UC/Curso: Ciber
Grupo 5:
- Catarina P
- Inês Neve
- Leonardo
- Miguel G
- Rui Barbo

52% (B) HomeNET (100%): identificam corretamente e justificam. Estratégia, uso de funções estatísticas, streams e

Trabalho Prátic

1. Home net = 10.10.100.0/24

Após uma análise inicial do tráfego, foi concluído que muito provavelmente a origem deste tráfego é o IP 10.10.100.121. Este é o endpoint com o maior número de pacotes transmitidos/recebidos.

Ao observar outros endpoints na lista, notamos que muitos IPs começam por 10.10.100.x, o que confirma que a rede local desta captura de tráfego é a rede 10.10.100.0/24.

2. Síntese do tráfego (caracterização geral e análise estatística)

Para realizar uma análise abrangente do tráfego, foram utilizadas ferramentas disponíveis no Wireshark, acessíveis através do menu Statistics. Dentro deste menu, encontramos as ferramentas EndPoints, I/O Graph e Capture File Properties para obter dados relevantes.

Utilizando a base de dados fornecida pela MaxMind e a ferramenta EndPoints, é possível identificar os participantes nas comunicações e sua localização aproximada.

Na Figura 1, é apresentado o mapa com as localizações dos IPs envolvidos nesta captura de tráfego.

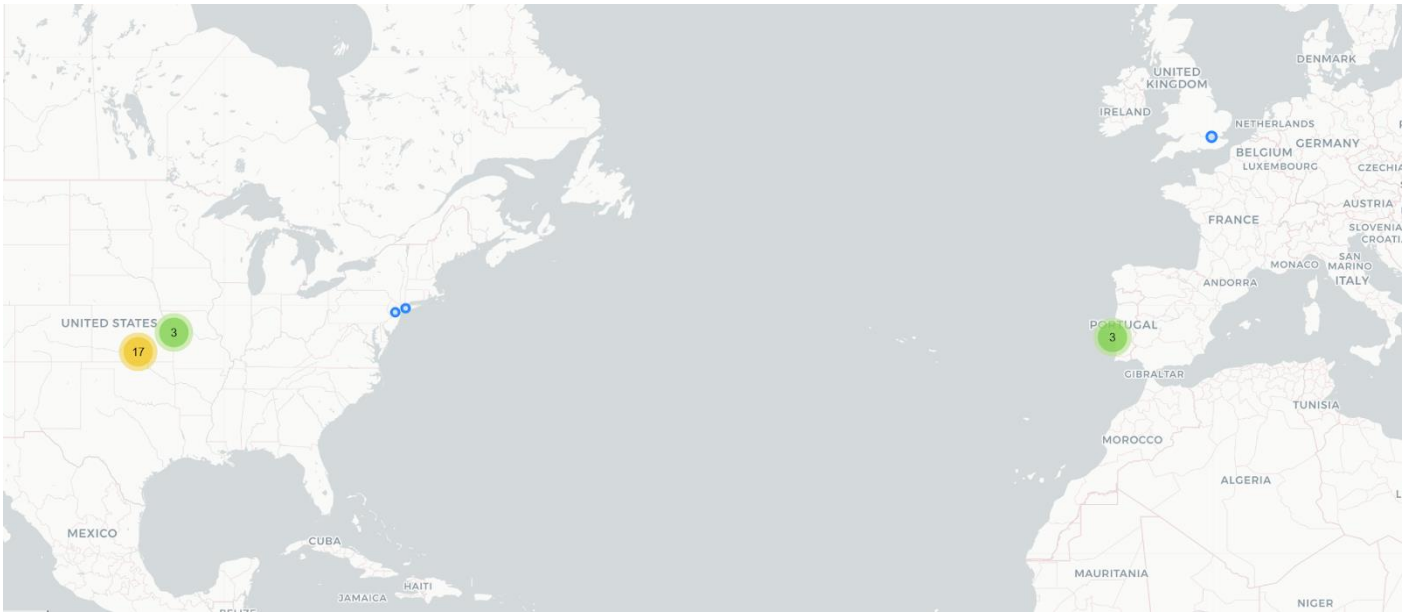


Figura 1 - Mapa com as localizações dos IPs.

Na figura 2 é possível observar a data da captura inicial - 21/10/2009 e a hora de início – 18:10:20, e também da data da captura final - 01/04/2024 a hora de fim 18:16:18 e o tempo de captura 43 minutos e 18 segundos.

não é coerente

Time

First packet:	2009-10-21 18:10:20
Last packet:	2024-04-01 18:16:18
Elapsed:	00:43:18

Figura 2 - Tempo de captura.

Na figura 3, observa-se as estatísticas relativamente à captura, i.e., o número de pacotes capturados (9064), o número total de bytes (9639607), entre outros.

Statistics

Measurement	Captured	Displayed	Marked
Packets	9064	9064 (100.0%)	—
Time span, s	455846757.978	455846757.978	—
Average pps	0.0	0.0	—
Average packet size, B	1064	1064	—
Bytes	9639607	9639607 (100.0%)	0
Average bytes/s	0	0	—
Average bits/s	0	0	—

Figura 3 - Estatísticas de Captura.

Na figura 4 é observável a divisão do tráfego que existe ao longo do tempo, também ajuda a situar em contexto temporal os vários protocolos.

Neste gráfico foram extraídos os pacotes existente de há aproximadamente 15 anos. Como?

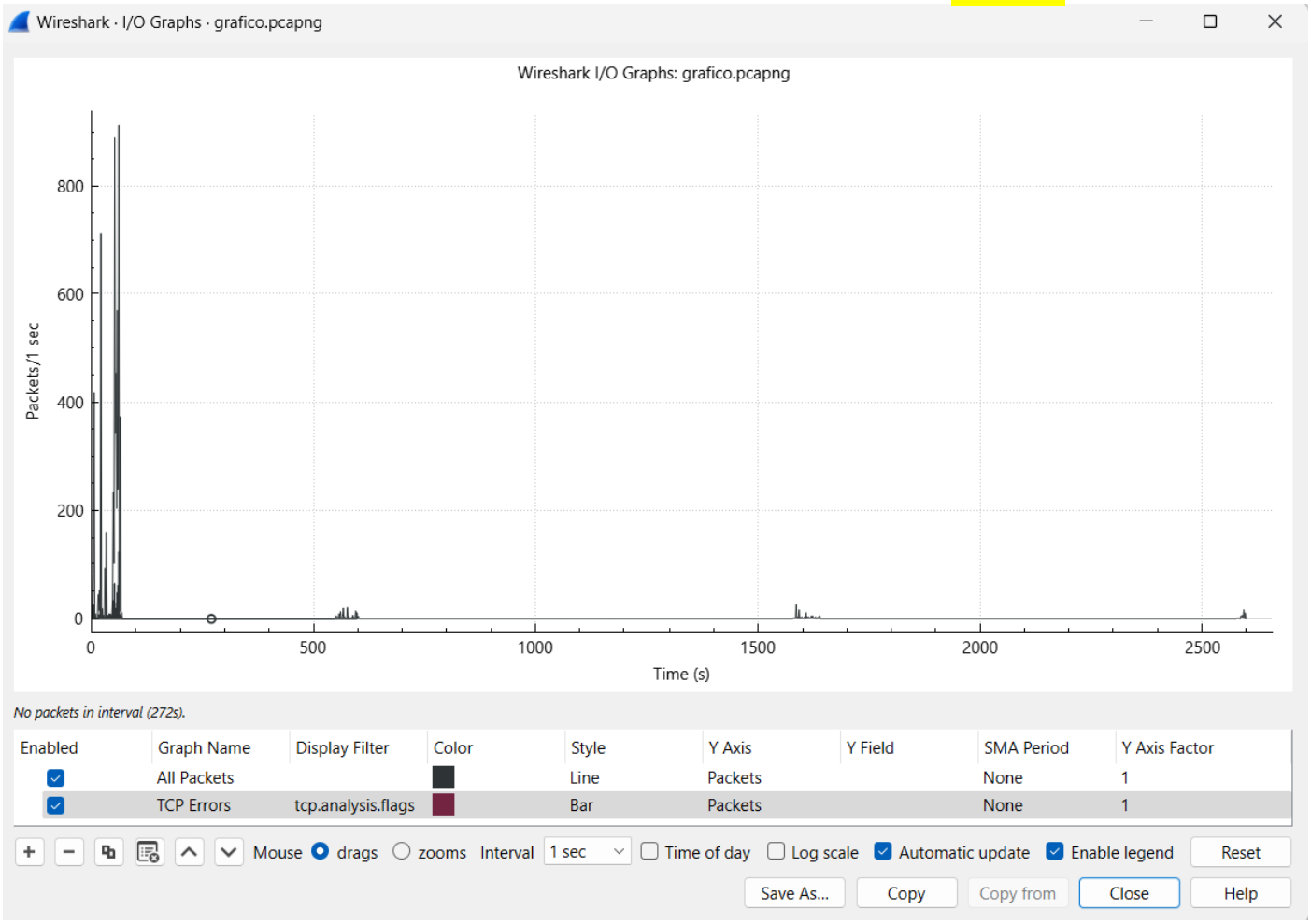
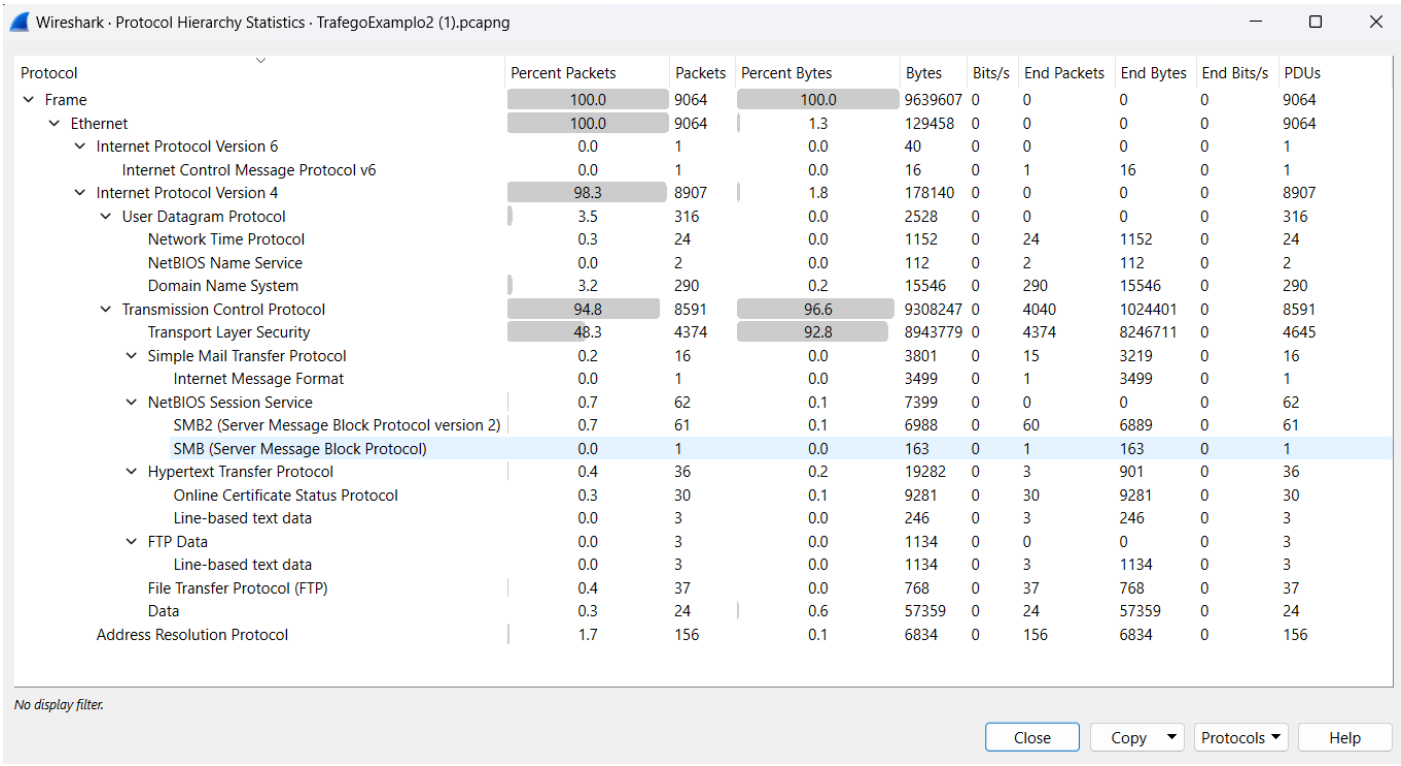


Figura 4 – Gráfico de captura de tráfego

Na figura 5, pode-se analisar a hierarquia de protocolos. O protocolo mais utilizado foi o TCP, correspondendo a 94.8% do tráfego, seguido do protocolo UDP, que corresponde a 3.5% do tráfego. O protocolo ARP representa uma percentagem muito pequena do tráfego (1.7%) o que, à partida, indica que não haverá atividade suspeita na utilização deste protocolo. O protocolo ICMP representa uma percentagem nula.

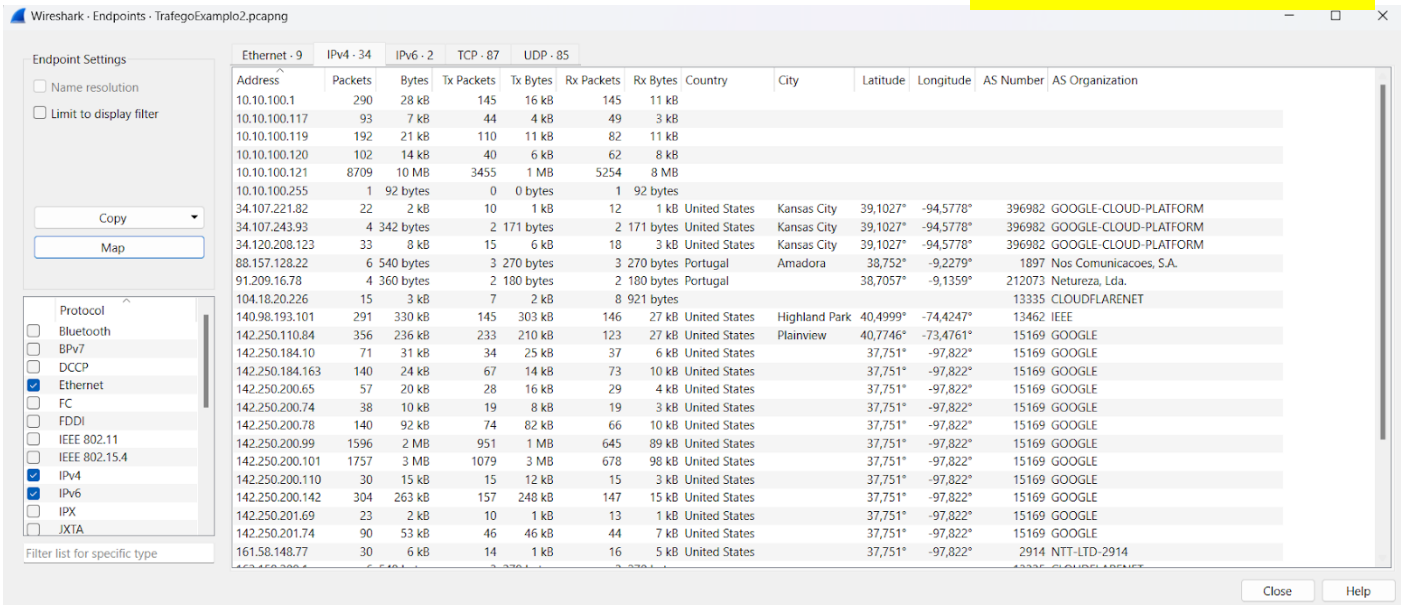


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	9064	100.0	9639607	0	0	0	0	9064
Ethernet	100.0	9064	1.3	129458	0	0	0	0	9064
Internet Protocol Version 6	0.0	1	0.0	40	0	0	0	0	1
Internet Control Message Protocol v6	0.0	1	0.0	16	0	1	16	0	1
Internet Protocol Version 4	98.3	8907	1.8	178140	0	0	0	0	8907
User Datagram Protocol	3.5	316	0.0	2528	0	0	0	0	316
Network Time Protocol	0.3	24	0.0	1152	0	24	1152	0	24
NetBIOS Name Service	0.0	2	0.0	112	0	2	112	0	2
Domain Name System	3.2	290	0.2	15546	0	290	15546	0	290
Transmission Control Protocol	94.8	8591	96.6	9308247	0	4040	1024401	0	8591
Transport Layer Security	48.3	4374	92.8	8943779	0	4374	8246711	0	4645
Simple Mail Transfer Protocol	0.2	16	0.0	3801	0	15	3219	0	16
Internet Message Format	0.0	1	0.0	3499	0	1	3499	0	1
NetBIOS Session Service	0.7	62	0.1	7399	0	0	0	0	62
SMB2 (Server Message Block Protocol version 2)	0.7	61	0.1	6988	0	60	6889	0	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	0	3	901	0	36
Online Certificate Status Protocol	0.3	30	0.1	9281	0	30	9281	0	30
Line-based text data	0.0	3	0.0	246	0	3	246	0	3
FTP Data	0.0	3	0.0	1134	0	0	0	0	3
Line-based text data	0.0	3	0.0	1134	0	3	1134	0	3
File Transfer Protocol (FTP)	0.4	37	0.0	768	0	37	768	0	37
Data	0.3	24	0.6	57359	0	24	57359	0	24
Address Resolution Protocol	1.7	156	0.1	6834	0	156	6834	0	156

Figura 5 - Hierarquia de protocolos.

A figura 6, mostra os endpoints IPv4 existentes nesta captura. Pode-se observar que a maioria dos pacotes capturados são pertencentes a endereços dentro da home net.

Só vejo 3 (excluindo a gw e o broadca



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
10.10.100.1	290	28 kB	145	16 kB	145	11 kB						
10.10.100.117	93	7 kB	44	4 kB	49	3 kB						
10.10.100.119	192	21 kB	110	11 kB	82	11 kB						
10.10.100.120	102	14 kB	40	6 kB	62	8 kB						
10.10.100.121	8709	10 MB	3455	1 MB	5254	8 MB						
10.10.100.255	1	92 bytes	0	0 bytes	1	92 bytes						
34.107.221.82	22	2 kB	10	1 kB	12	1 kB	United States	Kansas City	39,1027°	-94,5778°	396982	GOOGLE-CLOUD-PLATFORM
34.107.243.93	4	342 bytes	2	171 bytes	2	171 bytes	United States	Kansas City	39,1027°	-94,5778°	396982	GOOGLE-CLOUD-PLATFORM
34.120.208.123	33	8 kB	15	6 kB	18	3 kB	United States	Kansas City	39,1027°	-94,5778°	396982	GOOGLE-CLOUD-PLATFORM
88.157.128.22	6	540 bytes	3	270 bytes	3	270 bytes	Portugal	Amadora	38,752°	-9,2279°	1897	Nos Comunicacoes, S.A.
91.209.16.78	4	360 bytes	2	180 bytes	2	180 bytes	Portugal		38,7057°	-9,1359°	212073	Netureza, Lda.
104.18.20.226	15	3 kB	7	2 kB	8	921 bytes					13335	CLOUDFLARENET
140.98.193.101	291	330 kB	145	303 kB	146	27 kB	United States	Highland Park	40,4999°	-74,4247°	13462	IEEE
142.250.110.84	356	236 kB	233	210 kB	123	27 kB	United States	Plainview	40,7746°	-73,4761°	15169	GOOGLE
142.250.184.10	71	31 kB	34	25 kB	37	6 kB	United States		37,751°	-97,822°	15169	GOOGLE
142.250.184.163	140	24 kB	67	14 kB	73	10 kB	United States		37,751°	-97,822°	15169	GOOGLE
142.250.200.65	57	20 kB	28	16 kB	29	4 kB	United States		37,751°	-97,822°	15169	GOOGLE
142.250.200.74	38	10 kB	19	8 kB	19	3 kB	United States		37,751°	-97,822°	15169	GOOGLE
142.250.200.78	140	92 kB	74	82 kB	66	10 kB	United States		37,751°	-97,822°	15169	GOOGLE
142.250.200.99	1596	2 MB	951	1 MB	645	89 kB	United States		37,751°	-97,822°	15169	GOOGLE
142.250.200.101	1757	3 MB	1079	3 MB	678	98 kB	United States		37,751°	-97,822°	15169	GOOGLE
142.250.200.110	30	15 kB	15	12 kB	15	3 kB	United States		37,751°	-97,822°	15169	GOOGLE
142.250.200.142	304	263 kB	157	248 kB	147	15 kB	United States		37,751°	-97,822°	15169	GOOGLE
142.250.201.69	23	2 kB	10	1 kB	13	1 kB	United States		37,751°	-97,822°	15169	GOOGLE
142.250.201.74	90	53 kB	46	46 kB	44	7 kB	United States		37,751°	-97,822°	15169	GOOGLE
161.58.148.77	30	6 kB	14	1 kB	16	5 kB	United States		37,751°	-97,822°	2914	NTT-LTD-2914

Figura 6 - IPV4 Endpoints.

3. Estratégia de análise

A estratégia de análise segue os seguintes passos:

1. Através do menu Statistic → Protocol Hierarchy, é possível observar quais os protocolos mais utilizados, como já demonstrado na seção anterior.

2. Inicialmente analisam-se stream a stream e os seus respetivos pacotes, começando pelas TCP e depois pelas stream UDP.

3. Posteriormente, utilizou-se outra estratégia para se verificar as conclusões já tiradas. Através do menu Statistic → Conversations selecionou-se a opção Name Resolution e também o Rel Start para se puder observar o tempo por ordem crescente para facilitar a interpretação.

e como procederam depois

4. Síntese da análise

4.1 TCP e UDP

Nº ordem ou *streams*	Tempo (s)	Src/Dest não indicam portas	Comentário
Stream 0 0-17	2.92444 a 20.17867	Src:10.10.100.121 Dst: 216.58.209.68 (google.com) 142.250.201.69 (gmail.com) Como analisaram em conjunto	TCP: Acesso a página web Google.com através do web browser Mozilla Firefox; Ocorre uma validação de certificado (por parte do web server?); Acesso (por parte do web server) a API "gstatic" (pertencente à google), que funciona como uma base de dados de componentes web (imagens, CSS). Processo de autenticação no Gmail (usando o protocolo ocsp para verificação do certificado); Acesso por parte do web server a API (gstatic e fonts.gstatic); Acesso a definições da conta google (e definições da conta youtube); Ocorreram algumas situações de erro relacionadas com perda de pacotes, congestionamento da rede e duplicação de pacotes. A sessão envolveu a transferência de 5351 pacotes e 5951 KBytes. UDP: A esta stream está associado o tráfego UDP correspondente à resolução dos endereços usados, através do protocolo DNS. Respostas negativas ("No such name") a pedidos de resolução de 2 endereços.
Stream 3 18-26	30.01021 a 32.67351	Src:10.10.100.121 Dst: 140.98.193.101 (services10.ieee)	TCP: Acesso a uma conta Google com autenticação, via um serviço na página IEEE; No início da sessão ocorreu uma validação de certificado com o protocolo ocsp; Não houve ocorrências de erros durante a sessão; Foi verificado que 10 segundos após inatividade, existe troca de pacotes TCP do tipo "Keep Alive"; A sessão envolveu a transferência de 944 pacotes e 1027 KBytes UDP: A esta stream está associado o tráfego UDP correspondente à resolução dos endereços usados, através do protocolo DNS.
Stream 4 28-40	50.00319 a 64.16128	Src:10.10.100.121 Dst: 216.58.209.78 (chat.google.com)	Sessão de acesso a serviços da Google; A sessão começa com um acesso a uma conta Google; Houve uma grande troca de pacotes com a página "chat.google.com" o que indica uma troca de mensagens; Existe também acesso a diferentes APIs da Google que vão buscar variados recursos necessários. Não foram verificadas ocorrências de erros nas transmissões. A sessão envolveu a transferência de 2030 pacotes e 2584 KBytes UDP: A esta stream está associado o tráfego UDP correspondente à resolução dos endereços usados, através do protocolo DNS.
Stream 5 41-47 exceto 42, 43	250.8727 a 599.7346	Src:10.10.100.119 Dst: 10.10.100.117 E as portas?FTP...	Login em PC na LAN (máquina virtual local); Execução de comandos (SYST, FEAT, EPSV, LIST, TYPE I, RETR); Download de ficheiros (teste.txt, overflowtest.c); Quit do PC; A sessão envolveu a transferência de 105 pacotes e 9157 KBytes há muitos mais detalhes visíveis
Stream 6 56-5[illegible] Incluem aqui a s	1583.254 a 1636.994	Src:10.10.100.119 Dst: 10.10.100.120	Mensagens de configuração usando protocolo SMB2. Criação, leitura e fecho do ficheiro "teste.txt". A sessão envolveu a transferência de 117 pacotes e 18.7 KBytes

4.2 UDP

Nº ordem ou *streams*	Tempo (s)	Src/Dest	Comentário
Stream 0 15	24.91494	Src: 10.10.100.121 Dst:162.159.200.1 (time.cloudfare)	Mensagens do protocolo NTP (cliente-servidor).
Stream 1 39	57.9418	Src: 10.10.100.121 Dst: 91.209.16.78 (smtp.in1.aqea.net)	Mensagens do protocolo NTP (cliente-servidor).
Stream 2 60	62.91119	Src: 10.10.100.121 Dst: 194.117.47.44 (ntp04.oal.ul.pt);	Mensagens do protocolo NTP (cliente-servidor).
Stream 3 67	585.966	Src: 10.10.100.121 Dst: 88.157.128.22 (static.cpe.netcabo.pt);	Mensagens do protocolo NTP (cliente-servidor).
Stream 4 75-76	2587.562	Src: 10.10.100.120 Dst: 10.10.100.255	Protocolo NBNS (NetBIOS Name Server) usado por hosts Windows. Este protocolo resolve endereços que se encontram na rede interna. Isto acontece porque o endereço não foi resolvido pelo DNS. O endereço mesmo assim não foi resolvido (10.10.100.117)
Stream 5 79	1618.992	Src: 10.10.100.120 Dst: 185.125.190.58 (prod-ntp-5.ntp2.ps5.canonical.com)	Mensagens do protocolo NTP (cliente-servidor).
Stream 7 80	1621.128	Src: 10.10.100.117 Dst:10.10.100.1	Resposta negativa para domínio (ubunto.localdomain).
Stream 6 77-78	2592.06	Src: 10.10.100.19 Dst: 10.10.100.1	Resolução de endereço falhada (No such name) para endereços: 117.100.10.10 e 119.100.10.10.

4.3 Tráfego Residual

Após analisar todo o tráfego TCP e UDP utilizamos o filtro “not tcp && not udp “para podermos filtrar os restantes pacotes. Nesta captura de tráfego obtivemos e observamos o protocolo ARP (usado na conversão de endereços de IP em endereços MAC da camada 2).

e que conclusão tiraram

E os streams TCP 48 a 55? Eram s

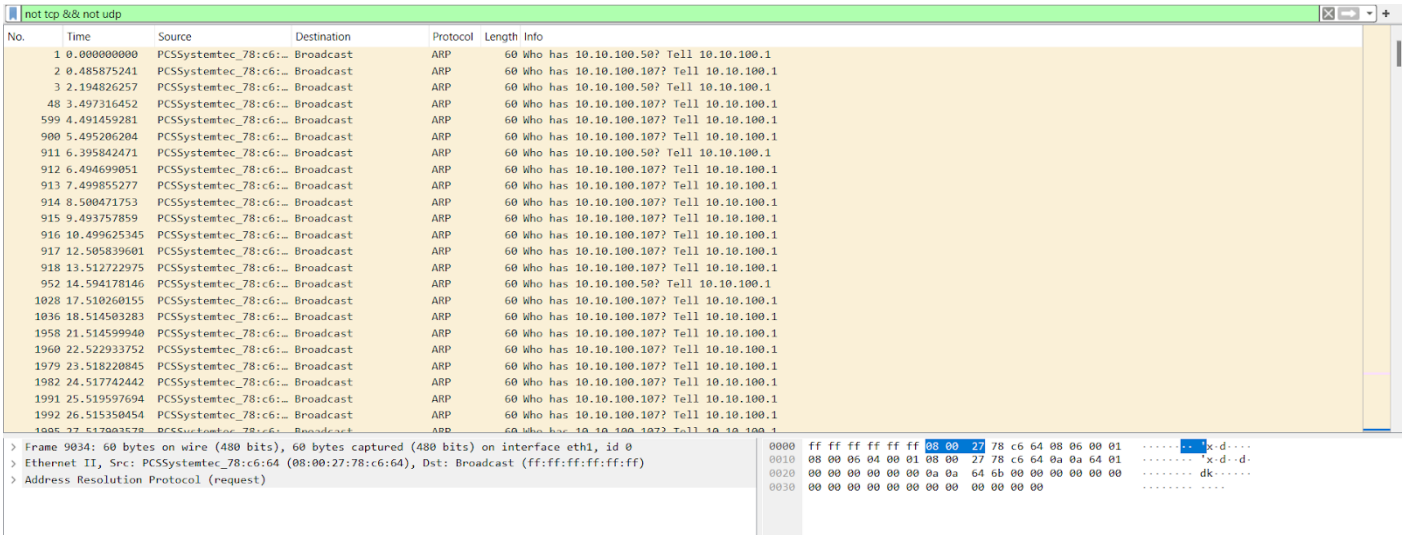


Figura 7 - Tráfego Residual

5. Conclusões

O tráfego observado parece ser predominantemente relacionado a atividades normais de navegação na web, autenticação em serviços online, troca de mensagens e tráfego DNS.

A análise abrangente do tráfego de rede forneceu uma visão detalhada das comunicações, participantes e padrões de tráfego na rede local 10.10.100.0/24. Estas informações são essenciais para a compreensão da atividade de rede, identificação de potenciais problemas e otimização do desempenho da rede.