UC/Curso: Segurança em Redes de Computadores/ MIEI
Grupo 5:
-A86617 Gonçalo Nogueira
-A74806 João Amorim
-A75876 Jorge Cardoso
-A78566 Marcos Silva
-A82529 Carlos Afonso

Trabalho Prático 3; ExemploTráfego.pcap

1. **Home net = 193.137.8.0/24**

Endereços
193.137.8.95
193.137.8.106
193.137.8.114
193.137.8.125
193.137.8.138
193.137.8.142
193.137.8.157
193.137.8.215

2. Estratégia de análise

Para descobrir a Home net efetuou-se a análise de todos os endereços IP's envolvidos, recorrendo à ferramenta do Wireshark "Statistics -> Endpoints". Posteriormente, sempre que se pretender obter informações relativamente a cada um dos IP's, será usada a plataforma " www.whatismyipaddress.com".

Como estratégia de análise, serão analisadas todas as Streams individualmente, consoante o protocolo usado, através de filtros (e.g tcp.stream) e da ferramenta do Wireshark "Follow Protocol Stream", onde Protocol corresponde ao nome do protocolo das Streams que pretendemos analisar. Serão inicialmente analisadas, por ordem, as Streams TCP, seguidas das Streams UDP. No final serão ainda analisados os pacotes referentes aos protocolos ICMP e ARP.

Para obtenção de dados estatisticos, foram usadas diversas ferramentes presentes no menu Statistics. Todos estes dados serão apresentados no final do relatório.

3. Síntese da análise

TCP Streams:

Nº ordem ou *streams*	Tempo (s)	Src/Dest	Comentário
Stream: 0 Packets: 3-15 184-205	1.457307 to 2.899311 **Total:** 1.442004	**Src:** endpub106.scom3.uminho.pt (106) – port 1137 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	Inicialmente, é estabelecida uma conexão TCP com recurso ao 3-Way Handshake Process nos pacotes 3,4 e 5, sendo enviado um segmento SYN para o servidor, seguido de uma resposta SYN+ACK do mesmo para o lado do cliente, sendo finalizado pelo ACK do cliente para o servidor. De seguida, é feito um pedido HTTP ao servidor para que

			seja fornecido acesso à pagina “moodle.dsi.uminho.pt”, em que as receções de informação são constantemente confirmadas com o use de ACK’s. A sessão termina através do envio de segmentos do tipo FIN, dos pacotes 202 ao 205. A sessão envolveu a transferência de 35 pacotes e 19266 bytes.
Stream: 1 Packets: 16-166	1.789632 to 2.250563 **Total:** 0.460931	**Src:** endpub106.scom3.uminho.pt (106) – port 1138 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	A partir desta Stream, até à Stream 15, serão enviados dos os elementos da página “moodle.dsi.uminho.pt” que foi pedida. É establecida uma conexão TCP sendo realizado um pedido HTTP GET /moodle/theme/standard/styles.php, sendo possível observar uma falha na receção de dados através do pacote 66. Esta falha leva ao envio de ACK’s duplicados, uma mecanisco para recuparação de pacotes, para que o pacote de dados em falta seja reenviado. É possível observar que o tamanho máximo de cada pacote corresponde a 1314 bytes,ou seja, se a resposta a enviar corresponder a um tamanho superior ao mencionado, esta é dividida e é apresentada a mensagem “Continuation”, que sinaliza o envio dos restantes dados, sempre em tamanho máximo de 1314 bytes. Após recebida toda a informação requisitado, a conexão é encerrada. A sessão envolveu a transferência de 151 pacotes, correspondendo a um total de 109160 bytes.
Stream: 2 **Packets:** 167-178	2.298130 to 2.755881 **Total:** 0.457751	**Src:** endpub106.scom3.uminho.pt (106) – port 1139 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	É establecida uma conexão TCP sendo realizado um pedido HTTP GET /moodle/theme/standardwhite/styles.php ao servidor. Nesta stream não são visiveis erros. A sessão envolveu a transferência de 12 pacotes, correspondendo a um total de 2337 bytes.
Stream: 3 **Packets:** 179-183 206-216	2.756597 to 3.180185 **Total:** 0.423588	**Src:** endpub106.scom3.uminho.pt (106) – port 1140 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	É establecida uma conexão TCP sendo realizado um pedido HTTP GET /moodle/theme/standardlogo/styles.php ao servidor. Observa-se novamente o envio de ACK’s duplicados, fazendo com que sejam enviados pacotes com a flag RST para que conexão seja terminada. A sessão envolveu a transferência de 16 pacotes, correspondendo a um total de 2176 bytes.
Stream: 4 **Packets:** 217 – 226	3.186662 to 3.214152 **Total:** 0.02749	**Src:** endpub106.scom3.uminho.pt (106) – port 1141 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	É establecida uma conexão TCP sendo realizado um pedido HTTP GET /moodle/lib/javascript-static.js ao servidor. Não são visiveis quaisquer erros. É enviada uma resposta HTTP ao cliente indicando que o mesmo já tem o recurso que pediu através da mensagem “304 Not Modified”, minimizando a transferência de informação, sendo então utilizado o recurso que já se encontra em cache. Os campos If-None-Match, If-Modified-Since e Etag presentes nos cabeçalhos permitam fazer a verificação desta informação.

			A sessão envolveu a transferência de 10 pacotes, correspondendo a um total de 1409 bytes.
Stream: 5 **Packets:** 227 – 238	3.222860 to 3.531489 **Total:** 0.308629	**Src:** endpub106.scom3.uminho.pt (106) – port 1142 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	É estabelecida uma conexão TCP sendo realizado um pedido HTTP GET /moodle/lib/javascript-mod.php ao servidor. Não são visiveis quaisquer erros. A sessão envolveu a transferência de 9 pacotes, correspondendo a um total de 1503 bytes.
Stream: 6 **Packets:** 234 – 236, 239 - 245	3.516297 to 3.544831 **Total:** 0.028534	**Src:** endpub106.scom3.uminho.pt (106) – port 1143 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	É estabelecida uma conexão TCP sendo realizado um pedido HTTP GET /moodle/lib/overlib.js ao servidor. Não são visiveis quaisquer erros. É enviada uma resposta HTTP ao cliente indicando que o mesmo já tem o recurso que pediu através da mensagem "304 Not Modified", minimizando a transferência de informação, sendo então utilizado o recurso que já se encontra em cache. Os campos If-None-Match, If-Modified-Since e Etag presentes nos cabeçalhos permitam fazer a verificação desta informação. A sessão envolveu a transferência de 10 pacotes, correspondendo a um total de 1399 bytes.
Stream: 7 **Packets:** 246 - 255	3.582964 to 3.613962 **Total:** 0.030998	**Src:** endpub106.scom3.uminho.pt (106) – port 1144 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	É estabelecida uma conexão TCP sendo realizado um pedido HTTP GET /moodle/lib/cookies.js ao servidor. Não são visiveis quaisquer erros. É enviada uma resposta HTTP ao cliente indicando que o mesmo já tem o recurso que pediu através da mensagem "304 Not Modified", minimizando a transferência de informação, sendo então utilizado o recurso que já se encontra em cache. Os campos If-None-Match, If-Modified-Since e Etag presentes nos cabeçalhos permitam fazer a verificação desta informação. A sessão envolveu a transferência de 10 pacotes, correspondendo a um total de 1397 bytes.
Stream: 8 **Packets:** 256 - 265	3.617197 to 3.648826 **Total:** 0.031629	**Src:** endpub106.scom3.uminho.pt (106) – port 1145 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	É estabelecida uma conexão TCP sendo realizado um pedido HTTP GET /moodle/lib/ufo.js ao servidor. Não são visiveis quaisquer erros. É enviada uma resposta HTTP ao cliente indicando que o mesmo já tem o recurso que pediu através da mensagem "304 Not Modified", minimizando a transferência de informação, sendo então utilizado o recurso que já se encontra em cache. Os campos If-None-Match, If-Modified-Since e Etag presentes nos cabeçalhos permitem fazer a verificação desta informação. A sessão envolveu a transferência de 10 pacotes, correspondendo a um total de 1395 bytes.
Stream: 9 **Packets:** 266, 268 – 271, 274 – 276	3.663604 to 3.713998 **Total:** 0.050394	**Src:** endpub106.scom3.uminho.pt (106) – port 1146 **Dest:** endpub215.scom3.uminho.pt	É estabelecida uma conexão TCP sendo realizado um pedido HTTP GET /moodle/theme/standardlogo/logo.gif ao servidor. Não são visiveis quaisquer erros. É enviada uma resposta HTTP ao cliente indicando que o mesmo já tem o recurso que pediu através da mensagem "304 Not Modified", minimizando a transferência de

278, 280		(215) – port 80	informação, sendo então utilizado o recurso que já se encontra em cache. Os campos If-None-Match, If-Modified-Since e Etag presentes nos cabeçalhos permitem fazer a verificação desta informação. A sessão envolveu a transferência de 10 pacotes, correspondendo a um total de 1428 bytes.
Stream: 10 **Packets:** 267, 272, 273, 277, 279, 281, 282, 284 - 286	3.675176 to 3.722428 **Total:** 0.047252	**Src:** endpub106.scom3.uminho.pt (106) – port 1147 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	É establecida uma conexão TCP sendo realizado um pedido de uma imagem no formato GIF através de HTTP GET /moodle/pix/spacer.gif ao servidor. Não são visiveis quaisquer erros. É enviada uma resposta HTTP 200 OK indicando o sucesso do pedido, sendo depois terminada a sessão. A sessão envolveu a transferência de 10 pacotes, correspondendo a um total de 1555 bytes.
Stream: 11 **Packets:** 283, 288, 289, 291, 293, 295 – 300 302	3.716224 to 3.771711 **Total:** 0.055487	**Src:** endpub106.scom3.uminho.pt (106) – port 1148 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	É establecida uma conexão TCP sendo realizado um pedido HTTP GET /moodle/calendar/overlib.cfg.php ao servidor. Não são visiveis quaisquer erros. É enviada uma resposta HTTP 200 OK indicando o sucesso do pedido, sendo depois terminada a sessão. A sessão envolveu a transferência de 12 pacotes, correspondendo a um total de 1726 bytes.
Stream: 12 **Packets:** 287, 290, 292, 294, 301, 303, 304, 306 - 308	3.722807 to 3.779233 **Total:** 0.056426	**Src:** endpub106.scom3.uminho.pt (106) – port 1149 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	É establecida uma conexão TCP sendo realizado um pedido de uma imagem no formato jpg através de HTTP GET /moodle/theme/standardwhite/gradient.jpg ao servidor. Não são visiveis quaisquer erros. É enviada uma resposta HTTP 200 OK indicando o sucesso do pedido, sendo depois terminada a sessão. A sessão envolveu a transferência de 10 pacotes, correspondendo a um total de 1939 bytes.
Stream: 13 **Packets:** 305, 310 – 313, 317 – 320, 322	3.775350 to 3.882527 **Total:** 0.107177	**Src:** endpub106.scom3.uminho.pt (106) – port 1150 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	É establecida uma conexão TCP sendo realizado um pedido de uma imagem no formato GIF através de HTTP GET /moodle/pix/t/switch_minus.gif ao servidor. Não são visiveis quaisquer erros. É enviada uma resposta HTTP 200 OK indicando o sucesso do pedido, sendo depois terminada a sessão. A sessão envolveu a transferência de 10 pacotes, correspondendo a um total de 1667 bytes.
Stream: 14 **Packets:** 309, 314 – 316, 321, 323, 324, 326 - 328	3.782558 to 3.889159 **Total:** 0.106601	**Src:** endpub106.scom3.uminho.pt (106) – port 1151 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	É establecida uma conexão TCP sendo realizado um pedido de uma imagem no formato GIF através de HTTP GET /moodle/pix/s/biggrin.gif ao servidor. Não são visiveis quaisquer erros. É enviada uma resposta HTTP 200 OK indicando o sucesso do pedido, sendo depois terminada a sessão. A sessão envolveu a transferência de 10 pacotes, correspondendo a um total de 1746 bytes.
Stream: 15	3.885260	**Src:**	É establecida uma conexão TCP sendo realizado um pedido

Packets: 325, 329 - 339	to 3.903881 **Total:** 0.018621	endpub106.scom3.uminho.pt (106) – port 1152 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	de uma imagem no formato GIF através de HTTP GET /moodle/pix/moodlelogo.gif ao servidor. Não são visiveis quaisquer erros. É enviada uma resposta HTTP 200 OK indicando o sucesso do pedido, sendo depois terminada a sessão. A sessão envolveu a transferência de 12 pacotes, correspondendo a um total de 4239 bytes.
Stream: 16 **Packets:** 340 – 347, 425	17.040244 to 82.495246 **Total:** 65.455002	**Src:** endpub106.scom3.uminho.pt (106) – port 1153 **Dest:** rate-limited-proxy-66-249-91-17.google.com (66.249.91.17) – port 80	É estabelecida uma conexão TCP, dando inicio a uma sessão HTTP entre o cliente e o servidor (mail.google.com). É possível observar o email da conta em questão (eu.nuno@gmail.com) e uma vez que a sessão é feita através de HTTP e não HTTPS, é possível visualizar os emails enviados. Neste caso a sessão é terminada com o envio de um pacote com flag RST. A sessão envolveu a transferência de 9 pacotes, correspondendo a um total de 2842 bytes.
Stream: 17 **Packets:** 352 – 356, 359 – 361, 368 - 373	23.819398 to 35.186792 **Total:** 11.367394	**Src:** endpub106.scom3.uminho.pt (106) – port 1154 **Dest:** piano.dsi.uminho.pt (193.137.8.95) – port 21	É estabelecida uma conexão TCP, dando inicio a uma sessão FTP entre o cliente e o servidor (piano.dsi.uminho.pt). É possível observar um pedido de login com o USER anonymous. Uma vez que o servidor se encontra protegido contra este tipo de tentativas, o pedido de login não é efetuado. A sessão envolveu a transferência de 14 pacotes, correspondendo a um total de 918 bytes.
Stream: 18 Packets: 375 – 395, 397 – 400, 403 – 424, 426 - 431	54.257406 to 82.845997 **Total:** 28.588591	**Src:** endpub106.scom3.uminho.pt (106) – port 1156 **Dest:** piano.dsi.uminho.pt (193.137.8.95) – port 23	É estabelecida uma conexão TCP, dando inicio a uma sessão TELNET entre o cliente e o servidor. É possível observar uma tentativa de login com login “guest” e password “guest”, muito provavelmente numa tentativa de bruteforce login, no entanto sem sucesso, uma vez que as credenciais estavam incorretas. A sessão envolveu a transferência de 53 pacotes, correspondendo a um total de 3239 bytes.
Stream: 19 **Packets:** 435, 437, 442	97.001824 to 106.000754 **Total:** 8.99893	**Src:** host-87-28-58-2222.business.telecomitalia.it (87.28.58.222) – port 11132 **Dest:** endpub157.scom3.uminho.pt (157) – port 30797	Tentativa de conexão ao servidor através do envio de um pedido SYN, não obtendo qualquer resposta por parte do mesmo. É possível observar ainda que o host envia continuamente pedidos de retransmissão, possívelmente com intenções maliciosas. A sessão envolveu a transferência de 3 pacotes, correspondendo a um total de 186 bytes.
Stream: 20 Packets: 436, 439, 444	98.607890 to 107.601622 **Total:** 8.993732	**Src:** host-87-28-58-2222.business.telecomitalia.it (87.28.58.222) – port 11139 **Dest:** endpub157.scom3.uminho.pt (215) – port 443	Tentativa de conexão ao servidor através do envio de um pedido SYN, não obtendo qualquer resposta por parte do mesmo. É possível observar ainda que o host envia continuamente pedidos de retransmissão, possívelmente com intenções maliciosas (DDOS?). A sessão envolveu a transferência de 3 pacotes, correspondendo a um total de 186 bytes.
Stream: 21	100.221796 to	**Src:** host-87-28-58-	Tentativa de conexão ao servidor através do envio de um pedido SYN, não obtendo qualquer resposta por parte do

Packets: 438, 440, 446	109.203745 **Total:** 8.981949	2222.business.telecomitalia.it (87.28.58.222) – port 11141 **Dest:** endpub215.scom3.uminho.pt (215) – port 80	mesmo. É possível observar ainda que o host envia continuamente pedidos de retransmissão, possívelmente com intenções maliciosas (DDOS?). A sessão envolveu a transferência de 3 pacotes, correspondendo a um total de 186 bytes.
Stream: 22 **Packets:** 451 - 458	137.534944 to 137.997816 **Total:** 0.462872	**Src:** endpub106.scom3.uminho.pt (106) – port 1157 **Dest:** rate-limited-proxy-66-249-91-17.google.com (66.249.91.17) – port 80	Tal como na Stream 16, é estabelecida uma conexão TCP, dando inicio a uma sessão HTTP entre o cliente e o servidor (mail.google.com). É possível observar o email da conta em questão (eu.nuno@gmail.com) e uma vez que a sessão é feita através de HTTP e não HTTPS, é possível visualizar os emails enviados. Neste caso, não é visivel um término de sessão, o que poderá pôr em risco o email em questão. A sessão envolveu a transferência de 8 pacotes, correspondendo a um total de 2788 bytes.
Stream: 23 **Packets:** 461 – 563 (Excluding previous mentioned packets)	143.664551 to 152.818884 **Total:** 9.154333	**Src:** endpub106.scom3.uminho.pt (106) – port 1158 **Dest:** endpub142.scom3.uminho.pt (142) – port 445	É estabelecida uma conexão TCP, dando inicio a uma sessão SMB entre o cliente e o servidor. Este tipo de protocolo disponibiliza o acesso partilhado em rede a ficheiros e impressoras. Durante esta Stream, é possível observar a perda de pacotes, sendo estes retransmitidos através do TCP Retransmission, assim como duas tentativas de login, sem sucesso, com o user "\" e "BOCASJNR\hsantos", às diretorias \\TROMBONE\IPC e \\TROMBONE\SOFT\AutoRun.inf, respetivamente. A sessão envolveu a transferência de 98 pacotes, correspondendo a um total de 17543 bytes.
Stream: 24 **Packets:** 464, 467, 469	143.676901 to 143.720977 **Total:** 0.044076	**Src:** endpub106.scom3.uminho.pt (106) – port 1159 **Dest:** Endpub142.scom3.uminho.pt (142) – port 80	Existe uma tentativa de conexão ao servidor sem sucesso. É enviado um pacote com a flag RST para terminar a sessão. A sessão envolveu a transferência de 3 pacotes, correspondendo a um total de 178 bytes.

UDP Streams:

Nº ordem ou *streams*	Tempo (s)	Src/Dest	Comentário
Stream: 0 **Packets:** 348, 350	23.779650 to 23.792078 **Total:** 0.012428	**Src:** endpub106.scom3.uminho.pt (106) – port 1030 **Dest:** endpub142.scom3.uminho.pt (142) – port 53	É efetuado um pedido DNS ao servidor endpub142.scom3.uminho.pt para obtenção do ip do DNS "piano.dsi.uminho.pt". Este responde-lhe com o ip "193.137.8.95". A sessão envolveu a transferência de 2 pacotes, correspondendo a um total de 174 bytes.
Stream: 1 **Packets:** 357,358, 365	25.535682 to 31.551484 **Total:**	**Src:** 41.224.211.188 – port 1030 **Dest:** endpub157.scom3.uminho.pt	A sessão envolveu a transferência de 93 pacotes, correspondendo a um total de 450 bytes. Sem Informação Adicional.

	6.015802	(157) – port 30797	
Stream: 2 **Packets:** 363, 366 374	31.271661 to 37.315007 **Total:** 6.043346	**Src:** 84.41.174.73 – port 38337 **Dest:** endpub157.scom3.uminho.pt (157) – port 30797	A sessão envolveu a transferência de 3 pacotes, correspondendo a um total de 408 bytes. Sem Informação Adicional.
Stream: 3 **Packets:** 363, 367	31.279818 to 33.316836 **Total:** 2.037018	**Src:** a217-70-68-212.cpe.netcabo.pt (217.70.68.212) – port 59342 **Dest:** endpub142.scom3.uminho.pt (142) – port 23897	A sessão envolveu a transferência de 2 pacotes, correspondendo a um total de 252 bytes. Sem Informação Adicional.
Stream: 4 **Packets:** 433, 434	93.723027 to 95.745304 **Total:** 2.022277	**Src:** endpub138.scom3.uminho.pt (138) – port 39284 **Dest:** endpub157.scom3.uminho.pt (157) – port 30797	A sessão envolveu a transferência de 2 pacotes, correspondendo a um total de 248 bytes. Sem Informação Adicional.
Stream: 5 **Packets:** 443, 445	106.453435 to 108.509339 **Total:** 2.055904	**Src:** acb1-84-91-17-250.netvisao.pt (84.91.17.250) – port 54035 **Dest:** endpub157.scom3.uminho.pt (157) – port 30797	A sessão envolveu a transferência de 2 pacotes, correspondendo a um total de 228 bytes. Sem Informação Adicional.
Stream: 6 **Packets:** 447, 449 450	118.301230 to 124.327858 **Total:** 6.026628	**Src:** 81-64-154-175.rev.numericable.fr (81.64.154.175) – port 43622 **Dest:** endpub157.scom3.uminho.pt (157) – port 30797	A sessão envolveu a transferência de 3 pacotes, correspondendo a um total de 405 bytes. Sem Informação Adicional.
Stream: 7 **Packets:** 462	143.672084 **Total:** 0	**Src:** endpub106.scom3.uminho.pt (142) – port 137 **Dest:** endpub106.scom3.uminho.pt (106) – port 137	É efetuado um pedido NetBIOS Name Service (NBNS) para que seja feita a tradução do DNS para um endereço IP, do serviço NETBIOS presente na TCP Stream 23

ICMP:

Nº ordem ou *streams*	Tempo (s)	Src/Dest	Comentário
Packets: 1, 362, 396, 432, 448, 540	0 to 150.336312	**Src:** endpub013.scom-glt.uminho.pt (193.137.88.13)	Envio de vários Ping Request, espaçados por aproximadamente 30 segundos, sem obter qualquer Ping Reply.

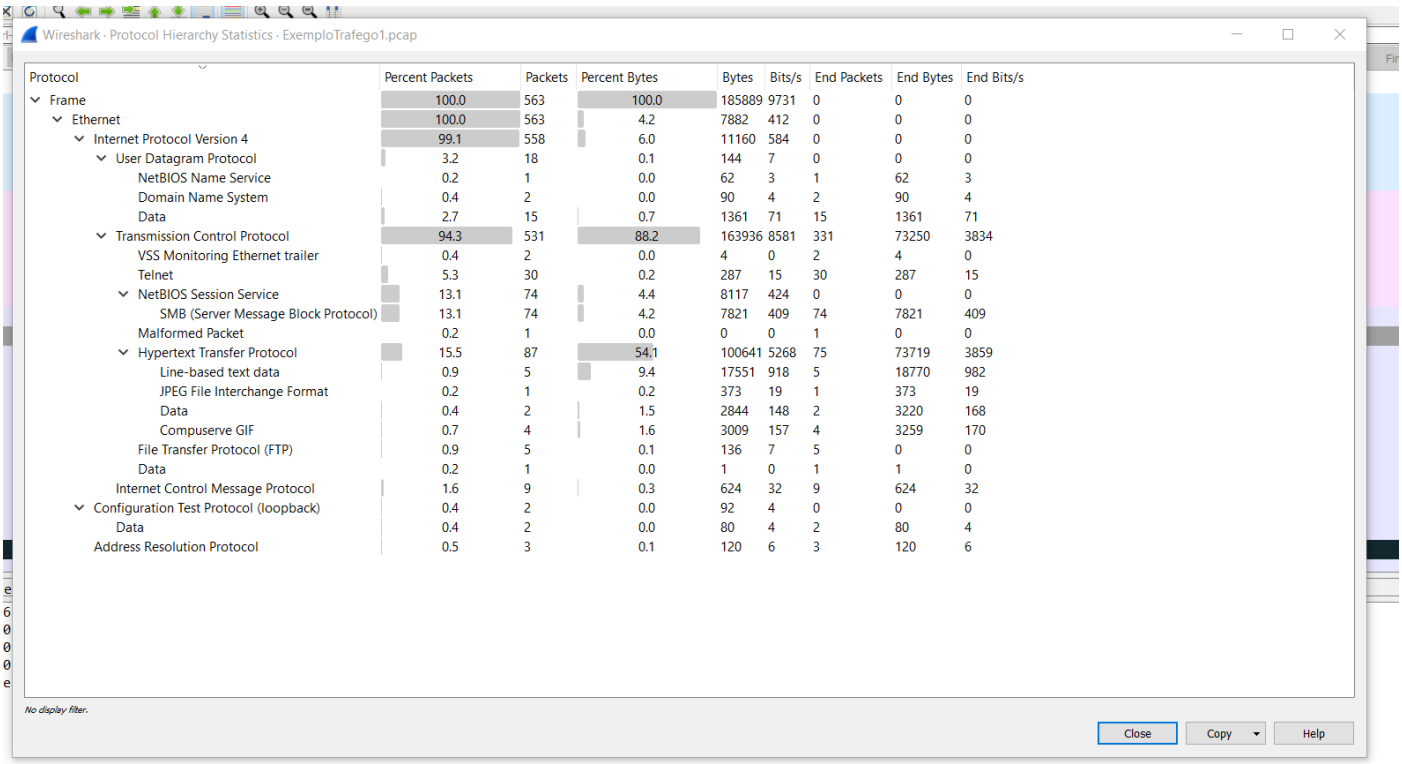
	Total: 150.336312	**Dest:** 172.16.170.81	A sessão envolveu 6 pacotes de tamanho igual a 684 bytes.
441	105.037733 **Total:** 0	**Src:** 172.16.40.125 **Dest:** 172.16.170.81	Ping Request without Ping Reply A sessão envolveu 1 pacote de tamanho igual a 98 bytes.
459, 460	143.654404 to 143.660955 **Total:** 0.006551	**Src:** endpub106.scom3.uminho.pt (106) **Dest:** endpub106.scom3.uminho.pt (142)	endpub106.scom3.uminho.pt efetuou um Ping Request para endpub106.scom3.uminho.pt, recebendo um Ping Reply, validando a conexão. A sessão envolveu 2 pacote de tamanho igual a 148 bytes.

ARP:

Este protocolo é usada na obtenção de endereços físicos (MAC address) de um determinado host, através do seu endereço de IP. Na captura fornecida para realização deste relatório, é possível observar a existência dos seguintes pacotes ARP:

Nº ordem ou *streams*	Tempo (s)	Src/Dest	Comentário
Packets: 2	1.456585 **Total:** 0	**Src:** HewlettP_b6:5a:a0 **Dest:** SamsungE_05:f4:c3	**Target MAC Address:** endpub106.scom3.uminho.pt (00:13:77:05:f4:c3) **Target IP Address:** endpub106.scom3.uminho.pt (193.137.8.106)
Packets: 349	23.786302 **Total:** 0	**Src:** SamsungE_05:f4:c3 **Dest:** HewlettP_b6:5a:a0	**Target MAC Address:** endpub142.scom3.uminho.pt (00:08:02:b6:66:cb) **Target IP Address:** endpub142.scom3.uminho.pt (193.137.8.142)
Packets: 351	23.819171 **Total:** 0	**Src:** DigitalE_1f:3d:ce **Dest:** SamsungE_05:f4:c3	**Target MAC Address:** endpub106.scom3.uminho.pt (00:13:77:05:f4:c3) **Target IP Address:** endpub106.scom3.uminho.pt (193.137.8.106)

Análise estatística



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	563	100.0	185889	9731	0	0	0
Ethernet	100.0	563	4.2	7882	412	0	0	0
Internet Protocol Version 4	99.1	558	6.0	11160	584	0	0	0
User Datagram Protocol	3.2	18	0.1	144	7	0	0	0
NetBIOS Name Service	0.2	1	0.0	62	3	1	62	3
Domain Name System	0.4	2	0.0	90	4	2	90	4
Data	2.7	15	0.7	1361	71	15	1361	71
Transmission Control Protocol	94.3	531	88.2	163936	8581	331	73250	3834
VSS Monitoring Ethernet trailer	0.4	2	0.0	4	0	2	4	0
Telnet	5.3	30	0.2	287	15	30	287	15
NetBIOS Session Service	13.1	74	4.4	8117	424	0	0	0
SMB (Server Message Block Protocol)	13.1	74	4.2	7821	409	74	7821	409
Malformed Packet	0.2	1	0.0	0	0	1	0	0
Hypertext Transfer Protocol	15.5	87	54.1	100641	5268	75	73719	3859
Line-based text data	0.9	5	9.4	17551	918	5	18770	982
JPEG File Interchange Format	0.2	1	0.2	373	19	1	373	19
Data	0.4	2	1.5	2844	148	2	3220	168
Compuserve GIF	0.7	4	1.6	3009	157	4	3259	170
File Transfer Protocol (FTP)	0.9	5	0.1	136	7	5	0	0
Data	0.2	1	0.0	1	0	1	1	0
Internet Control Message Protocol	1.6	9	0.3	624	32	9	624	32
Configuration Test Protocol (loopback)	0.4	2	0.0	92	4	0	0	0
Data	0.4	2	0.0	80	4	2	80	4
Address Resolution Protocol	0.5	3	0.1	120	6	3	120	6

Figura 1- Protocolos Usados e a sua Hierarquia

Analisando a figura 1 reportamos os seguintes protocolos usados:

- UDP- Protocolo usado sobre IP sem garantia de fiabilidade na entrega dos pacotes;
- NBNS-Função idêntica ao DNS, mas no âmbito das redes locais (NetBIOS/Windows);
- DNS-Sistema hierárquico de gestão de nomes de domínios, traduz nomes para endereços IP;
- TCP-Protocolo usado sobre IP com estabelecimento de uma sessão entre os intervenientes e com garantia de fiabilidade;
- TELNET-Permite uma comunicação baseada em texto, bidirecional e interativa, através de uma conexão virtual ao terminal;
- SMB-Disponibiliza o acesso partilhado em rede a ficheiros e impressoras;
- HTTP-Protocolo da camada de aplicação para a transmissão de informação de *Hypertext*, a base da comunicação com servidores Web e os navegadores;
- FTP-Protocolo para transferência de ficheiros em rede;
- ICMP-Protocolo de controlo integrante do IP, permite fornecer relatórios de erros à fonte remetente;
- LOOP-Usado para o mesmo efeito do ping, mas na camada de ligação de dados;
- ARP- Permite o mapeamento de endereços de rede (IP) para endereços físicos (MAC).

Através da análise da figura 1 podemos também concluir uma maior predominância do TCP como protocolo com o maior número de pacotes (94,3%) seguido de HTTP (15,5%), SMB (13,1%) e o UDP com apenas 3,2%, uma percentagem bastante inferior quando comparado com o TCP.

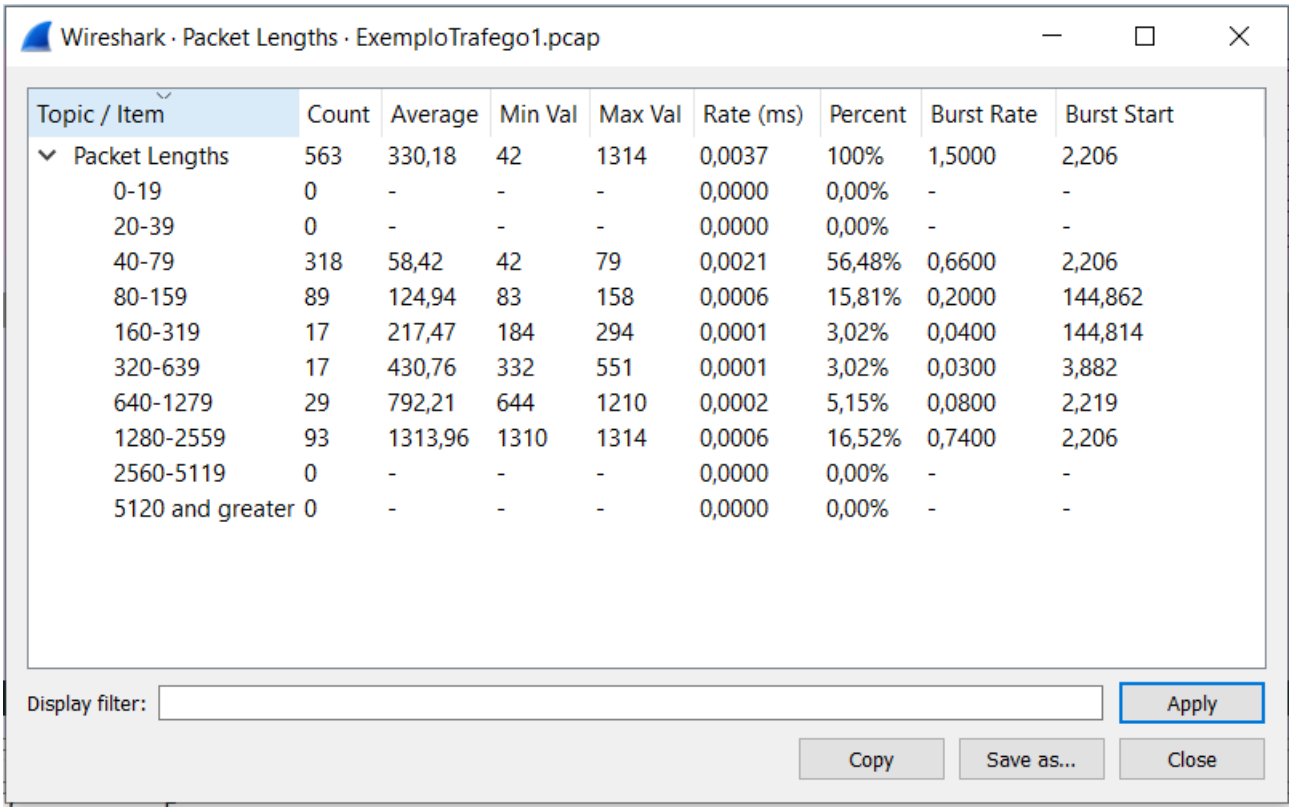


Figura 2- Tamanhos dos pacotes do tráfego analisado

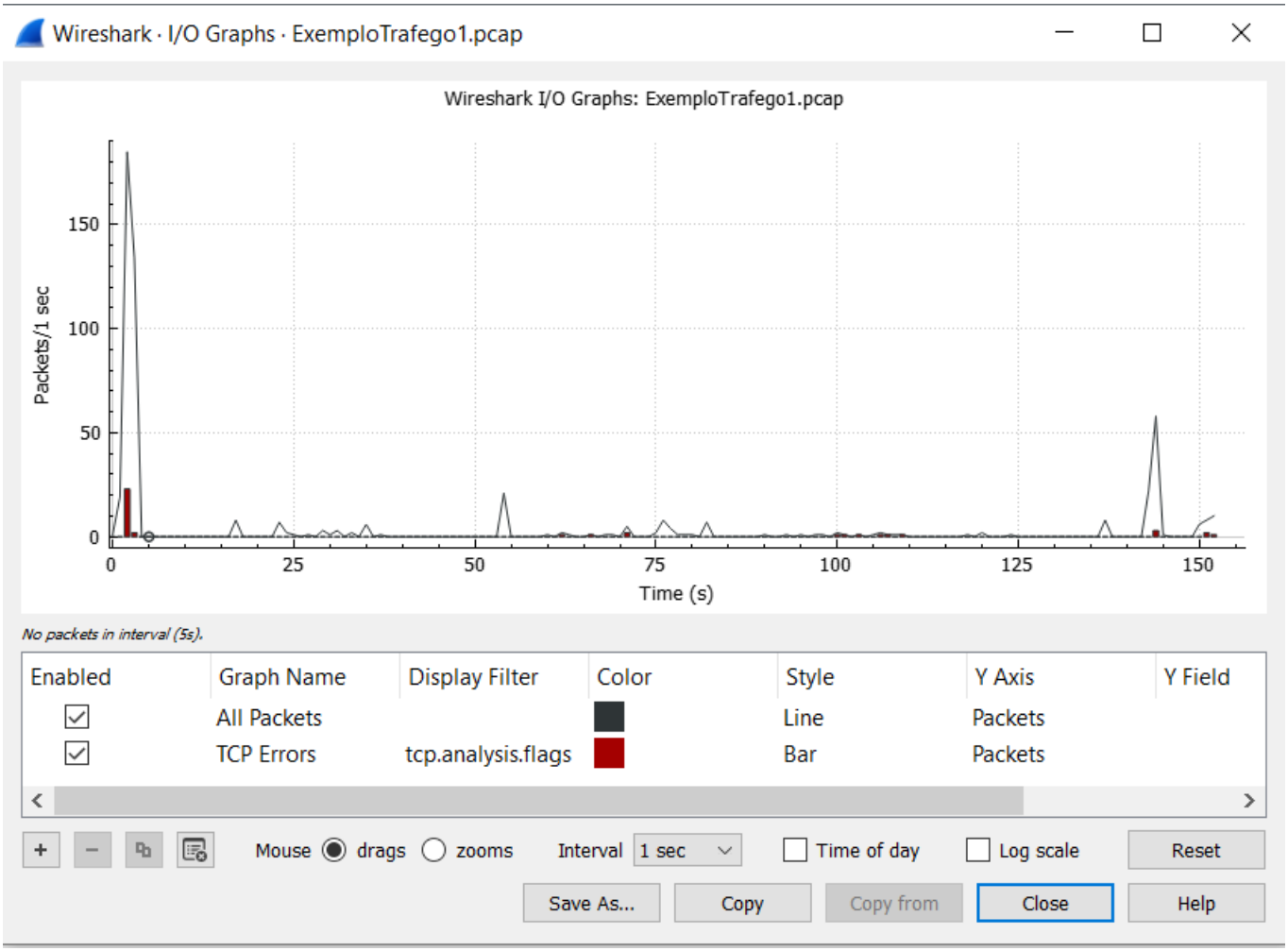


Figura 3- Timeline do tráfego capturado