Fora capturada um transferência de um arquivo de 150 Kbytes (alice.txt) para um servidor, feita através do protocolo HTTP. Os dados podem ser analisados abrindo o arquivo de captura gerado pelo software Wireshark.

Primeira análise dos pacotes capturados

Antes de analisar o comportamento da conexão TCP em detalhes, vamos fazer uma primeira análise dos pacotes capturados.
• No campo Filter digite http. Você verá uma mensagem HTTP POST indicando que o arquivo alice.txt será enviado para o servidor.
• No campo Filter digite tcp. O que você verá após aplicar o filtro é uma série de mensagens TCP e HTTP entre o seu computador e o servidor gaia.cs.umass.edu. Você pode observar os três pacotes iniciais de handshake contendo mensagens SYN e uma série de mensagens TCP enviadas do seu computador para gaia.cs.umass.edu. Você pode ver também os segmentos TCP ACK sendo retornados do servidor gaia.cs.umass.edu para o seu computador.

Responda as seguintes questões abaixo. Sempre que possível, anote e exporte os dados para um arquivo txt. Para exportar um pacote, use File->Print -> Selected packet only -> Packet summary line, digite o nome do arquivo de saída e selecione o mínimo de detalhe que você precisa para a resposta da questão.

1) Qual é o endereço IP e o número da porta usado pelo computador cliente para transferir o arquivo para gaia.cs.umass.edu? Provavelmente, o meio mais fácil para responder essa questão seja pela seleção da mensagem HTTP e então explorando os detalhes do pacote TCP usado para transportar essa mensagem.

Internet Protocol Version 4, Src: 192.168.0.8, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 43400, Dst Port: 80, Seq: 149145, Ack: 1, Len: 162

	Fonte	Destino
IP	192.168.0.8	128.119.245.12
PORT	43400	80

2) Qual é o endereço IP de gaia.cs.umass.edu? Em algum lugar da mensagem POST está indicado que o arquivo “alice.txt” será enviado para o servidor. Onde está essa informação?

gaia.cs.umass.edu : 128.119.245.12.

MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "--------------------------611061567139685546240914893 8"
[Type: multipart/form-data]
First boundary: ----------------------------611061567139685546240914893 8\r\n
Encapsulated multipart part: (text/plain)
Content-Disposition: form-data; name="file"; filename="alice.txt"\r\n
Content-Type: text/plain\r\n\r\n
Line-based text data: text/plain (3598 lines)
Last boundary: \r\n----------------------------611061567139685546240914893 8--\r\n

Básico sobre TCP

Responda as seguintes questões para os segmentos TCP. Para isso aplique o filtro tcp.

3) Qual é o número de sequência para o segmento TCP SYN usado para iniciar a conexão TCP entre o cliente e gaia.cs.umass.edu? Qual parâmetro do segmento permite identificar que ele é o do tipo SYN?

Transmission Control Protocol, Src Port: 43400, Dst Port: 80, Seq: 0, Len: 0
Source Port: 43400
Destination Port: 80
[Stream index: 3]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]

Acknowledgment number: 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....1. = Syn: Set
....0 = Fin: Not set
[TCP Flags: ··········S·]
Window size value: 29200
[Calculated window size: 29200]
Checksum: 0x9c36 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
[Timestamps]

O número de sequência real em hexadecimal é '0xAE412B05'. Se sabe que é um TCP SYN pelas flags.

4) Qual é o número de sequência do pacote SYNACK enviado por gaia.cs.umass.edu para o computador cliente em resposta ao SYN?

Transmission Control Protocol, Src Port: 80, Dst Port: 43400, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 43400
[Stream index: 3]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1010 .... = Header Length: 40 bytes (10)
Flags: 0x012 (SYN, ACK)
Window size value: 28960
[Calculated window size: 28960]
Checksum: 0xa9b0 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
[SEQ/ACK analysis]
[Timestamps]

O número de sequência real é '0x0A1F627C'.

5) Qual o número de sequência do segmento TCP contendo o comando HTTP POST? Este número de sequência está indicando os primeiros bytes a serem transferidos?

0XAE412B06. Ele indica que a transferência começou. Relativamente ele é o primeiro.

Transmission Control Protocol, Src Port: 43400, Dst Port: 80, Seq: 1, Ack: 1, Len: 1448
Source Port: 43400
Destination Port: 80
[Stream index: 3]
[TCP Segment Len: 1448]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1449 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 229
[Calculated window size: 29312]
[Window size scaling factor: 128]
Checksum: 0x0c45 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
[Timestamps]
TCP payload (1448 bytes)
[Reassembled PDU in frame: 3964]
TCP segment data (1448 bytes)

6) Transferência do arquivo:

a) Quais são os números de sequência para os primeiros 4 segmentos na conexão TCP?

0XAE412B06, 0xAE4130AE, 0XAE413656, 0XAE413BFE.

b) Qual é o comprimento de cada destes quatro primeiros segmentos TCP?

Transmission Control Protocol, Src Port: 43400, Dst Port: 80, Seq: 1, Ack: 1, Len: 1448
Source Port: 43400
Destination Port: 80
[Stream index: 3]
[TCP Segment Len: 1448]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1449 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 229
[Calculated window size: 29312]
[Window size scaling factor: 128]
Checksum: 0x0c45 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
[Timestamps]
TCP payload (1448 bytes)
[Reassembled PDU in frame: 3964]
TCP segment data (1448 bytes)

Cada um possui 1448 Bytes.

c) Em que instante de tempo esse segmento foi enviado?

1°: 1586960654.157864684s. 2°: 1586960654.157874554s.
3°: 1586960654.159477094s. 4°: 1586960654.159482707s

d) Quando foi recebido o ACK de cada pacote enviado ?

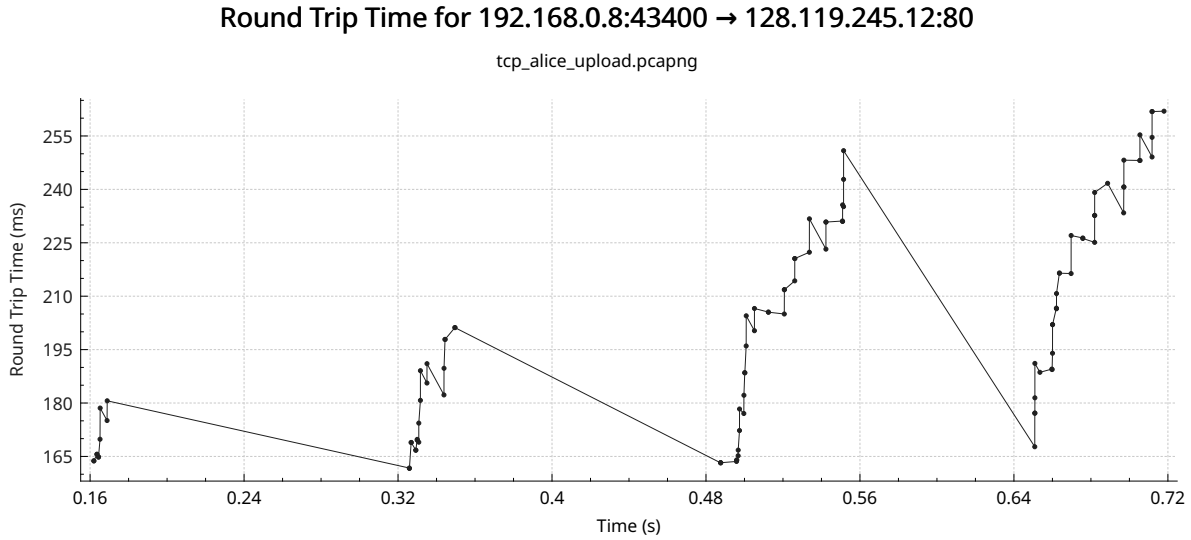
Só foi recebido o acknowledge do segundo pacote do arquivo
número de sequência: 2897 (relativo).

e) Dada a diferença entre quando cada segmento TCP foi enviado, e quando sua confirmação foi recebida, qual é o valor RTT (Round-trip time) para cada um dos quatro segmentos?

Foi recebido um ACK em 1586960654.321622985s do pacote de sequência 2897. Então o RTT = 1586960654.321622985 - 1586960654.159477094 = 0.162145891s. Então o RTT é de aproximadamente 160ms para os primeiros pacotes.

7) Para confirmar os RTTs calculados, selecione um pacote TCP na listagem da "janela de captura dos pacotes "que está sendo enviado a partir do cliente para o servidor gaia.cs.umass.edu. Em seguida, selecione: Statistics-> TCP Stream Graph-> Round Trip Time Graph.

Dê um printscreen da tela e cole o gráfico no espaço abaixo.



8) Qual é a quantidade mínima de espaço de buffer disponível anunciado pelos receptores no rastreamento inteiro (verificar através do campo *window* do header TCP)?

Transmission Control Protocol, Src Port: 80, Dst Port: 43400, Seq: 0, Ack: 1, Len: 0

Source Port: 80
Destination Port: 43400
[Stream index: 3]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1010 .... = Header Length: 40 bytes (10)

Flags: 0x012 (SYN, ACK)
Window size value: 28960
[Calculated window size: 28960]
Checksum: 0xa9b0 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
[SEQ/ACK analysis]
[Timestamps]

O mínimo anunciado pelo servidor foi de 28960 bytes.

9) Há algum pacote retransmitido no arquivo de rastreamento? O que você verificou no trace para responder a esta pergunta?

R: Houve um pedido de retransmissão mas não relacionado ao envio do arquivo alice.txt mas a uma outra comunicação. Em analyze→Expert Information, mostra dois warnings.

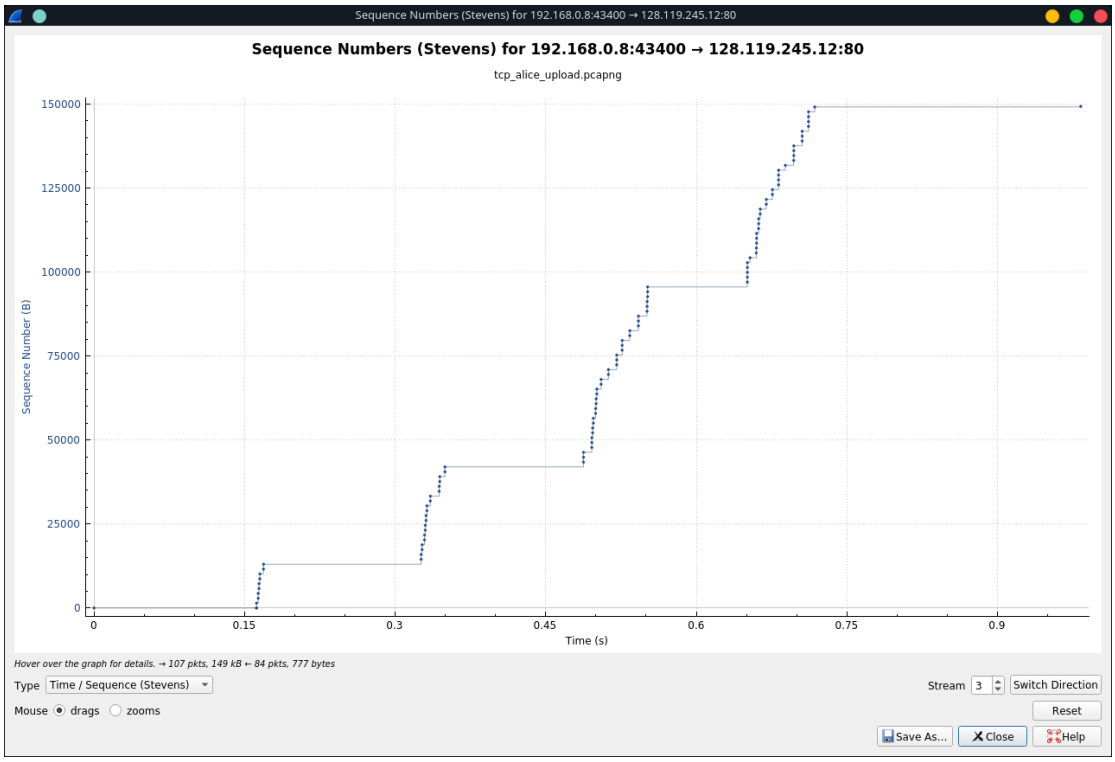
10) Qual a quantidade de dados que o receptor normalmente reconhece em um ACK?

R: Cerca de 3 a 5 pacotes por vez.

11) Qual é a taxa de transferência (throughput - bytes transferidos por unidade de tempo) para a conexão TCP? Explique como você calculou este valor.

R: 149k/0.983=152kbytes/s. Bytes transmitidos pelo tempo de envio.

12) Use a ferramenta Time-Sequence Graph (Stevens) para ver, em lote, a sequência de números de segmentos versus tempo enviados do cliente para o servidor gaia.cs.umass.edu. Você pode identificar onde a fase de partida lenta do TCP começa e termina, e onde evitar o congestionamento?



Slow start são as rajadas dos pacotes. A parte que evita o congestionamento é o intervalo que espera um acknowledge.

13) Agora vá em Statistics -> Conversations. Na janela que será aberta escolha a aba TCP. Essa janela mostra a quantidade de pacotes e de bytes trocados entre Address A e Address B. Observe os valores para os pacotes TCP e responda quantos pacotes foram enviados da sua máquina para o servidor http? E do servidor para sua máquina. Os valores são diferentes? Por quê?

Packets A → B: 107
Packets B → A: 084

Os valores são diferentes porque o servidor não confirmou todos os pacotes que recebeu.