UC/Curso: MIEGSI
Grupo 6:
- Ana Carolina Pereira (a89168)
- Catarina Fernandes (a89206)
- Frederica Martins (a85618)
- João Gomes (a82867)
- Gonçalo Cambão (a84910)

Trabalho Prático 4; ExemploTrafego.pcap

1. Home net = 193.137.8.0/24

2. Estratégia de análise

De modo a iniciar a análise do tráfego do ficheiro disponibilizado pelo docente, o grupo começou por definir a estratégia de análise. Esta passou pela identificação de sessões, que são o principal conceito para a análise realizada no presente trabalho. Deste modo, uma sessão corresponde à comunicação estabelecida entre duas máquinas com o IP associado, em que a conexão é realizada com recurso a um utilizador ou aplicação num intervalo de tempo contínuo. Assim, é necessário ter em consideração que duas comunicações diferentes, em tempos diferentes entre as mesmas duas máquinas, dão origem a sessões diferentes. Associado a cada sessão podem ocorrer diversas *streams*, que podem utilizar ou não o mesmo protocolo.

Após a compreensão destes conceitos, o grupo iniciou a identificação das sessões, acedendo às Conversations, disponíveis em Statistics e selecionando o separador que contém TCP. Através da verificação da tabela apresentada e do filtro *tcp.stream*, foram identificadas as sessões e as respetivas *streams*, sendo identificadas 7 sessões, que serão analisadas na tabela 1.

De seguida, o grupo optou por analisar o tráfego complementar, que considera os restantes protocolos, apresentados na tabela 2.

Por último, surgem algumas informações de natureza estatística em jeito de conclusão do trabalho realizado pelo grupo com recurso ao *Wireshark*.

3. Síntese da análise

Foram identificadas sete sessões com o protocolo TCP. Assim, inicialmente pretende-se realizar uma síntese da análise das sete sessões identificadas, com a identificação das *streams* correspondentes, tempo da sessão, IP de origem e de destino com referência à porta associada e os comentários relativos à análise da sessão.

Foram encontradas, com recurso à ferramenta *Conversations* do Wireshark, 25 *streams* TCP.

Nº Sessão	Nº ordem ou *streams*	Tempo (s)	Src (port)/Dest(port)	Comentário
1	3-339 Stream TCP 0-15	1.457307 a 3.903881	198.137.8.106 (1137 a 1152) – 193.137.8.215 (80)	A sessão inicia-se com um *handshake* triplo do protocolo TCP, ocorrente nas frames 3 a 5. Na frame 3, o cliente inicia uma conexão SYN (Seq=0). Em resposta, na frame seguinte, o servidor responde com uma flag SYN+ACK (Seq=0 e Ack=1, respetivamente), o que permite perceber que a ligação foi aceite. O estabelecimento da ligação é concluído por parte do cliente, na 5ª frame, quando este envia ao servidor uma flag ACK, confirmando a aceitação da ligação (Seq=1 e Ack=1). Na *frame* 6, o cliente estabelece uma comunicação HTTP, fazendo uma *request* GET ao Moodle DSI. As atividades ao longo da sessão, envolvem diversos pedidos HTTP e transferência de ficheiros de composição de página, imagens e ficheiros JavaScript, como é possível observar na figura 6, presente nos anexos. A comunicação foi realizada sem os protocolos SSL ou TLS. Além disso, foram verificadas algumas situações de erro que serão descritas abaixo: • Na *frame* 66: o segmento anterior não foi capturado • Nas *frames* 82, 87-91, 95-96, 98-102, 104-105, 112-115, 213-214: duplicação de ACKs • Nas *frames* 215-216: TCP RST → Quando um pacote TCP inesperado chega a um host, esse anfitrião geralmente responde enviando um pacote de *reset* na mesma ligação. A sessão contou a transferência de 337 pacotes e 153,916 KBytes.
2	340-347 425 Stream TCP 16	17.040244 a 17.496282 82.494246	193.137.8.106 (1153) – 66.249.91.17 (80)	Aqui é possível observar um *handshake* triplo como descrito na sessão acima. É, também, notável uma comunicação HTTP ao servidor "mail.google.com". Também é percetível a receção de emails provindos dos seguintes endereços:

				• membership@techtarget.com.au; • program@mentornet.net; • program.team@mentornet.net; • jennifercg@mentornet.net; Na *frame* 425, a sessão foi interrompida devido a um TCP RST. A sessão contou com a transferência de 9 pacotes e 2.842 KBytes.
3	352 – 359 359 – 361 368 – 373 Stream TCP 17	23.819398 a 24.152064 29.366994 a 29.511127 35.178098 a 35.186792	193.137.8.106 (1154) – 193.137.8.95 (21)	Nesta sessão, é possível verificar uma comunicação FTP, no qual se verifica uma tentativa de *login* de um utilizador *anonymous* no endereço piano.dsi.uminho.pt. Na *frame* 355, o servidor retorna uma confirmação, através do código 220. Utilizando o comando USER, na *frame* 359, existe a tentativa de acesso do *user anonymous*. Na *frame* seguinte, o servidor desconhece o utilizador e envia a respetiva resposta, através do código 530. Na *frame* 368, o utilizador, com o comando QUIT, sai do servidor, que aceita o pedido e se despede, usando o código 221 "*Goodbye*". Nesta sessão, não se verifica a ocorrência de erros. A sessão envolveu a transferência de 14 pacotes e 0.918 KBytes.
4	375-395 397-400 403-424 426-431 Stream TCP 18	54.257406 a 54.776733 62.211469 a 66.369249 71.181531 a 80.040495 82.814343 a 82.845997	193.137.8.106 (1156) – 193.137.8.95 (23)	Aqui é possível observar um *handshake* triplo como descrito anteriormente. É ainda realizada uma sessão TELNET no endereço piano.dsi.uminho.pt. Houve uma tentativa de acesso, usando as credenciais de *login* "*guest*" e *password* "*guest*". Esta tentativa levou a uma autenticação incorreta. De seguida, efetuou-se uma nova tentativa ("Wait for login retry ..."), que também falhou. Tendo sido possível observar as credenciais usadas, conclui-se que não houve encriptação das mesmas. Uma forma de evitar que isto aconteça seria recorrer ao uso do protocolo SSH. Além disso, foram verificadas algumas situações de erro que serão descritas abaixo: • Na *frames* 400 e 403: erro de retransmissão; • Na *frame* 404: segmento ACK não capturado; A comunicação deu-se por terminada com o envio dos pacotes com a *flag* FIN ACK, nas *frames* 428 e 430.

				A sessão envolveu a transferência de 53 pacotes e 3.239 KBytes.
5	435-440 442 444 446 Stream TCP 19-21	97.001824 a 103.200578 106.000754 107.601622 109.203745	87.28.58.157 (11132, 11139, 11141) - 193.137.8.157 (30797, 443, 80)	Nesta sessão é possível verificar que são realizados três pedidos diferentes para três portas diferentes, sendo que se trata de uma comunicação TCP. São enviados 3 pacotes do destino (SYN), no entanto não há resposta da origem. Foram identificados alguns erros ocorridos: • Nas frames 437, 439, 440, 442, 444, 446: retransmissão de pacotes. A sessão envolveu a transferência de 9 pacotes e 0.558KBytes.
6	451- 458 Stream TCP 22	137.534994 a 137.997816	193.137.8.106 (1157) - 66.249.91.17 (80)	Aqui é realizada uma sessão HTTP com o servidor “mail.google.com”. Também se verifica a informação do server GFE1.3 que informa a receção de emails provenientes dos seguintes endereços: • membership@techtarget.com.au; • program@mentornet.net; • program.team@mentornet.net; • jennifercg@mentornet.net; Ao contrário do que ocorreu na sessão 2, esta sessão não termina e o procedimento de término da conexão TCP não ocorre. A sessão envolveu a transferência de 8 pacotes e 2.788KBytes.
7	461-563 Stream TCP 23-24	143.664551 a 152.818884	193.137.8.106 (1158) - 193.137.8.142 (445)	Aqui é realizada uma comunicação SMB para aceder remotamente a ficheiros presentes no servidor TROMBONE@DSI. Foi efetuado um *login* com o *user* “\” e uma tentativa de acesso a uma diretoria “\\TROMBONE\IPC$”, à qual se verificou um error “STATUS_ACCESS_DENIED”. O utilizador faz, então, *log out* e é realizado outro acesso, desta vez com o utilizador “\hsantos”. Este *user* acede com sucesso à diretoria “\\TROMBONE\SOFT”, onde executa diversas *queries* de informação de ficheiros. Seguidamente, o utilizador realiza um pedido “FIND_FIRST2”, que gera uma transmissão de pacotes por TCP. Foram identificados alguns erros ocorridos: • Nas frames 496, 553: o segmento anterior não foi capturado; • Na frame 499: duplicação de ACKs; • Nas frames 500, 552, 554: retransmissão de pacotes. A sessão envolveu a transferência de 101 pacotes e 17.178KBytes.

Tabela 1 - Síntese da análise

4. Análise complementar

De seguida pretende-se realizar a análise do tráfego complementar, com os protocolos associados ao mesmo, uma vez que na análise inicial o grupo focou-se apenas nas sessões com o protocolo TCP. Assim, o tráfego analisado nesta etapa é o restante, que não foi identificado pelo Wireshark como sessão TCP.

Foram encontradas, com recurso à ferramenta *Conversations* do Wireshark, 8 *streams* UDP.

Nº ordem ou *streams*	**Tempo (s)**	**Src (port)/Dest(port)**	**Comentário**
348 350 Stream UDP 0	23.779650 23.792078	193.137.8.106 (1030) - 193.137.8.142 (53)	Utilização do protocolo DNS (Standard Query e Standard Response), que determina o endereço piano.dsi.uminho.pt.
357-358, 363, 364, 365, 366, 367, 374, 433-434, 443, 445, 447, 449-450 Stream UDP 1-6	25.535682 a 31.551484 31.271661 a 37.315007 93.723027 a 95.745304 106.453435 a 106.509339 118.301230 a 124.327858	41.244.211.188 (35953) - 193.137.8.157 (30797) 84.41.174.73 (38337) - 193.137.8.157 (30797) 217.70.68.212 (59342) – 193.137.8.154 (23897) 193.137.8.138 (39284) / 193.137.8.157 (30797) 84.91.17.250 (54035) / 193.137.8.157 (30797) 81.64.154.175 (43622) / 193.137.8.157 (30797)	Nestas *streams* são realizadas transferências de diversos pacotes UDP, sem a presença de erros. Todas estas comunicações transferem um número reduzido de pacotes, variando entre 1 e 3, sendo que cada pacote varia entre 100 e 250 no número de bytes. Isto não aparenta ser uma ameaça à rede ou à comunicação na mesma.
462 Stream UDP 7	143.672084	193.137.8.142 (137) – 193.137.8.106 (137)	Aqui utiliza-se o protocolo NBNS, de forma a determinar a resolução do IP, cujo nome é “TROMBONE”.
1, 362, 396, 432, 441, 448 459 e 540	0, 30.07743, 60.155486, 90.197338, 105.037733, 120.240131, 143.654404, 150.336312	193.137.88.13 - 172.16.170.81	Aqui foram realizadas várias comunicações ICMP, de forma a enviar Echo Request ao *host*, que fica à espera de um Echo Reply. Não foram encontradas respostas.
2, 349, 351	1.456585, 23.786302, 23.819171	00:08:02:b6:5a:a0 - 00:13:77:05:f4:c3 00:13:77:05:f4:c3 / 00:08:02:b6:66:cb	Nestas *frames* são realizadas respostas aos pedidos ARP dos determinados destinatários.

		00:00:f8:1f:3d:ce / 00:13:77:05:f4:c3	
401-402	68.947723, 69.513079	Cisco_ef:54:d9 - Cisco_ef:54:d9; Cisco_08:d6:19 – Cisco_08:d6:19	Utilização do protocolo LOOP.

Tabela 2 - Análise complementar

5. Informação de natureza estatística

Análise de informação geral sobre a captura

De modo a obter informações sobre a captura de rede efetuada, foram usadas algumas ferramentas estatísticas do *Wireshark.* A figura 1 apresenta um conjunto de informações básicas sobre o tráfego analisado, como o tempo da captura (em mm:ss e segundos), o tempo de registo do primeiro e último pacote, assim como outras métricas relevantes. Dentro dessas outras medidas salientam-se a importância do número de pacotes capturados no total (563), o tamanho médio de cada pacote (330 Bytes) e o número total (185889 Bytes) e médio (1216 Bytes/s) de Bytes capturados.

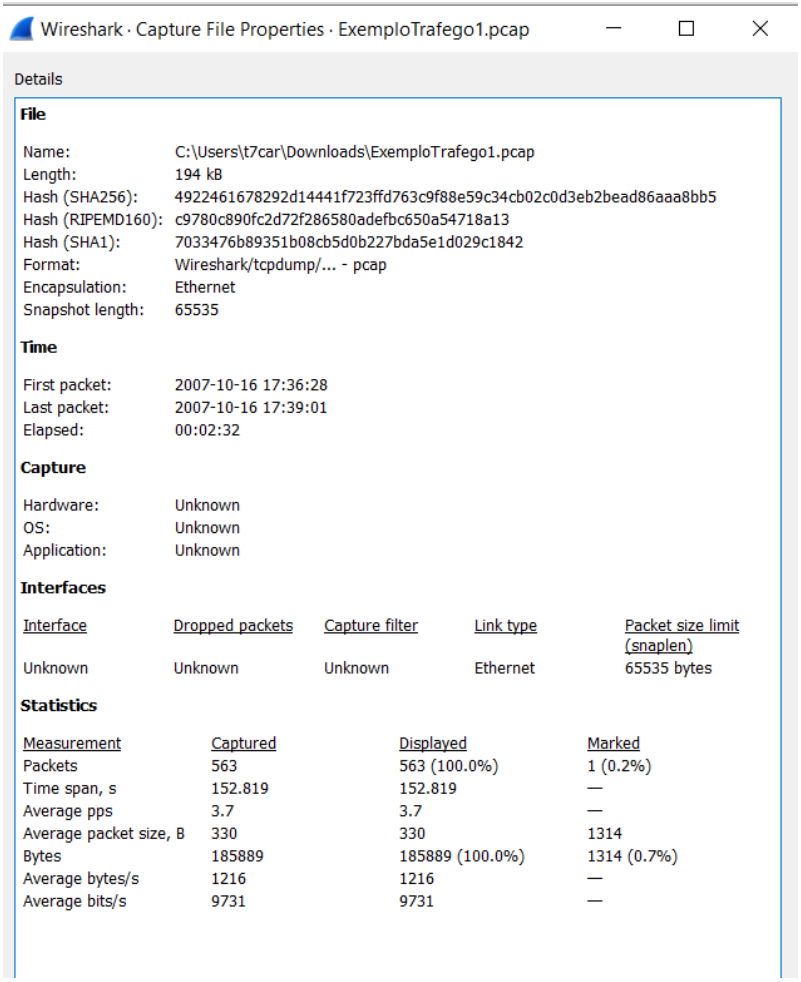
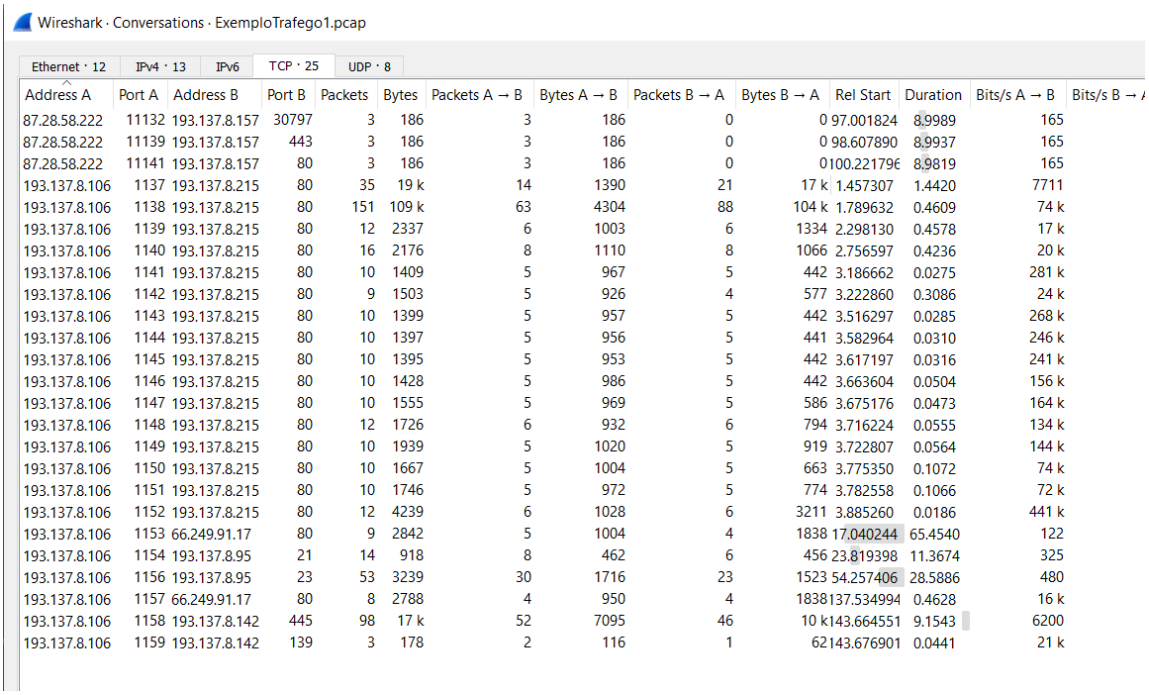


Figura 1 - Informação relativa ao tráfego

A próxima análise estatística foi realizada com recurso à ferramenta *Conversations* do Wireshark, utilizada anteriormente, permitindo ver com mais detalhe as 25 *streams* (que diz respeito à comunicação entre dois pontos). Para cada *stream*, existe um número de pacotes transmitidos associado, assim como a respetiva quantidade em Bytes. É ainda possível ver a duração, bem como o tempo relativo do começo de cada uma delas.



Wireshark · Conversations · ExemploTrafego1.pcap

Ethernet · 12 | IPv4 · 13 | IPv6 | TCP · 25 | UDP · 8

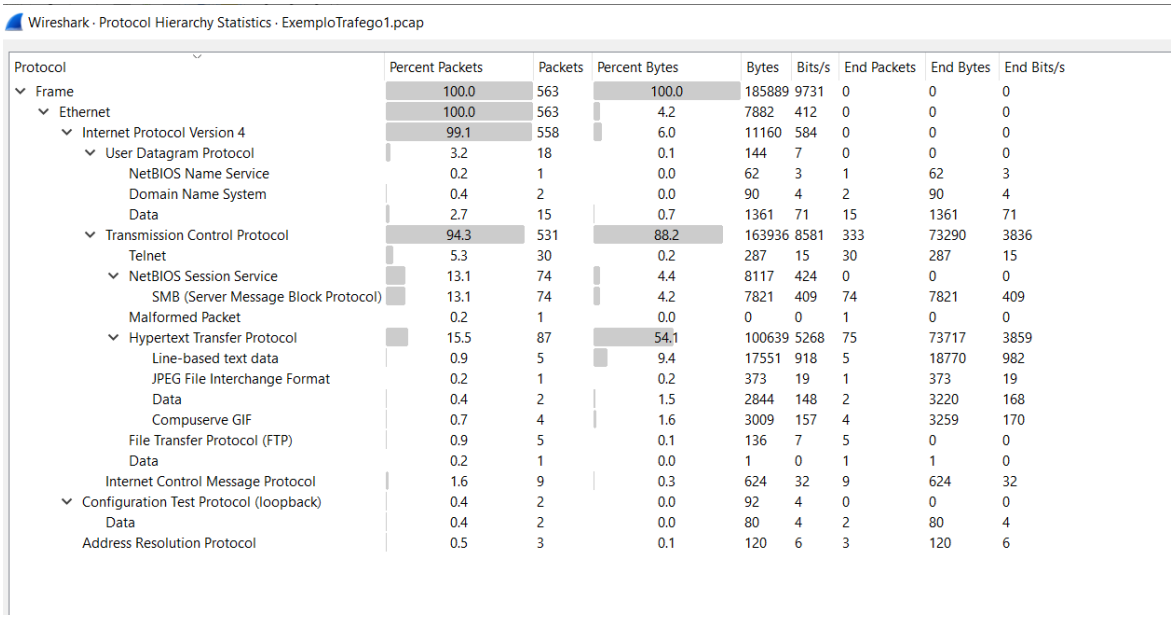
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
87.28.58.222	11132	193.137.8.157	30797	3	186	3	186	0	0	97.001824	8.9989	165	
87.28.58.222	11139	193.137.8.157	443	3	186	3	186	0	0	98.607890	8.9937	165	
87.28.58.222	11141	193.137.8.157	80	3	186	3	186	0	0	100.221796	8.9819	165	
193.137.8.106	1137	193.137.8.215	80	35	19 k	14	1390	21	17 k	1.457307	1.4420	7711	
193.137.8.106	1138	193.137.8.215	80	151	109 k	63	4304	88	104 k	1.789632	0.4609	74 k	
193.137.8.106	1139	193.137.8.215	80	12	2337	6	1003	6	1334	2.298130	0.4578	17 k	
193.137.8.106	1140	193.137.8.215	80	16	2176	8	1110	8	1066	2.756597	0.4236	20 k	
193.137.8.106	1141	193.137.8.215	80	10	1409	5	967	5	442	3.186662	0.0275	281 k	
193.137.8.106	1142	193.137.8.215	80	9	1503	5	926	4	577	3.222860	0.3086	24 k	
193.137.8.106	1143	193.137.8.215	80	10	1399	5	957	5	442	3.516297	0.0285	268 k	
193.137.8.106	1144	193.137.8.215	80	10	1397	5	956	5	441	3.582964	0.0310	246 k	
193.137.8.106	1145	193.137.8.215	80	10	1395	5	953	5	442	3.617197	0.0316	241 k	
193.137.8.106	1146	193.137.8.215	80	10	1428	5	986	5	442	3.663604	0.0504	156 k	
193.137.8.106	1147	193.137.8.215	80	10	1555	5	969	5	586	3.675176	0.0473	164 k	
193.137.8.106	1148	193.137.8.215	80	12	1726	6	932	6	794	3.716224	0.0555	134 k	
193.137.8.106	1149	193.137.8.215	80	10	1939	5	1020	5	919	3.722807	0.0564	144 k	
193.137.8.106	1150	193.137.8.215	80	10	1667	5	1004	5	663	3.775350	0.1072	74 k	
193.137.8.106	1151	193.137.8.215	80	10	1746	5	972	5	774	3.782558	0.1066	72 k	
193.137.8.106	1152	193.137.8.215	80	12	4239	6	1028	6	3211	3.885260	0.0186	441 k	
193.137.8.106	1153	66.249.91.17	80	9	2842	5	1004	4	1838	17.040244	65.4540	122	
193.137.8.106	1154	193.137.8.95	21	14	918	8	462	6	456	23.819398	11.3674	325	
193.137.8.106	1156	193.137.8.95	23	53	3239	30	1716	23	1523	54.257406	28.5886	480	
193.137.8.106	1157	66.249.91.17	80	8	2788	4	950	4	1838	137.534994	0.4628	16 k	
193.137.8.106	1158	193.137.8.142	445	98	17 k	52	7095	46	10 k	143.664551	9.1543	6200	
193.137.8.106	1159	193.137.8.142	139	3	178	2	116	1	62	143.676901	0.0441	21 k	

Figura 2 - Identificação das streams

De seguida, usando a *Protocol Hierarchy Statistics*, verifica-se as quantidades e divisões do número de pacotes, e o volume de dados pelos diferentes protocolos.

Com isto em mente, é possível chegar à conclusão que:

- 94.3% dos pacotes estão associados ao protocolo TCP;
- 15.5% dos pacotes associados ao protocolo HTTP;
- 13.1% associados ao protocolo SMB.



Wireshark · Protocol Hierarchy Statistics · ExemploTrafego1.pcap

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	333	73290	3836
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	100639	5268	75	73717	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 3 - Estatísticas associadas aos protocolos

Utilizando o *I/O Graphs*, foi possível obter a escala logarítmica e a escala normal. Pode-se, então, verificar o número de pacotes capturados no decorrer do tempo, assim como verificar os tempos em que surgiram erros TCP.

É possível, a partir da observação dos gráficos, que o mais número de pacotes capturados situa-se nos primeiros 5 segundos de captura. Além disso, verifica-se, também, que o maior volume de erros ocorreu no intervalo dos 100 aos 110 segundos, referentes à comunicação suspeita na sessão 5.

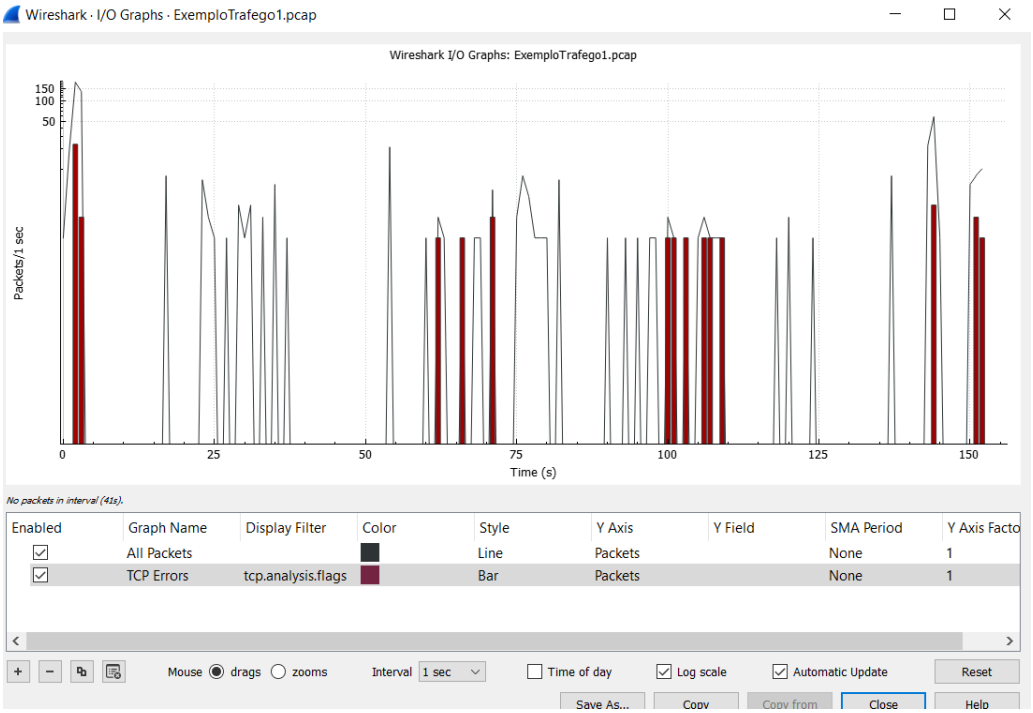


Figura 4 - Gráfico do tráfego em escala logarítmica

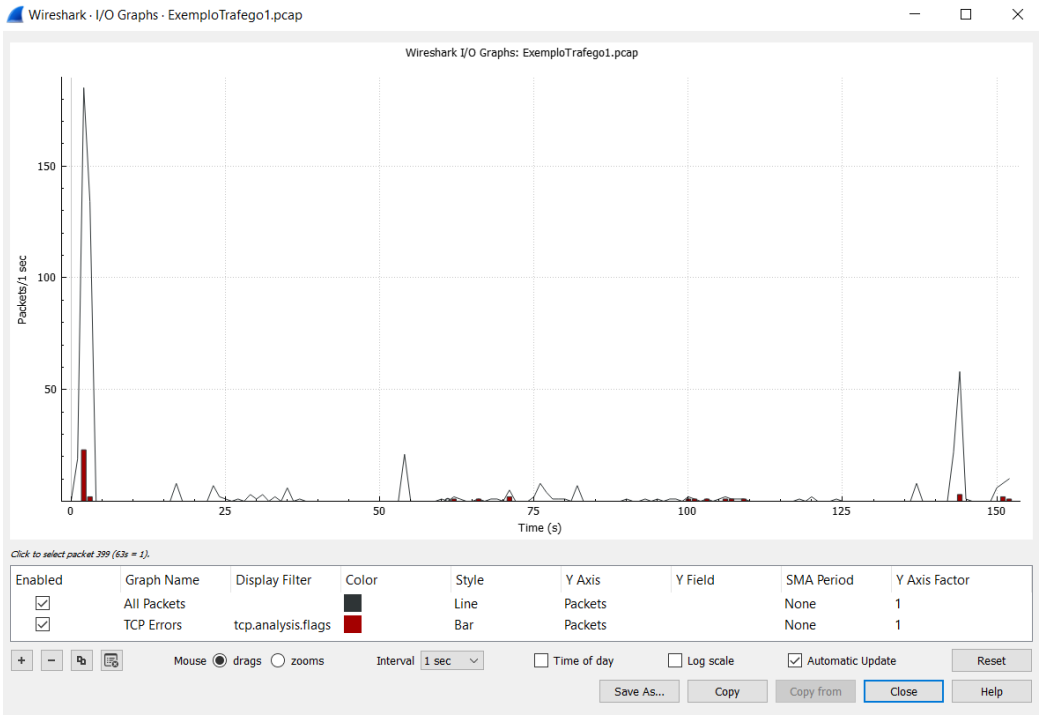


Figura 5 - Gráfico do tráfego em escala normal

6. Anexo

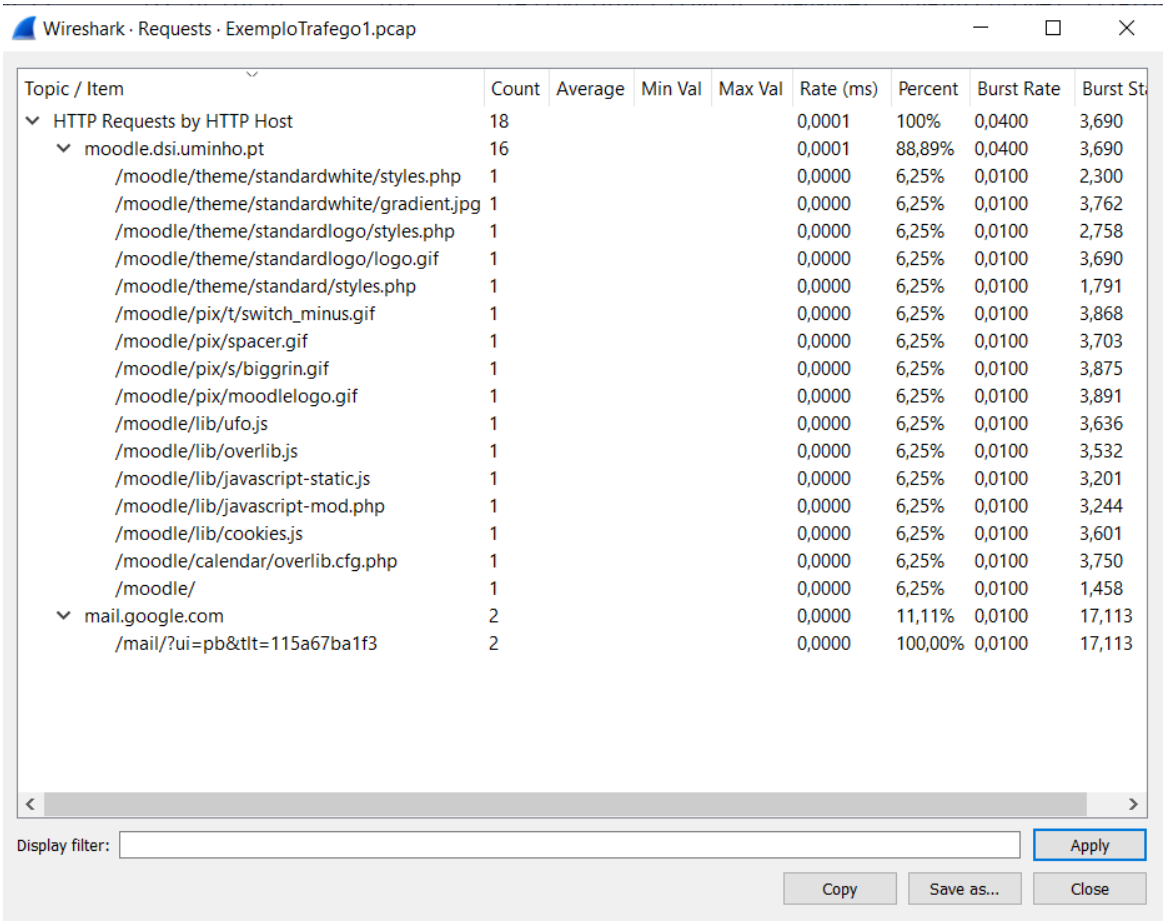


Figura 6 - Pedidos HTTP