

Universidade do Minho
Escola de Engenharia

CIBERSEGURANÇA

TP4 - ANÁLISE DE TRÁFEGO

Autores:

Inês Barreira Marques - a84913@alunos.uminho.pt

José Carlos Peixoto Ferreira - a85497@alunos.uminho.pt

Marcos Alexandre Ferreira Martins - a84481@alunos.uminho.pt

Rui Filipe Ribeiro Freitas - pg47639@alunos.uminho.pt

Tiago João Pereira Ferreira - pg47692@alunos.uminho.pt

30 de abril de 2022

Índice

1	Home net=193.137.8.0/24	3
2	Estratégia de análise	3
2.1	Descoberta de informação relativas aos IPs	3
2.2	Análise dos pacotes	3
2.3	Estatísticas da captura de tráfego	4
3	Síntese de análise	5
3.1	TCP	5
3.2	UDP	16
3.3	ICMP	18
3.4	Tráfego Residual	19
3.5	Análise Geral	19

Lista de Figuras

1	Informações sobre os endereços IP.	3
2	Conteúdo dos pacotes trocados.	4
3	Tráfego Residual.	19
4	Mapa das localizações IP.	19
5	Gráfico com a captura de tráfego.	20
6	Gráfico com a captura de tráfego.	21
7	Informações extra (1).	21
8	Informações extra (2).	21
9	Tentativa de login	22

Lista de Tabelas

1	TCP Streams	5
1	TCP Streams	6
1	TCP Streams	7
1	TCP Streams	8
1	TCP Streams	9
1	TCP Streams	10
1	TCP Streams	11
1	TCP Streams	12
1	TCP Streams	13
1	TCP Streams	14
1	TCP Streams	15
1	TCP Streams	16
2	UDP Streams	16
2	UDP Streams	17
2	UDP Streams	18
3	ICMP Streams	18

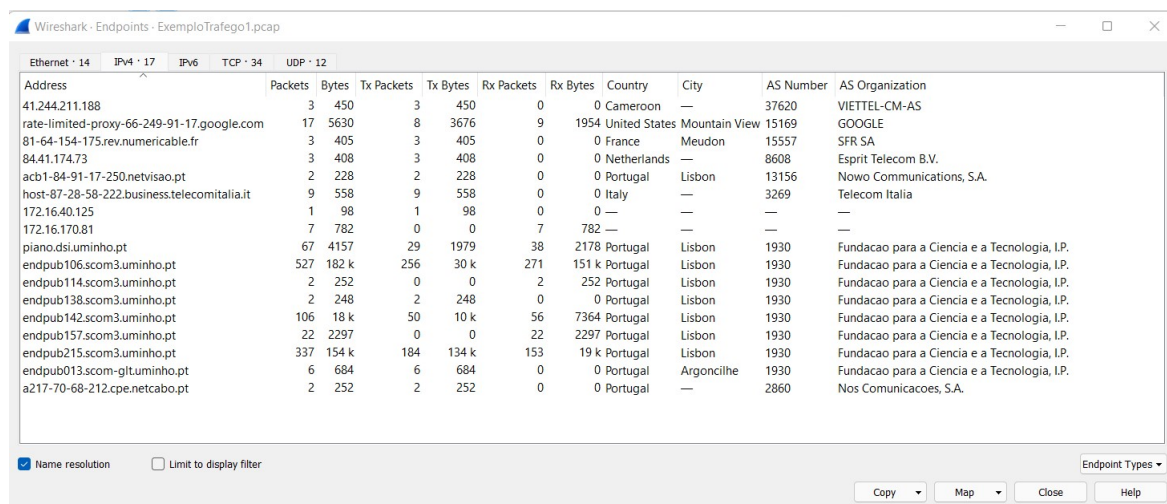
1 Home net=193.137.8.0/24

Através da análise do tráfego foi possível concluir que o tráfego foi capturado muito provavelmente através do IP 193.137.8.106 visto ser o endpoint com o maior número de pacotes a serem transmitidos/recebidos. Como na lista de endpoints é possível observar outros IPs começados por 193.137.8.x, isto leva a crer que a rede local nesta captura era de facto a rede 193.137.8.0/24.

2 Estratégia de análise

2.1 Descoberta de informação relativas aos IPs

Inicialmente foi necessário descobrir todos os endereços IP envolvidos na troca de pacotes a analisar e as suas respetivas informações. De modo a obter essas informações sobre os IPs foi utilizada a ferramenta *Statistics -> Endpoints* no *Wireshark*. Relativamente à obtenção de informações mais detalhadas sobre os IPs, como o país, a cidade e o número do AS foi acedida uma base de dados disponibilizada pela empresa MaxMind. De seguida é apresentada uma captura de ecrã com os resultados obtidos.



Wireshark - Endpoints - ExemploTrafego1.pcap

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
41.244.211.188	3	450	3	450	0	0	Cameroon	—	37620	VIETTEL-CM-AS
rate-limited-proxy-66-249-91-17.google.com	17	5630	8	3676	9	1954	United States	Mountain View	15169	GOOGLE
81-64-154-175.rev.numericable.fr	3	405	3	405	0	0	France	Meudon	15557	SFR SA
84.41.174.73	3	408	3	408	0	0	Netherlands	—	8608	Esprit Telecom B.V.
acb1-84-91-17-250.netvisao.pt	2	228	2	228	0	0	Portugal	Lisbon	13156	Nowo Communications, S.A.
host-87-28-58-222.business.telecomitalia.it	9	558	9	558	0	0	Italy	—	3269	Telecom Italia
172.16.40.125	1	98	1	98	0	0	—	—	—	—
172.16.170.81	7	782	0	0	7	782	—	—	—	—
piano.dsi.uminho.pt	67	4157	29	1979	38	2178	Portugal	Lisbon	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub106.scom3.uminho.pt	527	182 k	256	30 k	271	151 k	Portugal	Lisbon	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub114.scom3.uminho.pt	2	252	0	0	2	252	Portugal	Lisbon	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub138.scom3.uminho.pt	2	248	2	248	0	0	Portugal	Lisbon	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub142.scom3.uminho.pt	106	18 k	50	10 k	56	7364	Portugal	Lisbon	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub157.scom3.uminho.pt	22	2297	0	0	22	2297	Portugal	Lisbon	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub215.scom3.uminho.pt	337	154 k	184	134 k	153	19 k	Portugal	Lisbon	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
endpub013.scom-glt.uminho.pt	6	684	6	684	0	0	Portugal	Argoncilhe	1930	Fundacao para a Ciencia e a Tecnologia, I.P.
a217-70-68-212.cpe.netcabo.pt	2	252	2	252	0	0	Portugal	—	2860	Nos Comunicacoes, S.A.

☒ Name resolution
 ☐ Limit to display filter

Endpoint Types ▾

Copy Map Close Help

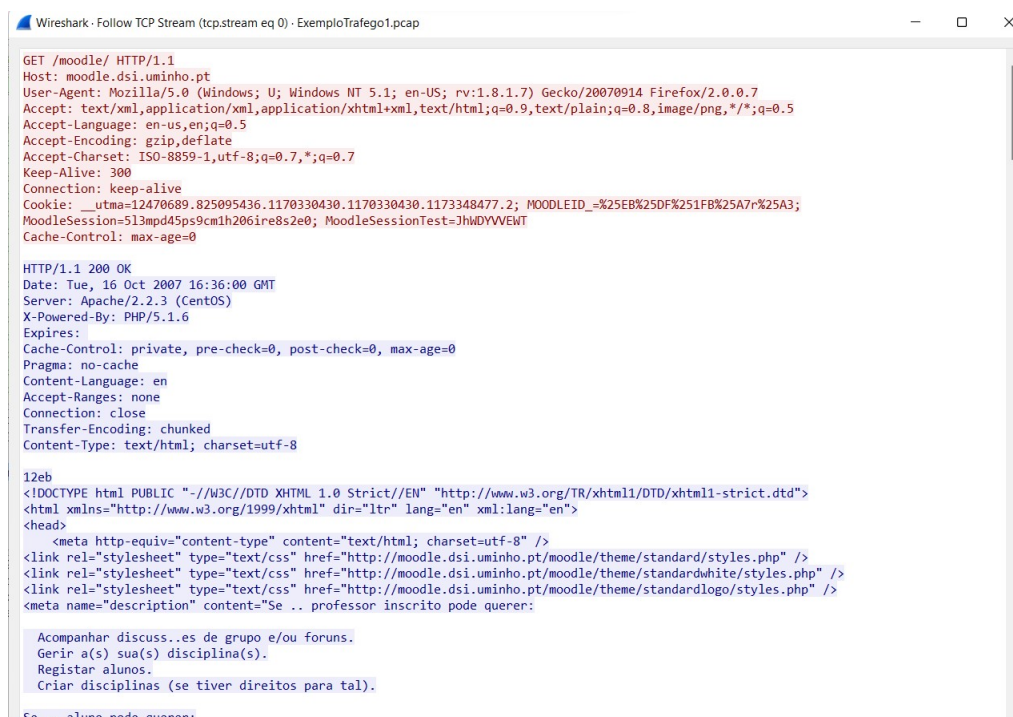
Figura 1: Informações sobre os endereços IP.

2.2 Análise dos pacotes

Após obtida a informação sobre os IPs o grupo passou à análise de pacotes em que foi dividido o trabalho de modo a tornar a realização mais eficiente. A análise começou com as

streams TCP com o trabalho a ser dividido de igual forma pelo grupo de modo a que cada elemento fizesse a análise de 5 streams TCP das 25 totais. De seguida foi necessário realizar a análise de pacotes UDP, ICMP e dos restantes sendo que como se tratavam de um menor número de pacotes esta análise foi realizada em conjunto pelo grupo. De salientar que para a realização desta secção foi necessário algum estudo do funcionamento do Wireshark de modo a sermos mais eficientes na realização da procura de streams.

Tanto nas streams TCP como UDP é possível filtrar de modo a obter a conversação total entre 2 endpoints como demonstrado de seguida.



```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · ExemploTrafego1.pcap

GET /moodle/ HTTP/1.1
Host: moodle.dsi.uminho.pt
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.7) Gecko/20070914 Firefox/2.0.0.7
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: utma=12470689.825095436.1170330430.1170330430.1173348477.2; MOODLEID_=%25EB%25DF%251FB%25A7r%25A3; MoodleSession=513mpd45ps9cm1h206ire8s2e0; MoodleSessionTest=JhMDVVWENT
Cache-Control: max-age=0

HTTP/1.1 200 OK
Date: Tue, 16 Oct 2007 16:36:00 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Expires:
Cache-Control: private, pre-check=0, post-check=0, max-age=0
Pragma: no-cache
Content-Language: en
Accept-Ranges: none
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

12eb
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en" xml:lang="en">
<head>
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<link rel="stylesheet" type="text/css" href="http://moodle.dsi.uminho.pt/moodle/theme/standard/styles.php" />
<link rel="stylesheet" type="text/css" href="http://moodle.dsi.uminho.pt/moodle/theme/standardwhite/styles.php" />
<link rel="stylesheet" type="text/css" href="http://moodle.dsi.uminho.pt/moodle/theme/standardlogo/styles.php" />
<meta name="description" content="Se .. professor inscrito pode querer:
Acompanhar discussões de grupo e/ou foruns.
Gerir a(s) sua(s) disciplina(s).
Registrar alunos.
Criar disciplinas (se tiver direitos para tal).
Se .. aluno pode querer:"

```

Figura 2: Conteúdo dos pacotes trocados.

Através da análise da figura 2, é possível obter o conteúdo dos pacotes TCP trocados entre o host x (sublinhado a vermelho) e o servidor y (sublinhado a azul).

2.3 Estatísticas da captura de tráfego

Após realizada a procura e síntese de cada uma das streams e dos restantes pacotes foi possível obter alguns dados estatísticos relativamente ao tráfego em que para isso foi utilizado o menu *Statistics* do *Wireshark*. Todos estes passos anteriores serão mais aprofundados na secção seguinte.

3 Síntese de análise

3.1 TCP

Para uma melhor eficiência na procura de erros no tráfego foi necessário dividir o trabalho pelo grupo em que as 25 streams TCP foram divididas em grupos de 5 tendo sido cada grupo de streams analisado por uma pessoa diferente. Os resultados obtidos estão demonstrados na tabela seguinte.

Tabela 1: TCP Streams

Nº de Streams	Tempo (s)	Fonte/Destino	Comentário
Stream 0 Pacotes: 0-15 184-205	Início: 1.457307 Fim: 2.899311 Duração: 1.442004	Origem: endpub106.scom3.uminho.pt (porta - 1137) Destino: endpub215.scom3.uminho.pt (porta - 80)	É efetuada uma conexão TCP entre o pacote 3 e 5. No pacote 6 é realizado um pedido HTTP para aceder à página web “moodle.dsi.uminho.pt” e entre os pacotes 202 e 205 é terminada a sessão TCP. Foram transmitidos 35 pacotes com um tamanho total de 19 kBytes.
Stream 1 Pacotes: 16-166	Início: 1.789632 Fim: 2.250563 Duração: 0.4609	Origem: endpub106.scom3.uminho.pt (porta - 1138) Destino: endpub215.scom3.uminho.pt (porta - 80)	É efetuada uma conexão TCP com sucesso e em seguida é realizado um pedido HTTP do tipo GET “/moodle/theme/standard/styles.php”. O pacote 66 chegou com erros o que despoletou o envio de ACK’s e retransmissão do mesmo pacote. Podemos também verificar a existência de vários pacotes do tipo “continuation”. Isto acontece, uma vez que tipicamente os pacotes não podem exceder os 1314 bytes. Isto indica que o que estava a ser transmitido tinha um tamanho superior a 1314 bytes. Foram transmitidos 151 pacotes com um tamanho total de 109 kBytes.

Tabela 1: TCP Streams

Nº de Streams	Tempo (s)	Fonte/Destino	Comentário
Stream 2 Pacotes: 167-178	Início: 2.298130 Fim: 2.755881 Duração: 0.4578	Origem: endpub106.scom3.uminho.pt (porta - 1139) Destino: endpub215.scom3.uminho.pt (porta - 80)	É efetuada uma conexão TCP com sucesso e em seguida é realizado um pedido HTTP do tipo GET “/moodle/theme/standardwhite/styles.php”. Não foram detetados erros na receção dos dados. Foram transmitidos 12 pacotes com um tamanho total de 2337 bytes.
Stream 3 Pacotes: 179-183 206-216	Início: 2.756597 Fim: 3.180185 Duração: 0.4236	Origem: endpub106.scom3.uminho.pt (porta - 1140) Destino: endpub215.scom3.uminho.pt (porta - 80)	É efetuada uma conexão TCP com sucesso e em seguida é realizado um pedido HTTP do tipo GET “/moodle/theme/standardlogo/styles.php “. É fechada a conexão depois de transmitida a informação, no entanto são recebidos dois pacotes com ACK's duplicados (213 e 214), o que faz com que sejam enviados dois pacotes do tipo RST (215 e 216). Foram transmitidos 16 pacotes com um tamanho total de 2176 bytes.
Stream 4 Pacotes: 217-226	Início: 3.18662 Fim: 3.214152 Duração: 0.0275	Origem: endpub106.scom3.uminho.pt (porta - 1141) Destino: endpub215.scom3.uminho.pt (porta - 80)	É efetuada uma conexão TCP com sucesso e em seguida é realizado um pedido HTTP do tipo GET “/moodle/lib/javascript-static.js “. O servidor responde com o código 304 (Not Modified), este significa que o cliente já possui uma cópia em cache do recurso que está a pedir. Foram transmitidos 10 pacotes com um tamanho total de 1409 bytes.

Tabela 1: TCP Streams

Nº de Streams	Tempo (s)	Fonte/Destino	Comentário
Stream 5 Pacotes: 227-233 237 238	Início: 3.222860 Fim: 3.531489 Duração: 0.3086	Origem: endpub106.scom3.uminho.pt (porta - 1142) Destino: endpub215.scom3.uminho.pt (porta - 80)	É estabelecida uma conexão TCP do pacote 227 ao 229 através de um <i>Three-way Handshake</i> . No pacote 230 é feito um pedido HTTP GET "moodle/lib/javascript-mod.php HTTP/1.1" e a resposta é enviada no pacote 230 do tipo "HTTP 200 OK". Os pacotes 233, 237 e 238 são para o encerramento da ligação. Não ocorreram erros nesta stream e foram transmitidos 9 pacotes com um total de 1503 bytes.
Stream 6 Pacotes: 234-236 239-245	Início: 3.222860 Fim: 3.544831 Duração: 0.321971	Origem: endpub106.scom3.uminho.pt (porta - 1143) Destino: endpub215.scom3.uminho.pt (porta - 80)	É estabelecida uma conexão TCP do pacote 234 ao 236 através de um <i>Three-way Handshake</i> . No pacote 239 é feito um pedido HTTP GET "moodle/lib/overlib.js HTTP/1.1" e a resposta é enviada no pacote 241 do tipo "HTTP/1.1 Not Modified". Do pacote 242 ao 245 são para o encerramento da ligação. Não há ocorrência de erros nesta stream e foram transmitidos 10 pacotes com um total de 1399 bytes.
Stream 7 Pacotes: 246-255	Início: 1.457307 Fim: 2.899311 Duração: 1.442004	Origem: endpub106.scom3.uminho.pt (porta - 1144) Destino: endpub215.scom3.uminho.pt (porta - 80)	É estabelecida uma conexão TCP do pacote 246 ao 248 através de um <i>Three-way Handshake</i> . No pacote 249 é feito um pedido HTTP GET "moodle/lib/-cookies.js HTTP/1.1" e a resposta é enviada no pacote 251 do tipo "HTTP/1.1 Not Modified". Os pacotes 252, 253, 254 e 255 são para o encerramento da ligação. Não há ocorrência de erros nesta stream, foram transmitidos 10 pacotes com um total de 1397 bytes.

Tabela 1: TCP Streams

Nº de Streams	Tempo (s)	Fonte/Destino	Comentário
Stream 8 Pacotes: 256-265	Início: 3.617197 Fim: 3.648826 Duração: 0.031629	Origem: endpub106.scom3.uminho.pt (porta - 1145) Destino: endpub215.scom3.uminho.pt (porta - 80)	É estabelecida uma conexão TCP do pacote 256 ao 258 através de um <i>Three-way Handshake</i> . No pacote 270 é feito um pedido HTTP GET "moodle/lib/ufo.js HTTP/1.1" e a resposta é enviada no pacote 261 do tipo "HTTP/1.1 Not Modified". Do pacote 262 ao 265 são para o encerramento da ligação. Não há ocorrência de erros nesta stream e foram transmitidos 10 pacotes com um total de 1395 bytes.
Stream 9 Pacotes: 266-271 274-276 278 280	Início: 3.663604 Fim: 3.713998 Duração: 0.050394	Origem: endpub106.scom3.uminho.pt (porta - 1146) Destino: endpub215.scom3.uminho.pt (porta - 80)	É estabelecida uma conexão TCP nos pacotes 266, 268 e 269 através de um <i>Three-way Handshake</i> . No pacote 270 é feito um pedido HTTP GET "moodle/theme/standardlogo/logo.gif HTTP/1.1" e a resposta é enviada no pacote 274 do tipo "HTTP/1.1 Not Modified". Os pacotes 275, 276, 278 e 280 são para o encerramento da ligação. Não há ocorrência de erros nesta stream, foram transmitidos 10 pacotes com um total de 1428 bytes transmitidos.
Stream 10 Pacotes: 267, 272, 273, 277, 279, 281, 282, 284, 285, 286	Início: 3.675176 Fim: 3.722428 Duração: 0.047252	Origem: endpub106.scom3.uminho.pt (porta - 1147) Destino: endpub215.scom3.uminho.pt (porta - 80)	É estabelecida uma conexão TCP recorrendo a um Three Way Handshake, sucede-se de um pedido GET do protocolo HTTP a "/moodle/pix/spacer.gif". Recebe uma resposta HTTP 200 OK demonstrando assim que não ocorreu erros. Após isto é finalizada a conexão sem problemas. Nesta conexão foram enviados 10 pacotes com um total de 1555 bytes. Os protocolos usados nesta conexão foram a Ethernet, o IP, o TCP, o HTTP e o Compuserve GIF.

Tabela 1: TCP Streams

Nº de Streams	Tempo (s)	Fonte/Destino	Comentário
Stream 11 Pacotes: 283, 288, 289, 291, 293, 295- 300, 302	Início: 3.716224 Fim: 3.771711 Duração: 0.055487	Origem: endpub106.scom3.uminho.pt (porta - 1148) Destino: endpub215.scom3.uminho.pt (porta - 80)	É estabelecida uma conexão TCP através de um Three-way handshake, sucede-se um pedido GET do protocolo HTTP a "/moodle/calendar/overlib.cfg.php". Recebe uma resposta do tipo HTTP 200 OK, verificando que não ocorreu erros. Ao contrário da stream 10, encontra-se um pacote que contém a flag [PSH,ACK] indicando que o pacote contém o final do conteúdo pedido. Após isto é finalizada a conexão sem problemas. Nesta conexão são enviados 12 pacotes com um total de 1726 bytes. Os protocolos usados nesta conexão foram o Ethernet, o IP, o TCP, o HTTP e o Line-based text data.
Stream 12 Pacotes: 287, 290, 292, 294, 301, 303, 304, 306- 308	Início: 3.722807 Fim: 3.779233 Duração: 0.0566426	Origem: endpub106.scom3.uminho.pt (porta - 1149) Destino: endpub215.scom3.uminho.pt (porta - 80)	É estabelecida uma conexão TCP através de um Three-way handshake, sucede-se um pedido GET do protocolo HTTP a "/moodle/theme/standardwhite/gradient.jpg". Recebe uma resposta HTTP 200 OK demonstrando assim que não ocorreu erros. Após isto é finalizada a conexão sem problemas. Nesta conexão são enviados 10 pacotes com um total de 1939 bytes. Os protocolos usados nesta conexão foram a Ethernet, o IP, o TCP, o HTTP e o JPEG File Interchange Format.

Tabela 1: TCP Streams

Nº de Streams	Tempo (s)	Fonte/Destino	Comentário
Stream 13 Pacotes: 305, 310-313, 317-320, 322	Início: 3.775350 Fim: 3.882527 Duração: 0.107177	Origem: endpub106.scom3.uminho.pt (porta - 1150) Destino: endpub215.scom3.uminho.pt (porta - 80)	É estabelecida uma conexão TCP através de um Three-way handshake, sucede-se um pedido GET do protocolo HTTP a "/moodle/pix/t/switch_minus.gif". Recebe uma resposta HTTP 200 OK demonstrando assim que não ocorreu erros. Após isto é finalizada a conexão sem problemas. Nesta conexão são enviados 10 pacotes com um total de 1667 bytes. Os protocolos usados nesta conexão foram a Ethernet, o IP, o TCP, o HTTP e o Compuserve GIF.
Stream 14 Pacotes: 309, 314-316, 321, 323, 324, 326-328	Início: 3.782558 Fim: 3.889159 Duração: 0.106601	Origem: endpub106.scom3.uminho.pt (porta - 1151) Destino: endpub215.scom3.uminho.pt (porta - 80)	É estabelecida uma conexão TCP através de um Three-way handshake, sucede-se um pedido GET do protocolo HTTP a "moodle/pix/s/biggrin.gif". Recebe uma resposta HTTP 200 OK demonstrando assim que não ocorreu erros. Após isto é finalizada a conexão sem problemas. Nesta conexão são enviados 12 pacotes com um total de 1746 bytes. Os protocolos usados nesta conexão foram a Ethernet, o IP, o TCP, o HTTP e o Compuserve GIF.
Stream 15 Pacotes: 325, 329-339	Início: 3.885260 Fim: 3.90386 Duração: 0.0186	Origem: endpub106.scom3.uminho.pt (porta - 1152) Destino: endpub215.scom3.uminho.pt (porta - 80)	É estabelecida uma conexão TCP através de um Three-way handshake, sucede-se um pedido GET do protocolo HTTP a "moodle/pix/s/moodlelogo.gif". Recebe uma resposta HTTP 200 OK demonstrando assim que não ocorreu erros. Após isto é finalizada a conexão sem problemas. Nesta conexão são enviados 12 pacotes com um total de 4239 bytes. Os protocolos usados nesta conexão foram a Ethernet, o IP, o TCP, o HTTP e o Compuserve GIF.

Tabela 1: TCP Streams

Nº de Streams	Tempo (s)	Fonte/Destino	Comentário
Stream 16 Pacotes: 340- 347,425	Início: 17.040244 Fim: 82.494244 Duração: 65.4540	Origem: endpub106.scom3.uminho.pt (porta - 1153) Destino: rate-limited-proxy-66-249-91- 17.google.com (porta - 80)	<p>É estabelecida uma conexão TCP através de um Three-way handshake, sucede-se um pedido HTTP do tipo GET a "/mail/?ui=pb&tl=115a67ba1f3".</p> <p>Pelo facto de não existir nenhum tipo de segurança, é possível encontrar um endereço de e-mail "eu.nuno@gmail.com". É recebida uma resposta do tipo HTTP 200 OK. Por fim a conexão é interrompida com um pacote RST o que pode significar que um dos intervenientes pode ter ido a baixo. Nesta conexão são enviados 9 pacotes com um total de 2842 bytes.</p>
Stream 17 Pacotes: 352-356, 359-361, 368-373	Início: 23.819398 Fim: 35.186798 Duração: 11.3674	Origem: endpub106.scom3.uminho.pt (porta - 1154) Destino: piano.dsi.uminho.pt (porta - 21)	<p>É estabelecida uma conexão TCP através de um Three-way handshake, sucede-se de um pedido FTP ao servidor "piano.dsi.uminho.pt". O servidor responde com o código 220 mostrando-se disponível. O cliente faz um pedido de login com um utilizador anonymous, sendo este utilizador predefinido dos servidores FTP, tendo como resposta do servidor ao utilizador como desconhecido, encerrando a comunicação. Pode-se portanto concluir que o servidor está protegido contra tentativas de adivinhar as credenciais originais. Nesta conexão são enviados 14 pacotes com um total de 918 bytes.</p>

Tabela 1: TCP Streams

Nº de Streams	Tempo (s)	Fonte/Destino	Comentário
Stream 18 Pacotes: 375-400, 403-424, 426-431	Início: 54.25406 Fim: 82.846006 Duração: 28.5886	Origem: endpub106.scom3.uminho.pt (porta - 1156) Destino: piano.dsi.uminho.pt (porta - 23)	É estabelecida uma conexão TCP através de um Three-way handshake. Sucede-se uma conexão TELNET ao servidor "piano.dsi.uminho.pt". Este protocolo concede uma forma de aceder a um terminal remotamente através da rede. É enviado um pacote TCP Keep-Alive para manter a conexão ativa. É verificada uma tentativa de login por parte do cliente com o username guest, existindo retransmissão dos pacotes devido a segmentos ACK não capturados. É enviada a password byte a byte, porém esta está incorreta e o servidor envia uma mensagem a informar o utilizador, pedindo novas credenciais. Por fim o cliente envia um "." em que o servidor responde com um "^ D" e a conexão termina. Nesta conexão são enviados 53 pacotes com um total de 3239 bytes.
Stream 19 Pacotes: 435,437,442	Início: 97.0018824 Fim: 106.000724 Duração: 8.9989	Origem: host-87-28-58-222.business.telecomitalia.it (porta - 11132) Destino: endpub157.scom3.uminho.pt (porta - 30797)	Um dispositivo, com o endereço 87.28.58.222, da empresa Telecom Itália tenta iniciar uma conexão TCP com o servidor de endereço 193.137.8.157 com um envio de um SYN. Não obtendo resposta do servidor, é retransmitido o SYN mais duas vezes. Nesta conexão são enviados 3 pacotes com um total de 186 bytes.

Tabela 1: TCP Streams

Nº de Streams	Tempo (s)	Fonte/Destino	Comentário
Stream 20 Pacotes: 436, 439 e 444	Início: 98.607890 Fim: 107.601622 Duração: 8.993732	Origem: host-87-28-58-222.business.telecomitalia.it (porta - 11139) Destino: endpub157.scom3.uminho.pt (porta - 443)	O endereço de origem é um dispositivo da empresa Telecomitalia que tenta iniciar uma conexão TCP através de um [SYN] com o servidor endpub157.scom3.uminho.pt sendo que não é obtida resposta e por isso continua a fazer pedidos de retransmissão (TCP Retransmission). Foram transmitidos 3 pacotes com um total de 186 bytes.
Stream 21 Pacotes: 438, 440 e 446	Início: 100.221796 Fim: 109.203745 Duração: 8.981949	Origem: host-87-28-58-222.business.telecomitalia.it (porta - 11141) Destino: endpub157.scom3.uminho.pt (porta - 80)	O endereço de origem é um dispositivo da empresa Telecomitalia que tenta iniciar uma conexão TCP através de um [SYN] com o servidor endpub157.scom3.uminho.pt sendo que não é obtida resposta e por isso continua a fazer pedidos de retransmissão (TCP Retransmission). Foram transmitidos 3 pacotes com um total de 186 bytes. Estas ultimas 3 streams (19,20 e 21) correspondem todas a tentativas de conexão TCP por parte de um dispositivo da Telecomitalia que não foram bem sucedidas provavelmente devido a inatividade por parte do servidor da uminho.

Tabela 1: TCP Streams

Nº de Streams	Tempo (s)	Fonte/Destino	Comentário
Stream 22 Pacotes: 451 - 458	Início: 137.534994 Fim: 137.997816 Duração: 0.462822	Origem: endpub106.scom3.uminho.pt (porta - 1157) Destino: rate-limited-proxy-66-249-91-17.google.com (porta - 80)	Esta stream começa com um pedido de conexão com o envio de um pacote [SYN] da origem para o destino e o respetivo [SYN,ACK] de volta assim como o respetivo envio [ACK] que dá por concluído o 3-way handshake. Após isso é realizado um pedido GET de uma página HTTP onde é possível observar um pedido de um utilizador com o mail "eu.nuno@gmail.com". Para além disso, é também possível visualizar algumas das mensagens trocadas, isto pois é utilizado HTTP e não HTTPS que não permite a encriptação do conteúdo da página. De salientar que a conexão não é terminada sendo esta uma vulnerabilidade. Foram transmitidos 8 pacotes com um total de 2788 bytes.

Tabela 1: TCP Streams

Nº de Streams	Tempo (s)	Fonte/Destino	Comentário
Stream 23 Pacotes: 461, 463, 465, 466, 468, 470- 539, 541- 563	Início: 143.664551 Fim: 152.818884 Duração: 9.154333	Origem: endpub106.scom3.uminho.pt (porta - 1158) Destino: endpub142.scom3.uminho.pt (porta - 445)	Nesta stream é realizada uma sessão SMB(Server Message Block), um protocolo de partilha de ficheiros. Deste modo é possível fazer com que o cliente possa criar, alterar e ler ficheiros de um servidor que aloja esses ficheiros. É normalmente utilizado por sistemas operativos Windows sendo que é vulnerável a vários tipos de ataques. Através da análise individual dos pacotes foi possível observar 2 casos interessantes, um no pacote 472 com a tentativa de login com o user "(root) na diretoria "\\TROMBONE\IPC\$"com a tentativa a ser recusada no pacote 475. Outro caso foi no pacote 480 com a tentativa de login com o user "BOCASJNR\hsantos"na diretoria "\\TROMBONE\SOFT"tentando aceder ao ficheiro "Auto-Run.inf"(demonstrado no pacote 484). Esta tentativa foi no entanto recusada como demonstrado no pacote 485 com uma mensagem de erro. Para além disso ocorreram também perdas de pacotes assim como retransmissões com TCP Retransmission. Foram transmitidos 98 pacotes com um total de 17k bytes.

Tabela 1: TCP Streams

Nº de Streams	Tempo (s)	Fonte/Destino	Comentário
Stream 24 Pacotes: 464, 467 e 469	Início: 143.676901 Fim: 143.720977 Duração: 0.044076	Origem: endpub106.scom3.uminho.pt (porta - 1159) Destino: endpub142.scom3.uminho.pt (porta - 139)	Nesta stream ocorreu uma tentativa de ligação entre o host endpub106.scom3.uminho.pt com o serviço endpub142.scom3.uminho.pt com o envio do pacote 464 que é um pacote [SYN] e recebe um pacote [SYN,ACK]. No entanto acaba por enviar um pacote [RST] encerrando a conexão da porta 139. Foram transmitidos 3 pacotes com um total de 178 bytes.

3.2 UDP

Relativamente ao tráfego UDP, como este se tratava de um número reduzido de pacotes, a captura foi realizada em grupo visto que assim também era possível haver uma maior concordância sobre o que era encontrado. Os resultados obtidos na captura deste tráfego estão representados na tabela que se segue.

Tabela 2: UDP Streams

Nº de Streams	Tempo	Fonte/Destino	Comentário
Stream 0 Pacotes: 348, 350	Início: 23.779650 Fim: 23.792078 Duração: 0.012428	Origem: endpub106.scom3.uminho.pt (porta - 1030) Destino: endpub142.scom3.uminho.pt (porta - 53)	Foi realizado um pedido DNS pelo host (endpub106.scom3.uminho.pt) ao servidor de destino (endpub142.scom3.uminho.pt) para este devolver o ip correspondente ao domain name "piano.dsi.uminho.pt" em que este responde com o IP "193.137.8.95". Foram transmitidos 2 pacotes com um total de 174 bytes.

Tabela 2: UDP Streams

Nº de Streams	Tempo	Fonte/Destino	Comentário
Stream 1 Pacotes: 357, 358 e 359	Início: 25.535682 Fim: 31.551484 Duração: 6.015802	Origem: endpub106.scom3.uminho.pt (porta - 1030) Destino: endpub142.scom3.uminho.pt (porta - 53)	Através da análise do tráfego não foi possível chegar a qualquer conclusão relativamente aos pacotes trocados apenas que foram enviados 3 pacotes com um total de 450 bytes.
Stream 2 Pacotes: 363, 366 e 374	Início: 31.271661 Fim: 37.315007 Duração: 6.043346	Origem: 84.41.174.73 (porta - 38337) Destino: endpub157.scom3.uminho.pt (porta - 30797)	Através da análise do tráfego não foi possível chegar a qualquer conclusão relativamente aos pacotes trocados, apenas que foram enviados 3 pacotes com um total de 408 bytes.
Stream 3 Pacotes: 364 e 367	Início: 31.279818 Fim: 33.316836 Duração: 2.037018	Origem: a217-70-68- 212.cpe.netcabo.pt (porta - 59342) Destino: endpub114.scom3.uminho.pt (porta - 23897)	Através da análise do tráfego não foi possível chegar a qualquer conclusão relativamente aos pacotes trocados, apenas que foram enviados 2 pacotes com um total de 252 bytes.
Stream 4 Pacotes: 433 e 434	Início: 93.723027 Fim: 95.745304 Duração: 2.022277	Origem: endpub138.scom3.uminho.pt (porta - 39284) Destino: endpub157.scom3.uminho.pt (porta - 30797)	Através da análise do tráfego não foi possível chegar a qualquer conclusão relativamente aos pacotes trocados, apenas que foram enviados 2 pacotes com um total de 248 bytes.
Stream 5 Pacotes: 443 e 445	Início: 106.453435 Fim: 108.509339 Duração: 2.055904	Origem: acb1-84-91-17- 250.netvisao.pt (porta - 54035) Destino: endpub157.scom3.uminho.pt (porta - 30797)	Através da análise do tráfego não foi possível chegar a qualquer conclusão relativamente aos pacotes trocados, apenas que foram enviados 2 pacotes com um total de 228 bytes.
Stream 6 Pacotes: 447, 449 e 450	Início: 118.301230 Fim: 124.327858 Duração: 6.026628	Origem: 81-64-154- 175.rev.numericable.fr (porta - 43622) Destino: endpub157.scom3.uminho.pt (porta - 30797)	Através da análise do tráfego não foi possível chegar a qualquer conclusão relativamente aos pacotes trocados, apenas que foram enviados 3 pacotes com um total de 405 bytes.

Tabela 2: UDP Streams

Nº de Streams	Tempo	Fonte/Destino	Comentário
Stream 7 Pacotes: 462	Início: 143.672084 Fim: 143.672084	Origem: endpub142.scom3.uminho.pt (porta - 137) Destino: endpub106.scom3.uminho.pt (porta - 137)	Esta stream corresponde a um pedido NBNS (NetBIOS Name Service) ao servidor endpub106.scom3.uminho.pt através do pacote 462 que serve para traduzir tal como o DNS um url no seu respetivo endereço IP. Foi transmitido apenas um pacote com 104 bytes. .

3.3 ICMP

Após termos filtrado todo o tráfego TCP e UDP foi necessário realizar a análise da captura do tráfego ICMP que é um protocolo utilizado para comunicar informações da camada de rede. Os resultados são os demonstrados de seguida.

Tabela 3: ICMP Streams

Nº de Pacotes	Tempo (s)	Fonte/Destino	Comentário
Pacotes: 1, 362, 396, 432, 448, 540	Início: 0 Fim: 150.336312 Duração: 150.336312	Origem: endpub013.scom-glt.uminho.pt Destino: 172.16.170.81	É realizado de 30 em 30 segundos um "ping request", não sendo obtida qualquer resposta.
Pacotes: 441	Início: 105.037733	Origem: 172.16.40.125 Destino: 172.16.170.81	Realizado um "ping request" sem resposta.
Pacotes: 459, 460	Início: 143.654404 Fim: 143.660955 Duração: 0.006551	Origem: endpub106.scom3.uminho.pt Destino: endpub142.scom3.uminho.pt	É realizado um "ping request" do (106) para o (142) com sucesso.

3.4 Tráfego Residual

Após termos realizado a análise de todo o tráfego TCP, UDP e ICMP foi realizado o filtro "not tcp && not udp && not icmp" de modo a filtrar os restantes pacotes. Nesta captura foi possível identificar o protocolo ARP, que é usado na conversão de endereços da camada IP em endereços MAC da camada 2. Isto é demonstrado na Figura 3 na parte das informações. Este protocolo pode ser usado por atacantes para captar tráfego através da resposta ARP.

Relativamente ao tráfego sob o protocolo LOOP é possível observar as portas que estão a enviar e a receber tráfego, sendo que este protocolo é responsável por detetar loops inesperados na rede através da receção de tráfego na mesma porta em que este foi enviado.

not tcp && not udp && not icmp						
No.	Time	Source	Destination	Protocol	Length	Info
2	1.456585	endpub215.scom3.umi...	endpub106.scom3.umi...	ARP	60	193.137.8.215 is at 00:08:02:b6:5a:a0
349	23.786302	endpub106.scom3.umi...	endpub142.scom3.umi...	ARP	42	193.137.8.106 is at 00:13:77:05:f4:c3
351	23.819171	piano.dsi.uminho.pt	endpub106.scom3.umi...	ARP	60	193.137.8.95 is at 00:00:f8:1f:3d:ce
401	68.947723	Cisco_ef:54:d9	Cisco_ef:54:d9	LOOP	60	Reply
402	69.513079	Cisco_08:d6:19	Cisco_08:d6:19	LOOP	60	Reply

Figura 3: Tráfego Residual.

3.5 Análise Geral

De forma a que fosse possível realizar uma análise geral do tráfego foram usadas as ferramentas da secção *Statistics* do *Wireshark* como os Endpoints, I/O Graph e o Capture File Properties para obtenção de dados.

No menu Endpoints, com recurso a bases de dados disponibilizadas pela empresa Max-Mind, é possível verificar quem são os intervenientes nas comunicações e a sua localização aproximada. Na figura seguinte é possível observar um mapa com as localizações dos IPs intervenientes neste captura de tráfego.

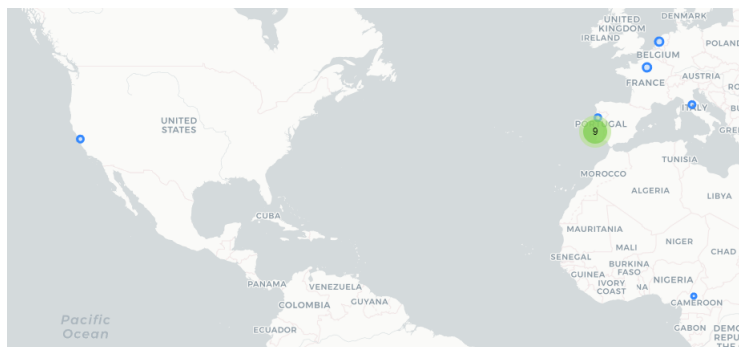


Figura 4: Mapa das localizações IP.

Na figura abaixo é possível observar a divisão de tráfego existente ao longo do tempo, sendo os pacotes TCP predominantes (a azul no gráfico). Esta divisão apresenta um número de 531 pacotes TCP, 18 UDP, 9 ICMP e por fim 3 pacotes ARP e 2 LOOP. Este gráfico serve também para situar num contexto temporal onde ocorreram os vários tipos de pacotes.

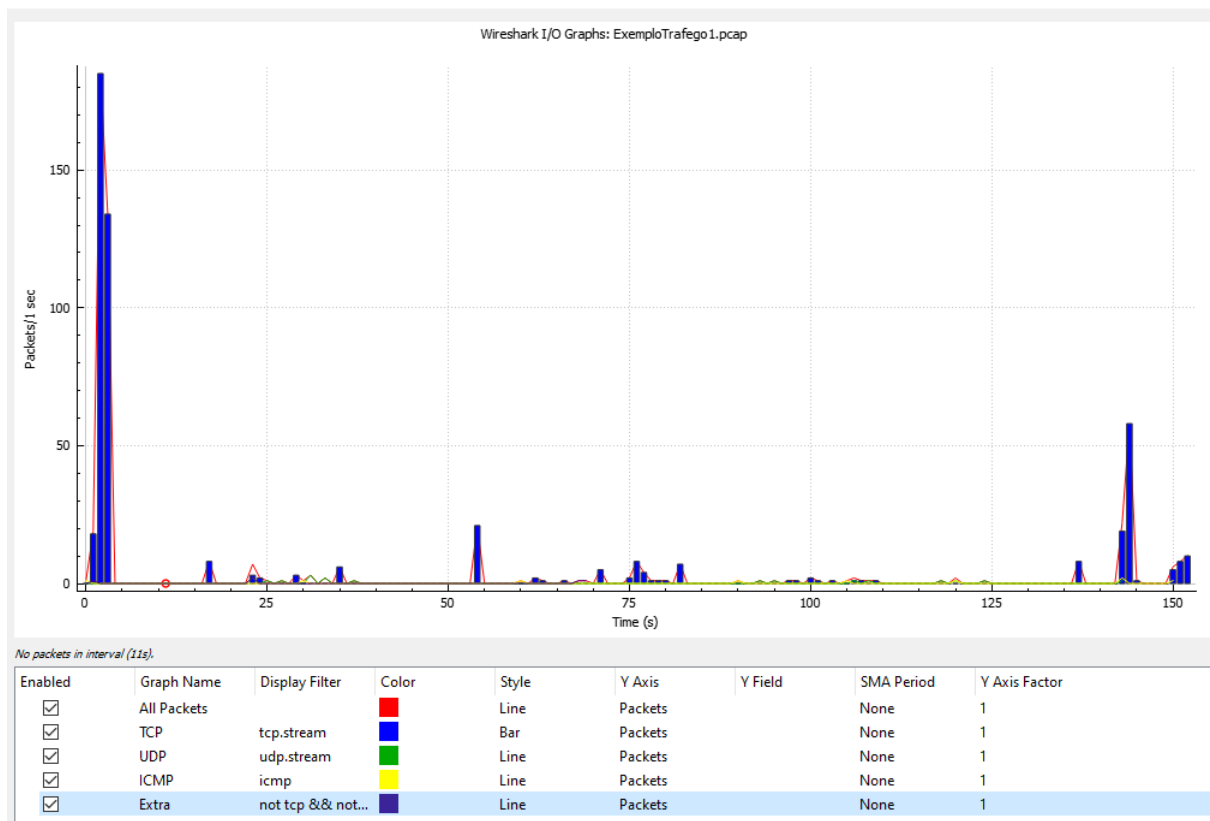


Figura 5: Gráfico com a captura de tráfego.

Para obter informações mais aprofundadas sobre os tipos de pacotes foi utilizado o menu *Statistics -> Protocol Hierarchy* cujos resultados são apresentados na próxima figura. Neste menu é possível observar as percentagens tanto de pacotes TCP como os restantes sendo que é de salientar os 94.3% de pacotes TCP. Para além disso é possível retirar ilações extras sobre o tráfego como a quantidade de bytes assim como a sua percentagem, a taxa de transferência, entre outros aspetos.

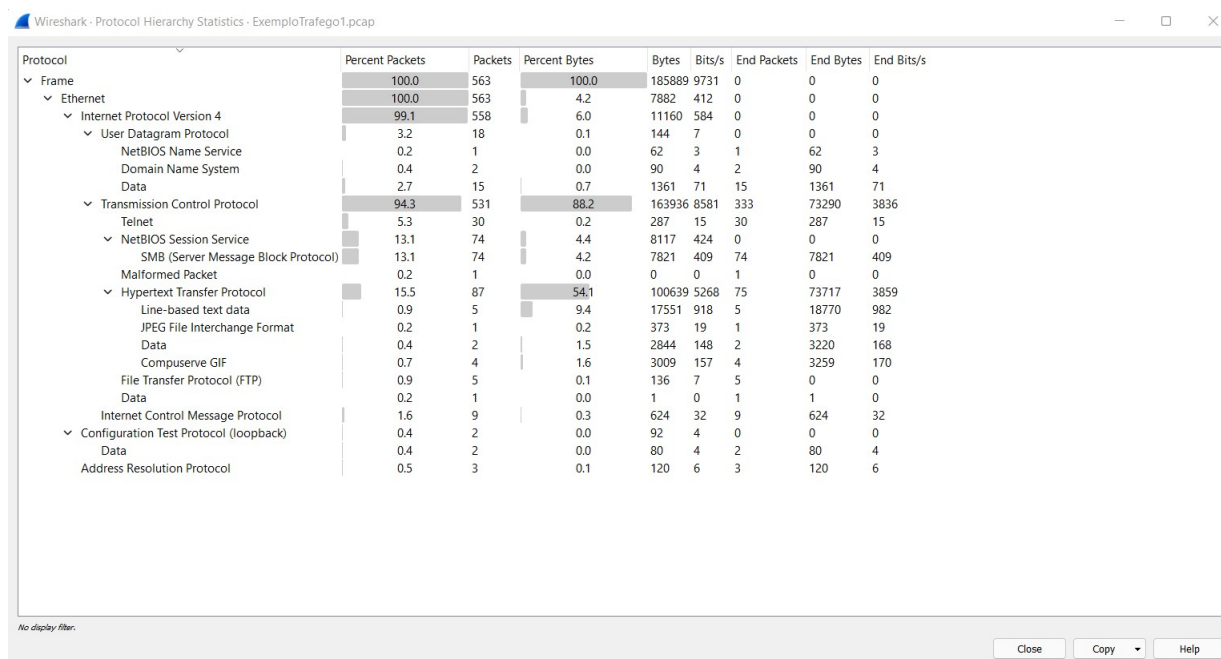


Figura 6: Gráfico com a captura de tráfego.

Ao observar o menu Capture File Properties é possível obter o número total de pacotes, o tempo decorrido neste tráfego, o débito médio, entre outros aspetos. Estas informações gerais do tráfego são apresentadas nas figuras seguintes.

Time

First packet: 2007-10-16 17:36:28
 Last packet: 2007-10-16 17:39:01
 Elapsed: 00:02:32

Figura 7: Informações extra (1).

Statistics

Measurement	Captured	Displayed	Marked
Packets	563	563 (100.0%)	—
Time span, s	152.819	152.819	—
Average pps	3.7	3.7	—
Average packet size, B	330	330	—
Bytes	185889	185889 (100.0%)	0
Average bytes/s	1216	1216	—
Average bits/s	9731	9731	—

Figura 8: Informações extra (2).

Depois de analisado o tráfego, nomeadamente em streams, foi possível concluir que se trata na maioria de streams TCP e algumas streams UDP. Dentro das streams TCP a stream 18 foi a que despertou mais interesse por parte do grupo, pois foi possível observar uma password, isto devido ao facto de o protocolo TELNET não implementar encriptação, tornando este propício a ataques.

Na figura seguinte está representada a tentativa de login efetuada na stream 18 e como se pode comprovar é possível ver a password, que neste caso em específico está errada, no entanto é considerada uma vulnerabilidade, pois um atacante que esteja a capturar o tráfego na rede pode ter acesso à mesma.

```
....login: guest
guest
Password:guest

Login incorrect

Wait for login retry ...

Login incorrect
login: .^D..
```

Figura 9: Tentativa de login