MANUAL SOBRE COMO CLONAR UNA SIM v.1.6

By LUK - luk@hackhispano.com

==============================================

Ingredientes:

- Tarjeta original a clonar (Movistar, Airtel o Amena).

- Tarjeta GoldWafer (16f84 y 24c16), en esta tarjeta sera grabada la nueva SIM.

- Programador recomendado PHOENIX y TE20X (Se oueden usar otros como millenium...)

- Software: Cardinal v68 (para sacar el IMSI y el KI), IC-Prog (para grabar el pic y la eeprom).

- Paciencia, mucha paciencia.

**Procedimiento**:

Conectamos el PHOENIX al enchufe y al ordenador mediante el puerto de serie. Insertamos la tarjeta en el Phoenix, la SIM´s

Tiene un tamaño muy pequeño por lo que utilizaremos un adaptador para "agrandarla", usaremos como adaptador cualquier

Adaptador de los que te vienen cuando compras una tarjeta nueva. Con la tarjeta dentro ejecutamos el CARDINAL. Al abrirlo de

Sale un cuadradito azul, pichas en "clik here"-->"smartcard"-->Sim Editor", a continuación te saldrá una ventana, en ella, en la barra de herramientas pincharemos en el menú "SIM" y luego en "SIM info". Te aparecerá una nueva ventana, en ella picharemos sobre el botón "Load", al pichar este botón el programador parpadeara unos segundos y aparecerán los datos en la pantalla. En el campo IMSI aparecerá un numero de 15 caracteres, una vez obtenido el IMSI, le quitas el primer digito, inviertes las parejas y añades al principio 08 29.

Ejemplo.

21 78 63 95 36 51 ...

Suprimes el 2

1 78 63 95 36 51 ...

Inviertes las parejas

71 68 93 35 56 1...

Añades 08 29 delante

08 29 71 68 93 35 56 1...

Y ya tienes el IMSI correcto ¡Apunta ese número en un papel!. Bien, ya tenemos en IMSI.

A continuación vamos a sacar el KI, para ello, igual que antes, ejecutamos el CARDINAL y pichas en "clik here"-->"smartcard"-->Sim Editor", a continuación te saldrá una ventana, en ella, en la barra de herramientas pincharemos en el menú SECURITY y después en "Find key KI". Te saldrá una nueva ventana (si te sale un cuadro de dialogo pincha en NO), para empezar a sacar el KI pulsaremos en el botón START. A continuación empezaran a correr números en el campo "Current RAND", en aproximadamente 10 horas (depende de la CPU) nos saldrá donde las interrogaciones un numero de 32 caracteres ¡Apunta también ese número!. Perfecto, ya tenemos el IMSI y el KI, enhorabuena.

Ahora vamos a crear el hex del PIC, para ello grabaremos el siguiente fichero.

:10000000DF209A01FF30650086004F30660008301F

:10001000620012309300890144203F3A031D1128E9

:100020001A144420890A9820930B1128DF200530E8

:1000300093000C3084004E20DF20A0300C02031D02

:100040005B280D08A43A03194229843A03198B2A24

:10005000903A0319202A703A0319B329163A031962

:10006000202A243A0319AE29403A03193E2A6E3A4F

:1000700003193E2A543A0319A02A723A03195F2839

:10008000043A03196E2A5D2883160814831208089F

:100090000800DF200D089828303084006820800098

:1000A000840A930B4E2808006B3060286730602864

:1000B00008308C0089296E3060286D3060289030BF

:1000C0008C019D00DF201D0898200C089820162820

:1000D000831686178312861F6B28861B6D280930AE

:1000E0009B009A10861B6D28D1201A189C0D1A1C93

:1000F0009C0CD720861F8B2802309A060000031420

:100100009B0B75281A0C1A060139031D8D281A1825

:100110009C091C08080003108028D720831686132A

:1001200083128613D720861783168617D120682856

:100130009D009C001A189C0909309B009A10D12040

:10014000831686178312861FA32803100318AA2874

:10015000C720AE28CD2002309A060000D4201A18FD

:100160009C0D1A1C9C0C9B0BA6281A0C1A06013914

:10017000031DBC28C720BD28CD20D720CD20D720E7

:10018000861FC428DF200800DF201D08982886135A

:10019000831686138312861308008316861783122C

:1001A00008000A309E00DA2816309E00DC2818303D

:1001B0009E000000000000009E0BDC2808003B3081

:1001C0009E00DC282608A400250D0E39A038A300C7

:1001D00008008616061600000612000086120800A7

:1001E000031C061203180616861600008612080065

:1001F00083160616831286160310061A0314861237

:1002000008000830A100A20DF020A10B0329F8205E

:1002100083160612831208000830A100F820A20DF0

:10022000A10B0E290829E9202308A2000121240896

:10023000A200012106122721E9202308A20022148E

:1002400001210C210314F0202721220808000612A6

:10025000000086160000061608008C00E92023081E

:10026000A20001212408A20001210C08A200012102

:1002700006122721E920A030A2000121272103181E

:100280003A2908000E080F04031D542802301002FA

:10029000031D56284920023093004C203F30300285

:1002A000031D6429B108031D642916308C00300831

:1002B000A9003108AB0030089F003108A000AC0154

:1002C000AC0A2E109F3061287F303002031D742944

:1002D00010303102031955292030310203195529F4

:1002E00021303102031955296F303002031980295A

:1002F0002F303002031D8729E2303102031D872988

:1003000031088B21031987290F308C005B290430B9

:100310008C00943061288C00123089000330A500D5

:100320004730A6004420FF390319AD290C060319F4

:10033000A829890A4420890A91007C23043A0319D8

:10034000A229910A110A7C23A6070318A50A92295B

:10035000890A44208C007C23031108002908A80086

:100360002B08AA00B7291F08A8002008AA004920C6

:100370002E18D5293F302802031DC12900308C00DA

:10038000DD297F302802031DC82916308C00DD29A5

:100390006F301F020319EE292F301F020319EE29B7

:1003A00003019820900BD0295F283030840000088A

:1003B0009820840A900BD7295F28A400A630A300B8

:1003C000930105301302031DE7292A08E8291321A8

:1003D0009820930AA40A900BE1295F2820088B211A

:1003E00092008C0A853098200D309820043012023B

:1003F0000230031DFE2903019820013093001922C9

:100400001F089820200898200430120203190C2A93

:100410000930930019225F2804309820003098207A

:10042000013093001922063093008F308C0019227E

:100430005F280C087C2398208C0A930B192A08004B

:1004400020088B2103195828043A031D5828073027

:100450002002031D352A1B30A6022D080319352A58

:1004600092000930A607920B322A0F08A60703183C

:10047000A50AD6300D020319802A642A20088B2190

:1004800003195828043A031958288F038F030319B6

:10049000542A8F030319522A8F0B58280E08031D64

:1004A000AC00552AAC03552AAC0A2C0892000B303C

:1004B0000C077C235E2AA6070318A50A920B5B2A69

:1004C000DC300D020319802A4920E22013219820F4

:1004D000A60A0319A50A900B652A5F2844300E026C

:1004E000031D54284B300F02031D542810301002F6

:1004F000031D56280230A5002D0E3039C03EA6003F

:100500000D099820E22068202D21A60A0319A50ACA

:10051000900B802A5F2808301002031D56284920BE

:10052000083093004C200F30B005B105B205B3057B

:10053000300EB104320E3304FF3E0339AD005F28A4

:1005400010301002031D56282E1449201008930065

:10055000403084004E20073094003030840010304A

:100560009300A430A3002D0E3039C03EA400132107

:100570008000A40A840A930BB72A04309300013048

:100580009900103098009C01190392001803910003

:1005900011081C079500303E8400000896001808DA

:1005A0008407000897001608512380001808840269

:1005B0001708512380009103911FC82A0310180DBA

:1005C0009C079203921FC62A0310990D980C93035F

:1005D000931FC32A30308400023091001030930002

:1005E000000E840A00049200840A11088402120892

:1005F000800011088407910A930BF02A94080319CC

:10060000252B1030930040309600910180309900E6

:10061000083092009501110D9800980E0F30980542

:100620003030180784000008190595040310990C50

:1006300011309107920B0B2B1608840015088000CF

:10064000960A930B062B9403AD2A023092003F309A

:100650008400073093000310800D8403930B2C2B30

:10066000920B272B0730930039308400000892004A

:10067000053084021208800006308407930B362B65

:10068000BB010C308C006229A030A3001B089B0129

:10069000170703189B0A160703189B0A9B101B06D3

:1006A000642B9B000A148A141308572382008207C4

:1006B0006F346A34663462344434A3001B0817076D

:1006C00016070800A2305D23A4001329A4305D237F

:1006D0007F39642BA4305D233F39803E642BA430E6

:1006E0005D23A400240C0F397F3E7C23A300241833

:1006F000A30E230E0F3908000A148A148200FC345A

:10070000A4341E34B7345034E7341234D834A3340C

:1007100049346034323456348934BD34FC34FF34C7

:10072000BB34033402340034003404340434013460

:10073000043409341B3404340934113404341834B7

:100740001134043401341B340434033412340434BB

:1007500004341B34043405341B340434023411349F

:1007600004340A341234043410341134043402349E

:100770001B3404340C34113404340B341134043479

:1007800003340B34043401340B3404340A340F348E

:10079000143403346434043400341134FB3422340C

:1007A0000334023401341C3414340034B0340434BF

:1007B00000341134FB34BB34033402340134B0341C

:1007C000143400341C34043400341134FB34BB348E

:1007D0000334023401340E3434340034033404342A

:1007E000403412341B34BB348334023403340334B6

:1007F000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F09

:084000000F000F000F000F007C

:02400E00F93F78

:104200003F002F00000080006900AF0002000400A2

:10421000010031000000000000000E0083003E009D

:104220009F00160007009800E200C50005009500F9

:1042300020009B0030009E003100A1003700A40048

:104240003800A7004100AA004300AD004500B000BF

:104250007400B3007800B6007B00B9007E00BC009B

:10426000AD00BF00AE00C2003900EC003D00E00030

:104270003C00D4003A00C8000000FF00FF00FF002F

:00000001FF

Copia todo ese código en el bloc de notas y nómbralo como: GSMSIMPIC.HEX

Ahora vamos a crear el hex de la eeprom, esto es algo más complicado, copia el siguiente código y grabarlo como GSMSIMEPP.HEX

:1000000066B1BAA2029C704B3719080CFBC1F6BC52

:100010006DD597352A4FBF73E9F2A4DFD1946CA157

:10002000FC25F42F40D306EDB9A08B714C8A3B46DA

:10003000431A0D9D3FB3DD1ED624A645987CCF7490

:10004000F7C229544701310E5F23A915604ED7E14D

:10005000B6F31C5CC976044AF880110B9284F53023

:10006000955A782757E66AE8AF137EBECA8D89B0E5

:10007000FA1B6528DBE33A1433B262D88C16207978

:100080003D67CB481D6E55D4B4CC96B70F42ACC477

:1000900038C59E00642D990790DEA3A73C87D2E760

:1000A000AEA526F9E022DCE5D9D0F144CEBD7DFF36

:1000B000EF36A8597B7A499175EA8F6381C8C0529F

:1000C00068AA88EB5D51CDADEC5E69342EE4C605BF

:1000D00039FE619B8E85C7ABBB3241B57F6B93E226

:1000E000B8DA83214D561F2C583EEE12182B9A1762

:1000F000509F866F0972035B1082530AC3F0FD772D

:10010000130B50722B01455E27127F756103552B2F

:100110001B7C46532F473F0A2F594F040E3B0B05BC

:10012000236B67441556245B557E20326D5E78063E

:10013000354F1C2D635F292258445D376E7D69144D

:100140005A504C60173C594079380E4A6508134E96

:100150004C42682E6F32200327003A195C16123386

:1001600039417774166D07563B5D3E6E4E634D43C5

:100170000C71576266055821263817084B2D0D4B18

:100180005F3F1C317B7814702C1E0F626A02671D62

:10019000526B2A7C181E29106C6475284928077236

:1001A000527324700C6664545C3048610936374AD7

:1001B000717B111A353A0409457A15762A3C1B4998

:1001C000767D220F417354403E514601186F79539A

:1001D0006851317F30691F0A065B57251036747EDF

:1001E0001F260D00486A4D3D1A432E1D60253D34E3

:1001F00065112C6C473442392133195A02777A231E

:1002000034322C061531293B27331920332F342B58

:10021000250428223D0C1C043A17080F0C1609125D

:10022000370A212332012B03390D3E0E072A2C3BBE

:100230003E391B06081F1A3629162D1427031038BD

:100240003002151C242A3C212212000B180A113DF1

:100250001D0E2D1A372E0B11362E09181E3C2000AC

:100260001426021E3A230110382817300D13131BD1

:100270001F352F263F0F3105253519243F1D050752

:1002800001051D0619011217111300091819061F7F

:100290001C14181E041B030D0F100E120403080972

:1002A00014000C1A15081C021D020F070B160E0A6B

:1002B00011150C1E1A1B101F0B070D170A0516131C

:1002C000B1B1B1B1B1B1B1B1B1B1B1B1B1B1B1B11E

:1002D000B2B2B2B2B2B2B2B2B2B2B2B2B2B2B2B2FE

:1002E000B3B3B3B3B3B3B3B3B3B3B3B3B3B3B3B3DE

:1002F000B4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B4BE

:10030000851401F03F00018000FFFF430909020549

:100310000400838A838A851400307F10028000FBEA

:10032000FF030909000E0400838A838AA1A1A1A109

:10033000A1A1A1A1A1A2A2A2A2A2A2A2A2A2A3A3A0

:10034000A3A3A3A3A3A3A3A4A4A4A4A4A4A4A4A474

:10035000988311111111111111F1FFFFFFFFFFFF20

:10036000FFFFFFFFFFFF07FFFFFFFFFFFFFFFFFF95

:10037000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF8D

:10038000000000CF3F000CFFFFFF0000FFFFFFFF5A

:10039000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF6D

:1003A000FFFFFFFFFFFFFFFF0002FFFFFFFFFFFF59

:1003B000FFFFFFFFFFFFFFFFFFFFFFFFFF0000FF4B

:1003C0000100FFFF02000000FFFFFFFFFFFFFFFF34

:1003D000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF2D

:1003E000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF1D

:1003F000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0D

:10040000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC

:10041000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEC

:10042000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFDC

:10043000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFCC

:10044000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFBC

:10045000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFAC

:10046000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF9C

:10047000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF8C

:10048000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF7C

:10049000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF6C

:1004A000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF5C

:1004B000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF4C

:1004C000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF3C

:1004D000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF2C

:1004E000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF1C

:1004F000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0C

:10050000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFB

:10051000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEB

:10052000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFDB

:10053000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFCB

:10054000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFBB

:10055000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFAB

:10056000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF9B

:10057000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF8B

:10058000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF7B

:10059000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF6B

:1005A000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF5B

:1005B000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF4B

:1005C000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF3B

:1005D000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF2B

:1005E000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF1B

:1005F000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0B

:10060000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFA

:10061000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEA

:10062000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFDA

:10063000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFCA

:10064000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFBA

:10065000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFAA

:10066000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF9A

:10067000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF8A

:10068000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF7A

:10069000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF6A

:1006A000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF5A

:1006B000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF4A

:1006C000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF3A

:1006D000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF2A

:1006E000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF1A

:1006F000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0A

:10070000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF9

:10071000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE9

:10072000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFD9

:10073000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC9

:10074000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFB9

:10075000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFA9

:10076000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF99

:10077000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF89

:10078000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF79

:10079000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF69

:1007A000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF59

:1007B000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF49

:1007C000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF39

:1007D000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF29

:1007E000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF19

:1007F000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF09

:00000001FF

Bien, ya tenemos el archivo de la eeprom, ahora deberemos hacer lo siguiente en el:

1. Remplaza A1A1A1A1A1A1A1A1A1 por el IMSI

2. Remplaza B1B1B1B1B1B1B1B1B1B1B1B1B1B1B1B1 por el KI

Bien, ya hemos modificado el hex de la eeprom, ahora deberemos recalcular los datos del hex, para ello usaremos un programa llamado "hexcsum", este programa lo podéis por el IRC o cualquier foro de GSM, bien, cuando tengamos el programa haremos lo siguiente. Copia el hexcsum.exe a la carpeta donde tengas el GSMSIMEPP.hex, entra en esa carpeta por ms-dos y escribe: hexcsum GSMSIMEPP.HEX > GSMSIMEPP2.HEX al hacer eso se creara un archivo llamado GSMSIMEPP2.HEX, este archivo ya está listo para grabar en la eeprom.

Para grabar la tarjeta haremos lo siguiente.

Abre el IC-PROG y pulsa en el menú "comando" y en Asistente SmartCard. Se te abrirá uno para grabar la eeprom a través de la pic. Ueno, al abrirlo conectáis el t20 (el grabador de pic) con la Gold y le dais a continuar, os grabara un archivo raro llamado load. Cuando haya terminado desconectáis el t20 y conectáis el phoenix (con la gold), dais a continuar y os pedirá el archivo de la eeprom, seleccionáis el GSMSIMEPP2.HEX y dais a abrir y a continuar, os grabara la eeprom.

Cuando la eeprom ya este grabada desconectáis el phoenix y volvéis a conectar el t20 y al grabar seleccionáis el GSMSIMPIC.HEX. YA ESTA !!!!!

Ahora con un cutter o tijeras recortáis la tarjeta haciéndola coincidir con una original y a teléfono.

Un saludo

LUK

www.hackhispano.com