

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 início 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 para essa tarefa foi:

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

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

No.	Time	Source	Destination	Protocol	Length	Info
244	7.442947691	gaspanote.local	tiktok.com	TCP	74	57740 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3769072336 TSecr=0 WS=128
245	7.443568283	gaspanote.local	tiktok.com	TCP	74	57742 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3769072336 TSecr=0 WS=128
248	7.579700251	tiktok.com	gaspanote.local	TCP	66	https(443) → 57740 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1444 SACK_PERM=1 WS=1024
249	7.579845680	gaspanote.local	tiktok.com	TCP	54	57740 → https(443) [ACK] Seq=1 Ack=1 Win=64256 Len=0
250	7.580413299	gaspanote.local	tiktok.com	TLSv1.2	571	Client Hello
251	7.594503269	tiktok.com	gaspanote.local	TCP	66	https(443) → 57742 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1444 SACK_PERM=1 WS=1024
252	7.594630712	gaspanote.local	tiktok.com	TCP	54	57742 → https(443) [ACK] Seq=1 Ack=1 Win=64256 Len=0
253	7.595287481	gaspanote.local	tiktok.com	TLSv1.2	571	Client Hello
257	7.716237865	tiktok.com	gaspanote.local	TCP	60	https(443) → 57740 [ACK] Seq=1 Ack=518 Win=30720 Len=0
258	7.717064397	tiktok.com	gaspanote.local	TLSv1.2	1506	Server Hello
259	7.717126136	gaspanote.local	tiktok.com	TCP	54	57740 → https(443) [ACK] Seq=518 Ack=1453 Win=64128 Len=0
260	7.717126357	tiktok.com	gaspanote.local	TLSv1.2	1506	Certificate (TCP segment of a reassembled PDU)
261	7.717207081	gaspanote.local	tiktok.com	TCP	54	57740 → https(443) [ACK] Seq=518 Ack=2905 Win=63488 Len=0
262	7.726232915	tiktok.com	gaspanote.local	TLSv1.2	815	Certificate Status, Server Key Exchange, Server Hello Done
263	7.726291853	gaspanote.local	tiktok.com	TCP	54	57740 → https(443) [ACK] Seq=518 Ack=3666 Win=64128 Len=0
264	7.733439518	gaspanote.local	tiktok.com	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
265	7.733860157	gaspanote.local	tiktok.com	TLSv1.2	617	Application Data
266	7.746989055	tiktok.com	gaspanote.local	TCP	60	https(443) → 57742 [ACK] Seq=1 Ack=518 Win=30720 Len=0
267	7.747813737	tiktok.com	gaspanote.local	TLSv1.2	1506	Server Hello
268	7.747808636	gaspanote.local	tiktok.com	TCP	54	57742 → https(443) [ACK] Seq=518 Ack=1453 Win=64128 Len=0
269	7.747935217	tiktok.com	gaspanote.local	TLSv1.2	1506	Certificate (TCP segment of a reassembled PDU)
270	7.747967235	gaspanote.local	tiktok.com	TCP	54	57742 → https(443) [ACK] Seq=518 Ack=2905 Win=63488 Len=0
276	7.757922927	tiktok.com	gaspanote.local	TLSv1.2	815	Certificate Status, Server Key Exchange, Server Hello Done
277	7.757976409	gaspanote.local	tiktok.com	TCP	54	57742 → https(443) [ACK] Seq=518 Ack=3666 Win=64128 Len=0
278	7.760012178	gaspanote.local	tiktok.com	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
282	7.868607207	tiktok.com	gaspanote.local	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
283	7.868707828	gaspanote.local	tiktok.com	TCP	54	57740 → https(443) [ACK] Seq=1207 Ack=3940 Win=64128 Len=0
284	7.870559534	tiktok.com	gaspanote.local	TLSv1.2	680	Application Data
285	7.870616462	gaspanote.local	tiktok.com	TCP	54	57740 → https(443) [ACK] Seq=1207 Ack=4566 Win=64128 Len=0
293	7.910958595	tiktok.com	gaspanote.local	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
294	7.911004578	gaspanote.local	tiktok.com	TCP	54	57742 → https(443) [ACK] Seq=644 Ack=3940 Win=64128 Len=0

▶ Frame 260: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface 0
 ▶ Ethernet II, Src: gateway (94:ea:ea:90:73:0a), Dst: gaspanote.local (e4:54:e8:22:b2:56)
 ▶ Internet Protocol Version 4, Src: tiktok.com (130.44.212.184), Dst: gaspanote.local (192.168.15.6)
 ▶ Transmission Control Protocol, Src Port: https (443), Dst Port: 57740 (57740), Seq: 1453, Ack: 518, Len: 1452
 ▶ [2 Reassembled TCP Segments (2741 bytes): #258(1359), #260(1382)]
 ▼ Secure Sockets Layer
 ▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 2736
 ▼ Handshake Protocol: Certificate
 Handshake Type: Certificate (11)
 Length: 2732
 Certificates Length: 2729
 ▼ Certificates (2729 bytes)
 Certificate Length: 1518
 ▶ Certificate: 308205ea308204d2a003020102021008aa0b86f3410ffe05... (id-at-commonName=*tiktok.com)
 Certificate Length: 1205
 ▶ Certificate: 308204b130820399a003020102021008a5a246cd4b5c8c83... (id-at-commonName=RapidSSL RSA CA 2018,id-at-organizationalUnitName=www.digicert.com,id-at-organizationName=DigiCert Inc,id-at-countryName=US)

0000 e4 54 e8 22 b2 56 94 ea ea 90 73 0a 08 00 45 00 ...T..V...s..E..
 0010 05 d4 69 6f 40 00 2e 06 b7 21 82 2c d4 b8 c0 a8 ...100...!;...
 0020 0f 06 01 bb e1 8c ff 0d 7c a7 36 5e a4 04 50 10|6A..P..
 0030 00 1e 09 64 00 00 37 49 96 55 90 70 48 61 a7 45 ...d..I..U:PNa..
 0040 07 07 02 92 03 02 e2 67 eb d3 03 aa f8 5b 54 27g.....T..
 0050 ee 45 a5 82 43 2d 38 b1 a5 6d 73 bb d0 7e b3 15 ...-C-8-..ms....
 0060 91 7f 0c db 53 d7 54 5c 7d df 76 9f 27 b1 7c 98 ...S-T..-v-..t..
 0070 dc 46 4c 51 d2 1d db b6 a2 22 c6 ec 22 d7 74 6b ...FLQ....".-..-..k

Frame (1506 bytes) Reassembled TCP (2741 bytes)
 tiktok.pcapng Packets: 32079 · Displayed: 31 (0.1%) Profile: Default

Figura 1: Interface do Wireshark com as seções destacadas