

APRESENTAÇÃO DE LAUDO PERICIAL

Processo: 00000000-05.2025.6.18.0000

Autor: Ministério Público do Estado de Alguem Estado (MPAE) / (Senhora Beltrana)

Réu: Suspeitos de envio indevido de dados (Colabores Senhor Pessoa e Senhora Pessoa da Empresa Tal De Alguem Lugar – MG)

LAUDO PERICIAL

No dia 22 de abril de 2025, este Perito realizou **diligência pericial presencial** nas dependências da **Empresa Tal De Alguem Lugar – MG**, com metodologia e resultados apresentados no documento **ID 123456789**. Na sequência do trabalho pericial, no período de 23 de abril de 2025 a 22 de maio de 2025, em ambiente laboratorial (CyberOne – Laboratório de Computação Forense, Perícia Computacional e Inteligência Cibernética), este Perito examinou o conjunto completo das evidências digitais pertinentes ao processo.

No período de 23 a 26 de maio de 2025, este Perito elaborou o presente Laudo Pericial, descrevendo com verdade e com todas as circunstâncias o conjunto completo de informações que possa interessar ao Tribunal de Justiça de Alguem Estado, no âmbito do processo em epígrafe. Todas as tarefas periciais foram realizadas em conformidade com o que preconiza a Lei No. 13.105, de 16 de março de 2015, em seu Artigo 473, do Código de Processo Civil, que, em suma, estabelece os parâmetros para elaboração de laudos periciais e pareceres técnicos periciais, que servem como diretrizes para o trabalho do Perito. A Computação Forense e a Perícia Forense Computacional consistem, basicamente, no uso de métodos técnicos e científicos para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais com validade probatória em juízo. Este Perito observou o que preconiza a Norma ABNT ISO/IEC 27037:2013, que apresenta as diretrizes para identificação, coleta, aquisição, extração e preservação de evidências digitais em todas as etapas de um processo judicial e/ou de investigação, preservando, assim, a **cadeia de custódia**.

OBJETIVOS DA PERÍCIA

O trabalho pericial realizado por este **Perito** teve como objetivo geral a **verificação de conformidade** dos pacotes de dados da rede de comunicação desta empresa, com o que preconiza a **Lei Geral de Proteção de Dados (LGPD)** (Lei nº 13.709, de 14 de agosto de 2018).

Este **Perito** aplicou técnicas e procedimentos típicos da Perícia Forense Computacional, notadamente aqueles baseados em Interceptação e Monitoramento de Redes de Comunicação, que consistem no uso de ferramentas, procedimentos e estratégias para coletar, analisar e validar evidências digitais que possam ser encontradas ao monitorar e analisar tráfego de pacotes de uma rede de comunicação.

Na realização dos exames periciais, os seguintes objetivos específicos foram definidos e alcançados:

1. realizar, em diligência presencial, uma escuta na rede de comunicação utilizando a ferramenta **WireShark**.
2. salvar toda a captura com os pacotes de dados em um arquivo do tipo **PCAP (Packet Capture)**, para realizar a análise em ambiente laboratorial;
3. confrontar e analisar os dados e informações coletados com o que preconiza a **Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018)**.
4. elaborar e apresentar o laudo pericial.

OBJETOS PARA PERÍCIA

O material examinado por este Perito é composto pelos seguintes objetos digitais:

1. Um arquivo, em formato PCAP (*Packet Capture*) e denominado **captura03102023.pcap**, gerado a partir da ferramenta **WireShark** durante a Diligência Pericial Presencial, contendo os pacotes de dados da rede de comunicação, com todas as transferências e recebimentos de dados capturados no dia **22 de abril de 2025**; a integridade do arquivo pode ser verificada, a qualquer tempo, pela HASH MD5 **5038820266FBB0F78248389D3EA1241F** e pela HASH SHA-256 **345CFF9E00C4D70BC1CED692CFADDAE39614704FD09D4A39AB078994C07A4354** ;

QUESITOS

A parte Ré, através de seus patronos, não apresentou quesitos nos autos do processo. Os quesitos periciais (num total de 6 – seis), que deveriam ser analisados e respondidos por este Perito, foram apresentados pela parte autora – o **Ministério Público do Estado de Alagoas (MPAE)** – no documento **ID 987654321**.

METODOLOGIA

Na **primeira etapa do trabalho pericial**, este Perito realizou **diligência pericial presencial** nas dependências da **Empresa Tal De Algum Lugar – MG**, no dia **22 de abril de 2025**, onde foi recebido por **Senhora Beltrana** (Diretora Executiva desde 15 de março de 2018), parte autora do Inquérito Policial, **Senhora Pessoa** (Assistente Administrativa desde 12 de janeiro de 2021) e **Senhor Pessoa** (Assistente de Departamento Pessoal desde 13 de janeiro de 2020 e reconduzido ao cargo em 01 de janeiro de 2022), colaboradores da empresa apontados como rés no presente caso.

A senhora Beltrana, na qualidade de responsável pela denúncia e gestora da empresa, acompanhou toda a diligência, fornecendo informações relevantes sobre os procedimentos internos, bem como acesso aos computadores utilizados pela organização.

O Senhor Pessoa e a Senhora Pessoa, indicados como possíveis responsáveis pela utilização indevida da rede de comunicação da empresa, também acompanharam a diligência e atenderam todos os pedidos formulados por este Perito, e prestando esclarecimentos sobre seus respectivos acessos e funções dentro da empresa.

Todos os profissionais citados colaboraram prontamente, sempre no contexto **exclusivo** da atividade pericial relacionada ao objeto do inquérito policial examinado.

O sistema de comunicação da **Empresa Tal**, tanto em sua infraestrutura de rede quanto em suas ferramentas de comunicação interna e armazenamento de documentos no servidor, é disponibilizado aos colaboradores, com o suporte técnico pela referida empresa, a **Empresa TI**, inscrita no CNPJ sob o número 00.00.000/0001-00, sediada na cidade de **Tal Lugar – MG**, em contrato celebrado com a **Empresa Tal**.

Compete à referida empresa contratada a oferta da completa infraestrutura de rede e suporte ao funcionamento da rede corporativa e aos sistemas utilizados, infraestrutura que é mantida na sede da empresa contratada. Neste contexto, compete aos colaboradores da **Empresa Tal**, a utilização adequada dessa rede, respeitando os protocolos internos de segurança e confiabilidade, bem como as normas de conduta determinadas pela política interna da organização.

A **Senhora Beltrana**, Diretora executiva da **Empresa Tal** e parte autora na presente ação, também respondeu aos questionamentos deste **Perito**, ressaltando que têm ciência do processo judicial em curso e do objeto principal desta atividade pericial, que compreende a análise de tráfego dos

pacotes de dados da rede corporativa, bem como a verificação de sua conformidade com as normas internas da empresa e a **Lei Geral de Proteção de Dados (LGPD)**.

Como principal resultado desta diligência, foi gerado um arquivo de captura de pacotes da rede, em formato PCAP (*Packet Capture*), esta captura foi realizada diretamente na infraestrutura de rede da empresa, com consentimento e mediante autorização judicial. Para esta captura, foi utilizada a ferramenta **Wireshark**, configurada em modo promíscuo, garantindo a interceptação de todos os pacotes transmitidos e recebidos pelos dispositivos conectados na rede local.

O procedimento foi realizado em ambiente controlado, com o acompanhamento da **Senhora Beltrana**, Diretora Executiva da empresa.

Durante a captura, foram tomadas medidas para evitar qualquer alteração nos dados coletados, bem como preservar a confidencialidade das informações.

O resultado desta captura originou o arquivo denominado **captura03102023.pcap**, que está devidamente anexado a este laudo pericial. Para assegurar a integridade do referido arquivo, e possibilitar sua verificação e comprovação a qualquer tempo, este **Perito** calculou, utilizando a ferramenta **HashCalc**, os seguintes códigos HASH:

MD5	5038820266FBB0F78248389D3EA1241F
SHA-256	345CFF9E00C4D70BC1CED692CFADDAE39614704FD09D4A39AB078994C07A4354

Tal procedimento, garante a autenticidade e integridade da evidência digital coletada, preservando sua cadeia de custódia.

Na segunda etapa do trabalho pericial, em ambiente laboratorial, este Perito criou uma cópia da evidência digital coletada durante a diligência presencial, para não correr o risco de comprometer o arquivo original, e os exames foram realizados a partir da cópia idêntica da evidência digital coletada. Utilizando as ferramentas **Wireshark** e **Tshark**, esta última, sendo a versão de linha de comando do **Wireshark**, adequada para filtragem e análise precisa de grandes volumes de dados de rede. Ambas ferramentas são amplamente reconhecidas pela comunidade técnica e forense, sendo utilizadas para inspecionar pacotes de dados em nível detalhado, possibilitando análises como, verificação de protocolos de comunicação, fluxos de tráfego e endereços IP (*Internet Protocol*). Durante esta etapa, foram utilizado alguns comandos no **Tshark** para verificar a quantidade total de pacotes capturados e a quantidade de endereços IPs(*Internet Protocol*) diferentes que interagiram de alguma forma na rede de comunicação da empresa, em seguida o **Wireshark** foi utilizado principalmente para visualização gráfica, e utilização de filtros para analisar

se havia registros de acessos em sites específicos e determinar o horário de acesso e os navegadores web utilizados, por fim foi utilizado filtros para verificar se houve envio de e-mail com arquivos em anexo, e analisar o conteúdo do mesmo, esta análise de tráfego foi realizada a partir dos quesitos periciais apresentados pelo **Ministério Público do Estado de Alagoas (MPAE)**, no documento **ID 123456789**.

Na terceira etapa do trabalho pericial, este Perito elaborou este laudo e o entregou de forma eletrônica, via Plataforma Canvas, na seção Tarefas e no formato DOCX.

RESPOSTAS AOS QUESITOS

Realizadas todas as etapas do trabalho técnico, este Perito apresenta as respostas aos quesitos formulados e apresentados pelo **Ministério Público do Estado de Alagoas (MPAE)** no documento **ID 123456789**.

1. Quantos pacotes foram capturados na rede de comunicação?

Resposta: Via linha de comando, com a ferramenta **Tshark**, foi utilizado o seguinte comando: **"tshark -r captura.pcap -q -z io,stat,0"**, este comando exibe um resumo com estatísticas, como o total de pacotes e o número de Bytes do arquivo de captura, conforme mostra a **Figura 01**. Após esta verificação foi constatado um total de **304.199**(Trezentos e quatro mil, cento e noventa e nove) pacotes.

```
C:\Users\Bruno\Downloads>tshark -r captura03102023.pcap -q -z io,stat,0

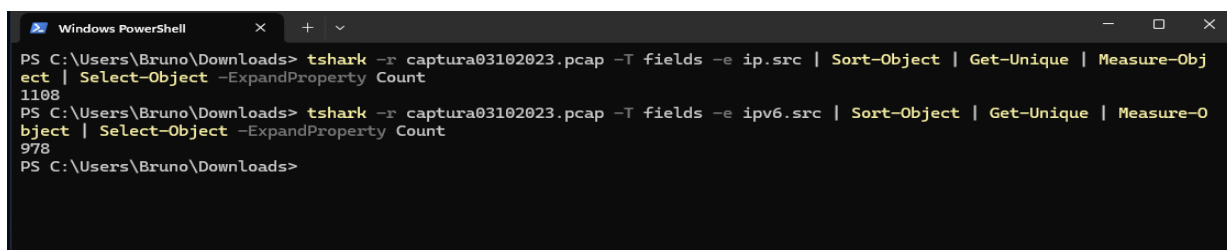
=====
| IO Statistics
|
| Duration: 1490.2 secs
| Interval: 1490.2 secs
|
| Col 1: Frames and bytes
|-----|
| Interval      | 1 | Frames | Bytes |
|-----|
| 0.0 <-> 1490.2 | 304199 | 68533126 |
|-----|

C:\Users\Bruno\Downloads>
```

Figura 01 – Imagem da saída do comando, mostrando um resumo com estatísticas do arquivo de captura do tipo PCAP (*Packet Capture*)

2. Quantos endereços IP (Internet Protocol) diferentes foram identificados na origem dos pacotes?

Resposta: Utilizou-se a ferramenta Tshark em linha de comando, utilizado os comandos “tshark -r captura.pcap -T fields -e ip.src | Sort-Object | Get-Unique | Measure-Object | Select-Object -ExpandProperty Count” e “tshark -r captura.pcap -T fields -e ipv6.src | Sort-Object | Get-Unique | Measure-Object | Select-Object -ExpandProperty Count”, conforme mostra a **Figura 02**, para calcular o número de IPV4(*Internet Protocol Version 4*) e IPV6(*Internet Protocol Version 6*) de origem, respectivamente, resultando em **1108(Mil Cento e Oito) endereços IPV4** e **978(Novecentos e Setenta e Oito) endereços IPV6** identificados na origem dos pacotes.

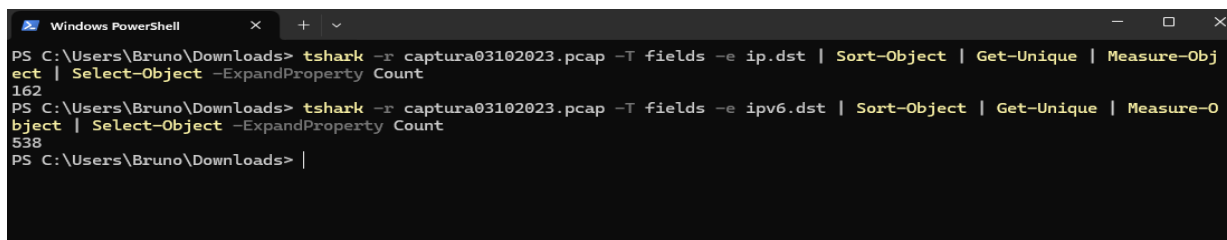


```
Windows PowerShell
PS C:\Users\Bruno\Downloads> tshark -r captura03102023.pcap -T fields -e ip.src | Sort-Object | Get-Unique | Measure-Object | Select-Object -ExpandProperty Count
1108
PS C:\Users\Bruno\Downloads> tshark -r captura03102023.pcap -T fields -e ipv6.src | Sort-Object | Get-Unique | Measure-Object | Select-Object -ExpandProperty Count
978
PS C:\Users\Bruno\Downloads>
```

Figura 02 – Imagem dos comandos que foram executados via linha de comando utilizando a ferramenta Tshark para calcular o número de endereços IP na origem dos pacotes

3. Quantos endereços IP (Internet Protocol) diferentes foram identificados no destino dos pacotes?

Resposta: Utilizou-se novamente a ferramenta Tshark em linha de comando, utilizados comandos “tshark -r captura03102023.pcap -T fields -e ip.dst | Sort-Object | Get-Unique | Measure-Object | Select-Object -ExpandProperty Count” e “tshark -r captura03102023.pcap -T fields -e ipv6.dst | Sort-Object | Get-Unique | Measure-Object | Select-Object -ExpandProperty Count”, conforme mostra a **Figura 03**, para calcular o número de IPV4 e IPV6 de destino, respectivamente, resultando em **162(Cento e Sessenta e Dois) endereços IPV4** e **538(Quinhentos e Trinta e Oito) endereços IPV6** identificados no destino dos pacotes.



```
Windows PowerShell
PS C:\Users\Bruno\Downloads> tshark -r captura03102023.pcap -T fields -e ip.dst | Sort-Object | Get-Unique | Measure-Object | Select-Object -ExpandProperty Count
162
PS C:\Users\Bruno\Downloads> tshark -r captura03102023.pcap -T fields -e ipv6.dst | Sort-Object | Get-Unique | Measure-Object | Select-Object -ExpandProperty Count
538
PS C:\Users\Bruno\Downloads> |
```

Figura 03 – Imagem dos comandos que foram executados via linha de comando utilizando a ferramenta Tshark para calcular o número de endereços IP no destino dos pacotes

4. Nos pacotes capturados, há algum registro de acesso ao site www.pucminas.br? Em caso afirmativo, qual(is) a(s) data(s) e horário(s) do(s) acesso(s)? É possível informar o(s) navegador(es) web utilizado(s)?

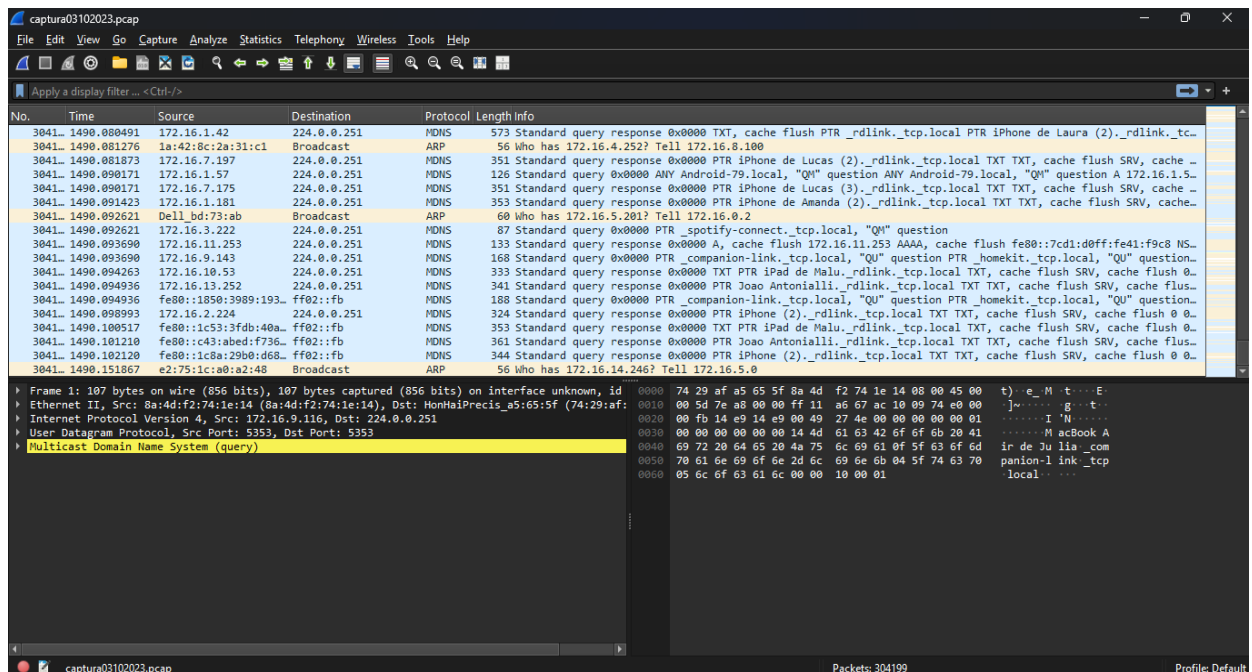


Figura 04 – Imagem da interface gráfica da ferramenta Wireshark durante a análise dos pacotes

Resposta: Utilizando a ferramenta **Wireshark**, para uma análise visual dos pacotes e com aplicação de filtros, no intuito de verificar o possível acesso ao site www.pucminas.br, primeiramente, foi utilizado o filtro: **"dns.qry.name contains \"www.pucminas.br\""**, com a finalidade de analisar se houve consultas no protocolo DNS (*Domain Name System*) para resolução do nome de domínio do site, que resultou em uma comunicação do IP (*Internet Protocol*) de origem **172.16.1.167** com o servidor DNS, conforme mostra a **Figura 05**, por fim foi utilizado o filtro **"frame contains \"www.pucminas.br\""**, para exibir qualquer pacote de rede que mencione o domínio www.pucminas.br, conforme mostra a **Figura 06**, resultando na confirmação de apenas **1 (um)** acesso, realizado pelo IP (*Internet Protocol*), **172.16.1.167**, na data de **03 de outubro de 2023 às 10:08:43**, via protocolo TLS1.2(*Transport Layer Security*), um protocolo criptografado, portanto **não é possível informar qual navegador web foi utilizado**.

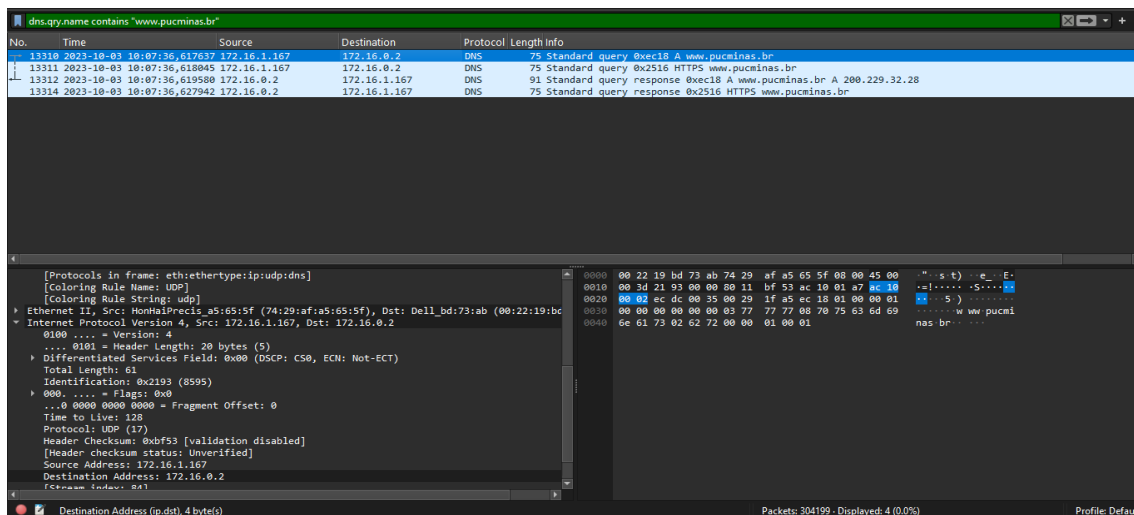


Figura 05 – Imagem da ferramenta Wireshark com o filtro de DNS para verificar se houve a resolução do domínio do site PUC Minas

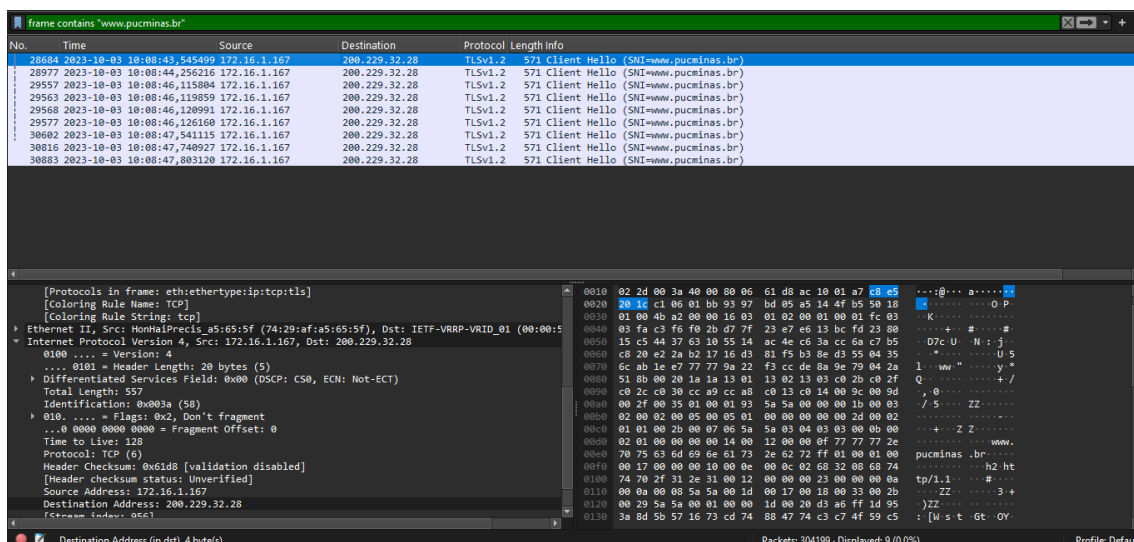


Figura 06 – Imagem da ferramenta Wireshark com o filtro para verificar os protocolos que contêm o domínio do site PUC Minas

5. Nos pacotes capturados, há algum registro de acesso à plataforma YouTube? Em caso afirmativo, qual a data e o horário em que ocorreu cada acesso?

Resposta: Na ferramenta **Wireshark**, após a utilização do filtro **"dns.qry.name contains "youtube"**, que foi utilizado para filtrar os possíveis acessos à plataforma **YouTube**, foi constatado que houve apenas **1 (um)** registro de acesso vindo do IP (*Internet Protocol*) **172.16.1.167** para o IP (*Internet Protocol*) de destino **172.16.0.2**, correspondendo ao endereço do servidor DNS(*Domain Name System*) que realizou as consultas ao domínio, o acesso foi realizado no dia **03 de outubro de 2023 às 10:24:52**, como mostra a **Figura 07**.

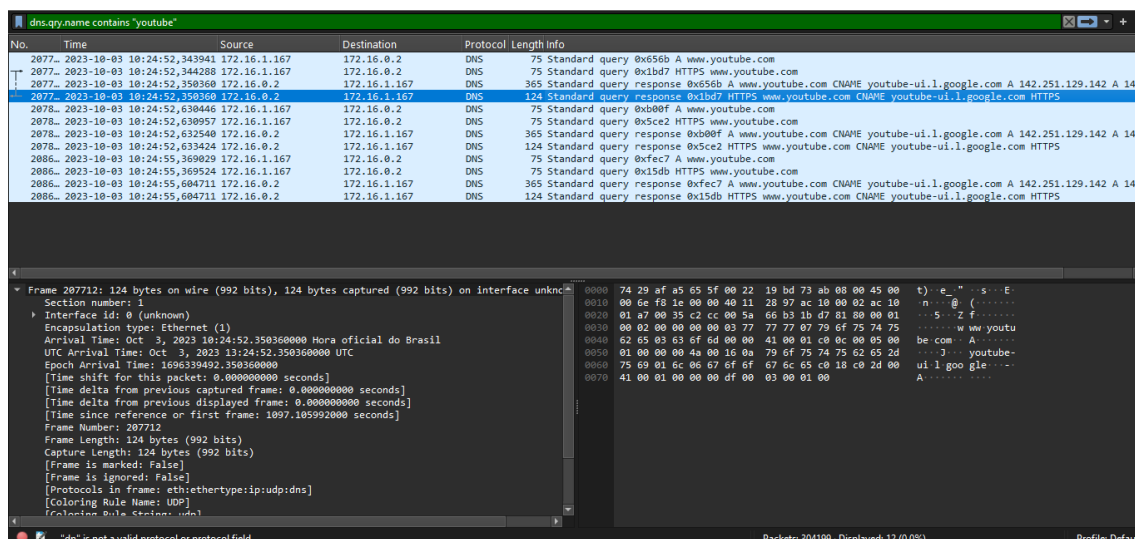


Figura 07 – Imagem da ferramenta Wireshark com o filtro para exibir os acessos à plataforma YouTube

6. Nos pacotes capturados, houve algum envio de e-mail com arquivo em anexo? Em caso afirmativo, qual o tipo de arquivo enviado, a data e a hora do envio? É possível identificar o destinatário do e-mail? Caso o arquivo seja um documento em formato PDF, é possível identificar o seu conteúdo?

Resposta: Ao realizar análise do protocolo SMTP (*Simple Mail Transfer Protocol*), com filtros de protocolo na ferramenta **Wireshark**, este **Perito** comprovou que não possui nenhum tráfego deste pacote, que corresponde ao envio de e-mails, conforme mostra a **Figura 08**. Portanto, conclui-se que não houve nenhum envio de e-mail durante o período da captura de pacotes.

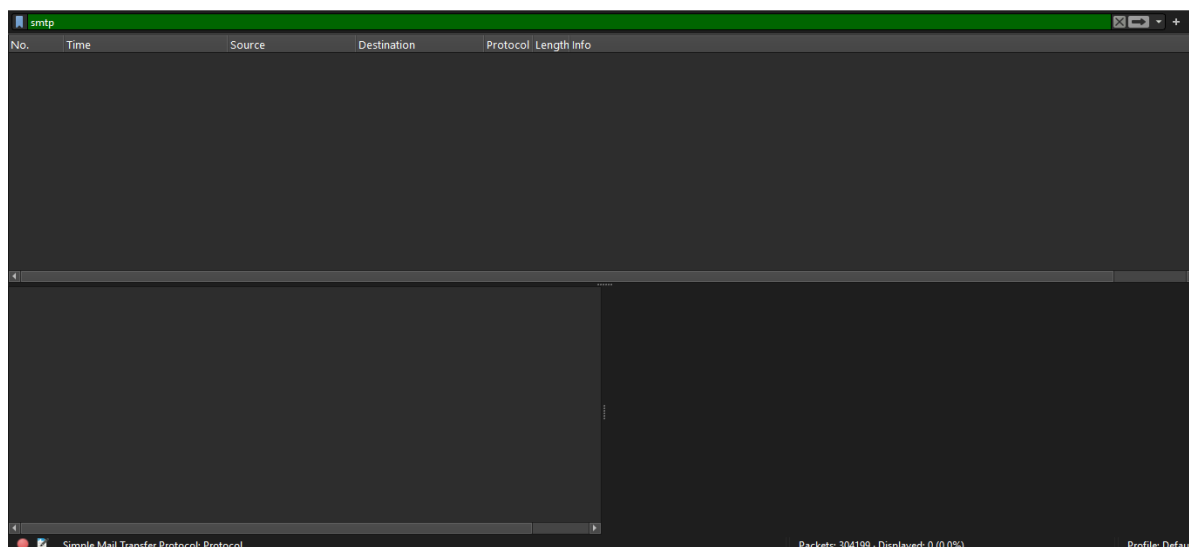


Figura 08 – Imagem do resultado da ferramenta Wireshark com filtragem por pacotes SMTP (*Simple Mail Transfer Protocol*)

CONCLUSÃO

No período, entre **23 de abril de 2025 e 22 de maio de 2025**, em que este Perito verificou e analisou os pacotes de dados da rede capturados durante a diligência presencial, a análise permitiu verificar de forma precisa os acessos realizados, os protocolos utilizados, os endereços IP (*Internet Protocol*) envolvidos e o comportamento do tráfego de rede durante o período monitorado.

A partir desta análise, constatou-se que a maior parte das comunicações capturadas se encontra dentro dos padrões esperados para uma rede corporativa. Embora tenha sido identificado acesso a plataformas de conteúdo, como o *YouTube*, este evento ocorreu de forma pontual e isolada. Durante a análise não foram detectados envios de e-mails com anexos destinados a terceiros, não havendo evidências de utilização indevida de dados sensíveis da empresa, nem transmissões de arquivos de natureza confidencial, portanto estando em conformidade com o que preconiza a **Lei Geral de Proteção de Dados (LGPD)**.

Em relação aos quesitos apresentados, este Perito respondeu integralmente aos 6 (seis) questionamentos formulados, fornecendo dados como número de pacotes e endereços IP (*Internet Protocol*), e também dados de acessos a determinados *websites*, data e hora do acesso e análise da existência de anexos sendo enviados via e-mail.

Por fim, destaca-se, que não foram identificadas ações que possam configurar infração à segurança da informação ou uso indevido da rede corporativa, no que diz respeito ao compartilhamento de dados sigilosos da empresa.

Foram estes os elementos analisados, periciados e passíveis de serem apresentados por este Perito. Nada mais havendo a constar, este Perito encerra o presente Laudo Pericial, elaborado em 11 (onze) páginas e contendo 01 (um) anexo.

Poços de Caldas – MG, 22 de maio de 2025.

Bruno Felipe Barretto de França

Estudante do 4º Período de Ciência da Computação | Perito Ad Hoc das Forças de Segurança e Lei

Sobre o Perito (conforme preconiza o inciso II, § 2º do artigo 465 do CPC)

Bruno Felipe Barretto de França, Estudante de Ciência da Computação

Em 2023 iniciou o Curso de Ciência da Computação da Pontifícia Universidade Católica de Minas Gerais – PUC Minas (www.pucpcaldas.br), campus de Poços de Caldas, e encontra-se no 4º período do curso.