## La FOCA en Linux [1 de 2]

Publicado por Vicente Motos on miércoles, 15 de septiembre de 2010 Etiquetas: foca , herramientas , metadatos , series

La verdad es que la **FOCA** (**F**ingerprinting **O**rganizations with **C**ollected **A**rchives) es una de esas herramientas que me hubiese gustado tener incluso unos años antes, fundamentalmente por la cantidad de trabajo que te ahorra en algunos proyectos y auditorías.

Ahora la última versión de la FOCA es *sexy*, trae funciones nuevas y un logo cojonudo (hecho por el creador de Cálico Electrónico) y la utilizan empresas, agencias de seguridad gubernamentales, pentesters e incluso "hackers".

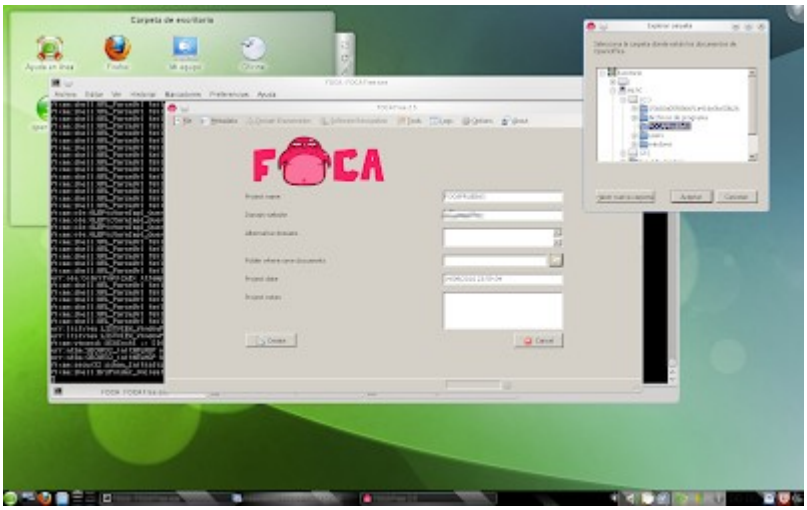
Si todavía no conoces la FOCA, decirte que es una herramienta que automatiza la recolección de información sobre una organización. Principalmente utiliza varios motores de búsqueda para descubrir ficheros en un sitio web, descargarlos y analizar sus **metadatos** descubriendo direcciones de correo electrónico, nombres de usuario, versiones de software, sistemas operativos, nombres y direcciones IP de servidores internos, impresoras, unidades de red mapeadas, etc.

También y como te comentaba, las últimas versiones añaden características nuevas a la FOCA como fingerprinting de servidores web y SMTP y DNS caché snooping, por lo que no debes de dejar de leer los manuales de usuario para conocerla en profundidad.

Además puede combinarse con otras herramientas interesantes como SET (Social Engineering Toolkit) y van apareciendo nuevas formas o hackings para utilizarla. Precisamente en este punto es cuando pensé en **ejecutar la FOCA en un sistema Linux**, no para tocar los huevos (*¡que el Maligno me perdone!*), si no para aprovechar el sistema operativo y las tools que tengo en mi portátil y ver cómo puedo utilizar la FOCA con nuevos horizontes, una FOCA entre pingüinos…

Y es que, aunque algunas diapositivas de presentaciones de la FOCA (este año Rooted CON y Defcon 18) rezan lo contrario, en cierta manera la FOCA (como muchas aplicaciones de Windows) si puede correr en Linux. Cuando escriba el siguiente artículo explicaré cómo en unos pocos pasos...


*No, no... Yes, we can!*



- Parte 1 de 2
- Parte 2 de 2

**1 comentarios :**

1. *VTacius*17 de septiembre de 2010, 6:25

   Tengo ya unas cuantas menciones acerca de este software, lástima que por ahora estoy ocupado para investigarlo. Se oye interesante.

La **FOCA** es una aplicación gratuita pero no es de código abierto. Sabemos que está programada en **C#** y que necesita el **framework .NET** para funcionar. Sólo con esto, veremos lo sencillo que es hacer que la FOCA muerda el anzuelo para que funcione en Linux…

Lo primero que se me ocurrió fue utilizar **Mono** (*¡esto parece un zoo!*), precisamente una implementación del framework .NET de Microsoft, multiplataforma y basado en los estándares ECMA para C# y el CLR (Common Language Runtime). Tras varias pruebas al final desistí y determiné que la FOCA no funcionaba (o no supe hacerla funcionar) con Mono. No obstante sí que aproveché el IDE Monodevelop para depurar el ejecutable de la FOCA en mi **Windows 7** y, a través del log de la traza de la aplicación, ver los módulos que carga en tiempo real. El objetivo: copiar las DLLs adicionales que utiliza para llevárnoslas al sistema operativo Linux:

```
10/06/2009 23:22 10.752 Accessibility.dll
19/04/2010 10:34 17.920 Microsoft.VisualStudio.HostingProcess.Utilities.Sync.dll
21/05/2010 00:49 4.550.656 mscorlib.dll
14/07/2009 10:47 307.200 mscorlib.Resources.dll
10/06/2009 23:14 110.592 SMdiagnostics.dll
10/06/2009 23:23 425.984 System.configuration.dll
10/06/2009 23:14 667.648 System.Core.dll
14/07/2009 10:48 61.440 System.Core.Resources.dll
10/06/2009 23:23 3.178.496 System.dll
10/06/2009 23:23 626.688 System.Drawing.dll
14/07/2009 10:47 204.800 system.Resources.dll
10/06/2009 23:13 970.752 System.Runtime.Serialization.dll
14/07/2009 10:48 98.304 System.RunTime.Serialization.Resources.dll
10/06/2009 23:13 5.963.776 System.ServiceModel.dll
10/06/2009 23:14 569.344 System.ServiceModel.Web.dll
10/06/2009 23:23 5.242.880 System.Web.dll
10/06/2009 23:23 5.025.792 System.Windows.Forms.dll
14/07/2009 10:47 425.984 System.Windows.Forms.Resources.dll
10/06/2009 23:23 2.048.000 System.XML.dll
14/07/2009 10:47 163.840 System.xml.Resources.dll
03/03/2010 01:24 1.249.280 WindowsBase.dll
```

Ahora sólo tenemos que buscar en el sistema las librerías listadas arriba y copiarlas al directorio de instalación de la FOCA. Una vez que tenemos todas las librerías y los ejecutables, los empaquetamos en un zip y pensamos en la otra gran alternativa: **Wine**, una reimplementación del API de Win16/32 para sistemas operativos basados en Unix.

Nos cambiamos de sistema operativo y empezamos a trabajar en Linux. He probado con las últimas versiones de Debian, Ubuntu y openSuSE. En todas ellas la FOCA funciona pero es en la última en la que todo ha ido más o menos a la primera. Nuestro ejemplo se basa por tanto en **openSuSE 11.3** con KDE y utilizar la FOCA es tan sencillo como seguir los siguientes pasos:

- Descomprimir el zip con todos los ejecutables y librerías que utiliza la FOCA
- Instalar wine:

```
# yast2 --install wine
```

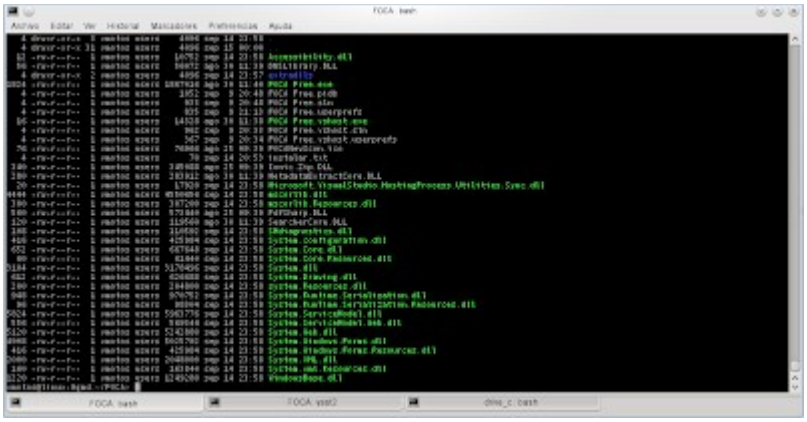
- Instalar componentes necesarios: Microsoft .NET Framework 2.0, gdiplus y fontfix (mejor con Winetricks)

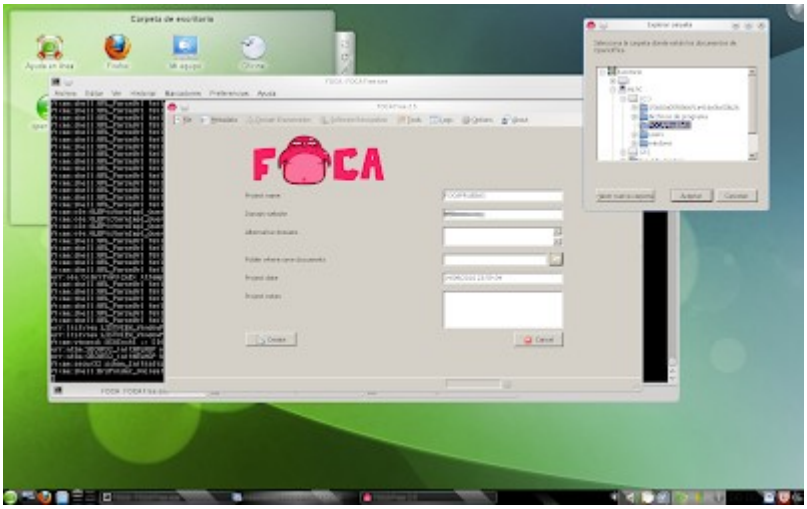
```
# winetricks dotnet20 gdiplus fontfix
```

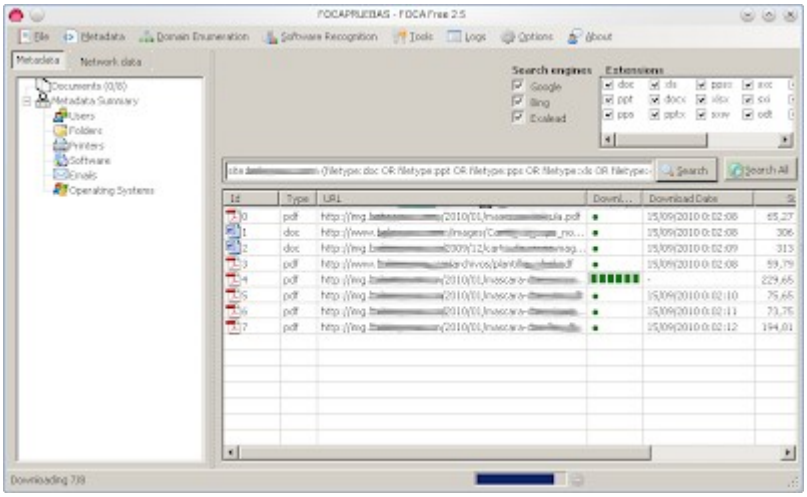
- Ejecutar la FOCA por medio de Wine

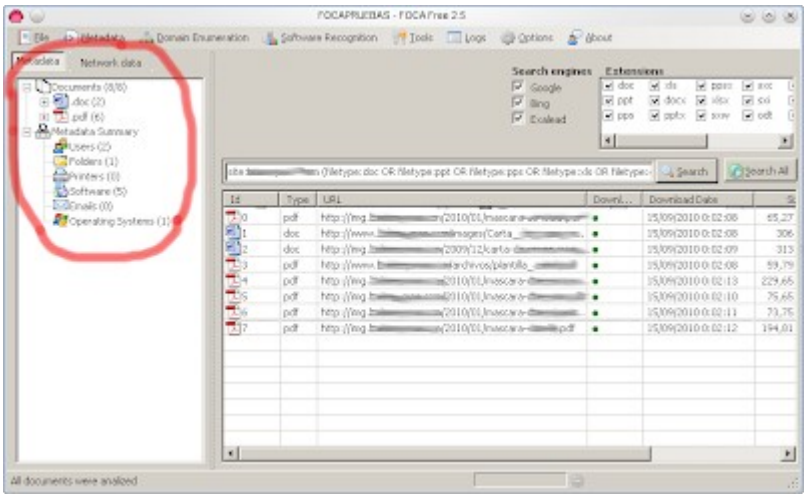
```
# wine 'FOCA Free.exe'
```

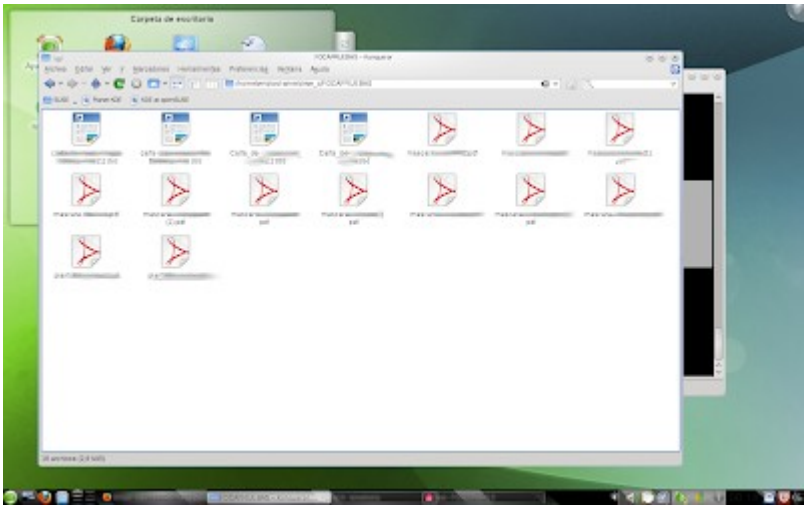
- Y , ¡divertirse!

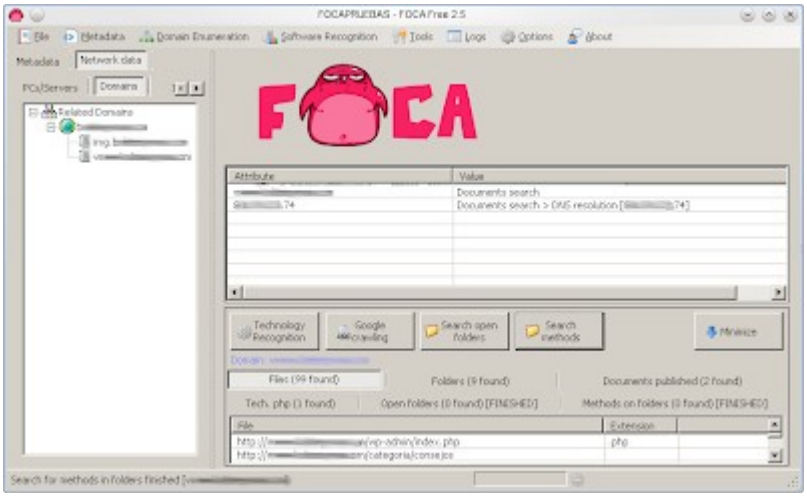





FOCAPRUEBAS - FOCA Free 2.5
File
Metadata
Domain Enumeration
Software Recognition
Tools
Logs
Options
About
Metadata
Network data
Documents (0/0)
Metadata Summary
Users
Folders
Printers
Software
Emails
Operating Systems
Search engines
Google
Bing
Exalead
Extensions
doc
xls
pps
exc
ppt
docx
xlsx
sxi
pps
pptx
sxw
odt
Search
Search All
Id
Type
URL
Downl...
Download Date
Downloading 7/9


FOCAPRUEBAS - FOCA Free 2.5
File
Metadata
Domain Enumeration
Software Recognition
Tools
Logs
Options
About
Metadata
Network data
Documents (8/8)
doc (2)
pdf (6)
Metadata Summary
Users (2)
Folders (1)
Printers (0)
Software (5)
Emails (0)
Operating Systems (1)
Search engines
Google
Bing
Exalead
Extensions
Search
Search All
Id
Type
URL
Downl...
Download Date
All documents were analized


Carpeta de escritorio



- Parte 1 de 2
- Parte 2 de 2

-

**15 comentarios :**

1. *VTacius*17 de septiembre de 2010, 6:28

   No se porque esta gente no se anima a migrarla, creo que les sería algo fácil tomando en cuenta que si las condiciones son tales... Por mi parte, la mayoría de las aplicaciones que hago en la U solo necesitan de abrirse y Voila!... Por otra parte, sería una muestra más de las cualidades del proyecto mono, que tanto descrédito ha tenido en otros blogs.

   Responder

2. *vmotos*17 de septiembre de 2010, 12:43

   Hablando de Mono, supongo que la FOCA podría llegar a funcionar completamente si se analizara el proyecto de Visual Studio con MoMA (http://mono-tools.com/Moma.aspx) y se hicieran algunas modificaciones. Además mejoraría su portabilidad porque muchas distribuciones de Linux vienen ya con Mono instalado por defecto y no sería necesario lanzarla con Wine o reescribirla en Perl como decía Chema en su blog...;-)

   Responder

3. *Anónimo*19 de octubre de 2010, 10:38

Molaría, para los que no usamos windows, un .rar con las dll's, que supongo que tendrás recopiladas, ¿no?

Responder

4. *vmotos*19 de octubre de 2010, 13:04

   Bueno.. si mola entonces puedes descargarlas en https://sites.google.com/site/h4ckpl4y3s/DllsFOCA.rar

   Saludos!

   Responder

5. 

   *Javier*7 de noviembre de 2010, 19:14

   Hola.. La instalada de foca me fue sensacional pero el problema que tengo es de como poder analizar un archivo que tengo en mi pc.. la opcion de arrastrar el archivo no va.. "No se puede arrastras" quiero sabe si ustedes han podido hacerlo y como la hace.

   Exitos y larga vida.

   Responder

6. *vmotos*9 de noviembre de 2010, 14:47

   Hola Javier. Efectivamente he comprobado que no se puede arrastrar ningún elemento o añadir con el botón derecho porque el menú contextual no aparece. Yo primero probé en Ubuntu y todo funcionaba correctamente, sin embargo la instalación era un quebradero de cabeza y por eso opté por OpenSuSE. Quizás falta instalar algún otro componente (winetricks) o es un tema de ruta o permisos. Tengo que hacer más pruebas...¿Alguien que le funcione bien en esta distribución o en otras?

   Responder

7. 

   *Javier*10 de noviembre de 2010, 4:18

Hola vmotos ya tengo la solución.. Dado el caso que no se puede arrastrar los archivos a foca y el click derecho no funciona. La única forma de hacerlo es con la tecla que hace la función del click derecho.. (La tecla se encuentra al lado de Ctrl mano derecha).Éxitos..

Responder

8. *vmotos*10 de noviembre de 2010, 15:57

   ¡Qué curioso! Muchas gracias Javier!

   Responder

9. *Carlos*19 de mayo de 2011, 19:27

   Hola!! Gracias por el aporte, pero tengo un problema con la instalación...

   wine: cannot find L"C:\\windows\\system32\\\2018FOCA.exe"

   Y gúguel no sabe nada... este archivo existe?? tal vez por usar la última versión??
   Gracias de todos modos!!

   Responder

10. *Carlos*19 de mayo de 2011, 20:26

    Arreglado... que soy un cazurro y no había descargado el .NET Framework...
    Gracias!!

    Responder

11. *Anónimo*8 de octubre de 2012, 22:06

    La foca no se migra a linux porque ya existen herramientas para todo eso lo que claro, jajaja, ponte a usarlas una por una y en tu terminal ahi, vamos, que no es tarea facil, pero haberlas ahilas y guenas mu guenas. aparte si se tiene que usar windows pues se usa windows. la etica real es usar todo lo disponible y no ser un pardillo encerrado en los comandos. si esta pa windows pues se corre en windows, pasando de perder el tiempo no? si te apetece no me meto claro. un besitooo!! jajaja

Responder

12. 

*Luciano Katze*6 de marzo de 2014, 1:15

Emm no se si es que estoy haciendo algo horriblemente mal, jeje pero no puedo >_< jaja

Responder

13. 

*James Kellerman*10 de enero de 2016, 2:38

Hola. Como se instala FOCA en Ubuntu 14.04?

Responder

14. 

*lanuit*2 de diciembre de 2016, 22:00

Buennnassss..
Creo necesitar algo de ayuda. Creo que he seguido los pasos indicados y cuando pensaba irme a cenar después de un ´wine Foca.exe' Kali me ha vomitado lo siguiente:

Unhandled exception: 0xe0434f4d in 32-bit code (0x7b83ae1c).
Register dump:
CS:0073 SS:007b DS:007b ES:007b FS:003b GS:0033
EIP:7b83ae1c ESP:0032d344 EBP:0032d3c8 EFLAGS:00000216( - -- I -A-P- )
EAX:7b827985 EBX:00000008 ECX:0032d370 EDX:0032d3f0
ESI:00000000 EDI:00000000
Stack dump:
0x0032d344: 00134f1c 1cd63819 0032d450 79f96eb3
0x0032d354: 79f949a6 0032d400 e0434f4d 00000001
0x0032d364: 00000000 7b83ae1c 00000001 80131018
0x0032d374: 00000036 790c2000 00000036 00000006
0x0032d384: 790fabcc 79e7be3f e0434f4d 0032d9f4
0x0032d394: 790c2000 02000036 0032d9a0 79e814da
Backtrace:
=>0 0x7b83ae1c in kernel32 (+0x2ae1c) (0x0032d3c8)
1 0x7f7a6511 (0x0032d408)
2 0x7a0febc8 in mscorwks (+0x28ebc7) (0x0032f1e4)
3 0x79e7d58c in mscorwks (+0xd58b) (0x0032f23c)
4 0x79e7bb73 in mscorwks (+0xbb72) (0x0032f28c)

5 0x00a501be (0x0032f2a4)
6 0x08e89ea4 (0x0032f310)
7 0x79e88f63 in mscorwks (+0x18f62) (0x0032f320)
8 0x79e88ee4 in mscorwks (+0x18ee3) (0x0032f3a0)
9 0x79e88e31 in mscorwks (+0x18e30) (0x0032f4e0)
10 0x79e88d19 in mscorwks (+0x18d18) (0x0032f5b4)
11 0x003767f8 (0x00376520)
12 0x20200009 (0x09052c9f)
0x7b83ae1c: addl $12,%esp
Modules:
Module Address Debug info Name (40 modules)
PE 400000- 93a000 Deferred foca
PE 30e0000- 3d66000 Deferred system.windows.forms.ni
PE 8a00000- 8aa4000 Deferred metadataextractcore
PE 8b60000- 8b9a000 Deferred dnslibrary
PE 5e380000-5e409000 Deferred diasymreader
PE 64020000-64033000 Deferred mscorsec
PE 641f0000-6420d000 Deferred shfusion
PE 69be0000-6a148000 Deferred system.xml.ni
PE 70d00000-70e91000 Deferred gdiplus
PE 79000000-79045000 Deferred mscoree
PE 79060000-790b3000 Deferred mscorjit
PE 790c0000-79ba6000 Deferred mscorlib.ni
PE 79e70000-7a3d1000 Export mscorwks
PE 7a440000-7abfe000 Deferred system.ni
PE 7ade0000-7af74000 Deferred system.drawing.ni
PE 7b810000-7b9b0000 Export kernel32
PE 7bc10000-7bc14000 Deferred ntdll
PE 7ebf0000-7ebf4000 Deferred shfolder
PE 7ed10000-7ed14000 Deferred psapi
PE 7ed70000-7ed74000 Deferred rpcrt4
PE 7ee00000-7ee08000 Deferred ole32
PE 7ef30000-7ef34000 Deferred ws2_32
PE 7ef70000-7f0cf000 Deferred shell32
PE 7f1a0000-7f1aa000 Deferred mpr
PE 7f1c0000-7f1d8000 Deferred wininet
PE 7f240000-7f243000 Deferred cryptnet
PE 7f250000-7f254000 Deferred rsaenh
PE 7f290000-7f293000 Deferred imagehlp
PE 7f2b0000-7f2b4000 Deferred uxtheme
PE 7f4e0000-7f4e3000 Deferred softpub
PE 7f4f0000-7f4f4000 Deferred winex11

PE 7f580000-7f5af000 Deferred comctl32
PE 7f680000-7f6c1000 Deferred crypt32
PE 7f750000-7f754000 Deferred wintrust
PE 7f850000-7f854000 Deferred imm32
PE 7fa20000-7fa24000 Deferred version
PE 7fa50000-7fa57000 Deferred gdi32
PE 7fb70000-7fbab000 Deferred user32
PE 7fcb0000-7fcb8000 Deferred shlwapi
PE 7fd30000-7fd34000 Deferred advapi32
Threads:
process tid prio (all id:s are in hex)
00000008 (D) Z:\root\Escritorio\FocaPro\bin\FOCA.exe
0000002f 0
0000002e 0
0000002d 2
0000002c 0
00000009 0 <==
0000000e services.exe
00000026 0
00000025 0
0000001e 0
00000010 0
0000000f 0
00000014 explorer.exe
0000002b 0
0000002a 0
00000029 0
00000015 0
0000001c winedevice.exe
00000024 0
00000021 0
00000020 0
0000001d 0
00000022 plugplay.exe
00000028 0
00000027 0
00000023 0
System information:
Wine build: wine-1.8.5 (Debian 1.8.5-1)
Platform: i386
Version: Windows 5.1 (0)
Host system: Linux

Host version: 4.6.0-kali1-686-pae

Creo que me quedo sin cena hoy.
Alguien al otro lado que me arroje algo de luz ??

Muchas gracias!!

Responder
Respuestas

1. *Anónimo*16 de noviembre de 2017, 19:31

   Eso me pasa a mi .... lo solucionastes??