.2.15	35.244.181.201	TCP	54 38730 → 443 [ACK] Seq=47 Ack=47 Win=62780 Len=0
	10 5.762445560	10.0.2.15	193.136.9.240	TCP	74 [TCP Retransmission] 58072 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2608127992
	11 6.125880638	193.136.9.240	10.0.2.15	TCP	60 80 → 58072 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
	12 6.125959503	10.0.2.15	193.136.9.240	TCP	54 58072 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
	13 6.126136849	10.0.2.15	193.136.9.240	HTTP	215 GET /disciplinas/CC-MIEI HTTP/1.1
	14 6.126525146	193.136.9.240	10.0.2.15	TCP	Ave. 1 1 2 1 42 1
	15 7.168291813	10.0.2.15	93.184.220.29	TCP	✓ Wireshark - Packet 13 · wget_marco.pcapng
	16 7.169167424	93.184.220.29	10.0.2.15	TCP	
4	17 7.590921765	193.136.9.240	10.0.2.15	HTTP	> Frame 13: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface enp0s3, id 0
	18 7.590947995	10.0.2.15	193.136.9.240	TCP	> Ethernet II, Src: PcsCompu_d1:8b:d0 (08:00:27:d1:8b:d0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
	19 7.594813888	10.0.2.15	193.136.9.240	HTTP	> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 193.136.9.240
L	20 7.595334842	193.136.9.240	10.0.2.15	TCP	▼ Transmission Control Protocol, Src Port: 58072, Dst Port: 80, Seq: 1, Ack: 1, Len: 161
					Source Port: 58072  Destination Port: 80  [Stream index: 2]  [TCP Segment Len: 161]  Sequence Number: 1 (relative sequence number)  Sequence Number: 1346818286  [Next Sequence Number: 162 (relative sequence number)]  Acknowledgment Number: 1 (relative ack number)  Acknowledgment number (raw): 39680002  0101 = Header Length: 20 bytes (5)  Flags: 0x018 (PSH, ACK)  Window: 64240  [Calculated window size: 64240]  [Window size scaling factor: -2 (no window scaling used)]  Checksum: 0xd842 [unverified]  [Checksum Status: Unverified]  Urgent Pointer: 0  [SEQ/ACK analysis]  T(P payload (161 bytes)  **Hypurtext Transfer Protocol**

Figura 5: Browser/HTTP

Figura 6: nslookup

```
Length Info

86 Standard query 0xaf85 AAAA cc2021.ddns.net OPT

86 Standard query response 0xaf85 AAAA cc2021.ddns.net OPT

73 34980 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM=1 TSval=4143114761 TSecr=0 WS=128

60 22 → 34988 [SYN] ACK] Seq=0 Ack=1 Win=65236 Len=0 MSS=1460

54 34980 → 22 [ACK] Seq=1 Ack=1 Win=64240 Len=0

95 Client: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1)

60 22 → 34988 [ACK] Seq=1 Ack=42 Win=6535 Len=0

95 Server: Protocol (SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.4)

54 34980 → 22 [ACK] Seq=42 Ack=42 Win=654199 Len=0

1566 Client: Key Exchange Init

Wireschark - Packet 8 - ssh.pcapng
   Time
1 0.000000000
2 0.003182055
3 0.003620994
4 0.024913805
5 0.024990087
6 0.025383014
7 0.025702255
8 0.076341754
9 0.076356722
10 0.076949052
11 0.077304443
12 0.077304443
13 0.0998617333
                                                                                                                                                                                           10.0.2.15
192.168.1.1
10.0.2.15
193.136.9.183
                                                                                                                                                                                                                                                                                                                                                                                                                                 192.168.1.1
10.0.2.15
193.136.9.183
10.0.2.15
                                                                                                                                                                                        193.136.9.183
10.0.2.15
10.0.2.15
193.136.9.183
193.136.9.183
10.0.2.15
10.0.2.15
193.136.9.183
193.136.9.183
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           TCP
SSHv2
                                                                                                                                                                                                                                                                                                                                                                                                                                       193.136.9.183
193.136.9.183
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        TCP
                                                                                                                                                                                                                                                                                                                                                                                                                                 10.0.2.15
10.0.2.15
193.136.9.183
193.136.9.183
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        SSHv2
TCP
SSHv2
TCP
TCP
                                                                                                                                                                                                                                                                                                                                                                                                                                    10.0.2.15
10.0.2.15
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  Wireshark-Packet 8-sshpcapng

➤ Frame 8: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface enp0s3, id 0

➤ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_d1:8b:d0 (08:00:27:d1:8b:d0)

➤ Internet Protocol Version 4, Src: 193.136.9.183, Dst: 10.0.2.15

➤ Transmission Control Protocol, Src Port: 22, Dst Port: 34980, Seq: 1, Ack: 42, Len: 41

➤ Source Port: 22

■ Destination Port: 34980

[Stream index: 0]

[TCP Segment Len: 41]

➤ Sequence Number: 41 (relative sequence number)

➤ Sequence Number: 42 (relative sequence number)

Acknowledgment Number: 42 (relative ack number)

Acknowledgment number (raw): 3981942264

0101 ... = Header Length: 20 bytes (5)

➤ Flags: 0x018 (PSH, ACK)

Window: 65535

[Calculated window size: 65535]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x35ca [unverified]

Urgent Pointer: 0

➤ [SEO/ACK analysis]

➤ [Timestamps]

TCP payload (41 bytes)

➤ SSH Protocol

Protocol: SSH-2.0-OpenSSH_5.9p1 Debian-Subuntu1.4

[Direction: server-to-client]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        SSHv2
TCP
SSHv2
         13 0.098617339
14 0.098634449
                                                                                                                                                                                              193.136.9.183
                                                                                                                                                                                                                                                                                                                                                                                                                                 10.0.2.15
                                                                                                                                                                                              10.0.2.15
10.0.2.15
                                                                                                                                                                                                                                                                                                                                                                                                                                 193.136.9.183
193.136.9.183
      15 0.099090043
16 0.099402922
17 0.137444449
                                                                                                                                                                                  193.136.9.183

193.136.9.183

10.0.2.15

193.136.9.183

10.0.2.15

193.136.9.183

193.136.9.183

193.136.9.183

193.136.9.183

193.136.9.183

10.0.2.15

193.136.9.183

193.136.9.183

193.136.9.183

193.136.9.183

193.136.9.183

193.136.9.183

193.136.9.183
                                                                                                                                                                                                                                                                                                                                                                                                                                 10.0.2.15
10.0.2.15
193.136.9.183
193.136.9.183
         18 0.137459770
19 0.138381113
19 0. 138381113
20 0. 138884045
21 0. 139516015
22 0. 140007273
23 0. 158988658
24 0. 159330453
25 0. 159603235
26 11. 662981353
27 11. 764390254
28 18. 012755897
29 18. 013236552
30 18. 09242179
31 18. 092442179
32 18. 092482977
31 18. 298344530
36 18. 298346530
36 18. 298346530
36 18. 298374639
                                                                                                                                                                                                                                                                                                                                                                                                                              10.0.2.15
193.136.9.183
10.0.2.15
10.0.2.15
10.0.2.15
193.136.9.183
10.0.2.15
193.136.9.183
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
10.0.2.15
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           TCP
SSHv2
```

Figura 7: SSH

```
Source
10.0.2.15
10.0.2.15
10.0.2.15
10.4.16.88.20
104.16.18.94
104.16.18.94
104.16.18.94
10.0.2.15
104.16.88.20
10.0.2.15
104.2.15
162.159.130.234
10.0.2.15
192.168.1.1
10.0.2.15
193.136.9.240
162.159.130.234
10.0.2.15
                                                                                                                                                                                                                                                                                                                                                                                                   Length Info
93 Application Data
Time
1 0.0000000000
2 0.00010997
3 0.003362592
4 0.003362932
5 0.013800334
6 0.013817646
7 0.016478521
9 0.936657545
10 0.937575040
11 1.225704798
12 1.239050435
13 1.239753910
16 1.27316248
15 1.27316248
                                                                                                                                                                                                                                                                                                                    TLSv1.2
TLSv1.2
TCP
TCP
TLSv1.2
                                                                                                                                                                                                      104.16.88.20

104.16.18.94

10.0.2.15

10.0.2.15

10.0.2.15

10.0.2.15

10.0.2.15

104.16.18.94

10.0.2.15

104.16.18.94

10.0.2.15

104.16.88.20

102.159.130.234

10.0.2.15

192.168.1.1

10.0.2.15

193.136.9.240

10.0.2.15

100.0.2.15

100.0.2.15

100.0.2.15

100.0.2.15

100.0.2.15

100.0.2.15

100.0.2.15

100.0.2.15

100.0.2.15

100.0.2.15

100.0.2.15

100.0.2.15

100.0.2.15
                                                                                                                                                                                                       104.16.88.20
                                                                                                                                                                                                                                                                                                                                                                                                                93 Application Data
93 Application Data
93 Application Data
60 443 + 41218 [ACK] Seq=1 Ack=40 Win=65535 Len=0
60 443 + 462246 [ACK] Seq=1 Ack=40 Win=65535 Len=0
93 Application Data
54 46246 + 443 [ACK] Seq=40 Ack=40 Win=62780 Len=0
93 Application Data
54 41218 + 443 [ACK] Seq=40 Ack=40 Win=63540 Len=0
97 Application Data
60 443 + 49768 [ACK] Seq=40 Ack=40 Win=65535 Len=0
86 Standard query expanse 0x4cab AAAA marco.uminho.pt OPT
98 Echo (ping) request id=0x0002, seq=1/256, ttl=54 (reply in 14)
98 Echo (ping) reply id=0x0002, seq=1/256, ttl=52 (request in 13)
87 Application Data
54 49768 + 443 [ACK] Seq=44 Ack=34 Win=65535 Len=0
98 Echo (ping) request id=0x0002, seq=1/256, ttl=52 (request in 13)
98 Echo (ping) reply id=0x0002, seq=2/512, ttl=64 (reply in 18)
98 Echo (ping) reply id=0x0002, seq=2/512, ttl=52 (request in 17)
98 Echo (ping) reply id=0x0002, seq=3/768, ttl=64 (reply in 22)
                                                                                                                                                                                                                                                                                                                      TLSV1.2
TCP
TLSv1.2
TCP
TLSv1.2
TCP
DNS
DNS
ICMP
ICMP
                                                                                                                                                                                                                                                                                                                    TLSv1.2
TCP
ICMP
ICMP
ICMP
ICMP
ICMP
ICSv1.2
TCP
ICMP
ICMP
ICMP
ICMP
 16 1.273165248
17 2.234211708
18 2.254428788
19 3.242289167
20 3.252127139
21 3.252144880

✓ Wireshark · Packet 13 · ping.pcapng

                                                                                                                                                                                                          162.159.130.234
                                                                                          10.0.2.15
                                                                                          193.136.9.240
  22 3.262983180
                                                                                                                                                                                                         10.0.2.15
193.136.9.240
                                                                                                                                                                                                                                                                                                                                                                                                             Frame 13: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0 Ethernet II, Src: PcsCompu_d1:8b:d0 (08:00:27:d1:8b:d0), Dst: RealtekU_12:35:02 (52:54:00:12:35:02) Internet Protocol Version 4, Src: 10.0.2.15, Dst: 193.136.9.240 Internet Control Message Protocol
  23 4.252876009
                                                                                          10.0.2.15
                                                                                        10.0.2.15
193.136.9.240
162.159.130.234
                                                                                                                                                                                                       10.0.2.15
10.0.2.15
162.159.130.234
193.136.9.240
    24 4.273421845
 25 4.595711620
26 4.595726803
27 5.255721178
                                                                                                                                                                                                                                                                                                                      TLSv1.2
                                                                                       10.0.2.15
```

Figura 8: Ping

2. Uma representação num diagrama temporal das transferências da file1 por FTP e TFTP respetivamente. Se for caso disso, identifique as fases de estabelecimento de conexão, transferência de dados e fim de conexão. Identifica também claramente os tipos de segmentos trocados e os números de sequência usados quer nos dados como nas confirmações.

(Nota: a transferência por FTP envolve mais que uma conexão FTP, nomeadamente uma de controlo [ftp] e outra de dados [ftp-data]. Faça o diagrama apenas para a conexão de transferência de dados do ficheiro mais pequeno)

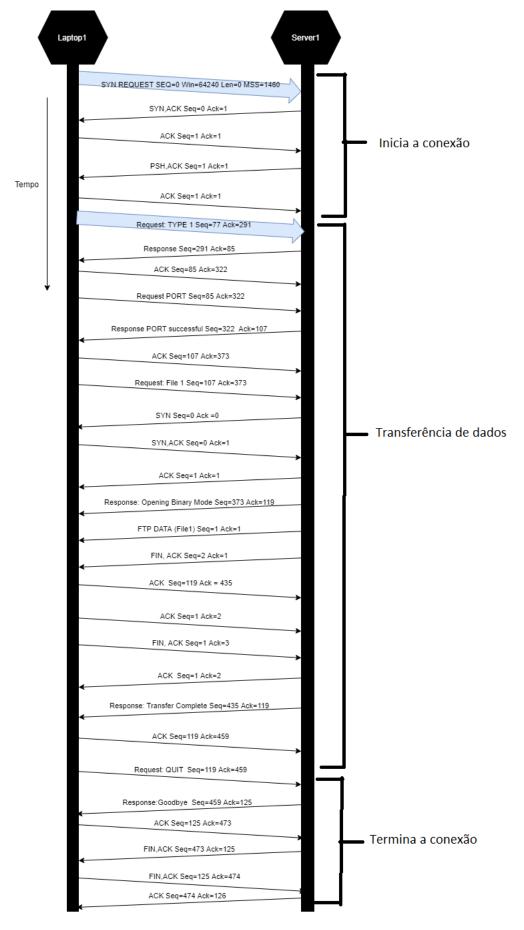


Figura 9: Diagrama Temporal da transferência do ficheiro file1 por FTP (Protocolo TCP)

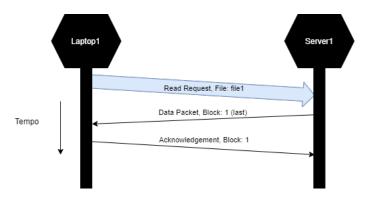


Figura 10: Diagrama Temporal da transferência do ficheiro file1 por TFTP (Protocolo UDP)

3. Com base nas experiências realizadas, distinga e compare sucintamente as quatro aplicações de transferência de ficheiros que usou nos seguintes pontos a (i) uso da camada de transporte; (ii) eficiência na transferência; (iii) complexidade; (iv) segurança;

#### FTP

A aplicação *FTP* (*File Transfer Protocol*) faz recurso ao protocolo de transporte *TCP* (por norma nas portas 20 e 21) para efetuar as trocas de informação. Desta forma antes que sejam efectuadas transferências é primeiro estabelecida uma conexão na porta 21, onde são adicionalmente confirmadas as credenciais do utilizador e transmitidos os seus pedidos.

Para se realizar uma transmissão de dados o cliente da aplicação começa por fazer um pedido de controlo FTP para indicar ao servidor que pretende fazer uma transferência de um dado tipo de dados. Posteriormente o servidor envia uma mensagem de resposta ao cliente que prossegue com um pedido para abrir um segundo canal de transmissão TCP (na porta 20) para efetuar a transferência. Caso tenha disponibilidade o servidor responde ao cliente com a porta do novo canal que transmite por fim o identificador do ficheiro que quer transferir. De seguida o servidor inicia a transmissão do ficheiro, começando por enviar no segundo canal uma mensagem a indicar tipo de dados especificado na fase de request seguido de uma série de mensagens FTP-DATA contendo o ficheiro em si. Por fim quando a transmissão acaba, o transmissor termina a conexão no segundo canal TCP e assim que esta operação for confirmada envia uma mensagem a confirmar o fim da transmissão.

Desta forma, podemos concluir que este método de transferência é bastante complexo e permite uma transmissão diversificada de dados e que devido a usar um segundo canal o utilizador pode continuar a trabalhar no sistema remoto enquanto ocorrem trocas de ficheiros. Porém ao implicar uma grande troca de mensagens entre o servidor e cliente (quer pelas mensagens de controlo *TCP* quer pela abertura de um novo canal *TCP*), é muito ineficiente pode provocar atrasos significativos durante as transferências principalmente se as conexões estiverem sujeitas a perdas de informação onde seja necessário fazer várias retransmissões.Por outro lado, como nenhuma da informação é encriptada ou protegida os intervenientes estão sujeitos a ataques de *middleman* que pode ser bastante perigoso visto que existem várias trocas de credenciais durante a conexão.

#### SFTP

O protocolo *SFTP* (*SSH File Transfer Protocol*) é um protocolo de transferência de ficheiros seguro que se baseia no protocolo de aplicação *SSH* e no protocolo de transporte *TCP* (por norma com recurso à porta 22).

Baseia-se bastante no processo do protocolo *FTP*, no entanto devido ao uso de encriptação *SSH*, há uma maior segurança comparativamente ao mesmo. Por outro lado a troca de informação é feita apenas em um canal que diminui bastante a quantidade de mensagens envolvidas tornando-o mais eficiente do que o *FTP* tendo a consequência de impedir que o utilizador aceda ao sistema remoto durante transferências. Outra melhoria existente é o facto de o cliente *ssh* armazenar alguma informação sobre o servidor, não sendo assim necessário comunicar com o servidor para todas as primitivas do sistema. Um exemplo disto é o comando *pwd* (*Print Working Directory*), que embora no *FTP* implicava comunicação com o servidor, com *SFTP*, o cliente nunca consulta o servidor.

### TFTP

A aplicação *TFTP* (*Trivial File Transfer Protocol*) utiliza o protocolo de transporte *UDP* (por norma na porta 69) para efetuar as trocas de informação. As transferências baseadas em *TFTP* começam sempre com um pedido de leitura ou escrita que também tem a finalidade de pedir uma conexão. Assim que o servidor autorizar o pedido, a conexão fica aberta. Não utiliza nenhum mecanismo de segurança relativamente à autenticação do utilizador ou á encriptação de mensagens, pelo que se revela um protocolo pouco seguro.

Dado que utiliza o protocolo *UDP*, não existe uma grande complexidade. Quando um cliente pretende fazer uma transferência envia uma mensagem com o pedido. De seguida o servidor responde com o ficheiro que quando recebido pela aplicação do cliente envia uma mensagem de confirmação. Desta forma a maioria dos erros fecham a conexão e são sinalizados emitindo um pacote de erro, sendo que este pacote não é reconhecido nem retransmitido.

Também, devido ao *UDP*, tem uma elevada eficiência por causa de ter o overhead mais pequeno de todas estas aplicações porém não oferece uma solução viável para transferência de dados devido ás possíveis falhas.

#### HTTP (WGET)

O protocolo de aplicação HTTP (Hypertext Transfer Protocol) é utilizado para a comunicação de dados pela porta *TCP default* 80 (apesar de outras portas poderem ser configuradas para serem utilizadas). Para estabelecer uma conexão, o cliente começa por enviar um pedido de conexão (SYN) ao Servidor que, por sua vez, responde com um Acknowledge (SYN, ACK). Por último, o cliente responde com um acknowledge, confirmando que a conexão foi estabelecida (processo TCP 3-Way Handshake).

Para pedir uma transferência de um ficheiro ao servidor, o cliente começa por lhe enviar um pedido (GET) do mesmo. De seguida, o servidor responde com um acknowledge e depois envia os dados do ficheiro pretendido.

Para terminar a conexão, o cliente envia essa intenção ao servidor utilizando para o efeito uma mensagem FIN, ACK, ao qual o servidor responde com um Acknowledge a confirmar o término da conexão.

Concluindo, o protocolo HTTP é uma solução simples para a transferência de ficheiros uma vez que o consegue fazer com um número baixo de mensagens, porém não é a solução mais segura visto que e o facto de ser necessário abrir uma nova conexão *TCP* por ficheiro transmito pode atrasos significativos caso se esteja a transmitir grandes volumes de ficheiros. Estes problemas no entanto foram resolvidos no protocolo *HTTPS* (*Hypertext Transfer Protocol Secure*), que não só adiciona uma camada de encriptação SSL/TLS sobre os dados mas também permite a transferência de vários ficheiros pela mesma conexão *TCP*.

4. As características das ligações de rede têm uma enorme influência nos níveis de Transporte e de Aplicação. Discuta, relacionando a resposta com as experiências realizadas, as influências das situações de perda ou duplicação de pacotes IP no desempenho global de Aplicações fiáveis (se possível, relacionando com alguns dos mecanismos de transporte envolvidos).

**Nota**: Para responder a esta pergunta deve em primeiro lugar efetuar as transferências pedidas no enunciado, quer a partir do sistema Laptop1 na LAN4, quer do sistema Corvo a LAN3, pois só assim poderá ligar esta resposta à prática. Na topologia, o sistema Corvo tem conetividade ao Backbone através de um link que funciona com perdas, atrasos e duplicações, que é o link entre o swicth SwitchLan3 e o router Router4. Nos testes podem mesmo ajustar esses parâmetros.

Os protocolos de transporte TCP e UDP são os mais usados e o processo de escolha de qual deles se usa depende do objetivo pretendido.

O TCP é um protocolo fiável que utiliza mecanismos de deteção de erros e de recuperação, para garantir que caso haja um erro no transporte, os pacotes continuam a ser enviados na ordem correta e sem erros. No entanto, dados todos estes mecanismos existentes no protocolo *TCP* este está dependente da qualidade da rede. Caso a rede seja de fraca qualidade, há uma muito maior probabilidade de perda de pacotes, o que fará com que haja um tráfego muito maior devido à necessidade de reenviarem esses pacotes. Podemos observar um pedido de retransmissão resultante de um erro de envio na captura realizada para a transferência de ficheiro usando *FTP* a partir do computador Corvo (fig. 11).

Por sua vez o protocolo UDP é quase uma antítese do protocolo *TCP*, já que é um protocolo não fiável e não se preocupa em reenviar pacotes que tenham sido corrompidos, deixando essa tarefa para as aplicações em si. Esta menor complexidade faz com que este protocolo seja muito favorável para redes com menor qualidade ou de *streaming*, visto que, ao contrário do protocolo fiável *TCP*, não provoca a sobrecarga da rede. Devido a esta falta de viabilidade podem aparecer situações de perda de dados como é o caso da transmissão *TFTP* da figura 12, em que falta um pacote *TFTP* de *Acknowledgment* que pode ter sido causada pela perda do pacote de *Data* ou pela perda do *Acknowledgment* entre a *Backbone* da topologia e a interface *Corvo*.

No	. Time	Source	Destination	Protocol	Length Info
	1 0.000000000	10.1.1.254	224.0.0.5	OSPF	78 Hello Packet
	2 0.217046209	fe80::200:ff:feaa:10	ff02::5	OSPF	90 Hello Packet
	3 2.000787179	10.1.1.254	224.0.0.5	OSPF	78 Hello Packet
	4 4.003822737	10.1.1.254	224.0.0.5	OSPF	78 Hello Packet
	5 6.006772151	10.1.1.254	224.0.0.5	OSPF	78 Hello Packet
	6 6.634553418	10.3.3.3	10.1.1.1	TCP	74 54970 + 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=921306737 TSecr=0 WS=128
- 11	7 6.634814705	10.1.1.1	10.3.3.3	TCP	74 21 → 54970 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=481498743 TSecr=921306737 WS=128
	8 6.641588562	10.3.3.3	10.1.1.1	TCP	66 54970 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=921306748 TSecr=481498743
+	9 6.643608302	10.1.1.1	10.3.3.3	FTP	86 Response: 220 (vsFTPd 3.0.3)
	10 6.863563692	10.1.1.1	10.3.3.3		86 [TCP Retransmission] 21 → 54970 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=20 TSval=481498971 TSecr=921306748
	11 6.870998635	10.3.3.3	10.1.1.1	TCP	78 54970 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=921306977 TSecr=481498971 SLE=1 SRE=21
	12 8.006725772	10.1.1.254	224.0.0.5	OSPF	78 Hello Packet
	13 10.009427475	10.1.1.254	224.0.0.5	OSPF	78 Hello Packet
	14 10.253791748	fe80::200:ff:feaa:10	ff02::5	OSPF	90 Hello Packet
	15 11.825604983	00:00:00_aa:00:10	00:00:00_aa:00:14	ARP	42 Who has 10.1.1.1? Tell 10.1.1.254

Figura 11: Exemplo de um pedido de retransmissão (Protocolo TCP)

No.		Time	Source	Destination	Protocol	Length	Info
	166	116.165164202	10.1.1.254	224.0.0.5	OSPF	78	Hello Packet
	167	118.171352745	10.1.1.254	224.0.0.5	OSPF	78	Hello Packet
	168	119.095806027	10.3.3.3	10.1.1.1	TFTP	56	Read Request, File: file1, Transfer type: octet
	169	119.098671612	10.1.1.1	10.3.3.3	TFTP	47	Data Packet, Block: 1 (last)
	170	119.591156377	00:00:00_aa:00:10	00:00:00_aa:00:14	ARP	42	Who has 10.1.1.1? Tell 10.1.1.254
	171	119.591484299	00:00:00_aa:00:14	00:00:00_aa:00:10	ARP	42	10.1.1.1 is at 00:00:00:aa:00:14
	172	120.171623761	10.1.1.254	224.0.0.5	OSPF	78	Hello Packet
	173	121.968557479	fe80::200:ff:feaa:10	ff02::5	OSPF	90	Hello Packet

Figura 12: Exemplo de um pacote TFTP de Acknowledgment em falta (Protocolo UCP)

### Conclusão

Com este trabalho pudemos colocar em prática os conhecimentos adquiridos nas aulas teóricas da Unidade Curricular, fazendo com que tenhamos consolidado muito melhor as temáticas lecionadas, nomeadamente os diferentes tipos de protocolos de transporte e de aplicação. Para observarmos estes protocolos, utilizamos as ferramentas *CORE* e *Wireshark*.

Na verdade, ao observar a captura de tráfego no *Wireshark* torna bastante evidente as diferenças entre os vários protocolos estudados nesta fase. Ser capaz de ver diretamente o impacto dos diferentes protocolos no tempo de resposta do pedido de transferência de um ficheiro e verificar a retransmissão de pacotes a ocorrer no protocolo de transporte *TCP* quando ocorrem erros, ajudou-nos a entender a necessidade de existirem vários protocolos de aplicação tais como *FTP*, *SFTP*, *TFTP* e *HTTP* e protocolos de transporte como *UDP* e *TCP*.