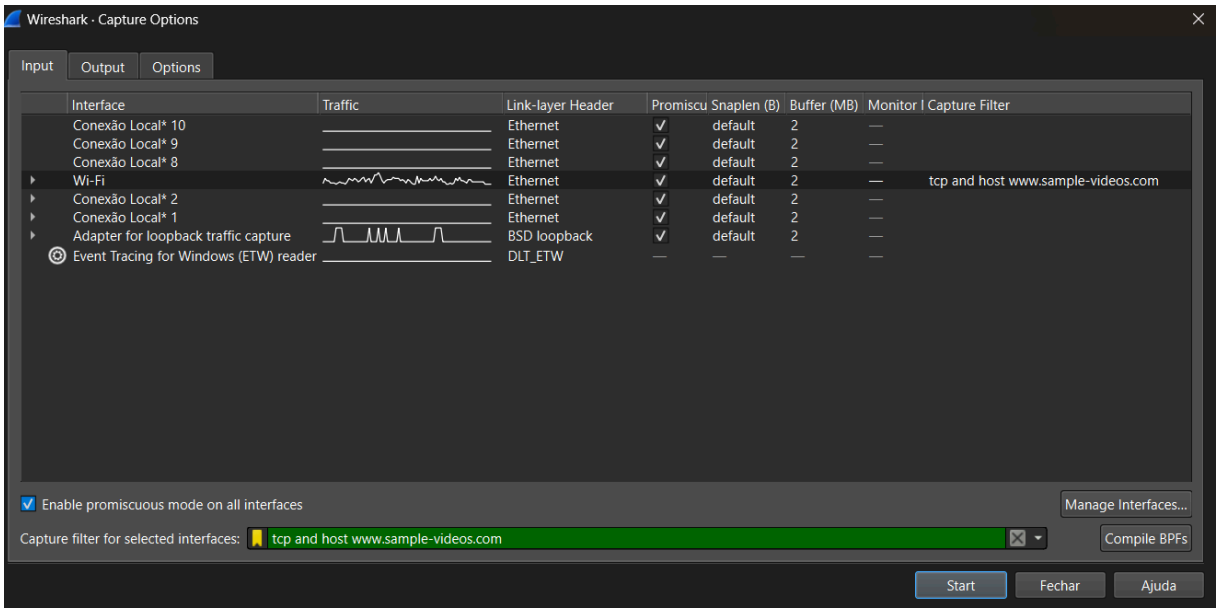
Disciplina: Redes de Computadores II
Turma: T01 Bloco: 4
Professor: Rayner Gomes Sousa
Alunos: Marcos Antônio e Vandirleya Barbosa

Laboratório TCP

Etapa 1 - Capturar um Rastro

a) Configuração do Filtro de Captura:

A primeira etapa consistiu na configuração do filtro de captura no Wireshark, com o objetivo de capturar exclusivamente o tráfego TCP associado a um host específico. O filtro aplicado foi 'tcp and host www.sample-videos.com', onde 'www.sample-videos.com' representa o host cujo tráfego TCP foi capturado. Este filtro assegura que as informações de rede relacionadas ao host especificado sejam capturadas e realçadas.



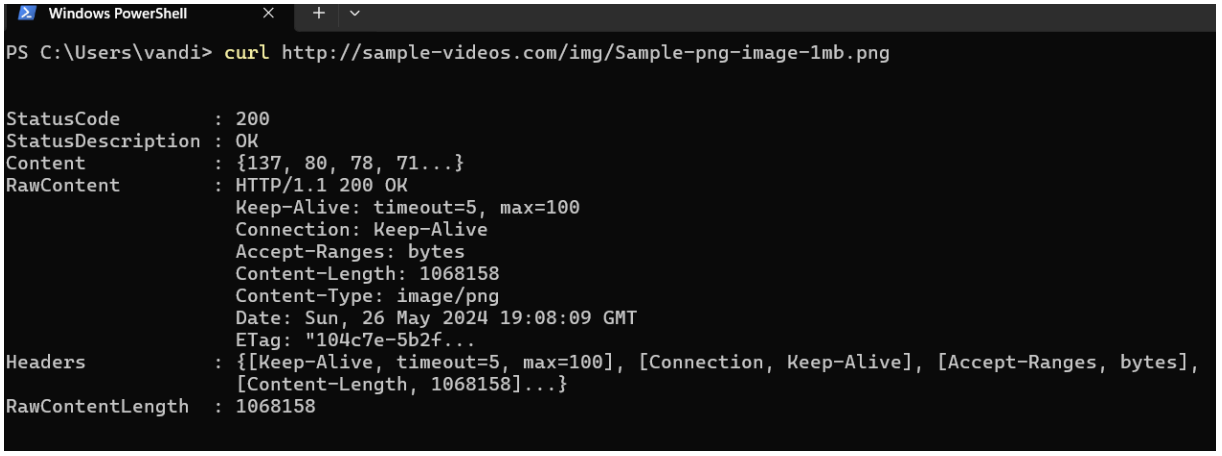
b) Preparação para a Captura

Depois de configurar o filtro de captura, demos início à captura de tráfego no Wireshark. Fizemos uma verificação para assegurar que a interface de rede selecionada estava correta, garantindo assim que o Wireshark estivesse capturando pacotes na interface de rede adequada. Em seguida, selecionamos "wifi" e prosseguimos para configurar o download via terminal, permitindo que o Wireshark capturasse os pacotes.

c) *Download* do Recurso da *Web*

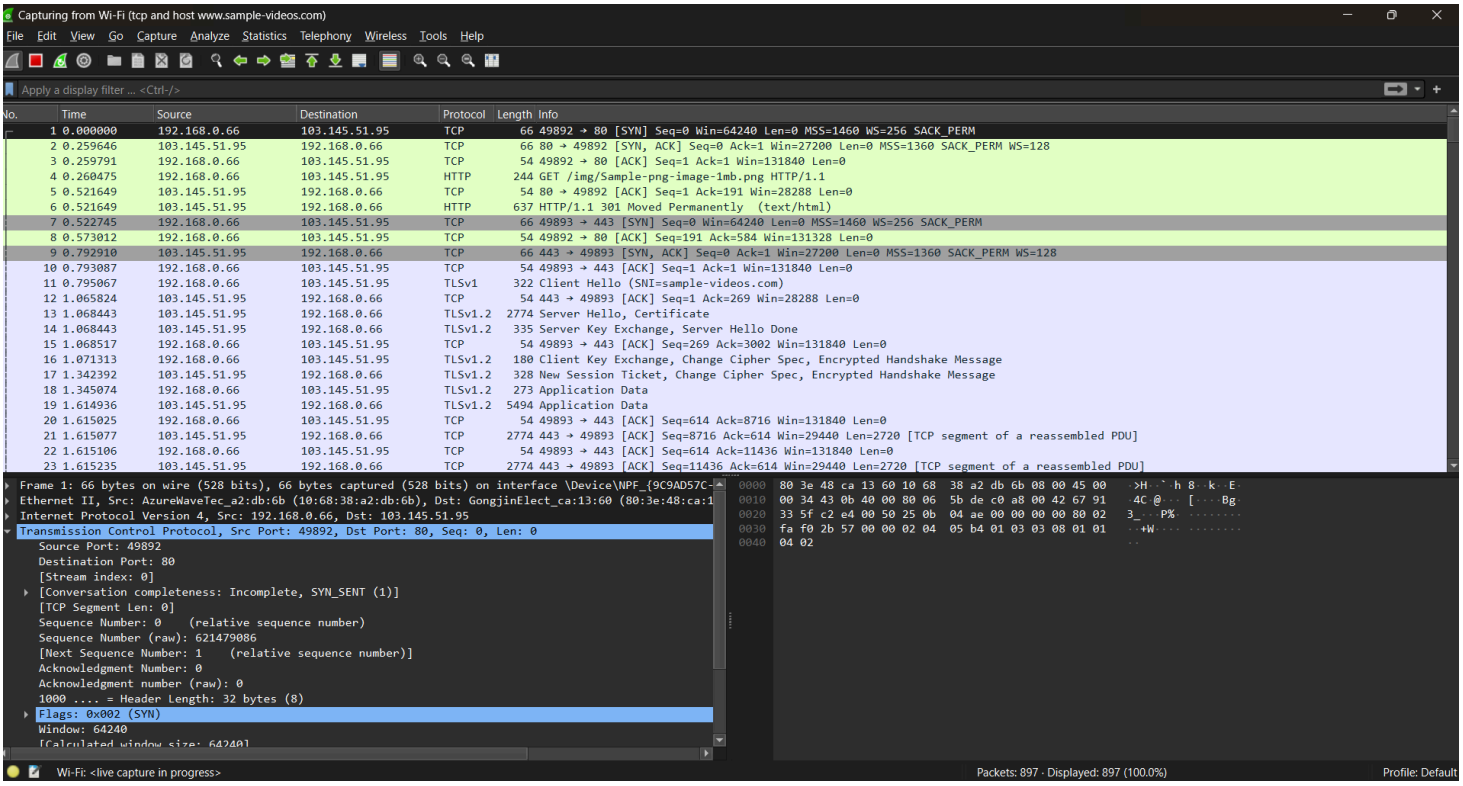
Em seguida, executamos o download de um recurso da web usando o terminal e o comando curl. Utilizamos o link 'https://sample-videos.com/img/Sample-png-image-1mb.png', que aponta para uma imagem PNG de 1 MB. A figura abaixo mostra o comando sendo utilizado no

terminal.



d) Para de Captura e Resultados

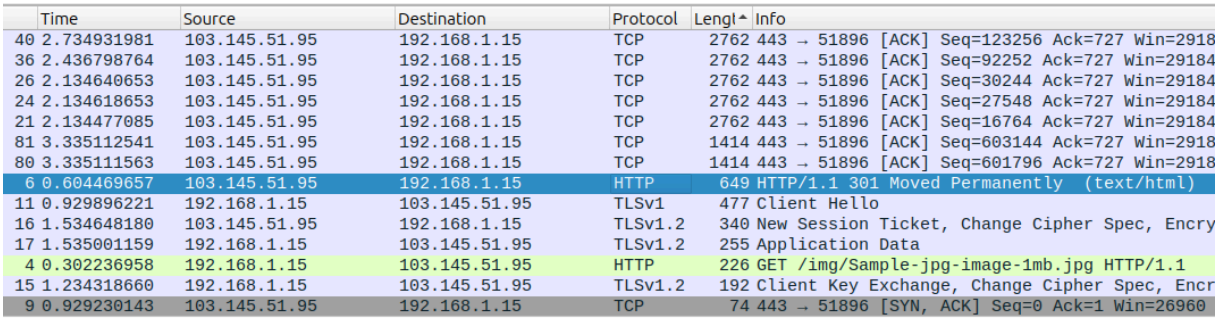
Após a conclusão do download do recurso da web, interrompemos a captura de tráfego no Wireshark para cessar a gravação de pacotes. Procedemos então à análise dos resultados da captura de tráfego no Wireshark. Verificamos se os pacotes capturados correspondiam ao tráfego TCP entre o nosso computador e o host www.sample-videos.com. Examinamos os detalhes dos pacotes TCP capturados, incluindo os cabeçalhos TCP e os dados transmitidos. A figura a seguir ilustra o tráfego capturado no Wireshark



Etapa 2 - Inspecione o rastreamento

1) **Selecionar um pacote longo no meio do traço**

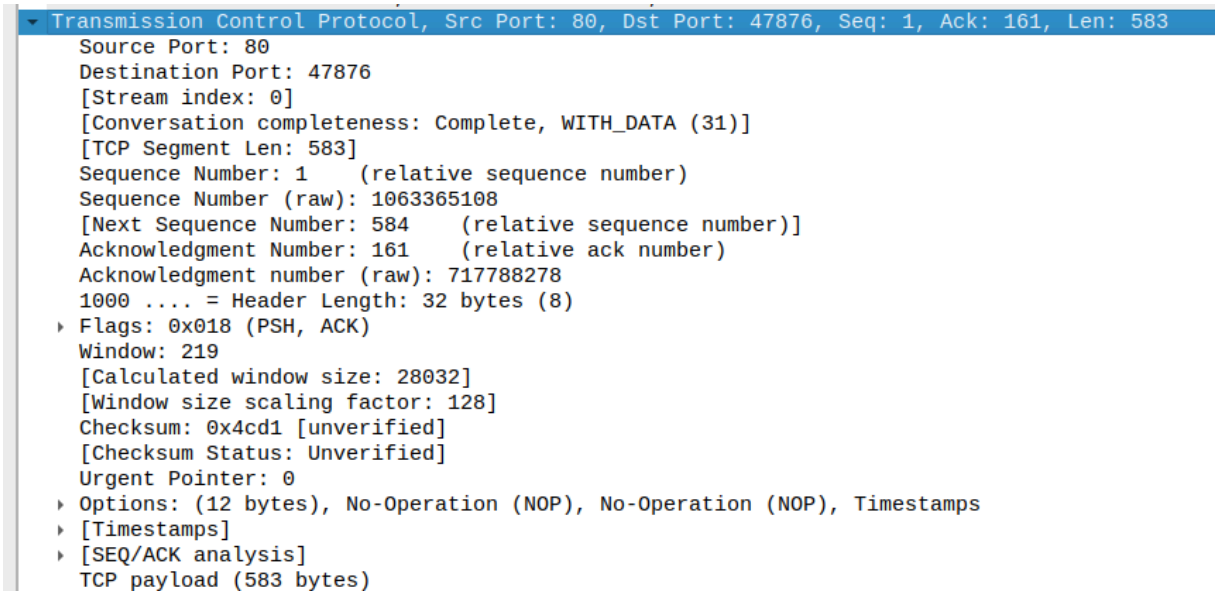
Abrimos o arquivo de captura no Wireshark. No painel superior, que lista os pacotes capturados, procuramos por um pacote longo localizado no meio do traço que tinha o protocolo listado como TCP. Ao encontrar, clicamos este pacote para selecioná-lo.



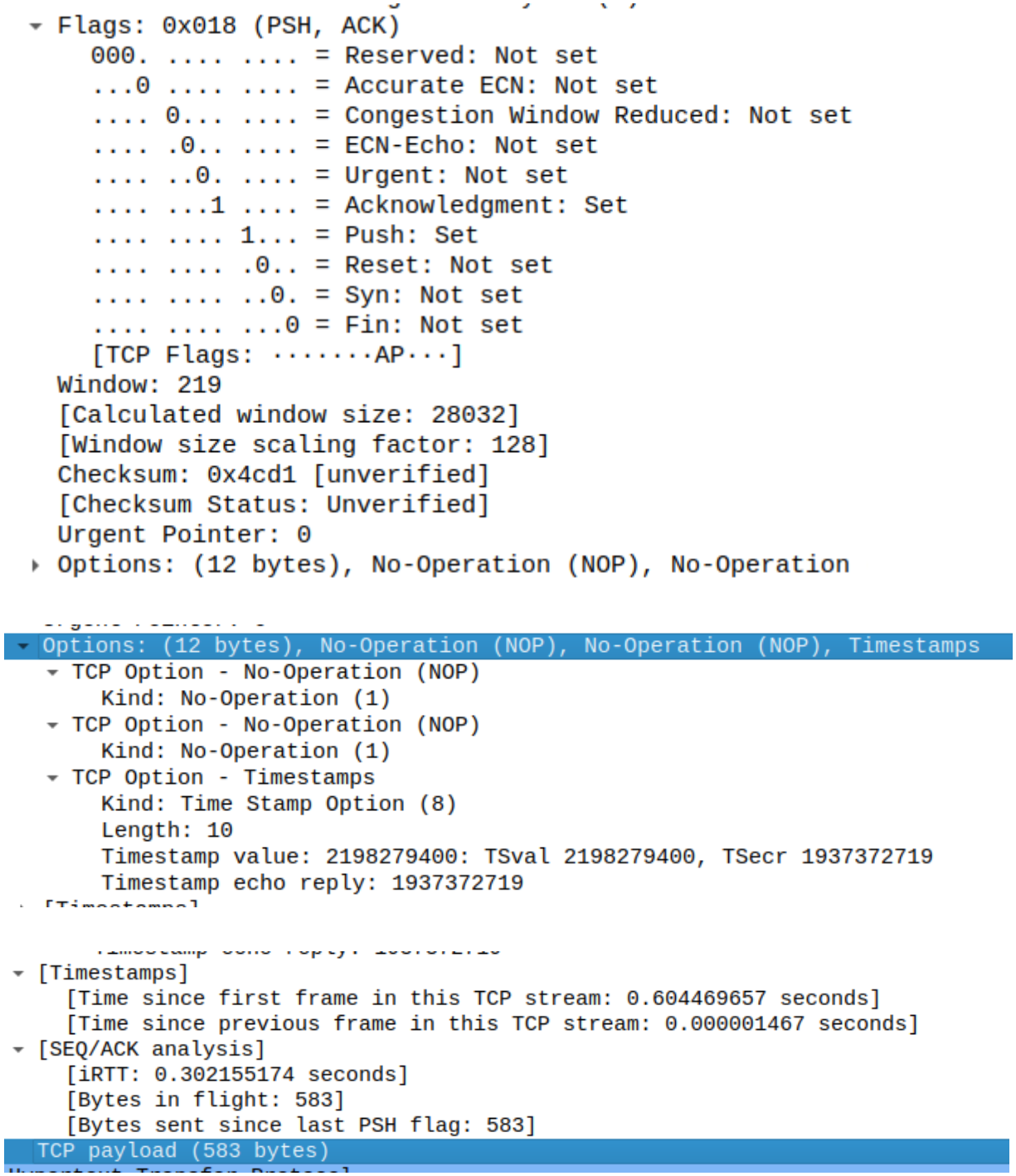
	Time	Source	Destination	Protocol	Lengt	Info
40	2.734931981	103.145.51.95	192.168.1.15	TCP	2762	443 → 51896 [ACK] Seq=123256 Ack=727 Win=2918
36	2.436798764	103.145.51.95	192.168.1.15	TCP	2762	443 → 51896 [ACK] Seq=92252 Ack=727 Win=29184
26	2.134640653	103.145.51.95	192.168.1.15	TCP	2762	443 → 51896 [ACK] Seq=30244 Ack=727 Win=29184
24	2.134618653	103.145.51.95	192.168.1.15	TCP	2762	443 → 51896 [ACK] Seq=27548 Ack=727 Win=29184
21	2.134477085	103.145.51.95	192.168.1.15	TCP	2762	443 → 51896 [ACK] Seq=16764 Ack=727 Win=29184
81	3.335112541	103.145.51.95	192.168.1.15	TCP	1414	443 → 51896 [ACK] Seq=603144 Ack=727 Win=2918
80	3.335111563	103.145.51.95	192.168.1.15	TCP	1414	443 → 51896 [ACK] Seq=601796 Ack=727 Win=2918
6	0.604469657	103.145.51.95	192.168.1.15	HTTP	649	HTTP/1.1 301 Moved Permanently (text/html)
11	0.929896221	192.168.1.15	103.145.51.95	TLSv1	477	Client Hello
16	1.534648180	103.145.51.95	192.168.1.15	TLSv1.2	340	New Session Ticket, Change Cipher Spec, Encry
17	1.535001159	192.168.1.15	103.145.51.95	TLSv1.2	255	Application Data
4	0.302236958	192.168.1.15	103.145.51.95	HTTP	226	GET /img/Sample-jpg-image-1mb.jpg HTTP/1.1
15	1.234318660	192.168.1.15	103.145.51.95	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encr
9	0.929230143	103.145.51.95	192.168.1.15	TCP	74	443 → 51896 [SYN, ACK] Seq=0 Ack=1 Win=26960

2) Expandir a seção do protocolo TCP

No painel do meio, que mostra os detalhes do pacote, foi localizada a seção do protocolo TCP. A seção foi expandida clicando nela para visualizar mais informações.



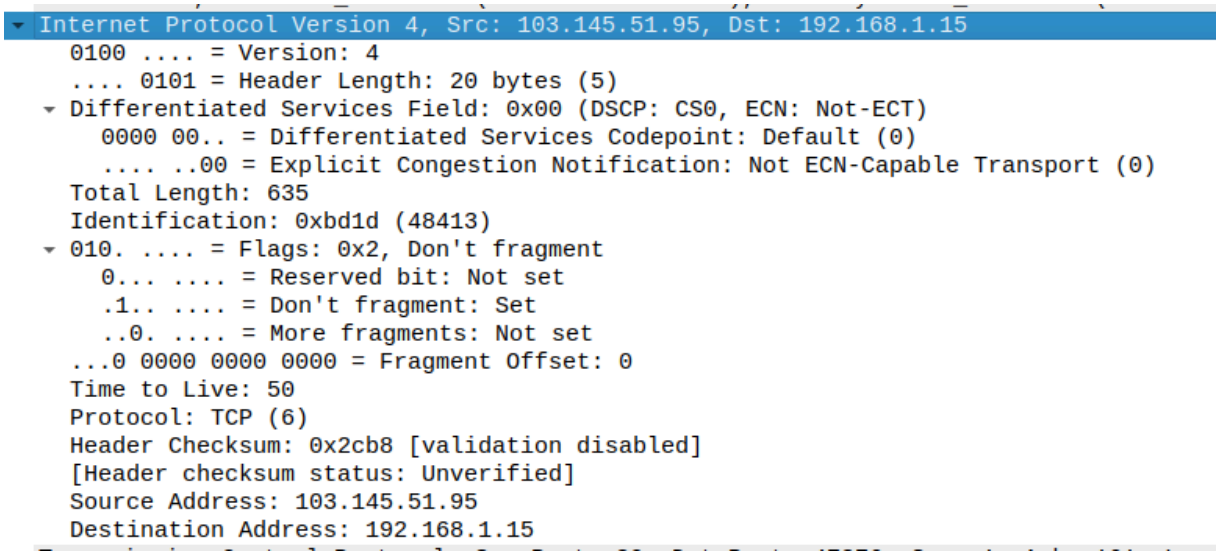
```
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 47876, Seq: 1, Ack: 161, Len: 583
    Source Port: 80
    Destination Port: 47876
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 583]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1063365108
    [Next Sequence Number: 584    (relative sequence number)]
    Acknowledgment Number: 161    (relative ack number)
    Acknowledgment number (raw): 717788278
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 219
    [Calculated window size: 28032]
    [Window size scaling factor: 128]
    Checksum: 0x4cd1 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (583 bytes)
```



3) **Examinar camadas de protocolo**

Foi iniciada a inspeção dos campos do TCP. Primeiramente, foram observadas as portas de origem e destino. A porta de origem corresponde ao número da porta do servidor que enviou o pacote, porta 80 para um servidor web, e a porta de destino é a porta no computador receptor do pacote. Em seguida, foi verificado o número de sequência, que indica a posição no fluxo de bytes do primeiro byte do payload do pacote. Também foi observado o campo de reconhecimento (ACK), que indica a última posição recebida no fluxo de bytes reverso. Após isso, foi verificado o comprimento do cabeçalho, que informa o comprimento do cabeçalho TCP. O campo de flags foi inspecionado, contendo múltiplos bits que indicam o tipo de segmento

TCP. Este campo foi expandido para visualizar os possíveis flags, como SYN, ACK, FIN, etc. Além disso, foi observado o checksum, utilizado para detectar erros de transmissão. Se presente, o campo de opções foi inspecionado, podendo conter várias opções, sendo este campo expandido para exploração das opções disponíveis. Finalmente, se presente, foi inspecionado o payload TCP, contendo os bytes que estão sendo transportados. Assim, foi concluída a análise do pacote TCP selecionado.



Etapa 3 - Estrutura do Segmento TCP

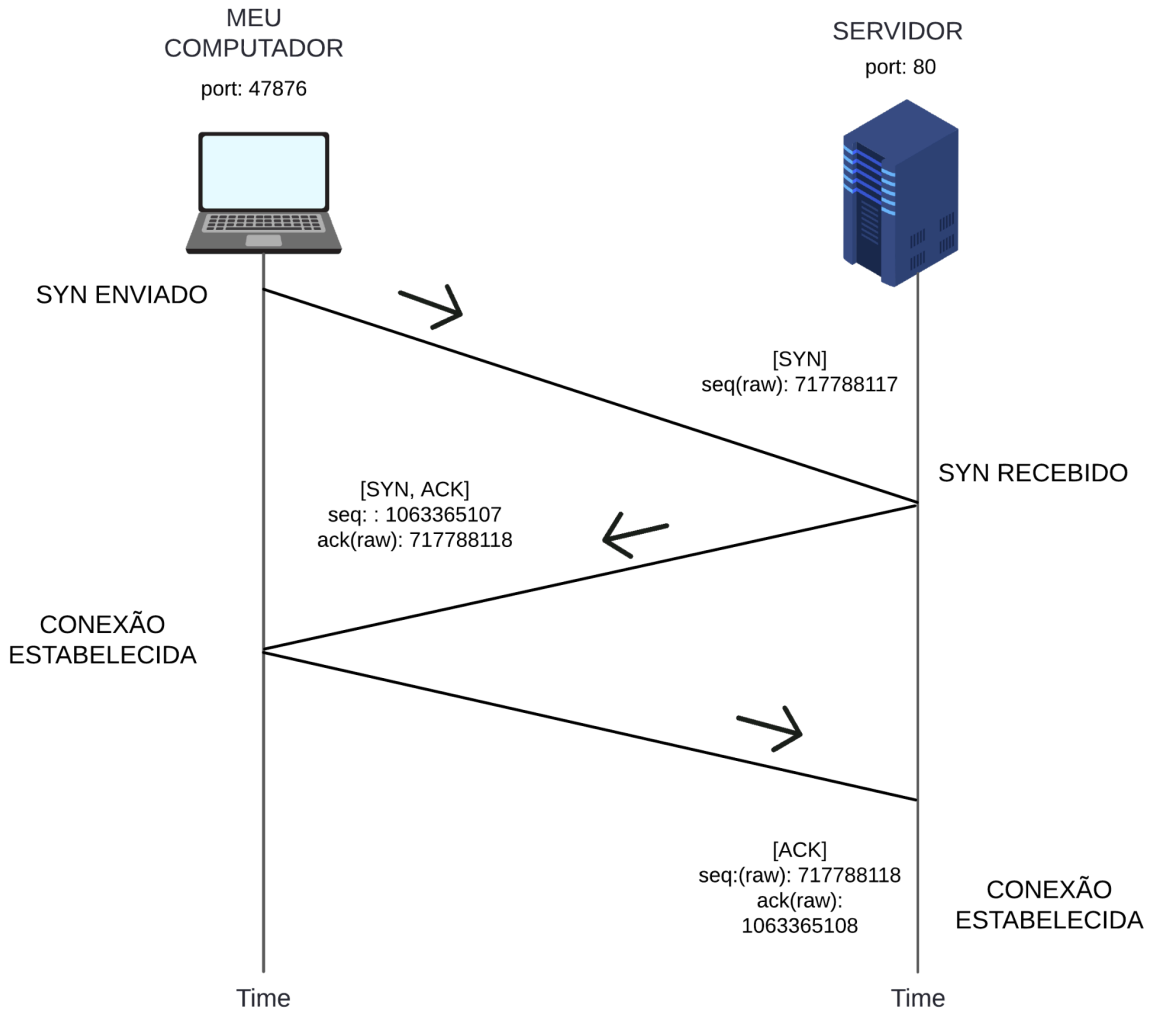
A tabela abaixo descreve os campos de um segmento TCP, conforme observado no Wireshark, incluindo a posição e o tamanho de cada campo em bytes. A porta de origem do segmento TCP é indicada pelo campo “Source Port”, que neste caso é a porta 80, a porta padrão para servidores web. O campo “Destination Port” indica a porta de destino no computador receptor, que é a porta 47876. O número de sequência relativo é indicado pelo campo “Sequence Number”, que mostra a posição no fluxo de bytes do primeiro byte do payload do pacote. Há também o número de sequência bruto, que representa a posição no fluxo de bytes em um formato não relativo. O campo “Next Sequence Number” indica o próximo número de sequência esperado, em termos relativos.

O número de reconhecimento relativo é indicado pelo campo “Acknowledgment Number”, mostrando a última posição recebida no fluxo de bytes reverso. Há também o número de reconhecimento bruto, que representa a última posição recebida em um formato não relativo. O campo “Window” especifica o tamanho da janela, que é a quantidade de dados que o receptor está disposto a aceitar. O campo “Flags” contém os bits de flags que indicam o tipo de segmento TCP. Neste caso, os bits PSH (Push) e ACK (Acknowledgment) estão definidos. O campo “Checksum” é utilizado para detectar erros de transmissão. No caso, o valor é 0x4cd1, mas ainda não foi verificado. O campo “Urgent Pointer” indica se há dados urgentes que precisam ser processados imediatamente. Neste segmento, o valor é 0, indicando que não há dados urgentes. O comprimento do cabeçalho TCP é de 32 bytes, conforme indicado pelo campo “Header Length”. O campo “Options” contém opções adicionais, com um comprimento total de 12 bytes. Inclui duas operações de No-Operation (NOP) e Carimbos de Tempo (Timestamps).

<table>
<tr><td colspan="2">Source Port: 80 (2bytes)</td><td colspan="2">Destination Port: 47876 (2bytes)</td></tr>
<tr><td colspan="4">Sequence Number: 1 (relative sequence number) (4bytes)
Sequence Number (raw): 1063365108 (4bytes)
[Next Sequence Number: 584 (relative sequence number)]</td></tr>
<tr><td colspan="4">Acknowledgment Number: 161 (relative ack number) (4bytes)
Acknowledgment number (raw): 717788278 (4bytes)</td></tr>
<tr><td>Window: 219 (2bytes)</td><td>Flags: 0x018 (PSH, ACK) (2bytes)</td><td>Checksum: 0x4cd1 [unverified] (2bytes)</td><td>Urgent Pointer: 0 (2bytes)</td></tr>
<tr><td colspan="2">1000 .... = Header Length: 32 bytes (8) (1byte)</td><td colspan="2">Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps</td></tr>
</table>

Etapa 4 - Estabelecimento/Encerramento da Conexão TCP

Estabelecendo conexão TCP:



1 - Opções TCP Transportadas nos Pacotes SYN

1. Maximum Segment Size (MSS)
    - Descrição: Informa o maior segmento que pode ser recebido.
    - Detalhes:
        - Kind: 2
        - Length: 4
        - MSS Value: 1460 bytes
2. SACK Permitted
    - Descrição: Indica suporte a reconhecimentos seletivos.
    - Detalhes:
        - Kind: 4
        - Length: 2
3. Timestamps
    - Descrição: Inclui carimbos de tempo para estimar o RTT.
    - Detalhes:
        - Kind: 8
        - Length: 10

        - Timestamp value: 1937372417
        - Timestamp echo reply: 0
4. No-Operation (NOP)
    - Descrição: Usado para formatação de opções.
    - Detalhes:
        - Kind: 1
5. Window Scale
    - Descrição: Indica a escala da janela de recepção, permitindo janelas maiores.
    - Detalhes:
        - Kind: 3
        - Length: 3
        - Shift count: 7
        - Multiplier: 128

Resumo das Opções TCP no Pacote SYN:

- Maximum Segment Size (MSS): 1460 bytes
- SACK Permitted: Suporte a reconhecimentos seletivos
- Timestamps: Inclui carimbos de tempo com valor de 1937372417 e resposta de eco 0
- No-Operation (NOP): Usado para formatação
- Window Scale: Multiplicador de janela de 128 (Shift count: 7)

2 - Opções TCP Transportadas nos Pacotes SYN-ACK

1. Maximum Segment Size (MSS)
    - Descrição: Informa o maior segmento que pode ser recebido.
    - Detalhes:
        - Kind: 2
        - Length: 4
        - MSS Value: 1360 bytes
2. SACK Permitted
    - Descrição: Indica suporte a reconhecimentos seletivos.
    - Detalhes:
        - Kind: 4
        - Length: 2
3. Timestamps
    - Descrição: Inclui carimbos de tempo para estimar o RTT.
    - Detalhes:
        - Kind: 8
        - Length: 10
        - Timestamp value: 2198279098
        - Timestamp echo reply: 1937372417
4. No-Operation (NOP)

        - Descrição: Usado para formatação de opções.
        - Detalhes:
            - Kind: 1
5. Window Scale
    - Descrição: Indica a escala da janela de recepção, permitindo janelas maiores.
    - Detalhes:
        - Kind: 3
        - Length: 3
        - Shift count: 7
        - Multiplier: 128

Informações Adicionais:

- Timestamps:
    - Time since first frame in this TCP stream: 0.302105516 seconds
    - Time since previous frame in this TCP stream: 0.302105516 seconds
- SEQ/ACK Analysis:
    - This is an ACK to the segment in frame: 1
    - The RTT to ACK the segment was: 0.302105516 seconds
    - iRTT: 0.302155174 seconds

Resumo das Opções TCP no Pacote SYN-ACK:

- Maximum Segment Size (MSS): 1360 bytes
- SACK Permitted: Suporte a reconhecimentos seletivos
- Timestamps: Inclui carimbos de tempo com valor de 2198279098 e resposta de eco 1937372417
- No-Operation (NOP): Usado para formatação
- Window Scale: Multiplicador de janela de 128 (Shift count: 7)

3 - Opções TCP Transportadas no Último Pacote ACK

1. No-Operation (NOP)
    - Descrição: Usado para formatação de opções.
    - Detalhes:
        - Kind: 1
2. No-Operation (NOP)
    - Descrição: Usado para formatação de opções.
    - Detalhes:
        - Kind: 1
3. Timestamps
    - Descrição: Inclui carimbos de tempo para estimar o RTT.
    - Detalhes:
        - Kind: 8

- Length: 10
- Timestamp value: 1937372719
- Timestamp echo reply: 2198279098

Informações Adicionais:

- Timestamps:
  - Time since first frame in this TCP stream: 0.302155174 seconds
  - Time since previous frame in this TCP stream: 0.000049658 seconds
- SEQ/ACK Analysis:
  - This is an ACK to the segment in frame: 2
  - The RTT to ACK the segment was: 0.000049658 seconds
  - iRTT: 0.302155174 seconds

Resumo das Opções TCP no Último Pacote ACK:

- No-Operation (NOP): Usado para formatação (duas instâncias)
- Timestamps: Inclui carimbos de tempo com valor de 1937372719 e resposta de eco 2198279098

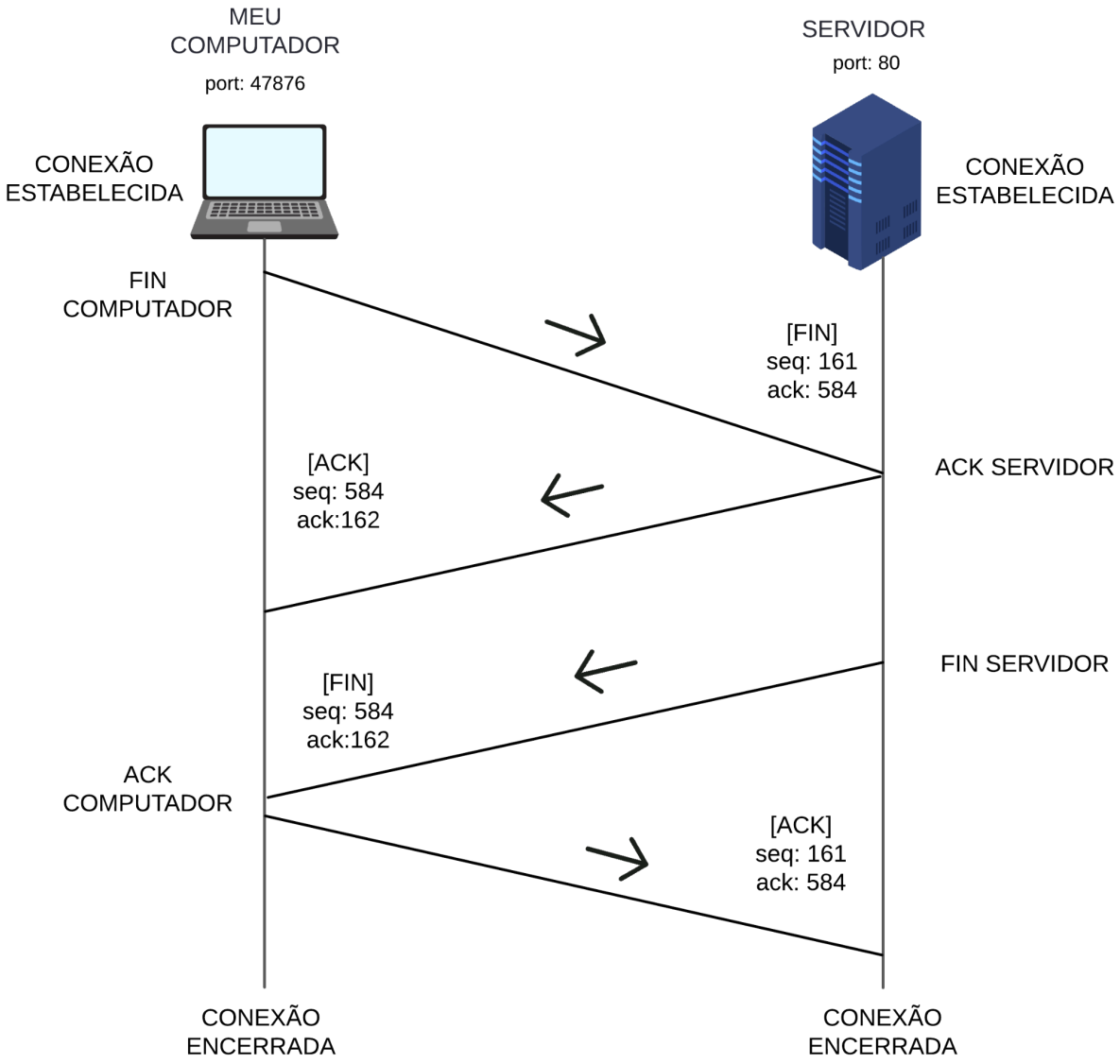
4 - Opções TCP Transportadas no Pacote FIN, ACK

1. No-Operation (NOP)
   - Descrição: Usado para formatação de opções.
   - Detalhes:
     - Kind: 1
2. No-Operation (NOP)
   - Descrição: Usado para formatação de opções.
   - Detalhes:
     - Kind: 1
3. Timestamps
   - Descrição: Inclui carimbos de tempo para estimar o RTT.
   - Detalhes:
     - Kind: 8
     - Length: 10
     - Timestamp value: 1937374254
     - Timestamp echo reply: 2198279400

Informações Adicionais:

- Timestamps:
  - Time since first frame in this TCP stream: 1.836581191 seconds
  - Time since previous frame in this TCP stream: 1.232060620 seconds

Encerrando conexão TCP:



4 - Primeiro Pacote FIN, ACK

Opções TCP Transportadas

1. No-Operation (NOP)
    - Descrição: Usado para formatação de opções.
    - Detalhes:
        - Kind: 1
2. No-Operation (NOP)
    - Descrição: Usado para formatação de opções.
    - Detalhes:
        - Kind: 1
3. Timestamps
    - Descrição: Inclui carimbos de tempo para estimar o RTT.
    - Detalhes:
        - Kind: 8
        - Length: 10
        - Timestamp value: 1937374254
        - Timestamp echo reply: 2198279400

Informações Adicionais:

- Timestamps:
    - Time since first frame in this TCP stream: 1.836581191 seconds
    - Time since previous frame in this TCP stream: 1.232060620 seconds

5 - Segundo Pacote FIN, ACK

Opções TCP Transportadas

1. No-Operation (NOP)
    - Descrição: Usado para formatação de opções.
    - Detalhes:
        - Kind: 1
2. No-Operation (NOP)
    - Descrição: Usado para formatação de opções.
    - Detalhes:
        - Kind: 1
3. Timestamps
    - Descrição: Inclui carimbos de tempo para estimar o RTT.
    - Detalhes:
        - Kind: 8
        - Length: 10
        - Timestamp value: 2198280934
        - Timestamp echo reply: 1937374254

Informações Adicionais:

- Timestamps:
    - Time since first frame in this TCP stream: 2.137638878 seconds
    - Time since previous frame in this TCP stream: 0.301057687 seconds
- SEQ/ACK Analysis:
    - This is an ACK to the segment in frame: 20
    - The RTT to ACK the segment was: 0.301057687 seconds
    - iRTT: 0.302155174 seconds

Resumo dos Pacotes FIN, ACK

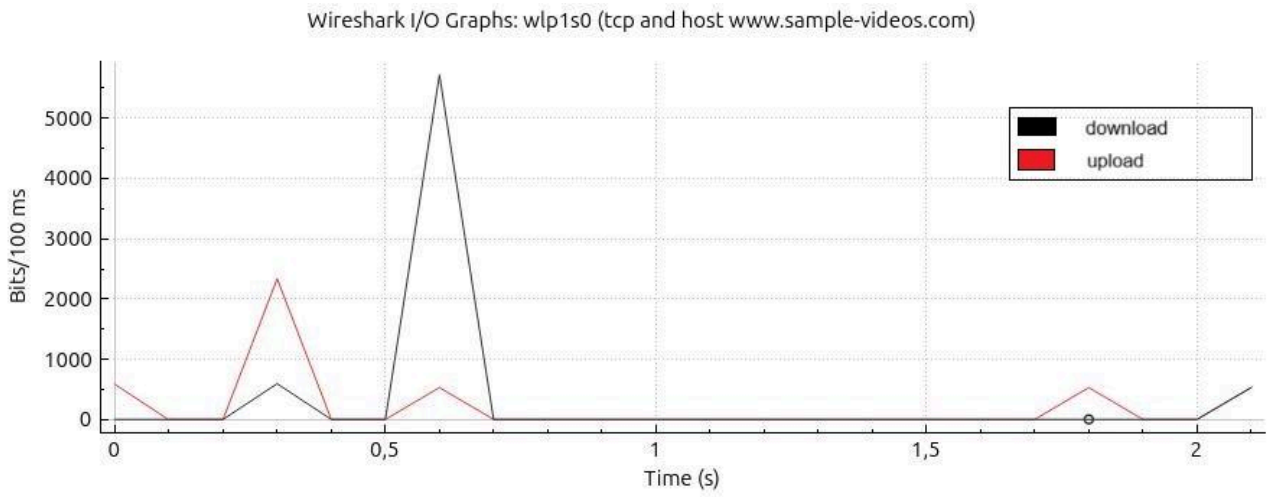
Primeiro Pacote FIN, ACK

- No-Operation (NOP): Usado para formatação (duas instâncias)
- Timestamps: Valor do carimbo de tempo: 1937374254, resposta de eco: 2198279400

Segundo Pacote FIN, ACK

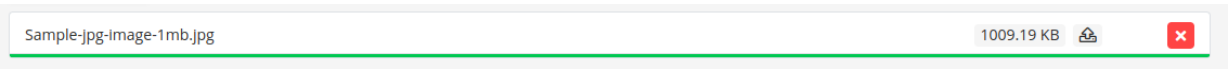
- No-Operation (NOP): Usado para formatação (duas instâncias)
- Timestamps: Valor do carimbo de tempo: 2198280934, resposta de eco: 1937374254

Etapa 5 - Transferência de Dados TCP



Address A	Port A	Address B	Port B	Bytes	Pacotes	Duration	Bits/s A → B
192.168.1.15	47876	103.145.51.95	80	0	0	2.137652218	0
192.168.1.15	51896	103.145.51.95	443	1047236	115	3.60830866	9968

- Pacotes: 115
- Bytes: 1.047.236
- ID do Fluxo: -1
- Total de Pacotes: 125
- Percentual Filtrado: 92%
- Pacotes de A para B: 57
- Bytes de A para B: 4.496
- Pacotes de B para A: 58
- Bytes de B para A: 1.042.740
- Tempo de Início Relativo: 0
- Duração: 4.238782114 segundos
- Taxa de Bits de A para B: 8.485 bits/s
- Taxa de Bits de B para A: 1.967.999 bits/s



Bytes=KB×1024
Então, para converter 1009.19 KB em bytes:
Bytes=1009.19×1024

Bytes=1009.19×1024

Bytes≈1,033,795.84
Bytes≈1,033,795.84

porcentagem dessa taxa de download = 1.042.740 / 1.033.795,84 ≈ 0,991 ou 99.1%

Frame	Tempo de Chegada (segundos)	Tamanho (bytes)
5	0.604468190	66
7	0.604520571	66
20	1.836581191	66
30	2.137638878	66
31	2.137652218	66

- ACK 1: 66 bytes
- ACK 2: 66 bytes
- ACK 3: 66 bytes
- ACK 4: 66 bytes
- ACK 5: 66 bytes

E os tempos de chegada são:

- Tempo de chegada do ACK 1: 0.604468190 segundos
- Tempo de chegada do ACK 2: 0.604520571 segundos
- Tempo de chegada do ACK 3: 1.836581191 segundos
- Tempo de chegada do ACK 4: 2.137638878 segundos
- Tempo de chegada do ACK 5: 2.137652218 segundos

Vamos calcular os valores:

1. Frequência média de chegada dos pacotes ACK:

$$\text{Frequência} = \frac{5}{2.137652218 - 0.604468190} \approx \frac{5}{1.533184028} \approx 3.26 \text{ ACKs/segundo}$$

2. Tamanho médio dos pacotes ACK:

$$\text{Tamanho médio} = \frac{66 + 66 + 66 + 66 + 66}{5} = \frac{330}{5} = 66 \text{ bytes}$$

3. Taxa de upload em pacotes/segundo: A frequência média de chegada dos pacotes ACK, que é aproximadamente 3.26 ACKs/segundo.

$$\text{Tempo Total Decorrido} = \text{Tempo de Chegada do Último ACK} - \text{Tempo de Chegada}$$

$$\text{Frequência Média} = \frac{\text{Número Total de Pacotes ACK}}{\text{Tempo Total Decorrido}}$$

$$\text{Frequência} = \frac{5}{2.137652218 - 0.604468190} \approx \frac{5}{1.533184028} \approx 3.26 \text{ ACKs/segundo}$$

4. Taxa de upload em bits/segundo:

$$\text{Taxa de upload (bits/segundo)} = 3.26 \text{ ACKs/segundo} \times 66 \text{ bytes/pacote} \times 8 \text{ bits}$$

Portanto, a taxa de dados aproximada na direção de upload devido aos pacotes ACK é de aproximadamente 3.26 pacotes/segundo e 1716.48 bits/segundo.