Universidade do Minho
Escola de Engenharia

Departamento de Informática

Comunicações por Computador

Trabalho Prático nº 1

Protocolos da Camada de Transporte

Ano Letivo 2020/2021

Grupo 1 - PL1

Ana Filipa Pereira A89589
Carolina Santejo A89500
Raquel Costa A89464

Conteúdo

1 Questões e Respostas

1.1 Questão 1

P: Inclua no relatório uma tabela em que identifique, para cada comando executado, qual o protocolo de aplicação, o protocolo de transporte, porta de atendimento e overheadde transporte, como ilustrado no exemplo seguinte:

R:

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	-	-	-	-
traceroute	DNS Protocol	UDP	33453	8
telnet	telnet	TCP	57548	20
ftp	ftp	TCP	21	20
Tftp	tftp	UDP	69	8
browser/http	http	TCP	34282	20
nslookup	DNS	UDP	53	8
ssh	ssh	TCP	54766	20

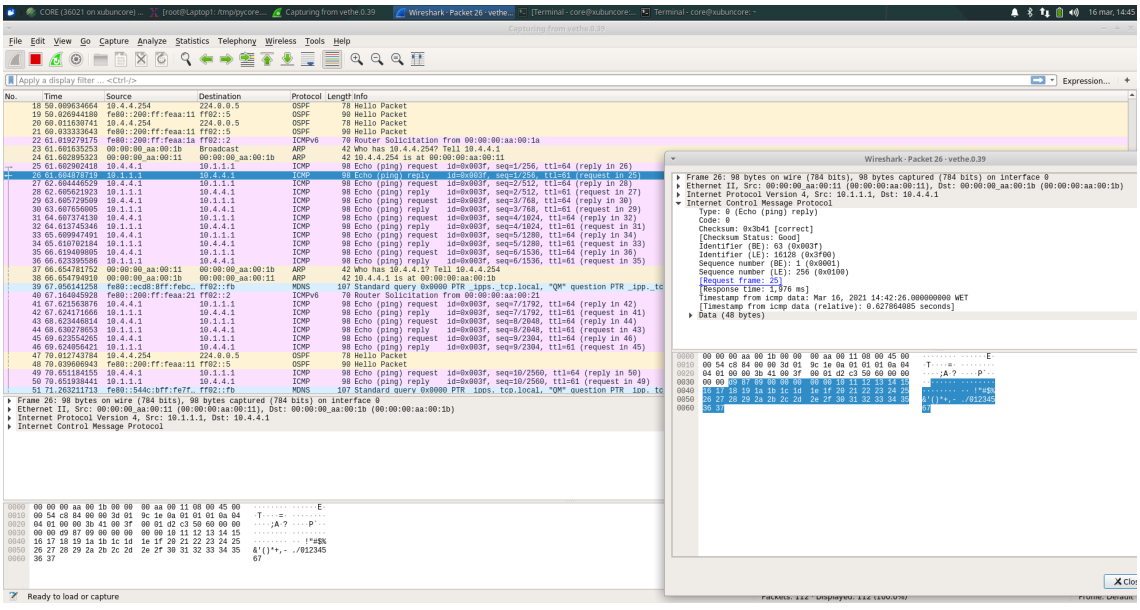


Figura 1: Ping.

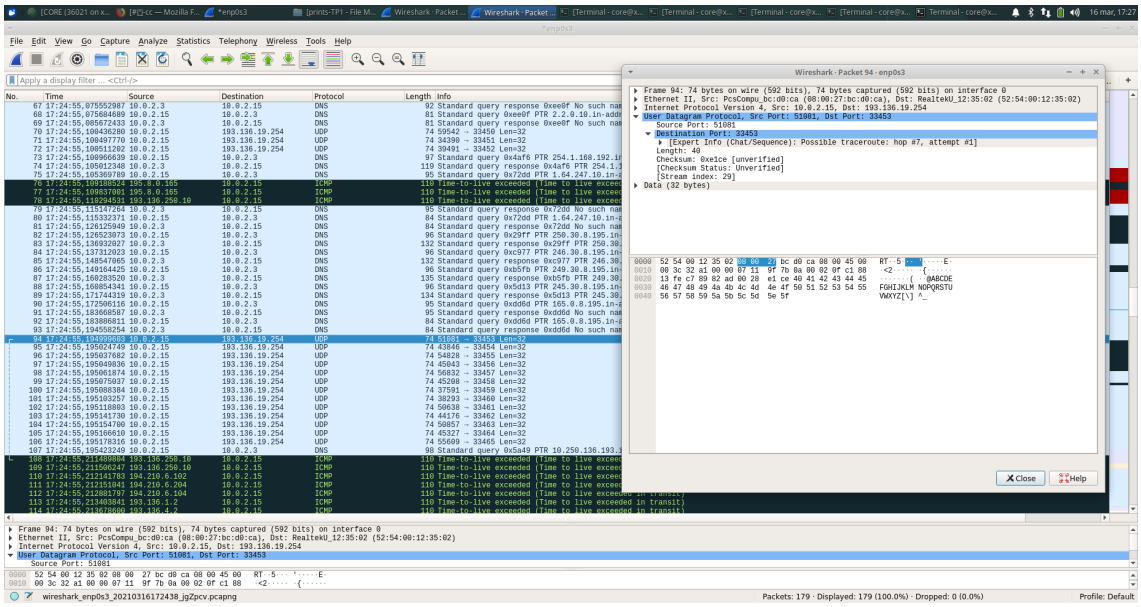


Figura 2: Traceroute.

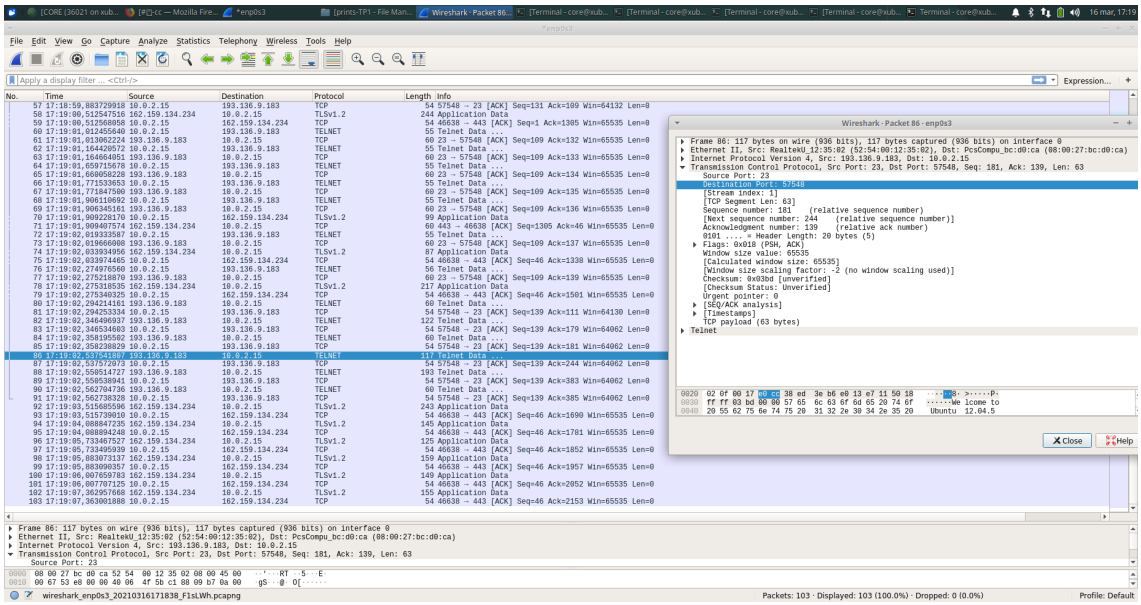


Figura 3: Telnet.

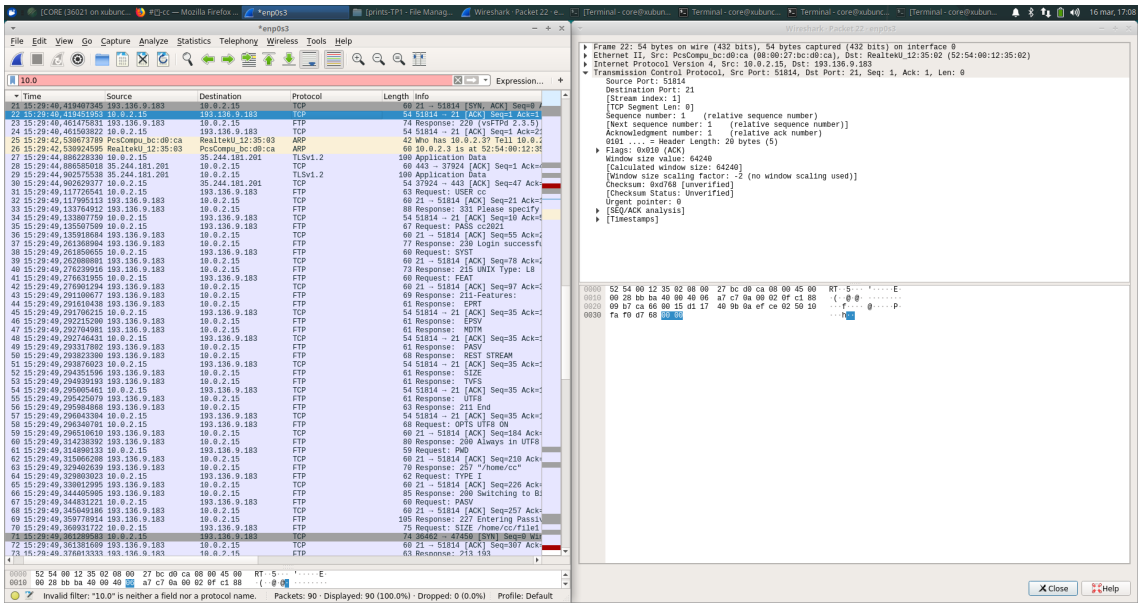


Figura 4: Ftp.

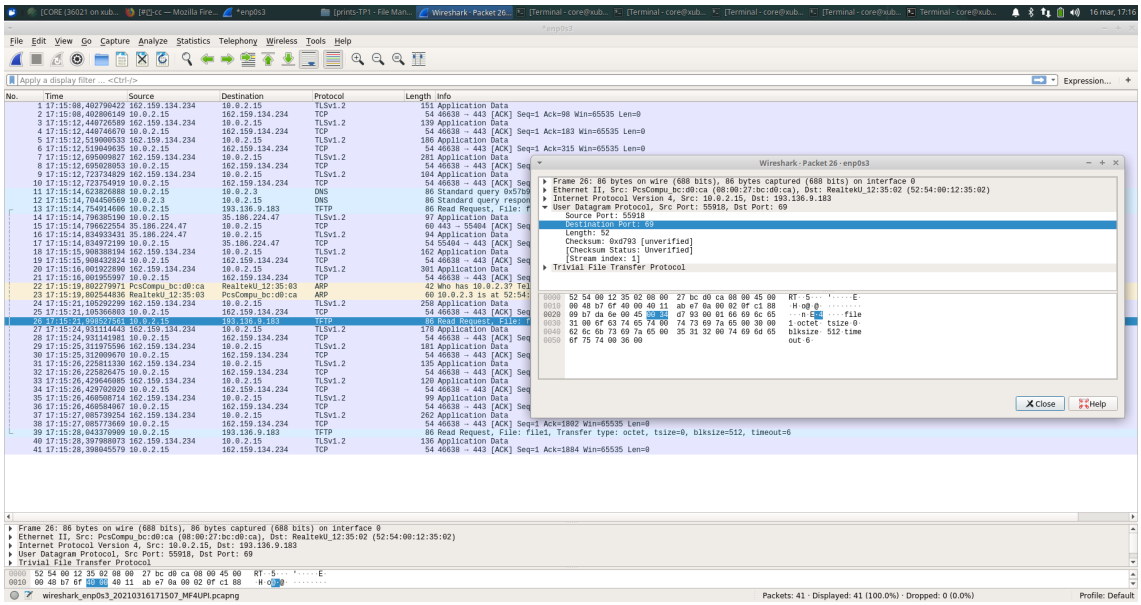


Figura 5: Tftp.

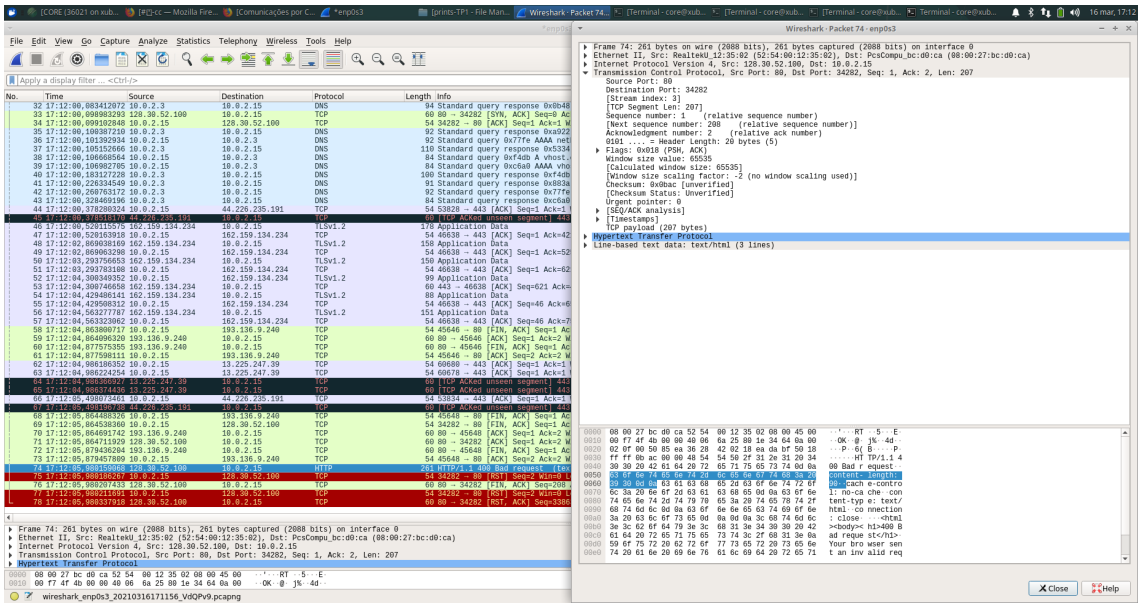


Figura 6: Browser/http.

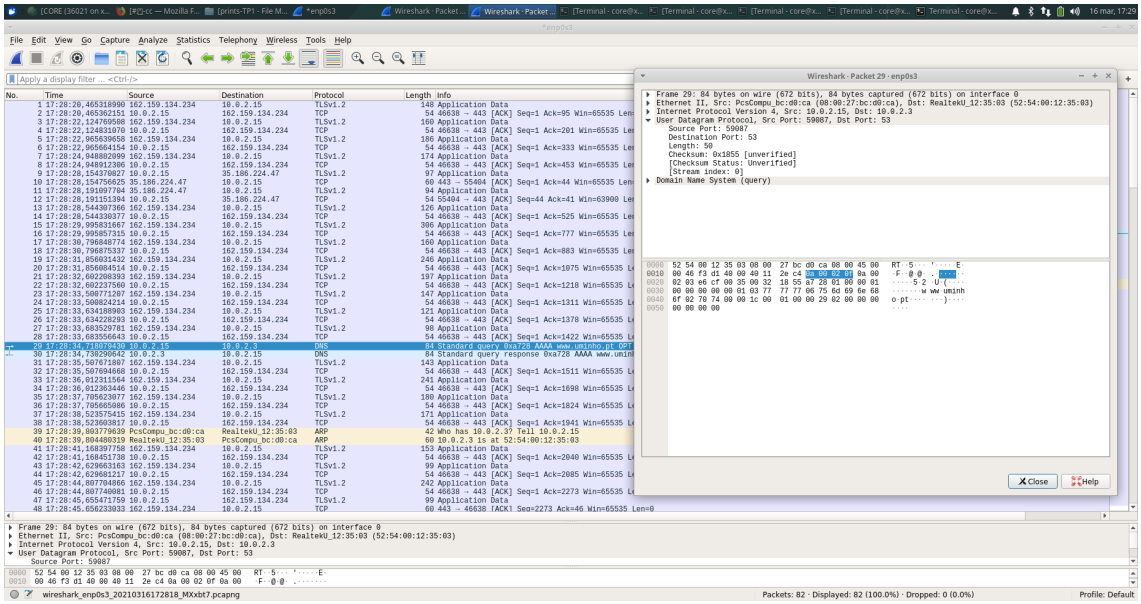


Figura 7: Nslookup.

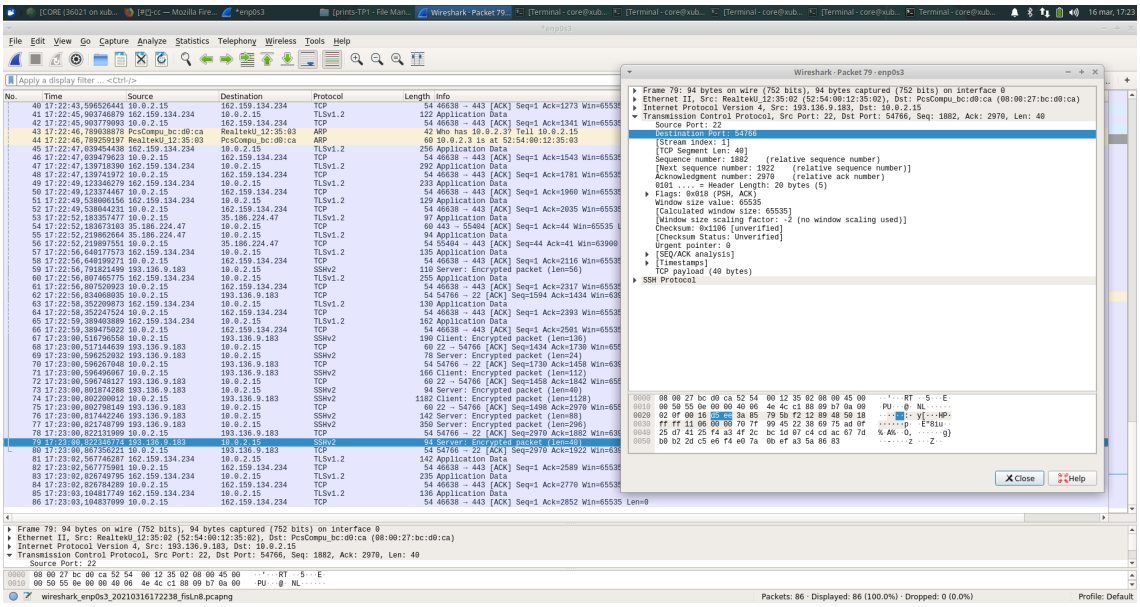
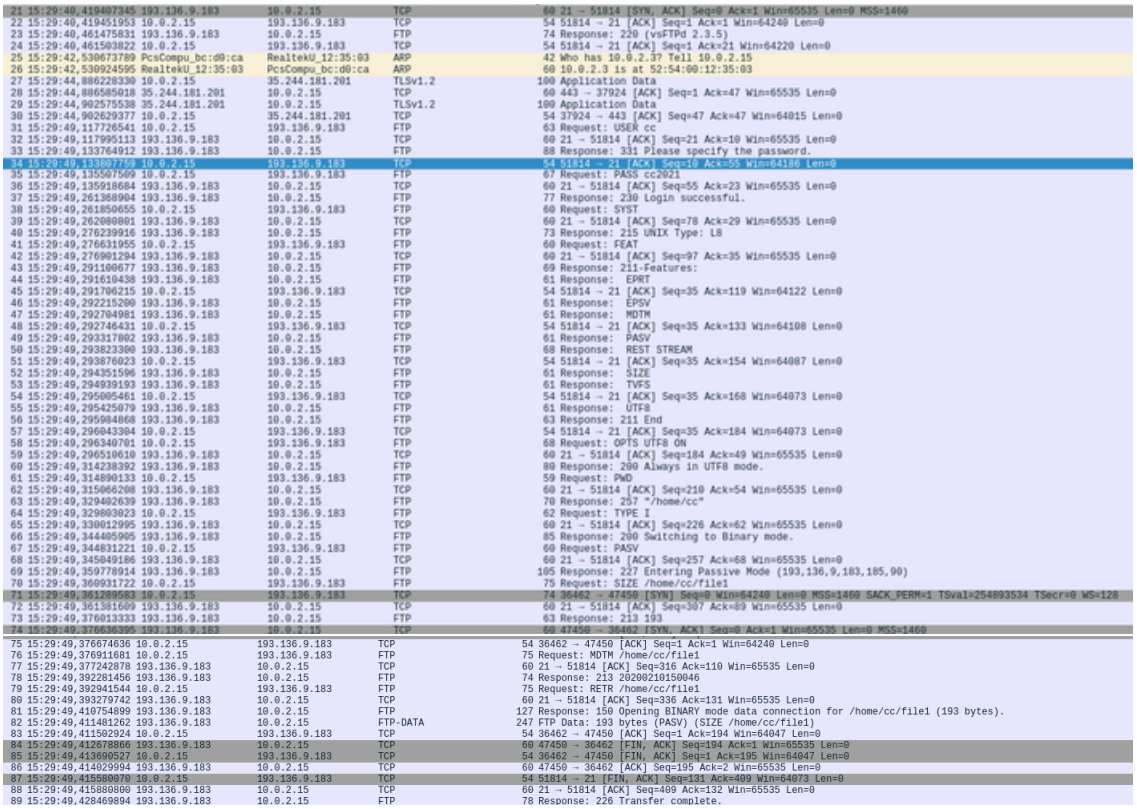


Figura 8: Ssh.

1.2 Questão 2

P: Uma representação num diagrama temporal das transferências da file1por FTPe TFTPrespetivamente. Se for caso disso, identifiqueas 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 envolvemais 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)

R:



21	15:29:40,419407345	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
22	15:29:40,419451953	10.0.2.15	193.136.9.183	TCP	54 51814 → 21 [ACK] Seq=1 Ack=1 Win=64240 Len=0
23	15:29:40,461475831	193.136.9.183	10.0.2.15	FTP	74 Response: 220 (vsFTPd 2.3.5)
24	15:29:40,461503822	10.0.2.15	193.136.9.183	TCP	54 51814 → 21 [ACK] Seq=1 Ack=21 Win=64220 Len=0
25	15:29:42,530673789	PcsCompu_bc:d0:ca	RealtekU_12:35:03	ARP	42 Who has 10.0.2.3? Tell 10.0.2.15
26	15:29:42,530924595	RealtekU_12:35:03	PcsCompu_bc:d0:ca	ARP	60 10.0.2.3 is at 52:54:00:12:35:03
27	15:29:44,886228330	10.0.2.15	35.244.181.201	TLSv1.2	100 Application Data
28	15:29:44,886585018	35.244.181.201	10.0.2.15	TCP	60 443 → 37924 [ACK] Seq=1 Ack=47 Win=65535 Len=0
29	15:29:44,902575538	35.244.181.201	10.0.2.15	TLSv1.2	100 Application Data
30	15:29:44,902629377	10.0.2.15	35.244.181.201	TCP	54 37924 → 443 [ACK] Seq=47 Ack=47 Win=64015 Len=0
31	15:29:49,117726541	10.0.2.15	193.136.9.183	FTP	63 Request: USER cc
32	15:29:49,117995113	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [ACK] Seq=21 Ack=10 Win=65535 Len=0
33	15:29:49,133764912	193.136.9.183	10.0.2.15	FTP	88 Response: 331 Please specify the password.
34	15:29:49,133807160	10.0.2.15	193.136.9.183	TCP	54 51814 → 21 [ACK] Seq=10 Ack=55 Win=64180 Len=0
35	15:29:49,135507509	10.0.2.15	193.136.9.183	FTP	67 Request: PASS cc2021
36	15:29:49,135918684	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [ACK] Seq=55 Ack=23 Win=65535 Len=0
37	15:29:49,261368904	193.136.9.183	10.0.2.15	FTP	77 Response: 230 Login successful.
38	15:29:49,261850655	10.0.2.15	193.136.9.183	FTP	60 Request: SYST
39	15:29:49,262080001	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [ACK] Seq=78 Ack=29 Win=65535 Len=0
40	15:29:49,276239916	193.136.9.183	10.0.2.15	FTP	73 Response: 215 UNIX Type: L8
41	15:29:49,276631955	10.0.2.15	193.136.9.183	FTP	60 Request: FEAT
42	15:29:49,276901294	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [ACK] Seq=97 Ack=35 Win=65535 Len=0
43	15:29:49,291100677	193.136.9.183	10.0.2.15	FTP	69 Response: 211-Features:
44	15:29:49,291610438	193.136.9.183	10.0.2.15	FTP	61 Response: EPRT
45	15:29:49,291706215	10.0.2.15	193.136.9.183	TCP	54 51814 → 21 [ACK] Seq=35 Ack=119 Win=64122 Len=0
46	15:29:49,292215200	193.136.9.183	10.0.2.15	FTP	61 Response: EPSV
47	15:29:49,292704981	193.136.9.183	10.0.2.15	FTP	61 Response: MDTM
48	15:29:49,292746431	10.0.2.15	193.136.9.183	TCP	54 51814 → 21 [ACK] Seq=35 Ack=133 Win=64108 Len=0
49	15:29:49,293317802	193.136.9.183	10.0.2.15	FTP	61 Response: PASV
50	15:29:49,293823300	193.136.9.183	10.0.2.15	FTP	68 Response: REST STREAM
51	15:29:49,293876023	10.0.2.15	193.136.9.183	TCP	54 51814 → 21 [ACK] Seq=35 Ack=154 Win=64087 Len=0
52	15:29:49,294351596	193.136.9.183	10.0.2.15	FTP	61 Response: SIZE
53	15:29:49,294939193	193.136.9.183	10.0.2.15	FTP	61 Response: TVFS
54	15:29:49,295005461	10.0.2.15	193.136.9.183	TCP	54 51814 → 21 [ACK] Seq=35 Ack=168 Win=64073 Len=0
55	15:29:49,295425079	193.136.9.183	10.0.2.15	FTP	61 Response: UTF8
56	15:29:49,295984868	193.136.9.183	10.0.2.15	FTP	63 Response: 211 End
57	15:29:49,296043304	10.0.2.15	193.136.9.183	TCP	54 51814 → 21 [ACK] Seq=35 Ack=184 Win=64073 Len=0
58	15:29:49,296340701	10.0.2.15	193.136.9.183	FTP	68 Request: OPTS UTF8 ON
59	15:29:49,296510610	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [ACK] Seq=184 Ack=49 Win=65535 Len=0
60	15:29:49,314238392	193.136.9.183	10.0.2.15	FTP	80 Response: 200 Always in UTF8 mode.
61	15:29:49,314890133	10.0.2.15	193.136.9.183	FTP	59 Request: PWD
62	15:29:49,315066208	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [ACK] Seq=210 Ack=54 Win=65535 Len=0
63	15:29:49,329402639	193.136.9.183	10.0.2.15	FTP	70 Response: 257 "/home/cc"
64	15:29:49,329893023	10.0.2.15	193.136.9.183	FTP	62 Request: TYPE I
65	15:29:49,330012995	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [ACK] Seq=226 Ack=62 Win=65535 Len=0
66	15:29:49,344405905	193.136.9.183	10.0.2.15	FTP	85 Response: 200 Switching to Binary mode.
67	15:29:49,344831221	10.0.2.15	193.136.9.183	FTP	60 Request: PASV
68	15:29:49,345049186	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [ACK] Seq=257 Ack=68 Win=65535 Len=0
69	15:29:49,359778914	193.136.9.183	10.0.2.15	FTP	105 Response: 227 Entering Passive Mode (193,136,9,183,185,90)
70	15:29:49,360931722	10.0.2.15	193.136.9.183	FTP	75 Request: SIZE /home/cc/file1
71	15:29:49,361289581	10.0.2.15	193.136.9.183	TCP	74 36462 → 47450 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=254893534 TSecr=0 WS=128
72	15:29:49,361381609	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [ACK] Seq=307 Ack=89 Win=65535 Len=0
73	15:29:49,376013333	193.136.9.183	10.0.2.15	FTP	63 Response: 213 193
74	15:29:49,376636395	193.136.9.183	10.0.2.15	TCP	60 47450 → 36462 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
75	15:29:49,376674636	10.0.2.15	193.136.9.183	TCP	54 36462 → 47450 [ACK] Seq=1 Ack=1 Win=64240 Len=0
76	15:29:49,376911681	10.0.2.15	193.136.9.183	FTP	75 Request: MDTM /home/cc/file1
77	15:29:49,377242878	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [ACK] Seq=316 Ack=110 Win=65535 Len=0
78	15:29:49,392281456	193.136.9.183	10.0.2.15	FTP	74 Response: 213 20200210150046
79	15:29:49,392941544	10.0.2.15	193.136.9.183	FTP	75 Request: RETR /home/cc/file1
80	15:29:49,393279742	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [ACK] Seq=336 Ack=131 Win=65535 Len=0
81	15:29:49,410754899	193.136.9.183	10.0.2.15	FTP	127 Response: 150 Opening BINARY mode data connection for /home/cc/file1 (193 bytes).
82	15:29:49,411481262	193.136.9.183	10.0.2.15	FTP-DATA	247 FTP Data: 193 bytes (PASV) (SIZE /home/cc/file1)
83	15:29:49,411502924	10.0.2.15	193.136.9.183	TCP	54 36462 → 47450 [ACK] Seq=1 Ack=194 Win=64047 Len=0
84	15:29:49,412678866	193.136.9.183	10.0.2.15	TCP	60 47450 → 36462 [FIN, ACK] Seq=194 Ack=1 Win=65535 Len=0
85	15:29:49,413690527	10.0.2.15	193.136.9.183	TCP	54 36462 → 47450 [FIN, ACK] Seq=1 Ack=195 Win=64047 Len=0
86	15:29:49,414029994	193.136.9.183	10.0.2.15	TCP	60 47450 → 36462 [ACK] Seq=195 Ack=2 Win=65535 Len=0
87	15:29:49,415580070	10.0.2.15	193.136.9.183	TCP	54 51814 → 21 [FIN, ACK] Seq=131 Ack=409 Win=64073 Len=0
88	15:29:49,415880800	193.136.9.183	10.0.2.15	TCP	60 21 → 51814 [ACK] Seq=409 Ack=132 Win=65535 Len=0
89	15:29:49,428469894	193.136.9.183	10.0.2.15	FTP	78 Response: 226 Transfer complete.

Figura 9: Ftp - Captura de tráfego.

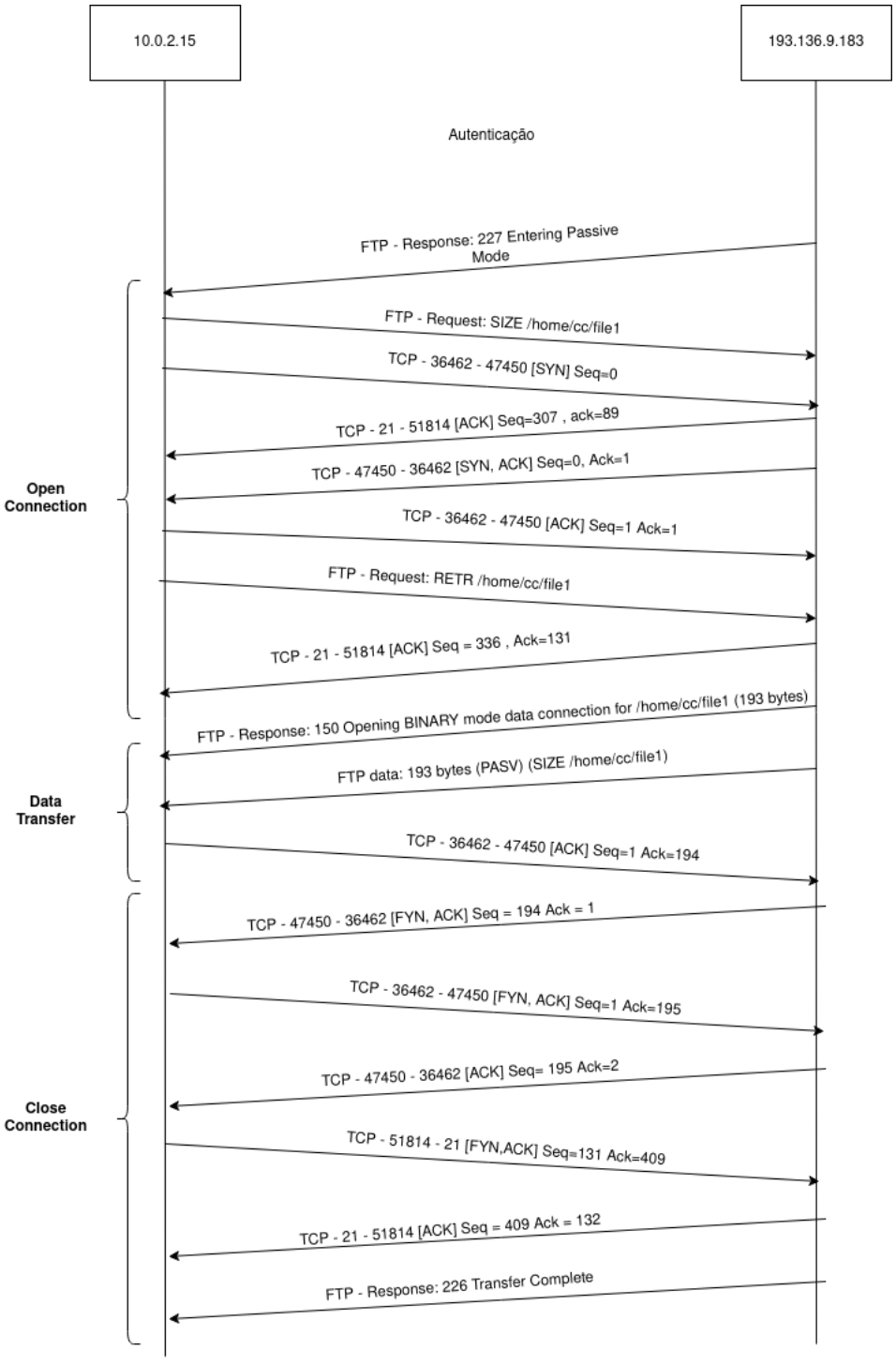


Figura 10: Ftp - Diagrama Temporal

NOTA: Não foi possível voltar a capturar o tráfego do acesso em tftp para cc2021.ddns.net, como forma de justificação do diagrama temporal representado na Figura 11. Para tal, pedimos que se tenha em conta a Figura 5.

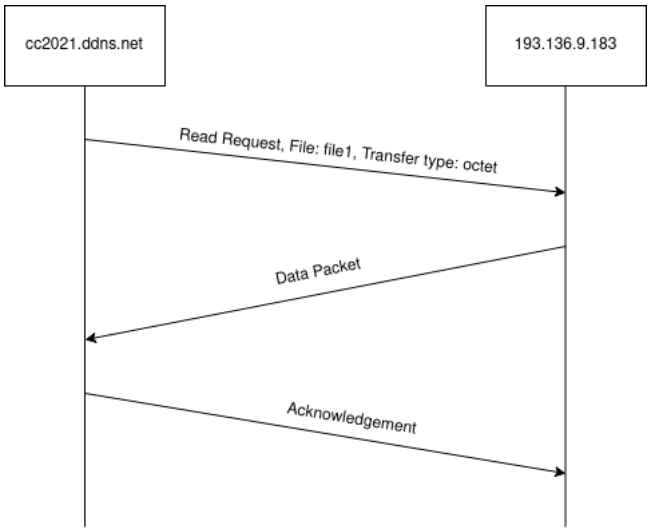


Figura 11: Tftp - Diagrama Temporal

1.3 Questão 3

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

R: Pela análise de pacotes no wireshark, podemos comparar as quatro aplicações de transferências de ficheiros em diversos pontos, dos quais destacaremos alguns. A nível do uso da camada de transporte, as aplicações SFTP, FTP e HTTP utilizam o protocolo TCP, enquanto que a aplicação TFTP utiliza o protocolo UDP. Quanto á eficiência de transferência podemos afirmar que: a aplicação SFTP utiliza ligações SSH que causam maior overhead e por isso diminuem a eficiência de transmissão. O facto de o SFTP ser fiável, também contribui para esta baixa eficiência. A aplicação FTP tem um elevado overhead e por isso também possui uma baixa eficiência de transferência. A aplicação TFTP tem uma elevada eficiência de transmissão devido ao baixo overhead. A aplicação HTTP possui também uma elevada eficiência de transmissão. Quanto á complexidade podemos afirmar que: as aplicações SFTP e FTP disponibilizam diversas funcionalidades tornando-os mais complexos. A aplicação TFTP é pouco complexa uma vez que implementa o protocolo UDP, não tendo este,

muitas funcionalidades (por exemplo, não tem mecanismos de autenticação). A aplicação HTTP é pouco complexa. Por fim, quanto á segurança podemos afirmar que: a aplicação SFTP é considerada segura na medida em que recorre a autenticação e encriptação de informação. Além disto, a utilização de ligações SSH a tornam também mais segura. A aplicação FTP apesar de recorrer á autenticação, é pouco segura. Por exemplo, durante a análise de pacotes utilizando o wireshark, era possível ler as passwords, não havendo qualquer tipo de encriptação. A aplicação TFTP não recorre a autenticação ou encriptação, sendo por isso pouco seguro. A aplicação HTTP recorre a autenticação, mas não recorre á encriptação, sendo por isso, pouco seguro.

1.4 Questão 4

P: 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).

R: Observando a figura x podemos verificar que houve perda de 5% dos pacotes enviados e 3 foram duplicados, isto porque havia problemas de rede e não havia nenhum protocolo para garantir o transporte ponto a ponto. Por outro lado, na figura y podemos comprovar pela captura que foi utilizado o protocolo TCP, que garante a entrega de todos os pacotes enviados. No entanto, isto implica o envio de várias mensagens de controlo, aumentando assim a complexidade da transmissão e originando uma maior sobrecarga da rede. Quanto ao UDP, estamos perante um protocolo muito menos complexo mas não fiável, o que implica ser a camada superior (aplicação) a garantir a receção dos dados. Este pode ser implementado em casos que seja necessário enviar pacotes rapidamente.

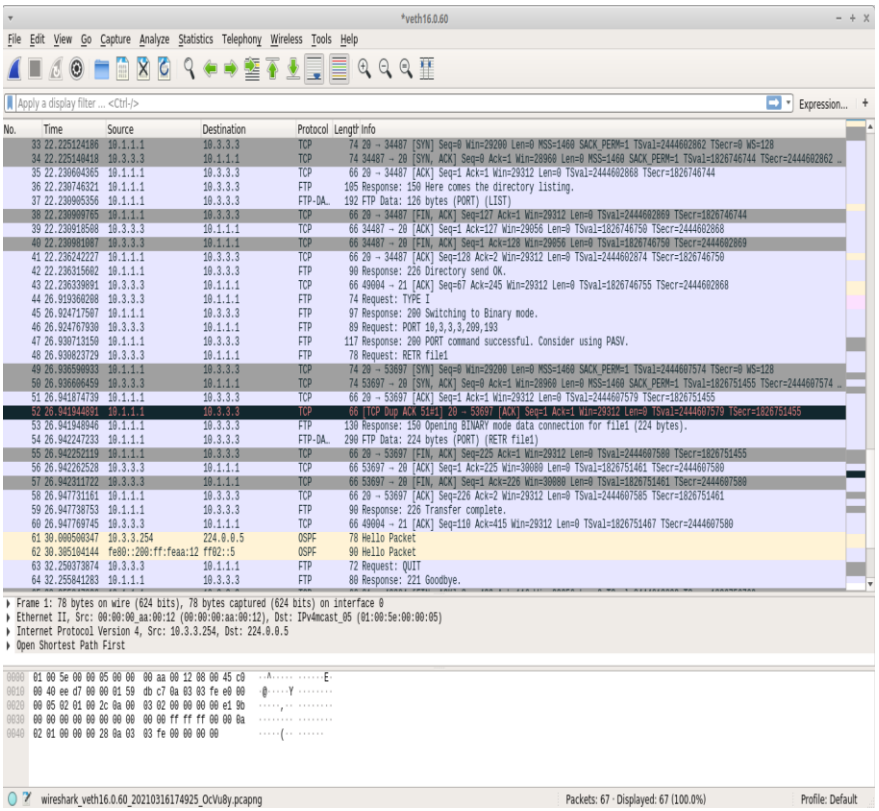


Figura 12: Captura de Tráfego da transferência do ficehiro file1.

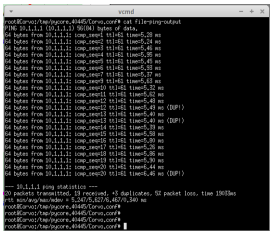


Figura 13: Ping do laptop Corvo para o Server1.

2 Conclusões

Ao longo deste guião, o grupo conseguiu aplicar e consolidar todos os conceitos abordados durante as aulas teórico-práticas, nomeadamente, a camada de transporte e os diversos protocolos de transporte e aplicacionais existentes. A nível de protocolos de transporte, o TCP e o UDP foram os que receberam maior atenção. Por fim, foi feita, utilizando a ferramenta wireshark, uma análise do tráfego gerado pelo uso dos vários protocolos.