

- André Moraes (A83899)
- Francisco Lopes (A85367)
- Miguel Oliveira (A83819)
- Nelson Faria (A84727)
- Pedro Fernandes (A85853)
- Tiago Magalhães (A84485)

87% Trabalho muito bom. Assinalo apenas algumas lacunas: an

Trabalho Prático 4; ExemploTrafego1.pcap

1. Home net = 193.137.8.0/24

(Todos os endereços desta rede são indicados apenas pelo endereço da máquina, colocado entre parênteses)

2. Estratégia de análise

Numa primeira fase, começamos por perceber quais os end-points existentes no tráfego a ser analisado, assim como a ocorrência de PDU's de cada protocolo, e, inclusivé, pertencentes a diferentes camadas da pilha protocolar. Verificamos que ao nível de rede apenas é utilizado o protocolo IPv4 (inexistência de qualquer pacote IPv6). No que toca à camada de transporte, reparamos que dos 549 PDU's pertencentes à camada de transporte, 531 pertencem ao protocolo TCP (que serve de base para protocolos como http, smb, entre outros), sendo o UDP usado principalmente para pesquisas ao DNS (2 pacotes), consultas NBNS (1 pacote) e **ainda outros (15 pacotes)**.

Numa fase mais avançada resolvemos isolar e analisar separadamente cada uma das sessões estabelecidas entre os diferentes *end-points*. Para tal, tiramos partido da ferramenta "Conversations", a qual nos permite filtrar, no meio de todo o tráfego capturado, cada uma das streams entre 2 *end-points*. Coube-nos depois a nós perceber, mediante as streams obtidas, aquelas que em conjunto formam uma sessão lógica de comunicação entre duas entidades distintas, e ainda as outras que, por si só, constituem uma sessão.

Tendo separado todas essas sessões terminamos a nossa análise dando uma especial ênfase àquele tráfego que não se encaixa em nenhuma sessão lógica de comunicação, isto é, aquilo que designamos como sendo, "o lixo". A partir disto, tiramos também algumas conclusões.

3. Síntese da análise

Notas:

1. As entidades às quais um certo endereço IP pertence são definidas de acordo com a versão mais recente disponível da base de dados GeoIPLite, da autoria da "MaxMind".
2. **As linhas com cor de** devem ser analisadas com mais cuidado e prioridade mais alta, visto que contêm pacotes particularmente suspeitos.
3. A porta 30797 no destino 193.137.8.157 parece ser bem conhecida publicamente, visto que vários endereços IP completamente distintos enviam pacotes UDP para esta porta. **Aparentemente, este destino está à escuta nesta porta, e está a receber algum tipo de informação de vários endereços diferentes**. Não podemos tirar conclusões definitivas. No entanto, tendo em conta que o tráfego é UDP, que é menos útil para algo como "port scanning", para além do facto que usam sempre a mesma porta, parece indicar que este tráfego era esperado.

Nº	Nº ordem ou streams	Tempo (s)	Src/Dest	Comentário
1	357, 358, 365	25.535 a 31.551	41.244.211.188 – (157)	Endereço de origem não está presente em servidor DNS. Endereço de destino pertence à "Fundação para a Ciência e Tecnologia".

Qual a lógica de começar por

				<p>Foram trocados apenas 3 pacotes UDP(450 bytes), todos na mesma direção, de acordo com as duas primeiras afirmações.</p> <p>O endereço IP de origem está localizado nos Camarões, visto que a organização é a “Viettel”, a maior ISP do país. Deve ser verificado se é esperado tráfego desta localização.</p>
2	340-347, 425	17.040 a 17.496, 82.494	(106) – 66.249.91.17	<p>Endereço de origem pertence à “Fundação para a Ciência e Tecnologia”.</p> <p>Endereço de destino é um <i>proxy</i> pertencente à “Google”.</p> <p>É estabelecida uma sessão HTTP e feito um GET, “GET /mail/?ui=pb&lt=115a67ba1f3 HTTP/1.1”, sendo o host “mail.google.com”.</p> <p>É respondido com um código de sucesso e é transferido o conteúdo. No entanto, ocorreu algum erro, provavelmente no fecho da <i>stream</i>, visto que cerca de 65 segundos depois o originador do pedido HTTP enviou um pacote de “Reset”. Nos dados nestes pacotes foi possível observar emails e nomes, o que revela informação sensível. Foram transferidos um total de 9 pacotes com 2842 bytes de informação.</p>
3	451-458	137.534 a 137.998	(106) – 66.249.91.17	<p>Aparenta ser uma nova tentativa da conexão analisada na linha anterior. É novamente estabelecida uma sessão HTTP e o pedido é exatamente o mesmo. De facto, a única diferença entre estes pacotes e os da linha anterior é o tempo absoluto no qual ocorreram e o facto de que no fim a <i>stream</i> aparenta ter sido fechada com sucesso, visto que não existe o pacote extra de “Reset”. Forte possibilidade de ser um teste a uma app que usa a API REST do Gmail. Foram transferidos um total de 8 pacotes não contendo erros com 2788 bytes de informação.</p>
4	447, 449, 450	118.301 a 124.327	81.64.154.175 – (157)	<p>Idêntico à primeira linha de análise. As únicas diferenças são o endereço e porta de origem, e o conteúdo em si. No entanto, este endereço está presente em servidores DNS, resolvendo para “81-64-154-175.rev.numericable.fr”. Novamente, é recomendado verificar se tráfego desta localização, na França, é esperado. Foram transferidos 3 pacotes UDP e um total de 405 bytes.</p>
5	363, 366, 374	31.271 a 37.315	84.41.174.73 – (157)	<p>Idêntico à primeira linha de análise. As únicas diferenças são o endereço e porta de origem, e o conteúdo em si. Segundo a base de dados da MaxMind, este IP estará localizado nos Países Baixos, visto que a ISP é a “Esprit Telecom”. Novamente, é recomendado verificar se tráfego desta localização é esperado. Foram transferidos 3 pacotes UDP e um total de 408 bytes.</p>
6	443, 445	106.453 a 108.509	84.91.17.250 – (157)	<p>Idêntico à primeira sessão analisada. As únicas diferenças são o endereço e porta de origem, o conteúdo em si, e o número de pacotes, que</p>

				neste caso são apenas 2. Segundo a base de dados da MaxMind, este IP estará localizado em Portugal, visto que a ISP é a “netVisão”. Novamente, é recomendado verificar se tráfego desta localização é esperado. Foram transferidos 2 pacotes UDP e um total de 228 bytes.
7	435, 437, 442	97.002 a 106.001	87.28.58.222 – (157)	Neste caso em particular, o host identificado com o endereço 87.28.58.222 procura estabelecer conexão com a máquina identificada pelo IP 193.137.8.157 na porta 30797. Segundo a base de dados MaxMind, este IP está localizado em Itália(Telecom Italia), pelo que devemos verificar a legitimidade deste pedido, tendo em conta que podemos estar perante um ataque de “port scanning”. Foram enviados 3 pacotes TCP, que resultaram em retransmissão, uma vez que não houve conexão com tamanho total de 186 bytes.
8	436, 439, 444	98.608 a 107.602	87.28.58.222 – (157)	Para o caso desta sessão, verificamos que é em tudo comparável com a anterior, exceto o facto de que aqui o eventual ataque de “port scanning” seria direcionado à porta 443, ou seja, a que normalmente é usada para comunicações HTTPS. Foram enviados 3 pacotes TCP, que resultaram em retransmissão, uma vez que não houve conexão com tamanho total de 186 bytes.
9	438, 440, 446	100.222 a 109.204	87.28.58.222 – (157)	Como no caso descrito na linha 7 da tabela, e tendo em conta que a entidade que solicita a conexão é a mesma, sugerimos novamente que poderemos estar perante uma nova tentativa de “port scanning”, agora sendo feito à porta 80 (HTTP). Devemos verificar a legitimidade deste tráfego oriundo de Itália. Foram enviados 3 pacotes TCP, que resultaram em retransmissão, uma vez que não houve conexão com tamanho total de 186 bytes.
10	348, 350, 352-356, 359-361, 368-373	23.779 23.792 23.819 a 24.152 29.366 a 29.511 35.178 a 35.186	(106) – (95)	Trata-se de uma sessão FTP (com conexão TCP à porta 21), porém antes ocorreu um pedido DNS para resolução de nomes à máquina(193.137.8.142), após resolução o cliente, ao qual está associado o IP 193.137.8.106, pretendeu efetuar <i>login</i> como utilizador “anonymous”. No entanto, o servidor respondeu dizendo que tal utilizador não existia. Posto isto, o cliente desistiu da tentativa de autenticação, terminando por aqui a conexão. Foram transferidos no total 14 pacotes com 918 bytes de informação. É de salientar que tendo por base a análise desta conversaç�o conseguimos verificar uma das debilidades do protocolo de transferência de ficheiro FTP, que reside no facto de não se verificar a cifragem das mensagens trocadas entre servidor e cliente.
11	3-339	1.457 a 3.903	(106) - (215)	Sessão HTTP entre o cliente 193.137.8.106 e o servidor HTTP (193.137.8.106), onde ocorreu um pedido <i>get</i> da página principal moodle e foram abertas <i>streams</i> onde foram transferidos

			alguns erros	<p>elementos necessários para carregar a página tais como: ficheiros como imagens, <i>javascript</i>, php, etc.</p> <p>Nesta sessão foram transferidos no total 337 pacotes e um total de 154k Bytes de informação.</p>
12	375-431	54.257 a 82.845	(106) - (95)	<p>Ocorre uma sessão TELNET e observa-se uma das inseguranças do TELNET que é a revelação de informações. Assim, foi possível observar credenciais de um <i>login</i>, visto que tanto o "username" como a password são enviadas sem qualquer encriptação. Para além disso, o username e password usados são um pouco suspeitos, sendo ambos "guest". É possível que um atacante tivesse a tentar entrar numa conta "default" do sistema. Por fim, se a "Fundação para a Ciência e Tecnologia" está à espera de tráfego por telnet, este deve ser imediatamente descontinuado, devido à falta de segurança descrita acima. Foram transferidos 31 pacotes que totalizam 288 bytes de informação.</p>
13	459-563	143.654 a 152.818	(106) - (142)	<p>É estabelecida uma sessão SMB (porta 445). Nesta sessão foi possível observar caminhos de diretorias bem como nomes de <i>users</i>. Foram transferidos 106 pacotes, sendo que 7 pacotes continham erros, no total foram transferidos 18k bytes.</p> <p>Ocorre também uma resolução de nomes NBNS (através da porta 137). É trocado apenas um pacote identificado como sendo pertencente ao protocolo NBNS, mediado pelo protocolo de transporte UDP, transação muito provavelmente desencadeada por algum evento ocorrido no decorrer da conexão SMB.</p>
14	464, 467, 469	143.677 a 143.721	(106) - (142) redundante	<p>Nesta sessão em concreto, é estabelecida uma conexão TCP através de um pacote SYN enviado pelo host identificado pelo IP 193.137.8.106 para o host identificado pelo endereço 193.137.8.142, obtendo o esperado SYN+ACK como resposta, informando, ainda que implicitamente, que o cliente de que este servidor está à escuta na porta 139. No entanto, após esta resposta por parte do servidor, o cliente termina a conexão de forma inesperada, recorrendo a um pacote RST. Este tipo de conexão acaba por ser algo suspeita, podendo eventualmente constituir um exemplo prático de <i>port scanning</i>. No entanto, e tendo em conta que esta conexão é feita entre dispositivos internamente, na mesma rede local, acaba por se torna mais "fácil" verificar se tal ocorrência constitui ou não um ataque de <i>port scanning</i>.</p>
15	364, 367	31.279 33.316	217.70.68.212 - (114)	<p>Tráfego UDP de uma entidade externa à nossa rede local para uma existente na nossa rede local na porta 59342. Deve-se verificar se é esperado receber este tipo de tráfego vindo do exterior. Foram transferidos 2 pacotes UDP, com tamanho total de 252 bytes.</p>

16	433-434	93.723 a 95.745	(138)-(157)	Análise parecida à da linha 5, no entanto são transferidos menos pacotes e a máquina de origem é da mesma rede local. Foram transferidos 2 pacotes UDP mais uma vez na porta 30797, com tamanho total de 248 bytes.
17	348, 350	23.780 a 23.792	(106) - (142)	Foi direcionado um pedido de resolução do nome piano.dsi.uminho.pt, que antecedeu a sessão FTP, para o host com endereço 193.137.8.142 proveniente da máquina identificada com o IP 193.137.8.106. Este obteve o endereço associado ao nome respetivo, isto é, 193.137.8.95. Uma sessão completamente normal no contexto do protocolo DNS.

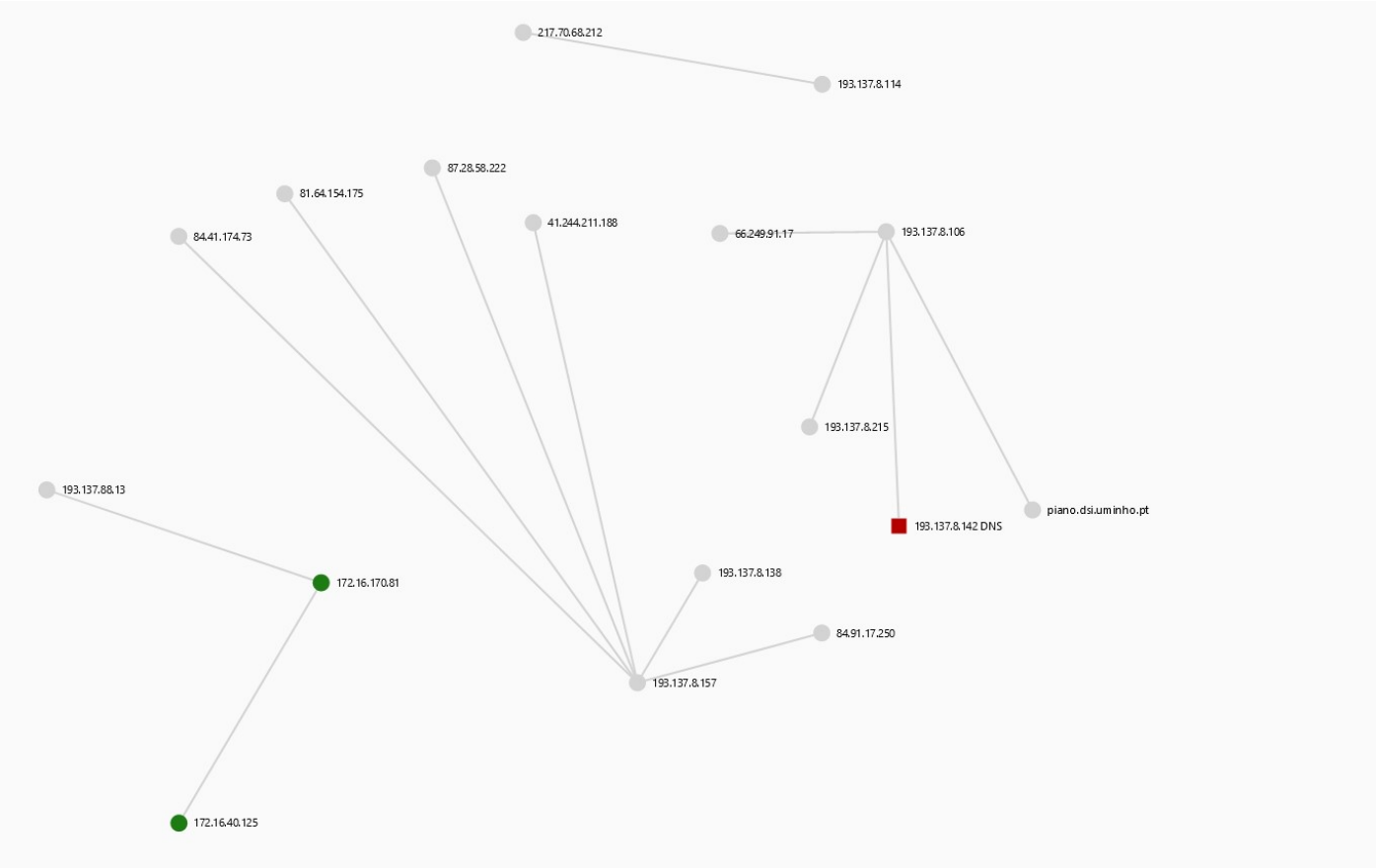


Figura 1 - Comunicação entre as várias máquinas presentes.

Em suma, pela imagem acima podemos observar as conexões entre as várias máquinas presentes neste tráfego, a máquina com IP 193.137.8.106, teve sessões normais com as máquinas: 66.249.91.17(sessão HTTP para gmail), com a máquina 193.137.8.142 que parece ser um servidor DNS desta *subnet*, bem como recebe sessões SMB sendo também um servidor para este protocolo, com a 193.137.8.215(sessão HTTP página moodle) e uma sessão FTP com a máquina 193.137.8.95 (piano.dsi.uminho.pt).

Já a máquina 193.137.8.157 parece ter a porta 30797 pública, uma vez que esta recebeu tráfego de endereços estrangeiros, é assim necessário verificar se este tráfego é esperado, também recebeu tráfego UDP de uma máquina da mesma rede local (193.137.8.138), no entanto recebeu tráfego TCP da máquina 84.91.17.259 para a porta 30797 o que não era esperado, uma vez que parece ser reservada para tráfego UDP, bem como para as portas 80 e 443 destinadas a comunicações HTTP e HTTPS respetivamente, o que nos leva a pensar que podemos estar perante um ataque de *port scan*.

Quanto ao tráfego residual é possível observar pouco tráfego ARP (podemos observar pela imagem abaixo), o que é normal apenas existiu atualização de *cache*, o que demonstra que não estamos perante ataques do tipo *ARP spoofing*, no entanto existiram comunicações ICMP entre uma máquina de endereço privado (172.16.40.125) e 193.137.86.13 para a máquina 172.16.170.81 (imagem acima canto inferior esquerdo) sem sucesso, tal como seria de esperar. Não deixamos de considerar algo suspeito e duvidoso a presença de tráfego ICMP cuja origem e destino do mesmo se encontram em redes distintas, pelo que chamamos a atenção no sentido de verificar a finalidade por trás do uso do mesmo nas circunstâncias descritas. Encontramos por fim dois pacotes de “*Configuration Test Protocol*”, tráfego gerado automaticamente pelos routers, neste caso, como podemos verificar, da “Cisco”.

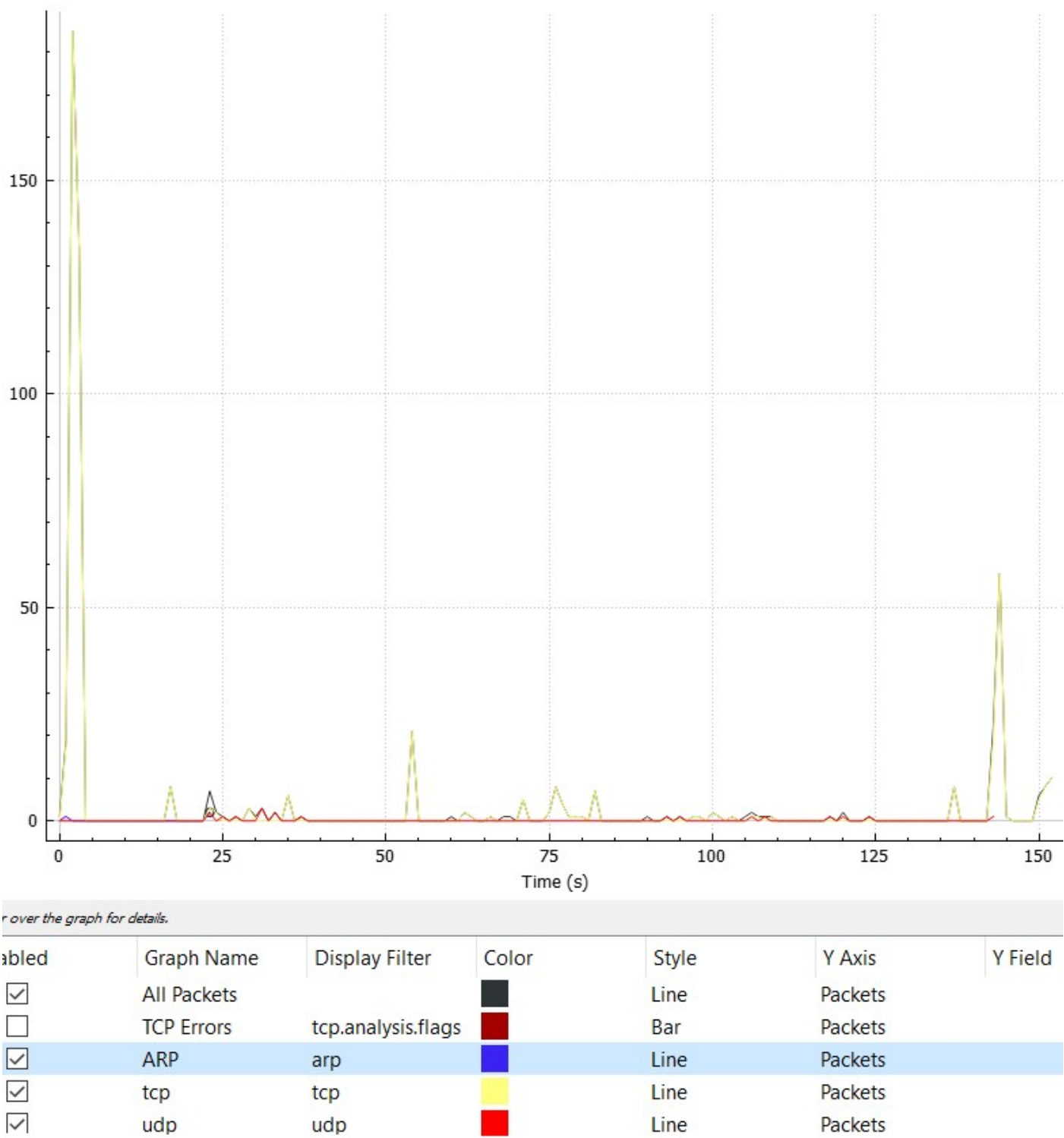


Figura 2 - Gráfico com ocorrências de tráfego ARP, TCP e UDP.