



Universidade Federal do Ceará

Disciplina: Redes de Computadores

Profa Atslands Rocha

Capturando o Way Handshake do TCP (Fonte: Kurose 6/7, colaboração parte 1: Prof<sup>a</sup> Nídia Campos)

Objetivo:

Analisar as mensagens de estabelecimento de conexão do protocolo TCP.

Entregáveis: Cada aluno deve fazer o upload no Google Classroom das respostas às questões e o arquivo .pcap desta prática (extensão do packet tracer).

### TAREFA 1 - Detectar o endereço IP do seu host

PASSO 1. Use o comando ipconfig para descobrir seu endereço IP da conexão local ou conexão sem fio.

```
C:\WINDOWS\system32>ipconfig

Configuração de IP do Windows

Adaptador Ethernet Ethernet:

    Estado da mídia. . . . . : mídia desconectada
    Sufixo DNS específico de conexão. . . . . :

Adaptador de Rede sem Fio Conexão Local* 1:

    Estado da mídia. . . . . : mídia desconectada
    Sufixo DNS específico de conexão. . . . . :

Adaptador de Rede sem Fio Conexão Local* 3:

    Estado da mídia. . . . . : mídia desconectada
    Sufixo DNS específico de conexão. . . . . :

Adaptador de Rede sem Fio Wi-Fi:

    Sufixo DNS específico de conexão. . . . . :
    Endereço IPv6 de link local . . . . . : fe80::30d0:36c1:7d59:46cc%22
    Endereço IPv4. . . . . : 192.168.0.104
    Máscara de Sub-rede . . . . . : 255.255.255.0
    Gateway Padrão. . . . . : 192.168.0.1

C:\WINDOWS\system32>
```

### TAREFA 2 - Detectar o endereço IP do servidor de destino

PASSO 1. Escolha um site web para você abrir no navegador.

PASSO 2. Execute o comando nslookup para descobrir o endereço IP do servidor web. O servidor deve ter apenas um endereço IP.

```
C:\ Prompt de Comando
C:\Users\neand>nslookup gaia.cs.umass.edu
Servidor: UnKnown
Address: 192.168.0.1

Não é resposta autoritativa:
Nome: gaia.cs.umass.edu
Address: 128.119.245.12

C:\Users\neand>
```

### TAREFA 3 - Usar o navegador web para se estabelecer conexão TCP

PASSO 1 - Desabilite todas as interfaces de rede do seu host, exceto a interface de rede que possui o endereço IP registrado na Tarefa 1.

PASSO 2 - Configure o Wireshark para capturar mensagens.

PASSO 3 - No navegador web, abra o site escolhido.

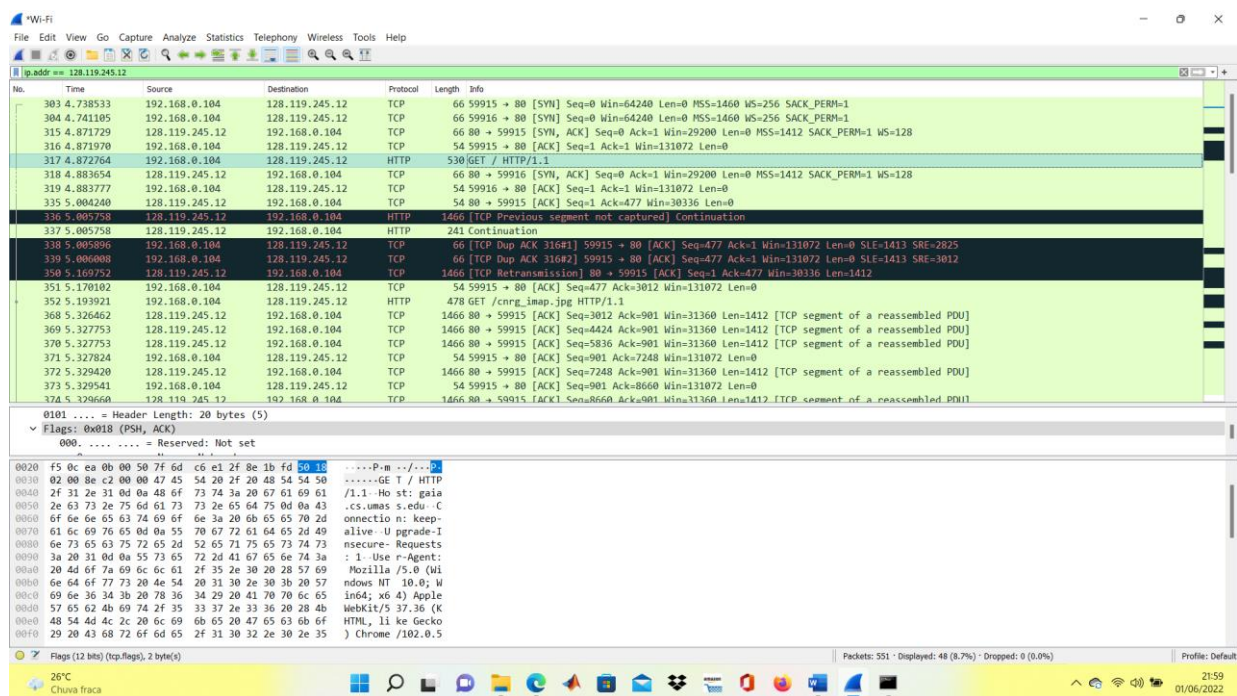
PASSO 4 - Pare o Wireshark e salve o trace da captura em um arquivo .pcap.

### TAREFA 4 - Analisar as três mensagens de estabelecimento de conexão do TCP

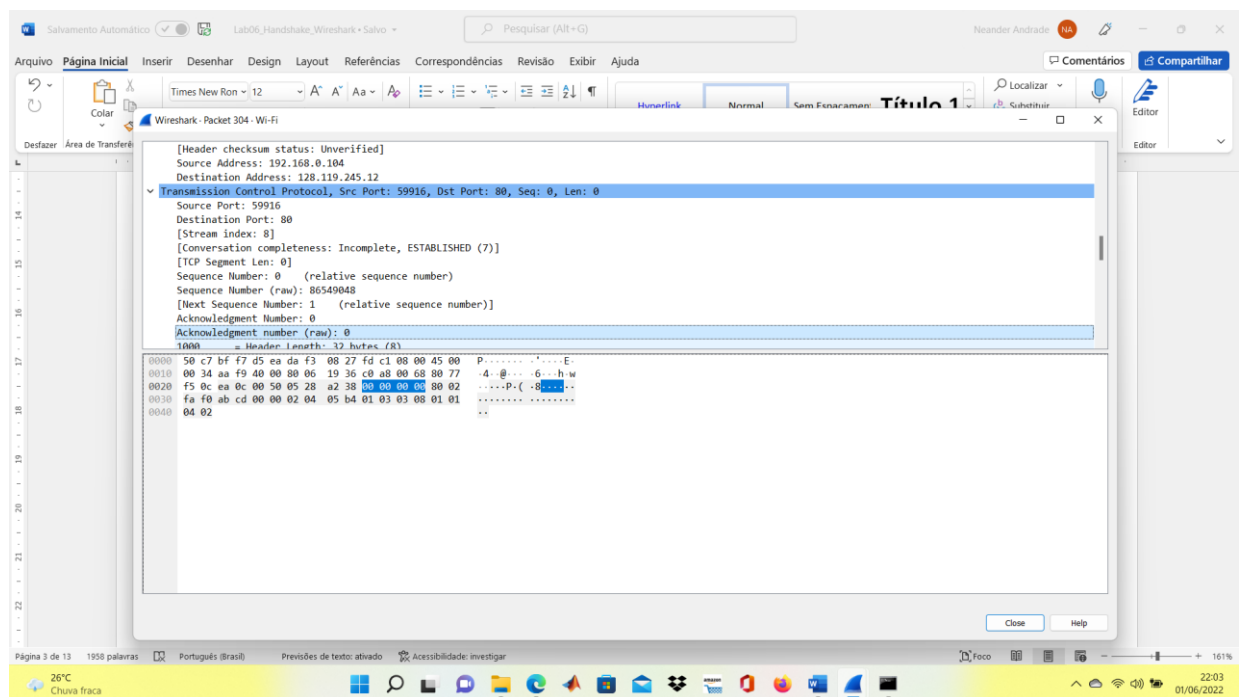
PASSO 1 - Na captura do Wireshark, filtre todas as mensagens que possui o IP do servidor web. Use o filtro `ip.addr== ENDEREÇO_IP_DO_SERVIDOR_WEB`

PASSO 2 - Localize a mensagem HTTP Request solicitando o site que você escolheu. As mensagens de apresentação do TCP (*Three-Way Handshake*) se encontram antes desse HTTP Request.

317 4.872764 192.168.0.104 128.119.245.12 HTTP 530 GET / HTTP/1.1



<<<<<<<<cole aqui as três capturas de telas>>>>>>>>>>>>>>>>>>>



The image shows a Wireshark packet capture window. The main pane displays a list of captured packets. Packet 315 is selected, and its details pane is open, showing the following information:

- Header checksum status:** Unverified
- Source Address:** 128.119.245.12
- Destination Address:** 192.168.0.104
- Transmission Control Protocol, Src Port: 80, Dst Port: 59915, Seq: 0, Ack: 1, Len: 0**
- Source Port:** 80
- Destination Port:** 59915
- [Stream index: 7]**
- [Conversation completeness: Complete, WITH\_DATA (31)]**
- [TCP Segment Len: 0]**
- Sequence Number:** 0 (relative sequence number)
- Sequence Number (raw):** 797842428
- [Next Sequence Number: 1 (relative sequence number)]**
- Acknowledgment Number:** 1 (relative ack number)
- Acknowledgment number (raw):** 2137900769
- 1000 ... = Header Length: 32 bytes (8)**

The packet bytes pane shows the raw data of the packet, which is a SYN packet with a sequence number of 0.

The image shows a Wireshark packet capture window. The main pane displays a list of captured packets. Packet 316 is selected, and its details pane is open, showing the following information:

- Source Address:** 192.168.0.104
- Destination Address:** 128.119.245.12
- Transmission Control Protocol, Src Port: 59915, Dst Port: 80, Seq: 1, Ack: 1, Len: 0**
- Source Port:** 59915
- Destination Port:** 80
- [Stream index: 7]**
- [Conversation completeness: Complete, WITH\_DATA (31)]**
- [TCP Segment Len: 0]**
- Sequence Number:** 1 (relative sequence number)
- Sequence Number (raw):** 2137900769
- [Next Sequence Number: 1 (relative sequence number)]**
- Acknowledgment Number:** 1 (relative ack number)
- Acknowledgment number (raw):** 797842429
- 0101 ... = Header Length: 20 bytes (5)**

The packet bytes pane shows the raw data of the packet, which is an ACK packet with a sequence number of 1 and an acknowledgment number of 1.

PASSO 4 - Preencha os campos abaixo usando as informações dos pacotes capturados.

Primeiro Segmento TCP	Segundo Segmento TCP	Terceiro Segmento TCP
Source port: 59915	Source port:59916	Source port: 80
Destination port: 80	Destination port: 80	Destination port:59915
Sequence Number: 0	Sequence Number: 0	Sequence Number: 0
ACK Number: 0	ACK Number: 0	ACK Number: 1
Marque com um X as flags que foram habilitadas:	Marque com um X as flags que foram habilitadas:	Marque com um X as flags que foram habilitadas:
<input type="checkbox"/> ACK	<input type="checkbox"/> ACK	<input checked="" type="checkbox"/> ACK
<input type="checkbox"/> Push	<input type="checkbox"/> Push	<input type="checkbox"/> Push
<input checked="" type="checkbox"/> Syn	<input checked="" type="checkbox"/> Syn	<input checked="" type="checkbox"/> Syn
<input type="checkbox"/> Fin	<input type="checkbox"/> Fin	<input type="checkbox"/> Fin

## 2 QUESTÃO

Vamos investigar o comportamento do protocolo TCP analisando um rastro dos segmentos TCP enviados e recebidos na transferência de um arquivo de 150KB (contendo o texto de Lewis Carrol's – Aventuras de Alice no País das Maravilhas) do seu computador para um servidor remoto.

### 1. Capturando uma transferência TCP em massa do seu computador para um servidor remoto

Antes de começar nossa exploração do TCP, precisamos usar o Wireshark para obter um rastreamento de pacotes da transferência TCP de um arquivo do computador para um servidor remoto. Você fará isso acessando uma página da Web que permitirá que você digite o nome de um arquivo armazenado em seu computador (que contém o texto ASCII de Alice no País das Maravilhas) e, em seguida, transfira o arquivo para um servidor Web usando o HTTP POST.

Estamos usando o método POST em vez do método GET, pois gostaríamos de transferir uma grande quantidade de dados do computador para outro computador.

Faça o seguinte:

- Inicie o seu navegador web. Vá para <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> e recupere uma cópia ASCII de Alice no País das Maravilhas. Armazene este arquivo em algum lugar no seu computador.
- Em seguida, vá para <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>.

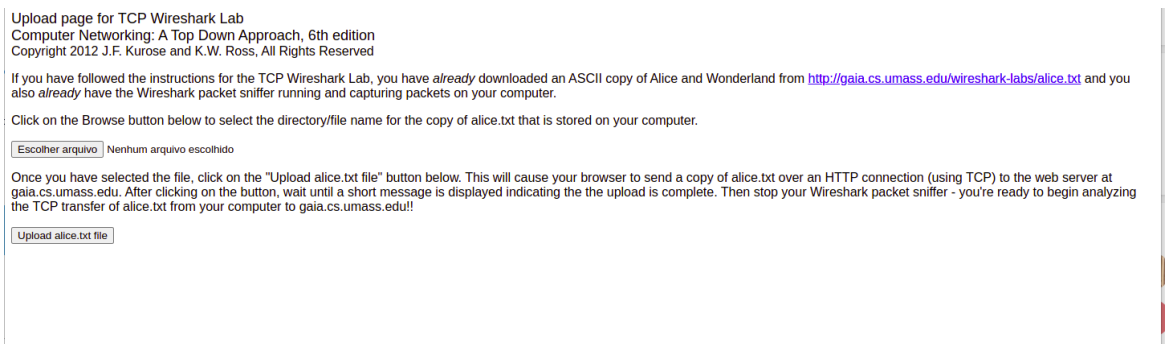


Figura 1: Página para fazer upload do arquivo alice.txt do seu computador para gaia.cs.umass.edu

- Na página, utilize o botão '*Escolher arquivo*' deste formulário para introduzir o nome do arquivo (nome completo do caminho) no computador que contém Alice no País das Maravilhas (ou fazê-lo manualmente). Não pressione o botão "Carregar arquivo alice.txt".
- Agora inicie o Wireshark e comece a captura de pacotes (Capture-> Start) e pressione OK na tela Wireshark Packet Capture Options (não precisaremos selecionar nenhuma opção aqui).
- Voltando ao seu navegador, pressione o botão "Upload alice.txt file" para carregar o arquivo para o servidor gaia.cs.umass.edu. Uma vez que o arquivo foi carregado, uma breve mensagem de parabéns será exibida na janela do navegador.
- Pare a captura de pacotes do Wireshark.

## 2. Um primeiro olhar para o trace capturado

Antes de analisar detalhadamente o comportamento da conexão TCP, vamos dar uma visão geral do rastreamento. Vamos começar examinando a mensagem HTTP POST que carregou o arquivo alice.txt para gaia.cs.umass.edu do seu computador. Encontre esse arquivo em seu rastreamento do Wireshark e expanda a mensagem HTTP para que possamos dar uma olhada na mensagem HTTP POST com mais cuidado. Sua tela do Wireshark deve se parecer com a Figura 2.

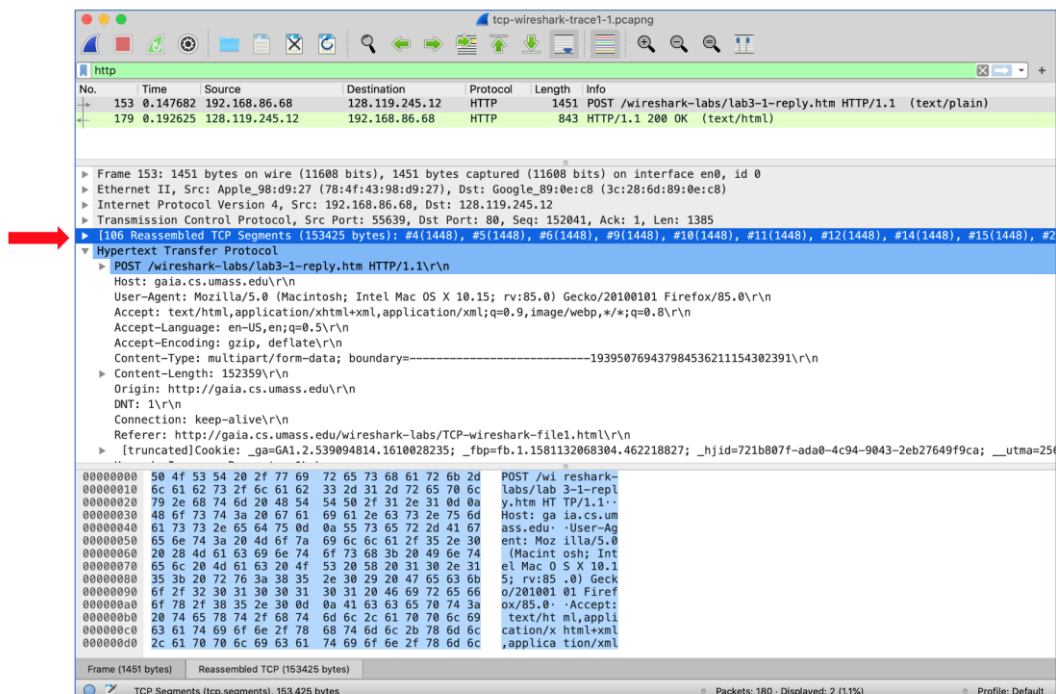
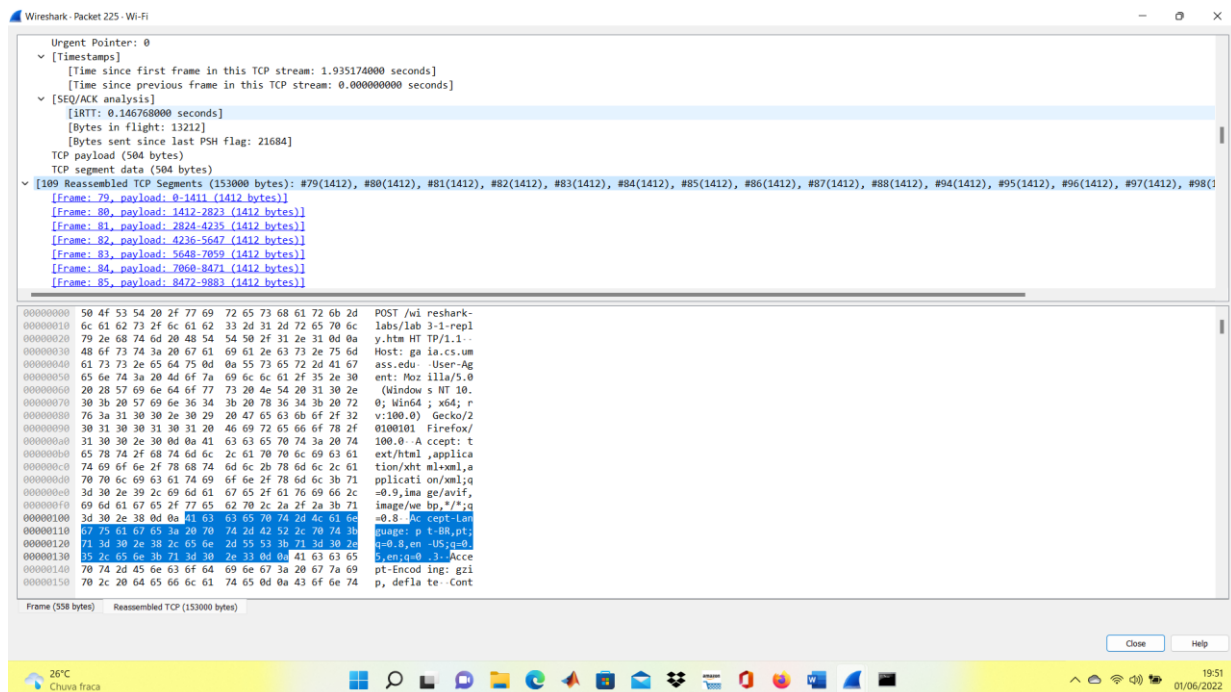


Figura 2: Expandindo a mensagem HTTP POST que carregou alice.txt do seu computador para gaia.cs.umass.edu

Há algumas coisas a serem observadas aqui:

O corpo da mensagem HTTP POST da camada de aplicativo contém o conteúdo do arquivo alice.txt, que é um arquivo grande com mais de 152 K bytes. OK – não é tão grande, mas vai ser muito grande para esta mensagem HTTP POST estar contida em apenas um segmento TCP!

De fato, conforme mostrado na janela do Wireshark na Figura 2, vemos que a mensagem HTTP POST foi espalhada por 106 segmentos TCP. Isso é mostrado onde a seta vermelha é colocada na Figura 3 [Aparte: o Wireshark não tem uma seta vermelha assim; nós o adicionamos à figura para ser útil ☺]. Se você olhar com mais cuidado, verá que o Wireshark também está sendo muito útil para você, informando que o primeiro segmento TCP que contém o início da mensagem POST é o pacote nº 4 no rastreamento específico para o exemplo da Figura 2, que é o rastreamento tcp-wireshark-trace1-1 observado na nota de rodapé 2. O segundo segmento TCP contendo a mensagem POST no pacote #5 no rastreamento e assim por diante.



Vamos agora “sujar as mãos” olhando alguns segmentos TCP.

Primeiro, filtre os pacotes exibidos na janela do Wireshark digitando “tcp” (minúsculas, sem aspas, e não se esqueça de pressionar o retorno após inserir!) Sua tela do Wireshark deve se parecer com a Figura 4. Na Figura 4, observamos o segmento TCP que tem seu bit SYN definido – esta é a primeira mensagem TCP no handshake de três vias que configura a conexão TCP para gaia.cs.umass.edu que eventualmente carregará a mensagem HTTP POST e o arquivo alice.txt. Também notamos o segmento SYNACK (a segunda etapa do handshake de três vias TCP), bem como o segmento TCP (pacote nº 4, conforme discutido acima) que carrega a mensagem POST e o início do arquivo alice.txt. Claro, se você estiver pegando seu próprio arquivo de rastreamento, os números dos pacotes serão diferentes, mas você deverá ver um comportamento semelhante ao mostrado nas Figuras 2 e 3.

TCP SYN      TCP SYNACK returned from gaia      TCP segment to gaia with first 1448 bytes of alice.txt

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.86.68	128.119.245.12	TCP	78	55639 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=725607531
2	0.022414	128.119.245.12	192.168.86.68	TCP	74	80 → 55639 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_
3	0.022505	192.168.86.68	128.119.245.12	TCP	66	55639 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=725607531 TS
4	0.024047	192.168.86.68	128.119.245.12	TCP	1514	55639 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=1448 TSval=725607532

[Next sequence number: 1 (relative sequence number)]  
 Acknowledgment number: 0  
 Acknowledgment number (raw): 0  
 1011 .... = Header Length: 44 bytes (11)  
 ▶ **Flags: 0x002 (SYN)**  
 Window size value: 65535  
 [Calculated window size: 65535]  
 Checksum: 0xa1e4 [unverified]  
 [Checksum Status: Unverified]

0000 3c 28 6d 89 0e c8 78 4f 43 98 d9 27 08 00 45 00 <(m...x0 C...E  
 0010 00 40 00 00 00 40 00 ae 47 c0 a8 56 44 80 77 .@...@...G...VD.w  
 0020 f5 0c d9 57 00 50 fc 86 22 e3 00 00 00 b0 02 ...W.P...  
 0030 ff ff a1 e4 00 00 02 04 05 b4 01 03 03 06 01 01 ...+?..U...  
 0040 08 0a 2b 3f e4 55 00 00 00 00 04 02 00 00

Figura 2: Segmentos TCP envolvidos no envio da mensagem HTTP POST (incluindo o arquivo alice.txt) para gaia.cs.umass.edu

No.	Time	Source	Destination	Protocol	Length	Info
67	12.663949	149.154.174.100	192.168.0.104	TLSv1.2	170	Application Data
68	12.716170	192.168.0.104	149.154.174.100	TCP	54	58291 → 443 [ACK] Seq=1389 Ack=945 Win=512 Len=0
71	13.341815	192.168.0.104	128.119.245.12	TCP	66	58450 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
72	13.488391	128.119.245.12	192.168.0.104	TCP	66	80 → 58450 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM=1 WS=128

▼ Frame 71: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{F8473590-02D6-40FC-9BCA-AA25233183}, id 0  
 Interface id: 0 (\Device\NPF\_{F8473590-02D6-40FC-9BCA-AA25233183})  
 Interface name: \Device\NPF\_{F8473590-02D6-40FC-9BCA-AA25233183}  
 Interface description: Wi-Fi  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Jun 1, 2022 19:34:59.825955000 Hora oficial do Brasil  
 [Time shift for this packet: 0.000000000 seconds]  
 Epoch Time: 1654122099.825955000 seconds  
 [Time delta from previous captured frame: 0.000030000 seconds]  
 [Time delta from previous displayed frame: 0.625645000 seconds]  
 [Time since reference or first frame: 13.341815000 seconds]  
 Frame Number: 71  
 Frame Length: 66 bytes (528 bits)

0000 50 c7 bf f7 d5 ea da f3 08 27 fd c1 00 00 45 00 P.....E  
 0010 00 34 a9 73 40 00 00 06 1a bc c0 a8 08 68 80 77 .4.s@...h.w  
 0020 f5 0c e4 52 00 50 98 5f e2 f5 00 00 00 80 02 ...R.P...  
 0030 fa f0 dd 92 00 00 02 04 05 b4 01 03 03 06 01 01 ...+?..U...  
 0040 04 02

Antes de analisar o comportamento da conexão TCP em detalhes, filtre os pacotes exibidos na janela do Wireshark digitando "tcp" na janela de especificação do filtro de exibição na parte superior da janela do Wireshark.

Pergunta: Você deve ver é uma série de mensagens TCP e HTTP entre seu computador e gaia.cs.umass.edu. Você deve ver o handshake inicial de três vias contendo uma mensagem SYN. Você deve ver uma mensagem HTTP POST. Além disso, o que há de diferente da primeira experiência acima?

Responda às seguintes perguntas:

1. Qual é o endereço IP e o número de porta TCP usado pelo computador cliente (origem) que está transferindo o arquivo para gaia.cs.umass.edu?

Internet Protocol Version 4, Src: 192.168.0.104, Dst: 128.119.245.12

2. Qual é o endereço IP de gaia.cs.umass.edu? Em que número de porta está enviando e recebendo segmentos TCP para essa conexão?

Transmission Control Protocol, Src Port: 58450, Dst Port: 80, Seq: 152497, Ack: 1, Len: 504

IP: 128.119.245.12, porta: 80

3. Qual é o endereço IP e o número da porta TCP usado pelo computador cliente (origem) para transferir o arquivo para gaia.cs.umass.edu?

IP: 192.168.0.104, porta: 58450

Nota: Uma vez que este laboratório é sobre TCP em vez de HTTP, vamos mudar a janela "listagem de pacotes capturados" do Wireshark para que mostre informações sobre os segmentos TCP contendo as mensagens HTTP, em vez de sobre as mensagens HTTP. Para que o Wireshark faça isso, selecione Analisar-> Protocolos habilitados. Em seguida, desmarque a caixa HTTP e selecione OK.

4. Qual é o número de sequência do segmento TCP SYN que é usado para iniciar a conexão TCP entre o computador cliente e gaia.cs.umass.edu? O que é no segmento que identifica o segmento como um segmento SYN?

Sequence Number: 0 (relative sequence number)

Há um campo dentre as informações do pacote com o seguinte dado: [SYN]

The image shows a Wireshark packet capture window. The top pane displays a list of packets. Packet 71 is highlighted, showing a TCP SYN packet from 192.168.0.104 to 128.119.245.12. The packet details pane shows the TCP header with the sequence number 0 and the SYN flag set. The packet bytes pane shows the raw data of the packet, including the Ethernet II header and the TCP header.

No.	Time	Source	Destination	Protocol	Length	Info
71	13.341815	192.168.0.104	128.119.245.12	TCP	66	58450 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

5. Qual é o número de sequência do segmento SYNACK enviado por gaia.cs.umass.edu para o computador cliente em resposta ao SYN? Qual é o valor do campo

Reconhecimento no segmento SYNACK? Como gaia.cs.umass.edu determinou esse valor? O que é no segmento que identifica o segmento como um segmento SYNACK?

O campo reconhecimento (**Acknowledgment**) tem valor 1.

Sequence Number: 0 (relative sequence number)

O segment é identificado pelas flags.

Flags: 0x012 (SYN, ACK)

000. .... = Reserved: Not set

...0 .... = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 .... = **Acknowledgment: Set**

.... .... 0... = Push: Not set

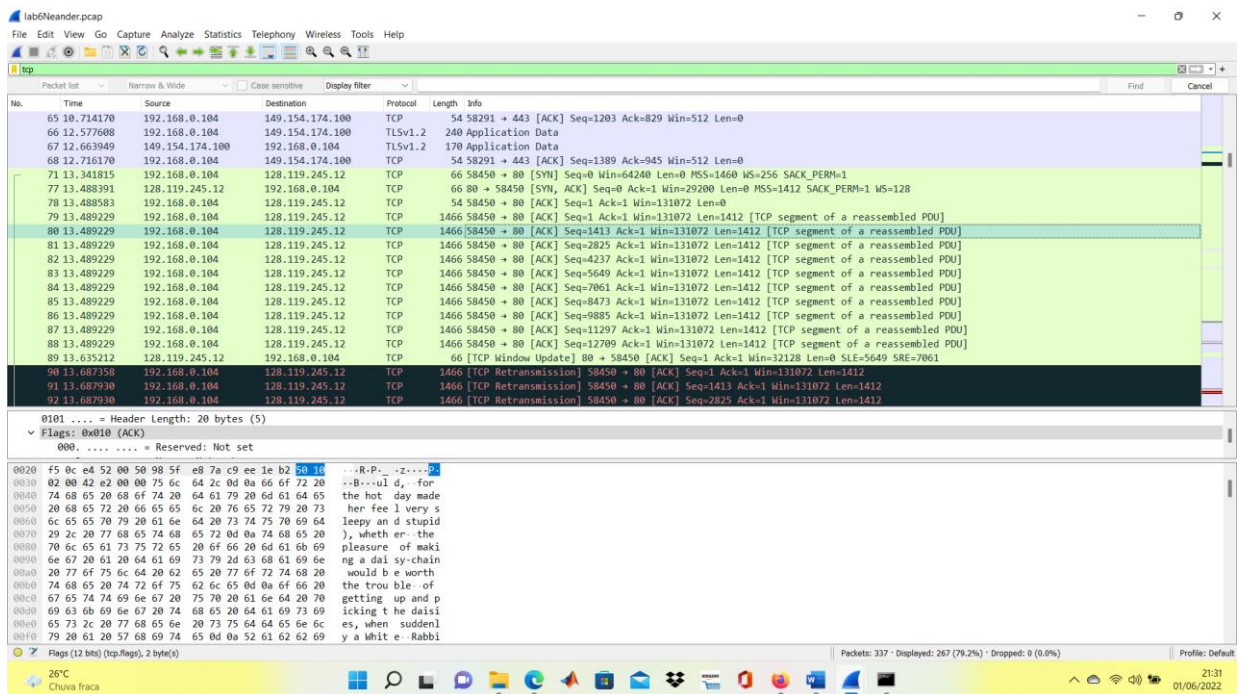
.... .... .0.. = Reset: Not set

.... .... ..1. = Syn: Set

6. Qual é o número de sequência do segmento TCP que contém o comando HTTP POST? Observe que, para encontrar o comando POST, você precisará digitar no campo de conteúdo de pacote na parte inferior da janela Wireshark, procurando um segmento com um "POST" dentro de seu campo DATA.

Sequence Number: 152497 (relative sequence number)

7. Considere o segmento TCP contendo o HTTP POST como o primeiro segmento na conexão TCP. Quais são os números de sequência dos primeiros seis segmentos na conexão TCP (incluindo o segmento que contém o HTTP POST)? Em que horário foi enviado cada segmento? Quando foi recebido o ACK para cada segmento?



- Sequence Number: 1 (relative sequence number) Arrival Time: Jun 1, 2022 19:34:59.973369000 Hora oficial do Brasil
- Sequence Number: 1413 (relative sequence number) Arrival Time: Jun 1, 2022 19:34:59.973369000 Hora oficial do Brasil
- Sequence Number: 2825 (relative sequence number) Arrival Time: Jun 1, 2022 19:34:59.973369000 Hora oficial do Brasil
- Sequence Number: 4237 (relative sequence number) Arrival Time: Jun 1, 2022 19:34:59.973369000 Hora oficial do Brasil
- Sequence Number: 5649 (relative sequence number) Arrival Time: Jun 1, 2022 19:34:59.973369000 Hora oficial do Brasil
- Sequence Number: 7061 (relative sequence number) Arrival Time: Jun 1, 2022 19:34:59.973369000 Hora oficial do Brasil

8. Qual é o comprimento de cada um dos seis primeiros segmentos TCP?

Todos tem Len=1412 bytes de comprimento.

9. Existem segmentos retransmitidos no ficheiro de rastreio? O que você verificou (no rastro) para responder a esta pergunta?

Há mensagens com campos [TCP Retransmission], supõe-se que esses pacotes foram reenviados.

The image shows a Wireshark packet capture of a TCP stream. The packet list on the left shows several packets, including a SYN, ACK, and multiple retransmissions of a segment. The packet details pane shows the selected packet's structure, including the TCP header and the application data. The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII view shows a message that appears to be a mix of English and Chinese characters, possibly a test message or a corrupted packet.

Nota: Veja sobre o RTT: Wireshark tem um recurso interessante que permite traçar o RTT para cada um dos segmentos TCP enviados. Selecione um segmento TCP na janela "lista de pacotes capturados" que está sendo enviada do cliente para o servidor `gaia.cs.umass.edu`. Em seguida, selecione: Statistics-> TCP Stream Graph-> Round Trip Time Graph.

**OBS: NÃO ESQUEÇA DE ENVIAR O LAB**

