



OWASP

Open Web Application  
Security Project

# 101 Sombras del Malware

Israel Aráoz Severiche

**C|EH,C|HFI, LA27001**



**@iara0z**

**Defenet**  
Information Technology Security  
Information Technology Security

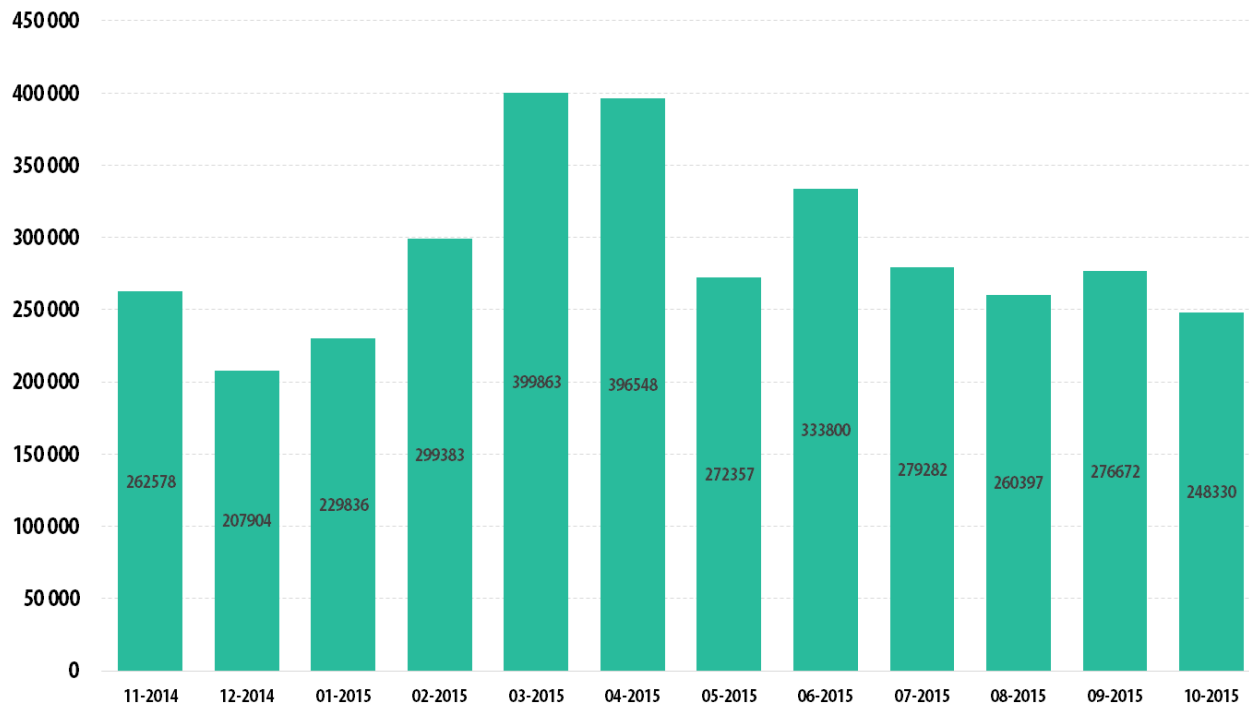
# Agenda

- Situación Actual
- Objetivo del Análisis de Malware
- Tipos de Análisis
- Estático
- Dinámico
- Preguntas

# Nslookup Israel.araoz

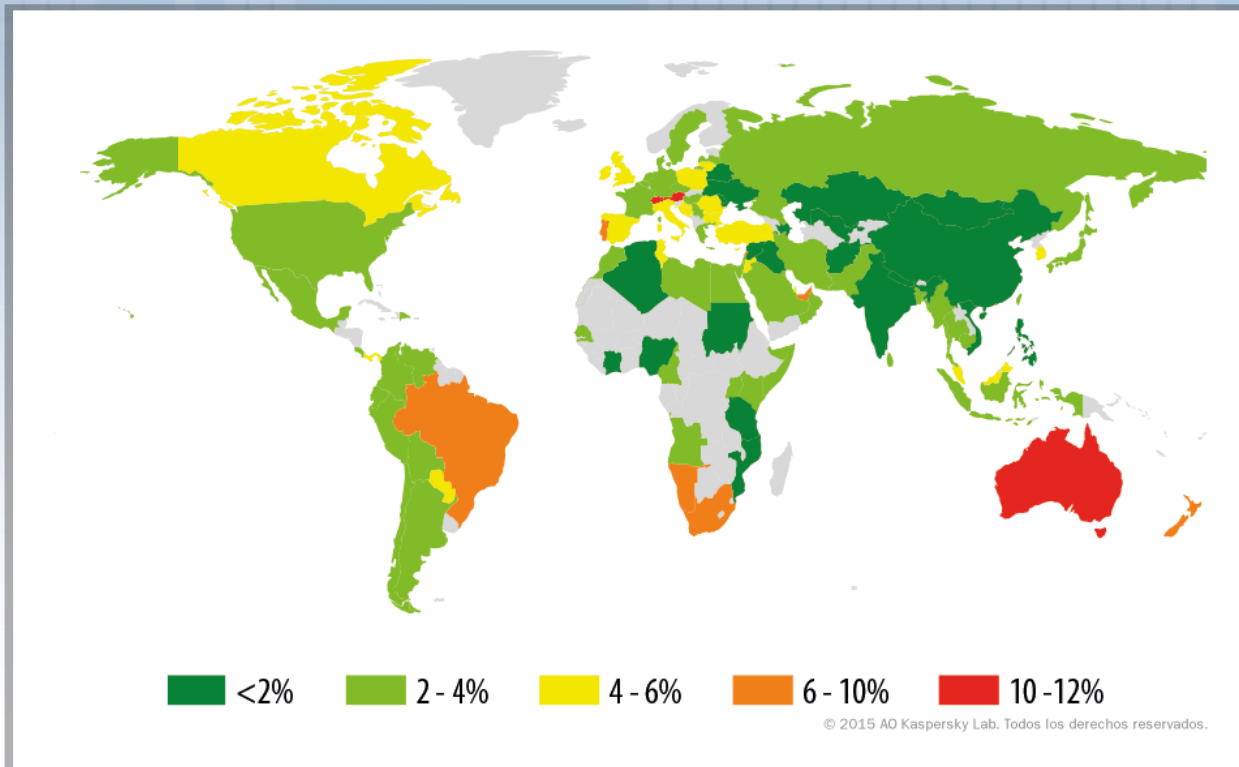
- Ing. Sistemas
- Esp. Seguridad Informática
- Certified Ethical Hacker
- Computer Hacking Forensic Investigator
- PECB Lead Auditor ISO 27001
- Miembro ACK Security

# Situación Actual



© 2015 AO Kaspersky Lab. Todos los derechos reservados.

# Situación Actual




# Situación Actual

TECNOLOGÍA   MOVILIDAD   CIENCIA   ELECTRÓNICA   ESTILO DE VIDA

Tesla Model 3   Triviatech   Windows 10   Guías MC   Motor

## Hospital afectado por ransomware paga rescate de 40 bitcoins



NO

Real  
aum  
nec

+VI

nv

Isidro Ros | 18 de febrero, 2016 | 7 comentarios

# Situación Actual

## CAZADOR DE MALWARE CONFIRMA QUE TELÉFONO DE NISMAN ESTABA INFECTADO

Un experto en seguridad informática de Estados Unidos confirmó que Alberto Nisman fue espiado por seis semanas antes de su muerte a través de un virus troyano encontrado en el celular del fiscal que permitía escuchar llamadas, capturar la pantalla e interceptar mensajes.

7 agosto, 2015

0 Comentarios



El "cazador de malware", Morgan Marquis-Boire, que escribe en sitios contraculturales como Vibe y The Intercept, anunció ayer durante la conferencia "Black Hat" en Las Vegas que analizó personalmente el troyano que infectó el celular de Nisman y confirmó que se trata de AlienSpy, una herramienta de acceso remoto que permite interceptar llamadas.

El malware había sido descubierto durante las pericias que ordenó la fiscal Fein tras la muerte de Nisman. Sin embargo, los peritos informáticos negaron en ese entonces que permitiera escuchar las llamadas, aunque reconocieron sus limitaciones para determinar los alcances del troyano.

Como explicó el sitio Vice, tras analizar el virus, Marquis-Boire buscó el nombre bajo el cual el troyano ingresó al celular del fiscal en un repositorio online, donde se listan aquellos archivos que fueron detectados por software

antivirus y antimalware.





# Situación Actual

**.Seguridad**

Cultura de prevención para TI

Portada

REVISTA .SEGURIDAD, DEFENSA DIGITAL | 1 251 478, 1 251 477 | REVISTA BIMESTRAL

## CPL Malware y su alcance en Brasil

Escrito por [Matías Porolli](#), [Pablo Ramos](#) | publicado el Lun, 15/06/2015 - 12:55 [numero-24](#) [Brasil](#) [CPL](#) [archivo ejecutable](#) [malware](#) [troyano](#) [troyano bancario](#)



Durante la primera semana de mayo, desde el Laboratorio de ESET Latinoamérica, publicamos un artículo relacionado a una de las investigaciones desarrolladas en la región, la implementación de troyanos bancarios propagados como archivos CPL en Brasil. En el [artículo completo](#) encontrarán el análisis técnico de estas amenazas y las principales particularidades de sus algoritmos de cifrado. En este texto vamos a analizar la evolución a lo largo del tiempo en cuanto a la actividad de este tipo de archivos en la región latinoamericana, correspondiente a una parte del artículo publicado.

# Objetivo del Análisis de Malware

- **Proporcionar Información que permita responder cuestiones en relación a una intrusión en una red, incidentes de seguridad, ataques dirigidos.**
- **Determinar lo que un binario sospecho puede llegar hacer como:**
  - **Modificación al S.O (User Space , Kernel Space)**
  - **Trafico de Red (Dropper)**
  - **Permisos**
  - **Secuestro de Información (Criptoanálisis)**

# Tipos de Análisis del Malware

- Análisis
- Análisis



A problem has been detected and windows has been shut down to prevent damage to your computer.

The end-user manually generated the crashdump.

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

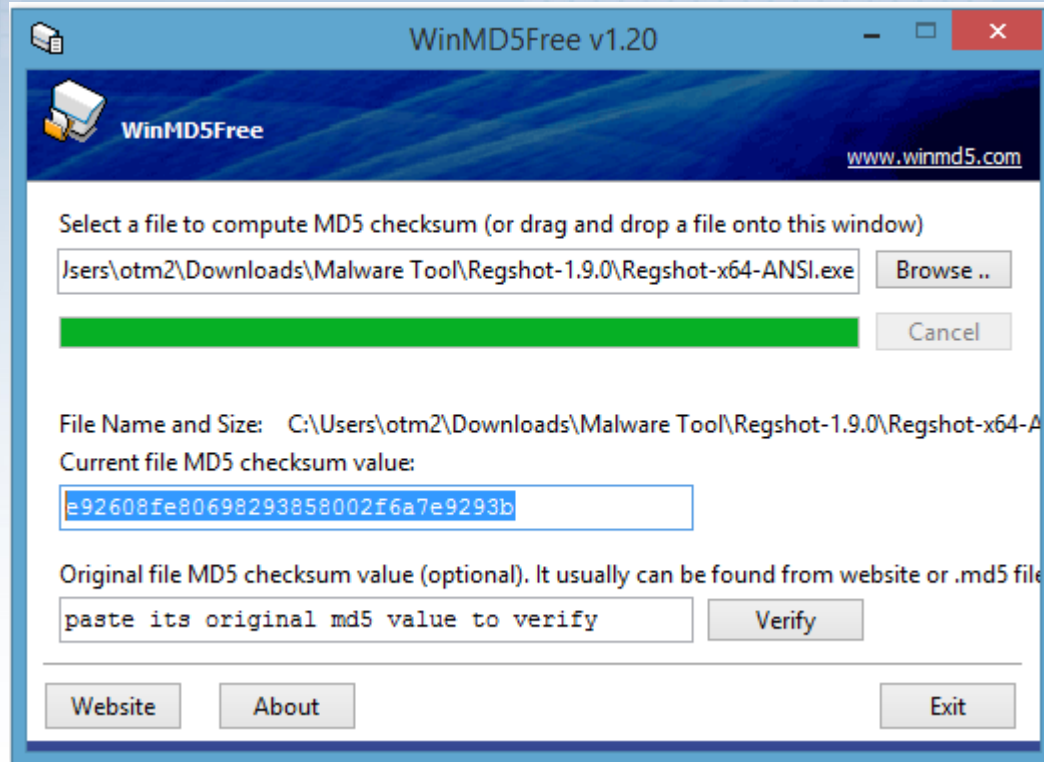
\*\*\* STOP: 0x000000E2 (0x00000000,0x00000000,0x00000000,0x00000000)

Beginning dump of physical memory

Physical memory dump complete.

Contact your system administrator or technical support group for further assistance.

# Hashing



# Identificando dependencias (DLL, funciones y otras cosas...)

The screenshot shows the Dependency Walker application for ILSPY.EXE. The dependency tree on the left shows the following structure:

- ILSPY.EXE (1)
- MSCOREE.DLL
- KERNEL32.DLL
- USER32.DLL
- OLEAUT32.DLL
- MSVCRT.DLL
- NTDLL.DLL
- COMBASE.DLL
- API-MS-WIN-CORE-REGISTRY-L1-1-0.DLL
- API-MS-WIN-CORE-COM-L1-1-1.DLL
- API-MS-WIN-CORE-LOCALIZATION-L1-2-1.DLL
- API-MS-WIN-CORE-SYNCH-L1-2-0.DLL
- API-MS-WIN-CORE-STRING-L1-1-0.DLL
- API-MS-WIN-CORE-PROCESSENvironment-L1-2-0.DLL

Numbered arrows indicate the following actions:

- 1: Selecting ILSPY.EXE in the tree.
- 2: Expanding the tree to show dependencies.
- 3: Clicking on USER32.DLL in the tree.
- 4: Clicking on the function list table.
- 5: Clicking on the Module list table.

The function list table shows the following data:

PI	Ordinal ^	Hint	Function	Entry Point
☑	N/A	N/A	GetProcessWindowStation	Not Bound
☑	N/A	N/A	GetObjectInformationW	Not Bound
☑	N/A	N/A	MessageBoxW	Not Bound
☑	N/A	N/A	LoadStringW	Not Bound

The function list table also shows the following data:

E	Ordinal ^	Hint	Function	Entry Point
0#	1502 (0x05DE)	N/A	N/A	0x00059A10
☑	1503 (0x05DF)	0 (0x0000)	ActivateKeyboardLayout	0x00036160
☑	1504 (0x05E0)	1 (0x0001)	AddClipboardFormatListener	0x00036180
☑	1505 (0x05E1)	2 (0x0002)	AdjustWindowRect	0x000244D0
☑	1506 (0x05E2)	3 (0x0003)	AdjustWindowRectEx	0x0001E450
☑	1507 (0x05E3)	4 (0x0004)	AlignRects	0x00080CE0
☑	1508 (0x05E4)	5 (0x0005)	AllowForegroundActivation	0x00054990

The Module list table shows the following data:

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU
SHCORE.DLL	23/01/2015 01:02a	22/01/2015 10:47p	560.392	A	0x0008DBDA	0x0008DBDA	x86
SHLWAPI.DLL	20/11/2014 07:18p	28/10/2014 08:43p	278.352	A	0x00049E52	0x00049E52	x86
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	22/08/2013 12:17a	22/08/2013 12:17a	3.584	HA	0x00007682	0x00007682	x86
API-MS-WIN-CORE-COMM-L1-1-0.DLL	22/08/2013 12:14a	22/08/2013 12:14a	3.584	HA	0x0000EAEF	0x0000EAEF	x86
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	22/08/2013 12:14a	22/08/2013 12:14a	3.584	HA	0x000090A4	0x000090A4	x86
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL	22/08/2013 12:14a	22/08/2013 12:14a	4.096	HA	0x00001528	0x00001528	x86

# DLL Comunes

DLL	Descripción
Kernel32.dll	Diferentes funcionalidad como manipulación de memoria, archivos y hardware.
Advapi32.dll	Proporciona acceso a Registro de Windows y a la Gestor de Servicios del S.O
Use32.dll	Acceso a la Interfaz de usuario, tales como botones, barra de desplazamiento, componentes para controlar y responder a las acciones del Usuario.
Gdi32.dll	Manipulación de gráficos
Ntdll.dll	Interfaz al Kernel de Windows, es utilizado para funciones no comunes , acceso a manipulación de procesos. (Rootkit)
Wsock32.dll Ws2_32.dll	Acceso a funcionalidades de red , conexión , creación de socket, transferencia de archivos.
Wininet.dll	Funciones “higher-level” protocolos como FTP,HTTP and NTP

# PE - Ejecutable de Windows

Ejecutable	Descripción
.text	Código del ejecutable (Instrucciones del CPU)
.rdata	Datos de solo lectura, accedidos de forma global por el programa.
.data	Almacena los datos globales accedidos durante la ejecución de la aplicación.
.idata	Almacena información de importación de funciones.
.edata	Almacena información de exportación de funciones.
.pdata	Solo para ejecutables de 64 bits y almacena información sobre excepciones.
.rsrc	Almacena recursos necesarios del ejecutable (Iconos, Imágenes y cadenas)
.reloc	Información sobre archivos DLL



# PEView

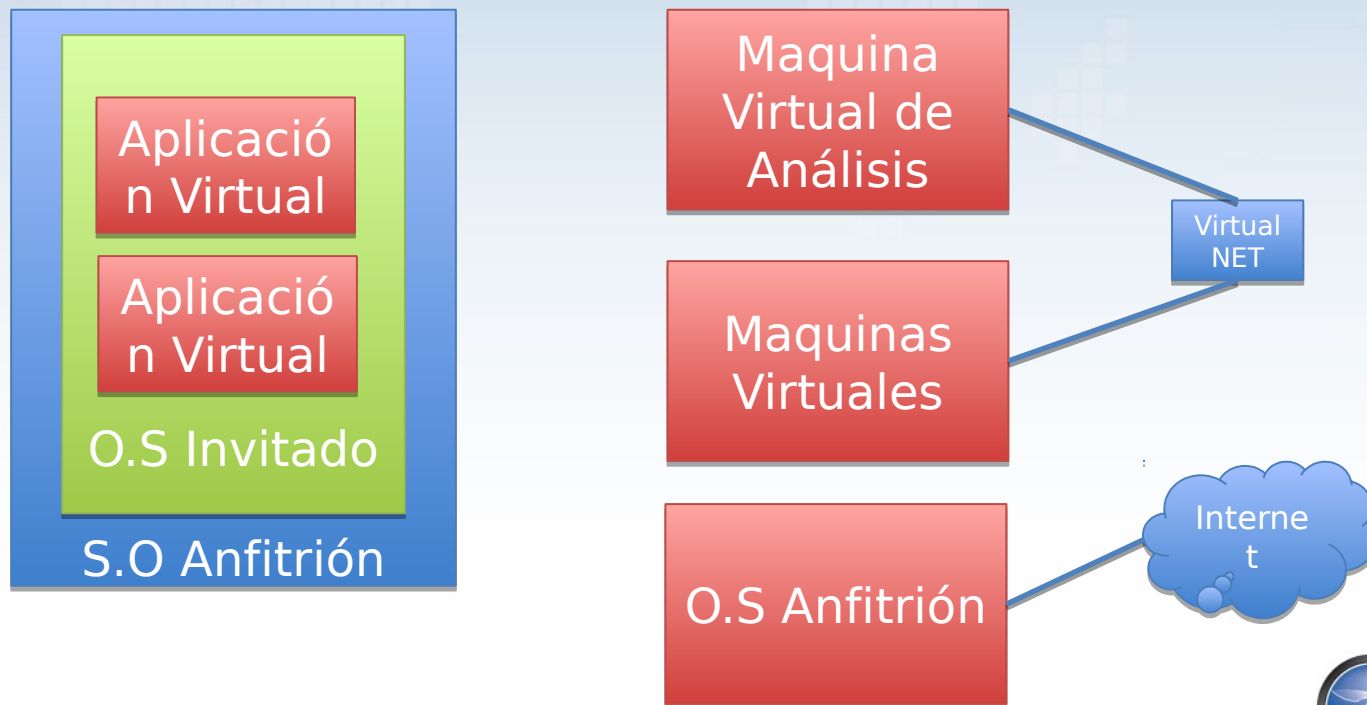
	pFile	Data	Description	Value
... IMAGE_DOS_HEADER	00000084	014C	Machine	IMAGE_FILE_MACHINE_I386
... MS-DOS Stub Program	00000086	0004	Number of Sections	
... IMAGE_NT_HEADERS	00000088	50214653	Time Date Stamp	2012/08/07 mar 16:46:11 UTC
... Signature	0000008C	00000000	Pointer to Symbol Table	
... IMAGE_FILE_HEADER	00000090	00000000	Number of Symbols	
... IMAGE_OPTIONAL_HEADER	00000094	00E0	Size of Optional Header	
... IMAGE_SECTION_HEADER .text	00000096	010E	Characteristics	
... IMAGE_SECTION_HEADER .sdata			0002	IMAGE_FILE_EXECUTABLE_IMAGE
... IMAGE_SECTION_HEADER .rsrc			0004	IMAGE_FILE_LINE_NUMS_STRIPPED
... IMAGE_SECTION_HEADER .reloc			0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
... SECTION .text			0100	IMAGE_FILE_32BIT_MACHINE
... SECTION .sdata				
... SECTION .rsrc				
... SECTION .reloc				
... IMAGE_BASE_RELOCATION				

# Cuando lo básico no alcanza..



# Implementando un entorno seguro

- Un entorno virtual minimiza el riesgo de infección en un análisis.



# Comparando Llaves del Registro

- Generar un archivo con la configuración actual del Editor de Registro.
- Ejecutar el Malware
- Generar una imagen del editor de

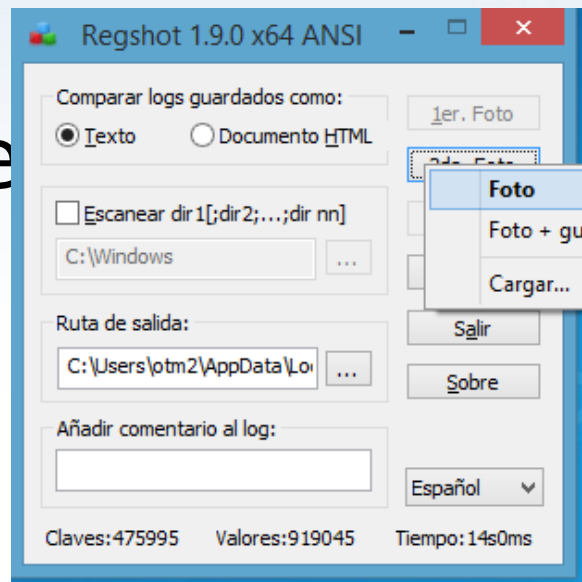
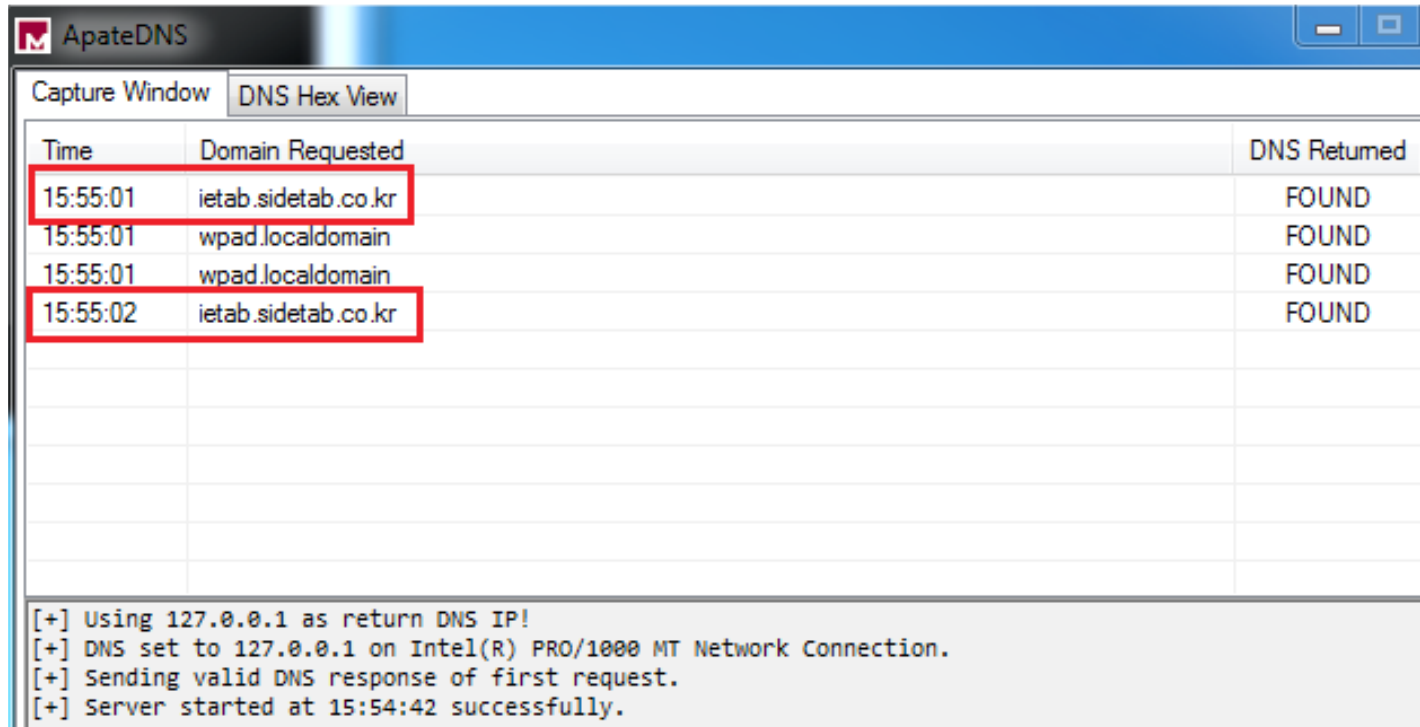


Imagen del

# ApateDNS



The screenshot shows the ApateDNS application window. The title bar reads "ApateDNS". Below the title bar, there are two tabs: "Capture Window" and "DNS Hex View". The "Capture Window" tab is active, displaying a table with three columns: "Time", "Domain Requested", and "DNS Returned". The table contains four rows of data, with the first and fourth rows highlighted with red boxes. Below the table, there is a log area with several status messages.

Time	Domain Requested	DNS Returned
15:55:01	ietab.sidetab.co.kr	FOUND
15:55:01	wpad.localdomain	FOUND
15:55:01	wpad.localdomain	FOUND
15:55:02	ietab.sidetab.co.kr	FOUND

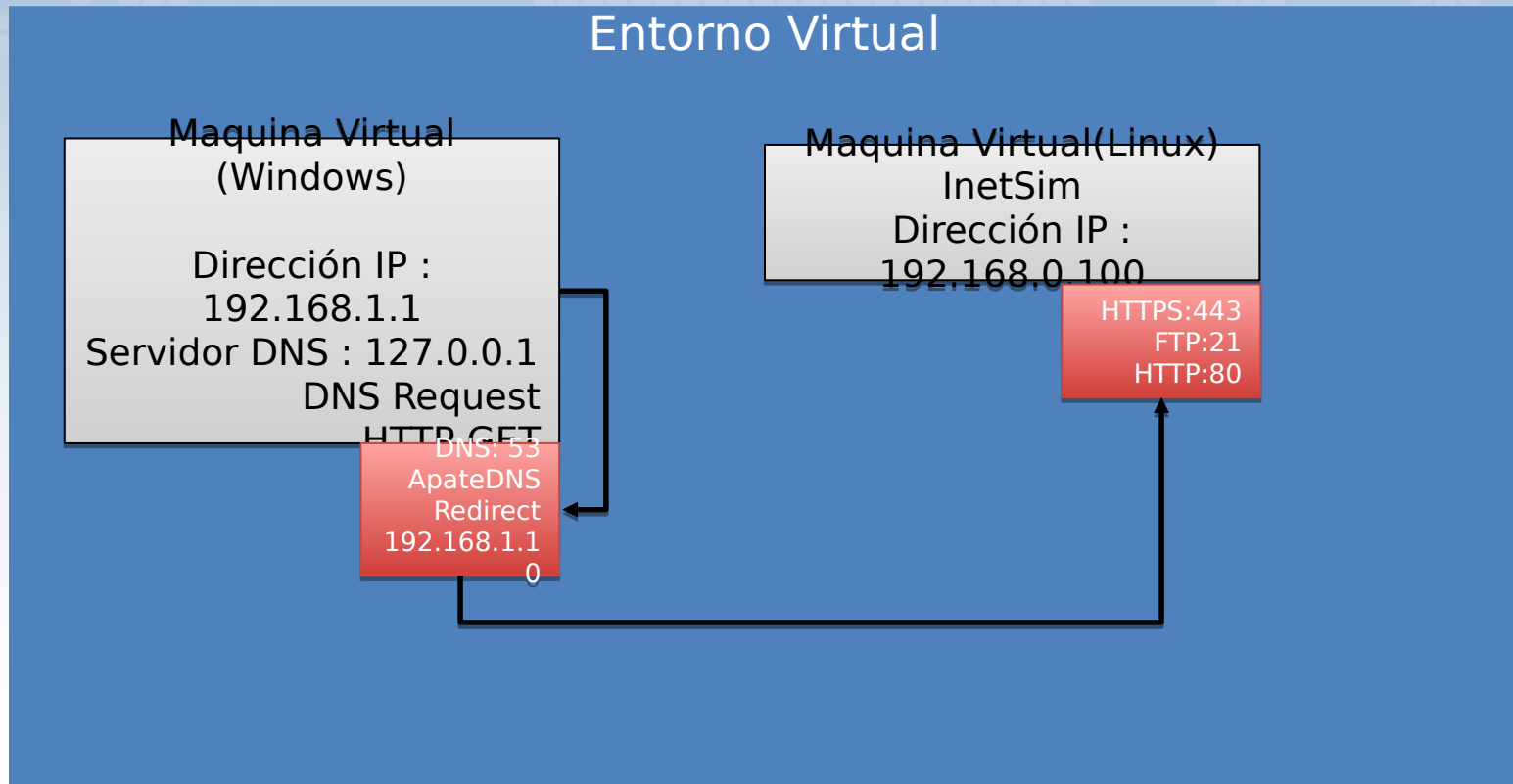
[+] Using 127.0.0.1 as return DNS IP!  
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Network Connection.  
[+] Sending valid DNS response of first request.  
[+] Server started at 15:54:42 successfully.

# InetSIM

```
[2] 7976
[root@KVM inetsim-1.2.4]# INetSim 1.2.4 (2013-08-15) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /MiT/inetsim-1.2.4/log/
Using data directory:    /MiT/inetsim-1.2.4/data/
Using report directory:  /MiT/inetsim-1.2.4/report/
Using configuration file: /MiT/inetsim-1.2.4/conf/inetsim.conf
Parsing configuration file.
Warning: Service 'https' listed, but no SSL support at line 31
Warning: Service 'smtps' listed, but no SSL support at line 33
Warning: Service 'pop3s' listed, but no SSL support at line 35
Warning: Service 'ftps' listed, but no SSL support at line 37
Configuration file parsed successfully.
=== INetSim main process started (PID 7976) ===
Session ID:      test
Listening on:    192.168.0.100

Forking services...
* dns_53_tcp_udp - started (PID 7978)
* irc_6667_tcp   - started (PID 7984)
* ntp_123_udp    - started (PID 7985)
* finger_79_tcp  - started (PID 7986)
* time_37_tcp    - started (PID 7989)
```

# Análisis Dinámico



# TCP Stream

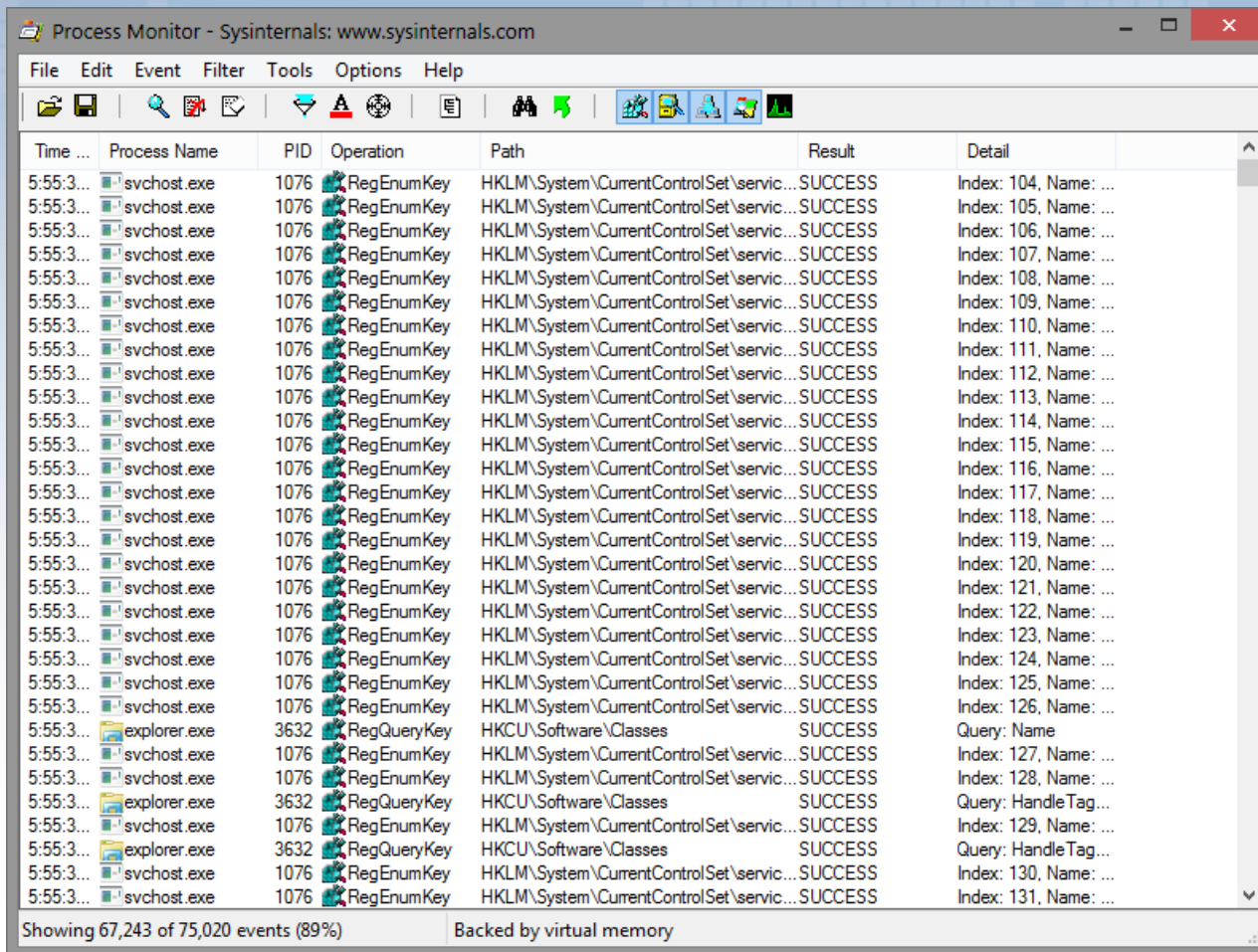
```
CONNECT cse.google.com:443 HTTP/1.1
Host: cse.google.com:443
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.110 Safari/537.36

HTTP/1.1 200 Connection Established
Date: Fri, 08 Apr 2016 21:42:38 GMT
Proxy-Connection: Keep-Alive
Via: 1.1 SYPFBOFCPX03.rd.local

.....UDP.....M...j.B...kB:.TV}..
.. .m..x...d.y.t.j...Un.....:T.....+./.....
... ..5./..
.....cse.google.com.....#...,'8x%..Pb.f.NU.k.....3..'|. ....h.k|6/P.....e.FcN.0".6.H.)wK..8B...7[...
T.?.9.K.4.G.e.e.a}..h.W.>|...M.m.-...?.....O>...*Mv9..$.R~.K....<;.....d.& .g.p..F.;Cu..c.<...L...Bo}y.4].{.....
.....3t.....h2.spdy/3.1.http/1.1uP.....
.....U.....Q...M..W.%.....!..s
..<...C.r&<$}.p&. .m..x...d.y.t.j...Un.....:T.....(,=.^..8
z...F.....:L...?.B.nS.x.U.>.<d.d.....(.....Y.Tu..e._.
N..t.tE_*=10d&.K...A.
```



# Explorador de Procesos



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

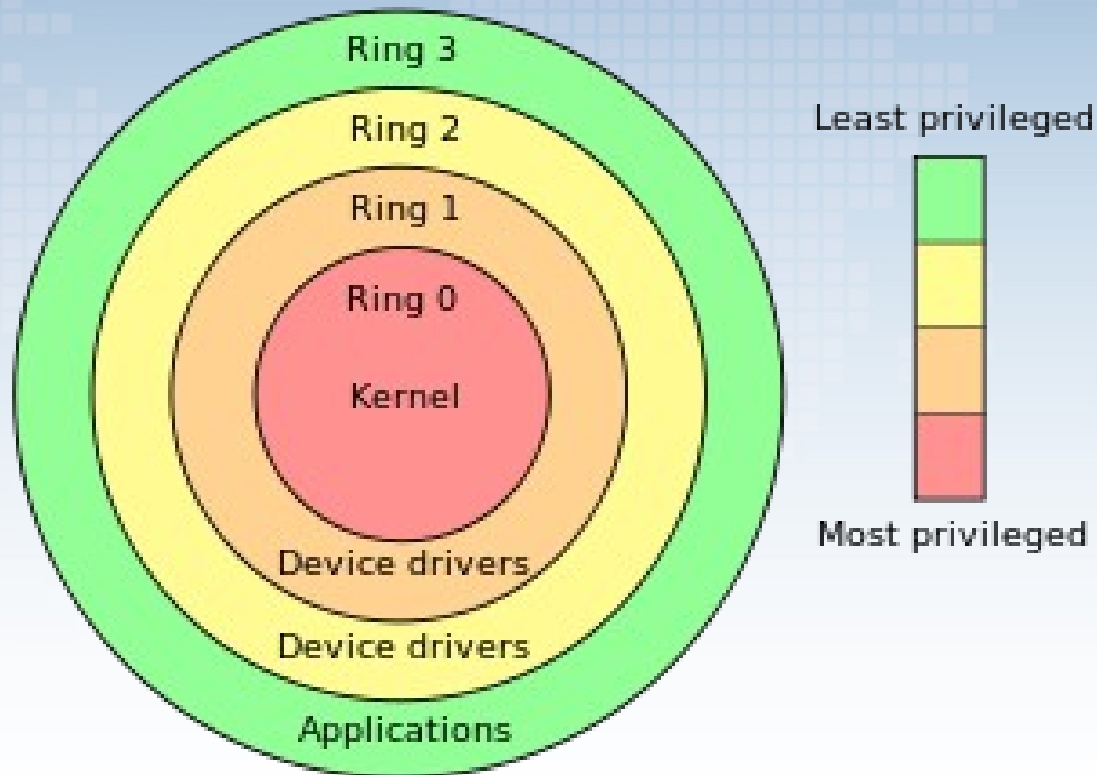
Time ...	Process Name	PID	Operation	Path	Result	Detail
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 104, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 105, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 106, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 107, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 108, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 109, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 110, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 111, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 112, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 113, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 114, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 115, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 116, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 117, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 118, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 119, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 120, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 121, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 122, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 123, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 124, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 125, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 126, Name: ...
5:55:3...	explorer.exe	3632	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 127, Name: ...
5:55:3...	explorer.exe	3632	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 129, Name: ...
5:55:3...	explorer.exe	3632	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 130, Name: ...
5:55:3...	svchost.exe	1076	RegEnumKey	HKLM\System\CurrentControlSet\servic...	SUCCESS	Index: 131, Name: ...

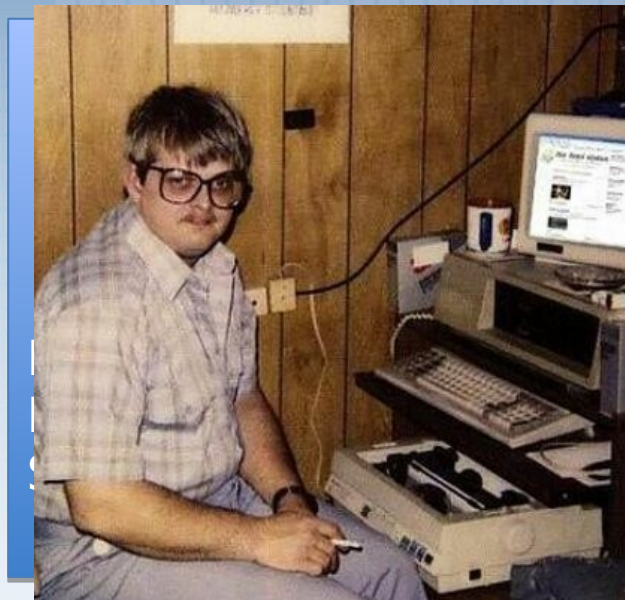
Showing 67,243 of 75,020 events (89%)      Backed by virtual memory



Existen algunas condiciones previas en materia de “lectura”  
Para este tipo de Análisis...

# Entendiendo....





## Como lo veo la CPU

55  
8B EC  
8B EC 40

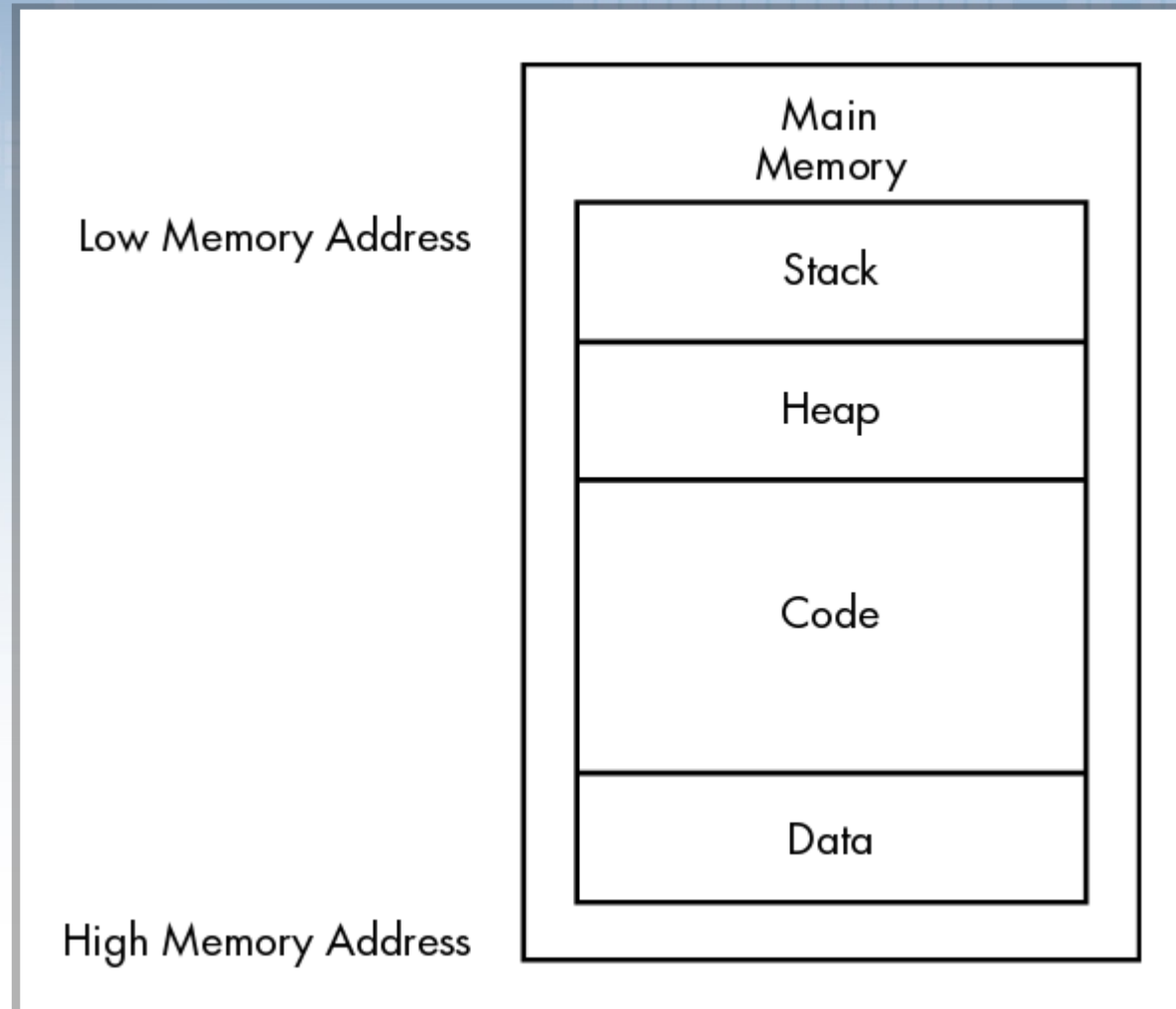
# Stack...

- **Data** : Segmento de la memoria donde se almacenan valores “estáticos” o valores Globales (Constantes, variables Globales)
- **Code** : Este segmento controla lo “que hace” el programa, Instrucciones ejecutadas por la “CPU”

# Stack

- **Heap** : Segmento de la memoria que almacena información “dinámica”, variables que solo son utilizadas en determinadas funciones.
- **“Stack”** : Utilizada para almacenar variables locales, parámetros de funciones y controlar el flujo de la ejecución del ejecutable

# La memoria Principal



# Ensamblador

- Registros (EAX, ECX, EDX, EBX, ESP, EBP, ESI, EDI)
- Saltos Condicionales(JNZ, JZ, JE,JNZ)
- Banderas (ZF,CF,SF,T

cmp dst, src	ZF	CF
dst = src	1	0
dst < src	0	1
dst > src	0	0

mov eax, ebx

Copies the contents of EBX into the EAX register

mov eax, 0x42

Copies the value 0x42 into the EAX register



# IDA Pro

The screenshot displays the IDA Pro interface with the following components:

- Debugger:** Library loaded: C:\WINNT\system32\NTDLL.DLL, C:\WINNT\system32\ADVAPI32.dll, C:\WINNT\system32\KERNEL32.DLL
- Threads:** Thread 00000350, Line 1 of 1
- IDA View-EIP:** Assembly code listing instructions such as `call ds:InitCommonControls`, `test eax, eax`, `jnz short loc_43124E`, `push ds:lpSt`, `call ds:MessageBoxA`, and `mov eax, dword_45A1C4`. The instruction `mov eax, dword_45A1C4` is highlighted in blue.
- IDA View-ESP:** Stack view showing memory addresses and values, including `var_4 dd 65h`, `retaddr dd 43CC53h`, and `Stack_PAGE_ dd 12D9C4h`.
- General registers:** Register values including `EAX: 00000001`, `EBX: 7FFDF000`, `ECX: 00000065`, `EDX: 77FD0170`, `ESI: 00000000`, `EDI: 0012D9C4`, `EBP: 0012FF34`, `ESP: 0012FF34`, `EIP: 00431219`, and `EFL: 00000206`.

<code>int a = 0;</code>	00401006	<code>mov [ebp+var_4], 0</code>
<code>int b = 1;</code>	0040100D	<code>mov [ebp+var_8], 1</code>
<code>a = a + 11;</code>	00401014	<code>mov eax, [ebp+var_4]</code>
<code>a = a - b;</code>	00401017	<code>add eax, 0Bh</code>
<code>a--;</code>	0040101A	<code>mov [ebp+var_4], eax</code>
<code>b++;</code>	0040101D	<code>mov ecx, [ebp+var_4]</code>
<code>b = a % 3;</code>	00401020	<code>sub ecx, [ebp+var_8]</code>
	00401023	<code>mov [ebp+var_4], ecx</code>
	00401026	<code>mov eax, [ebp+var_4]</code>
	00401029	<code>sub edx, 1</code>
	0040102C	<code>mov [ebp+var_4], edx</code>
	0040102F	<code>mov eax, [ebp+var_8]</code>
	00401032	<code>add eax, 1</code>
	00401035	<code>mov [ebp+var_8], eax</code>
	00401038	<code>mov eax, [ebp+var_4]</code>
	0040103B	<code>cdq</code>
	0040103C	<code>mov ecx, 3</code>
	00401041	<code>idiv ecx</code>
	00401043	<code>mov [ebp+var_8], edx</code>

# Pasando de C a Ensamblador

```
int x = 1;  
int y = 2;
```

```
if(x == y){
```

```
    printf("x equals y.\n");
```

```
}else{
```

```
    printf("x is not equal to y.\n");
```

```
}
```

```
00401006
```

```
    mov     [ebp+var_8], 1
```

```
0040100D
```

```
    mov     [ebp+var_4], 2
```

```
00401014
```

```
    mov     eax, [ebp+var_8]
```

```
00401017
```

```
    cmp     eax, [ebp+var_4]
```

```
0040101A
```

```
    jnz     short loc_40102B
```

```
0040101C
```

```
    push   offset aXEqualsY_ ; "x equals y.\n"
```

```
00401021
```

```
    call   printf
```

```
00401026
```

```
    add     esp, 4
```

```
00401029
```

```
    jmp     short loc_401038
```

```
0040102B loc_40102B:
```

```
0040102B
```

```
    push   offset aXIsNotEqualToY ; "x is not equal to y.\n"
```

```
00401030
```

```
    call   printf
```

# Pregunta 1

- ¿Cuales son los 2 tipos de Análisis ?



# Pregunta 2

- Nombre de la Herramienta utilizada para resolver peticiones DNS de



# Pregunta 3

- ¿Para que sirve la herramienta



# ¿Preguntas ?



# GRACIAS!

