

A thin, light brown L-shaped line is positioned to the left of the main title.

# Laboratório Virtual de Redes

Usando o Wireshark

A thin, light brown L-shaped line is positioned to the right of the subtitle.

## Tutorial com GNS3

Esse tutorial foi construído utilizando o Sistema Operacional Windows 10 e software Wireshark, versão 4.0.6.



## Primeira Etapa: Preparação ou Download do software Wireshark

**Passo 1:** Certifique-se de ter o Wireshark instalado em seu computador. Você pode baixá-lo em <https://www.wireshark.org/>, role a página e na seção download clique na versão do seu Sistema Operacional.

### Download Wireshark

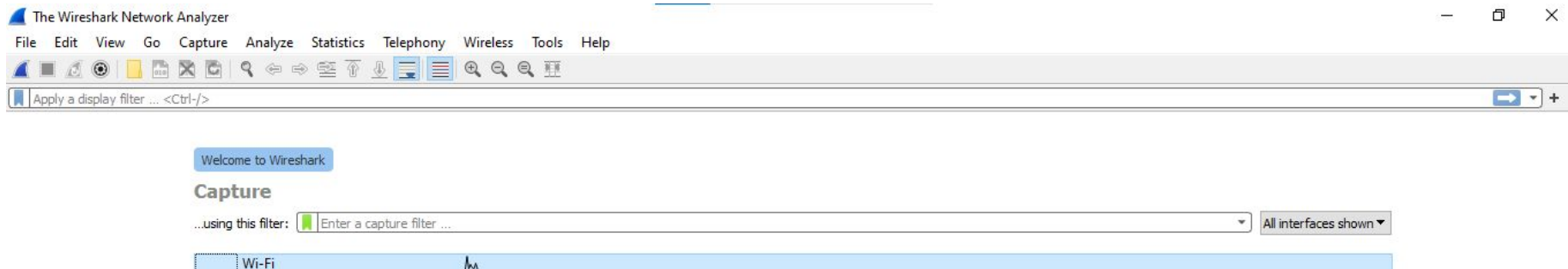
The current stable release of Wireshark is 4.0.6. It supersedes all previous releases.

#### ▼ Stable Release: 4.0.6

-  Windows Intel Installer
-  Windows Intel PortableApps®
-  macOS Arm Disk Image
-  macOS Intel Disk Image
-  Source Code

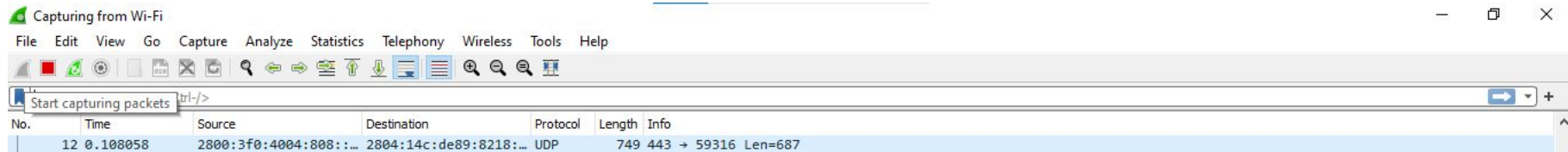
# Primeira Etapa: Preparação ou Download do software Wireshark

**Passo 2:** Abra o Wireshark e selecione a interface de rede correta para capturar o tráfego. Isso geralmente é a interface Ethernet ou Wi-Fi conectada ao seu computador.



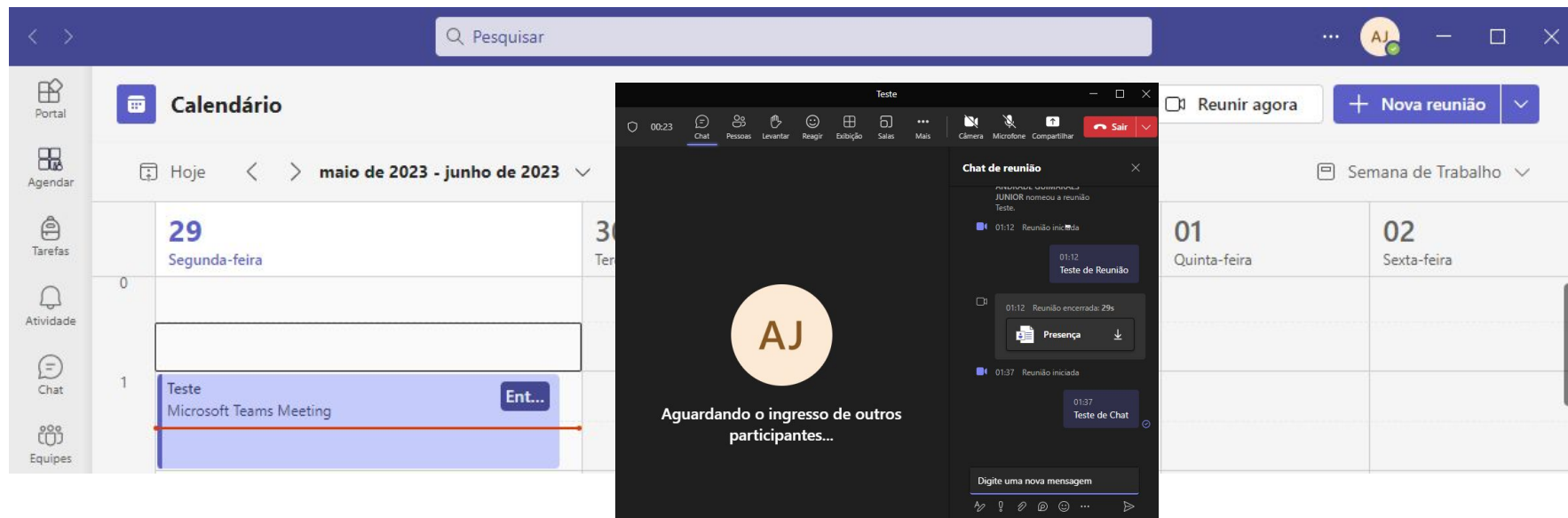
## Segunda Etapa: Iniciando a captura

**Passo 1:** Inicie a captura de pacotes no Wireshark clicando no botão "Start" ou no ícone de play.



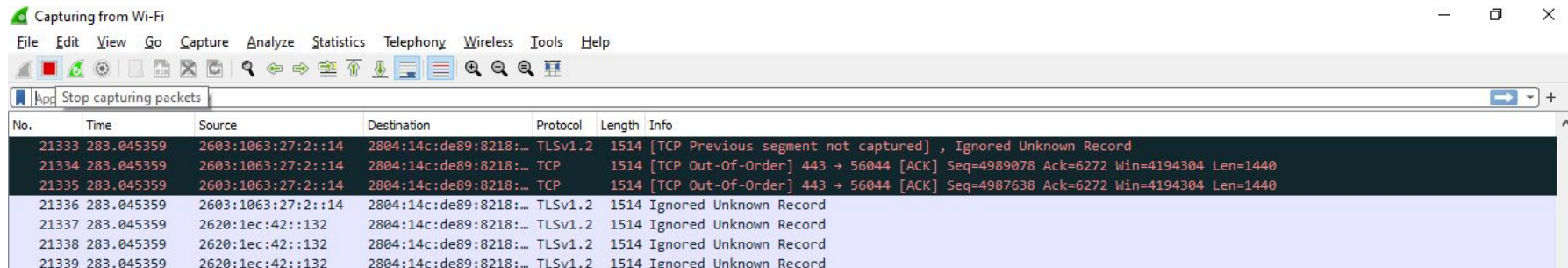
## Segunda Etapa: Iniciando a captura

**Passo 2:** Abra o aplicativo Microsoft Teams em seu computador. Faça login em sua conta do Microsoft Teams e participe de uma reunião ou realize uma chamada.



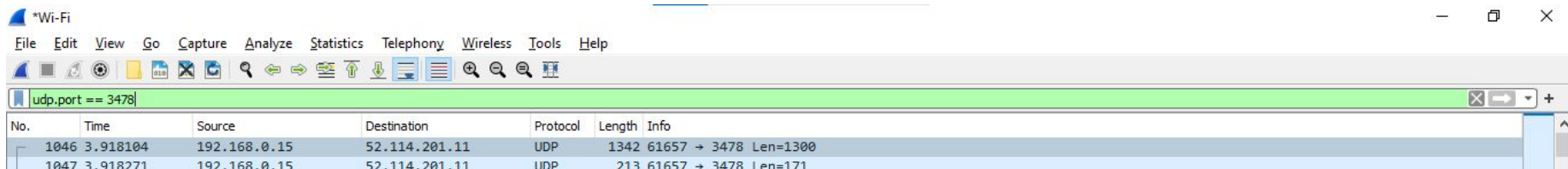
## Terceira Etapa: Capturando o tráfego do Microsoft Teams

**Passo 1:** Volte para o Wireshark e pare a captura de pacotes clicando no botão "Stop" ou no ícone de pause. Agora, você verá uma lista de pacotes capturados no Wireshark.



## Quarta Etapa: Filtrando o tráfego do Microsoft Teams

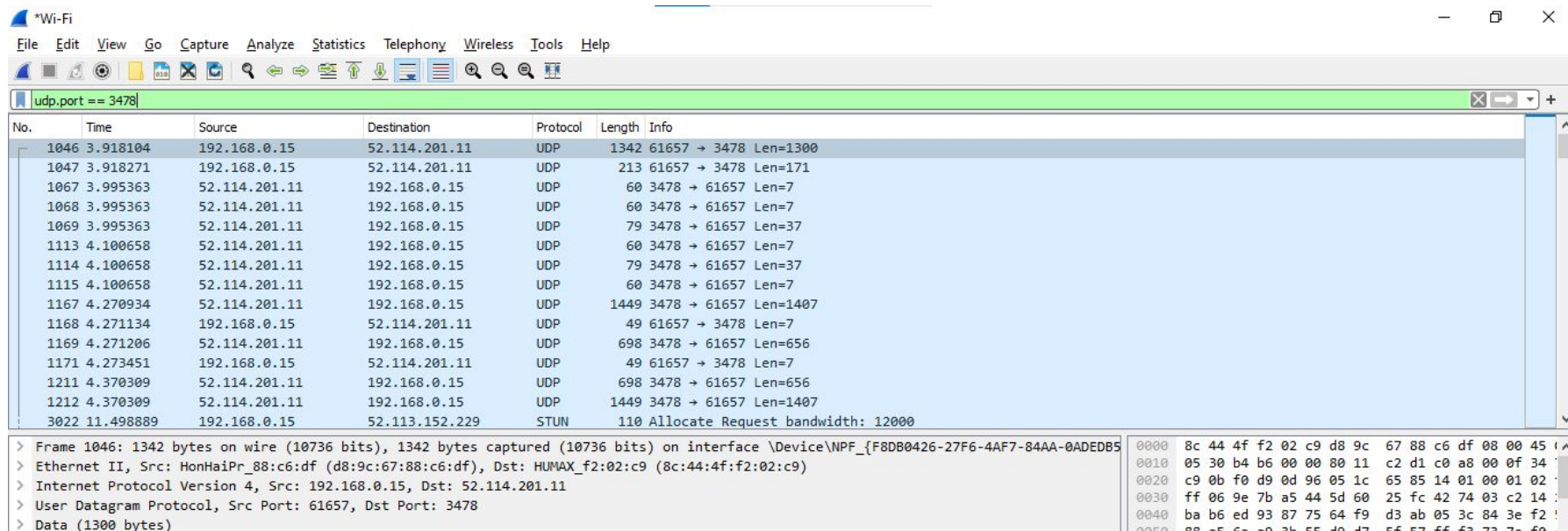
**Passo 1:** Para facilitar a análise, você pode aplicar um filtro no Wireshark para exibir apenas os pacotes relacionados ao Microsoft Teams. Digite o seguinte filtro na barra de filtro do Wireshark: `udp.port == 3478 or udp.port == 443 or udp.port == 3479 or udp.port == 3480`.





## Quarta Etapa: Filtrando o tráfego do Microsoft Teams

**Passo 2:** Pressione Enter para aplicar o filtro. Agora, você verá apenas os pacotes relevantes para o Microsoft Teams.



The image shows a Wireshark network traffic capture window titled "Wi-Fi". The filter bar at the top contains the expression `udp.port == 3478`. The packet list pane displays a series of captured packets, all of which are filtered to show only those related to Microsoft Teams traffic (UDP port 3478). The selected packet is No. 1046, which is a UDP packet from 192.168.0.15 to 52.114.201.11, length 1342 bytes, containing a 1300-byte payload. The packet details pane on the right shows the structure of this packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (1300 bytes). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

| No.  | Time      | Source        | Destination    | Protocol | Length | Info                              |
|------|-----------|---------------|----------------|----------|--------|-----------------------------------|
| 1046 | 3.918104  | 192.168.0.15  | 52.114.201.11  | UDP      | 1342   | 61657 → 3478 Len=1300             |
| 1047 | 3.918271  | 192.168.0.15  | 52.114.201.11  | UDP      | 213    | 61657 → 3478 Len=171              |
| 1067 | 3.995363  | 52.114.201.11 | 192.168.0.15   | UDP      | 60     | 3478 → 61657 Len=7                |
| 1068 | 3.995363  | 52.114.201.11 | 192.168.0.15   | UDP      | 60     | 3478 → 61657 Len=7                |
| 1069 | 3.995363  | 52.114.201.11 | 192.168.0.15   | UDP      | 79     | 3478 → 61657 Len=37               |
| 1113 | 4.100658  | 52.114.201.11 | 192.168.0.15   | UDP      | 60     | 3478 → 61657 Len=7                |
| 1114 | 4.100658  | 52.114.201.11 | 192.168.0.15   | UDP      | 79     | 3478 → 61657 Len=37               |
| 1115 | 4.100658  | 52.114.201.11 | 192.168.0.15   | UDP      | 60     | 3478 → 61657 Len=7                |
| 1167 | 4.270934  | 52.114.201.11 | 192.168.0.15   | UDP      | 1449   | 3478 → 61657 Len=1407             |
| 1168 | 4.271134  | 192.168.0.15  | 52.114.201.11  | UDP      | 49     | 61657 → 3478 Len=7                |
| 1169 | 4.271206  | 52.114.201.11 | 192.168.0.15   | UDP      | 698    | 3478 → 61657 Len=656              |
| 1171 | 4.273451  | 192.168.0.15  | 52.114.201.11  | UDP      | 49     | 61657 → 3478 Len=7                |
| 1211 | 4.370309  | 52.114.201.11 | 192.168.0.15   | UDP      | 698    | 3478 → 61657 Len=656              |
| 1212 | 4.370309  | 52.114.201.11 | 192.168.0.15   | UDP      | 1449   | 3478 → 61657 Len=1407             |
| 3022 | 11.498889 | 192.168.0.15  | 52.113.152.229 | STUN     | 110    | Allocate Request bandwidth: 12000 |

> Frame 1046: 1342 bytes on wire (10736 bits), 1342 bytes captured (10736 bits) on interface \Device\NPF\_{F8DB0426-27F6-4AF7-84AA-0ADEDB5} Ethernet II, Src: HonHaiPr\_88:c6:df (d8:9c:67:88:c6:df), Dst: HUMAN\_f2:02:c9 (8c:44:4f:f2:02:c9)  
> Internet Protocol Version 4, Src: 192.168.0.15, Dst: 52.114.201.11  
> User Datagram Protocol, Src Port: 61657, Dst Port: 3478  
> Data (1300 bytes)

## Quinta Etapa: Analisando o tráfego do Microsoft Teams

**Passo 1:** Observe os pacotes capturados relacionados ao Microsoft Teams. Você verá protocolos como UDP, TCP, TLS/SSL e outros.

```
> Frame 1046: 1342 bytes on wire (10736 bits), 1342 bytes captured (10736 bits) on interface \Device\NPF_{F8DB0426-27F6-4AF7-84AA-0ADEDB5}
> Ethernet II, Src: HonHaiPr_88:c6:df (d8:9c:67:88:c6:df), Dst: HUMAX_f2:02:c9 (8c:44:4f:f2:02:c9)
> Internet Protocol Version 4, Src: 192.168.0.15, Dst: 52.114.201.11
> User Datagram Protocol, Src Port: 61657, Dst Port: 3478
> Data (1300 bytes)
```

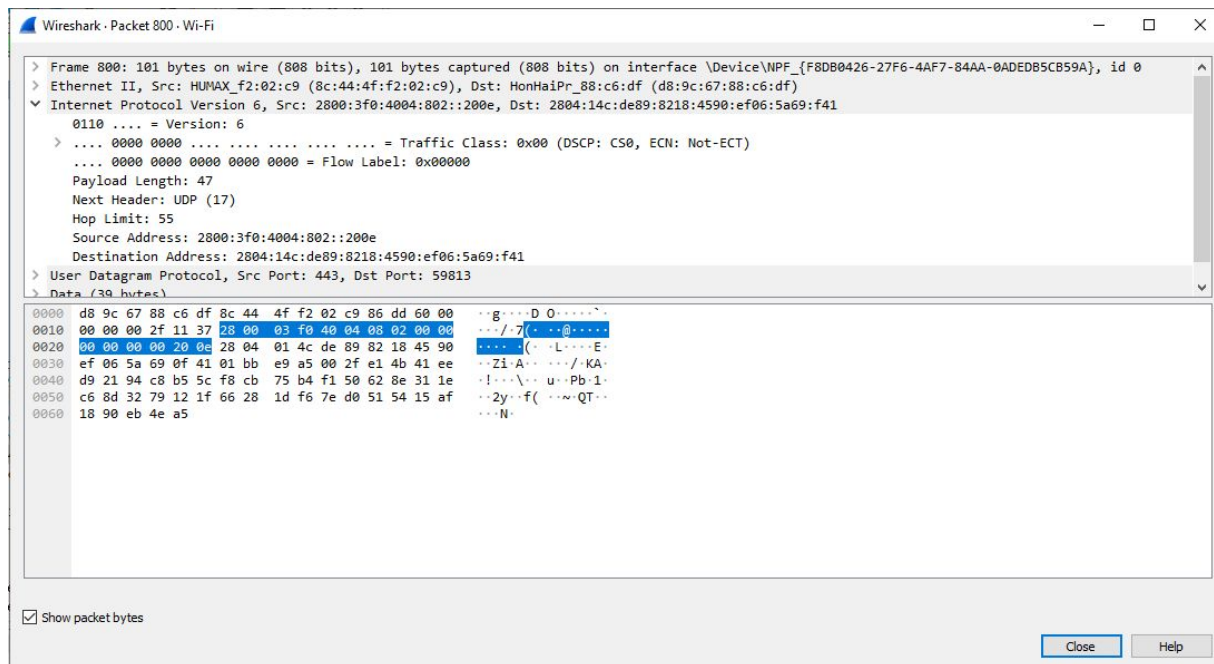
## Quinta Etapa: Analisando o tráfego do Microsoft Teams

**Passo 2:** Expanda os pacotes para visualizar os detalhes, como cabeçalhos, informações de endereço IP, informações de porta e outras informações relevantes.

```
▼ User Datagram Protocol, Src Port: 61657, Dst Port: 3478
  Source Port: 61657
  Destination Port: 3478
  Length: 1308
  Checksum: 0x6585 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 14]
▼ [Timestamps]
  [Time since first frame: 0.000000000 seconds]
  [Time since previous frame: 0.000000000 seconds]
  UDP payload (1300 bytes)
▼ Data (1300 bytes)
  Data: 1401000102ffff069e7ba5445d6025fc427403c21426bab6ed93877564f9d3ab053c843e...
  [Length: 1300]
```

## Quinta Etapa: Analisando o tráfego do Microsoft Teams

**Passo 3:** Observe os pacotes relacionados às chamadas de áudio e vídeo, mensagens de chat, compartilhamento de tela e outras funcionalidades do Microsoft Teams.





Parabéns! Você montou um cenário cujo objetivo é capturar e analisar o tráfego de rede gerado pelo aplicativo Microsoft Teams, utilizando a ferramenta de análise de pacotes Wireshark. O tutorial fornece um guia passo a passo detalhado sobre como realizar a captura, filtragem e análise do tráfego específico do Microsoft Teams no Wireshark.