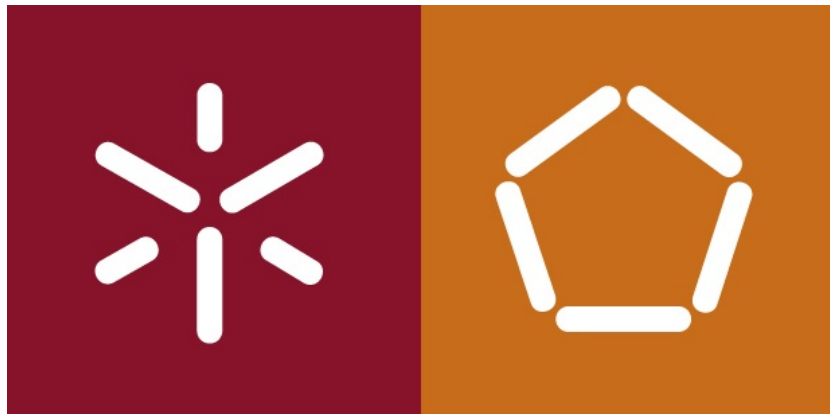


UNIVERSIDADE DO MINHO
MESTRADO INTEGRADO EM ENGENHARIA INFORMÁTICA



Comunicações por Computador - Protocolos
da Camada de Transporte (TP1)

PL3 GRUPO 1

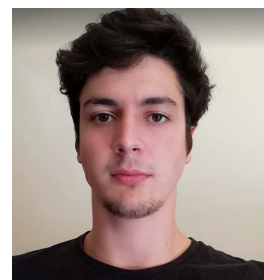
Trabalho realizado por:



A75119
Adriana Gonçalves



A74618
Bernardo Viseu



A75480
Marco Gonçalves

Braga, 24 de junho de 2021

Conteúdo

1	<i>Introdução</i>	2
2	Parte I	2
3	Parte II	6
3.1	Ficheiros Utilizados	6
3.2	i)	6
3.2.1	Ping	7
3.3	SFTP	9
3.3.1	ii)	9
3.3.2	iii)	11
3.4	FTP	12
3.4.1	ii)	12
3.4.2	iii)	12
3.5	TFTP	13
3.5.1	ii)	13
3.5.2	iii)	13
3.6	HTTP	14
3.6.1	ii)	14
3.6.2	iii)	14
4	<i>Conclusão</i>	15

1 Introdução

Para a realização deste trabalho utilizamos a máquina virtual disponibilizada pelos docentes desta UC. Este trabalho prático está dividido em 2 partes, a parte I refere-se ao uso da camada de transporte por parte das aplicações onde nos é pedido para fazer uma análise ao tráfego quando usamos o browser, ftp, tftp, telnet, ssh, nslookup e traceroute. Já a parte II refere-se á instalação, configuração e utilização de serviços de transferência de ficheiros onde nos é pedido que utilizando a topologia disponibilizada pelos docentes seja transferido o mesmo ficheiro usando 4 serviços diferentes SFTP, FTP, TFTP e HTTP.

2 Parte I

```
* aula2 traceroute cisco.di.uminho.pt
traceroute to cisco.di.uminho.pt (193.136.19.254), 30 hops max, 60 byte packets
 1 _gateway (192.168.68.1)  8.719 ms  8.609 ms  7.323 ms
 2 dsldevice.lan (192.168.1.254)  8.292 ms  9.240 ms  11.570 ms
 3 10.213.128.1 (10.213.128.1)  33.007 ms  36.483 ms  42.639 ms
 4 * * * telepac10-hsi.cprm.net (195.8.30.250)  33.949 ms
 5 dvs-cr1-bu10-200.cprm.net (195.8.30.249)  39.227 ms  44.530 ms  bt-cr1-bu10-200.cprm.net (195.8.30.245)  40.217 ms
 6 195.8.0.165 (195.8.0.165)  52.300 ms  51.260 ms  lis2-cr1--hull-0-0.cprm.net (195.8.1.57)  50.219 ms
 7 FCCN.AS1930.gigapix.pt (193.136.250.10)  57.138 ms  FCCN.AS1930.gigapix.pt (193.136.251.1)  57.059 ms  FCCN.AS1930.gigapix.pt (193.136.250.10)  135.056 ms
 8 Router30.Lisboa.fccn.pt (194.210.6.104)  27.948 ms  Router60.Lisboa.fccn.pt (194.210.6.202)  138.748 ms  134.872 ms
 9 Router23.Backbone1.Porto.fccn.pt (193.136.1.2)  142.515 ms  Router43.Backbone2.Porto.fccn.pt (193.136.4.2)  151.808 ms  Router23.Backbone1.Porto.fccn.pt (193.136.1.2)  153.520 ms
10 ROUTER42.10GE.Porto.fccn.pt (193.137.4.5)  197.960 ms  203.773 ms  196.057 ms
11 UMinho.Braga.fccn.pt (193.136.4.100)  214.664 ms  212.614 ms  212.546 ms
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
* aula2
```

Figura 2: Captura de *traceroute*

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.0.2.15	192.168.1.254	DNS	86	Standard query 0xaba0 AAAA marco.uminho.pt OPT
2	0.026793435	192.168.1.254	10.0.2.15	DNS	140	Standard query response 0xaba0 AAAA marco.uminho.pt SOA
3	0.02743005	10.0.2.15	193.136.9.240	TCP	60	80 -- 44802 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
4	0.046996871	193.136.9.240	10.0.2.15	TCP	60	80 -- 44802 [ACK] Seq=1 Ack=163 Win=65535 Len=0 MSS=1460
5	0.047033595	10.0.2.15	193.136.9.240	TCP	54	44802 -- 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.047106448	10.0.2.15	193.136.9.240	HTTP	216	GET /disciplinas/CC-WIE/ HTTP/1.1
7	0.047296499	193.136.9.240	10.0.2.15	TCP	60	80 -- 44802 [ACK] Seq=1 Ack=163 Win=65535 Len=0
8	0.070649580	193.136.9.240	10.0.2.15	TCP	2974	80 -- 44802 [ACK] Seq=1 Ack=163 Win=65535 Len=2920 [TCP segment of data stream 0x00000000: 80 → 44802, Seq=1, Win=65535, Len=2920]
9	0.070655081	10.0.2.15	193.136.9.240	TCP	54	44802 -- 80 [ACK] Seq=163 Ack=2921 Win=62780 Len=0
10	0.070830528	193.136.9.240	10.0.2.15	TCP	2974	80 -- 44802 [PSH, ACK] Seq=2921 Ack=163 Win=65535 Len=2920 [TCP segment of data stream 0x00000000: 80 → 44802, Seq=1, Win=65535, Len=2920]
11	0.070836899	10.0.2.15	193.136.9.240	TCP	54	44802 -- 80 [ACK] Seq=163 Ack=5841 Win=61320 Len=0
12	0.074083149	193.136.9.240	10.0.2.15	TCP	1514	80 -- 44802 [PSH, ACK] Seq=5841 Ack=163 Win=65535 Len=1460
13	0.074091190	10.0.2.15	193.136.9.240	TCP	54	44802 -- 80 [ACK] Seq=163 Ack=7301 Win=62780 Len=0
14	0.077068220	193.136.9.240	10.0.2.15	HTTP	1504	HTTP/1.1 200 OK (text/html)
15	0.077076950	10.0.2.15	193.136.9.240	TCP	54	44802 -- 80 [ACK] Seq=163 Ack=8751 Win=62780 Len=0
16	0.077445637	10.0.2.15	193.136.9.240	TCP	54	44802 -- 80 [FIN, ACK] Seq=163 Ack=8751 Win=62780 Len=0
17	0.07527889	193.136.9.240	10.0.2.15	TCP	60	80 -- 44802 [ACK] Seq=8751 Ack=164 Win=65535 Len=0
18	0.080975478	193.136.9.240	10.0.2.15	TCP	60	80 -- 44802 [FIN, ACK] Seq=8751 Ack=164 Win=65535 Len=0
19	0.090993649	10.0.2.15	193.136.9.240	TCP	54	44802 -- 80 [ACK] Seq=164 Ack=8752 Win=62780 Len=0
20	5.254573467	PcsCompu_d1:8b:d0	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
21	5.254779060	RealtekU_12:35:02	PcsCompu_d1:8b:d0	ARP	60	10.0.2.2 is at 52:54:00:12:35:02

Total Length: 60
Identification: 0x3226 (12838)
Flags: 0x4000, Don't Fragment
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x310f [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.15
Destination: 193.136.9.240
Transmission Control Protocol, Src Port: 44802, Dst Port: 80, Seq: 0, Len: 0
Source Port: 44802
Destination Port: 80
[Stream index: 0]
TCP Segment Len: 61
0000 52 54 00 12 35 02 08 00 27 d1 8b d0 08 00 45 00 RT: 5E:
0010 00 3c 32 26 40 00 40 06 31 0f 0a 00 02 0f 51 08 --200-0-1.....
0020 00 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..PK.....
0030 1a 19 07 d5 00 00 02 04 05 b4 04 02 08 0a 18 a1
0040 1b cf 00 00 00 00 01 03 03 07
.....

Figura 3: Captura de browser

No.	Time	Source	Destination	Protocol	Length	Info
158	1.285050934	193.136.9.183	192.168.68.109	FTP	86	Response: 220 (vsFTPd 2.3.5)
308	2.666141839	192.168.68.109	193.136.9.183	FTP	75	Request: USER cc
315	2.759457972	193.136.9.183	192.168.68.109	FTP	100	Response: 331 Please specify the password.
544	4.725186267	192.168.68.109	193.136.9.183	FTP	79	Request: PASS cc2021
558	4.825208190	193.136.9.183	192.168.68.109	FTP	89	Response: 230 Login successful.
560	4.825313789	192.168.68.109	193.136.9.183	FTP	72	Request: SYST
563	4.855343064	193.136.9.183	192.168.68.109	FTP	85	Response: 215 UNIX Type: L8

Figura 4: Captura de TFP

No.	Time	Source	Destination	Protocol	Length	Info
203	1.155754584	192.168.68.109	193.136.9.183	TELNET	93	Telnet Data ...
2599	16.215060619	193.136.9.183	192.168.68.109	TELNET	78	Telnet Data ...
2623	16.279240750	193.136.9.183	192.168.68.109	TELNET	105	Telnet Data ...
2625	16.279844161	192.168.68.109	193.136.9.183	TELNET	167	Telnet Data ...
2635	16.324574935	193.136.9.183	192.168.68.109	TELNET	69	Telnet Data ...
2637	16.324781223	192.168.68.109	193.136.9.183	TELNET	69	Telnet Data ...
2643	16.383516517	193.136.9.183	192.168.68.109	TELNET	69	Telnet Data ...
2645	16.383688182	192.168.68.109	193.136.9.183	TELNET	69	Telnet Data ...
2652	16.419191554	193.136.9.183	192.168.68.109	TELNET	103	Telnet Data ...
3284	20.367587248	192.168.68.109	193.136.9.183	TELNET	67	Telnet Data ...
3291	20.397891173	193.136.9.183	192.168.68.109	TELNET	67	Telnet Data ...
3307	20.515645002	192.168.68.109	193.136.9.183	TELNET	67	Telnet Data ...
3315	20.544719185	193.136.9.183	192.168.68.109	TELNET	67	Telnet Data ...
3325	20.629103733	192.168.68.109	193.136.9.183	TELNET	68	Telnet Data ...
3330	20.657593829	193.136.9.183	192.168.68.109	TELNET	78	Telnet Data ...
3479	21.560477210	192.168.68.109	193.136.9.183	TELNET	67	Telnet Data ...
3499	21.695817585	192.168.68.109	193.136.9.183	TELNET	67	Telnet Data ...
3551	22.053915808	192.168.68.109	193.136.9.183	TELNET	67	Telnet Data ...
3574	22.182259098	192.168.68.109	193.136.9.183	TELNET	67	Telnet Data ...
3638	22.485234013	192.168.68.109	193.136.9.183	TELNET	67	Telnet Data ...
3665	22.664951659	192.168.68.109	193.136.9.183	TELNET	67	Telnet Data ...
3711	22.907202766	192.168.68.109	193.136.9.183	TELNET	68	Telnet Data ...
3719	22.938377616	193.136.9.183	192.168.68.109	TELNET	68	Telnet Data ...
3732	23.024599252	193.136.9.183	192.168.68.109	TELNET	134	Telnet Data ...
3739	23.074085292	193.136.9.183	192.168.68.109	TELNET	68	Telnet Data ...
3768	23.216172541	193.136.9.183	192.168.68.109	TELNET	129	Telnet Data ...
3782	23.252652037	193.136.9.183	192.168.68.109	TELNET	205	Telnet Data ...
7345	48.266114900	193.136.9.183	192.168.68.109	TELNET	68	Telnet Data ...
7979	52.086289426	192.168.68.109	193.136.9.183	TELNET	67	Telnet Data ...
7987	52.123583610	193.136.9.183	192.168.68.109	TELNET	67	Telnet Data ...
8014	52.295033543	192.168.68.109	193.136.9.183	TELNET	67	Telnet Data ...
8021	52.335477280	193.136.9.183	192.168.68.109	TELNET	67	Telnet Data ...
8043	52.402506530	192.168.68.109	193.136.9.183	TELNET	67	Telnet Data ...
8049	52.467410938	193.136.9.183	192.168.68.109	TELNET	67	Telnet Data ...
8073	52.615093553	192.168.68.109	193.136.9.183	TELNET	67	Telnet Data ...
8078	52.650215039	193.136.9.183	192.168.68.109	TELNET	67	Telnet Data ...
8105	52.798309863	192.168.68.109	193.136.9.183	TELNET	68	Telnet Data ...
8111	52.830817388	193.136.9.183	192.168.68.109	TELNET	68	Telnet Data ...

Figura 5: Captura de telnet

No.	Time	Source	Destination	Protocol	Length	Info
1	0.060600000	10.0.2.15	192.168.1.254	DNS	75	Standard query 0xb8b8 A cc2021.ddns.net
2	0.060140941	10.0.2.15	192.168.1.254	DNS	75	Standard query 0x2d96 AAAA cc2021.ddns.net
3	0.057972665	192.168.1.254	10.0.2.15	DNS	91	Standard query response 0xb8b8 A cc2021.ddns.net A 193.136.9.183
4	0.113074838	192.168.1.254	10.0.2.15	DNS	135	Standard query response 0x2d96 AAAA cc2021.ddns.net SOA nfi.n...
5	0.113390509	10.0.2.15	193.136.9.183	TCP	74	54314 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
6	0.127879481	193.136.9.183	10.0.2.15	TCP	60	22 → 54314 [ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
7	0.127915629	10.0.2.15	193.136.9.183	TCP	54	54314 → 22 [ACK] Seq=1 Ack=1 Win=64240 Len=0
8	0.128169986	10.0.2.15	193.136.9.183	SSHv2	95	Client: Protocol (SSH-2.0-OpenSSH.8.2p1 Ubuntu-4ubuntu0.1)
9	0.128334542	193.136.9.183	10.0.2.15	TCP	60	22 → 54314 [ACK] Seq=1 Ack=42 Win=65535 Len=0
10	0.172031073	193.136.9.183	10.0.2.15	SSHv2	95	Server: Protocol (SSH-2.0-OpenSSH.5.9p1 Debian-Subuntu1.4)
11	0.172058080	10.0.2.15	193.136.9.183	TCP	54	54314 → 22 [ACK] Seq=42 Ack=42 Win=64199 Len=0
12	0.172382158	10.0.2.15	193.136.9.183	SSHv2	1566	Client: Key Exchange Init
13	0.17254223	193.136.9.183	10.0.2.15	TCP	60	22 → 54314 [ACK] Seq=42 Ack=1502 Win=65535 Len=0
14	0.17254311	193.136.9.183	10.0.2.15	TCP	60	22 → 54314 [ACK] Seq=42 Ack=1554 Win=65535 Len=0
15	0.188546538	193.136.9.183	10.0.2.15	SSHv2	1038	Server: Key Exchange Init
16	0.188566949	10.0.2.15	193.136.9.183	TCP	54	54314 → 22 [ACK] Seq=1554 Ack=1026 Win=63960 Len=0
17	0.188888307	10.0.2.15	193.136.9.183	SSHv2	134	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
18	0.189091995	193.136.9.183	10.0.2.15	TCP	60	22 → 54314 [ACK] Seq=1026 Ack=1634 Win=65535 Len=0
19	0.228760232	193.136.9.183	10.0.2.15	SSHv2	366	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New...
20	0.228777590	10.0.2.15	193.136.9.183	TCP	54	54314 → 22 [ACK] Seq=1634 Ack=1338 Win=63960 Len=0
21	0.229519359	10.0.2.15	193.136.9.183	SSHv2	70	Client: New Keys
22	0.229647623	193.136.9.183	10.0.2.15	TCP	60	22 → 54314 [ACK] Seq=1338 Ack=1650 Win=65535 Len=0
23	0.230022409	193.136.9.183	10.0.2.15	SSHv2	94	Client: Encrypted packet (len=40)
24	0.230194809	193.136.9.183	10.0.2.15	TCP	60	22 → 54314 [ACK] Seq=1338 Ack=1690 Win=65535 Len=0
25	0.245689000	193.136.9.183	10.0.2.15	SSHv2	94	Server: Encrypted packet (len=40)
26	0.245790038	10.0.2.15	193.136.9.183	SSHv2	110	Client: Encrypted packet (len=56)
27	0.246065822	193.136.9.183	10.0.2.15	TCP	60	22 → 54314 [ACK] Seq=1378 Ack=1746 Win=65535 Len=0
28	0.246171779	193.136.9.183	10.0.2.15	SSHv2	110	Server: Encrypted packet (len=56)
29	0.317806788	10.0.2.15	193.136.9.183	TCP	54	54314 → 22 [ACK] Seq=1746 Ack=1434 Win=63960 Len=0
30	0.3171911589	10.0.2.15	193.136.9.183	SSHv2	190	Client: Encrypted packet (len=136)
31	0.3172192708	193.136.9.183	10.0.2.15	TCP	60	22 → 54314 [ACK] Seq=1434 Ack=1882 Win=65535 Len=0
32	0.249583688	193.136.9.183	10.0.2.15	SSHv2	78	Server: Encrypted packet (len=24)
33	0.249533460	10.0.2.15	193.136.9.183	TCP	54	54314 → 22 [ACK] Seq=1882 Ack=1458 Win=63960 Len=0
34	0.249760817	10.0.2.15	193.136.9.183	SSHv2	166	Client: Encrypted packet (len=112)
35	0.249955144	193.136.9.183	10.0.2.15	TCP	60	22 → 54314 [ACK] Seq=1458 Ack=1994 Win=65535 Len=0
36	0.2470661615	193.136.9.183	10.0.2.15	SSHv2	94	Server: Encrypted packet (len=40)
37	0.2470678838	10.0.2.15	193.136.9.183	TCP	54	54314 → 22 [ACK] Seq=1994 Ack=1498 Win=63960 Len=0
38	0.2470904990	10.0.2.15	193.136.9.183	SSHv2	1182	Client: Encrypted packet (len=128)
39	0.2470932776	193.136.9.183	10.0.2.15	TCP	60	22 → 54314 [ACK] Seq=1498 Ack=3122 Win=65535 Len=0
40	0.2487596560	193.136.9.183	10.0.2.15	SSHv2	142	Server: Encrypted packet (len=88)
41	0.2487615477	10.0.2.15	193.136.9.183	TCP	54	54314 → 22 [ACK] Seq=3122 Ack=1586 Win=63960 Len=0
42	0.2490451054	193.136.9.183	10.0.2.15	SSHv2	350	Server: Encrypted packet (len=296)
43	0.2490458623	10.0.2.15	193.136.9.183	TCP	54	54314 → 22 [ACK] Seq=3122 Ack=1882 Win=63960 Len=0

cc2021.ddns.net: type A, class IN, addr 193.136.9.183

Name: cc2021.ddns.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 60 (1 minute)

Data length: 4

Address: 193.136.9.183

0010 00 4d ec 20 00 00 11 bf ca c0 a8 01 fe 0a 00 M
Source (ip.src), 4 bytes
Packets: 43 · Displayed: 43 (100.0%) Profile: Default

Figura 6: Captura de ssh

```

→ aula2 nslookup www.uminho.pt
Server:          192.168.1.254
Address:         192.168.1.254#53

Non-authoritative answer:
Name:   www.uminho.pt
Address: 193.137.9.114

→ aula2

```

Figura 7: Captura de nslookup

Comando usado	Protocolo de Aplicação	Protocolo de Transporte	Porta de atendimento	Overhead de Transporte
ping		ICMP	7	16
tracert		UDP	33434	
telnet	TELNET	TCP	23	20
ftp	FTP	TCP	21	20
Tftp	TFTP	UDP	69	22
browser/http	HTTP	TCP	80	20
nslookup	DNS	UDP	40777	53
ssh	SSHv2	TCP	22	20

3 Parte II

O ii) tem como objectivo transferir de diferentes formas o file1 e o file2 cliente servidor e o iii) tem como objetivo analisar os tempos de transmissão dos ficheiros.

3.1 Ficheiros Utilizados

Houve um pequeno problema ao seguir o enunciado e o file1 não é o ficheiro /etc/hosts mas simplesmente um ficheiro com a string "Este é o file1"o que para o que é pedido durante o exercício não representa nenhum problema. Já o file2 é uma cópia do /bin/ls.

3.2 i)

Este ponto tem como objectivo testar a conectividade do Laptop1(10.4.4.1) e do Corvo(10.3.3.3) com o Server1(10.1.1.1).

3.2.1 Ping

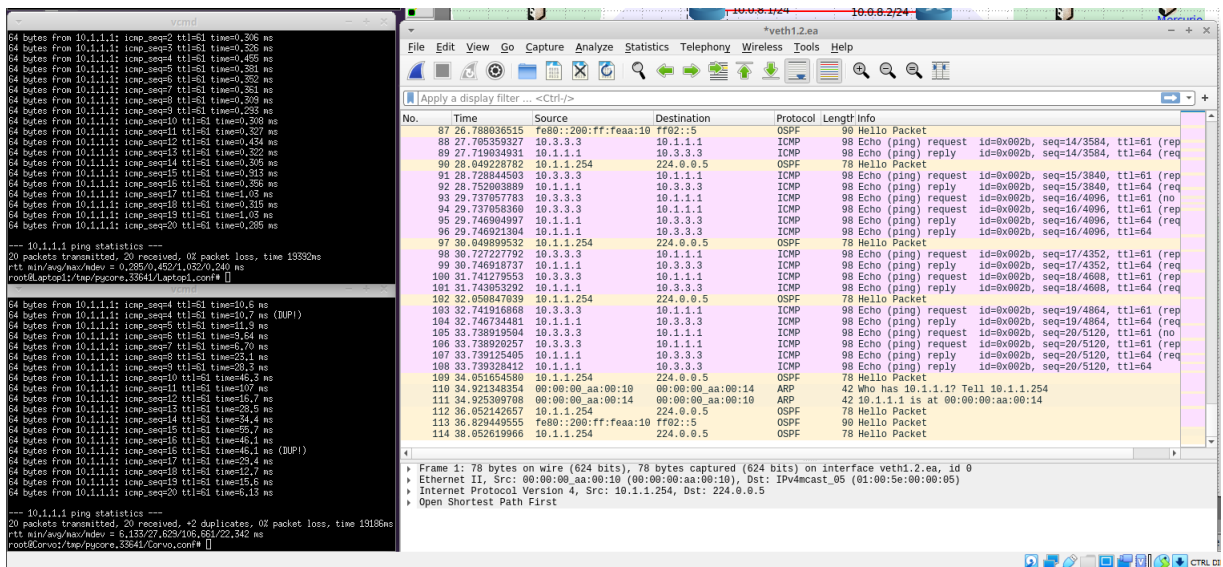


Figura 8: Captura do Ping ao servidor


```
vcmd
64 bytes from 10.1.1.1: icmp_seq=3 ttl=61 time=7.79 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=61 time=13.9 ms
64 bytes from 10.1.1.1: icmp_seq=5 ttl=61 time=0.749 ms
64 bytes from 10.1.1.1: icmp_seq=6 ttl=61 time=16.7 ms
64 bytes from 10.1.1.1: icmp_seq=7 ttl=61 time=63.2 ms
64 bytes from 10.1.1.1: icmp_seq=8 ttl=61 time=0.336 ms
64 bytes from 10.1.1.1: icmp_seq=9 ttl=61 time=0.548 ms
64 bytes from 10.1.1.1: icmp_seq=10 ttl=61 time=0.570 ms
64 bytes from 10.1.1.1: icmp_seq=11 ttl=61 time=0.369 ms
64 bytes from 10.1.1.1: icmp_seq=12 ttl=61 time=0.873 ms
64 bytes from 10.1.1.1: icmp_seq=13 ttl=61 time=0.320 ms
64 bytes from 10.1.1.1: icmp_seq=14 ttl=61 time=0.912 ms
64 bytes from 10.1.1.1: icmp_seq=15 ttl=61 time=0.316 ms
64 bytes from 10.1.1.1: icmp_seq=16 ttl=61 time=0.540 ms
64 bytes from 10.1.1.1: icmp_seq=17 ttl=61 time=0.531 ms
64 bytes from 10.1.1.1: icmp_seq=18 ttl=61 time=0.533 ms
64 bytes from 10.1.1.1: icmp_seq=19 ttl=61 time=0.294 ms
64 bytes from 10.1.1.1: icmp_seq=20 ttl=61 time=0.316 ms

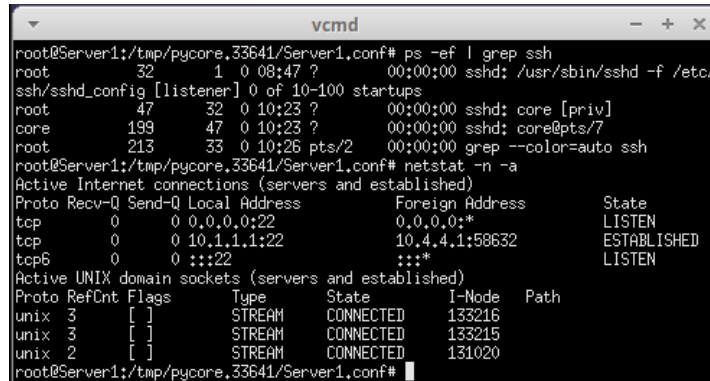
--- 10.1.1.1 ping statistics ---
file-ping-putut-Laptopl::20 packets transmitted, 20 received, 0% packet loss, time 19369ms
:rtt min/avg/max/mdev = 0.294/5.792/63.216/13.962 ms
(END)(END)(END)(END)(END)

vcmd
64 bytes from 10.1.1.1: icmp_seq=4 ttl=61 time=7.40 ms
64 bytes from 10.1.1.1: icmp_seq=5 ttl=61 time=5.91 ms
64 bytes from 10.1.1.1: icmp_seq=6 ttl=61 time=5.29 ms
64 bytes from 10.1.1.1: icmp_seq=7 ttl=61 time=9.41 ms
64 bytes from 10.1.1.1: icmp_seq=8 ttl=61 time=5.77 ms
64 bytes from 10.1.1.1: icmp_seq=8 ttl=61 time=5.77 ms (DUP!)
64 bytes from 10.1.1.1: icmp_seq=9 ttl=61 time=5.97 ms
64 bytes from 10.1.1.1: icmp_seq=10 ttl=61 time=5.67 ms
64 bytes from 10.1.1.1: icmp_seq=11 ttl=61 time=6.13 ms
64 bytes from 10.1.1.1: icmp_seq=12 ttl=61 time=5.44 ms
64 bytes from 10.1.1.1: icmp_seq=13 ttl=61 time=6.22 ms
64 bytes from 10.1.1.1: icmp_seq=14 ttl=61 time=5.43 ms
64 bytes from 10.1.1.1: icmp_seq=14 ttl=61 time=5.43 ms (DUP!)
64 bytes from 10.1.1.1: icmp_seq=16 ttl=61 time=5.45 ms
64 bytes from 10.1.1.1: icmp_seq=17 ttl=61 time=6.81 ms
64 bytes from 10.1.1.1: icmp_seq=18 ttl=61 time=5.31 ms
64 bytes from 10.1.1.1: icmp_seq=19 ttl=61 time=5.91 ms
64 bytes from 10.1.1.1: icmp_seq=20 ttl=61 time=6.13 ms
file-ping-output-corvo
:--- 10.1.1.1 ping statistics ---
:20 packets transmitted, 19 received, +3 duplicates, 5% packet loss, time 19125ms
:rtt min/avg/max/mdev = 5.287/6.160/9.406/0.942 ms
(END)(END)[]
```

Figura 9: Captura do Less ao output do ping

3.3 SFTP

3.3.1 ii)



```
root@Server1:/tmp/pycore.33641/Server1.conf# ps -ef | grep ssh
root      32      1  0 08:47 ?        00:00:00 sshd: /usr/sbin/sshd -f /etc/
ssh/sshd_config [listener] 0 of 10-100 startups
root      47      32  0 10:23 ?        00:00:00 sshd: core [priv]
core     199      47  0 10:23 ?        00:00:00 sshd: core@pts/7
root     213      33  0 10:26 pts/2    00:00:00 grep --color=auto ssh
root@Server1:/tmp/pycore.33641/Server1.conf# netstat -n -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp      0      0 10.1.1.1:22             10.4.4.1:59632         ESTABLISHED
tcp6     0      0 :::22                   :::*                    LISTEN
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node  Path
unix    3      [ ]       STREAM    CONNECTED    133216
unix    3      [ ]       STREAM    CONNECTED    133215
unix    2      [ ]       STREAM    CONNECTED    131020
root@Server1:/tmp/pycore.33641/Server1.conf#
```

Figura 10: Captura prova que o Server1 tem ssh a correr.

```
vcmd
Warning: Permanently added '10.1.1.1' (RSA) to the list of known hosts.
core@10.1.1.1's password:
Connected to 10.1.1.1.
sftp> cd /sr
sftp> cd /srv/
ftp/  tftp/

sftp> cd /srv/f
sftp> cd /srv/ftp/
sftp> get fil
file1  file2

sftp> get file
file1  file2

sftp> get file1
sftp> get file1
Fetching /srv/ftp/file1 to file1
/srv/ftp/file1          100% 18    9.0KB/s  00:00
sftp> get file2
Fetching /srv/ftp/file2 to file2
/srv/ftp/file2          100% 139KB 15.8MB/s  00:00
sftp> quit
root@Laptop1:/tmp/pycore.34771/Laptop1.conf# S

root@Corvo:/tmp/pycore.34771/Corvo.conf# sftp core@10.1.1.1
core@10.1.1.1's password:
Connected to 10.1.1.1.
sftp> cd /s
sbin/  snap/  srv/  swapfile sys/

sftp> cd /sr
sftp> cd /srv/ftp
sftp> cd /srv/ftp/
sftp> get fil
file1  file2

sftp> get file
file1  file2

sftp> get file1
sftp> get file1
Fetching /srv/ftp/file1 to file1
/srv/ftp/file1          100% 18    1.2KB/s  00:00
sftp> get file2
Fetching /srv/ftp/file2 to file2
/srv/ftp/file2          100% 139KB 1.6MB/s  00:00
sftp> quit
root@Corvo:/tmp/pycore.34771/Corvo.conf#
```

Figura 11: Captura do comandos utilizados nos clientes

3.3.2 iii)

The image shows a Wireshark packet capture window titled 'sftp.pcapng'. The main pane displays a list of 38 captured packets. The first 19 packets are OSPF Hello packets (protocol 89) sent from 10.1.1.254 to 224.0.0.5. The remaining 19 packets are encrypted traffic (SSH or TCP) between 10.1.1.1 and 10.4.4.1. The packet details pane at the bottom shows the structure of a frame: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw hex and ASCII data of the captured frame.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.1.1.254	224.0.0.5	OSPF	78	Hello Packet
2	1.277959919	10.4.4.1	10.1.1.1	SSH	134	Client: Encrypted packet (len=68)
3	1.278232042	10.1.1.1	10.4.4.1	SSH	142	Server: Encrypted packet (len=76)
4	1.278421534	10.4.4.1	10.1.1.1	TCP	66	50502 → 22 [ACK] Seq=69 Ack=77 Win=501 Len=0 TSval=2418692422 TSecr=31968
5	1.278516518	10.4.4.1	10.1.1.1	SSH	134	Client: Encrypted packet (len=68)
6	1.278798605	10.1.1.1	10.4.4.1	SSH	142	Server: Encrypted packet (len=76)
7	1.278940664	10.4.4.1	10.1.1.1	TCP	66	50502 → 22 [ACK] Seq=137 Ack=153 Win=501 Len=0 TSval=2418692422 TSecr=31968
8	1.279063373	10.4.4.1	10.1.1.1	SSH	142	Client: Encrypted packet (len=76)
9	1.279256847	10.1.1.1	10.4.4.1	SSH	118	Server: Encrypted packet (len=52)
10	1.279409385	10.4.4.1	10.1.1.1	TCP	66	50502 → 22 [ACK] Seq=213 Ack=205 Win=501 Len=0 TSval=2418692423 TSecr=31968
11	1.279602540	10.4.4.1	10.1.1.1	SSH	134	Client: Encrypted packet (len=68)
12	1.279893814	10.1.1.1	10.4.4.1	SSH	134	Server: Encrypted packet (len=68)
13	1.280085446	10.4.4.1	10.1.1.1	TCP	66	50502 → 22 [ACK] Seq=281 Ack=273 Win=501 Len=0 TSval=2418692423 TSecr=31968
14	1.280502819	10.4.4.1	10.1.1.1	SSH	134	Client: Encrypted packet (len=68)
15	1.280687355	10.1.1.1	10.4.4.1	SSH	134	Server: Encrypted packet (len=68)
16	1.280878823	10.4.4.1	10.1.1.1	TCP	66	50502 → 22 [ACK] Seq=349 Ack=341 Win=501 Len=0 TSval=2418692424 TSecr=31968
17	1.280990555	10.4.4.1	10.1.1.1	SSH	118	Client: Encrypted packet (len=52)
18	1.281243248	10.1.1.1	10.4.4.1	SSH	134	Server: Encrypted packet (len=68)
19	1.281395928	10.4.4.1	10.1.1.1	TCP	66	50502 → 22 [ACK] Seq=401 Ack=409 Win=501 Len=0 TSval=2418692425 TSecr=31968
20	2.000708960	10.1.1.254	224.0.0.5	OSPF	78	Hello Packet
21	3.867240466	fe80::200:ff:feaa:10	ff02::5	OSPF	90	Hello Packet
22	4.001680505	10.1.1.254	224.0.0.5	OSPF	78	Hello Packet
23	6.003450549	10.1.1.254	224.0.0.5	OSPF	78	Hello Packet
24	8.005102285	10.1.1.254	224.0.0.5	OSPF	78	Hello Packet
25	10.005561099	10.1.1.254	224.0.0.5	OSPF	78	Hello Packet
26	12.006497823	10.1.1.254	224.0.0.5	OSPF	78	Hello Packet
27	12.923944557	10.4.4.1	10.1.1.1	SSH	134	Client: Encrypted packet (len=68)
28	12.924211300	10.1.1.1	10.4.4.1	SSH	142	Server: Encrypted packet (len=76)
29	12.924402978	10.4.4.1	10.1.1.1	TCP	66	50502 → 22 [ACK] Seq=469 Ack=485 Win=501 Len=0 TSval=2418704068 TSecr=31968
30	12.924535893	10.4.4.1	10.1.1.1	SSH	134	Client: Encrypted packet (len=68)
31	12.925492083	10.1.1.1	10.4.4.1	SSH	142	Server: Encrypted packet (len=76)
32	12.925761716	10.4.4.1	10.1.1.1	TCP	66	50502 → 22 [ACK] Seq=537 Ack=561 Win=501 Len=0 TSval=2418704069 TSecr=31968
33	12.925809000	10.4.4.1	10.1.1.1	SSH	142	Client: Encrypted packet (len=76)
34	12.926017666	10.1.1.1	10.4.4.1	SSH	118	Server: Encrypted packet (len=52)
35	12.926274111	10.4.4.1	10.1.1.1	TCP	66	50502 → 22 [ACK] Seq=613 Ack=613 Win=501 Len=0 TSval=2418704069 TSecr=31968
36	12.926367536	10.4.4.1	10.1.1.1	SSH	134	Client: Encrypted packet (len=68)
37	12.926806738	10.1.1.1	10.4.4.1	SSH	1514	Server: Encrypted packet (len=1448)
38	12.926902801	10.1.1.1	10.4.4.1	SSH	1514	Server: Encrypted packet (len=1448)

Frame 196: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface veth1.2.a2, id 0
 Ethernet II, Src: 00:00:00:aa:00:10 (00:00:00:aa:00:10), Dst: 00:00:00:aa:00:14 (00:00:00:aa:00:14)
 Internet Protocol Version 4, Src: 10.4.4.1, Dst: 10.1.1.1
 Transmission Control Protocol, Src Port: 50502, Dst Port: 22, Seq: 1154, Ack: 143478, Len: 0

0000 00 00 00 aa 00 14 00 00 00 aa 00 10 08 00 45 08
 0010 00 34 00 00 40 00 3d 06 24 b6 0a 04 04 01 0a 01
 0020 01 01 c5 46 00 16 b6 1e d2 bc 6c 68 0b 23 80 10
 0030 06 1d d1 12 00 00 01 01 08 0a 90 2a 8e eb be 8b
 0040 e3 21

Figura 12: Captura do wireshark sobre os pacotes transmitidos

Neste caso não conseguimos identificar ao certo quais eram os pacotes para transmitir os dados uma vez que eles se encontram encriptados o que torna as coisas complicadas de analisar.

3.4 FTP

3.4.1 ii)

No.	Time	Source	Destination	Protocol	Length	Info
4	5.688751079	10.4.4.1	10.1.1.1	FTP	74	Request: TYPE I
5	5.688930987	10.1.1.1	10.4.4.1	FTP	97	Response: 200 Switching to Binary mode.
7	5.689261220	10.4.4.1	10.1.1.1	FTP	88	Request: PORT 10,4,4,1,163,79
8	5.689451159	10.1.1.1	10.4.4.1	FTP	117	Response: 200 PORT command successful. Consider using PASV.
10	5.689666433	10.4.4.1	10.1.1.1	FTP	78	Request: RETR file1
14	5.690492662	10.1.1.1	10.4.4.1	FTP	129	Response: 150 Opening BINARY mode data connection for file1 (16 bytes).
21	5.691391015	10.1.1.1	10.4.4.1	FTP	90	Response: 226 Transfer complete.
29	15.928607874	10.4.4.1	10.1.1.1	FTP	88	Request: PORT 10,4,4,1,162,43
30	15.928821396	10.1.1.1	10.4.4.1	FTP	117	Response: 200 PORT command successful. Consider using PASV.
32	15.929049275	10.4.4.1	10.1.1.1	FTP	78	Request: RETR file2
36	15.930635939	10.1.1.1	10.4.4.1	FTP	133	Response: 150 Opening BINARY mode data connection for file2 (142144 bytes).
218	15.936052844	10.1.1.1	10.4.4.1	FTP	90	Response: 226 Transfer complete.
223	18.170128407	10.4.4.1	10.1.1.1	FTP	72	Request: QUIT
224	18.170310175	10.1.1.1	10.4.4.1	FTP	80	Response: 221 Goodbye.
245	41.426636500	10.1.1.1	10.3.3.3	FTP	86	Response: 220 (vsFTPd 3.0.3)
249	43.571628342	10.3.3.3	10.1.1.1	FTP	77	Request: USER core
251	43.576479106	10.1.1.1	10.3.3.3	FTP	100	Response: 331 Please specify the password.
255	45.812332889	10.3.3.3	10.1.1.1	FTP	77	Request: PASS core
257	45.826171380	10.1.1.1	10.3.3.3	FTP	89	Response: 230 Login successful.
260	46.045173745	10.3.3.3	10.1.1.1	FTP	72	Request: SYST
262	46.045714290	10.1.1.1	10.3.3.3	FTP	85	Response: 215 UNIX Type: L8
267	50.703946170	10.3.3.3	10.1.1.1	FTP	80	Request: CWD /srv/ftp
268	50.704249870	10.1.1.1	10.3.3.3	FTP	103	Response: 250 Directory successfully changed.
275	58.878272433	10.3.3.3	10.1.1.1	FTP	74	Request: TYPE I
276	58.878477884	10.1.1.1	10.3.3.3	FTP	97	Response: 200 Switching to Binary mode.
278	59.099764461	10.3.3.3	10.1.1.1	FTP	89	Request: PORT 10,3,3,3,168,191
279	59.100257866	10.1.1.1	10.3.3.3	FTP	117	Response: 200 PORT command successful. Consider using PASV.
281	59.106223457	10.3.3.3	10.1.1.1	FTP	78	Request: RETR file1
285	59.113932994	10.1.1.1	10.3.3.3	FTP	129	Response: 150 Opening BINARY mode data connection for file1 (16 bytes).
293	59.121104201	10.1.1.1	10.3.3.3	FTP	90	Response: 226 Transfer complete.
303	71.113518498	10.3.3.3	10.1.1.1	FTP	89	Request: PORT 10,3,3,3,135,231
304	71.114251442	10.1.1.1	10.3.3.3	FTP	117	Response: 200 PORT command successful. Consider using PASV.
305	71.119658218	10.3.3.3	10.1.1.1	FTP	78	Request: RETR file2
309	71.127066528	10.1.1.1	10.3.3.3	FTP	133	Response: 150 Opening BINARY mode data connection for file2 (142144 bytes).
459	71.164007518	10.1.1.1	10.3.3.3	FTP	90	Response: 226 Transfer complete.
469	75.990586775	10.3.3.3	10.1.1.1	FTP	72	Request: QUIT
470	75.990878687	10.1.1.1	10.3.3.3	FTP	80	Response: 221 Goodbye.

Figura 13: Captura do wireshark

3.4.2 iii)

Tempo do finish ack do cliente com o ultimo pacote - Tempo FTP Request = tempo que demora ao ficheiro a ser entregue. Isto no ftp.pcapng.

Laptop1:

- file1: $5.691060937 - 5.689666433 = 0.001394504s$
No. 10 - 19
- file2: $15.935854187 - 15.929049275 = 0.006804912s$
No. 216 - 32

Corvo:

- file1 : $59.120208049 - 59.106223457 = 0.013984592s$
No. 289 - 281

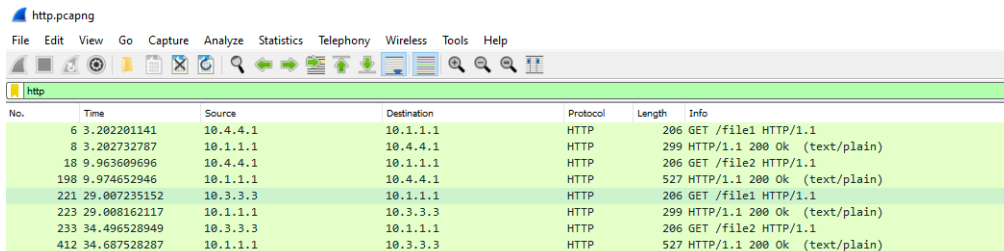
- file2: 15.205868935-14.005765403 = 1.200103532s
No. 537 - 17

Corvo:

- file1 : 40.437013071-40.430254907 = 0.006758164s
No. 594 - 590
- file2 : 48.751033743-46.775804624 = 1.975229119s
No. 12557 - 603

3.6 HTTP

3.6.1 ii)



No.	Time	Source	Destination	Protocol	Length	Info
6	3.202201141	10.4.4.1	10.1.1.1	HTTP	206	GET /file1 HTTP/1.1
8	3.202732787	10.1.1.1	10.4.4.1	HTTP	299	HTTP/1.1 200 OK (text/plain)
18	9.963609696	10.4.4.1	10.1.1.1	HTTP	206	GET /file2 HTTP/1.1
198	9.974652946	10.1.1.1	10.4.4.1	HTTP	527	HTTP/1.1 200 OK (text/plain)
221	29.007235152	10.3.3.3	10.1.1.1	HTTP	206	GET /file1 HTTP/1.1
223	29.008162117	10.1.1.1	10.3.3.3	HTTP	299	HTTP/1.1 200 OK (text/plain)
233	34.496528949	10.3.3.3	10.1.1.1	HTTP	206	GET /file2 HTTP/1.1
412	34.687528287	10.1.1.1	10.3.3.3	HTTP	527	HTTP/1.1 200 OK (text/plain)

Figura 15: wget dos 2 files a partir dos 2 clientes

3.6.2 iii)

Como utilizamos o wget como cliente temos que ignorar os primeiros pacotes que servem para estabelecer a conexão.

Tempo do finish ack do cliente com o ultimo pacote - Tempo HTTP get = tempo que demora ao ficheiro a ser entregue. Isto no http.pcapng.

Laptop1:

- file1: 3.203568160-3.202201141 = 0.001367019s
No. 9 - 6
- file2: 9.975453863-9.963609696 = 0.011844167s
No. 203 - 15

Corvo:

- file1 : 29.014536911-29.007235152 = 0.007301759s
No. 224 - 221
- file2 : 34.693224152-34.496528949 = 0.196695203s
No. 415 - 223

4 *Conclusão*

Com este trabalho podemos observar os diferentes comportamentos dos vários protocolos, de aplicação e transporte, de forma a compreendê-los melhor. Para tal, foram realizados vários testes através do core, e juntamente com o Wireshark, pudemos acompanhar todo o processo de transferência de dados.

Em suma, esta fase do trabalho ajudou a aprimorar os conhecimentos que o grupo tinha acerca dos diferentes protocolos de aplicação e de transporte dadas nesta Unidade Curricular, caso queiramos transferir dados optaremos por escolher o ssh uma vez que os pacotes vão encriptados.