



Universidade do Minho
Escola de Engenharia

Mestrado em Engenharia de Telecomunicações e Informática

Unidade Curricular de Cibersegurança

Docente: Henrique Santos

TP 3: Análise de Tráfego

Bárbara Fonseca PG53677

Camila Pinto PG53712

Eduarda Dinis PG53793

Gonçalo Dias PG53833

Bruno Santos A93087

Guimarães, abril de 2024

1. Introdução

Este trabalho foi realizado no contexto da UC de Cibersegurança e tinha como objetivo entendermos melhor como funciona a ferramenta Wireshark e desenvolvimento de competências na análise e interpretação de tráfego.

Inicialmente estávamos um bocado perdidos, uma vez que não tínhamos sensibilidade no que toca a olhar para tráfego, o que dificultou bastante a realização do trabalho numa fase mais inicial; porém, com o decorrer das aulas e depois de tiradas algumas dúvidas com o professor, a tarefa tornou-se cada vez mais simples, ainda que tivéssemos, mesmo assim, alguma dificuldade; os tutoriais fornecidos também foram uma grande ajuda para saber como se manipulava o Wireshark.

Foi também relativamente difícil, numa fase inicial, a que o grupo chegasse a um consenso sobre o que considerávamos que seria uma sessão, o que fez com que o trabalho também não tivesse sido resolvido mais rapidamente, porém, uma vez que estávamos todos na mesma página, e tendo em conta que já tínhamos tido algumas explicações do professor, conseguimos desenvolver a solução.

2. Home net

Subrede da rede Home Net = 10.10.100.0/24

3. Estratégia da análise

Como já referido, inicialmente, não sabíamos como usar da melhor forma o Wireshark e isso complicou a análise, mas uma vez que o grupo percebeu o que queria fazer, decidimos criar um Excel para poder analisar todo o tráfego numa só página de forma mais simples.

Nesta secção do relatório vamos tentar explicar qual foi o nosso raciocínio para a realização de algumas etapas e como é que estávamos a visualizar o tráfego/o problema em si.

Numa fase inicial, estávamos apenas a ver as *streams* todas, usando o filtro “tcp.stream eq x” sendo o x as iterações de cada stream e depois fomos anotando as streams que pareciam da mesma sessão usando os seguintes critérios: IP de origem, IP de destino, *PORT* origem e *PORT* destino. Também usamos a estatística Endpoints para ver esta informação. Ao ver apenas estes critérios, tínhamos imensas sessões e a solução não nos parecia a mais correta, por isso pensamos em como podíamos analisar com mais facilidade o tráfego e o que pensamos foi fazer um Excel com essas informações, foi nesta altura que descobrimos que existia o *Follow TCP stream*, que nos facilitou imenso a análise do tráfego. Depois de termos criado o Excel com as informações que consideramos relevantes, pesquisamos sobre todos os domínios/protocolos que não conhecíamos, pois certas informações não nos fazia sentido uma vez que não sabíamos o que eram, por exemplo o “incoming.telemetry.mozilla.org” ou então o “fonts.gstatic.com”.

| Nº da stream | IP origem | IP destino | Port origem | Port destino | Website |
|--------------|---------------|-----------------|-------------|--------------|--------------------------------|
| 0 | 10.10.100.121 | 216.58.209.68 | 47492 | 443 | www.google.com |
| 1 | 10.10.100.121 | 142.250.184.163 | 47524 | 80 | ocsp.pki.goog |
| 2 | 10.10.100.121 | 34.120.208.123 | 48294 | 443 | incoming.telemetry.mozilla.org |
| 3 | 10.10.100.121 | 142.250.200.99 | 47112 | 443 | www.gstatic.com |
| 4 | 10.10.100.121 | 142.250.200.99 | 47114 | 443 | www.gstatic.com |
| 5 | 10.10.100.121 | 142.250.184.163 | 47532 | 80 | ocsp.pki.goog |
| 6 | 10.10.100.121 | 142.250.200.142 | 52742 | 443 | apis.google.com |
| 7 | 10.10.100.121 | 142.250.184.163 | 47518 | 80 | Em branco |
| 8 | 10.10.100.121 | 142.250.184.163 | 47516 | 80 | Em branco |
| 9 | 10.10.100.121 | 142.250.184.163 | 47520 | 80 | Em branco |
| 10 | 10.10.100.121 | 216.58.209.68 | 47484 | 443 | Cifrada |
| 11 | 10.10.100.121 | 142.250.201.69 | 37152 | 80 | gmail.com |
| 12 | 10.10.100.121 | 142.250.201.69 | 37154 | 80 | Em branco |
| 13 | 10.10.100.121 | 142.250.200.101 | 36830 | 443 | mail.google.com |
| 14 | 10.10.100.121 | 142.250.110.84 | 38478 | 443 | accounts.google.com |
| 15 | 10.10.100.121 | 216.58.215.131 | 58028 | 443 | fonts.gstatic.com |
| 16 | 10.10.100.121 | 216.58.215.131 | 58030 | 443 | fonts.gstatic.com |
| 17 | 10.10.100.121 | 142.250.200.78 | 51294 | 443 | accounts.youtube.com |
| 18 | 10.10.100.121 | 216.58.215.174 | 38452 | 443 | play.google.com |
| 19 | 10.10.100.121 | 216.58.215.174 | 38454 | 443 | play.google.com |
| 20 | 10.10.100.121 | 140.98.193.101 | 40012 | 443 | services10.ieeee.org |
| 21 | 10.10.100.121 | 104.18.20.226 | 51802 | 80 | ocsp.globalsign.com |
| 22 | 10.10.100.121 | 140.98.193.101 | 40016 | 443 | services10.ieeee.org |
| 23 | 10.10.100.121 | 140.98.193.101 | 40018 | 443 | services10.ieeee.org |
| 24 | 10.10.100.121 | 140.98.193.101 | 40020 | 443 | services10.ieeee.org |
| 25 | 10.10.100.121 | 140.98.193.101 | 40022 | 443 | services10.ieeee.org |
| 26 | 10.10.100.121 | 140.98.193.101 | 40024 | 443 | services10.ieeee.org |
| 27 | 10.10.100.121 | 142.250.200.99 | 47152 | 443 | ssl.gstatic.com |
| 28 | 10.10.100.121 | 173.194.76.94 | 38466 | 443 | accounts.google.pt |

Figura 1. Divisão das Sessões

| | | | | |
|----|---------------|-----------------|-------|--|
| 29 | 10.10.100.121 | 216.58.209.78 | 55110 | 443 chat.google.com |
| 30 | 10.10.100.121 | 142.250.200.110 | 47102 | 443 lh3.google.com |
| 31 | 10.10.100.121 | 142.250.184.10 | 51852 | 443 ogads-pa.clients6.google.com |
| 32 | 10.10.100.121 | 142.250.184.10 | 51854 | 443 ogads-pa.clients6.google.com |
| 33 | 10.10.100.121 | 142.250.201.74 | 58678 | 443 waa-pa.clients6.google.com |
| 34 | 10.10.100.121 | 142.250.201.74 | 58680 | 443 waa-pa.clients6.google.com |
| 35 | 10.10.100.121 | 142.250.184.163 | 47584 | 80 ocsp.pki.goog |
| 36 | 10.10.100.121 | 142.250.184.163 | 47586 | 80 em branco |
| 37 | 10.10.100.121 | 142.250.200.65 | 34796 | 443 lh3.googleusercontent.com |
| 38 | 10.10.100.121 | 142.250.200.78 | 51336 | 443 ogs.google.com |
| 39 | 10.10.100.121 | 142.250.200.74 | 51818 | 443 safebrowsing.googleapis.com |
| 40 | 10.10.100.121 | 142.250.184.163 | 47594 | 80 ocsp.pki.goog |
| 41 | 10.10.100.119 | 10.10.100.117 | 42388 | 21 algum login |
| 42 | 10.10.100.121 | 34.107.221.82 | 51822 | 80 detectportal.firefox.com |
| 43 | 10.10.100.121 | 34.107.221.82 | 51826 | 80 detectportal.firefox.com |
| 44 | 10.10.100.119 | 10.10.100.117 | 54606 | 29522 acesso a ficheiros? |
| 45 | 10.10.100.121 | 34.107.243.93 | 59488 | 443 cifrado |
| 46 | 10.10.100.119 | 10.10.100.117 | 38470 | 35884 um codigo de "Execution Hijacked" |
| 47 | 10.10.100.119 | 10.10.100.117 | 53910 | 56996 Ficheiro de teste para transmiss..o. |
| 48 | 10.10.100.119 | 10.10.100.120 | 49171 | 80 em branco |
| 49 | 10.10.100.119 | 10.10.100.117 | 49171 | 80 em branco |
| 50 | 10.10.100.119 | 10.10.100.120 | 49171 | 22 em branco |
| 51 | 10.10.100.119 | 10.10.100.117 | 49171 | 22 em branco |
| 53 | 10.10.100.119 | 10.10.100.120 | 49171 | 139 em branco |
| 53 | 10.10.100.119 | 10.10.100.117 | 49171 | 139 em branco |
| 54 | 10.10.100.119 | 10.10.100.120 | 49171 | 25 em branco |
| 55 | 10.10.100.119 | 10.10.100.117 | 49171 | 25 em branco |
| 56 | 10.10.100.119 | 10.10.100.120 | 56078 | 445 microsoft smb |
| 57 | 10.10.100.121 | 161.58.148.77 | 1182 | 587 troca de mails? |

Figura 2. Divisão das Sessões

As figuras 1 e 2 mostram como fizemos a divisão das sessões após termos feito o Excel; antes de termos feito isto tínhamos, sensivelmente, 7 sessões, o que não correspondia a uma boa solução tendo em conta que não sabíamos ao certo como se classificava uma sessão.

Voltando às figuras, cada cor (verde, azul, vermelho) indica uma sessão diferente e aqui podemos observar que considerávamos o acesso aos serviços da IEEE como sendo uma sessão em si; fizemos esta consideração porque a porta de origem era completamente diferente e já não se tratava de um serviço Google, como nas *streams* diretamente acima. Considerando também que, nas *streams* diretamente abaixo, se tratava, mais uma vez, de domínios da Google, relacionamos as streams de cima com estas agora referidas, isolando os serviços da IEEE. Também pensamos que pudessem haver dois clientes na mesma rede a usar a internet simultaneamente e que um tivesse a aceder à Google e outro à IEEE, fazendo com que os Timestamps fossem praticamente os mesmos.

Posteriormente, vimos que o acesso à IEEE não era uma sessão em si, isto foi conseguido pela ajuda do professor, que nos indicou que das streams 0 até à 41 (não incluída) era tudo a mesma sessão. Para provarmos isto, analisamos uma estatística que não tínhamos analisado ainda que é o Rel Start, que nos mostra a *timeline* relativa de cada conversação,

que nos mostra que há mudanças de sessões observando este campo, uma vez que o tempo muda drasticamente, como podemos observar nas imagens seguintes.

Wireshark - Conversations - Cyber_shark.pcapng

| 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 |
|---------------|--------|-----------------|--------|---------|--------|---------------|-------------|---------------|-------------|------------------|----------|--------------|--------------|
| 10.10.100.121 | 1182 | 161.58.148.77 | 587 | 30 | 5584 | 16 | 4513 | 14 | 1071 | 455844159.731390 | 3.7464 | 9636 | 2286 |
| 10.10.100.121 | 47492 | 216.58.209.68 | 443 | 751 | 744 k | 290 | 42 k | 461 | 702 k | 2.924449 | 52.5112 | 6422 | 107 k |
| 10.10.100.121 | 47524 | 142.250.184.163 | 80 | 47 | 12 k | 24 | 4953 | 23 | 7839 | 3.020387 | 61.8305 | 640 | 1014 |
| 10.10.100.121 | 48294 | 34.120.208.123 | 443 | 33 | 8263 | 18 | 2614 | 15 | 5649 | 3.593778 | 58.9890 | 354 | 766 |
| 10.10.100.121 | 47112 | 142.250.200.99 | 443 | 23 | 7290 | 14 | 1724 | 9 | 5566 | 4.086093 | 0.3357 | 41 k | 132 k |
| 10.10.100.121 | 47114 | 142.250.200.99 | 443 | 1551 | 1535 k | 618 | 85 k | 933 | 1449 k | 4.086093 | 58.7192 | 11 k | 197 k |
| 10.10.100.121 | 47532 | 142.250.184.163 | 80 | 27 | 5022 | 14 | 2052 | 13 | 2970 | 4.185160 | 61.6675 | 266 | 385 |
| 10.10.100.121 | 52742 | 142.250.200.142 | 443 | 304 | 262 k | 147 | 14 k | 157 | 248 k | 4.935762 | 56.5381 | 2066 | 35 k |
| 10.10.100.121 | 47518 | 142.250.184.163 | 80 | 14 | 924 | 7 | 462 | 7 | 462 | 5.229774 | 60.2272 | 61 | 61 |
| 10.10.100.121 | 47516 | 142.250.184.163 | 80 | 14 | 924 | 7 | 462 | 7 | 462 | 5.246657 | 60.2429 | 61 | 61 |
| 10.10.100.121 | 47520 | 142.250.184.163 | 80 | 14 | 924 | 7 | 462 | 7 | 462 | 5.250666 | 60.2312 | 61 | 61 |
| 10.10.100.121 | 47484 | 216.58.209.68 | 443 | 42 | 5265 | 14 | 1425 | 28 | 3840 | 14.093827 | 0.8074 | 14 k | 38 k |
| 10.10.100.121 | 37152 | 142.250.201.69 | 80 | 17 | 2064 | 9 | 922 | 8 | 1142 | 16.598423 | 50.2212 | 146 | 181 |
| 10.10.100.121 | 37154 | 142.250.201.69 | 80 | 6 | 412 | 4 | 272 | 2 | 140 | 16.598423 | 5.9447 | 366 | 188 |
| 10.10.100.121 | 36830 | 142.250.200.101 | 443 | 1757 | 2822 k | 678 | 98 k | 1079 | 2724 k | 16.896994 | 46.3305 | 16 k | 470 k |
| 10.10.100.121 | 38478 | 142.250.110.84 | 443 | 356 | 236 k | 123 | 26 k | 233 | 209 k | 18.549180 | 40.1820 | 5289 | 41 k |
| 10.10.100.121 | 58028 | 216.58.215.131 | 443 | 23 | 7272 | 14 | 1706 | 9 | 5566 | 19.404943 | 0.1680 | 81 k | 265 k |
| 10.10.100.121 | 58030 | 216.58.215.131 | 443 | 254 | 216 k | 118 | 10 k | 136 | 205 k | 19.405067 | 40.4939 | 2022 | 40 k |
| 10.10.100.121 | 51294 | 142.250.200.78 | 443 | 118 | 82 k | 52 | 8515 | 66 | 74 k | 20.178670 | 39.4504 | 1726 | 15 k |
| 10.10.100.121 | 38452 | 216.58.215.174 | 443 | 587 | 681 k | 634 | 139 | 448 | 46 k | 30.010210 | 34.0360 | 149 k | 11 k |
| 10.10.100.121 | 38454 | 216.58.215.174 | 443 | 51 | 13 k | 26 | 3404 | 25 | 9852 | 30.010378 | 32.6375 | 834 | 2414 |
| 10.10.100.121 | 40012 | 140.98.193.101 | 443 | 111 | 149 k | 56 | 11 k | 55 | 138 k | 30.259777 | 37.5049 | 2423 | 29 k |
| 10.10.100.121 | 51802 | 104.18.20.226 | 80 | 15 | 3299 | 8 | 921 | 7 | 2378 | 30.875181 | 30.1385 | 244 | 631 |
| 10.10.100.121 | 40016 | 140.98.193.101 | 443 | 29 | 18 k | 14 | 3310 | 15 | 15 k | 31.225765 | 31.2591 | 847 | 3992 |
| 10.10.100.121 | 40018 | 140.98.193.101 | 443 | 77 | 109 k | 38 | 5757 | 39 | 103 k | 31.227000 | 31.3740 | 1467 | 26 k |
| 10.10.100.121 | 40020 | 140.98.193.101 | 443 | 42 | 39 k | 20 | 3692 | 22 | 36 k | 31.228489 | 31.2440 | 945 | 9229 |
| 10.10.100.121 | 40022 | 140.98.193.101 | 443 | 15 | 5862 | 9 | 1207 | 6 | 4655 | 32.208558 | 5.9848 | 1613 | 6222 |
| 10.10.100.121 | 40024 | 140.98.193.101 | 443 | 17 | 5994 | 9 | 1207 | 8 | 4787 | 32.209690 | 5.9804 | 1614 | 6403 |
| 10.10.100.121 | 47152 | 142.250.200.99 | 443 | 22 | 7225 | 13 | 1658 | 9 | 5567 | 48.201946 | 0.1432 | 92 k | 310 k |
| 10.10.100.121 | 38466 | 173.194.76.94 | 443 | 29 | 11 k | 15 | 3141 | 14 | 8600 | 50.003194 | 0.3828 | 65 k | 179 k |
| 10.10.100.121 | 55110 | 216.58.209.78 | 443 | 1,669 | 2429 k | 595 | 122 k | 1,074 | 2307 k | 51.328823 | 12.8325 | 76 k | 1438 k |
| 10.10.100.121 | 47102 | 142.250.200.110 | 443 | 30 | 15 k | 15 | 3475 | 15 | 11 k | 53.826919 | 0.1895 | 146 k | 488 k |
| 10.10.100.121 | 51852 | 142.250.184.10 | 443 | 38 | 16 k | 19 | 4047 | 19 | 12 k | 54.447312 | 0.0263 | 51 k | 164 k |
| 10.10.100.121 | 51854 | 142.250.184.10 | 443 | 33 | 14 k | 18 | 2404 | 15 | 11 k | 54.447373 | 0.3204 | 60 k | 298 k |

Figura 3. Estatísticas "Conversations"

Wireshark - Conversations - Cyber_shark.pcapng

| | | | | | | | | | | | | | |
|---------------|-------|-----------------|-------|----|------|----|------|----|------|-------------|---------|-------|--------|
| 10.10.100.121 | 34796 | 142.250.200.65 | 443 | 57 | 20 k | 29 | 4414 | 28 | 15 k | 55.596280 | 5.0111 | 7046 | 25 k |
| 10.10.100.121 | 51336 | 142.250.200.78 | 443 | 22 | 9708 | 14 | 1724 | 8 | 7984 | 56.559522 | 0.1397 | 98 k | 457 k |
| 10.10.100.121 | 51818 | 142.250.200.74 | 443 | 38 | 10 k | 19 | 2803 | 19 | 7595 | 57.352067 | 1.2764 | 17 k | 47 k |
| 10.10.100.121 | 47594 | 142.250.184.163 | 80 | 9 | 1686 | 5 | 712 | 4 | 974 | 57.438776 | 10.1971 | 558 | 764 |
| 10.10.100.119 | 42386 | 10.10.100.117 | 21 | 55 | 3788 | 28 | 1690 | 27 | 2098 | 550.872770 | 48.8619 | 276 | 343 |
| 10.10.100.121 | 51822 | 34.107.221.82 | 80 | 11 | 1230 | 6 | 684 | 5 | 546 | 557.113110 | 39.9482 | 136 | 109 |
| 10.10.100.121 | 51826 | 34.107.221.82 | 80 | 11 | 1235 | 6 | 689 | 5 | 546 | 557.195391 | 39.9085 | 138 | 109 |
| 10.10.100.119 | 54606 | 10.10.100.117 | 29522 | 8 | 1308 | 4 | 236 | 4 | 1072 | 564.533449 | 0.0052 | 366 k | 1664 k |
| 10.10.100.121 | 59488 | 34.107.243.93 | 443 | 4 | 342 | 2 | 171 | 2 | 171 | 565.735093 | 0.0303 | 45 k | 45 k |
| 10.10.100.119 | 38470 | 10.10.100.117 | 35884 | 8 | 741 | 4 | 236 | 4 | 505 | 573.519980 | 0.0039 | — | — |
| 10.10.100.117 | 56996 | 10.10.100.119 | 53910 | 8 | 513 | 3 | 186 | 5 | 327 | 594.606556 | 0.0051 | 290 k | 510 k |
| 10.10.100.119 | 56078 | 10.10.100.120 | 445 | 87 | 13 k | 53 | 7152 | 34 | 6005 | 1583.254058 | 53.7408 | 1064 | 893 |
| 10.10.100.119 | 49717 | 10.10.100.120 | 80 | 3 | 172 | 2 | 112 | 1 | 60 | 2592.467409 | 0.0010 | — | — |
| 10.10.100.119 | 49717 | 10.10.100.117 | 80 | 3 | 172 | 2 | 112 | 1 | 60 | 2592.468606 | 0.0010 | — | — |
| 10.10.100.119 | 49717 | 10.10.100.120 | 22 | 3 | 172 | 2 | 112 | 1 | 60 | 2592.872077 | 0.0004 | — | — |
| 10.10.100.119 | 49717 | 10.10.100.117 | 22 | 3 | 172 | 2 | 112 | 1 | 60 | 2592.872498 | 0.0004 | — | — |
| 10.10.100.119 | 49717 | 10.10.100.120 | 139 | 3 | 172 | 2 | 112 | 1 | 60 | 2593.274349 | 0.0005 | — | — |
| 10.10.100.119 | 49717 | 10.10.100.117 | 139 | 3 | 172 | 2 | 112 | 1 | 60 | 2593.274866 | 0.0003 | — | — |
| 10.10.100.119 | 49717 | 10.10.100.120 | 25 | 2 | 118 | 1 | 58 | 1 | 60 | 2593.679101 | 0.0009 | — | — |
| 10.10.100.119 | 49717 | 10.10.100.117 | 25 | 2 | 118 | 1 | 58 | 1 | 60 | 2593.680246 | 0.0009 | — | — |

Figura 4. Continuação Estatísticas "Conversations"

Vemos, na Figura 4 por exemplo, que há uma mudança de 57.438776 para 550.872770, indicando uma mudança de sessão tendo em conta que o tempo muda drasticamente.

Depois de usar este método para análise, mais o restante conhecimento adquirido anteriormente, solidificou ainda mais o nosso conceito de sessão e o nosso excel passou a ser como está nas imagens seguintes (Figuras 4 e 5), fazendo com que esta fosse a nossa solução final. Mais uma vez, cada cor representa uma sessão e as *streams* de cor diferente (as últimas duas) não associamos a nenhuma sessão, tendo em conta que o Rel Start destas *streams* está isolado das outras. É de notar que nas imagens seguintes apenas estão presentes as *streams* TCP.

| Nº da stream | IP origem | IP destino | Port origem | Port destino | Website/Domínio |
|--------------|---------------|-----------------|-------------|--------------|--|
| 0 | 10.10.100.121 | 216.58.209.68 | 47492 | 443 | www.google.com |
| 1 | 10.10.100.121 | 142.250.184.163 | 47524 | 80 | ocsp.pki.goog |
| 2 | 10.10.100.121 | 34.120.208.123 | 48294 | 443 | incoming.telemetry.mozilla.org |
| 3 | 10.10.100.121 | 142.250.200.99 | 47112 | 443 | www.gstatic.com |
| 4 | 10.10.100.121 | 142.250.200.99 | 47114 | 443 | www.gstatic.com |
| 5 | 10.10.100.121 | 142.250.184.163 | 47532 | 80 | ocsp.pki.goog |
| 6 | 10.10.100.121 | 142.250.200.142 | 52742 | 443 | apis.google.com |
| 7 | 10.10.100.121 | 142.250.184.163 | 47518 | 80 | Em branco |
| 8 | 10.10.100.121 | 142.250.184.163 | 47516 | 80 | Em branco |
| 9 | 10.10.100.121 | 142.250.184.163 | 47520 | 80 | Em branco |
| 10 | 10.10.100.121 | 216.58.209.68 | 47484 | 443 | Cifrada |
| 11 | 10.10.100.121 | 142.250.201.69 | 37152 | 80 | gmail.com |
| 12 | 10.10.100.121 | 142.250.201.69 | 37154 | 80 | Em branco |
| 13 | 10.10.100.121 | 142.250.200.101 | 36830 | 443 | mail.google.com |
| 14 | 10.10.100.121 | 142.250.110.84 | 38478 | 443 | accounts.google.com |
| 15 | 10.10.100.121 | 216.58.215.131 | 58028 | 443 | fonts.gstatic.com |
| 16 | 10.10.100.121 | 216.58.215.131 | 58030 | 443 | fonts.gstatic.com |
| 17 | 10.10.100.121 | 142.250.200.78 | 51294 | 443 | accounts.youtube.com |
| 18 | 10.10.100.121 | 216.58.215.174 | 38452 | 443 | play.google.com |
| 19 | 10.10.100.121 | 216.58.215.174 | 38454 | 443 | play.google.com |
| 20 | 10.10.100.121 | 140.98.193.101 | 40012 | 443 | services10.ieee.org |
| 21 | 10.10.100.121 | 104.18.20.226 | 51802 | 80 | ocsp.globalsign.com |
| 22 | 10.10.100.121 | 140.98.193.101 | 40016 | 443 | services10.ieee.org |
| 23 | 10.10.100.121 | 140.98.193.101 | 40018 | 443 | services10.ieee.org |
| 24 | 10.10.100.121 | 140.98.193.101 | 40020 | 443 | services10.ieee.org |
| 25 | 10.10.100.121 | 140.98.193.101 | 40022 | 443 | services10.ieee.org |
| 26 | 10.10.100.121 | 140.98.193.101 | 40024 | 443 | services10.ieee.org |
| 27 | 10.10.100.121 | 142.250.200.99 | 47152 | 443 | ssl.gstatic.com |
| 28 | 10.10.100.121 | 173.194.76.94 | 38466 | 443 | accounts.google.pt |

Figura 5. Divisão Final das Sessões

| | | | | | |
|----|---------------|-----------------|-------|-------|--------------------------------------|
| 29 | 10.10.100.121 | 216.58.209.78 | 55110 | 443 | chat.google.com |
| 30 | 10.10.100.121 | 142.250.200.110 | 47102 | 443 | lh3.google.com |
| 31 | 10.10.100.121 | 142.250.184.10 | 51852 | 443 | ogads-pa.clients6.google.com |
| 32 | 10.10.100.121 | 142.250.184.10 | 51854 | 443 | ogads-pa.clients6.google.com |
| 33 | 10.10.100.121 | 142.250.201.74 | 58678 | 443 | waa-pa.clients6.google.com |
| 34 | 10.10.100.121 | 142.250.201.74 | 58680 | 443 | waa-pa.clients6.google.com |
| 35 | 10.10.100.121 | 142.250.184.163 | 47584 | 80 | ocsp.pki.goog |
| 36 | 10.10.100.121 | 142.250.184.163 | 47586 | 80 | em branco |
| 37 | 10.10.100.121 | 142.250.200.65 | 34796 | 443 | lh3.googleusercontent.com |
| 38 | 10.10.100.121 | 142.250.200.78 | 51336 | 443 | ogs.google.com |
| 39 | 10.10.100.121 | 142.250.200.74 | 51818 | 443 | safebrowsing.googleapis.com |
| 40 | 10.10.100.121 | 142.250.184.163 | 47594 | 80 | ocsp.pki.goog |
| 41 | 10.10.100.119 | 10.10.100.117 | 42388 | 21 | Login |
| 42 | 10.10.100.121 | 34.107.221.82 | 51822 | 80 | detectportal.firefox.com |
| 43 | 10.10.100.121 | 34.107.221.82 | 51826 | 80 | detectportal.firefox.com |
| 44 | 10.10.100.119 | 10.10.100.117 | 54606 | 29522 | Diretoria com ficheiros |
| 45 | 10.10.100.121 | 34.107.243.93 | 59488 | 443 | Cifrado |
| 46 | 10.10.100.119 | 10.10.100.117 | 38470 | 35884 | Execution Hijacked |
| 47 | 10.10.100.119 | 10.10.100.117 | 53910 | 56996 | Ficheiro de teste para transmiss..o. |
| 48 | 10.10.100.119 | 10.10.100.120 | 49171 | 80 | Em branco |
| 49 | 10.10.100.119 | 10.10.100.117 | 49171 | 80 | Em branco |
| 50 | 10.10.100.119 | 10.10.100.120 | 49171 | 22 | Em branco |
| 51 | 10.10.100.119 | 10.10.100.117 | 49171 | 22 | Em branco |
| 53 | 10.10.100.119 | 10.10.100.120 | 49171 | 139 | Em branco |
| 53 | 10.10.100.119 | 10.10.100.117 | 49171 | 139 | Em branco |
| 54 | 10.10.100.119 | 10.10.100.120 | 49171 | 25 | Em branco |
| 55 | 10.10.100.119 | 10.10.100.117 | 49171 | 25 | Em branco |
| 56 | 10.10.100.119 | 10.10.100.120 | 56078 | 445 | microsoft smb |
| 57 | 10.10.100.121 | 161.58.148.77 | 1182 | 587 | troca de mails? |

Figura 6. Continuação Divisão Final das Sessões

4. Síntese da Análise

O tráfego UDP foi também analisado usando filtros e fazendo TCP streams, porém não foram encontradas nenhuma anomalias, a maior parte destas *streams* UDP eram os serviços da Google.

Analisamos também os pacotes que não faziam parte das sessões TCP, isto foi conseguido através do filtro “!tcp.stream” e o que observamos foram *broadcasts* usando o protocolo ARP e observamos também protocolos DNS a serem usados. Tirando as UDP *streams*, usam todos o protocolo ARP menos um pacote que utiliza ICMPv6 que serve para gestão da rede.

Como nos foi recomendado, também procuramos por tráfego fragmentado, porém, não encontramos nenhum tráfego deste tipo, fazendo com que a identificação de atividades maliciosas na rede não seja tão óbvia uma vez que este tipo de tráfego não está presente.

Nesta tabela, não estarão presentes os IP/PORT de origem e destino, uma vez que a imagem da divisão da sessões em cima torna a visualização destes dados mais clara.

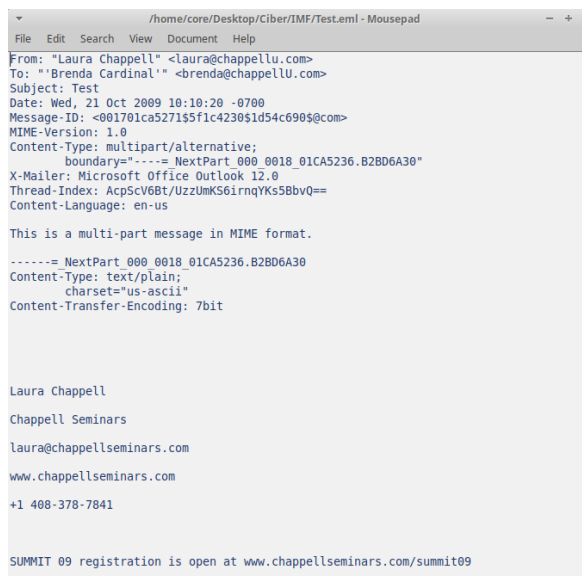
Nota: para facilitar o cálculo do tamanho total dos pacotes e do número de pacotes consultamos a estatística conversações, portanto, o número exato de *bytes* transmitido não é mostrado, sendo que a *stream* 0, por exemplo aparece como sendo 744k *bytes*, quando na verdade são 744603 *bytes*, portanto haverá alguma imprecisão no número total de *bytes*.

| Nº de streams | Tempo (s) | Comentário |
|-----------------|-------------------|--|
| Stream x – y | 00.00 a 00.00 | ----- |
| Streams 0 - 40 | 2.92 a 67.63 | <p>Nesta sessão, foram trocados 8347 pacotes com um tamanho total de 7132661 bytes.</p> <p>Nesta sessão podemos observar que o utilizador usufruiu dos serviços da Google, tais como o Gmail, acesso ao Youtube ou até acesso à página da IEEE. Esta sessão foi a mais demorada e a que teve mais tráfego de pacotes, tendo em conta que o utilizador usou bastantes serviços diferentes que requerem a que várias ligações sejam estabelecidas para aceder a um determinado serviço.</p> |
| Streams 41-47 | 550.87 a 594.61 | <p>Nesta sessão foram trocados 105 pacotes com um tamanho total de 9157 bytes.</p> <p>Nesta sessão é estabelecida uma conexão a um servidor FTP, que é um protocolo que é usado para a transferência de ficheiros entre um cliente e um servidor. É feito um login com uma certa password e depois é feito um download de um ficheiro de texto e de um ficheiro em C.</p> <p>Na stream 41 é possível observar que é usada uma Virtual Machine para esta interação, daí haverem vários IP de origem nesta sessão.</p> |
| Streams 48 - 55 | 2592.46 a 2593.68 | <p>Nesta sessão foram trocados 22 pacotes com um tamanho total de 1268 bytes.</p> <p>Nesta sessão há várias tentativas de aceder a um serviço uma vez que os pacotes [SYN] e [SYN, ACK] estão presentes, porém, este acesso não é realizado tendo em conta que, de seguida, existe um pacote de reset [RST] indicando que a ação não foi realizada com sucesso. Esta tentativa de acesso pode ser considerada como maliciosa, uma vez que este processo se repete múltiplas vezes, porém, também pode significar falhas na ligação ou então um encerramento abrupto da sessão.</p> |

Tabela 1. Sessões

A *stream* 56 não foi considerada uma vez que não conseguimos relacioná-la a nenhuma das sessões, uma vez que, por exemplo, o seu tempo relativo é cerca de 1583.25 e a *stream* anterior a esta (de acordo com o tempo relativo) é a 47 e a seguinte a 48. Porém, observamos que esta *stream* utiliza SMB2, o que não é normal, tendo em conta que este protocolo já não é muito utilizado, o que poderia indicar que alguém possivelmente pudesse estar a fazer um *exploit* com este protocolo, porém, não identificamos nenhuma anomalia.

A *stream* 57 também não foi considerada tendo em conta que o seu timestamp é do ano de 2009, portanto é altamente improvável que seja a mesma sessão das restantes, contudo, observamos que esta *stream* é interessante uma vez que se trata de uma troca de *e-mails*.



The screenshot shows a window titled "/home/core/Desktop/Ciber/IMF/Test.eml - Mousepad". The email content is as follows:

```
File Edit Search View Document Help
From: "Laura Chappell" <laura@chappellu.com>
To: "Brenda Cardinal" <brenda@chappellu.com>
Subject: Test
Date: Wed, 21 Oct 2009 10:10:20 -0700
Message-ID: <001701ca52715f1c423051d54c6905@com>
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="-----= NextPart_000_0018_01CA5236.B2BD6A30"
X-Mailer: Microsoft Office Outlook 12.0
Thread-Index: AcpScV6Bt/UzzUmKS6irnqYKs5BbvQ==
Content-Language: en-us

This is a multi-part message in MIME format.
-----= NextPart_000_0018_01CA5236.B2BD6A30
Content-Type: text/plain;
        charset="us-ascii"
Content-Transfer-Encoding: 7bit

Laura Chappell
Chappell Seminars
laura@chappellseminars.com
www.chappellseminars.com
+1 408-378-7841

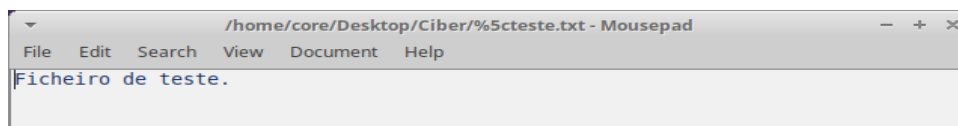
SUMMIT 09 registration is open at www.chappellseminars.com/summit09
```

Figura 7. Follow TCP Stream 57

Voltado ao restante tráfego, ao longo destas sessões, foram transmitidos pacotes [*TCP Keep-Alive*] que servem para detetar se a conexão está parada ou deixou de responder, esta verificação é importante uma vez que não convém ao utilizador ficar sem resposta e não haver um protocolo que faça essa verificação.

Também observamos que houve perdas de pacotes nesta sessão, tal é comprovado com a presença dos pacotes [*TCP ACKed unseen segment*] e [*TCP dup ACK*], que indicam problemas com pacotes, tanto como o pedido da retransmissão de pacotes bem como a perda dos mesmos. Tendo em conta que alguns pacotes se encontram com estes avisos, poderá haver problemas na rede que teriam que ser investigados.

Na sessão 2 o utilizador realizou um *download* de um ficheiro .txt, a Figura 8 mostra o ficheiro que conseguimos observar pelo Wireshark.



The screenshot shows a window titled "/home/core/Desktop/Ciber/%5cteste.txt - Mousepad". The text content is:

```
File Edit Search View Document Help
Ficheiro de teste.
```

Figura 8. Ficheiro Transferido na Sessão 2.

5. Conclusão

Com este trabalho, vimos como é verdadeiramente trabalhar com o Wireshark e visualizar tráfego numa rede, agora que adquirimos este conhecimento, estamos bastante mais à vontade a olhar e a interpretar para pacotes, protocolos, portas, *stream*, etc. Posto isto, sentimos que foi um trabalho enriquecedor e que complementou a nossa formação como engenheiros de telecomunicações.

É da nossa opinião também que, apesar de não termos recebido muitas informações no início do desenvolvimento do projeto, isto fez com que a nossa pesquisa fosse mais intensa e que a nossa compreensão do trabalho fosse mais profunda, mesmo tendo em conta de que andamos meio “perdidos” para obter uma solução final que foi a apresentada neste relatório.