

به نام خدا

محمد مهدی آقاجانی

۹۳۳۱۰۵۶

تمرین عملی اول

استاد : دکتر شهریاری

سؤال اول

پروتکل های مورد استفاده بیشتر , tcp , sslv2 , ssl می باشد

ip.addr == 149.154.165.120

No.

Time

Source

Destination

Protocol

Length

Info

2920

84.041816894

149.154.165.120

10.42.0.11

TCP

1294

[TCP segment of a reassembled PDU]

2921

84.042748058

149.154.165.120

10.42.0.11

TCP

1294

[TCP segment of a reassembled PDU]

2922

84.044687611

149.154.165.120

10.42.0.11

TCP

1294

[TCP segment of a reassembled PDU]

2923

84.045832578

149.154.165.120

10.42.0.11

TCP

1294

[TCP segment of a reassembled PDU]

2924

84.047501080

149.154.165.120

10.42.0.11

TCP

1294

[TCP segment of a reassembled PDU]

2925

84.048696867

149.154.165.120

10.42.0.11

TCP

1294

[TCP segment of a reassembled PDU]

2926

84.049879690

149.154.165.120

10.42.0.11

TCP

1294

[TCP segment of a reassembled PDU]

2927

84.051281374

149.154.165.120

10.42.0.11

TCP

1078

[TCP segment of a reassembled PDU]

2928

84.103580465

10.42.0.11

149.154.165.120

TCP

78

36456 → 443 [ACK] Seq=1986408388 Ack=3567806553 Win=770368 Len=0 TSval=9223083 TSecr=1494150038 S...

2929

84.103671770

10.42.0.11

149.154.165.120

TCP

78

36456 → 443 [ACK] Seq=1986408388 Ack=3567807781 Win=769152 Len=0 TSval=9223084 TSecr=1494150041 S...

2930

84.103876757

10.42.0.11

149.154.165.120

TCP

78

36456 → 443 [ACK] Seq=1986408388 Ack=3567806553 Win=770368 Len=0 TSval=9223084 TSecr=1494150038 S...

2931

84.104047084

10.42.0.11

149.154.165.120

TCP

78

[TCP Dup ACK 2930#1] 36456 → 443 [ACK] Seq=1986408388 Ack=3567806553 Win=770368 Len=0 TSval=9223084 TSecr=1494150041 S...

2932

84.104153015

10.42.0.11

149.154.165.120

TCP

78

[TCP Dup ACK 2930#2] 36456 → 443 [ACK] Seq=1986408388 Ack=3567806553 Win=770368 Len=0 TSval=9223084 TSecr=1494150041 S...

2933

84.104368773

10.42.0.11

149.154.165.120

TCP

78

36456 → 443 [ACK] Seq=1986408388 Ack=3567807781 Win=769152 Len=0 TSval=9223084 TSecr=1494150041 S...

2934

84.104473988

10.42.0.11

149.154.165.120

TCP

66

36456 → 443 [ACK] Seq=1986408388 Ack=3567849533 Win=729344 Len=0 TSval=9223084 TSecr=1494150041 S...

2935

84.117742271

10.42.0.11

149.154.165.120

TCP

66

36456 → 443 [ACK] Seq=1986408388 Ack=3567866509 Win=783808 Len=0 TSval=9223092 TSecr=1494150046

2936

84.188311935

10.42.0.11

149.154.165.120

TCP

235

[TCP segment of a reassembled PDU]

2937

84.222605907

149.154.165.120

10.42.0.11

TCP

1294

[TCP segment of a reassembled PDU]

2938

84.223603234

149.154.165.120

10.42.0.11

TCP

1294

[TCP segment of a reassembled PDU]

2939

84.224546517

149.154.165.120

10.42.0.11

TCP

1294

[TCP segment of a reassembled PDU]

2940

84.225776602

149.154.165.120

10.42.0.11

TCP

1294

[TCP segment of a reassembled PDU]

Fragment offset: 0

Time to live: 64

Protocol: TCP (6)

Header checksum: 0x6d6b [validation disabled]

[Header checksum status: Unverified]

Source: 10.42.0.11

Destination: 149.154.165.120

[Source GeoIP: Unknown]

[Destination GeoIP: United Kingdom, AS62041 Telegram Messenger LLP, 51.500000, -0.130000]

Transmission Control Protocol, Src Port: 36456, Dst Port: 443, Seq: 1986408388, Ack: 3567807781, Len: 0

0000

40 b8 9a 64 8c 23 bc 6e 64 6e 8b be 08 09 45 00

0..d.#.n dn....E.

0010

00 40 08 05 40 00 00 6d 6b 0a 2a 00 00 95 9a

.0..0.0. mk.*....

0020

15 78 8e 68 01 bb 76 6e 2f c4 d4 a8 6d 25 b0 10

.x.h..vf /...mk..

0030

2e f2 27 ee 00 00 01 01 08 0a 00 8c bb ac 59 0e

..f.....Y.....

0040

eb 99 01 01 05 0a d4 a8 71 f1 d4 a9 10 3e

.....Q.....

بسته های رد و بدل شده تماماً رمز شده می باشند.

یک نکته مشهود این می باشد که تلگرام چندین سرور مختلف دارد که در هر بار اتصال به یکی از آن ها متصل می شود

همچنین برای ارسال داده ها از پروتکل SSL استفاده میکند تا داده ها رمز شده باقی بمانند.

سؤال دوم

(بخش اول)

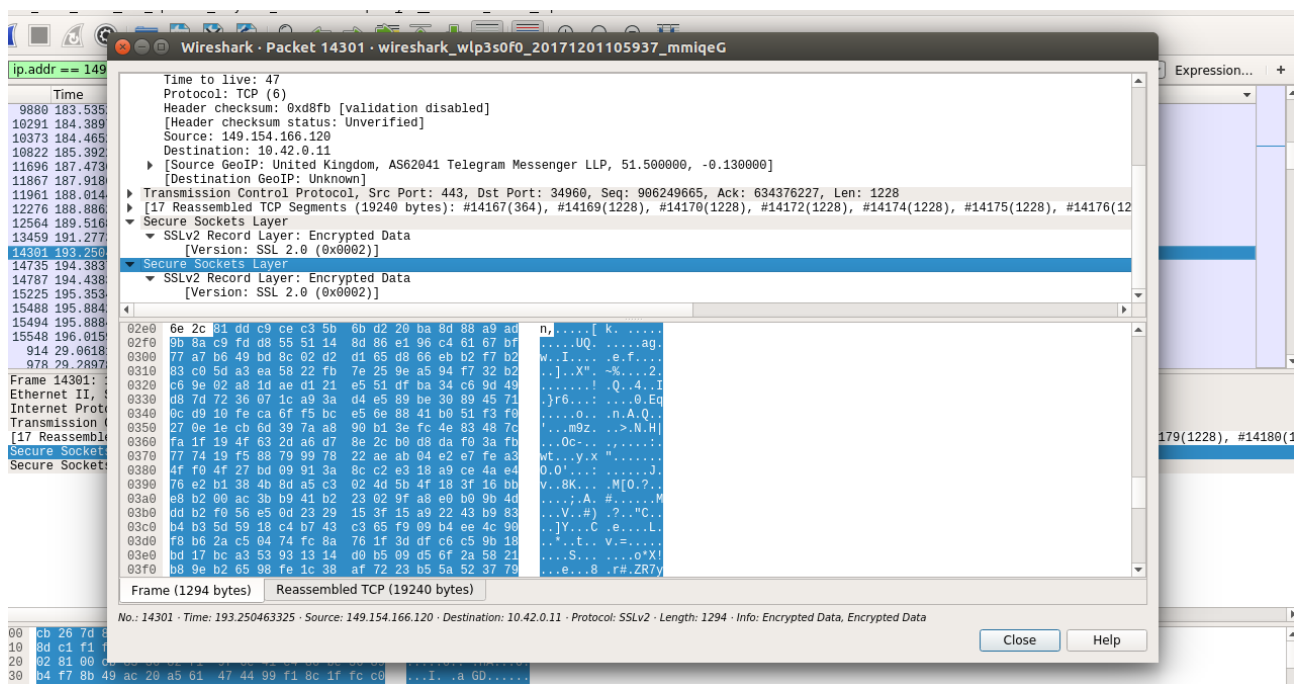
91.108.4.134

149.154.166.120

149.154.167.92

(بخش دوم)

ابتدا عملیات برقراری ارتباط را انجام میدهد سپس با استفاده از SSL داده‌ها را میفرستد که در شکل زیر قابل مشاهده است



ip.addr == 149.154.167.92																	
No.	Time	Source	Destination	Protocol	Length	Info											
22492	818.776179435	10.42.0.11	149.154.167.92	TCP	74	46800 → 443	[SYN]	Seq=3782716549 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=9695353 TSecr=0 W									
22617	822.057228849	10.42.0.11	149.154.167.92	TCP	66	46801 → 443	[ACK]	Seq=690354919 Ack=3032262106 Win=87616 Len=0 TSval=9695683 TSecr=1960103976									
22625	822.374163061	10.42.0.11	149.154.167.92	TCP	66	46801 → 443	[ACK]	Seq=690355161 Ack=3032262195 Win=87616 Len=0 TSval=9695715 TSecr=1960104054									
22626	822.376245762	10.42.0.11	149.154.167.92	TCP	66	46801 → 443	[ACK]	Seq=690355161 Ack=3032262284 Win=87616 Len=0 TSval=9695715 TSecr=1960104054									
22609	821.749591620	10.42.0.11	149.154.167.92	TCP	74	46801 → 443	[SYN]	Seq=690354918 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=9695682 TSecr=0 W									
21537	706.267190757	149.154.167.92	10.42.0.11	TCP	66	80 → 36337	[ACK]	Seq=673258626 Ack=3477987902 Win=28032 Len=0 TSval=1498954157 TSecr=9684882									
21790	711.672746637	149.154.167.92	10.42.0.11	TCP	66	80 → 36337	[ACK]	Seq=673258626 Ack=3477987991 Win=28032 Len=0 TSval=1498959563 TSecr=9684618									
21815	714.055727119	149.154.167.92	10.42.0.11	TCP	66	80 → 36337	[ACK]	Seq=673258626 Ack=3477988096 Win=28032 Len=0 TSval=1498961946 TSecr=9684860									
21825	714.159596588	149.154.167.92	10.42.0.11	TCP	66	80 → 36337	[ACK]	Seq=673258626 Ack=3477988185 Win=28032 Len=0 TSval=1498962050 TSecr=9684870									
21826	714.222876602	149.154.167.92	10.42.0.11	TCP	66	80 → 36337	[ACK]	Seq=673258626 Ack=3477988290 Win=28032 Len=0 TSval=1498962113 TSecr=9684877									
21828	714.258772340	149.154.167.92	10.42.0.11	TCP	66	80 → 36337	[ACK]	Seq=673258626 Ack=3477988395 Win=28032 Len=0 TSval=1498962149 TSecr=9684881									
21830	714.324198098	149.154.167.92	10.42.0.11	TCP	66	80 → 36337	[FIN, ACK]	Seq=673258626 Ack=3477988396 Win=28032 Len=0 TSval=1498962214 TSecr=9684881									
21528	706.016519683	149.154.167.92	10.42.0.11	TCP	74	80 → 36337	[SYN, ACK]	Seq=673258625 Ack=3477987749 Win=26960 Len=0 MSS=1360 SACK_PERM=1 TSval=									
21659	708.624062863	149.154.167.92	10.42.0.11	TCP	66	80 → 36338	[ACK]	Seq=1601220504 Ack=1798662234 Win=28032 Len=0 TSval=1498956514 TSecr=9684317									
22045	728.767738592	149.154.167.92	10.42.0.11	TCP	66	80 → 36338	[FIN, ACK]	Seq=1601220504 Ack=1798662235 Win=28032 Len=0 TSval=1498976657 TSecr=9684317									
21633	708.382643225	149.154.167.92	10.42.0.11	TCP	74	80 → 36338	[SYN, ACK]	Seq=1601220503 Ack=1798661992 Win=26960 Len=0 MSS=1360 SACK_PERM=1 TSva=									
20837	675.116242378	10.42.0.11	149.154.167.92	SSL	308	Continuation Data											
20851	675.424562006	149.154.167.92	10.42.0.11	SSL	244	Continuation Data											
21845	714.435159943	10.42.0.11	149.154.167.92	SSL	411	Continuation Data											
▶ Frame 20831: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0																	
▶ Ethernet II, Src: SonyMob1_6e:8b:be (bc:6e:64:6e:8b:be), Dst: HonHaiPr_64:8c:23 (40:b8:9a:64:8c:23)																	
▶ Internet Protocol Version 4, Src: 10.42.0.11, Dst: 149.154.167.92																	
0100 = Version: 4																	
... 0101 = Header Length: 20 bytes (5)																	
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)																	
Total Length: 60																	
Identification: 0x9d3f (40255)																	
▶ Flags: 0x02 (Don't Fragment)																	
Fragment offset: 0																	
Time to live: 64																	
Protocol: TCP (6)																	
Header checksum: 0x5651 [validation disabled]																	
[Header checksum status: Unverified]																	
Source: 10.42.0.11																	
Destination: 149.154.167.92																	
[Source GeoIP: Unknown]																	
▶ Destination GeoIP: United Kingdom, AS62041, Telegram Messenger LTD, 51.500000, 0.120000																	
0000	40	b8	9a	64	8c	23	bc	6e	64	6e	8b	be	08	00	45	00	@..d.#.n dn...E.
0010	00	3c	9d	3f	40	00	40	06	56	51	0a	2a	00	0b	95	9a	..<.7@.0. VQ.*....
0020	a7	5c	b6	c7	01	bb	74	19	25	00	00	00	00	00	a0	02	..t. %.
0030	ff	ff	f6	66	00	00	02	04	05	b4	04	02	08	0a	00	93	...f.
0040	b8	3f	00	00	00	00	01	03	03	06							..?.....

بخش سوم)

در حالت ابتدایی رمزنگاری وجود دارد ولی ضعیف تر از حالت secret chat می باشد همچنین در حالت secret chat به صورت

انتها به انتها رمزگذاری انجام می شود

No.	Time	Source	Destination	Protocol	Length	Info
53	5.411846456	10.42.0.11	149.154.167.92	SSL	155	Continuation Data
60	5.723883925	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345364 Ack=4238594482 Win=8848 Len=0 TSval=1960342793 TSecr=9742375
61	5.723889443	149.154.167.92	10.42.0.11	SSL	155	Continuation Data
62	5.794576413	10.42.0.11	149.154.167.92	TCP	66	46816 → 443 [ACK] Seq=4238594482 Ack=3180345453 Win=1595 Len=0 TSval=9742412 TSecr=1960342794
169	13.037803523	10.42.0.11	149.154.167.92	SSL	187	Continuation Data
170	13.348789694	149.154.167.92	10.42.0.11	SSL	70	Continuation Data
171	13.367381580	149.154.167.92	10.42.0.11	SSL	187	Continuation Data
172	13.372466795	10.42.0.11	149.154.167.92	TCP	66	46816 → 443 [ACK] Seq=4238594603 Ack=3180345457 Win=1595 Len=0 TSval=9743172 TSecr=1960344700
173	13.377948163	10.42.0.11	149.154.167.92	TCP	66	46816 → 443 [ACK] Seq=4238594603 Ack=3180345578 Win=1595 Len=0 TSval=9743172 TSecr=1960344705
174	13.378997679	10.42.0.11	149.154.167.92	SSL	155	Continuation Data
175	13.730731609	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594692 Win=8848 Len=0 TSval=1960344796 TSecr=9743173
176	18.471595189	10.42.0.11	149.154.167.92	TCP	66	443 → 46816 [FIN, ACK] Seq=3163759211 Ack=4231269472 Win=1386 Len=0 TSval=9743673 TSecr=19603
179	18.777789479	149.154.167.92	10.42.0.11	TCP	66	443 → 46820 [FIN, ACK] Seq=4231269472 Ack=3163759212 Win=7508 Len=0 TSval=1960346680 TSecr=97
181	19.477911361	149.154.167.92	10.42.0.11	TCP	66	[TCP Spurious Retransmission] 443 → 46820 [FIN, ACK] Seq=4231269472 Ack=3163759212 Win=7508 L
182	19.603844188	10.42.0.11	149.154.167.92	TCP	66	[TCP Spurious Retransmission] 46820 → 443 [FIN, ACK] Seq=3163759211 Ack=4231269472 Win=1386 L
183	19.782967768	10.42.0.11	149.154.167.92	SSL	187	Continuation Data
184	19.910853127	149.154.167.92	10.42.0.11	TCP	78	[TCP Dup ACK 179#1] 443 → 46820 [ACK] Seq=4231269473 Ack=3163759212 Win=7508 Len=0 TSval=1960
185	20.092676944	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801
186	20.093210157	149.154.167.92	10.42.0.11	SSL	70	Continuation Data
187	20.120071848	149.154.167.92	10.42.0.11	SSL	187	Continuation Data

0100 ... = Version: 4
 ... 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 141
 Identification: 0x684a (26698)
 ▶ Flags: 0x02 (Don't Fragment)
 Fragment offset: 0
 Time to live: 64
 Protocol: TCP (6)
 Header checksum: 0x8af5 [validation disabled]
 [Header checksum status: Unverified]
 Source: 10.42.0.11
 Destination: 149.154.167.92
 [Source GeoIP: Unknown]
 ▶ [Destination GeoIP: United Kingdom, AS62041 Telegram Messenger LLP, 51.500000, -0.130000]
 ▶ Transmission Control Protocol, Src Port: 46816, Dst Port: 443, Seq: 4238594393, Ack: 3180345364, Len: 89

0030 06 3b 1d 1e 00 00 01 01 08 0a 00 94 a8 27 74 d8 .:.....t.
 0040 6f 36 92 b2 36 2e a3 7e 52 3c 7c 82 ef 30 3b 2b o6.6.-~ R[...0;
 0050 9e 51 45 37 7f 0d 44 8d 6a 62 14 c5 94 11 0a 1e P[...D. j[...
 0060 54 7a c0 9d 19 67 d6 e2 75 7b 60 f0 b0 ef 19 7d T[...g. u[...
 0070 2c ea 04 ca eb b6 a0 de 97 da bc 79 1d a2 1a 38 [Z...y...
 0080 b1 8d 35 86 ae 89 45 86 be 59 c9 fd 1e 83 f1 a8 .5...E..y...
 0090 2f 21 e8 64 11 b7 8d 28 47 62 d9 /!d...{ Gb.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Wireshark · Packet 3134 · wireshark_wlp3s0f0_20171201113500_QZ1xTJ

ip.addr == 149

No.	Time	Source	Destination	Protocol	Length	Info
3049	268.832	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345364 Ack=4238594482 Win=8848 Len=0 TSval=1960342793 TSecr=9742375
3090	278.555	149.154.167.92	10.42.0.11	SSL	155	Continuation Data
3091	278.805	149.154.167.92	10.42.0.11	SSL	155	Continuation Data
3092	278.873	10.42.0.11	149.154.167.92	TCP	66	46816 → 443 [ACK] Seq=4238594482 Ack=3180345453 Win=1595 Len=0 TSval=9742412 TSecr=1960342794
3093	278.882	10.42.0.11	149.154.167.92	SSL	187	Continuation Data
3094	279.238	149.154.167.92	10.42.0.11	SSL	70	Continuation Data
3099	284.962	10.42.0.11	149.154.167.92	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594692 Win=8848 Len=0 TSval=1960344796 TSecr=9743173
3100	285.273	10.42.0.11	149.154.167.92	TCP	66	443 → 46820 [FIN, ACK] Seq=4231269472 Ack=3163759212 Win=7508 Len=0 TSval=1960346680 TSecr=97
3101	285.273	10.42.0.11	149.154.167.92	TCP	66	[TCP Spurious Retransmission] 443 → 46820 [FIN, ACK] Seq=4231269472 Ack=3163759212 Win=7508 L
3102	285.794	10.42.0.11	149.154.167.92	SSL	187	Continuation Data
3103	285.902	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801
3105	286.043	149.154.167.92	10.42.0.11	SSL	70	Continuation Data
3106	286.105	149.154.167.92	10.42.0.11	SSL	187	Continuation Data
3134	304.488	149.154.167.92	10.42.0.11	TCP	78	[TCP Dup ACK 179#1] 443 → 46820 [ACK] Seq=4231269473 Ack=3163759212 Win=7508 Len=0 TSval=1960
3140	305.890	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801
3157	306.420	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801
3170	306.734	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801
3171	306.736	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801
3172	306.740	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801
3191	307.047	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801
3192	307.049	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801
3198	307.119	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801
3207	307.294	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801
3211	307.349	149.154.167.92	10.42.0.11	TCP	66	443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801

Internet Protocol Version 4, Src: 149.154.167.92, Dst: 10.42.0.11

0100 ... = Version: 4
 ... 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 141
 Identification: 0x684a (26698)
 ▶ Flags: 0x02 (Don't Fragment)
 Fragment offset: 0
 Time to live: 64
 Protocol: TCP (6)
 Header checksum: 0x8af5 [validation disabled]
 [Header checksum status: Unverified]
 Source: 149.154.167.92
 Destination: 10.42.0.11
 [Source GeoIP: United Kingdom, AS62041 Telegram Messenger LLP, 51.500000, -0.130000]
 ▶ [Destination GeoIP: Unknown]
 ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 46816, Seq: 44830124, Ack: 3201893934, Len: 121

0000 bc 6e 64 6e 8b be 40 b8 9a 64 8c 23 08 00 45 48 .ndn...0..d.#..EH
 0010 00 ad 9c 1d 00 00 30 06 a6 ba 95 9a a7 5c 0a 2a0.....\..
 0020 00 0b 01 bb b7 05 02 ac 0d ac be d9 06 2e 80 18
 0030 1e 60 6f a5 00 00 01 01 08 0a 74 da e7 ba 00 95o.....t.....
 0040 9c 0f b0 ae a7 7f 72 a2 ff 44 9b a4 d0 09 4f 3br...D...0;
 0050 4b f2 f0 07 2a 57 90 7b ad 20 ed 70 60 90 8e 39W.{...V...9
 0060 8e e6 b0 27 40 90 78 d6 19 bb 27 08 39 62 58 a80.x...9bX..
 0070 e6 17 cd 9e 9d 8e dc 11 61 02 df a7 7e e1 ca dbn...a...-...
 0080 c9 27 6e b6 23 fd cc a3 fe 54 4a 3c d2 f0 d4 dcn.#...Tj<...
 0090 8c 2d f8 89 71 12 3b a3 0a 54 b8 d2 31 a1 d7 80q...T..1...
 00a0 91 e7 a9 44 7b eb 9b a3 55 f5 c2 b7 48 33 3e d0D(...U...H3>..
 00b0 1c 8c 5d b6 cf a5 29 1f d0 d8 b7).).).)

No.: 3134 · Time: 304.488660821 · Source: 149.154.167.92 · Destination: 10.42.0.11 · Protocol: SSL · Length: 187 · Info: Continuation Data

Close Help

No.	Time	Source	Destination	Protocol	Length	Info
4930	480.367786297	10.42.0.11	149.154.167.92	XMPP/X...	155	UNKNOWN PACKET
4931	480.596579374	149.154.167.92	10.42.0.11	XMPP/X...	155	UNKNOWN PACKET
4932	480.674958431	10.42.0.11	149.154.167.92	TCP	66	49648 → 5222 [ACK] Seq=1823294739 Ack=3773067332 Win=103040 Len=0 TSval=9824275 TSecr=1960548073
4933	480.712778742	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067332 Ack=1823294739 Win=35392 Len=0 TSval=1960548103 TSecr=9824242
4934	483.763304979	10.42.0.11	149.154.167.92	XMPP/X...	171	UNKNOWN PACKET
4935	484.069234501	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067332 Ack=1823294844 Win=35392 Len=0 TSval=1960548942 TSecr=9824576
4936	484.165147934	149.154.167.92	10.42.0.11	XMPP/X...	155	UNKNOWN PACKET
4937	484.188602386	10.42.0.11	149.154.167.92	TCP	66	49648 → 5222 [ACK] Seq=1823294844 Ack=3773067421 Win=103040 Len=0 TSval=9824629 TSecr=1960548965
4938	484.188719139	10.42.0.11	149.154.167.92	XMPP/X...	155	UNKNOWN PACKET
4939	484.495001167	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067421 Ack=1823294933 Win=35392 Len=0 TSval=1960549048 TSecr=9824629
4940	485.633631891	10.42.0.11	149.154.167.92	XMPP/X...	283	UNKNOWN PACKET
4941	485.939485188	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067421 Ack=1823295150 Win=36464 Len=0 TSval=1960549409 TSecr=9824773
4942	485.951890451	149.154.167.92	10.42.0.11	XMPP/X...	155	UNKNOWN PACKET
4943	486.020901041	10.42.0.11	149.154.167.92	XMPP/X...	155	UNKNOWN PACKET
4944	486.373513398	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067510 Ack=1823295239 Win=36464 Len=0 TSval=1960549518 TSecr=9824812
4955	497.506854786	149.154.167.92	10.42.0.11	XMPP/X...	171	UNKNOWN PACKET
4956	497.585401786	10.42.0.11	149.154.167.92	XMPP/X...	155	UNKNOWN PACKET
4957	497.890494518	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067615 Ack=1823295328 Win=36464 Len=0 TSval=1960552397 TSecr=9825962
4958	498.047648826	149.154.167.92	10.42.0.11	XMPP/X...	171	UNKNOWN PACKET
4959	498.085046762	10.42.0.11	149.154.167.92	XMPP/X...	155	UNKNOWN PACKET
4960	498.389148930	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067720 Ack=1823295417 Win=36464 Len=0 TSval=1960552522 TSecr=9826018
4961	498.591779485	149.154.167.92	10.42.0.11	XMPP/X...	171	UNKNOWN PACKET
4962	498.712244848	10.42.0.11	149.154.167.92	XMPP/X...	155	[TCP Spurious Retransmission] UNKNOWN PACKET
4963	499.017324096	149.154.167.92	10.42.0.11	TCP	78	[TCP Dup ACK 4960#1] 5222 → 49648 [ACK] Seq=3773067825 Ack=1823295417 Win=36464 Len=0 TSval=19605...
.....0..... = IG bit: Individual address (unicast)						
Type: IPv4 (0x0800)						
Internet Protocol Version 4, Src: 149.154.167.92, Dst: 10.42.0.11						
Transmission Control Protocol, Src Port: 5222, Dst Port: 49648, Seq: 3773067421, Ack: 1823295150, Len: 89						
XMPP Protocol						
▶ eXtensible Markup Language						
▶ [Expert Info (Note/Undecoded): Unknown packet: <NULL>]						

سؤال سوم

استفاده از ابزارهای مانیتورینگ به خصوص در سازمان هایی که ترافیک های یک کشور را بررسی میکنند بسیار مهم است. مثلاً ممکن است بدافزاری که اقدام به باج گیری میکند هنوز یک کشور خاص را آلوده نکرده اگر بتواند درگاه ها را تحلیل ترافیک کرد بسته های آلوده به این بدافزار ها را میتوان شناسایی نمود و جلوی گسترش بیش از اندازه آن را گرفت.

یا مثلاً فرض کنید یک کشور که دارای چندین درگاه برای ورود ترافیک میباشد و الگوری های منظمی از این ترافیک دارد ناگهان به این موضوع برخورد میکند که از یک درگاه ترافیک بیش از اندازه وارد کشور شده است همین میتواند مسوولان را نسبت به این موضوع حساس کند که احتمالاً حمله ای در حال رخ دادن است..

از طرفی در تصمیم گیری های کلان یک کشور میتوان با تحلیل ترافیک و مشخص نمود الگوی تمایل مردم به محتواهای مختلف ، سلیقه مردم یک کشور را مشخص نمود مثلاً تصور کنید کشوری که بیشترین ترافیک داخلی آن مربوط به سایت های خبری باشد بعد از چند سال ترافیک اصلی آن بر روی سرور های سایت های سرگرمی قرار میگیرد این به منزله تغییر ذایقه مردم می باشد.