

- António Lourenço - 68452
- Jorge Ribeiro - 60027
- Pedro Alves - 61893

## Trabalho Prático 4;

### ExemploTrafego1.pcap

#### 1. Home net = 193.137.8.0/24 (scom3.uminho.pt)

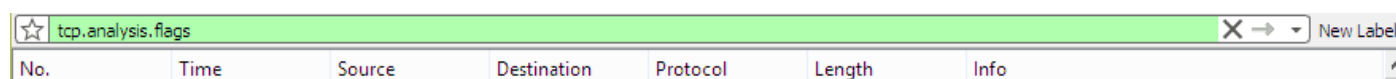
#### 2. Estratégia de análise

##### 2.1 Personalização do Wireshark

Antes da estratégia de análise propriamente dita, importa falar um pouco sobre a ambientação ao Wireshark e personalização da ferramenta.

O Wireshark é altamente customizável e flexível, esta é uma característica central da ferramenta. É muito fácil editar e criar colunas (e através delas reordenar os pacotes de várias formas), reorganizar o tráfego de acordo com os parâmetros das colunas, alterar preferências dos protocolos, criar botões para filtros usados recorrentemente, criar novas referências de tempo, etc. Através dos perfis é possível criar e alternar rapidamente entre diferentes vistas do tráfego. O primeiro passo foi então personalizar o perfil do Wireshark de modo a visualizar o tráfego de uma forma mais eficaz.

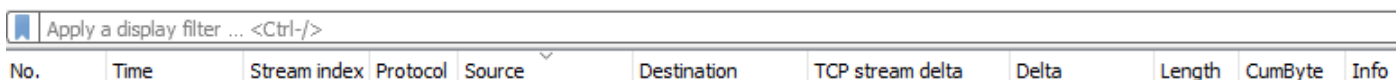
Vista original do perfil por defeito:



No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

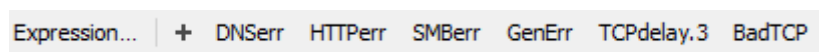
Vista depois da reconfiguração do perfil:

Colunas:



No.	Time	Stream index	Protocol	Source	Destination	TCP stream delta	Delta	Length	CumByte	Info
-----	------	--------------	----------	--------	-------------	------------------	-------	--------	---------	------

Botões:



Expression...	+	DNSerr	HTTPerr	SMBerr	GenErr	TCPdelay.3	BadTCP
---------------	---	--------	---------	--------	--------	------------	--------

As possibilidades de reconfiguração são infinitas, vamos falar um pouco das mais importantes que são perceptíveis nas imagens acima.

Nas preferências do protocolo TCP, foi ativada a opção “calculate conversation timestamps” (de onde vai aparecer o TCP stream delta) e desativada a opção “allow subdissector to reassemble TCP streams” (evita o aparecimento de alguns falsos atrasos no TCP por agrupar automaticamente alguns grupos de pacotes, por exemplo,

isto poderia acontecer ao fazer download de uma imagem por HTTP). Os deltas são importantes para detetar atrasos de resposta fora do comum e daí procurar problemas. O “stream index” é um campo gerado pelo Wireshark (são todos os campos entre parêntesis retos []), muito útil para identificar e perceber cada stream mais rapidamente.

Os botões representam filtros criados por nós (que podem assim ser usados recorrentemente e rapidamente) de modo a facilitar a descoberta de problemas. Estes serão aqui mostrados e explicados mais tarde, durante a parte final da síntese da análise.

## 2.2 Abordagem ao tráfego

Após o ponto anterior fica mais simples explicar os passos dados na análise do tráfego. Vamos enunciá-los por alto neste ponto e mais abaixo, na síntese da análise, estes serão postos em prática e explorados cada um em maior profundidade.

1. Retirar primeiras informações gerais sobre o ficheiro de captura de pacotes a ser analisado (número total de pacotes, tempo total da sessão de captura de pacotes, dimensão, etc).
2. Identificar sessões. Identificar e agrupar as streams em sessões (preencher o quadro). Referir que tipos de tráfego sobram.
3. Discutir o tráfego que não pertence às sessões TCP.
4. Gráfico que compara os erros tcp com o throughput do tráfego (em pacotes por segundo). Permite identificar rapidamente problemas que podem estar a interferir com a qualidade de comunicação sobre a rede.
5. Procura objetiva de problemas. Filtros, métodos de procura.

## 3. Síntese da análise

### 3.1. Dados gerais da captura

**Tempo total da sessão de captura de pacotes:** 152.819 segundos (2 minutos e 32.819 segundos)

**Número de total de pacotes capturados:** 563

**Tamanho do ficheiro:** 194 Kb

**Data de início da captura:** 16-10-2007 17h36m28s GMT

### 3.2. Identificação de sessões

Neste ponto foi útil juntar a coluna Stream Index (mencionado no ponto 2.1 Personalização e na imagem abaixo). Assim como a opção “Follow TCP Stream”.

Time	Stream index	Protocol	Source
3.903392	15	TCP	endpub106.scom3.uminho.pt
3.903636	15	TCP	endpub106.scom3.uminho.pt
3.903881	15	TCP	endpub215.scom3.uminho.pt
17.040244	16	TCP	endpub106.scom3.uminho.pt
17.112653	16	TCP	rate-limited-proxy-66-249-91-17...

Nº ordem ou streams	Tempo (s)	Src/Dest	Comentário
Stream: 0 - 15 Pacotes: 3 - 339	1.457307 a 3.903881	Src: endpub106.scom3.uminho.pt  Dest: Endpub215.scom3.uminho.pt	Sessão HTTP com o servidor; Durante a stream 1 ocorreram alguns erros, foi perdido um pacote [TCP Previous segment not captured], existem vários pacotes com ACK Duplicados, pacote [TCP Fast Retransmission]; Na stream 3 são enviados dois pacotes com ACK duplicados (213;214) depois de, supostamente, estar fechada a conexão, ou seja, não estava fechada de um dos lados, em resposta são enviados dois pacotes RST (Reset) para fechar a conexão (215;216); No total esta sessão envolveu 336 pacotes e 152.787KBytes;
Stream: 16 e 22  Pacotes: 340 – 347; 425; 451 – 458	17.040 a 137.997	Src: endpub106.scom3.uminho.pt  Dest: rate-limited-proxy-66-249-91-17.google.com	2 Sessões HTTP com o servidor (Sobre canal não seguro para email); Nesta stream não surgem pacotes [FIN,ACK] para terminar a conexão, em vez disso é terminada com um pacote [RST] (425); A comunicação foi feita sobre um canal não seguro (HTTP). É possível interceptar a mensagem HTTP e ler o seu conteúdo (exemplificado na imagem abaixo). Deveria ter sido usado o protocolo HTTPS. No total envolveu 38 pacotes e 5.630Kbytes. <pre>GET /mail/?ui=pb&amp;tl=115a67ba1f3 HTTP/1.1 User-Agent: Mozilla/5.0 (compatible; GNotify 1.0.25.0) Host: mail.google.com Connection: Keep-Alive Cache-Control: no-cache Cookie: GV=10115a9980eb7-6dec08d9f1dfd9f8b6151b4afca9a9f4; __utma=173272373.870200234.1175466843.1175466843.1175466843.1; gmailchat=eu.nuno@gmail.com/104902; S=gmail=280v8-GZ5SSMzZQu8Lkpwg:gmail_yj=7gECZkY1yCB029on0c6XoQ:gmpoxy=jd3pMfLR7ic:gmpoxy_yj=kkWdq9Ty1Gc:gmpoxy_yj_sub=w8G-7FLAEk0; PREF=ID=77a64c6088f3ea1c;TM=1167250258;LM=1167250258;S=USGBHPfj9i5dGP-M; SID=DQAAAHKAAAZEF93t00V4RhNjywuq0A1q05K15D7fy7oHDx6tbyp6nrUjce49LXvmTkdYgVSBhdsnX0poppXnB9nv56CSWQ9q2mEV_nXu0ibw2phTg3Rc6YXkRAlyGjU11F-ByEQDnPr0zp16S8nAnj6o3LkIL-9XdD0ZpU7Fc2VkdTbnkQ  HTTP/1.1 200 OK Cache-control: no-cache, no-store Pragma: no-cache Content-Type: application/octet-stream Content-Length: 1422 Server: GFE/1.3 Date: Tue, 16 Oct 2007 16:36:34 GMT  ....."....^all...^i...^u..7 1 .membership@techtargt.com.au..SearchStorage ANZ.....ETape encryption; Exchange Backup; 4PB of tape; Google's storage plans..0SearchStorage ANZ : Weekly Site RoundUp &amp;hellip;... ....."....^all...^i...^u..( " .program@mentornet.net. MentorNet.....[MentorNet DS]: Interviews..eFor Match with Sam Bartels) Henrique, Giving a good interview is a skill that we often learn &amp;hellip;... ....."....^all...^i...^u..4 . .membership@techtargt.com.au..TechTarget ANZ.....HNew White Papers: Intelligent storage; Security risk reduction; and more..jTechTarget ANZ : White Paper Update Welcome to TechTarget ANZ#39;s White Paper Update, featuring &amp;hellip;...</pre>
Stream: 17 Pacotes: 352 – 356; 359 – 361; 368 – 373;	23.819 a 35.186	Src: endpub106.scom3.uminho.pt  Dest: piano.dsi.uminho.pt	Sessão FTP com o servidor; O FTP não foi desenvolvido tendo em conta a segurança e privacidade e é por isso um protocolo especialmente vulnerável a vários tipos de ataques, tais como Brute Force attack, FTP bounce attack, captura de pacotes e Spoofing. Isto acontece primariamente por o FTP não encriptar os dados, enviando sempre tudo em texto simples, sendo possível aceder a essas informações com um simples sniffing. Na captura de tráfego com que trabalhamos é possível ver que houve bastante atividade durante a sessão FTP, embora não pareça ser problemática. Entre os pacotes 359 e 360 foi trocada informação de autenticação, mas como o USER era desconhecido, foi terminada a sessão FTP nos pacotes 368 e 369; Envolveu 14 pacotes e 918Bytes;

<u>Stream:</u> 18 <u>Pacotes:</u> 375 – 395 397 – 400 403 – 424 426 – 431	54.257 a 82.845	<u>Src:</u> endpub106.scom3.uminho.pt  <u>Dest:</u> piano.dsi.uminho.pt	<p>Sessão Telnet;</p> <p>Ocorreram alguns erros e foi necessário retransmitir alguns pacotes;</p> <p>Surge também um pacote [TCP ACKed unseen segment] que significa que algum pacote foi perdido ou “não capturado”;</p> <p>De notar o uso do velhinho TELNET, este não é seguro. É possível através do Wireshark ver os dados de autenticação introduzidos (imagem abaixo). É aconselhado, em vez do TELNET, o uso do SSH.</p> <p>A sessão envolveu 53 pacotes e 3.239KBytes;</p> <pre> Digital UNIX (piano.dsi.uminho.pt) (ttyp1) . . . ....login: guest guest Password:guest  Login incorrect  Wait for login retry ...  Login incorrect login: .^D.. </pre>
<u>Stream:</u> 19 a 21 <u>Pacotes:</u> 435 – 440; 442; 444; 446	97.001 a 109.203	<u>Src:</u> host222-58-static.28-87-b.business.telecomitalia.it  <u>Dest:</u> endpub157.scom3.uminho.pt	<p>Em todas as (3) streams no primeiro pacote é enviado um [SYN], no entanto não houve resposta por parte do servidor, tendo o pacote [SYN] sido retransmitido duas vezes, mas sem resposta.</p> <p>No total a sessão envolveu 9 pacotes;</p> <p>Há a tentativa de contacto desde um IP associado à business.telecomitalia.it (sem sucesso), após pesquisa foi notado que este domínio está associado ao envio de spam.</p> <p>Além disso, é suspeito devido ao uso portas “invulgares”;</p>
<u>Stream:</u> 23 e 24 <u>Pacotes:</u> 461; 463 – 539; 541 – 563	143.66 a 152.81	<u>Src:</u> endpub106.scom3.uminho.pt  <u>Dest:</u> endpub142.scom3.uminho.pt	<p>Nesta sessão foi utilizado o protocolo SMB que tem vulnerabilidades, pois os protocolos SMB e NetBIOS podem revelar informações de segurança de uma rede. O NetBIOS torna possível a um atacante mapear uma rede e navegar uma rede intranet comprometida. Desactivar estes dois serviços pode aumentar a segurança da rede.</p> <p>Nesta sessão alguns segmentos foram perdidos e foram retransmitidos alguns pacotes.</p> <p>Esta sessão envolveu 98 pacote e 17.543KBytes.</p> <p>Na stream 24 houve a tentativa de estabelecer uma ligação, no entanto foi imediatamente encerrada com um pacote [RST].</p>

### 3.3 Tráfego que não pertence às sessões

Ordenando o tráfego pela Coluna Stream Index é simples separar o tráfego que não pertence às sessões TCP. São 32 pacotes (imagem abaixo) pertencentes aos protocolos ICMP, NBNS, UDP, ARP e DNS.

540	150.336312	ICMP	endpub013.scom-glt.uminho.pt	172.16.170.81	5.173401	114	Echo (ping) request	id=0x0041, seq=18538/27...
462	143.672084	NBNS	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.007533	104	Name query response	NB 193.137.8.142
460	143.660955	ICMP	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.006551	74	Echo (ping) reply	id=0x0300, seq=768/3, t...
459	143.654404	ICMP	endpub106.scom3.uminho.pt	endpub142.scom3.uminho.pt	5.656588	74	Echo (ping) request	id=0x0300, seq=768/3, t...
450	124.327858	UDP	81-64-154-175.rev.numericable...	endpub157.scom3.uminho.pt	4.007710	135	43622 → 30797	Len=93
449	120.320148	UDP	81-64-154-175.rev.numericable...	endpub157.scom3.uminho.pt	0.080017	135	43622 → 30797	Len=93
448	120.240131	ICMP	endpub013.scom-glt.uminho.pt	172.16.170.81	1.938901	114	Echo (ping) request	id=0x0041, seq=18191/39...
447	118.301230	UDP	81-64-154-175.rev.numericable...	endpub157.scom3.uminho.pt	9.097485	135	43622 → 30797	Len=93
445	108.509339	UDP	acb1-84-91-17-250.netvisao.pt	endpub157.scom3.uminho.pt	0.907717	114	54035 → 30797	Len=72
443	106.453435	UDP	acb1-84-91-17-250.netvisao.pt	endpub157.scom3.uminho.pt	0.452681	114	54035 → 30797	Len=72
441	105.037733	ICMP	172.16.40.125	172.16.170.81	1.837155	98	Echo (ping) request	id=0x2c1e, seq=256/1, t...
434	95.745304	UDP	endpub138.scom3.uminho.pt	endpub157.scom3.uminho.pt	2.022277	124	39284 → 30797	Len=82
433	93.723027	UDP	endpub138.scom3.uminho.pt	endpub157.scom3.uminho.pt	3.525689	124	39284 → 30797	Len=82
432	90.197338	ICMP	endpub013.scom-glt.uminho.pt	172.16.170.81	7.351341	114	Echo (ping) request	id=0x0041, seq=17849/47...
402	69.513079	LOOP	CiscoInc_08:d6:d9	CiscoInc_08:d6:d9	0.565356	60	Reply	
401	68.947723	LOOP	CiscoInc_ef:54:d9	CiscoInc_ef:54:d9	2.578474	60	Reply	
396	60.155486	ICMP	endpub013.scom-glt.uminho.pt	172.16.170.81	5.378753	114	Echo (ping) request	id=0x0041, seq=17495/22...
374	37.315007	UDP	84.41.174.73	endpub157.scom3.uminho.pt	2.128215	136	38337 → 30797	Len=94
367	33.316836	UDP	a217-70-68-212.cpe.netcabo.pt	endpub114.scom3.uminho.pt	0.012492	126	59342 → 23897	Len=84
366	33.304344	UDP	84.41.174.73	endpub157.scom3.uminho.pt	1.752860	136	38337 → 30797	Len=94
365	31.551484	UDP	41.244.211.188	endpub157.scom3.uminho.pt	0.271666	150	35953 → 30797	Len=108
364	31.279818	UDP	a217-70-68-212.cpe.netcabo.pt	endpub114.scom3.uminho.pt	0.008157	126	59342 → 23897	Len=84
363	31.271661	UDP	84.41.174.73	endpub157.scom3.uminho.pt	1.194318	136	38337 → 30797	Len=94
362	30.077343	ICMP	endpub013.scom-glt.uminho.pt	172.16.170.81	0.566216	114	Echo (ping) request	id=0x0041, seq=17137/61...
358	27.548662	UDP	41.244.211.188	endpub157.scom3.uminho.pt	2.012980	150	35953 → 30797	Len=108
357	25.535682	UDP	41.244.211.188	endpub157.scom3.uminho.pt	1.383618	150	35953 → 30797	Len=108
351	23.819171	ARP	piano.dsi.uminho.pt	193.137.8.106	0.027093	60	193.137.8.95 is at 00:00:f8:1f:3d:ce	
350	23.792078	DNS	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.005776	95	Standard query response	0xbe32 A piano.dsi.u...
349	23.786302	ARP	193.137.8.106	HewlettP_b6:66:cb	0.006652	42	193.137.8.106 is at 00:13:77:05:f4:c3	
348	23.779650	DNS	endpub106.scom3.uminho.pt	endpub142.scom3.uminho.pt	6.283368	79	Standard query	0xbe32 A piano.dsi.uminho.pt
2	1.456585	ARP	193.137.8.215	193.137.8.106	1.456585	60	193.137.8.215 is at 00:08:02:b6:5a:a0	
1	0.000000	ICMP	endpub013.scom-glt.uminho.pt	172.16.170.81	0.000000	114	Echo (ping) request	id=0x0041, seq=16779/35...

Em relação a este tráfego, o UDP acontece em portas com número muito alto, o que levanta suspeitas. Assim como os elevados delta times.

Existe um pedido NBNS (NetBIOS Name Service), serviço que traduz nomes para endereços IP, mas que não é usado atualmente, apesar de apenas existir um pacote, vale a pena dizer que o uso deste pode ser desativado tanto do lado do cliente como do servidor, após verificar que não existe nenhuma aplicação que o use.

O ARP também não levanta suspeitas, teria de aparecer em muito maior número para poder ser problemático.

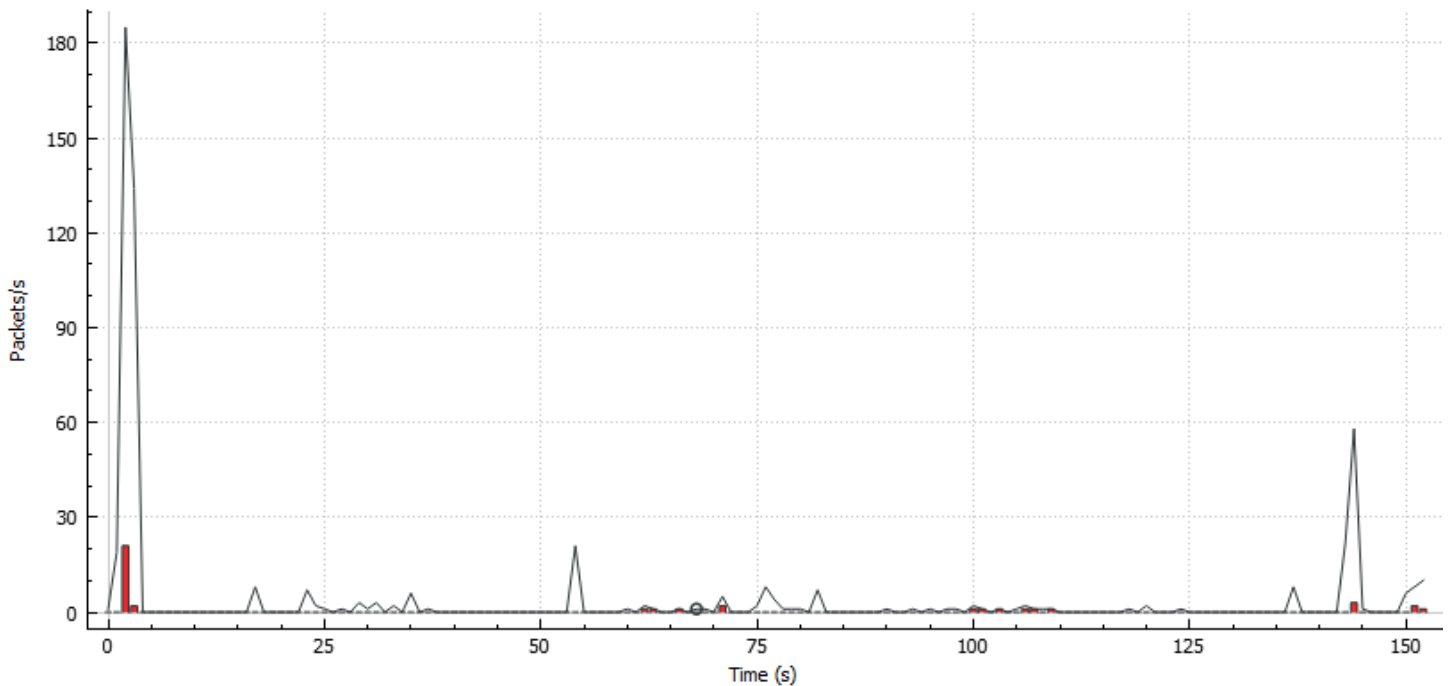
Quanto aos pacotes ICMP, os 'pings' no ICMP são geralmente inofensivos, a não ser que existam em grande quantidade. Como um 'ping' é representado normalmente por um pacote pequeno, é difícil que mesmo através de 'spoofing' sejam transmitidos muitos dados. Sendo que o maior problema será mesmo a transmissão de informações acerca da estrutura interna de uma rede, o que não é um problema caso esta já seja pública.

### 3.4. Gráfico que compara os erros tcp com o throughput do tráfego (em pacotes por segundo)




Com este gráfico procura-se responder à pergunta, existem problemas de rede a afetar o throughput? Throughput da rede é a taxa de envio bem-sucedido de mensagens sobre o canal de comunicação, pode ser medido em bits por segundo ou em pacotes de dados por segundo. Este gráfico é até chamado pela fundadora da Wireshark University como “the golden graph”.

Deste modo é possível encontrar rapidamente relações entre problemas no TCP e flutuação no throughput.

## Wireshark IO Graphs: Exemplo Trafego1



No packets in interval (72s).

Name	Display filter	Color	Style	Y Axis	Y Field	Smoothing
<input checked="" type="checkbox"/> All packets			Line	Packets/s		None
<input type="checkbox"/> TCP errors	tcp.analysis.flags		Bar	Packets/s		None
<input checked="" type="checkbox"/> Bad TCP	(tcp.analysis.flags && !tcp.analysis.window_update)		Bar	Packets/s		None

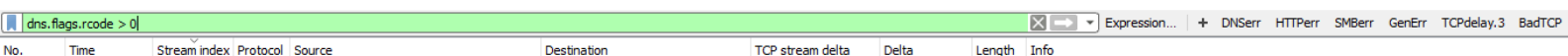
É possível clicar num ponto no gráfico e saltar para a stream correspondente. A notar problemas na rede ao por volta dos 2 segundos, como é possível ver no gráfico, existiram dificuldades na comunicação sobre o canal TCP.

Neste caso a causa daquela barra maior vermelha são acks duplicados, isto quer dizer que o recetor encontrou pacotes em falta e que existiram dificuldades na utilização do canal TCP ou na ordenação dos pacotes.

### 3.5. Procura de problemas, Métodos de procura

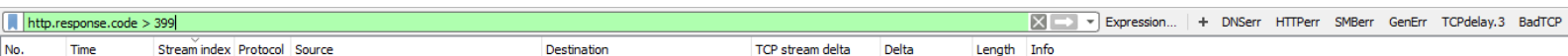
Os botões criados no ponto 2.1 (personalização), servirão agora para rapidamente procurar alguns tipos de erro.

1. Botão para procurar erros DNS (Filtro: `dns.flags.rcode > 0`)



Não existem erros DNS.

2. Botão para procurar erros no HTTP (Filtro: `http.response.code > 399`) (Não há erros HTTP)





### 3. Botão para procurar erros no SMB (Filtro: smb.nt\_status > 0 || smb2.nt\_status > 0)

smb.nt_status > 0    smb2.nt_status > 0										
No.	Time	Stream index	Protocol	Source	Destination	TCP stream delta	Delta	Length	Info	
547	151.215868	23	SMB	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.004715000	0.534715	93	NT Trans Response, FID: 0x4006, NT NOTIFY, Error: STATUS_CANCELLED	
542	150.681153	23	SMB	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.007556000	5.812621	93	NT Trans Response, FID: 0x4007, NT NOTIFY, Error: STATUS_CANCELLED	
512	144.868532	23	SMB	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.002390000	0.027901	93	Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED	
507	144.840631	23	SMB	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.026941000	0.028264	506	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MOR...	
505	144.812367	23	SMB	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.014271000	0.015072	93	Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_F...	
503	144.797295	23	SMB	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.014972000	0.487755	93	Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_F...	
485	144.309540	23	SMB	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.018604000	0.312405	93	Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_F...	
479	143.997135	23	SMB	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.071567000	0.086754	506	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MOR...	
475	143.910381	23	SMB	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.025090000	0.113263	93	Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED	
471	143.797118	23	SMB	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.075504000	0.000000	506	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MOR...	

Existem 10 pacotes com erros no SMB. Este ponto já foi abordado no ponto anterior, na especificação das sessões TCP do tráfego.

### 4. Atrasos no TCP; Filtro: ((tcp.time\_delta > .3) && (tcp.flags.fin == 0)) && (tcp.flags.reset == 0)

É sempre um bom critério procurar pelos maiores delta times do TCP para encontrar problemas. Foi definido aqui como sendo um delta problemático se esse for maior do que 300 milissegundos. Este critério poderia variar um pouco e o melhor seria mesmo se existissem Baselines. Baselines são capturas de tráfego nas mesmas condições sem qualquer problema, a sua observação permitiria chegar a um melhor critério. As outras duas condições são para evitar falsos positivos. Não interessam pacotes de fim de sessão ou de reset pois estes têm normalmente deltas maiores sem ter de facto nenhum problema.

((tcp.time_delta > .3) && (tcp.flags.fin == 0)) && (tcp.flags.reset == 0)										
No.	Time	Stream index	Protocol	Source	Destination	TCP stream delta	Delta	Length	Info	
554	152.647762	23	TCP	endpub142.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.812455000	1.974165	158	[TCP Retransmission] microsoft-ds → dbcontrol-oms [PSH, ACK] Seq=...	
541	150.673597	23	SMB	endpub106.scom3.uminho.pt	endpub142.scom3.uminho.pt	5.510686000	41.469852	94	NT Cancel Request	
446	109.203745	21	TCP	host222-58-static.28-87-b.bus...	endpub157.scom3.uminho.pt	6.003167000	1.602123	62	[TCP Retransmission] 11141 → http [SYN] Seq=0 Win=17520 Len=0 MSS...	
440	103.200578	21	TCP	host222-58-static.28-87-b.bus...	endpub157.scom3.uminho.pt	2.978782000	1.605241	62	[TCP Retransmission] 11141 → http [SYN] Seq=0 Win=17520 Len=0 MSS...	
444	107.601622	20	TCP	host222-58-static.28-87-b.bus...	endpub157.scom3.uminho.pt	6.006285000	1.600868	62	[TCP Retransmission] 11139 → https [SYN] Seq=0 Win=17520 Len=0 MS...	
439	101.595337	20	TCP	host222-58-static.28-87-b.bus...	endpub157.scom3.uminho.pt	2.987447000	1.589651	62	[TCP Retransmission] 11139 → https [SYN] Seq=0 Win=17520 Len=0 MS...	
442	106.000754	19	TCP	host222-58-static.28-87-b.bus...	endpub157.scom3.uminho.pt	5.995068000	2.800176	62	[TCP Retransmission] 11132 → 30797 [SYN] Seq=0 Win=17520 Len=0 MS...	
437	100.005686	19	TCP	host222-58-static.28-87-b.bus...	endpub157.scom3.uminho.pt	3.003862000	17.191343	62	[TCP Retransmission] 11132 → 30797 [SYN] Seq=0 Win=17520 Len=0 MS...	
426	82.814343	18	TELNET	endpub106.scom3.uminho.pt	piano.dsi.uminho.pt	2.773848000	2.957466	55	Telnet Data ...	
423	79.856877	18	TELNET	piano.dsi.uminho.pt	endpub106.scom3.uminho.pt	1.785082000	2.140571	78	Telnet Data ...	
418	77.716306	18	TELNET	endpub106.scom3.uminho.pt	piano.dsi.uminho.pt	0.992025000	1.686257	56	Telnet Data ...	
410	76.030049	18	TELNET	endpub106.scom3.uminho.pt	piano.dsi.uminho.pt	0.500991000	0.542735	55	Telnet Data ...	
408	75.487314	18	TELNET	endpub106.scom3.uminho.pt	piano.dsi.uminho.pt	3.977753000	4.305783	55	Telnet Data ...	
403	71.181531	18	TCP	endpub106.scom3.uminho.pt	piano.dsi.uminho.pt	4.812282000	4.812282	61	[TCP Retransmission] iascontrol-oms → telnet [PSH, ACK] Seq=62 Ac...	
400	66.369249	18	TCP	endpub106.scom3.uminho.pt	piano.dsi.uminho.pt	2.406302000	2.406302	59	[TCP Retransmission] iascontrol-oms → telnet [PSH, ACK] Seq=62 Ac...	
399	63.962947	18	TCP	endpub106.scom3.uminho.pt	piano.dsi.uminho.pt	1.202629000	1.202629	59	[TCP Retransmission] iascontrol-oms → telnet [PSH, ACK] Seq=62 Ac...	
398	62.760318	18	TCP	endpub106.scom3.uminho.pt	piano.dsi.uminho.pt	0.548849000	0.548849	55	[TCP Keep-Alive] iascontrol-oms → telnet [PSH, ACK] Seq=62 Ack=11...	
397	62.211469	18	TELNET	endpub106.scom3.uminho.pt	piano.dsi.uminho.pt	7.434736000	27.033371	55	Telnet Data ...	
368	35.178098	17	FTP	endpub106.scom3.uminho.pt	piano.dsi.uminho.pt	5.666971000	5.811104	60	Request: QUIT	
359	29.366994	17	FTP	endpub106.scom3.uminho.pt	piano.dsi.uminho.pt	5.214930000	11.871042	70	Request: USER anonymous	
345	17.495952	16	HTTP	rate-limited-proxy-66-249-91-...	endpub106.scom3.uminho.pt	0.300093000	14.327674	1314	HTTP/1.1 200 OK (application/octet-stream)	
206	3.168278	3	HTTP	endpub215.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.404107000	0.343562	644	HTTP/1.1 200 OK (text/css)	
172	2.739865	2	HTTP	endpub215.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.428361000	0.533748	1032	HTTP/1.1 200 OK (text/css)	
21	2.206117	1	HTTP	endpub215.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.403752000	0.431913	1314	HTTP/1.1 200 OK [Unreassembled Packet]	
184	2.824716	0	TCP	endpub215.scom3.uminho.pt	endpub106.scom3.uminho.pt	1.048997000	0.084851	1314	http → trim [ACK] Seq=5185 Ack=627 Win=6886 Len=1260	
8	1.774204	0	HTTP	endpub215.scom3.uminho.pt	endpub106.scom3.uminho.pt	0.304814000	0.000000	1314	HTTP/1.1 200 OK [Unreassembled Packet]	

Esta é uma visão muito interessante, existem aqui vários pacotes que podem indicar problemas, estes já foram discutidos ao longo deste documento.