UC/Curso: Cibersegurança / Mestrado em Engenharia de Telecomunicações e Informática
Group 4:
- Fernando João Santos Mendes PG55807
- Bruno Miguel Fernandes Araújo PG55806

Trabalho Prático 4;

1. **Home net = 10.10.100.0/24 ; TrafegoExamplo2a.pcapng**

No tráfego capturado temos presentes várias interfaces que se encontram nesta rede local, para obtenção desta informação vimos os endpoints e analisamos os ips que se encontram nesta rede. Temos então as interfaces com ip, **10.10.100.1** , **10.10.100.117**, **10.10.100.119**, **10.10.100.120** e **10.10.100.121** (O ip brodcast (**10.10.100.255**) foi usado algumas vezes mas obviamente não pode estar associado a uma interface)

2. **Estratégia de análise**

Para que fosse possível analisar e identificar tráfego na rede não desejável ou suspeito definimos uma estratégia que se caracteriza da seguinte forma:

- Num momento inicial procurou-se identificar quais as características do tráfego da rede em questão, de forma a entender quais os parâmetros e os indicadores de funcionamento inerentes ao mesmo;
- Numa fase posterior procurou-se responder a algumas questões orientativas para se retirar o contexto do tráfego e visar um melhor entendimento do mesmo (Quais os endpoints? Que protocolos ?);
- Por último e após a síntese de informação útil e necessária para a procura e análise na comunicação suspeitas, analisamos na íntegra tráfego através de filtros

3. **Análise**
    a. **Indicadores de funcionamento de tráfego:**

Statistics

Measurement	Captured	Displayed	Marked
Packets	9064	9064 (100.0%)	—
Time span, s	2598.247	2598.247	—
Average pps	3.5	3.5	—
Average packet size, B	1064	1064	—
Bytes	9639607	9639607 (100.0%)	0
Average bytes/s	3710	3710	—
Average bits/s	29 k	29 k	—

Figura 1- Estatísticas de tráfego

Segundo a figura 1 foi possível concluir que:

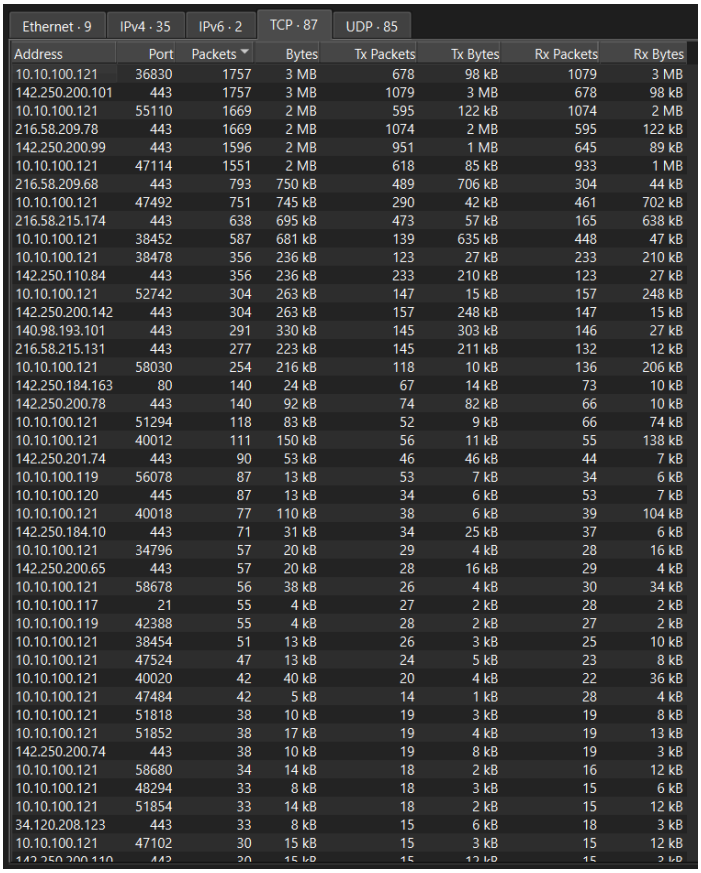
- A captura de rede registrou um total de 9064 pacotes, com uma captura a 100% o que indica que não houve perda de dados durante a análise e que todos os pacotes capturados foram processados corretamente.
- A taxa média de pacotes por segundo (3,5 pps) revela uma rede com atividade muito baixa, característica de ambientes como redes domésticas em momentos de inatividade ou dispositivos que realizam comunicações esporádicas. O tamanho médio dos pacotes é de 1064 bytes.
- A taxa média de transmissão foi de 3710 bytes por segundo (aproximadamente 3,7 kB/s), enquanto a velocidade em bits por segundo ficou em 29 kbps, indicando uma utilização mínima da largura de banda. Esses podem refletir um período de baixa atividade na rede como referido acima.

Caso existisse um histórico sobre os indicadores referidos em cima, da rede em questão, seria possível retirar conclusões imediatas sobre o ficheiro estudado.

As estatísticas acima descrevem uma rede com tráfego reduzido. O padrão observado é poderá corresponder a um ambiente onde a rede não está sob carga pesada, como em redes domésticas com poucos dispositivos ativos ou sistemas que operam em segundo plano sem necessidade de uma grande largura de banda.

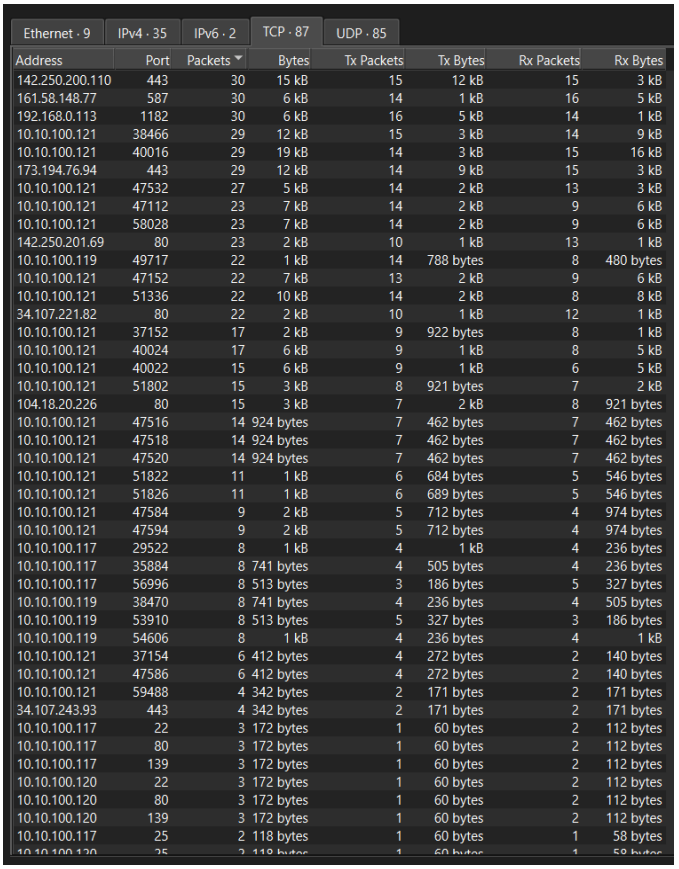
b. Quais os endpoints?

Para a identificação dos endpoints recorre-se às “Estatísticas” e escolhemos a opção Endpoints (Statistics —> Endpoints) ,desta forma foi possível analisar quais os endpoints mais relevantes desta captura. Nesta podemos analisar a informação por protocolos, e foi optado pelo TCP por ser o mais relevante e sistemático.



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.10.100.121	36830	1757	3 MB	678	98 kB	1079	3 MB
142.250.200.101	443	1757	3 MB	1079	3 MB	678	98 kB
10.10.100.121	55110	1669	2 MB	595	122 kB	1074	2 MB
216.58.209.78	443	1669	2 MB	1074	2 MB	595	122 kB
142.250.200.99	443	1596	2 MB	951	1 MB	645	89 kB
10.10.100.121	47114	1551	2 MB	618	85 kB	933	1 MB
216.58.209.68	443	793	750 kB	489	706 kB	304	44 kB
10.10.100.121	47492	751	745 kB	290	42 kB	461	702 kB
216.58.215.174	443	638	695 kB	473	57 kB	165	638 kB
10.10.100.121	38452	587	681 kB	139	635 kB	448	47 kB
10.10.100.121	38478	356	236 kB	123	27 kB	233	210 kB
142.250.110.84	443	356	236 kB	233	210 kB	123	27 kB
10.10.100.121	52742	304	263 kB	147	15 kB	157	248 kB
142.250.200.142	443	304	263 kB	157	248 kB	147	15 kB
140.98.193.101	443	291	330 kB	145	303 kB	146	27 kB
216.58.215.131	443	277	223 kB	145	211 kB	132	12 kB
10.10.100.121	58030	254	216 kB	118	10 kB	136	206 kB
142.250.184.163	80	140	24 kB	67	14 kB	73	10 kB
142.250.200.78	443	140	92 kB	74	82 kB	66	10 kB
10.10.100.121	51294	118	83 kB	52	9 kB	66	74 kB
10.10.100.121	40012	111	150 kB	56	11 kB	55	138 kB
142.250.201.74	443	90	53 kB	46	46 kB	44	7 kB
10.10.100.119	56078	87	13 kB	53	7 kB	34	6 kB
10.10.100.120	445	87	13 kB	34	6 kB	53	7 kB
10.10.100.121	40018	77	110 kB	38	6 kB	39	104 kB
142.250.184.10	443	71	31 kB	34	25 kB	37	6 kB
10.10.100.121	34796	57	20 kB	29	4 kB	28	16 kB
142.250.200.65	443	57	20 kB	28	16 kB	29	4 kB
10.10.100.121	58678	56	38 kB	26	4 kB	30	34 kB
10.10.100.117	21	55	4 kB	27	2 kB	28	2 kB
10.10.100.119	42388	55	4 kB	28	2 kB	27	2 kB
10.10.100.121	38454	51	13 kB	26	3 kB	25	10 kB
10.10.100.121	47524	47	13 kB	24	5 kB	23	8 kB
10.10.100.121	40020	42	40 kB	20	4 kB	22	36 kB
10.10.100.121	47484	42	5 kB	14	1 kB	28	4 kB
10.10.100.121	51818	38	10 kB	19	3 kB	19	8 kB
10.10.100.121	51852	38	17 kB	19	4 kB	19	13 kB
142.250.200.74	443	38	10 kB	19	8 kB	19	3 kB
10.10.100.121	58680	34	14 kB	18	2 kB	16	12 kB
10.10.100.121	48294	33	8 kB	18	3 kB	15	6 kB
10.10.100.121	51854	33	14 kB	18	2 kB	15	12 kB
34.120.208.123	443	33	8 kB	15	6 kB	18	3 kB
10.10.100.121	47102	30	15 kB	15	3 kB	15	12 kB

Figura 2 : Endpoints da Captura (Parte 1)



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
142.250.200.110	443	30	15 kB	15	12 kB	15	3 kB
161.58.148.77	587	30	6 kB	14	1 kB	16	5 kB
192.168.0.113	1182	30	6 kB	16	5 kB	14	1 kB
10.10.100.121	38466	29	12 kB	15	3 kB	14	9 kB
10.10.100.121	40016	29	19 kB	14	3 kB	15	16 kB
173.194.76.94	443	29	12 kB	14	9 kB	15	3 kB
10.10.100.121	47532	27	5 kB	14	2 kB	13	3 kB
10.10.100.121	47112	23	7 kB	14	2 kB	9	6 kB
10.10.100.121	58028	23	7 kB	14	2 kB	9	6 kB
142.250.201.69	80	23	2 kB	10	1 kB	13	1 kB
10.10.100.119	49717	22	1 kB	14	788 bytes	8	480 bytes
10.10.100.121	47152	22	7 kB	13	2 kB	9	6 kB
10.10.100.121	51336	22	10 kB	14	2 kB	8	8 kB
34.107.221.82	80	22	2 kB	10	1 kB	12	1 kB
10.10.100.121	37152	17	2 kB	9	922 bytes	8	1 kB
10.10.100.121	40024	17	6 kB	9	1 kB	8	5 kB
10.10.100.121	40022	15	6 kB	9	1 kB	6	5 kB
10.10.100.121	51802	15	3 kB	8	921 bytes	7	2 kB
104.18.20.226	80	15	3 kB	7	2 kB	8	921 bytes
10.10.100.121	47516	14	924 bytes	7	462 bytes	7	462 bytes
10.10.100.121	47518	14	924 bytes	7	462 bytes	7	462 bytes
10.10.100.121	47520	14	924 bytes	7	462 bytes	7	462 bytes
10.10.100.121	51822	11	1 kB	6	684 bytes	5	546 bytes
10.10.100.121	51826	11	1 kB	6	689 bytes	5	546 bytes
10.10.100.121	47584	9	2 kB	5	712 bytes	4	974 bytes
10.10.100.121	47594	9	2 kB	5	712 bytes	4	974 bytes
10.10.100.117	29522	8	1 kB	4	1 kB	4	236 bytes
10.10.100.117	35884	8	741 bytes	4	505 bytes	4	236 bytes
10.10.100.117	56996	8	513 bytes	3	186 bytes	5	327 bytes
10.10.100.119	38470	8	741 bytes	4	236 bytes	4	505 bytes
10.10.100.119	53910	8	513 bytes	5	327 bytes	3	186 bytes
10.10.100.119	54606	8	1 kB	4	236 bytes	4	1 kB
10.10.100.121	37154	6	412 bytes	4	272 bytes	2	140 bytes
10.10.100.121	47586	6	412 bytes	4	272 bytes	2	140 bytes
10.10.100.121	59488	4	342 bytes	2	171 bytes	2	171 bytes
34.107.243.93	443	4	342 bytes	2	171 bytes	2	171 bytes
10.10.100.117	22	3	172 bytes	1	60 bytes	2	112 bytes
10.10.100.117	80	3	172 bytes	1	60 bytes	2	112 bytes
10.10.100.117	139	3	172 bytes	1	60 bytes	2	112 bytes
10.10.100.120	22	3	172 bytes	1	60 bytes	2	112 bytes
10.10.100.120	80	3	172 bytes	1	60 bytes	2	112 bytes
10.10.100.120	139	3	172 bytes	1	60 bytes	2	112 bytes
10.10.100.117	25	2	118 bytes	1	60 bytes	1	58 bytes

Figura 3 : Endpoints da Captura (Parte 2)

Através das figuras 2 e 3, observa-se que temos endpoints na rede local, assim como alguns populares que encontram-se associados a serviços como os do google, entre outros.

c. GeoLocalização dos IP’s

Na Figura 4, podemos ver o mapa mundial com a identificação da localização dos IP 's envolvidos neste tráfego. Esta visualização foi possível graças à integração dos dados GeoIP da MaxMind no Wireshark, onde após o processo de instalação desta, passamos a ter disponível a opção de visualizar os endereços IP dos endpoints diretamente no mapa.

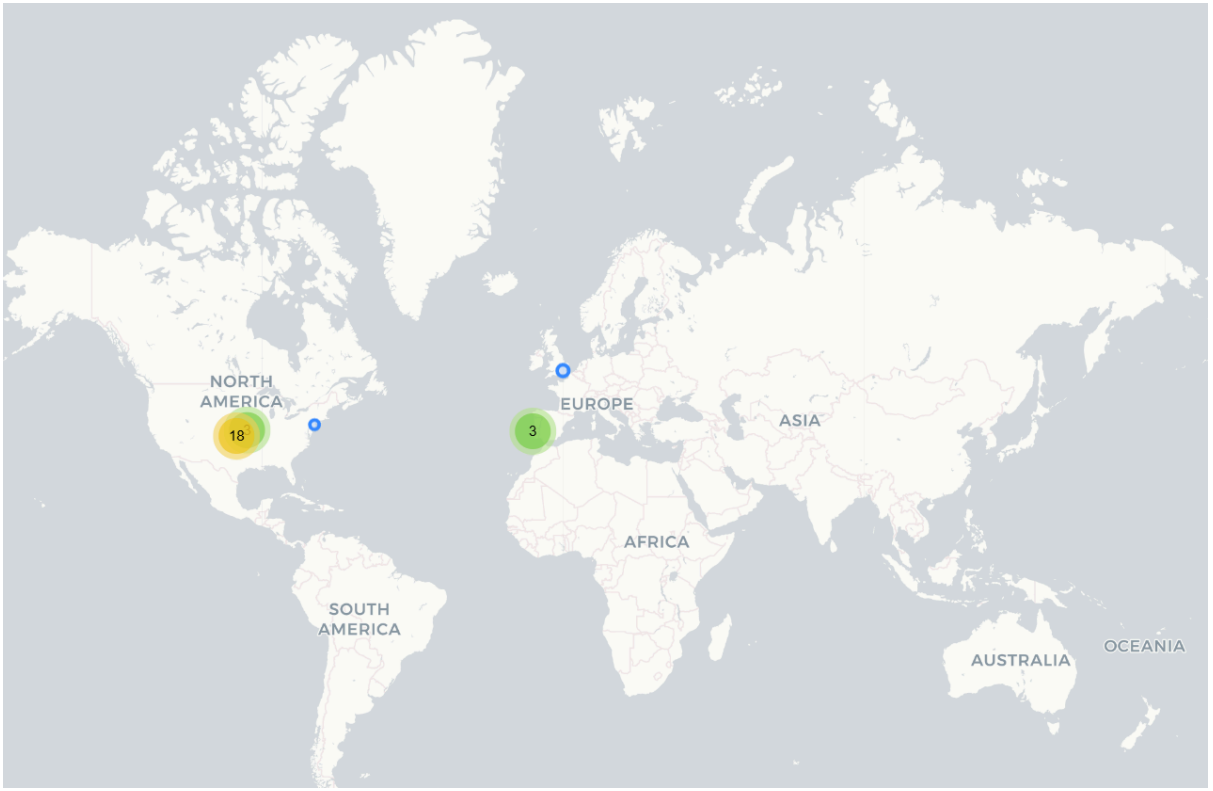


Figura 4 : Localização dos IP’s no mapa do mundo.

d. Gráfico I/O

A funcionalidade Gráfico I/O do Wireshark (disponível no menu Estatísticas) permite visualizar padrões ao longo do tempo no tráfego de rede. Este encontra-se ilustrado na a Figura X, onde podemos ,por exemplo , concluir que o burst inicial de pacotes poderá estar relacionado com o estabelecimento de uma conexão entre cliente e servidor.

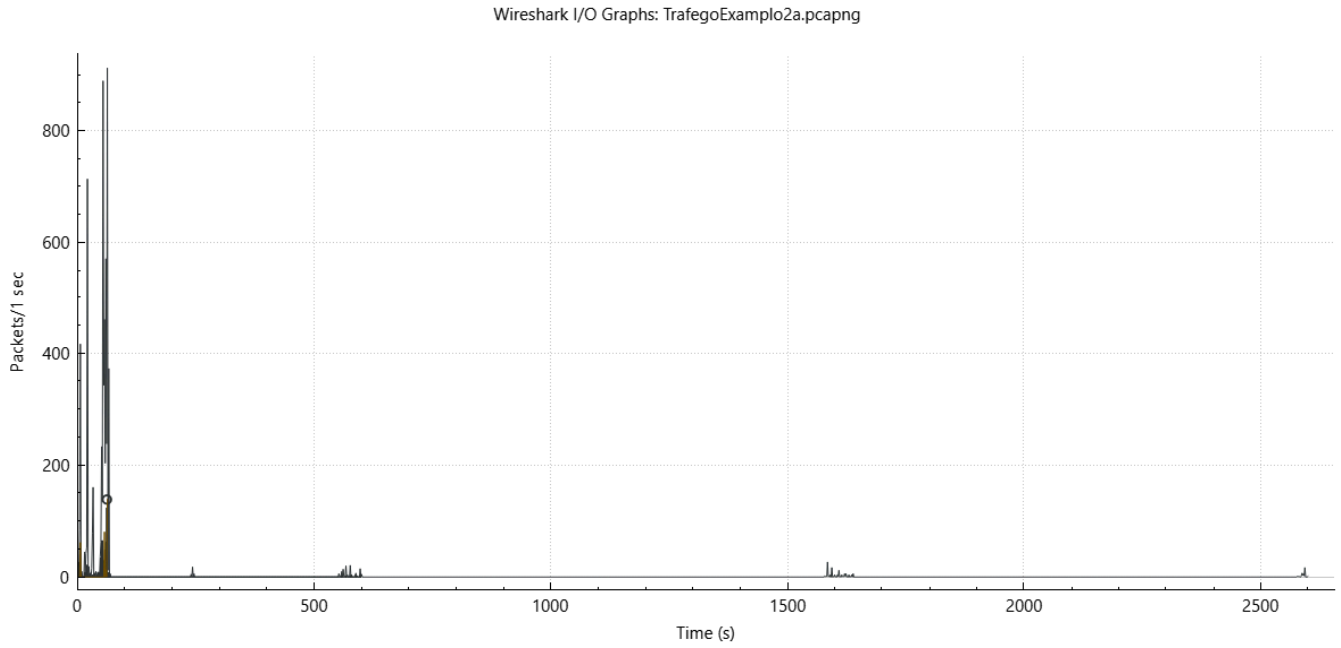


Figura 5 : Gráfico I/O da captura.

e. Quais os protocolos?

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	9064	100.0	9639607	29 k	0	0	0	9064
Ethernet	100.0	9064	1.3	129498	398	0	0	0	9064
Internet Protocol Version 6	0.0	1	0.0	40	0	0	0	0	1
Internet Control Message Protocol v6	0.0	1	0.0	16	0	1	16	0	1
Internet Protocol Version 4	98.3	8907	1.8	178140	548	0	0	0	8907
User Datagram Protocol	3.5	316	0.0	2528	7	0	0	0	316
Network Time Protocol	0.3	24	0.0	1152	3	24	1152	3	24
NetBIOS Name Service	0.0	2	0.0	112	0	2	112	0	2
Domain Name System	3.2	290	0.2	15546	47	290	15546	47	290
Transmission Control Protocol	94.8	8591	96.6	9308207	28 k	4035	1024154	3153	8591
Transport Layer Security	48.3	4374	92.8	8943779	27 k	4374	8246711	25 k	4645
Simple Mail Transfer Protocol	0.2	21	0.0	3908	12	20	3326	10	21
Internet Message Format	0.0	1	0.0	3499	10	1	3499	10	1
NetBIOS Session Service	0.7	62	0.1	7399	22	0	0	0	62
SMB2 (Server Message Block Protocol version 2)	0.7	61	0.1	6988	21	60	6889	21	61
SMB (Server Message Block Protocol)	0.0	1	0.0	163	0	1	163	0	1
Hypertext Transfer Protocol	0.4	36	0.2	19282	59	3	901	2	36
Online Certificate Status Protocol	0.3	30	0.1	9281	28	30	9281	28	30
Line-based text data	0.0	3	0.0	246	0	3	246	0	3
FTP Data	0.0	3	0.0	1134	3	0	0	0	3
Line-based text data	0.0	3	0.0	1134	3	3	1134	3	3
File Transfer Protocol (FTP)	0.4	37	0.0	768	2	37	768	2	37
Data	0.3	24	0.6	57359	176	24	57359	176	24
Address Resolution Protocol	1.7	156	0.1	6834	21	156	6834	21	156

Figura 6 : Protocolos presentes nesta captura de tráfego (Protocol Hierarchy)

Esta captura de rede apresenta uma diversidade significativa de protocolos, indicando um ambiente com múltiplos serviços e tipos de comunicação. Através da figura 6 conseguimos identificar os seguintes protocolos:

1. **Protocolos de Camada de Rede e Transporte**

O tráfego mostra uso simultâneo de **IPv4 e IPv6**, com predominância do IPv4. O IPv6 aparece apenas com tráfego ICMPv6, que normalmente é usado para descoberta de vizinhos e testes de conectividade em redes IPv6. A coexistência destes protocolos é comum em redes modernas durante períodos de transição.

O **TCP e UDP** são ambos utilizados, com o UDP sendo empregado para serviços como DNS (Domain Name System), NTP (Network Time Protocol) e NetBIOS Name Service. O TCP é usado para comunicações mais robustas como SMTP, HTTP, SMB e TLS. Esta distribuição é esperada em uma rede como aquela que serviu de estudo.

2. **Protocolos Críticos e Seu Significado**

DNS (Domain Name System):
Presente em praticamente todas as redes e é responsável pela resolução de nomes.

SMB/SMB2 (Server Message Block):
Protocolo de compartilhamento de arquivos. A presença deste é normal em redes Windows, mas merece atenção devido a vulnerabilidades como ataques de ransomware que exploram SMB.

HTTP e TLS (Hyper Text Transfer Protocol Secure e Transport Layer Security):
Indicam tráfego web, tanto não criptografado (HTTP) quanto seguro (TLS). É esperada a presença de Online Certificate Status Protocol (OCSP) em ligações TLS para verificação de certificados.

3. **Possíveis Anomalias e Casos Suspeitos**

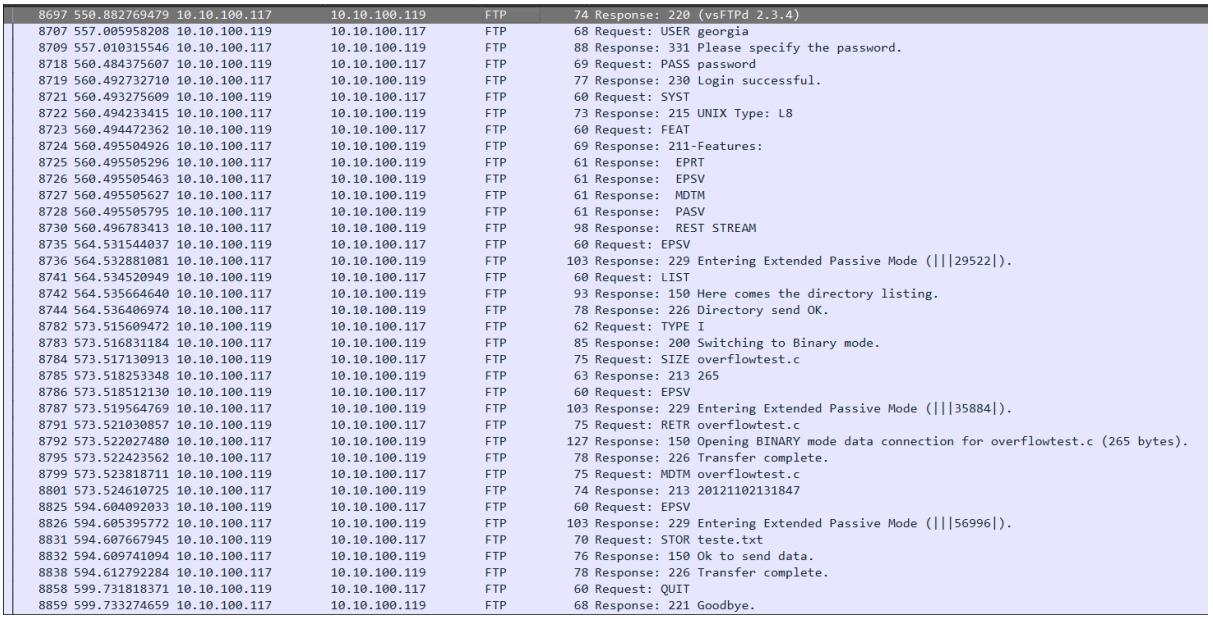
SMTP (Simple Mail Transfer Protocol):
Encontra-se relacionado com o envio de correio electrónico, funciona como o protocolo padrão para a transferência de mensagens entre servidores. No entanto, a sua implementação básica não utiliza encriptação, expondo credenciais de autenticação e conteúdo das mensagens, assim como é possível verificar na figura 7.

```
8666 239.956650   161.58.148.77    192.168.0.113    SMTP      87 S: 220 mmp1102.verio-web.com ESMTP
8667 239.957025   192.168.0.113    161.58.148.77    SMTP      66 C: EHLO vid01
8668 240.052320   161.58.148.77    192.168.0.113    SMTP     145 S: 250-mmp1102.verio-web.com | PIPELINING | 8BITMIME | SIZE 0 | AUTH LOGIN PLAIN
8669 240.052654   192.168.0.113    161.58.148.77    SMTP      66 C: AUTH LOGIN
8670 240.146314   161.58.148.77    192.168.0.113    SMTP      72 S: 334 VXNlcm5hbWU6
8671 240.146625   192.168.0.113    161.58.148.77    SMTP      72 C: User: bGF1cmEuY2hhcHA0
8672 240.256937   161.58.148.77    192.168.0.113    SMTP      72 S: 334 UGFzc3dvcmQ6
8673 240.257224   192.168.0.113    161.58.148.77    SMTP      68 C: Pass: YnViYmxlczI=
8674 240.358853   161.58.148.77    192.168.0.113    SMTP      81 S: 235 ok, go ahead (#2.0.0)
8675 240.359256   192.168.0.113    161.58.148.77    SMTP      88 C: MAIL FROM: <laura@chappellu.com>
8676 240.453086   161.58.148.77    192.168.0.113    SMTP      64 S: 250 ok
8677 240.453583   192.168.0.113    161.58.148.77    SMTP      87 C: RCPT TO: <brenda@chappellU.com>
8678 240.546767   161.58.148.77    192.168.0.113    SMTP      64 S: 250 ok
8679 240.547217   192.168.0.113    161.58.148.77    SMTP      60 C: DATA
8680 240.640708   161.58.148.77    192.168.0.113    SMTP      68 S: 354 go ahead
8681 240.649612   192.168.0.113    161.58.148.77    SMTP    1514 C: DATA fragment, 1460 bytes
8682 240.649623   192.168.0.113    161.58.148.77    SMTP    1514 C: DATA fragment, 1460 bytes
8684 240.744909   192.168.0.113    161.58.148.77    SMTP/I…  636 from: "Laura Chappell" <laura@chappellu.com>, subject: Test,  (text/plain) (text/html) | .
8685 240.844942   161.58.148.77    192.168.0.113    SMTP      81 S: 250 ok 1256145014 qp 3531
8687 243.351611   192.168.0.113    161.58.148.77    SMTP      60 C: QUIT
8690 243.506787   161.58.148.77    192.168.0.113    SMTP      81 S: 221 mmp1102.verio-web.com
```

Figura 7 : Tráfego SMTP na captura.

NetBIOS (Name Service e NetBIOS Session Service):
Embora legítimos em redes Windows antigas, hoje são considerados protocolos inseguros. Sua presença pode indicar sistemas desatualizados ou configurações inadequadas, potencialmente exploráveis.

FTP (Data e File Transfer Protocol):
O FTP é conhecido por transmitir credenciais em claro. Sua presença, especialmente sem FTPS e SFTP, representa um risco de segurança significativo.



8697	550.882769479	10.10.100.117	10.10.100.119	FTP	74 Response: 220 (vsFTPd 2.3.4)
8707	557.005958208	10.10.100.119	10.10.100.117	FTP	68 Request: USER georgia
8709	557.010315546	10.10.100.117	10.10.100.119	FTP	88 Response: 331 Please specify the password.
8718	560.484375607	10.10.100.119	10.10.100.117	FTP	69 Request: PASS password
8719	560.492732710	10.10.100.117	10.10.100.119	FTP	77 Response: 230 Login successful.
8721	560.493275609	10.10.100.119	10.10.100.117	FTP	60 Request: SYST
8722	560.494233415	10.10.100.117	10.10.100.119	FTP	73 Response: 215 UNIX Type: L8
8723	560.494472362	10.10.100.119	10.10.100.117	FTP	60 Request: FEAT
8724	560.495504926	10.10.100.117	10.10.100.119	FTP	69 Response: 211-Features:
8725	560.495505296	10.10.100.117	10.10.100.119	FTP	61 Response: EPRT
8726	560.495505463	10.10.100.117	10.10.100.119	FTP	61 Response: EPSV
8727	560.495505627	10.10.100.117	10.10.100.119	FTP	61 Response: MDTM
8728	560.495505795	10.10.100.117	10.10.100.119	FTP	61 Response: PASV
8730	560.496783413	10.10.100.117	10.10.100.119	FTP	98 Response: REST STREAM
8735	564.531544037	10.10.100.119	10.10.100.117	FTP	60 Request: EPSV
8736	564.532881081	10.10.100.117	10.10.100.119	FTP	103 Response: 229 Entering Extended Passive Mode (|||29522|).
8741	564.534520949	10.10.100.119	10.10.100.117	FTP	60 Request: LIST
8742	564.535664640	10.10.100.117	10.10.100.119	FTP	93 Response: 150 Here comes the directory listing.
8744	564.536406974	10.10.100.117	10.10.100.119	FTP	78 Response: 226 Directory send OK.
8782	573.515609472	10.10.100.119	10.10.100.117	FTP	62 Request: TYPE I
8783	573.516831184	10.10.100.117	10.10.100.119	FTP	85 Response: 200 Switching to Binary mode.
8784	573.517130913	10.10.100.119	10.10.100.117	FTP	75 Request: SIZE overflowtest.c
8785	573.518253348	10.10.100.117	10.10.100.119	FTP	63 Response: 213 265
8786	573.518512130	10.10.100.119	10.10.100.117	FTP	60 Request: EPSV
8787	573.519564769	10.10.100.117	10.10.100.119	FTP	103 Response: 229 Entering Extended Passive Mode (|||35884|).
8791	573.521030857	10.10.100.119	10.10.100.117	FTP	75 Request: RETR overflowtest.c
8792	573.522027480	10.10.100.117	10.10.100.119	FTP	127 Response: 150 Opening BINARY mode data connection for overflowtest.c (265 bytes).
8795	573.522423562	10.10.100.117	10.10.100.119	FTP	78 Response: 226 Transfer complete.
8799	573.523818711	10.10.100.119	10.10.100.117	FTP	75 Request: MDTM overflowtest.c
8801	573.524610725	10.10.100.117	10.10.100.119	FTP	74 Response: 213 20121102131847
8825	594.604092033	10.10.100.119	10.10.100.117	FTP	60 Request: EPSV
8826	594.605395772	10.10.100.117	10.10.100.119	FTP	103 Response: 229 Entering Extended Passive Mode (|||56996|).
8831	594.607667945	10.10.100.119	10.10.100.117	FTP	70 Request: STOR teste.txt
8832	594.609741094	10.10.100.117	10.10.100.119	FTP	76 Response: 150 Ok to send data.
8838	594.612792284	10.10.100.117	10.10.100.119	FTP	78 Response: 226 Transfer complete.
8858	599.731818371	10.10.100.119	10.10.100.117	FTP	60 Request: QUIT
8859	599.733274659	10.10.100.117	10.10.100.119	FTP	68 Response: 221 Goodbye.

Figura 8 : Tráfego FTP na captura.

Assim como no SMTP, verifica-se que a falta de encriptação nos protocolos expõe as comunicações, conforme a figura 8 é possível analisar que alguém que esteja em posição de escuta pode facilmente capturar credenciais de login (Trama 8707 – username; Trama 8718 – password), bem como fazer download dos ficheiros transferidos.

f. Análise às Streams do tráfego TCP

Analisaremos o conteúdo das comunicações (streams) através da funcionalidade **Follow TCP Stream** do Wireshark, que permite reconstruir e inspecionar fluxos de comunicação.

Nº Ordens ou streams	Tempo(s)	Src/Dst	Comentário
1	3.020 - 15.2177	10.10.100.121 (porta 47524)- 142.250.184.163 (porta 80)	Cliente (10.10.100.121) a obter conexão ao servidor da google (142.250.184.163) onde também obtém acesso a uma pki, para este efeito deu uso dos protocolos TCP e OSPF.

2	3.5937 - 62.5827	10.10.100.121 (porta 48294) - 34.120.208.123 (porta 443)	Cliente estabelece uma ligação segura com o website relacionado ao domínio de telemetria do mozilla. Além disto , é feita uma troca de dados relativos ao certificado do servidor (onde a pki previamente acedida irá se envolver) e as chaves do cliente.
3-4	4,086 - 62.805	10.10.100.121 (porta …) - 142.250.200.99 (porta 443)	Cliente acede a páginas estáticas do google onde obtém os recursos necessários através do domínio www.gstatic.com. A stream 4 comparando com a stream 3 tem pacotes ACK duplicados (“TCP Dup ACK”) e pacotes onde após a falha de um ack (“TCP ACKed unseen segment”) foi feita uma retransmissão.
5	4.185 - 65.85	10.10.100.121 (porta 47532) - 142.250.184.163 (porta 80)	O comportamento desta stream é similar ao da stream 1, isto acontece pois a pki demora a responder, logo existem situações como esta onde é necessário pedir novamente o acesso.
6	4.9357 - 61.4738	10.10.100.121 (porta 52742) - 142.250.200.163 (porta 443)	Comportamento semelhante ao da stream 3-4 com a diferença que nesta stream se acede para a apis.google.com
7-8-9	5.2297 - 65.481	10.10.100.121 (porta …) - 142.250.184.163 (porta 80)	É possível verificar que a estas streams contém apenas sequência repetitivas de TCP Dup ACK. Devida a um comportamento atípico é necessário ter atenção a uma possível anomalia.
10	14.0938 - 14.9012	10.10.100.121 (porta 47484) - 216.58.209.68 (porta 443 -google)	O ip destino dos pacotes enviados pelo cliente, encontra-se associado ao google, mais concretamente a serviços de email.
11-12	16.5984 - 66.8196	10.10.100.121 (porta …) - 142.250.201.69 (porta 80)	Este tráfego mostra uma conexão HTTP padrão, entre o cliente e o website https://mail.google.com/mail, relativo ao domain da stream anterior, seguida por pacotes TCP Keep-Alive para manter a conexão ativa..
13	16.89699 - 63.2270	10.10.100.121 (porta 36830) - 142.250.200.163 (porta 443)	Comportamento semelhante ao da stream 3-4 com a diferença que nesta stream se acede e troca-se dados com mail.google.com (é a conclusão do processo iniciado na stream 10)
14	18.54918 - 58.73114	10.10.100.121 (porta 38478)- 142.250.110.84(port a 443)	Comportamento semelhante à stream 3-4 com a diferença que está a aceder a accounts.google.com, um serviço de autenticação ou acesso a serviços Google.

15-16	19.40494 - 59.89	10.10.100.121(porta …) - 216.58.215.131 (porta 443	Após um handshake TLS 1.3 normal para fonts.gstatic.com, (website similar o da stream 1) o tráfego torna-se suspeito a partir de 53.24896s com retransmissões e ACKs duplicados, similar a anomalias anteriores.
17	20.17 - 59.62	10.10.100.121 (porta 51294) - 142.250.200.78(port a 443)	Acesso normal ao youtube com diversos pedidos e respostas.
18-19	30.010 - 62.64	10.10.100.121(porta …) - 216.58.215.174(port a 443)	Acesso normal ao google com diversos pedidos e respostas.
20	30.25 - 67.76	10.10.100.121 (porta 400012) - 140.98.193.101 (porta 443)	Acesso ao eservices10.ieee.org um subdominio de IEEE (Institute of Electrical and Electronics Engineers) que poderia ser ,por exemplo, o cliente a consultar um paper de investigação.
21	30.87 - 61.01	10.10.100.121 (porta 51802) - 104.18.20.226 porta 80)	Cloudflare (gestor de tráfego web comum). com o acesso de acordo com o esperado.
22-23-24-25-26	31.225 - 38.190	10.10.100.121 (porta …) - 140.98.193.101 porta 80)	Acesso ao eservices10.ieee.org igual à stream 20.
27	48.291 - 48.435	10.10.100.121 (porta 47152) - 140.250.200.99 (porta 80)	Acesso ao gstatic.com como na stream 3
28	50.0031 - 50.38	10.10.100.121 (porta 38466) - 173.194.76.94(porta 443)	Esta stream inicia com um handshake TLS 1.3 para o domínio accounts.google.pt, similar à stream 14.
29	51.3288 - 64.16	10.10.100.121 (porta 55110) - 216.58.209.78 (porta 443 - Google)	Assim como já aconteceu em streams previas esta tem presente uma conexão TLS 1.3 mas para o serviço chat.google.com, um serviço da Google de troca de mensagens entre indivíduos.

30	53.8269 - 54.016	10.10.100.121 (porta 47102) - 142.250.200.163 (porta 443 - Google)	Esta stream inicia com um handshake TLS 1.3 para o domínio lh3.google.com ,serviço da Google que armazena imagens relativas a icons de serviços etc.
31	54.44731 - 55.07	10.10.100.121 (porta 51852) - 142.250.184.10 (porta 443 - Google)	Novamente uma conexão TLS 1.3 mas para o subdomínio ogads-pa.clients6.google.com do google, um serviço legítimo da Google relacionado a anúncios.
32	54.44737 - 54.7677	10.10.100.121 (porta 51854) - 142.250.184.10 (porta 443 - Google)	Stream com conteúdo similar à stream anterior, mas contém um pacote com erro ack seguido de uma retransmissão.
33-34	54.54594 - 55.02489	10.10.100.121(porta …) - 142.250.201.74(porta 443)	Handshake TLS normal para waa-pa.clients6.google.com ,serviço legítimo do Google relacionado novamente com os anúncios mas com um papel diferente de análise de dados e sincronização dos serviços.
35	54.64133 - 64.81724	10.10.100.121 (porta 47584) - 142.250.184.163(porta 80)	Stream similar com a stream 1 e 5(um acesso à pki)
36	54.661 - 59.915	10.10.100.121(porta 47586) - 142.250.184.163(porta 80)	Apenas 6 pacotes TCP que poderão indicar uma continuação da stream 35
37	55.59628 - 60.60733	10.10.100.121(porta 34796) - 142.250.200.65(porta 443)	Iniciado com handshake TCP/TLS 1.3 normal, para "lh3.googleusercontent.com" , outro serviço de armazenamento (como na stream 30) mas que distribui conteúdos armazenados publicamente, por exemplo imagens guardadas no google Imagens.
38	56.55952 - 56.69921	10.10.100.121(porta 51336) - 142.250.200.78 (porta 443)	Comunicação com o domínio ogs.google.com, serviço associado a logins e autenticações em outras aplicações ou afins, por exemplo escolher a opção de login pelo Google noutros websites.
39	57.352 - 58.628	10.10.100.121(porta 51818) - 42.250.200.74(porta 443)	Comunicação com safeBrowsing.googleapis.com (serviço legítimo de segurança do Google) com tráfego normal e esperado para um dispositivo verificando atualizações de segurança ou validando URLs.

40	57.438 - 67.635	10.10.100.121(porta 47594) - 142.250.184.160 (porta 80)	O conteúdo encontra-se novamente relacionado á troca de dados com a pki, mas esta stream tem apenas um pouco numero de pacotes OSPF e TCP, em que alguns destes têm objetivo de manter viva a conexão.
41	239.7665 - 243.5669	192.168.0.113(porta 1182) - 161.58.148.77(porta 587) (verio-web.com).	**Esta stream revela uma vulnerabilidade crítica na transmissão de e-mails na rede, com exposição de credenciais e conteúdo sensível. Apesar de ser um tráfego legítimo de SMTP, a falta de encriptação representa um risco significativo à segurança da informação. É possível consultar os dados de autenticação do cliente, assim como todas as informações relacionadas com e-mail enviado (Remetente, destinatário, conteúdo etc.)**
42	550.87 - 599.7346	10.10.100.119 (porta 42388) - 10.10.100.117 (porta 21)	**Esta stream mostra a conexão FTP insegura . Como já mencionado no ponto e.3, este protocolo não tem encriptação como SMTP o que expõe dados de autenticação e até ficheiros transferidos pelo cliente.** **O cliente fez vários pedidos mas 3 se destacam pediu a lista da diretoria , o ficheiro overflowtest.c e o ficheiro teste.txt**
43	557.11 - 597.061	10.10.100.121 (porta 51822) - 34.107.221.82 (porta 80)	Esta stream mostra uma comunicação. A conexão inicia com um handshake TCP , seguido por uma requisição HTTP GET, após a transferência do ficheiro requerido, são observados múltiplos pacotes TCP Keep-Alive, indicando que a conexão foi mantida aberta para reutilização.
44	557.19 - 597.1039	10.10.100.121 (porta 51826) - 34.107.221.82 (porta 80)	Mesma situação que a stream 43
45-47-48	564.53 - 564.5386	10.10.100.119 (porta …) - 10.10.100.117 (porta …) (servidor FTP)	Comunicação FTP legítima, mas insegura devido à falta de encriptação. Nestas temos presente o FTP-DATA , onde se encontram os dados pedidos na stream 42. A stream 45 tem a lista de diretorias. A stream 47 o ficheiro overflowtest.c. E por fim a stream 48 com o ficheiro teste.txt.
46	565.735 - 565.765	10.10.100.121 (porta 59448) - 34.107.243.93 (porta 443)	Continuação da comunicação e troca de dados entre o cliente e o servidor da google, onde foram capturados poucos pacotes, exatamente 4 TCP, provavelmente relacionados com as streams previamente discutidas.

49-50-51-52-53-54-55-56	2592.467 - 2593.681	10.10.100.119 - 10.10.100.117 - 10.10.100.120	Comunicação TCP feita entre os dispositivos da rede local 10.10.100.0/24 (excluindo o cliente .121), estas "streams" foram mal definidas pelo wireshark, nem ocorre troca de dados entre estes, logo não deveriam ser consideradas como streams.
57	1583.254 - 1636.994	10.10.100.119 (porta 56078) - 10.10.100.120 (porta 445)	**A sessão começa com uma autenticação via NTLM, um método considerado vulnerável, seguida por operações normais de acesso a arquivos compartilhados, incluindo listagem e manipulação de arquivos. Trata-se de uma operação legítima, porém com vulnerabilidades.**

Análise de atividades possivelmente suspeitas do tráfego filtrado.

Em prol da procura por atividade suspeita e após a análise das streams TCP referidas acima, foi decidido filtrar o tráfego usando o seguinte filtro"**!tcp.stream && udp.stream >= 58**" e analisar o resultado. Desta forma removemos todo o tráfego envolvido nas tcp streams e apenas foram deixados pacotes que se encontram nas udp streams numeradas 58 para cima.

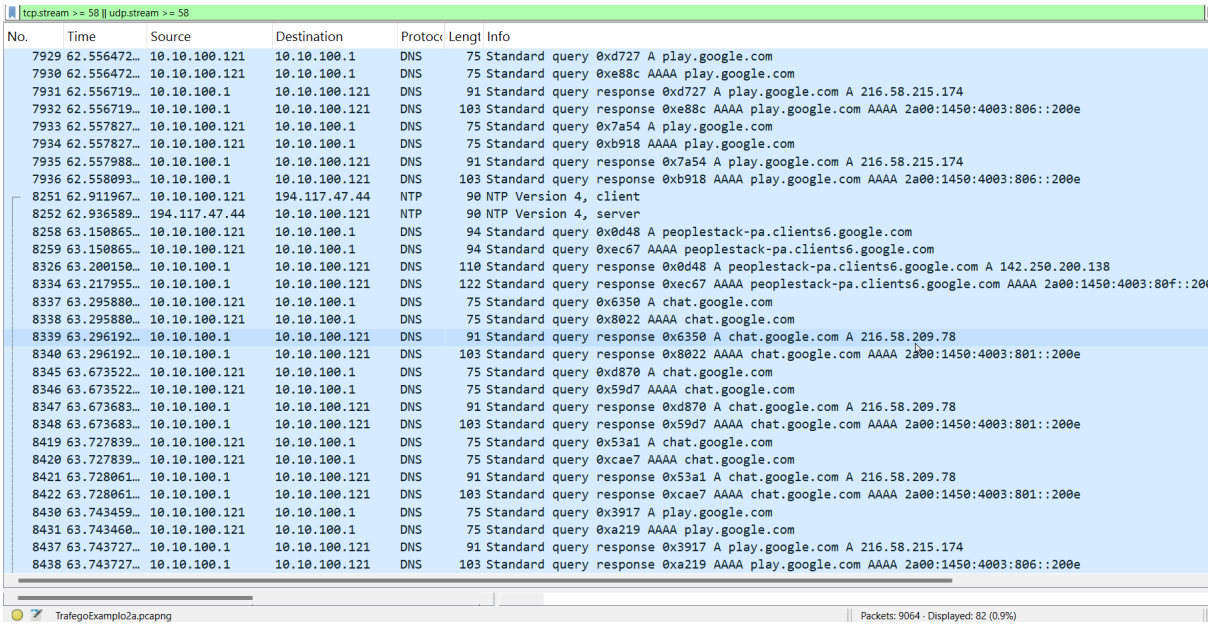


Figura 9 : Pacotes capturados após o filtro "**!tcp.stream && udp.stream >= 58**" (Parte 1).

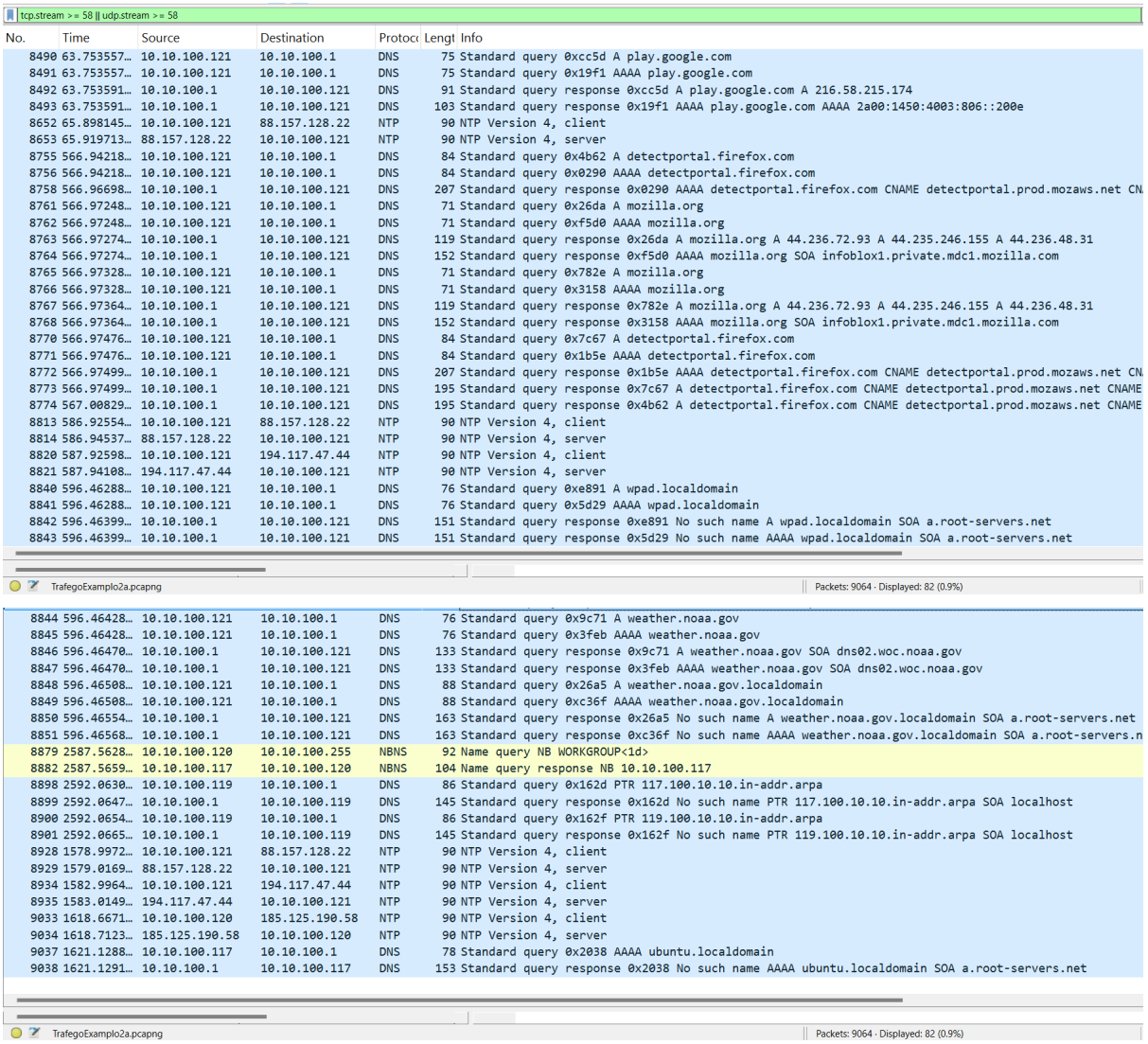


Figura 10 : Pacotes capturados após o filtro "**!tcp.stream && udp.stream >= 58**" (Parte 2).

1. Através dos pacotes 7929,7935, 8430, 8490 com Origem: 10.10.100.121 e Destino: 10.10.100.1 averiguamos várias consultas DNS idênticas para os mesmos domínios (play.google.com e chat.google.com) em curtos intervalos de tempo. Isso pode indicar tentativas de resolver os mesmos endereços repetidamente, possivelmente devido a falhas na cache DNS ou comportamento anômalo de um aplicativo.

2. Através dos pacotes 8840, 8844 com Origem: 10.10.100.121 e Destino: 10.10.100.1 averiguamos que existem consultas para domínios como "vpad.localdomain" e "weather.noaa.gov.localdomain" resultam em respostas "No such name". Isso pode indicar erros de configuração em aplicações ou tentativas de explorar resoluções internas mal configuradas.

3. Através dos pacotes 8652, 8813, 8820,8928 com Origem: 10.10.100.121 e Destino: 88.157.128.22, 194.117.47.44, 185.125.190.58 averiguamos que várias solicitações NTP (Network Time Protocol) para servidores externos. Embora o NTP seja legítimo, a frequência e a variedade de servidores podem sugerir sincronização excessiva ou tentativas de explorar vulnerabilidades em serviços NTP.

4. Através dos pacotes exemplo 8879, 8882 com Origem: 10.10.100.121 e Destino: 10.10.100.119 averiguamos que consultas NetBIOS (MONKGROUP) e PTR para endereços IP internos (117.100.10.10.in-addr.arpa) com respostas "No such name". Isso pode indicar tentativas de descoberta de hosts na rede interna ou configurações incorretas de DNS reverso.

5. Através dos pacotes exemplo 8842, 9038 com Origem: 10.10.100.121 e Destino: 10.10.100.121 e 10.10.100.117 averiguamos que existem respostas do DNS com referências a servidores raiz (a.root-servers.net) para domínios locais (ubuntu.localdomain). Isso sugere que a rede não está resolvendo corretamente nomes internos, possivelmente devido a falhas na configuração do DNS local.

As anomalias identificadas incluem desde comportamentos repetitivos (consultas DNS excessivas) até atividades potencialmente maliciosas (consultas NetBIOS e NTP incomuns). A maioria dos casos aponta para configurações inadequadas ou falhas na rede interna. Para uma análise mais rigorosa deveria todos os endereços deveriam ser averiguados para enquadrar melhor o comportamento da rede.

Por fim, falta então analisar o tráfego para além destas streams tcp e udp, para isso usamos o filtro "**!tcp.stream && !udp.stream**". Analisando o tráfego resultante, vemos que excluindo um pacote ICMPv6 solicitado por um router, temos só pedidos arps feitos para identificar os endereços mac dos dispositivos cuja interface se encontra da rede local, não conseguimos identificar qualquer anomalia, sem ser o facto de existirem alguns pedidos arps repetidos, o que significa que foi necessária mais do que uma tentativa para o dispositivo source obter a resposta que pretende.
Na figura 11 podemos então analisar uma parte deste tráfego, onde se verifica estes pedidos arps repetidos.

1996	29.513994006	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
2086	30.515311511	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
2345	33.521425868	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
2348	34.520927350	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
2355	35.521523494	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
2356	36.522798472	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
2378	42.526456714	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
2382	43.531409065	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
2385	44.528509278	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
2392	45.526582303	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
2393	46.529276438	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
2704	49.525900176	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
2763	50.533635693	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
3699	51.531789242	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
3799	52.529412538	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
4263	53.530247247	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
4415	54.530585936	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
4841	55.526322823	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
5217	56.535067572	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
5890	57.540141162	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
6191	58.538349281	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
8637	64.350080315	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.50? Tell 10.10.100.1
8642	65.346539858	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.50? Tell 10.10.100.1
8649	65.554889771	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
8654	66.552101957	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
8657	67.548469766	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.50? Tell 10.10.100.1
8658	67.549062423	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
8693	550.089665579	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
8699	552.101962178	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
8700	553.098554099	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1
8701	554.107054310	PCSSystemtec_78:c6:…	Broadcast	ARP	60 Who has 10.10.100.107? Tell 10.10.100.1

Figura 11 : Parte da captura do trafego após o filtro "**!tcp.stream && !udp.stream**".

Identificação das sessões

Para a identificação das sessões presentes neste tráfego tivemos em consideração os saltos no tempo entre as os pacotes iniciais das TCP streams e o contexto destas , nomeadamente o que estava a ser efetuado , protocolos envolvidos, etc.
Sendo assim conseguimos encontrar **7** sessões diferentes:

Primeira sessão: Ocorre nas streams de **1 a 9** (aproximadamente entre 3 e 5 segs), nesta sessão ocorre o acesso ao servidor da google, com acessos a pki , seguido de uma navegação em páginas estáticas do google.

Segunda sessão: Ocorre nas streams de **10 a 17** (aproximadamente entre 14 e 20 segs), esta sessão poderia ser até a mesma que a sessão anterior, sendo que acaba por ser uma retoma da anterior e trata-se também da navegação no google, concretamente serviços como gmail entre outros, mas optamos por separá-las para seguirmos o raciocínio dos saltos temporais como nas outras sessões.

Terceira sessão: Ocorre nas streams de **18 a 26** (aproximadamente entre 30 e 32 segs), nesta sessão temos a continuação de acessos a domínios do google, nomeadamente o "play.google.com" , mas já contém acessos a domínios e subdomínios associados ao IEEE, onde o cliente pode ter feito consultas de papers de investigação entre outros.
Quarta sessão: Ocorre nas streams de **27 a 40** (aproximadamente entre 48 e 57 segs), nesta sessão temos novamente acessos a domínios do google, serviços relacionados com publicidades, com partilha de documentos e imagens (possivelmente ferramentas como Google Docs), entre outros.

Quinta sessão: Ocorre na stream **41** (aproximadamente entre 239 e 243 segs), esta sessão é apenas esta trama pois foi nesta que houve todo o processo relativamente ao envio de um e-mail através do protocolo inseguro SMTP.

Sexta sessão: Ocorre nas streams de **42 a 48** (aproximadamente entre 550 e 594 segs), esta sessão está relacionada com todo o processo de pedido e obtenção de ficheiros/informações com protocolo inseguro FTP, assim como já mencionado com mais detalhe na tabela de análise das TCP streams, três pedidos de informações se destacam, nomeadamente o pedido das diretorias , o do ficheiro overflowtest.c e o do ficheiro teste.txt onde o requerente obteve-as nas streams 45,47 e 48, respetivamente.

Sétima sessão: Ocorre na stream **57** (aproximadamente entre 1583 e 1636 segs), esta última sessão está associada ao pedido de consulta do ficheiro teste.txt com o protocolo SMB2, este processo envolve vários passos iniciais desde a necessidade de um setup inicial, como a de saber a localização do ficheiro, após estes o requerente consegue consultar o seu ficheiro objetivo.

As streams **49 a 56** não foram atribuídas a uma sessão, sendo que como já previamente dito na tabela de análise das streams TCP, estas não são relevantes pois nem sequer ocorrem trocas de dados nelas.

Conclusão

Neste trabalho prático, seguimos uma metodologia estruturada para análise de tráfego da rede fornecida pelo educando. Recorrendo às ferramentas estatísticas do Wireshark, caracterizamos a rede local (10.10.100.0/24) , identificamos os principais endpoints ilustrando-os num mapa e analisamos os protocolos envolvidos neste tráfego, aproveitando para indicar possíveis anomalias.

Fizemos uma análise geral do tráfego da rede, começando por analisar as streams TCP's, agrupando-as em sessões e identificando vulnerabilidades significativas, seguido da análise de algumas streams UDP's onde também detectamos possíveis atividades suspeitas. Concluímos com uma análise do tráfego resultante após a filtração das streams TCP e UDP.

Concluímos que os objetivos foram plenamente alcançados, os resultados revelaram a necessidade de implementar medidas de segurança adicionais, principalmente a adoção de protocolos com mecanismos de encriptação. Este trabalho expandiu o nosso conhecimento, sendo que foi necessária alguma procura de novos conceitos assim como ajudou na consolidação daqueles que já foram mencionados nas aulas.

Distribuição de Tarefas

Ambos os membros do grupo contribuíram de forma equitativa para este projeto, investindo aproximadamente 10 horas cada, ligeiramente menor que o anterior. Grande parte desse tempo foi dedicado à análise das streams TCP's e à identificação das sessões,

Referências

1. **MaxMind**. (n.d.). *GitHub - MaxMind*. GitHub. https://github.com/maxmind
2. **Wireshark**. (n.d.). *Wireshark User's Guide*. https://www.wireshark.org/docs/wsug_html_chunked/
3. Slides fornecidos pelo educando.