Auditoria de Aplicación **Instagram**Seguridad Informática



Camilo Zepeda Hoffmann

Prof. Maximiliano Vega

Noviembre 02, 2017

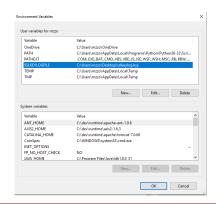
Host a Probar



Creación de PATH

Es necesario generar un nuevo PATH en las variables ambiente, declarando la dirección a apuntar y el archivo a generar, el cual será:

sslkeylog.log



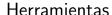




El archivo obtenido

Se aprecian los datos obtenidos en el archivo **sslkeylog.log**, donde se declara el cliente, llave y rsa.

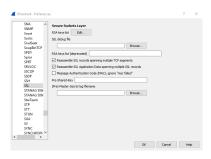
```
ssikeviog log - Notepad
 11 THIT BARDON 9997A17223-6756-6156-6156-6156-6156-6156-7256-646-6156-7256-6156-7-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7-6156-7-7
   CLIENT RANDON meddibi7621ec3460mfc135b28bb15396c5e1565fe87ff7b55mf2498c58cf63 b2c5m680fe6741m3ff731bm5e146d78bd93122917
 CLIDIT_MANDON [9350e721001.8617as00cc131ce1938e0eaf6b10640b3ef6c24c631fbe3occar e9fc317fbe10ff1ba60b701a0b2007e45864251
CLIDIT_NANDON [74524771183083151b666-74811625415280c1012ba220cce800cbe67589f1 7415414675f0asf4665c0f9asf4f66750
 CLIENT RANDON 0302deeb1b055066620019fc80f2cb54e7b0f2002f807351d2432f3bd5934b c16b15080f9a3093e07c5d8b4f97206c8346bfcec
   CLIMIT JANDON 040010440[200:3978050:725f]1b74044850677504380537040485137205f80 c305271c4f6500471c70fee0931f6030c44614600
 CLIDIT RANDON e0f4c5575a2dcae8e32be0911a22d234b26cbe000c4ecdec0007abc4307abd7b 7d3061a2bbc0ad0943650ef7bf36ad5fac9abbb05
 CLIDIT_NAMBON 509x6017726f5767361090761090f10f9bec7547087c3bb0f3c3450d108cc0e bf61442a10bf708abe38640512abe70812acf70827
CLIBIT_NAMBON f7x86c3efef9ccff12abi30d327a663eff8bcefe7f42b36c5d857ad65d665a7 56c68fbbc386x8f7a82d63a66c88b36fccb7bff3
CLIENT_NAMOON_26548275962746661283465c2476685957267c27597459668858978625554256_25901c586655754286757622675534676788667
CLIENT_NAMOON_56494997c57e3285891262244476665477c67c234914446579215669488748c_7f1e1546c666849475c8345518618797182c62464
 CLIBIT RANDON 47429418713148745245959C8726995944CR0cc228b17374221c1458228989 c364487594880497676774742217767774876599
 CLIENT RANDON D: ff#f#7#6#3037687#025717#00530f#87#17#005#c2#03205#2#c308597f9 filedd#b7820222446#5bfc89882cd8947c35770
 CLIENT NAMBON 4007(01807000071802400078804971538940030151577010975012007077 5421585000720797144250077804469007
 CLIENT RANDOM 7087778fc1b07esft990e8ff2da6b0be8jaa12f0e5c1573108817296080144fc eftbffd8cbee92266bd99c777bcff749167ae80
 CLIDIT RANDON 6173074e6d7x554ade0100e4fe0b405507077773b2accd57f052a05500434e0 0f310f2007743a0f5c1ae40fbccc550dcae6d0052
   CLIENT_NAMBOY edise2ptdc92b42x5d9f1269a8cfxfb41c80e2e4b402b3122b6b4286x
 CLIDIT RANDON 03ff9e2f327209ddda34e73b48e4260cee855fe1571f2ca38981aef60b1a9482 3ae6998828b7789e5945595a7c608328d876d2d
CLIENT_NAMON* cf0318541440444815bb052a2e2ELdf9fbef895c99843890995e1268171344556*7754844c959084482ab5e3a49c947e59955ec940c
CLIENT_NAMON* cf0318541440444815bb052a2e2ELdf9fbef895c99843890995e1268171344556*7754844c959084482ab5e3a49c947e59955ec940c
CLIENT_NAMON* cf0318541440444815bb052a2e2ELdf9fbef895c99843890995e1268171344556*7754844c959084482ab5e3a49c947e
 CLIDIT RANDON Secretaria (Secretaria (Secr
 CLIENT_NAMBON_COaff c07407:007f44:be093672b703f3a84402d33381e78077318bf3644939 d935f418144b00d4194e3bef80c531090000097
 CLIDIT RANDOM 47536772c187832a7a5231b7192b5a6b361447210e66b1530855a3230343fa3b 309082c80b6aade1818083w79637297b4790c600
 CLIENT NAMBON 3050548311d2541cf9a59839447ce9937285fef00ef96c95a0d148687957d967 67e5a4d8e7c0df88ff05cb181f618917f35c14396
                _mandon arc75ea78272e8246a0x2671c89689c92642559dc813f44dc4523837a8d48d 8e34x83479f6x1abe61844a588855ac6d641e2452
 CLIDIT RANDON bzeradno-31fzabra3007280630ccc5cfbb0re0c71b5be040407380ae3fzfdf5_2d70af785c0300fb003440e0028261118azes022a
 CLIENT_MANUAL_3/MONROSO/CECCUST/1/SCHRCCC/2004/25000/00/251/3/1/SCHRCC2/2004/25001/20/251/3/1/SCHRCC2/2004/25001/20/251/3/SCHRCC2/2004/25001/20/251/3/SCHRCC2/2004/25001/20/251/3/SCHRCC2/2004/25001/20/251/3/SCHRCC2/2004/25001/20/251/3/SCHRCC2/2004/25001/20/251/3/SCHRCC2/2004/25001/20/251/3/SCHRCC2/2004/25001/20/251/3/SCHRCC2/2004/25001/20/251/3/SCHRCC2/2004/25001/20/251/3/SCHRCC2/2004/25001/20/251/3/SCHRCC2/2004/25001/20/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/3/SCHRCC2/2004/251/SCHRCC2/2004/251/3/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/250/SCHRCC2/2004/250/SCHRCC2/2004/250/SCHRCC2/2004/251/SCHRCC2/2004/250/SCHRCC2/2004/250/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2/2004/251/SCHRCC2
 CLIBIT RANDON 16:7546562407314407115a377837000723051b0774750a113a45475799663aa 51d7155c1bfc132c3cb1000651bf28090cc00bac
 CLIBNT_NAMBON 50991ebbfc2bbf1c866b84982cfe235efbe64e49a15f51741ce8c4d4c5d49a2e 47c4e1d13f6de9847ece8985c946e537e09d6ddd
CLIBNT_NAMBON 8c2224e499f15756580906d2616892c242cb7871716844c5(14ce8)65809513 a7d9895(8889898780257286f655ea77867c96
 CLIDIT RANDON 200905CT7T00438811C54c0373f2700096f80007030cD73300758530704165 50007585105305157120375f67003027560074
 CLIENT_BANDON_C0779fac40bb245ccc028c093448556a9827f8b556ae047cebbd89b5774bc902_bfc32234cS0ed8e24e156ac0911dhaa44cBfcc9
 CLIENT RANDOM 87/09981743003(168)8552646850585396156198331867887cae61987ed8183 89881164408877c5868180e4946e6e6987888307F
```

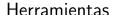




WireShark Implementación de Certificados

Ya en previa emisión de internet por parte del computador, es necesario proveer los certificados generados, contal de ver la respuesta dentro de la aplicación.







Búsqueda de Carpeta con Certificados

Es necesario proveer la ruta especifica en donde se encuentra el archivo generado por el PATH, de tal manera que trabajen como decifradores de las request generadas al hacer man-in-the-middle. Se consigue la ruta especifica en donde se encuentra el archivo generado por el PATH, de tal manera que trabajen como decifradores de las request generadas al hacer man-in-the-middle.

SL debug file		Br	owse	
SA keys list (deprecat	ed)			
Reassemble SSL rei	ords spanning multip	le TCP segments		
Reassemble SSL Ap	plication Data spanni	ng multiple SSL re	cords	
Message Authentic	ation Code (MAC), ign	nore "mac failed"		
re-Shared-Key				
Pre)-Master-Secret log	flename			
C: \Users\mzzo\Des	ktop\sslkeylog.log	Br	owse	





Uso de Wireshark

Se adjunta las imagen correspondiente a los paquetes recibidos dentro de la aplicación haciendo uso del celular como emisor de paquetes, de entre los cuales se logra apreciar ciertos paquetes.

Escape de				
PROPERTY AND	access now as	a prince story a	No. or other	CARTINE SECURIOR SECURIOR
				From 19th In MF the Pathon Admits
Name and district	of Pestandy Ire R			100, At 44, pr 28





Uso de Wireshark

Es posible apreciar lectura de los paquetes, entregando pauetes del tipo TCP y CLIENT HELLO, de la cuál se adjunta una recepción del paquete mayormente ilegible, pero aún así, no se encuentra información consistente y tangible de las respuestas. Lo que implica que no es posible captar la información de los usuarios o bien sentencias explotables.

