AP1Q3 - Camada de aplicação HTTP usando Wireshark

Vinicius Gasparini

REC - BCC - UDESC - 2020

A página web utilizada durante os experimentos foi https://tiktok.com. Para tal captura, optou-se por realizar sem nenhum tipo de filtragem, os filtros portanto foram inseridos pós captura.

A Figura 1 destaca 4 regiões.

1. **Primeira região vermelha**: destaca o inicio da conexão caracterizada pelas primeiras chamadas TCP.
2. **Região verde**: destaca todos os pacotes de abertura de conexão. Estão inclusos nesta fazer o *Client Hello, Server Hello, Certificate* e *Handshake*.
3. **Região azul**: nesta área é onde ocorre a troca de pacotes entre o servidor e nosso computador por meio de pacotes TCP e TLS
4. **Segunda região vermelha**: por fim ocorre a fase de fechamento de conexão.

Adicionalmente, a figura destaca por meio da seta verde a camada de Internet onde, na primeira troca de certificados, a fonte é `tiktok.com(130.44.212.184)` com destino a minha máquina, `gaspanote.local(192.168.15.6)`. Já a seta vermelha destaca a assinatura deste certificado enviado.

Para obter esses dados filtrados seguiu-se o seguinte processo:

1. Realizado a captura sem nenhum tipo de filtro.
2. Conforme visto em aula, o protocolo HTTPS faz uso do protocolo TCP comumente na porta 443 bem como utiliza o protocolo TLS.
3. Para facilitar visualização, os nomes foram resolvidos durante o processo de captura, porém foi necessário verificar o ip da conexão ao site alvo. Para tal, buscou-se um "Client Hello" em cima dos pacotes filtrados no passo 2.
4. Por fim, para garantir coesão dos pacotes filtrados foi realizado intersecção com o meu ip local (obtido via `$hostname -I`).

O filtro final utilizado pare essa tarefa foi:

```
(ssl || tcp.port == 443) && (ip.addr == 130.44.212.184 && ip.addr == 192.168.15.6)
```

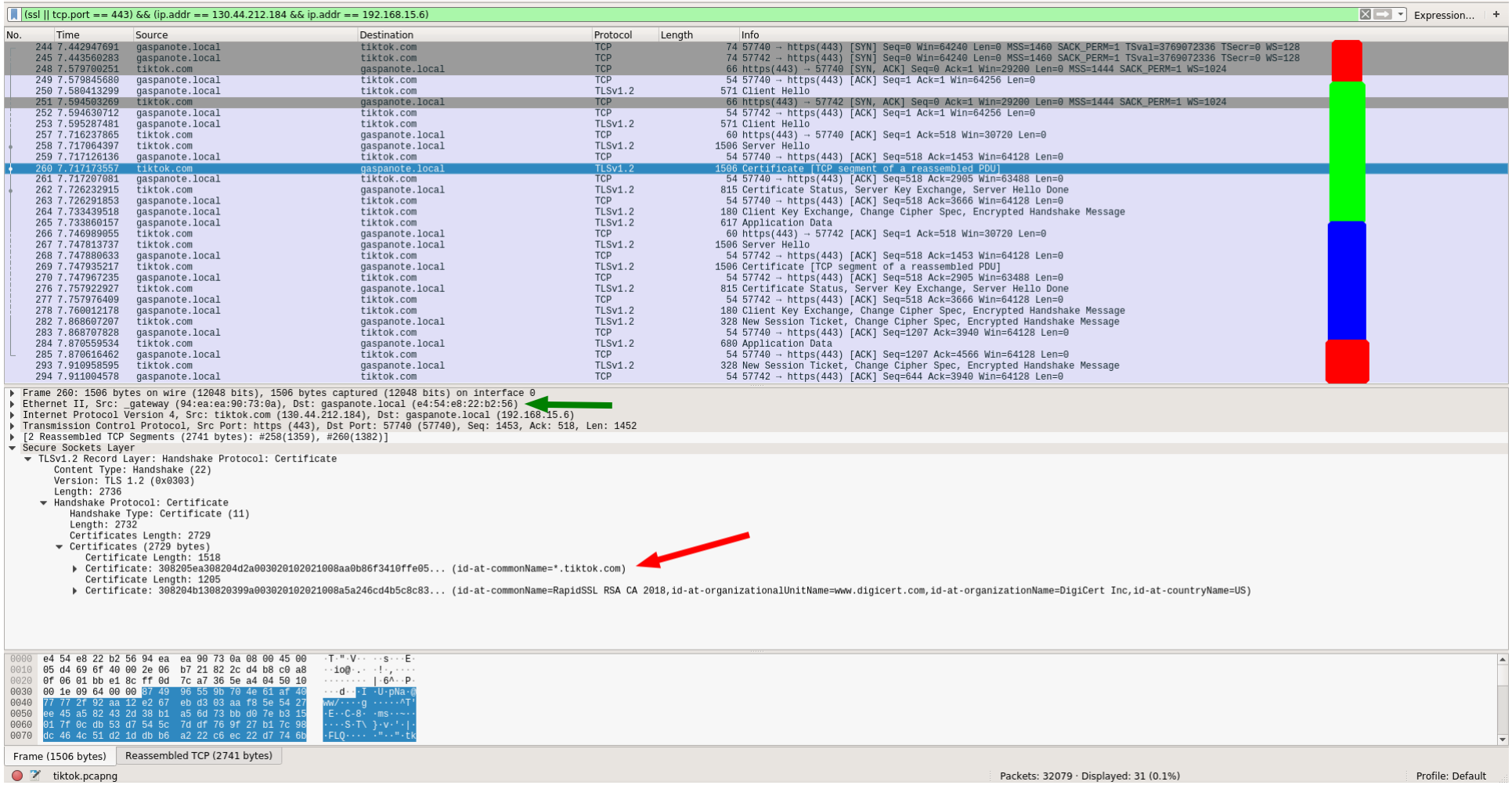

Figura 1: Interface do Wireshark com as seções destacadas