



Universidade do Minho
Escola de Engenharia

COMUNICAÇÃO POR COMPUTADORES

RELATÓRIO

TP1 - Protocolos da camada de transporte

Realizado por:

(Grupo 4)

Luís Fernandes a88539

Ricardo Silva a93195

Rui Alves a93252

PARTE 1:

QUESTÃO 1: “De que forma as perdas e duplicações de pacotes afetaram o desempenho das aplicações? Que camada lidou com as perdas e duplicações: transporte ou aplicação? Responda com base nas experiências feitas e nos resultados observados”.

RESPOSTA:

A camada de transporte foi a responsável pelas perdas e duplicações. O TCP e UDP são os protocolos de transporte utilizados.

As perdas e duplicações de pacotes afetam o desempenho das aplicações dependendo do protocolo de transporte utilizado, o protocolo **TCP**, diferente do **UDP**, é voltado à conexão e tem como garantia a integridade e ordem de todos os dados de forma segura, já protocolo **UDP** é rápido e não precisa de conexão, pode enviar “datagramas” de uma máquina à outra, mas sem garantia de que os dados enviados chegarão intactos e na ordem correta.

196	215.630465857	10.2.2.1	10.4.4.1	TCP	66	21 → 43922 [ACK] Seq=21 Ack=14 Win=65280 Len=0 TSval=37825366...
197	215.630469090	10.2.2.1	10.4.4.1	TCP	78	[TCP Dup ACK 196#1] 21 → 43922 [ACK] Seq=21 Ack=14 Win=65280
198	215.630578653	10.2.2.1	10.4.4.1	FTP	100	Response: 331 Please specify the password.
199	215.635670340	10.4.4.1	10.2.2.1	TCP	66	43922 → 21 [ACK] Seq=14 Ack=55 Win=64256 Len=0 TSval=24693970...
200	216.043673859	10.2.2.254	224.0.0.5	OSPF	78	Hello Packet
201	216.295901600	fe80::200:ff:feaa:10	ff02::5	OSPF	90	Hello Packet
202	217.381091500	fe80::10ec:b0ff:fe5...	ff02::2	ICMPv6	70	Router Solicitation from 36:3f:72:be:90:6d
203	218.043706158	10.2.2.254	224.0.0.5	OSPF	78	Hello Packet
204	220.043823739	10.2.2.254	224.0.0.5	OSPF	78	Hello Packet
205	222.045035041	10.2.2.254	224.0.0.5	OSPF	78	Hello Packet
206	224.046131268	10.2.2.254	224.0.0.5	OSPF	78	Hello Packet
207	224.375249008	10.4.4.1	10.2.2.1	FTP	96	Request: PASS a93252@alunos.uminho.pt
208	224.376260181	10.4.4.1	10.2.2.1	TCP	66	[TCP Retransmission] 43922 → 21 [PSH, ACK] Seq=14 Ack=55 Win=...
209	224.376142735	10.2.2.1	10.4.4.1	TCP	66	21 → 43922 [ACK] Seq=55 Ack=44 Win=65280 Len=0 TSval=37825454...
210	224.376147770	10.2.2.1	10.4.4.1	TCP	78	[TCP Dup ACK 209#1] 21 → 43922 [ACK] Seq=55 Ack=44 Win=65280
211	226.047016506	10.2.2.254	224.0.0.5	OSPF	78	Hello Packet
212	226.303136264	fe80::200:ff:feaa:10	ff02::5	OSPF	90	Hello Packet

Imagem 1: Exemplo de retransmissão e duplicados tratados pelo protocolo TCP (conexão FTP)

QUESTÃO 2: “Obtenha a partir do wireshark, ou desenhe manualmente, um diagrama temporal para a transferência de file1 por FTP. Foque-se apenas na transferência de dados [ftp-data] e não na conexão de controlo, pois o FTP usa mais que uma conexão em simultâneo. Identifique, se aplicável, as fases de início de conexão, transferência de dados e fim de conexão. Identifique também os tipos de segmentos trocados e os números de sequência usados quer nos dados como nas confirmações”.

RESPOSTA:

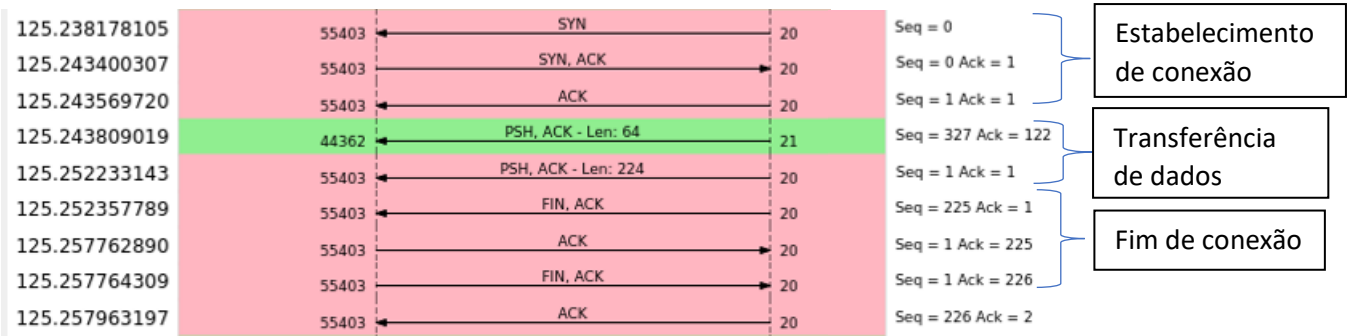


Imagem 2: Diagrama temporal de uma conexão FTP.

QUESTÃO 3: “Obtenha a partir do wireshark, ou desenhe manualmente, um diagrama temporal para a transferência de file1 por TFTP. Identifique, se aplicável, as fases de início de conexão, transferência de dados e fim de conexão. Identifique também os tipos de segmentos trocados e os números de sequência usados quer nos dados como nas confirmações”.

RESPOSTA:

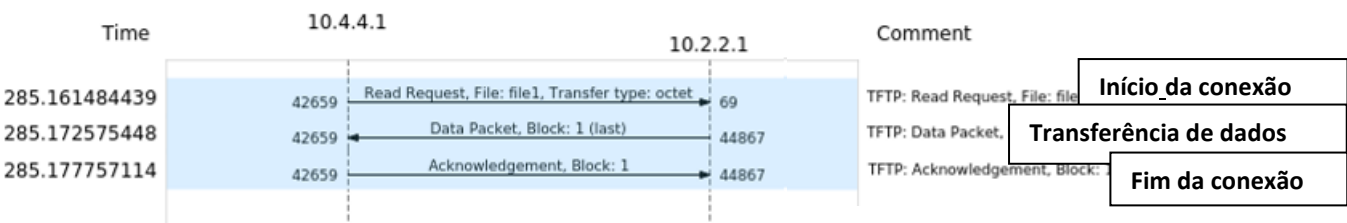


Imagem 3: Diagrama temporal de uma conexão TFTP.

QUESTÃO 4: *“Compare sucintamente as quatro aplicações de transferência de ficheiros que usou nos seguintes pontos (i) uso da camada de transporte; (ii) eficiência; (iii) complexidade; (iv) segurança”.*

RESPOSTA:

Pela análise da transferência por **SFTP**, é uma aplicação segura uma vez que pede autenticação por parte do utilizador, utiliza SSH que é um protocolo de rede bastante complexo, utiliza também o TCP como protocolo de transporte.

Em **FTP** apresenta um elevado overhead que compromete a sua eficiência, utiliza também o TCP como protocolo de transporte, e não apresenta nenhuma segurança adicional, sendo uma aplicação de baixa complexidade.

Na **TFTP** é um serviço pouco fiável de transferência de ficheiros uma vez que utiliza o UDP como protocolo de transporte, não oferece nenhuma segurança, mas devido ao seu baixo overhead é um serviço bastante mais eficiente.

No **HTTP** qualquer utilizador pode aceder ao conteúdo transferido e por isso é de baixa segurança, o HTTP foca em apresentar a informação, não se preocupando com a maneira de como essa informação é transmitida, isto quer dizer que o HTTP pode ser invadido e alterado. Utiliza também o TCP como protocolo de transporte.

PARTE 2:

Comando usado: (aplicação)	Protocolo de Aplicação (se aplicável)	Protocolo de transporte (se aplicável)	Porta de atendimento (se aplicável)	Overhead de transporte em bytes (se aplicável)
ping	-	-	-	-
tracert	-	UDP	33589	8
telnet	TELNET	TCP	23	20
ftp	FTP	TCP	21	20
Tftp	TFTP	UDP	69	8
http(browser)	HTTP	TCP	80	20
Nslookup	DNS	UDP	53	8
Ssh	SSHv2	TCP	22	20

No.	Time	Source	Destination	Protocol	Length	Info
80	55.587535329	10.0.2.15	193.136.19.254	UDP	74	44990 - 33494 Len=32
81	55.587558624	10.0.2.15	193.136.19.254	UDP	74	59979 - 33495 Len=32
82	55.587568321	10.0.2.15	193.136.19.254	UDP	74	48166 - 33495 Len=32
83	55.587577667	10.0.2.15	193.136.19.254	UDP	74	55271 - 33497 Len=32
84	56.386389195	10.0.2.15	193.136.19.254	UDP	74	57551 - 33498 Len=32
85	56.386413865	10.0.2.15	193.136.19.254	UDP	74	53876 - 33499 Len=32
86	56.386455900	10.0.2.15	193.136.19.254	UDP	74	59019 - 33500 Len=32
87	60.512002072	10.0.2.15	193.136.19.254	UDP	74	51321 - 33501 Len=32
88	60.512194391	10.0.2.15	193.136.19.254	UDP	74	49313 - 33502 Len=32
89	60.512249695	10.0.2.15	193.136.19.254	UDP	74	45137 - 33503 Len=32
90	60.512282827	10.0.2.15	193.136.19.254	UDP	74	58477 - 33504 Len=32
91	60.512499854	10.0.2.15	193.136.19.254	UDP	74	59880 - 33505 Len=32
92	60.512592439	10.0.2.15	193.136.19.254	UDP	74	43517 - 33506 Len=32
93	60.512649005	10.0.2.15	193.136.19.254	UDP	74	41608 - 33507 Len=32
94	60.512860462	10.0.2.15	193.136.19.254	UDP	74	39748 - 33508 Len=32
95	60.512950479	10.0.2.15	193.136.19.254	UDP	74	52136 - 33509 Len=32
96	60.513115044	10.0.2.15	193.136.19.254	UDP	74	34251 - 33510 Len=32
97	60.513292717	10.0.2.15	193.136.19.254	UDP	74	60822 - 33511 Len=32
98	60.513349203	10.0.2.15	193.136.19.254	UDP	74	44159 - 33512 Len=32
99	60.513388752	10.0.2.15	193.136.19.254	UDP	74	43500 - 33513 Len=32
100	61.381842591	10.0.2.15	193.136.19.254	UDP	74	43762 - 33514 Len=32
101	61.381946315	10.0.2.15	193.136.19.254	UDP	74	33255 - 33515 Len=32
102	61.381992854	10.0.2.15	193.136.19.254	UDP	74	35034 - 33516 Len=32
103	65.517648822	10.0.2.15	193.136.19.254	UDP	74	39197 - 33517 Len=32
104	65.517672565	10.0.2.15	193.136.19.254	UDP	74	47666 - 33518 Len=32
105	65.517684591	10.0.2.15	193.136.19.254	UDP	74	51152 - 33519 Len=32
106	65.517694763	10.0.2.15	193.136.19.254	UDP	74	33534 - 33520 Len=32
107	65.517706148	10.0.2.15	193.136.19.254	UDP	74	51794 - 33521 Len=32
108	65.517717484	10.0.2.15	193.136.19.254	UDP	74	58059 - 33522 Len=32
110 65.517730074 10.0.2.15 193.136.19.254 UDP 74 33568 - 33523 Len=32						
110 117.758349749 From: 1521:1260::f11:ff02::fb To: 1521:1260::f11:ff02::fb MONS 160 Standard query 0x0000 PTR _ftp._tcp.local, "Q" question PTR						
111 117.758398244 10.0.2.15 224.0.0.251 MONS 160 Standard query 0x0000 PTR _ftp._tcp.local, "Q" question PTR						
* Frame 108: 74 bytes on wire (592 bits): 74 bytes captured (592 bits) on interface enp0s3, id 0						
* Ethernet II, Src: PcsCompu, 9c:03:08:00:02:01, Dst: RealtekU, 12:35:02:52:54:00:12:35:02						
* Internet Protocol Version 4, Src: 10.0.2.15, Dst: 193.136.19.254						
0200 = Version: 4						
... 0001 = Header length: 20 bytes (5)						
* Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 60						
Identification: 0x38a1 (6305)						
* Flags: 0x0000						
Fragment offset: 0						
Time to live: 30						
Protocol: UDP (17)						
Header checksum: 0xa27b [validation disabled]						
[Header checksum status: Unverified]						
Source: 10.0.2.15						
Destination: 193.136.19.254						
* User Datagram Protocol, Src Port: 33589, Dst Port: 33523						
0000 0000 0000 0000 0000 0000 0000 0000						
Destination Port: 33523						
Length: 40						
Checksum: 0x61ce [unverified]						
0020 13 f6 02 f3 90 28 e1 ce 40 41 42 43 44 45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00						

Figura X: ROUTE

Figura X: TRACEROUTE

No.	Time	Source	Destination	Protocol	Length	Info
106	57.801112711	193.136.9.183	193.136.9.183	TELNET	50	Telnet Data ...
107	57.801148855	193.136.9.183	193.136.9.183	TCP	54	57576 - 23 [ACK] Seq=151 Ack=166 Win=64076 Len=0
108	57.182439627	193.136.9.183	193.136.9.183	TELNET	55	Telnet Data ...
109	57.182489936	193.136.9.183	193.136.9.183	TCP	60	23 - 57576 [ACK] Seq=166 Ack=152 Win=65535 Len=0
110	57.252518808	193.136.9.183	193.136.9.183	TELNET	60	Telnet Data ...
111	57.252562088	193.136.9.183	193.136.9.183	TCP	54	57576 - 23 [ACK] Seq=152 Ack=167 Win=64076 Len=0
112	57.531167487	193.136.9.183	193.136.9.183	TELNET	50	Telnet Data ...
113	57.531549415	193.136.9.183	193.136.9.183	TCP	60	23 - 57576 [ACK] Seq=167 Ack=154 Win=65535 Len=0
114	57.551189933	193.136.9.183	193.136.9.183	TELNET	66	Telnet Data ...
115	57.551210829	193.136.9.183	193.136.9.183	TCP	54	57576 - 23 [ACK] Seq=154 Ack=179 Win=64076 Len=0
116	59.389556665	193.136.9.183	193.136.9.183	TELNET	55	Telnet Data ...
117	59.389288854	193.136.9.183	193.136.9.183	TCP	60	23 - 57576 [ACK] Seq=170 Ack=195 Win=65535 Len=0
118	59.53066534	193.136.9.183	193.136.9.183	TELNET	55	Telnet Data ...
119	59.53143359	193.136.9.183	193.136.9.183	TCP	60	23 - 57576 [ACK] Seq=179 Ack=196 Win=65535 Len=0
120	60.053889350	193.136.9.183	193.136.9.183	TELNET	55	Telnet Data ...
121	60.054213503	193.136.9.183	193.136.9.183	TCP	60	23 - 57576 [ACK] Seq=179 Ack=197 Win=65535 Len=0
122	60.204886880	193.136.9.183	193.136.9.183	TELNET	55	Telnet Data ...
123	60.205519336	193.136.9.183	193.136.9.183	TCP	60	23 - 57576 [ACK] Seq=179 Ack=198 Win=65535 Len=0
124	60.328158864	193.136.9.183	193.136.9.183	TELNET	55	Telnet Data ...
125	60.328475070	193.136.9.183	193.136.9.183	TCP	60	23 - 57576 [ACK] Seq=179 Ack=199 Win=65535 Len=0
126	60.478365884	193.136.9.183	193.136.9.183	TELNET	55	Telnet Data ...
127	60.478639870	193.136.9.183	193.136.9.183	TCP	60	23 - 57576 [ACK] Seq=179 Ack=199 Win=65535 Len=0
128	60.648661186	193.136.9.183	193.136.9.183	TELNET	56	Telnet Data ...
129	60.648999885	193.136.9.183	193.136.9.183	TCP	60	23 - 57576 [ACK] Seq=179 Ack=162 Win=65535 Len=0
130	61.124912439	193.136.9.183	193.136.9.183	TELNET	69	Telnet Data ...
131	61.124974162	193.136.9.183	193.136.9.183	TCP	54	57576 - 23 [ACK] Seq=162 Ack=181 Win=64076 Len=0
132	61.181095480	193.136.9.183	193.136.9.183	TELNET	122	Telnet Data ...
133	61.181199881	193.136.9.183	193.136.9.183	TCP	54	57576 - 23 [ACK] Seq=162 Ack=249 Win=64076 Len=0
134	61.377889620	193.136.9.183	193.136.9.183	TELNET	117	Telnet Data ...
135	61.377129055	193.136.9.183	193.136.9.183	TCP	54	57576 - 23 [ACK] Seq=162 Ack=312 Win=64076 Len=0
136	61.435217120	193.136.9.183	193.136.9.183	TCP	54	57576 - 23 [ACK] Seq=162 Ack=453 Win=64076 Len=0
* Frame 136: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface enp8b3, id 0 * Ethernet II, Src: RealtekU12:35:82 (52:54:00:12:35:82), Dst: PcsCompu_06:03:48 (08:00:27:06:03:48) * Internet Protocol Version 4, Src: 193.136.9.183, Dst: 193.136.9.183 * ... * Version: 4 * ... * Header Length: 20 bytes (5) * Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) * Total Length: 181 * Identification: 0x037b (891) * Flags: 0x0000 * Fragment Offset: 0 * Time to live: 64 * Protocol: TCP (6) * Header checksum: 0xd97fa (validation disabled) * [Header checksum status: Unverified] * Source: 193.136.9.183 * Destination: 193.136.9.183 * Transmission Control Protocol, Src Port: 23, Dst Port: 57576, Seq: 312, Ack: 362, Len: 141 * Source Port: 23 * Destination Port: 57576 * [Stream index: 8] * [TCP Segment Len: 141]						

Figura Y: TELNET

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	193.136.9.183	193.136.9.183	DNS	86	Standard query 8d7be1 A cc2022.dns.net OPT
2	0.000075367	193.136.9.183	193.136.9.183	DNS	86	Standard query response 8d7be1 A cc2022.dns.net OPT
3	0.041313824	193.136.9.183	193.136.9.183	DNS	259	Standard query response 8d7be1 A cc2022.dns.net A 193.136.9.183
4	0.041784279	193.136.9.183	193.136.9.183	DNS	145	Standard query response 8d7be1 A cc2022.dns.net SOA nft.m...
5	0.048280717	193.136.9.183	193.136.9.183	TCP	74	46330 - 21 [ACK] Seq=78 Ack=23 Win=65535 Len=0
6	0.060000760	193.136.9.183	193.136.9.183	TCP	60	21 - 46330 [ACK] Seq=21 Ack=78 Win=65535 Len=0
7	0.060091773	193.136.9.183	193.136.9.183	TCP	54	46330 - 21 [ACK] Seq=1 Ack=21 Win=64220 Len=0
8	0.106015360	193.136.9.183	193.136.9.183	FTP	74	Response: 220 (vsftpd 2.3.5)
9	0.106040825	193.136.9.183	193.136.9.183	TCP	54	46330 - 21 [ACK] Seq=1 Ack=21 Win=64220 Len=0
10	3.482295873	193.136.9.183	193.136.9.183	FTP	63	Request: USER cc
11	3.492778290	193.136.9.183	193.136.9.183	TCP	60	21 - 46330 [ACK] Seq=21 Ack=19 Win=65535 Len=0
12	3.101837577	193.136.9.183	193.136.9.183	FTP	88	Response: 331 Please specify the password.
13	3.181858361	193.136.9.183	193.136.9.183	TCP	54	46330 - 21 [ACK] Seq=19 Ack=55 Win=64188 Len=0
14	6.812051742	193.136.9.183	193.136.9.183	FTP	67	Request: PASS cc2022
15	6.819259290	193.136.9.183	193.136.9.183	TCP	60	21 - 46330 [ACK] Seq=55 Ack=23 Win=65535 Len=0
16	6.911408890	193.136.9.183	193.136.9.183	FTP	77	Response: 230 Login successful.
17	6.912821686	193.136.9.183	193.136.9.183	TCP	54	46330 - 21 [ACK] Seq=23 Ack=78 Win=64163 Len=0
18	6.912633360	193.136.9.183	193.136.9.183	FTP	60	Request: SYST
19	6.912612188	193.136.9.183	193.136.9.183	TCP	60	21 - 46330 [ACK] Seq=78 Ack=29 Win=65535 Len=0
20	6.912612188	193.136.9.183	193.136.9.183	TCP	54	46330 - 21 [ACK] Seq=29 Ack=78 Win=64144 Len=0
21	6.933724730	193.136.9.183	193.136.9.183	TCP	54	46330 - 21 [ACK] Seq=29 Ack=78 Win=64144 Len=0
* Frame 20: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface enp8b3, id 0 * Ethernet II, Src: RealtekU12:35:82 (52:54:00:12:35:82), Dst: PcsCompu_06:03:48 (08:00:27:06:03:48) * Internet Protocol Version 4, Src: 193.136.9.183, Dst: 193.136.9.183 * ... * Version: 4 * ... * Header Length: 20 bytes (5) * Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) * Total Length: 59 * Identification: 0x831a (794) * Flags: 0x0000 * Fragment Offset: 0 * Time to live: 64 * Protocol: TCP (6) * Header checksum: 0xa905 (validation disabled) * [Header checksum status: Unverified] * Source: 193.136.9.183 * Destination: 193.136.9.183 * Transmission Control Protocol, Src Port: 21, Dst Port: 46330, Seq: 78, Ack: 29, Len: 19 * Source Port: 21 * Destination Port: 46330 * [Stream index: 8] * [TCP Segment Len: 19]						

Figura W: FTP

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000001538	10.0.2.15	192.168.1.1	DNS	86	Standard query 0x1195 AAAA cc2022.ddns.net OPT
3	0.050788822	192.168.1.1	10.0.2.15	DNS	359	Standard query response 0x9986 A cc2022.ddns.net A 193.136.9...
4	0.062229046	192.168.1.1	10.0.2.15	DNS	148	Standard query response 0x1195 AAAA cc2022.ddns.net SOA mfi.s...
5	0.062540911	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
6	7.275808888	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
7	12.359808234	PciCompu.06:03:48	RealtekU.12:35:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
8	12.359530766	RealtekU.12:35:02	PciCompu.06:03:48	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
9	14.282702876	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
10	15.202778936	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
11	18.303171750	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
12	19.312564921	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
13	142.322964830	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
14	49.331380795	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
15	56.338847124	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
16	63.348331662	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
17	68.422828579	PciCompu.06:03:48	RealtekU.12:35:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
18	68.422828579	RealtekU.12:35:02	PciCompu.06:03:48	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
19	70.354838874	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
20	77.364131798	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
21	84.375377099	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
22	91.384980139	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
23	98.392326356	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
24	105.401651234	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
25	112.418217922	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
26	119.420756129	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
27	124.488024024	PciCompu.06:03:48	RealtekU.12:35:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
28	124.487485041	RealtekU.12:35:02	PciCompu.06:03:48	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
29	128.429610720	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
30	133.445504652	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
31	140.455895508	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
32	147.464051767	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
33	154.471527211	10.0.2.15	193.136.9.183	TFTP	86	Read Request, File: file1, Transfer type: octet, tsiz=0, bla...
* Ethernet II, Src: PciCompu.06:03:48 (08:00:27:06:03:48), 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						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
* Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 72						
Identification: 0x37ef (14319)						
* Flags: 0x0000, Don't fragment						
Fragment offset: 0						
Time to live: 64						
Protocol: UDP (17)						
Header checksum: 0x2b68 [validation disabled]						
[Header checksum status: Unverified]						
Source: 10.0.2.15						
Destination: 193.136.9.183						
* User Datagram Protocol, Src Port: 55184, Dst Port: 69						
Source Port: 55184						
Destination Port: 69						
Length: 52						
Checksum: 0xd793 [unverified]						
[Checksum Status: Unverified]						
0020 00 b7 00 45 00 34 d7 93 00 01 66 69 6c 65 E-4 -- file						

Figura Z: TFTP

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.168.1.1	DNS	86	Standard query 0x8f31 A marco.uninho.pt OPT
2	0.000306374	10.0.2.15	192.168.1.1	DNS	86	Standard query 0x8f31 A marco.uninho.pt A 193.136.9...
3	0.015702328	192.168.1.1	10.0.2.15	DNS	358	Standard query response 0x8f31 A marco.uninho.pt A 193.136.9...
4	0.025658330	192.168.1.1	10.0.2.15	DNS	148	Standard query response 0x8f31 AAAA marco.uninho.pt SOA dms.c...
5	0.026225847	10.0.2.15	193.136.9.240	TCP	74	43824 -> 80 [RST] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	0.054577245	193.136.9.240	10.0.2.15	TCP	60	80 -> 43824 [RST] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
7	0.054619983	10.0.2.15	193.136.9.240	TCP	54	43824 -> 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
8	0.054656899	10.0.2.15	193.136.9.240	HTTP	215	GET /disciplinas/CC-LEI/ HTTP/1.1
9	0.055296463	193.136.9.240	10.0.2.15	TCP	60	80 -> 43824 [ACK] Seq=1 Ack=162 Win=65535 Len=0
10	0.072845997	193.136.9.240	10.0.2.15	TCP	1514	80 -> 43824 [PSH, ACK] Seq=1 Ack=162 Win=65535 Len=1460 [TCP seq...
11	0.072871468	10.0.2.15	193.136.9.240	TCP	54	43824 -> 80 [ACK] Seq=162 Ack=161 Win=62780 Len=0
12	0.074405883	193.136.9.240	10.0.2.15	TCP	4434	80 -> 43824 [ACK] Seq=1461 Ack=162 Win=65535 Len=4380 [TCP seq...
13	0.074480190	10.0.2.15	193.136.9.240	TCP	54	43824 -> 80 [ACK] Seq=162 Ack=5441 Win=61320 Len=0
14	0.074758023	193.136.9.240	10.0.2.15	TCP	1514	80 -> 43824 [PSH, ACK] Seq=5441 Ack=162 Win=65535 Len=1460 [TC...
15	0.074767703	10.0.2.15	193.136.9.240	TCP	54	43824 -> 80 [ACK] Seq=162 Ack=7301 Win=61320 Len=0
16	0.075110111	193.136.9.240	10.0.2.15	HTTP	1773	HTTP/1.1 200 OK (text/css)
17	0.075110115	10.0.2.15	193.136.9.240	TCP	54	43824 -> 80 [ACK] Seq=162 Ack=9020 Win=55053 Len=0
18	0.075866267	10.0.2.15	193.136.9.240	TCP	54	43824 -> 80 [FIN, ACK] Seq=162 Ack=9020 Win=62780 Len=0
19	0.076291243	193.136.9.240	10.0.2.15	TCP	60	80 -> 43824 [ACK] Seq=9020 Ack=163 Win=65535 Len=0
20	0.092950467	193.136.9.240	10.0.2.15	TCP	60	80 -> 43824 [FIN, ACK] Seq=9020 Ack=163 Win=65535 Len=0
21	0.092987833	10.0.2.15	193.136.9.240	TCP	54	43824 -> 80 [ACK] Seq=163 Ack=9021 Win=62780 Len=0
* Frame 16: 1773 bytes on wire (14184 bits), 1773 bytes captured (14184 bits) on interface enp0s3, id 0						
* Ethernet II, Src: RealtekU.12:35:02 (52:54:00:12:35:02), Dst: PciCompu.06:03:48 (08:00:27:06:03:48)						
* Internet Protocol Version 4, Src: 193.136.9.240, Dst: 10.0.2.15						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
* Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 1759						
Identification: 0x9305 (773)						
* Flags: 0x0000						
Fragment offset: 0						
Time to live: 64						
Protocol: TCP (6)						
Header checksum: 0x9980 [validation disabled]						
[Header checksum status: Unverified]						
Source: 193.136.9.240						
Destination: 10.0.2.15						
* Transmission Control Protocol, Src Port: 80, Dst Port: 43824, Seq: 7301, Ack: 162, Len: 1719						
Source Port: 80						
Destination Port: 43824						
[Stream index: 8]						
[TCP Segment Len: 1719]						
Frame 1773 bytes on wire (14184 bits), 1773 bytes captured (14184 bits) on interface enp0s3						

Figura V: HTTP

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000	192.168.1.1	192.168.1.1	ICMP	18	Standard query 0x0000 A www.uninho.pt OPT
2	0.00054520	192.168.1.1	192.168.1.1	DNS	355	Standard query response 0x0000 A www.uninho.pt A 193.137.9.11
3	0.041329991	192.168.1.1	192.168.1.1	DNS	84	Standard query 0x6654 AAAA www.uninho.pt OPT
4	0.092771761	192.168.1.1	192.168.1.1	DNS	138	Standard query response 0x6654 AAAA www.uninho.pt SOA dns.unl
5	5.169661991	PcsCompu.06:03:48	RealtekU.12:35:02	ARP	42	Who has 192.168.1.27 Tell 192.168.1.1
6	5.16986813	RealtekU.12:35:02	PcsCompu.06:03:48	ARP	60	192.168.1.2 is at 52:54:00:12:35:02
7	5.573239640	192.168.1.1	192.168.1.1	DNS	84	Standard query 0xf499 AAAA www.uninho.pt OPT
8	5.588948261	192.168.1.1	192.168.1.1	DNS	84	Standard query response 0xf499 AAAA www.uninho.pt OPT

* Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface em03, id 0
 * Ethernet II, Src: PcsCompu.06:03:48 (08:00:27:06:03:48), Dst: RealtekU.12:35:02 (52:54:00:12:35:02)
 * Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.1
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 * Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 70
 Identification: 0x10f (6591)
 * Flags: 0x0000, Don't fragment
 Fragment offset: 0
 Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0x5330 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.1
 Destination: 192.168.1.1
 * User Datagram Protocol, Src Port: 49767, Dst Port: 53

* Destination Port: 53
 Length: 50
 Checksum: 0xcdfb [unverified]

0020 01 01 00 00 35 00 32 cd fb 06 0c 01 00 00 01 5-2

Figura U: NSLOOKUP

No.	Time	Source	Destination	Protocol	Length	Info
13	20.245248434	193.136.9.183	193.136.9.183	SSHv2	356	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New
34	20.245288668	193.136.9.183	193.136.9.183	TCP	54	57430 -> 22 [ACK] Seq=1634 Acc=1338 Win=63968 Len=0
35	22.709460626	193.136.9.183	193.136.9.183	SSHv2	70	Client: New Keys
36	22.709909966	193.136.9.183	193.136.9.183	TCP	60	22 -> 57430 [ACK] Seq=1338 Acc=1650 Win=65535 Len=0
37	22.726197614	193.136.9.183	193.136.9.183	SSHv2	94	Client: Encrypted packet (len=40)
38	22.735833320	193.136.9.183	193.136.9.183	TCP	60	22 -> 57430 [ACK] Seq=1338 Acc=1690 Win=65535 Len=0
39	23.487049299	193.136.9.183	193.136.9.183	SSHv2	94	Server: Encrypted packet (len=40)
40	23.487067888	193.136.9.183	193.136.9.183	TCP	54	57430 -> 22 [ACK] Seq=1690 Acc=1378 Win=63968 Len=0
41	23.497264444	193.136.9.183	193.136.9.183	SSHv2	118	Client: Encrypted packet (len=56)
42	23.497484866	193.136.9.183	193.136.9.183	TCP	60	22 -> 57430 [ACK] Seq=1378 Acc=1748 Win=65535 Len=0
43	36.4326095109	193.136.9.183	193.136.9.183	SSHv2	118	Server: Encrypted packet (len=56)
44	36.472944450	193.136.9.183	193.136.9.183	TCP	54	57430 -> 22 [ACK] Seq=1748 Acc=1434 Win=63968 Len=0
45	42.52179437	193.136.9.183	193.136.9.183	SSHv2	190	Client: Encrypted packet (len=196)
46	42.521688632	193.136.9.183	193.136.9.183	TCP	60	22 -> 57430 [ACK] Seq=1434 Acc=1682 Win=65535 Len=0
47	45.187658638	193.136.9.183	193.136.9.183	SSHv2	118	Server: Encrypted packet (len=56)
48	45.187622994	193.136.9.183	193.136.9.183	TCP	54	57430 -> 22 [ACK] Seq=1682 Acc=1498 Win=63968 Len=0
49	49.59594886	193.136.9.183	193.136.9.183	SSHv2	190	Client: Encrypted packet (len=196)
50	49.596076174	193.136.9.183	193.136.9.183	TCP	60	22 -> 57430 [ACK] Seq=1498 Acc=2018 Win=65535 Len=0
51	52.113982413	193.136.9.183	193.136.9.183	SSHv2	78	Server: Encrypted packet (len=24)
52	52.114084609	193.136.9.183	193.136.9.183	TCP	54	57430 -> 22 [ACK] Seq=2018 Acc=1514 Win=63968 Len=0
53	52.114204976	193.136.9.183	193.136.9.183	SSHv2	166	Client: Encrypted packet (len=112)
54	52.114522754	193.136.9.183	193.136.9.183	TCP	60	22 -> 57430 [ACK] Seq=1514 Acc=2138 Win=65535 Len=0
55	53.889727790	193.136.9.183	193.136.9.183	SSHv2	94	Server: Encrypted packet (len=40)
56	53.889746565	193.136.9.183	193.136.9.183	TCP	54	57430 -> 22 [ACK] Seq=2138 Acc=1554 Win=63968 Len=0
57	53.889592205	193.136.9.183	193.136.9.183	SSHv2	1182	Client: Encrypted packet (len=1128)
58	53.889229593	193.136.9.183	193.136.9.183	TCP	60	22 -> 57430 [ACK] Seq=1554 Acc=3258 Win=65535 Len=0
59	54.445616697	193.136.9.183	193.136.9.183	SSHv2	142	Server: Encrypted packet (len=48)
60	54.445655251	193.136.9.183	193.136.9.183	TCP	54	57430 -> 22 [ACK] Seq=3258 Acc=1642 Win=63968 Len=0
61	54.448713929	193.136.9.183	193.136.9.183	SSHv2	358	Server: Encrypted packet (len=196)
62	54.448759504	193.136.9.183	193.136.9.183	TCP	54	57430 -> 22 [ACK] Seq=3258 Acc=1938 Win=63968 Len=0
63	54.450557027	193.136.9.183	193.136.9.183	TCP	54	57430 -> 22 [ACK] Seq=1938 Acc=1978 Win=63968 Len=0
64	54.450559313	193.136.9.183	193.136.9.183	TCP	54	57430 -> 22 [ACK] Seq=1978 Acc=1978 Win=63968 Len=0

* Frame 63: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface em03, id 0
 * Ethernet II, Src: RealtekU.12:35:02 (52:54:00:12:35:02), Dst: PcsCompu.06:03:48 (08:00:27:06:03:48)
 * Internet Protocol Version 4, Src: 193.136.9.183, Dst: 192.168.1.1
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 * Differentiated Services Field: 0x40 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 80
 Identification: 0xd40f (10739)
 * Flags: 0x0000
 Fragment offset: 0
 Time to live: 64
 Protocol: TCP (6)
 Header checksum: 0x9f4b [validation disabled]
 [Header checksum status: Unverified]
 Source: 193.136.9.183
 Destination: 192.168.1.1
 * Transmission Control Protocol, Src Port: 22, Dst Port: 57430, Seq: 1938, Ack: 3258, Len: 40
 Source Port: 22
 Destination Port: 57430
 [Stream index: 0]
 [TCP Segment Len: 40]

00 00 27 06 03 48 52 54 00 12 35 02 08 00 45 80S...E

Figura L: SSH

CONCLUSÃO:

Neste projeto transferiu-se o mesmo ficheiro usando 4 serviços diferentes: SFTP, FTP, TFTP e HTTP, capturando todos os pacotes trocados durante a transferência com o Wireshark, testamos também diferentes protocolos de transporte (TCP e UDP) e analisamos as suas diferenças, aprofundando assim o nosso conhecimento nestas áreas.

Em suma, consideramos que os requisitos mínimos foram cumpridos mesmo tendo surgido várias dúvidas na realização do trabalho.