



Universidade do Minho  
Escola de Engenharia

---

## **Universidade do Minho**

### **Trabalho Prático 4**

### **Análise de Tráfego**

### **Usando Wireshark**

---

1º Semestre – 2019/2020

Bruno Rodrigues      Pg41066

Carlos Alves      Pg41840

Paulo Bento      A81139

## Índice

Introdução .....	3
Estratégia.....	4
IP's presentes .....	4
Estatísticas Globais.....	6
Resultados da análise .....	6
Pacotes TCP .....	6
Pacotes UDP .....	9
Conclusão .....	12

## Introdução

Este trabalho prático, sugerido em aula na unidade curricular Segurança em Redes tem como objetivo fazer uso da ferramenta de captura **Wireshark** (ferramenta de captura e análise de tráfego), e desenvolver competências na definição e implementação de uma estratégia adequada à análise de tráfego.

Para este trabalho pratico foi então necessário que todos os elementos do grupo instalassem a ferramenta **Wireshark** e se familiarizassem com a mesma, de modo a poder analisar o tráfego disponibilizado pelo docente.

Neste relatório tentamos ser o máximo objetivos nas informações descritas e tentando não colocar demasiadas informações redundantes. Para isto foi pensado uma estratégia de abordagem a esta análise de tráfego que está descrita abaixo.

## Estratégia

Na realização da análise à captura do tráfego do ficheiro fornecido, começamos por identificar os IP's presentes e a sua respetiva localização e ISP. A nossa estratégia envolve principalmente a análise aprofundada de 2 protocolos (TCP e UDP). Dito isto, verificamos todo o tráfego TCP, onde fomos preenchendo a tabela abaixo ordenadamente, com as seguintes informações: *Order number*, *Time*, *Source/Destination* e ainda *Coment*.

Com isto analisamos o conteúdo de cada *stream*, de modo a observar pacotes/conteúdo suspeitos. Verificar se não ocorreu nenhuma alteração dos pacotes standard. Confirmando IP's e as portas usadas e ainda verificando quais os protocolos usados.

Utilizando a mesma estratégia referida acima, fizemos para o tráfego UDP. Onde ordenamos, verificamos se existe alguma relação com as *streams* TCP e por fim analisamos o seu conteúdo.

Para os restantes protocolos apenas foi feita uma análise rápida sem descrever detalhadamente.


Através das ferramentas *endpoints* e *conversations* do *Wireshark* é possível seguir esta estratégia. Ainda foi usada a ferramenta *I/O Graph* para analisar e tirar as últimas conclusões.

## IP's presentes

IP's observados nesta análise, respetiva localização e Provedor de Serviço Internet (ISP)

IP Address	Country	Region	City
193.137.8.215	Portugal 	Braga	Braga
ISP	Organization	Latitude	Longitude
Fundacao para a Ciencia e a Tecnologia, I.P.	Universidade do Minho (uminho.pt)	41.5503	-8.4201


Geolocation data from [ipinfo.io](https://ipinfo.io) (Product: API, real-time)

IP Address	Country	Region	City
66.249.91.17	United States 	California	Mountain View
ISP	Organization	Latitude	Longitude
Google LLC	Google LLC (google.com)	37.3860	-122.0838

**172.16.170.81 – Private network**

IP Address	Country	Region	City
41.244.211.188	Cameroon 	Littoral	Douala
ISP	Organization	Latitude	Longitude
VIETTEL CAMEROUN SARL	VIETTEL CAMEROUN SARL ( <a href="http://nexttel.com.cm">nexttel.com.cm</a> )	4.0483	9.7043

Geolocation data from [ipinfo.io](https://ipinfo.io) (Product: API, real-time)

IP Address	Country	Region	City
84.41.174.73	Netherlands 	North Holland	Amsterdam
ISP	Organization	Latitude	Longitude
Esprit Telecom B.V.	Esprit Telecom B.V. ( <a href="http://espritxb.nl">espritxb.nl</a> )	52.3991	4.9358

Geolocation data from [ipinfo.io](https://ipinfo.io) (Product: API, real-time)

IP Address	Country	Region	City
87.28.58.222	Italy 	Latium	Rome
ISP	Organization	Latitude	Longitude
Telecom Italia S.p.A.	Telecom Italia S.p.A. ( <a href="http://telecomitalia.it">telecomitalia.it</a> )	41.8919	12.5113

Geolocation data from [ipinfo.io](https://ipinfo.io) (Product: API, real-time)

IP Address	Country	Region	City
217.70.68.212	Portugal 	Lisbon	Lisbon
ISP	Organization	Latitude	Longitude
NOS COMUNICACOES, S.A.	NOS COMUNICACOES S.A. ( <a href="http://nos.pt">nos.pt</a> )	38.7167	-9.1333

Geolocation data from [ipinfo.io](https://ipinfo.io) (Product: API, real-time)

IP Address	Country	Region	City
81.64.154.175	France 	Île-de-France	Meudon
ISP	Organization	Latitude	Longitude
SFR SA	SFR SA ( <a href="http://sfr.fr">sfr.fr</a> )	48.8138	2.2350

## Estatísticas Globais

**Statistics**

<u>Measurement</u>	<u>Captured</u>	<u>Displayed</u>
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%)
Average bytes/s	1216	1216
Average bits/s	9731	9731

Observando a imagem acima, é possível determinar diversas informações sobre a captura em questão. Neste caso, foram capturados 563 pacotes num período de 152.819 segundos, 3.7 pacotes em média por segundo, tamanho medio dos pacotes foi de 330 Bytes, totalizando 185889 Bytes no final da captura.

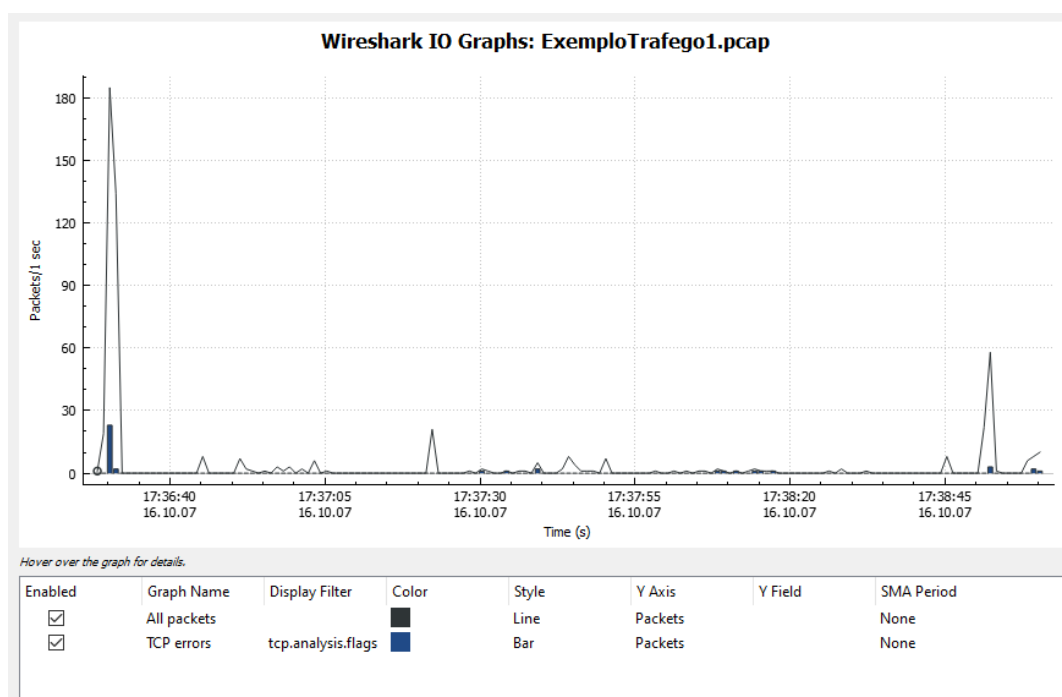
## Resultados da análise

## Pacotes TCP

<b>Order Nº</b>	<b>Time (s)</b>	<b>Src/Dest</b>	<b>Coment</b>
<b>0</b>	1.4420s (1.457307 - 2.899311)	193.137.8.106 porta 1137 - 193.137.8.215 porta 80	<ul style="list-style-type: none"> <li>Sessão HTTP entre o cliente e o servidor(<i>host</i>) moodle.dsi.uminho.pt para obter o <i>index.html</i> da página.</li> <li>Não foram detetados quaisquer erros.</li> <li>Nesta <i>stream</i> foram transferidos 35 pacotes TCP 19 <i>kBytes</i> de dados/informação.</li> </ul>
<b>1 até ao 15</b>	2.2115s	193.137.8.106 porta 1138,1140,1150... - 193.137.8.215 porta 80	<ul style="list-style-type: none"> <li>Pedidos dos respetivos itens que a página web necessita para carregar o conteúdo.</li> <li>Os erros encontrados nestas <i>streams</i> foram principalmente, gerados por alguns pacotes TCPDUP por parte do servidor. (<i>stream</i> 1 e 3)</li> <li>Nestas <i>stream's</i> foram transferidos 302 pacotes, 24521+109k = 133521 <i>Bytes</i> de informação.</li> </ul>
<b>16</b>	65.4540s	193.137.8.106 porta 1153 66.249.91.17 porta 80	<ul style="list-style-type: none"> <li>É realizado o envio de um <b>SYN</b> pelo cliente ao servidor, neste caso ao mail google; Em resposta o servidor enviou um <b>SYN-ACK</b> ao cliente. Por fim o cliente envia um <b>ACK</b> de volta ao servidor. (Nova sessão <i>html</i>).</li> <li>Foi possível observar certas informações: nomes pessoais, emails, inclusive o nome do docente.</li> </ul>

			<ul style="list-style-type: none"> <li>O último pacote evidencia que todos os dados enviados nos pacotes anteriores na sequência com um <b>ACK</b> e notifica o remetente que a conexão foi encerrada.</li> <li>Nesta <i>stream</i> foram transferidos 9 pacotes totalizando 2842 Bytes</li> </ul> <p>Packets A-&gt;B =5; Packets B-&gt;A=4</p>
17	11.3674s	193.137.8.106 porta 1154 - 193.137.8.95 porta 21	<ul style="list-style-type: none"> <li>Estabelecida uma sessão com <i>piano.dsi.uminho.pt</i>. Onde ocorreu um pedido de login, resultando no erro 530 <i>User anonymous unknown</i>. De seguida foi feito outro pedido, neste caso, de QUIT através da flag <b>FIN</b>.</li> <li>Nesta <i>stream</i> foram transferidos 14 pacotes de tamanho 918 Bytes</li> </ul>
18	28.5886s	193.137.8.106 porta 1156 - 193.137.8.95 porta 23	<ul style="list-style-type: none"> <li>Estabelecida uma sessão <b>TELNET</b> na porta 23, onde é realizado uma tentativa de login em <i>piano.dsi.uminho.pt</i>, resultando em login incorreto, devido a credenciais erradas (<i>User:guest, Password:guest</i>). Visto que o protocolo em uso é o <b>TELNET</b> é possível observar os dados em texto limpo.</li> <li>Nesta <i>stream</i> foram transferidos 53 pacotes – 3239 Bytes de dados.</li> </ul>
19 até 21	8.9989s - 8.9937s - 8.9819s	193.137.8.157 porta 30797 - 87.28.58.222 porta 11132 87.28.58.222 porta 11139 - 193.137.8.157 porta 443 87.28.58.222 porta 11141 - 193.137.8.157 porta 80	<ul style="list-style-type: none"> <li>É realizado o envio de um SYN por parte do cliente para o Servidor de modo tentar estabelecer ligação. Que acabou por não ser respondido.</li> <li>O 1º pacote é a ligação inicial, e os restantes pacotes são pacotes de retransmissão por <i>timeout</i>.</li> <li>Nestes 2 <i>stream</i> foram transferidos apenas 6(3 de cada <i>stream</i>) pacotes de tamanho total de 372(186+186) Bytes.</li> </ul>
22	0.4628s	193.137.8.106 porta 1157 -	<ul style="list-style-type: none"> <li>Nesta <i>stream</i> foi realizado o mesmo que na <i>stream</i> 16, mas sem ocorrer qualquer erro.</li> </ul>

		66.249.91.17 porta 80	<p>Sendo ainda possível observar todos os dados referidos na <i>stream</i> 16.</p> <ul style="list-style-type: none"> <li>Foram transferidos 8 pacotes de tamanho de 2788 Bytes.</li> </ul>
23	9.1543s	193.137.8.106 porta 1158 - 193.137.8.142 porta 445	<ul style="list-style-type: none"> <li>É realizada e estabelecida uma sessão <b>SMB</b>(<i>Server Message Block</i>) de transferência de ficheiros. Onde é possível observar as diferentes sessões efetuadas pelos utilizadores:  <b>BOCASJNR/hsantos</b></li> <li>Aparentemente não houve transferências de ficheiros, apenas navegação.</li> <li>É evidenciado o acesso negado em 2 ocasiões. Ocorre também a retransmissão de alguns pacotes e ainda é possível observar o cancelamento de pedidos <b>NT</b>.</li> <li>Foram transferidos 98 pacotes com o tamanho de 17 kBytes.</li> </ul>
24	0.0441s	193.137.8.106 porta 1159 - 193.137.8.142 porta 139	<ul style="list-style-type: none"> <li>Nesta <i>stream</i> é enviado um SYN pelo cliente ao servidor, no qual obteve como resposta um SYN-ACK por parte do servidor. Por fim o cliente notifica que a conexão foi encerrada.</li> <li>Foram transferidos 3 pacotes com o tamanho de 178 Bytes</li> </ul>



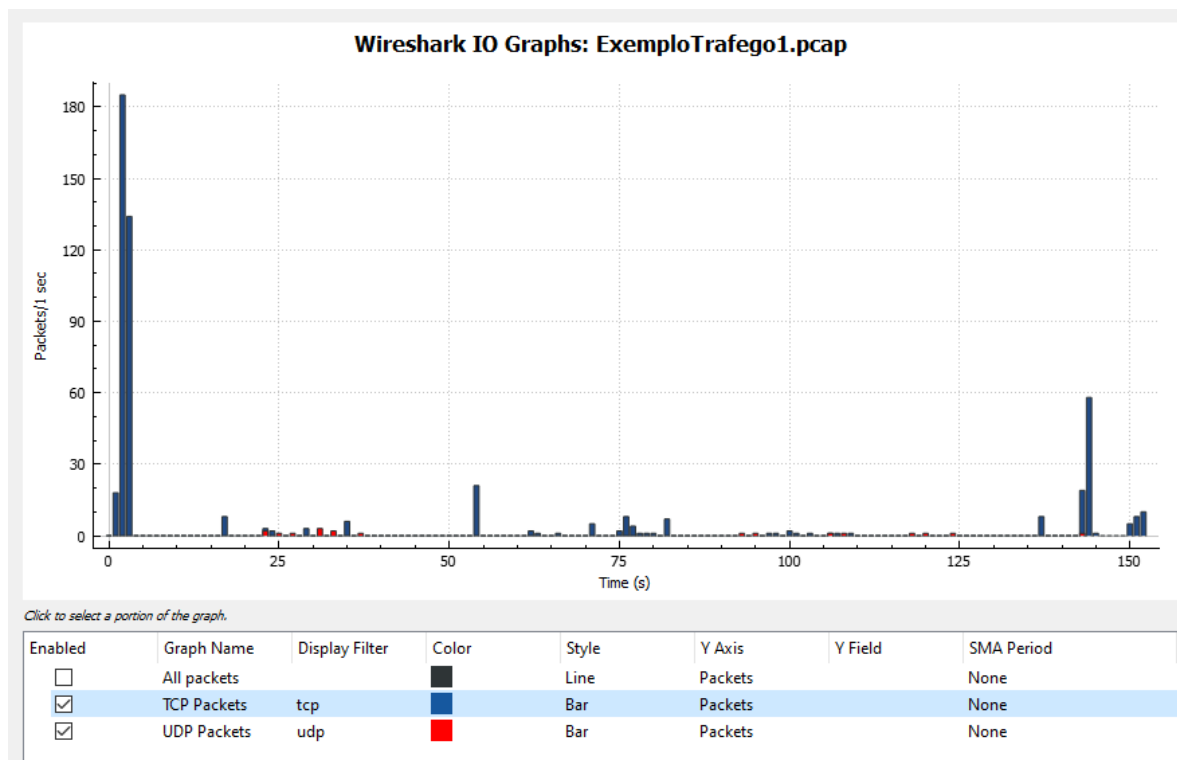
Relação de erros (pacotes TCP) com todos os pacotes



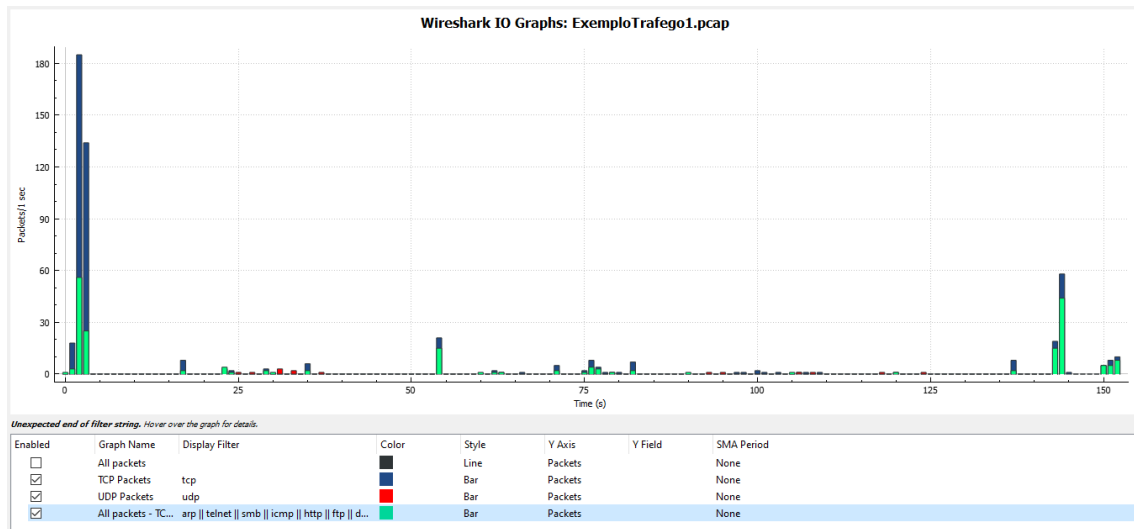
## Pacotes UDP

Order Nº	Time (s)	Src/Dest	Coment
0	0.0124s	193.137.8.106 porta 1030 - 193.137.8.142 porta 53	<ul style="list-style-type: none"> <li>Nesta <i>stream</i> é feito um pedido DNS em relação ao endereço piano.dsi.uminho.pt, no qual obteve como resposta <i>addr 193.137.8.95</i>.</li> <li>Referente a <b>TCP Stream 17</b>.</li> <li>Foram transferidos 2 pacotes com o tamanho de 174 Bytes.</li> </ul>
1 até ao 6	6.0158s    6.0433s   2.0370s   2.0223s   2.0559s   6.0266s	41.244.211.188 porta 35953 - 193.137.8.157 porta 30797  84.41.174.73 porta 38337 - 193.137.8.157 porta 30797  217.70.68.212 porta 59342 - 193.137.8.114 porta 23897  193.137.8.138 porta 39284 - 193.137.8.157 porta 30797  84.91.17.250 porta 54035 - 193.137.8.157 porta 30797  81.64.154.175 porta 43622 - 193.137.8.157 porta 30797	<ul style="list-style-type: none"> <li>Não foi possível retirar informações relevantes.</li> <li>Foram transferidos 15 pacotes com o tamanho de 1991 Bytes.</li> </ul>

7	0.0000s	193.137.8.106 porta 137 - 193.137.8.142 porta 137	<ul style="list-style-type: none"> <li>O pacote evidenciado nesta <i>stream</i> é referente á ultima <i>stream</i> <b>TCP(24)</b>, tem como objetivo converter nome legível por humanos num endereço IP</li> <li>Foram transferidos 1 pacote – 104 Bytes</li> </ul>



### Relação entre TCP Packets e UDP Packets



Como pode ser visto no gráfico acima, a percentagem de todos os pacotes juntos exceto os de TCP e UDP é bastante reduzida, logo não será feita qualquer análise escrita. Foi apenas realizada uma “busca” por anomalias nesses pacotes, concluindo que não determinamos nada de anormal.

## Conclusão

Neste trabalho tínhamos como objetivo escolher e implementar a melhor estratégia para analisar e interpretar tráfego de rede, bem como também familiarizarmo-nos com ferramentas para a execução destas tarefas.

A estratégia escolhida consistiu na análise aprofundada de dois protocolos, UDP e TCP. Foram analisados os endereços de IP, variação de pacotes e portas utilizadas pela rede.

Acreditamos que os requisitos necessários para a realização deste trabalho foram preenchidos, foi feita uma análise cuidada do tráfego de rede, como também uma filtração dos dados mais relevantes, sendo que estes foram expostos de forma clara e objetiva no decorrer do trabalho.

A dificuldade neste trabalho presenciou-se principalmente na estratégia que iríamos abordar para analisar o exemplo fornecido pelo docente. Além disto em alguns pacotes, a tarefa de descrever o seu objetivo tornou-se um pouco confusa, mas terminamos por conseguir descrever objetivamente a função de cada *stream*.

Ao ser realizado, este trabalho providenciou-nos conhecimento como também capacidades para compreender e executar análises de tráfego de rede, com recurso ao Wireshark, uma aplicação que providencia múltiplas ferramentas para este fim, sendo fundamental para a compreensão da matéria lecionada nas aulas teóricas da disciplina.