

github/truerandom

Definimos la variable de entorno, ella apunta al archivo donde se guardara el intercambio Diffie-Hellman

```
chaos@chaos:~/Criptografia/p7$ pwd
/home/chaos/Criptografia/p7
chaos@chaos:~/Criptografia/p7$ export SSLKEYLOGFILE='/home/chaos/Criptografia/p7/secrets.txt'
```

Ejecutamos wireshark:

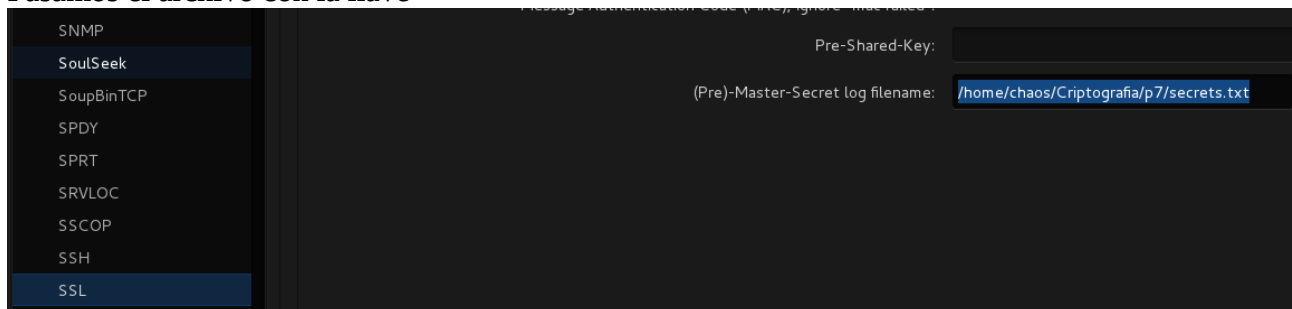
```
chaos@chaos:~/Criptografia/p7$ pwd
/home/chaos/Criptografia/p7
chaos@chaos:~/Criptografia/p7$ export SSLKEYLOGFILE='/home/chaos/Criptografia/p7/secrets.txt'
```

Capturamos y filtramos por el puerto 443:

Filter:	tcp.port == 443			Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info	
2	0.304563000	192.168.1.75	149.154.175.50	SSL	139	Continuation Data	
3	0.451465000	149.154.175.50	192.168.1.75	SSL	155	Continuation Data	
4	0.451514000	192.168.1.75	149.154.175.50	TCP	66	44038→443 [ACK] Seq=74 Ack=90 Win=3	
8	2.911589000	192.168.1.75	172.217.5.174	TLSv1.2	97	Encrypted Alert	
16	7.071578000	192.168.1.75	157.240.3.35	TLSv1.2	97	Encrypted Alert	
56	30.557060000	192.168.1.75	74.125.21.103	TCP	74	52268→443 [SYN] Seq=0 Win=29200 Len=0	
57	30.557274000	192.168.1.75	52.40.179.197	TCP	74	43274→443 [SYN] Seq=0 Win=29200 Len=0	
59	30.806964000	192.168.1.75	74.125.21.103	TCP	74	52270→443 [SYN] Seq=0 Win=29200 Len=0	
60	30.808189000	192.168.1.75	52.40.179.197	TCP	74	43276→443 [SYN] Seq=0 Win=29200 Len=0	

En la terminal donde definimos la variable, iniciamos firefox y navegamos en la pagina analizar (en este caso fue seguridad.unam.mx):

Pasamos el archivo con la llave



Comparacion de los paquetes antes y despues:

Antes:

490	43.313092000	192.168.1.75	132.248.124.130	TLSv1.2	810	Application Data
491	43.345051000	132.248.124.130	192.168.1.75	TLSv1.2	340	New Session Ticket, Change Cipher
493	43.365463000	132.248.124.130	192.168.1.75	TLSv1.2	1466	Application Data
494	43.365499000	192.168.1.75	132.248.124.130	TCP	66	42418→443 [ACK] Seq=1068 Ack=5883
495	43.366452000	132.248.124.130	192.168.1.75	TCP	1466	[TCP segment of a reassembled PDU]

▶ Frame 493: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface 0						
▶ Ethernet II, Src: d8:37:be:a9:42:be (d8:37:be:a9:42:be), Dst: ChinaSsj_22:10:28 (98:3f:9f:22:10:28)						
▶ Internet Protocol Version 4, Src: 132.248.124.130 (132.248.124.130), Dst: 192.168.1.75 (192.168.1.75)						
▶ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 42418 (42418), Seq: 4483, Ack: 1068, Len: 1400						
▶ Secure Sockets Layer						

0000	98 3f 9f 22 10 28 d8 37	be a9 42 be 08 00 45 00	..?..(.7 ..B...E.
0010	05 ac 4c cd 40 00 2e 06	37 11 84 f8 7c 82 c0 a8	..L.@... 7... ...
0020	01 4b 01 bb a5 b2 3d 72	bc a6 33 90 84 d7 80 10	..K....r...3.....
0030	00 86 7a fc 00 00 01 01	08 0a c0 cd e7 f3 00 aa	..Z.....
0040	ce 94 17 03 03 01 08 17	d9 dc ea 3f d0 36 4e 10?..6N.
0050	a9 00 0c c1 53 f5 17 d5	5a b3 43 47 12 e0 26 9d	...S... Z.CG..&.
0060	da 91 5e ce 6e f5 2e 08	22 23 75 c0 2e 4e 87 b4	..^..n... "#u..N..
0070	ea f5 4b fb c8 3b cf 91	a6 cb 64 4e 76 2b 92 b0	..K.;... ..dNv+..
0080	33 1f e5 0b e0 cb 19 03	94 86 1e 34 df 2b 9d 7e	3..... ..4.~
0090	03 f6 b7 1a 86 1a 0f d3	c8 d6 62 bf 48 b4 3b a4b.H;..
00a0	ee 64 8e a4 39 8a 26 8b	e7 17 de 89 7b fe 73 e3	..d..9.&....{.s.
00b0	af f3 22 25 0a 20 20 2f	24 20 5a 00 1f 0a 24 50	..F.....7...&D

Después:

491	43.34505100	132.248.124.130	192.168.1.75	TLSv1.2	340	New Session Ticket, Change Cipher Spec, R...
493	43.36546300	132.248.124.130	192.168.1.75	TLSv1.2	1466	[SSL segment of a reassembled PDU]
494	43.36549900	192.168.1.75	132.248.124.130	TCP	66	42418→443 [ACK] Seq=1068 Ack=5883 Win=432
495	43.36645200	132.248.124.130	192.168.1.75	TCP	1466	[TCP segment of a reassembled PDU]
496	43.36670500	132.248.124.130	192.168.1.75	TCP	1466	[TCP segment of a reassembled PDU]
497	43.36671800	192.168.1.75	132.248.124.130	TCP	66	42418→443 [ACK] Seq=1068 Ack=5883 Win=432

▶ Frame 493: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface 0
 ▶ Ethernet II, Src: d8:37:be:a9:42:be (d8:37:be:a9:42:be), Dst: ChinaSsj_22:10:28 (98:3f:9f:22:10:28)
 ▶ Internet Protocol Version 4, Src: 132.248.124.130 (132.248.124.130), Dst: 192.168.1.75 (192.168.1.75)
 ▶ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 42418 (42418), Seq: 4483, Ack: 1068, Len: 1400
 ▶ Secure Sockets Layer

```

0000  48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d  HTTP/1.1 200 OK.
0010  0a 44 61 74 65 3a 20 53 75 6e 2c 20 31 36 20 41  .Date: Sun, 16 A
0020  70 72 20 32 30 31 37 20 30 34 3a 35 37 3a 32 31  pr 2017 04:57:21
0030  20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70  GMT..Server: Ap
0040  61 63 68 65 0d 0a 58 2d 46 72 61 6d 65 2d 4f 70  ache..X-Frame-Op
0050  74 69 6f 6e 73 3a 20 53 41 4d 45 4f 52 49 47 49  tions: SAMEORIGI
0060  4e 0d 0a 56 61 72 79 3a 20 41 63 63 65 70 74 2d  N..Vary: Accept-
0070  45 6e 63 6f 64 69 6e 67 0d 0a 43 6f 6e 74 65 6e  Encoding..Conten
0080  74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d  t-Type: text/htm
  
```

Frame (1466 bytes) Decrypted SSL data (240 bytes)

Antes:

Filter:

tcp.port == 443 and ip.addr == 132.248.124.130

▼ Expression...

Clear

Apply

No.	Time	Source	Destination	Protocol	Length	Info
537	43.49838000	192.168.1.75	132.248.124.130	TLSv1.2	117	Change Cipher
538	43.49867800	192.168.1.75	132.248.124.130	TLSv1.2	859	Application Da
539	43.50380300	192.168.1.75	132.248.124.130	TLSv1.2	864	[SSL segment c
540	43.50384100	192.168.1.75	132.248.124.130	TLSv1.2	854	[SSL segment c
541	43.51263900	132.248.124.130	192.168.1.75	TCP	66	443→42421 [ACK
542	43.51390100	132.248.124.130	192.168.1.75	TCP	66	443→42423 [ACK
543	43.52209800	132.248.124.130	192.168.1.75	TLSv1.2	402	[SSL segment c
546	43.52937500	132.248.124.130	192.168.1.75	TCP	1466	[TCP segment c
547	43.52939500	192.168.1.75	132.248.124.130	TCP	66	42423→443 [ACK
548	43.52985000	132.248.124.130	192.168.1.75	TCP	1466	[TCP segment c
549	43.53046400	132.248.124.130	192.168.1.75	TCP	1466	[TCP segment c

▶ Frame 538: 859 bytes on wire (6872 bits), 859 bytes captured (6872 bits) on interface 0

▶ Ethernet II, Src: ChinaSsj_22:10:28 (98:3f:9f:22:10:28), Dst: d8:37:be:a9:42:be (d8:37:be:a9:42:be)

▶ Internet Protocol Version 4, Src: 192.168.1.75 (192.168.1.75), Dst: 132.248.124.130 (132.248.124.130)

▶ Transmission Control Protocol, Src Port: 42418 (42418), Dst Port: 443 (443), Seq: 1831, Ack: 1068, Len: 859

▶ Secure Sockets Layer

0000

d8 37 be a9 42 be 98 3f 9f 22 10 28 08 00 45 00

.7..B..? .."(..E.

0010

03 4d 4e e2 40 00 40 06 25 5b c0 a8 01 4b 84 f8

.MN.@.@. %[...K..

0020

7c 82 a5 b2 01 bb 33 90 87 d2 3d 72 de 7d 80 18

|.....3. ..=r.}..

0030

01 d5 f5 3e 00 00 01 01 08 0a 00 aa ce c2 c0 cd

...>....

0040

e8 14 17 03 03 03 14 00 00 00 00 00 00 03 fc

....

0050

7e d3 23 42 86 59 19 e4 da c2 29 2f 6f 77 92 e6

~.#B.Y.. ..)/ow..

0060

7a cb 8f d2 2d d8 02 77 05 e8 20 60 4a e0 d9 a6

z....w ..`J...

0070

c0 cd 99 61 c8 3f ee 1e 81 94 be bc 32 72 ed 99

...a.?..2r..

0080

f9 bb ac 16 cc 8a 75 55 0c cf 5b 8c c1 97 c7 39

....uU ..[....9

0090

b1 62 92 75 d8 7f 25 53 f3 11 00 78 02 a4 e1 58

.b.u..%S ...x...X

00a0

83 b4 14 af 07 ff 33 47 66 41 32 6d a3 77 c9 cb

....3G fA2m.w..

00b0

4e f3 41 ff 05 2a c0 a0 fa 74 df a6 bb 12 ba ba

MCA .. +

Despues:

```

▶ Frame 538: 859 bytes on wire (6872 bits), 859 bytes captured (6872 bits) on interface 0
▶ Ethernet II, Src: ChinaSsj_22:10:28 (98:3f:9f:22:10:28), Dst: d8:37:be:a9:42:be (d8:37:be:a9:42:be)
▶ Internet Protocol Version 4, Src: 192.168.1.75 (192.168.1.75), Dst: 132.248.124.130 (132.248.124.130)
▶ Transmission Control Protocol, Src Port: 42418 (42418), Dst Port: 443 (443), Seq: 1831, Ack: 13146, Len: 793
▶ Secure Sockets Layer

```

Frame (859 bytes) Decrypted SSL data (764 bytes)