ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ANÁLISIS DE ARCHIVOS DE ORIGEN DESCONOCIDO"

INFORME DE MATERIA DE GRADUACIÓN

Previa a la obtención del Título de:
"LICENCIATURA EN REDES Y SISTEMAS OPERATIVOS"

Presentada por:
GABRIELA DEL ROCIO RIVERA LOZANO
DAYANA ELIZABETH VERA RIVAS

GUAYAQUIL – ECUADOR

AÑO
2013

AGRADECIMIENTO

Me complace de sobre manera a través de este proyecto exteriorizar un infinito y sincero agradecimiento a mi Padre Celestial, por su guía y amor a lo largo mi vida, mis objetivos y metas.

A mi familia en especial a mi madre Paquita Lozano que con su infinito amor y fortaleza fue un pilar fundamental a lo largo de mis estudios.

A la familia Lozano Bajaña a quienes gracias a su apoyo incondicional y cariño y confianza no permitieron que desista de mis objetivos.

A mi compañera de Tesis Dayana, a mis amigos, compañeros y profesores que fueron parte importante de mi crecimiento profesional, por su tiempo y paciencia.

A la Escuela Superior Politécnica del Litoral por entereza, exigencia y la oportunidad que me brindo de ser una profesional.

Gabriela Rivera Lozano

Agradezco ante todo a Jehová por darme esa fortaleza necesaria para seguir adelante.

A mi familia que han sido y siguen siendo el respaldo incondicional, a todas las personas que me han brindado su apoyo y amistad a lo largo de toda mi carrera universitaria.

A ti Gaby gracias por tu ayuda para realizar este proyecto.

Dayana Vera Rivas

DEDICATORIA

A mi madre

Gabriela Rivera Lozano

A mis padres que son la base fundamental en todos los logros alcanzados en mi vida por apoyarme en todo momento por su amor y su sacrificio permanente.

Dayana Vera Rivas

TRIBUNAL DE SUSTENTACIÓN

_____

Ing. Karina Astudillo

PROFESOR DE MATERIA DE GRADUACIÓN

_____

Ing. Miguel Molina

PROFESOR DELEGADO POR EL DECANO DE LA FACULTAD

D E C L A R A C I Ó N E X P R E S A

"La responsabilidad del contenido de este Trabajo de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

(Reglamento de Graduación de la ESPOL)

Gabriela Rivera Lozano

Dayana Vera Rivas

RESUMEN

Este proyecto consistió en el exhaustivo análisis y obtención de información sobre archivos de origen desconocido para su revisión. Así encontrar información vital que permita descubrir pautas, acciones y procesos realizados al ejecutar los mismos, empleando métodos que distorsionen en lo menos posible los datos, con el objetivo de reconstruir todos los eventos posibles.

Se tiene como indicio que varios sistemas de Windows de una organización fueron comprometidos recientemente. Equipos en respuesta a estos incidentes tomaron las medidas necesarias para responder y proteger la red, durante la respuesta al incidente inicial se obtuvieron imágenes forenses, y el archivo sak.exe fue encontrado en varios sistemas, el objetivo es determinar todo lo que pueda acerca de este ejecutable.

Estas revisiones se hacen sobre y desde sistemas operativos Windows y Linux utilizando herramientas forenses existentes, contando con la imprescindible ayuda de aplicaciones web en la verificación de los resultados expuestos en el presente documento, se abordan técnicas de forensia usando comandos y distintas aplicaciones.

Se parte en la metodología utilizada en el análisis estático y dinámico y la reingeniería inversa.

Se presenta un informe que refleja el análisis forense realizado, esta asignación de datos se encuentra relacionada con el uso de aplicaciones para análisis forense en la recolección, comparación, análisis y evaluación de datos procedentes de cualquier medio informático logrando resultados de las posibles causas y objetivo de la ejecución de dicho archivo en sistemas Windows y la red de la organización en mención.

ÍNDICE GENERAL

RESUMEN ---------- **VII**
ÍNDICE GENERAL ---------- **IX**
ÍNDICE DE FIGURAS ---------- **XII**
ÍNDICE DE TABLAS ---------- **XIV**
INTRODUCCIÓN ---------- **XV**

ANTECEDENTES Y JUSTIFICACIÓN ---------- **1**
1.1 Antecedentes ---------- 1
1.2 Justificación ---------- 2
1.3 Descripción del proyecto ---------- 3
1.3.1 Objetivos Generales ---------- 4
1.3.2 Objetivos Específicos ---------- 4
MARCO TEÓRICO ---------- **6**
2.1 Análisis Forense ---------- 6
2.1.1 Objetivos del Análisis Forense ---------- 6
2.1.2 Preparación para el Análisis ---------- 6
2.1.3 Gestión de evidencias ---------- 7
2.1.4 Adquisición de datos ---------- 8
2.1.5 Protección del sistema ---------- 8
2.1.6 Dispositivos a analizar ---------- 9
2.2 Desarrollo de las investigaciones ---------- 9
2.3 Análisis de ataques ---------- 9
2.4 Prevención de ataques a sistemas ---------- 10
2.5 Dificultades al realizar un Análisis Forense ---------- 11
2.6 Aspectos legales ---------- 12
2.7 Análisis de Malware ---------- 12
2.7.1 Análisis Estático ---------- 13
2.7.2 Análisis Dinámico ---------- 13
2.8 Ingeniería Inversa ---------- 14
2.8.1 Propósito de la Ingeniería Inversa ---------- 14

HERRAMIENTAS PARA EL ANÁLISIS FORENSE ---- 16
3.1 Herramientas en Linux ---- 16
3.1.1 ls –al ---- 16
3.1.2 File ---- 16
3.1.3 Md5deep ---- 17
3.1.4 Strings ---- 17
3.2 Herramientas en Visual Studio ---- 17
3.2.1 cl ---- 17
3.2.2 dumpbin ---- 17
3.3 Herramientas Open Source ---- 18
3.3.1 Caine ---- 18
3.3.2 VirtualBox ---- 19
3.3.3 StraceNT ---- 19
3.3.4 Lordpe ---- 20
3.3.5 WinHex ---- 20
3.3.6 OllyDbg ---- 20
3.3.7 Anubi ---- 20
3.3.8 Procdump ---- 21
3.3.9 Antivirus Avast ---- 22
3.3.10 Fsg ---- 22
3.3.11 Stud_PE ---- 23
3.3.12 Netcat ---- 23
3.3.13 RDG Packer Detector ---- 23
3.3.14 Unfsg ---- 24
3.3.15 Virus Total ---- 24
3.4 Herramientas Comerciales ---- 25
3.4.1 IDA ---- 25
3.4.2 PE Explorer ---- 26
DESARROLLO DEL PROYECTO ---- 27
4.1 Descompresión del archivo ---- 27
4.2 Comando ls ---- 27
4.3 Hash del archivo ---- 28

4.4 Compilar en C ---- 28
4.5 Análisis Estático ---- 30
4.5.1 Hashing de ficheros con MD5DEEP ---- 30
4.5.2 Uso del comando File ---- 30
4.5.3 Análisis del comportamiento del ejecutable mediante Anubis ---- 31
4.5.4 Examinando PE con Dumpbin ---- 34
4.5.5 Revisión de las cadenas de caracteres ASCII y Unicode ---- 53
4.5.6 Editor Hexadecimal ---- 56
4.5.7 PE Explorer ---- 60
4.5.7.1 Dependencias ---- 60
4.5.8 Desensamblador IDA ---- 61
4.6 Análisis Dinámico ---- 65
4.6.1 Debugger OllyDBG ---- 66
4.6.2 Usando StraceNT ---- 70
4.7 Análisis de los archivos Sak.exe ---- 76
4.7.1 Información general de los archivos a analizar ---- 76
4.7.1.1 Archivos a analizar ---- 79
4.8 Análisis Estático ---- 81
4.8.1 Análisis SAK.EXE ---- 81
4.8.1.1 Análisis en dirección WEB ANUBIS de Archivos SAK ---- 81
4.8.2 Análisis Virus Total SAK.EXE ---- 87
4.8.2.1 Informe Virus Total ---- 87
4.8.3 Archivo generado por BIN TEXT ---- 95
4.8.4 Análisis del archivo con IDA PRO ---- 127
4.8.4.1 Expresiones del lenguaje ensamblador ---- 128
4.9 Análisis Dinámico ---- 129
CONCLUSIONES ---- 131
RECOMENDACIONES ---- 133
GLOSARIO DE TERMINOS ---- 135
BIBLIOGRAFÍA ---- 138

ÍNDICE DE FIGURAS

Figura 1.- Interfaz Gráfica Caine 18

Figura 2.- Interfaz Gráfica VirtualBox 19

Figura 3.- Interfaz Gráfica IDA 25

Figura 4.- Archivo Descomprimido 27

Figura 5.- Introduciendo el Md5deep con los archivos a analizar 28

Figura 6.- Abriendo el archivo en el Visual Studio 29

Figura 7.- Formulario de envío de archivos 31

Figura 8.- Abriendo el archivo con el WinHex 57

Figura 9.- Información de la cabecera del archivo 60

Figura 10.- Dependencias del archivo 61

Figura 11.- Abriendo el achivo en IDA 62

Figura 12.- Cargando el nuevo archivo en el IDA 63

Figura 13.- Visualización del archivo binario 64

Figura 14.- Elección del DLL 66

Figura 15.- Visualización del archivo hello.exe en OllyDbg 67

Figura 16.- Visualización del programa a Debuggear 67

Figura 17.- Registros del programa 68

Figura 18.- Stack del programa 69

Figura 19.- Visualización del hexadecimal del programa 69

Figura 20.- Listado de los ejecutables 69

Figura 21.- Memoria del programa 70

Figura 22.- Visualización del programa StraceNT 71

Figura 23.- Información general de los archivos a analizar 77

Figura 24.- Información general de los archivos 78

Figura 25.- Eliminación de los archivos que ya han sido analizados..... 78

Figura 26.- Ejecución del comando string 79

Figura 27.- Ejecución del comando file 80

Figura 28.- Análisis con el programa Avast 81

Figura 29.- Análisis con Virus Total..... 87

Figura 30.- Análisis con el programa FSG..... 93

Figura 31.- Hash de los archivos a analizar 94

Figura 32.- Análisis con RDG Packer Detector 94

Figura 33.- Desempaquetado del archivo..... 95

Figura 34.- Verificación de los archivos 95

Figura 35.- Análisis con el programa IDA PRO 127

Figura 36.- Password encontrado con el programa IDA..... 128

Figura 37.- Ejecución del password encontrado 129

Figura 38.- Análisis con el programa Lordpe..... 130

ÍNDICE DE TABLAS

Tabla I.- Análisis con Virus Total 88

Tabla II.- Análisis de todos los archivos con Virus Total 90

Tabla III.- Tabla comparativa con el Software Stud_PE 93

Tabla IV.- Archivo generado por BinText 126

Tabla V.- Expresiones del lenguaje ensamblador 128

INTRODUCCIÓN

En la medida que la Internet crece, lo hace de igual manera el número de acciones incursivas ilegales contra la seguridad de las redes corporativas.

Con el auge de los computadores y la TI, la seguridad informática se ha visto afectada. Durante la última década los ataques virtuales han crecido inimaginablemente estableciendo un escenario oscuro sobre la seguridad de la infraestructura informática en todo el mundo, lo que ha suscitado una serie de acciones que favorecen y refuerzan la seguridad, sin embargo, los hackers y delincuentes informáticos cada vez encuentran nuevas formas para continuar con su accionar.

Las actividades a desarrollar por el profesional de la informática forense deben servir para la correcta planificación preventiva de seguridad de una red corporativa.

Otro detalle importante del análisis forense es el grado de abstracción de la información recolectada. Aunque uno puede leer bit a bit la evidencia, resulta ineficiente por el tiempo que se tarda en encontrar la información (aunque en algunos casos sea la única manera). Apoyándose de las diferentes técnicas del análisis forense es posible dar solución a esta problemática, mitigar los problemas y mitigar los probables riesgos existentes.

Por esto es necesario dar a conocer alternativas a las típicas herramientas forenses

informáticas y mostrar técnicas diferentes, utilizando los comandos propios del sistema operativo y software adicional que permita encontrar, recuperar y reconstruir información analizada en esta investigación.

Para eso uno se ayuda con herramientas (algunas provistas por el sistema operativo). Hay varias herramientas en el mercado muchas de ellas libres y otras comerciales, que las usaremos en la búsqueda de la información que podamos obtener de archivos a revisar.[1]

[1](Contreras, F. , 2009)

CAPÍTULO 1

ANTECEDENTES Y JUSTIFICACIÓN

1.1 Antecedentes

El 22 de Noviembre de 1988, se ejecutó el primer ataque informático, el cual afectó a miles de ordenadores de empresas y personas particulares conectados a la Internet, inutilizándolos durante varios días, muy pocos tomaban en serio el tema de la seguridad en redes de computadores.

El analizar las amenazas informáticas cada día se ha vuelto mucho más complicado, debido a que dichas amenazas y ataques han crecido en complejidad a través del paso de los años, el día de hoy los virus informáticos van de paseo por el Internet y uno de los medios que cada día más utilizan son las nuevas tecnologías y la comunicación, cada día se hace más patente la preocupación por los temas relativos a la seguridad en la red y sus equipos informáticos, así como la necesidad de esta seguridad. Ahora no solo ha cambiado la manera en que se propagan los virus, sino que tambien han variado los motivos de los atacantes.

Dado que la Internet creció exponencialmente con la adhesión de redes importantes, tales como BITNET o HEPNET, se produjo un incremento en las ventas de ordenadores personales, y junto con ellos ahora los ataques informáticos.

Durante las investigaciones de los delitos informáticos, en particular intrusiones informáticas, nos encontraremos con archivos falsos con un propósito desconocido. Sabemos que el archivo está haciendo algo que el atacante quiere, pero lo único que tenemos es un archivo binario y tal vez alguna teoría acerca de lo que el archivo hace. Las herramientas de análisis serían mucho más simples si los atacantes dejaran su código fuente. La mayoría de los atacantes tienen algo en común con Microsoft: protegen su código fuente. Sin él, lo que queda es rastrear la funcionalidad del programa.[2]

1.2 Justificación

El análisis de equipos informáticos y redes es un tema de gran importancia actualmente, se vuelve necesaria la detección de ataques en dispositivos conectados a la red, el análisis forense para la recuperación de datos y la adquirir evidencias legales que sirvan como pruebas ante los tribunales.

Dentro del campo de la detección de ataques en equipos conectados en red, se analizan e implementan puntos necesarios para la búsqueda de las conexiones desde y hacia dispositivos conectados a Internet, susceptibles de ser vulnerados gracias a la explotación de alguna debilidad propia del sistema operativo que corre en ellos o resultado de alguna aplicación con un agujero (bug) de seguridad, con el objeto de detectar ataques e intrusiones.

[2](Gomez, A., & Monserrat, F., 2001)

En este análisis forense, se observarán los archivos posiblemente atacados intentando reconstruir la secuencia temporal de las actividades realizadas de forma que sirva tanto para ayudar a recuperar datos perdidos y volver al sistema a su estado de funcionamiento normal, como para obtener pruebas de la actividad delictiva. Esta fase concluirá con el desarrollo de una metodología que facilite el proceso de análisis forense.

La infraestructura informática nunca está protegida al cien por ciento frente a las vulnerabilidades.

Se busca ofrecer opciones similares, usar una política de seguridad de procedimientos que reciba, analice y posteriormente responda a este tipo de incidentes, ya sean inminentes o en curso, es un integrante indispensable de la infraestructura de los sistemas informáticos de la organización, debido a que los ataques a estos sistemas no sólo ha incrementado en número sino que también lo han hecho en capacidad destructiva y diversidad.

Presentaremos una aproximación científica sólida para la realización del análisis con las herramientas que están a nuestro alcance y aprenderemos cómo tomar un archivo ejecutable con una función desconocida y realizar operaciones en el mismo para obtener una perspectiva del destino del archivo.

1.3 Descripción del proyecto

En la organización se vieron comprometidos varios sistemas Windows debido a los

incidentes que tuvieron se tomaron la medidas necesarias para poder proteger la red durante la búsqueda y respuesta al incidente inicial, se obtuvieron imágenes forenses, y el archivo sak.exe fue encontrado en varios sistemas. Nuestro objetivo va ser determinar todo lo que podamos encontrar acerca de este ejecutable usando las herramientas necesarias para encontrar el propósito del archivo por el cual fue encontrado en los sistemas de la empresa.

1.3.1 Objetivos Generales

- Analizar y garantizar el proceso de extracción, conservación, identificación de las evidencias digitales.
- Interpretar la información para extraer conclusiones válidas, ayudando a su investigación y resolución.
- Mantener un registro exhaustivo del análisis y la documentación.

1.3.2 Objetivos Específicos

- Proporcionar las técnicas y principios que faciliten la investigación del incidente y su metodología básica, utilizando diferentes mecanismos de análisis
- Analizar los datos sin modificarlos. En este punto, es crucial proteger las evidencias físicas originales trabajando con copias idénticas de forma que en

caso de error se pueda recuperar la imagen original y continuar con el análisis de forma correcta.

- Encontrar las vulnerabilidades que se explotaron debido al ingreso de código malicioso.
- Proveer información de los datos comprometidos debido a una posible intrusión.
- Realizar un proceso de búsqueda detallada utilizando herramientas que nos puedan ayudar a determinar acerca del archivo encontrado para poder reconstruir a través de todos los medios los acontecimientos que tuvieron lugar, desde el momento que el sistema estuvo en su estado íntegro hasta el momento en el que haya sufrido alguna modificación.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Análisis Forense

Se refiere a la recopilación de evidencias y al proceso de analizar una copia completa de un sistema que ha sufrido una intrusión o ataque. Realizar un análisis forense nos permitirá, entre otras cosas, recuperarnos del incidente de una manera más segura y evitar en la medida posible que se repita la misma situación.

El análisis forense requiere que se realicen ciertos procedimientos de montaje y preparación de los datos recogidos antes de empezar a analizar los datos.

2.1.1 Objetivos del Análisis Forense

El análisis forense permite obtener la mayor cantidad posible de información sobre:

- El método utilizado por el atacante para introducirse en el sistema
- Las actividades ilícitas realizadas por el intruso en el sistema
- El alcance y las implicaciones de dichas actividades

2.1.2 Preparación para el Análisis

Analizando el sistema con las herramientas forenses específicas o no, se debe

de seguir los mismos pasos básicos siempre para prepararse para el análisis completo del sistema.

En algunos casos es necesario fotografiar el equipo afectado antes de mover cualquier detalle del mismo. Eso puede ser necesario como prueba del incidente en casos que posiblemente puedan acabar en una sala de juicio.

Empezar haciendo apuntes detallados. Tener bien detallados apuntes con la fecha y hora del inicio y fin de cualquier trabajo realizado será muy útil durante y al final del análisis. Es importante que todos los hechos pertinentes al caso durante la preparación, recuperación y análisis de las pruebas sobre un ataque, estén perfectamente documentados. Estas notas servirán como base para poder desarrollar un informe detallado de incidencia que se debe preparar una vez terminado el análisis.[3]

2.1.3 Gestión de evidencias

La gestión de evidencias tiene los mismos objetivos que la seguridad forense. Existen reglas legales que determinan si las evidencias potenciales pueden o no ser consideradas por un tribunal. Deben protegerse de posibles daños mecánicos o electromagnéticos las evidencias extraídas. Se debe establecer y mantener una continua cadena de custodia.

[3] (Sarkisov, E., & Dittrich, D. , 2000)

Se debe limitar la cantidad de veces que las operaciones de negocios se vean afectadas. Las evidencias deben obtenerse de manera que se asegure la autenticidad y validez. Además de que los procedimientos de búsqueda de computador no se deben dañar, destruir o comprometer las evidencias. Se debe prevenir que se introduzcan virus en el computador durante el proceso de análisis. [4]

2.1.4 Adquisición de datos

En este sentido, se debe tener en cuenta que tanto los procedimientos como las herramientas que se han de utilizar deberían estar certificados por una entidad de confianza. El proceso de adquisición de datos es una de las actividades más críticas en cuanto a la futura legalidad de la prueba se refiere.

La presentación de la prueba, ya sea en una disputa o en un juicio, debe hacer especial hincapié en cómo se ha realizado la adquisición de los datos analizados y cómo ello ha influido en la veracidad de las conclusiones extraídas del posterior análisis.

2.1.5 Protección del sistema

El objetivo de la protecció8n del sistema es preservar la integridad de los sistemas susceptibles de contener evidencias digitales. Hay que mantener a los sospechosos y a otras personas lejos del sistema bajo investigación para

[4] (Contreras, F. ,2009)

evitar cualquier manipulación. Se debe tener especial cuidado con la tecnología inalámbrica, ya que se podrían lanzar procesos de forma remota. Si un monitor muestra algún tipo de información, se debe registrar, por ejemplo, tomando una fotografía.

2.1.6 Dispositivos a analizar

Por lo general cuando estamos realizando un análisis forense tenemos varios medios de almacenamiento que debemos examinar además de cualquier tipo de dispositivo que almacene información por ejemplo: Discos Duros, USB, Memorias Digitales, celulares etc.[5]

2.2 Desarrollo de las investigaciones

Debemos poder identificar la evidencia ese es el primer paso importante en todo análisis forense. Es muy importante que la persona encargada de la investigación tenga la experiencia y un buen criterio debemos aplicar una metodología forense por eso tenemos que asegurarnos que toda la evidencia que hayamos encontrado fue correctamente preservada, recolectada y analizada de una manera minuciosa y que se hayan utilizado las mejores prácticas para asegurar la integridad de toda la evidencia.

2.3 Análisis de ataques

La mayor parte de los ataques que acaban con un acceso al sistema con privilegios de root siguen el mismo esquema:

[5] Cruz Allende, D. (2007)

- Se realiza un escaneo buscando equipos vulnerables que estén ejecutando un servicio con algún fallo de seguridad conocido.
- Se emplea un exploit contra el equipo, consiguiendo instalar una puerta de acceso al sistema.
- Obtener todos los datos disponibles sobre el sistema: versión, particiones, hora y fecha del ataque.

2.4 Prevención de ataques a sistemas

Ya que para muchas empresas es muy importante proteger su actividad productiva es importante que mantengan el número de incidentes razonablemente bajo, si los controles de seguridad son insuficientes y sufren continuos ataques a sus sistemas, esto puede repercutir negativamente en sus actividades, tanto desde el punto de vista económico como el de imagen.

Exista mucha información en libros de cómo se puede asegurar sus sistemas para que no sufran de ataques cibernéticos. Para poder evitar que sufran de ataques se puede considerar lo siguiente:

- Mantener la seguridad de la red, denegando cualquier tipo de acceso no autorizado expresamente, instalación de cortafuegos, detectores de intrusos , monitores de red, uso de redes privadas virtuales, uso de protocolos seguros.
- Utilizar un buen antivirus capaces de parar este tipo de código como virus, caballos de troya, gusanos.

- Disponer de una correcta gestión de parches y actualizaciones del hardware y software, ya que gran parte de los ataques se basan en explotar un número reducido de vulnerabilidades en sistemas y aplicaciones.
- Asegurarse que los servidores estén configurados para que proporcionen un número limitado de servicios y con un nivel de acceso restringido según el tipo de usuario. Además deben evitarse configuraciones por defecto, como claves predefinidas.
- Formar e informar a sus usuarios para que conozcan, acepten y sean capaces de aplicar las directrices de su política de seguridad. Informando y formando a los usuarios reducirá la frecuencia de los incidentes, sobre todo aquellos que impliquen la ejecución de código malicioso, o el saltarse la política de uso adecuado de los sistemas.[6]

2.5 Dificultades al realizar un Análisis Forense

Una de las principales dificultades que enfrentamos al momento de realizar un análisis forense es que la evidencia no haya sido alterada y es muy importante capturar inmediatamente la evidencia luego de un incidente; para luego preservarla adecuadamente y que esta no sufra alteraciones. En muchos casos cuando se trata de investigar algún fraude o delito informático, se requiere contar con la colaboración de instituciones del Estado; y en muchos casos termina en procesos legales que pueden durar muchos años.

[6] Contreras Vega, G., & Ochoa, C. (2004)

2.6 Aspectos legales

Si tras la realización de un primer análisis existen sospechas de que el incidente se ha provocado desde el interior la red, hay que plantearse la posibilidad de llevar a cabo una investigación interna a la organización para depurar responsabilidades. En esta situación además del equipo técnico de respuesta a incidentes, tendrá que contar con otros departamentos.

Si el incidente, realizado por atacantes internos o externos, ha provocado daños importantes a su organización ya sean económicos, de imagen corporativa o su reputación ha quedado en entredicho, se puede considerar abrir un proceso judicial contra sus atacantes. En este caso la investigación técnica deberá ser tratada como una investigación pericial técnica, incorporando procedimientos en materia de probatoria judicial, pues una evidencia digital no será considerada como prueba en un proceso judicial hasta que el juez así lo determine.

Por ello tendremos que convencerle de que hemos actuado de forma profesional, científica, veraz, con cautela e imparcial, y además explicárselo para que lo entienda pues es muy probable que el juez no tenga conocimientos avanzados en estos temas.[7]

2.7 Análisis de Malware

A no ser que se trate de un gusano basado en scripts, los autores de malware rara vez

[7] Lopez, M. (2007)

nos proporcionan el código fuente de sus creaciones.

A falta del código fuente, nos enfrentamos a un conjunto muy limitado de opciones para descubrir exactamente cómo el malware se comporta.

Las dos principales técnicas de análisis de malware son análisis dinámico y el análisis estático.

2.7.1 Análisis Estático

El análisis estático se realiza sin ejecutar el código malicioso ni desensamblar su código, puede realizar el análisis estático en cualquier sistema operativo, independientemente del tipo de código objeto, con este tipo de análisis se puede determinar el tipo de archivo que se está examinando revisar las cadenas de caracteres ASCII y Unicode contenidos en el archivo. En contraste, el análisis estático intenta comprender el comportamiento de un programa simplemente leyendo el código del programa, que, en el caso de programas maliciosos, por lo general consiste en una lista de desmontaje. El análisis estático tiene la ventaja de que puede revelar cómo se comportaría un programa en condiciones inusuales, ya que podemos examinar partes de un programa que normalmente no se ejecutan.

2.7.2 Análisis Dinámico

El análisis dinámico se lleva a cabo cuando se ejecuta el código malicioso e interpreta su interacción con el sistema operativo. Aunque esto puede ser peligroso porque puede causar cualquier efecto negativo en la estación de

trabajo forense. Sin embargo, este es a menudo la forma más esclarecedora de la herramienta de análisis. Con este tipo de análisis se puede ejecutar el programa para interceptar las llamadas al sistema, además de interactuar con el registro y poder realizar la monitorización de red.

En contraste, el análisis dinámico consiste en permitir que el malware se ejecute en un entorno cuidadosamente controlado, mientras que registra todos los aspectos de su comportamiento.

2.8 Ingeniería Inversa

La ingeniería inversa es desarmar un objeto para ver cómo funciona con el fin de duplicar o aumentar el objeto, se utiliza para descubrir vulnerabilidades en los archivos binarios y para identificar el contenido malicioso en un programa como un virus. Es una habilidad importante para el profesional de hoy en el área de seguridad informática.

2.8.1 Propósito de la Ingeniería Inversa

El propósito de las herramientas de la ingeniería inversa es a menudo para facilitar la comprensión de los programas cuando el código fuente no está disponible. Por lo general se utiliza en los siguientes casos:

- Análisis de malware
- Análisis del software de código cerrado para vulnerabilidades
- Análisis del software de código cerrado para la interoperabilidad

- Visualización de instrucciones de programa durante la depuración [8]

[8] Mandia, K., Prosise, C., & Pepe, M. (2003)

CAPÍTULO 3

HERRAMIENTAS PARA EL ANÁLISIS FORENSE

A continuación se revisarán las herramientas que fueron utilizadas para el análisis forense.

3.1 Herramientas en Linux

3.1.1 ls –al

Lista los archivos con mucho más detalle, especificando para cada archivo sus permisos, el número de enlaces rígidos, el nombre del propietario, el grupo al que pertenece, el tamaño en bytes y la fecha de la última modificación.

3.1.2 File

Se utiliza para saber de qué tipo es un archivo, bien porque carezca de extensión que lo identifique o bien porque haya sido renombrado, este comando nos dirá de qué se trata además para saber qué tipo de archivo tenemos delante. Hay ocasiones en las que nos encontraremos con archivos que no tienen extensión y por tanto no sabemos cómo tratarlo. El comando file nos dará una información muy valiosa.

3.1.3 Md5deep

Es una herramienta multiplataforma gratuita y portable que nos permite crear y comprobar los resúmenes hash de los ficheros que le indiquemos mediante la línea de comandos o scripts, puede confirmar tanto la integridad de los archivos y la autenticidad. Es muy útil para saber rápidamente si un archivo fue modificado.

3.1.4 Strings

El comando Strings devuelve en forma de cadena alfanumérica la expresión de tipo numérico, Fecha, Hora, cadena o Booleana, recorre el archivo binario y muestra en la salida los textos que haya encontrado dentro del archivo.

3.2 Herramientas en Visual Studio

3.2.1 cl

Este comando acepta los archivos de comandos del compilador como argumentos de la variable de entorno CL o de la línea de comandos permite utilizar varias líneas de opciones y nombres de archivo.

3.2.2 dumpbin

La utilidad dumpbin, que se incluye con la versión de 32 bits de Microsoft Visual C++, combina las capacidades de las utilidades link, lib. La combinación de estas características de herramientas tiene la capacidad de

proporcionar información sobre el formato y los símbolos proporcionada en el archivo ejecutable.

3.3 Herramientas Open Source

3.3.1 Caine

Es una distribución de Linux basada en Ubuntu 10.04 para científicos forenses y administradores responsables de seguridad. Preparada para combatir a los TI incompetentes, Caine cuenta con una razonable selección de software, una interfaz gráfica amigable y un soporte receptivo es una distribución útil y compacta.[9]

Figura 1.- Interfaz Gráfica Caine

[9] http://www.caine-live.net/

3.3.2 VirtualBox

Es un software de virtualización por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como sistemas invitados, dentro de otro sistema operativo anfitrión, cada uno con su propio ambiente virtual.[10]

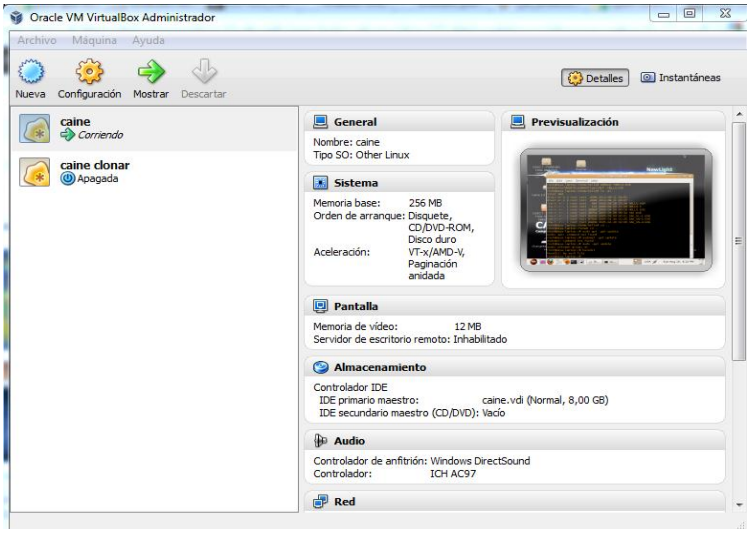


Figura 2.- Interfaz Gráfica VirtualBox

3.3.3 StraceNT

StraceNT es un rastreador de llamadas al sistema para Windows. Proporciona una funcionalidad similar a la de strace en Linux. Se puede rastrear todas las llamadas hechas por un proceso a las funciones importadas desde un archivo DLL. StraceNT puede ser muy útil en la depuración y el análisis del funcionamiento interno de un programa. Es útil para analizar la interacción del proceso con el sistema operativo.

[10] https://www.virtualbox.org

3.3.4 Lordpe

Herramienta para editar ciertas partes de los ejecutables y volcado de memoria de los procesos ejecutados. Es una arma de doble filo, junto a otras herramientas se puede dejar el server de un troyano indetectable a algunos antivirus o volcar el proceso de un malware cargado en memoria.

3.3.5 WinHex

Es un editor hexadecimal universal, y al mismo tiempo posiblemente la más potente utilidad de sistema jamás creada. Apropiado para informática forense, recuperación de archivos, peritaje informático, procesamiento de datos de bajo nivel y seguridad informática.

3.3.6 OllyDbg

Es un depurador de código ensamblador de 32 bits para sistemas operativos Microsoft Windows. Pone especial énfasis en el análisis del código binario, esto lo hace muy útil cuando no está dispone el código fuente del programa.

3.3.7 Anubi

Es un analizador de ejecutables online su objetivo es proporcionar a los usuarios de computadoras una herramienta que ayuda en la lucha contra el malware. Anubis es una herramienta para analizar el comportamiento de los ejecutables en sistemas operativos Windows con especial énfasis en el análisis de malware, generando informes que contienen información

suficiente para dar al usuario una impresión sobre el propósito y las acciones de un binario ejecutado.

Es la herramienta ideal para el análisis de malware y virus orientado a las personas que desean obtener mayor información y comprensión del propósito de un binario desconocido. El análisis es muy completo, entre algunas cosas importantes destaca:

- Uso de librerías y componentes externas.
- Archivos que genera el propio ejecutable o elimina.
- Carpetas que crea o elimina.
- Claves del registro que se ven afectadas o se crean.
- Crea una captura de pantalla del programa.
- Información detallada de tamaño, MD5.

3.3.8 Procdump

Es una herramienta que nos permite volcar y desempacar algunos archivos PE (Portable Ejecutable) protegidos sin necesidad de un depurador (debugger).Es un programa pensado más para la ingeniería inversa Podremos Volcar cualquier proceso/módulo de 32 bits en ejecución usando el motor CodeShot. Además de poder restaurar la tabla de importaciones y el encabezado PE y Alterar el encabezado de un archivo PE determinado.

3.3.9 Antivirus Avast

Es un software antivirus tiene un sistema antispam (control del correo basura) con filtro de mensajes fraudulentos. Nos proporciona protección contra correos electrónicos no deseados y que pueden llevar a páginas falsas de bancos además de un cortafuego que permite controlar todo el tráfico entrante y saliente del ordenador.

Y monitoriza la actividad del sistema usando varios sensores (sistema de ficheros, registro y red), avisando y bloqueando en caso de encontrar una actividad sospechosa.

3.3.10 Fsg

Rápido, Pequeño, Bueno es un compresor perfecto para archivos ejecutables, su código de descompresión sólo tiene 158 bytes, es compatible con Windows 95 / 98 / ME / 2K / XP Vista / 7.

Tiene las siguientes características:

- Diseñado para archivos asm ejecutables (kg, cracks, trojans)
- Cargador de pequeño tamaño.
- Importa el manejo.
- Soporte para ejecutables con tablas de exportación.
- Soporte TLS (Delphi, bcc exes)
- Soporte de revestimiento (flash, director, shockwave etc.)

- Soporte en línea del comando, por ejemplo \"fsg.exe notepad.exe\" (arrastrar y soltar también funciona)

3.3.11 Stud_PE

Stud PE es un analizador de ejecutables especialmente pensado para programas portables. Sus múltiples pestañas nos sirven para:

- Organizar los datos recopilados tras abrir el fichero EXE o DLL.
- Visor/volcado/eliminador de tareas
- Comparación de archivos PEHeader/binario
- Integración en el menú shell por arrastrar y soltar
- Editor básico en formato hexadecimal

3.3.12 Netcat

Es un pequeño programa creado para uso de los administradores de redes la estructura de sus comandos es poco familiar para el usuario medio. Netcat tiene infinidad de funciones, la especialidad de NetCat es el protocolo tcp/ip, y le dá a la máquina de windows, cierto poder sobre este protocolo que solo tenía UNIX, trabaja con líneas de comandos desde MS-DOS (o desde el Shell de Linux). El comando principal es nc con su respectiva variable.

3.3.13 RDG Packer Detector

Es un detector de packers, Cryptors, Compiladores, Packers Scrambler, Joiners, Installers. Posee sistema de detección potente analizando el archivo

completo, permitiendo la muli-detección de packers en varios casos. Permite crear signaturas tus propias signaturas de detección, tiene un analizador Crypto-Grafico, calcula el checksum de un archivo. Permite calcular el Entropy, informando si el programa analizado esta comprimido, encriptado o no. Además tiene un detector de OEP (Punto de entrada Original) de un programa.

3.3.14 Unfsg

UnFSG es un genérico independiente unpacker y reconstructor de los archivos lleno de FSG. Fue escrita en msvc6, todos los procedimientos han sido reescritos para lenguaje c.

3.3.15 Virus Total

VirusTotal es un servicio online gratuito que analiza los archivos y URLs que permiten la identificación de virus, gusanos, troyanos y otros tipos de contenido malicioso detectado por antivirus y escáneres sitio web. Al mismo tiempo, puede ser utilizado como un medio para detectar los falsos positivos, o sea recursos inocuos detectados como malicioso por uno o más escáneres.

VirusTotal misión es ayudar en la mejora de la industria antivirus y seguridad y hacer de Internet un lugar más seguro mediante el desarrollo de herramientas y servicios gratuitos.

3.4 Herramientas Comerciales

3.4.1 IDA

El desensamblador interactivo, más comúnmente conocido simplemente como IDA, es un desensamblador y un depurador comercial ampliamente utilizado para la ingeniería inversa. Es compatible con una gran variedad de formatos ejecutables para diferentes procesadores y sistemas operativos.

A pesar que IDA realiza un alto grado de análisis de código automático, en cierta medida, aprovechando las referencias cruzadas entre las secciones de código, el conocimiento de los parámetros de llamadas a la API, y otra información, se centra en ser interactivo. [11]

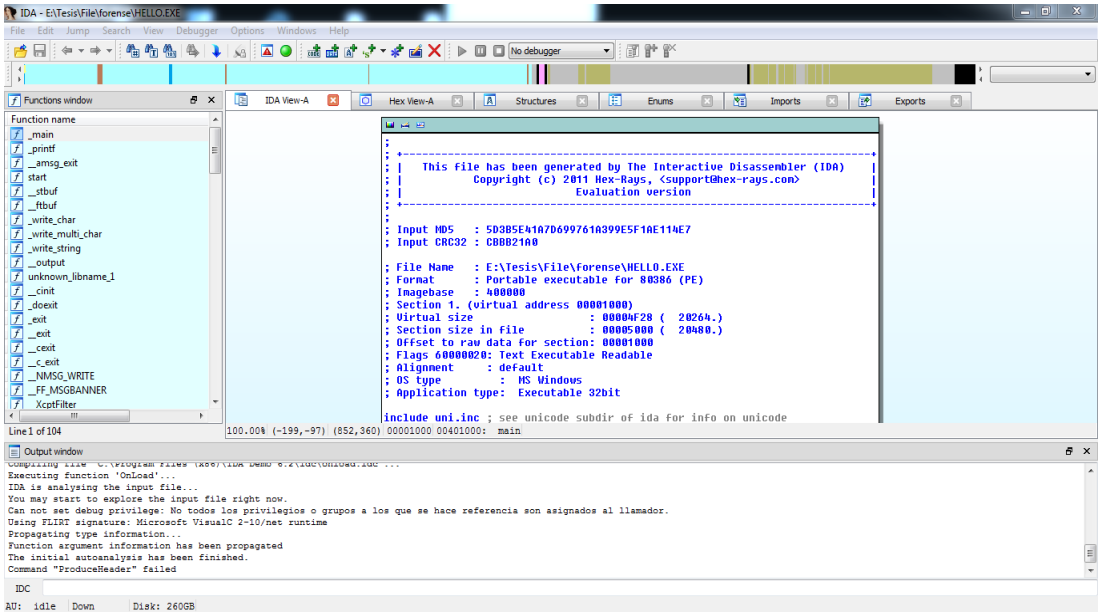


Figura 3.- Interfaz Gráfica IDA

[11] http://www.hex-rays.com/

3.4.2 PE Explorer

Diseñado para inspección y edición de archivos ejecutables de Windows, PE Explorer ofrece poderosas herramientas de análisis y edición para trabajar con formatos EXE, DLL, controles ActiveX y otros archivos ejecutables sobre plataformas de 32-bits de MS Windows.

Este programa, nos ayuda a inspeccionar códigos de programas para los que no tenemos el código fuente, es capaz de reconstruir partes del código fuente original del programa. Además permite efectuar análisis estáticos, revela mucha información acerca de la función del ejecutable y recoge tanta información como sea posible acerca del archivo ejecutable, sin ejecutarlo.

CAPÍTULO 4

DESARROLLO DEL PROYECTO

4.1 Descompresión del archivo

Se nos dio un archivo comprimido lo primero que haremos para poder realizar el análisis es descomprimirlo para poder visualizar los archivos a analizar, para ello utilizaremos el comando unrar e nombre del archivo

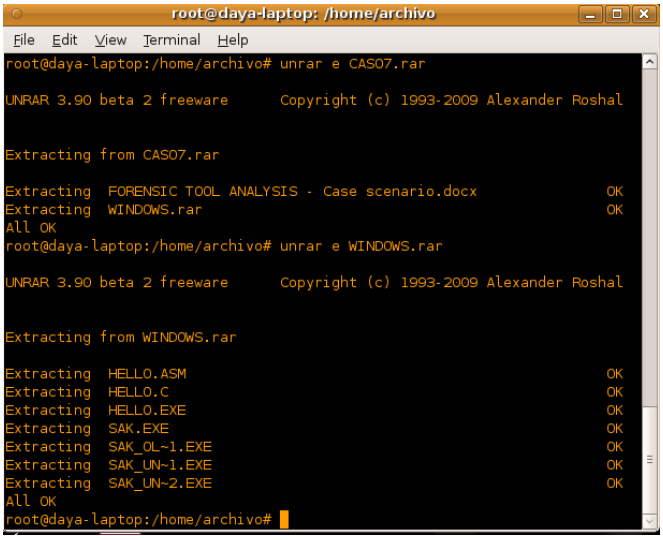


Figura 4.- Archivo Descomprimido

4.2 Comando ls

En esta sección analizaremos todo acerca del programa hello.exe a continuación observaremos la fecha y hora que fueron creados dichos archivos además observamos cuantos bytes tiene cada archivo, esto lo haremos con la ayuda de la línea de comando del programa caine mediante el siguiente comando:

```
# ls -al

-rw-r--r-- 1 root root   964 2005-04-28 23:38 HELLO.ASM
-rw-r--r-- 1 root root   101 2005-04-23 21:28 HELLO.C
-rw-r--r-- 1 root root 36864 2005-04-29 00:16 HELLO.EXE
```

4.3 Hash del archivo

Primero que todo antes de realizar cualquier tipo de análisis realizaremos un hash del fichero esto lo haremos mediante la línea de comandos para poder realizarlo descargaremos la herramienta md5deep luego de haberlo descargado lo pondremos en la carpeta en donde vamos a realizar el Hashing todos esto tendremos que hacerlo para que nos pueda funcionar en la línea de comandos del visual studio.

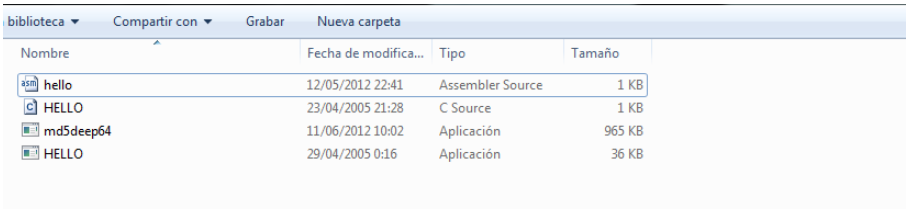


Figura 5.- Introduciendo el Md5deep con los archivos a analizar

Luego de eso utilizamos el comando el cual nos ayudara a verificar si el archivo fue o ha sido modificado.

```
> md5deep64 hello.exe

5d3b5e41a7d699761a399e5f1ae114e7  E:\Tesis\File\WINDOWS\hello.exe
```

4.4 Compilar en C

El programa a analizar está escrito en C lo abriremos con el programa Visual Studio. A continuación se muestra el código:

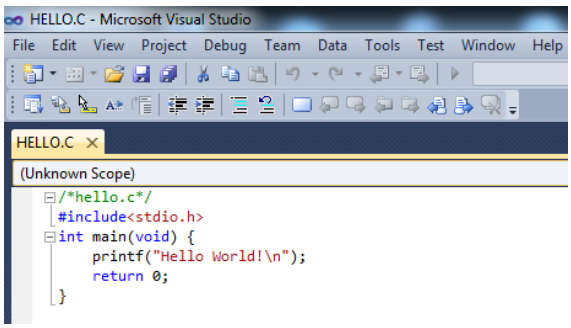


Figura 6.- Abriendo el archivo en el Visual Studio

Ahora lo siguiente que haremos será compilar el archivo como en nuestro caso estamos utilizando el programa Visual C de Microsoft usaremos el siguiente comando:

```
>cl hello.c

hello.c
Microsoft (R) Incremental Linker Version 10.00.30319.01
Copyright (C) Microsoft Corporation.  All rights reserved.
/out: hello.exe
hello.obj
```

Una vez compilado el código fuente se genera un archivo llamado archivo objeto o programa objeto que es luego enlazado, para generar el archivo ejecutable. Al ejecutarlo se producirá la salida deseada en una ventana de consola.

```
>  hello.exe
Hello World!
```

Ahora observamos el nuevo archivo objeto que se nos generó con su respectiva información además podemos observar que se modificó la fecha del archivo hello.exe.

```
# ls -al

-rw-r--r-- 1 root root     964 2005-04-28  23:38  HELLO.ASM
-rw-r--r-- 1 root root     101 2005-04-23  21:28  HELLO.C
-rw-r--r-- 1 root root   36864 2012-05-12  22:41  HELLO.EXE
-rw-r--r-- 1 root root     631 2012-05-12  22:41  HELLO.OBJ
```

Ahora para poder analizar de una mejor manera el archivo utilizaremos los dos métodos de análisis antes indicado: Análisis Estático y Análisis Dinámico. Con la combinación de estos dos métodos nosotros podremos saber todo acerca de la funcionabilidad del archivo.

4.5 Análisis Estático

En este tipo de análisis se realiza sin tener que ejecutar el programa además de realizar una extensa búsqueda en el archivo con varias herramientas.

4.5.1 Hashing de ficheros con MD5DEEP

Ahora vamos a realizar un Hashing con todos los archivo que tenemos este es un valor prácticamente único para cada archivo.

```
# md5deep64 -l -z

  101 cde0ae9578275011fd4037f6cb095cfe hello.c
  964 79852d0750f1ca0e15c9d711422ecdb3 hello.asm
  631 51d150d96f9675dbf69b99cf5c71c194 hello.obj
44544 928d8c2c52b7a99fb49b1a1d9fbb474e hello.exe
```

Al ejecutar el comando veremos el hash de cada uno de los archivos y el byte de cada uno, sino nos damos cuenta observamos que el hash del archivo hello.exe es diferente al primero que realizamos esto significa que fue modificado.

4.5.2 Uso del comando File

A continuación vamos a mostrar el siguiente comando el cual nos permite reconocer el formato del archivo y alguna otra información que nos pueda

ayudar a saber más sobre este archivo. Este comando es muy útil cuando se comienza a analizar y no se sabe bien que se tiene entre manos.

A continuación ejecutamos el comando con lo cual obtenemos lo siguiente:

```
# file hello.exe

HELLO.EXE:       PE32 executable for MS Windows (console) Intel 80386
32-bit
HELLO.ASM:       ASCII text, with CRLF line terminators
HELLO.C:         ASCII text, with CRLF line terminators
HELLO.OBJ:       ASCII text, with CRLF line terminators
```

El comando nos indica que el archivo hello.exe es un ejecutable para Intel con arquitectura x86 con entorno Windows y de 32bit. En los otros archivos la única información que nos muestra es que se trata de un código de caracteres con salto de líneas.

4.5.3 Análisis del comportamiento del ejecutable mediante Anubis

Usaremos la herramienta Anubis esta nos será de gran ayuda ya que es muy útil para saber algunos detalles de archivos antes de ejecutarlos con detalles que se envía muestra a los servidores de Anubis, con el propósito de evaluar el comportamiento del ejecutable. Tal y como se aprecia en el Gráfico, los servidores de Anubis permiten enviar archivos o direcciones URL.

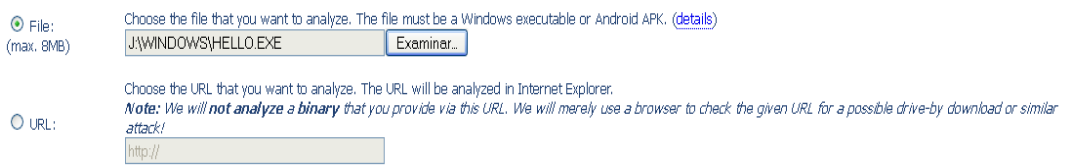


Figura 7.- Formulario de envío de archivos

A continuación se muestra lo que el programa encontró en el ejecutable.

```
[##############################################################################]
    Analysis Report for HELLO.EXE
                    MD5: 928d8c2c52b7a99fb49b1a1d9fbb474e
[##############################################################################]
Summary: No threats could be detected by Anubis.
         This does NOT imply that execution of this executable is safe.
[==============================================================================]
    Table of Contents
[==============================================================================]
- General information
- HELLO.EXE
  a) File Activities
[##############################################################################]
    1. General Information
[##############################################################################]
[==============================================================================]
    Information about Anubis' invocation
[==============================================================================]
        Time needed:        81 s
        Report created:     08/31/12, 09:03:39 UTC
        Termination reason: All tracked processes have exited
        Program version:    1.76.3886
[##############################################################################]
    2. HELLO.EXE
[##############################################################################]
[==============================================================================]
    General information about this executable
[==============================================================================]
        Analysis Reason: Primary Analysis Subject
```

```
        Filename:        HELLO.EXE
        MD5:             928d8c2c52b7a99fb49b1a1d9fbb474e
        SHA-1:           251876f2208a073896d457e75b1d227501c7e268
        File Size:       44544 Bytes
        Command Line:    "C:\HELLO.EXE"
        Process-status
        at analysis end: dead
        Exit Code:       0
[=============================================================================]
    Load-time Dlls
[=============================================================================]
        Module Name: [C:\WINDOWS\system32\ntdll.dll],
               Base Address: [0x7C900000], Size: [0x000AF000]
        Module Name: [C:\WINDOWS\system32\kernel32.dll],
               Base Address: [0x7C800000], Size: [0x000F6000]
[=============================================================================]
    Program output
[=============================================================================]
        Stdout:
Hello World!
[=============================================================================]
    2. a) HELLO.EXE - File Activities
[=============================================================================]
[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-]
    File System Control Communication:
[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-]
 File: [C:\Program Files\Common Files\], Control Code: [0x00090028], 1 time
```

4.5.4 Examinando PE con Dumpbin

Para poder examinar de una mejor manera el ejecutable usaremos el siguiente comando el cual nos muestra el encabezado del archivo y el encabezado de cada sección. Cuando se utiliza con una biblioteca, muestra el encabezado de cada objeto esto lo realizaremos con la ayuda de la línea de comando del visual studio.

Este comando nos indica que es archivo ejecutable de 32 bit de además nos indica que la última vez que fue compilado fue `Sat May 12 22:41:56 2012` además de mostrarnos cada una de las cabeceras del archivo.

```
>dumpbin /headers hello.exe

Microsoft (R) COFF/PE Dumper Version 10.00.30319.01
Copyright (C) Microsoft Corporation.  All rights reserved.


Dump of file hello.exe

PE signature found

File Type: EXECUTABLE IMAGE

FILE HEADER VALUES
             14C machine (x86)
               4 number of sections
        4FAF2D84 time date stamp Sat May 12 22:41:56 2012
               0 file pointer to symbol table
               0 number of symbols
              E0 size of optional header
             102 characteristics
                   Executable
                   32 bit word machine

OPTIONAL HEADER VALUES
             10B magic # (PE32)
           10.00 linker version
            6C00 size of code
            5C00 size of initialized data
               0 size of uninitialized data
            125B entry point (0040125B)
            1000 base of code
            8000 base of data
```

```
          400000 image base (00400000 to 0040EFFF)
            1000 section alignment
             200 file alignment
            5.01 operating system version
            0.00 image version
            5.01 subsystem version
               0 Win32 version
            F000 size of image
             400 size of headers
               0 checksum
               3 subsystem (Windows CUI)
            8140 DLL characteristics
                   Dynamic base
                   NX compatible
                   Terminal Server Aware
          100000 size of stack reserve
            1000 size of stack commit
          100000 size of heap reserve
            1000 size of heap commit
               0 loader flags
              10 number of directories
               0 [       0] RVA [size] of Export Directory
            9CA4 [      28] RVA [size] of Import Directory
               0 [       0] RVA [size] of Resource Directory
               0 [       0] RVA [size] of Exception Directory
               0 [       0] RVA [size] of Certificates Directory
            E000 [     6E4] RVA [size] of Base Relocation Directory
               0 [       0] RVA [size] of Debug Directory
               0 [       0] RVA [size] of Architecture Directory
               0 [       0] RVA [size] of Global Pointer Directory
               0 [       0] RVA [size] of Thread Storage Directory
            9980 [      40] RVA [size] of Load Configuration Directory
               0 [       0] RVA [size] of Bound Import Directory
            8000 [     100] RVA [size] of Import Address Table Directory
               0 [       0] RVA [size] of Delay Import Directory
               0 [       0] RVA [size] of COM Descriptor Directory
               0 [       0] RVA [size] of Reserved Directory


SECTION HEADER #1
   .text name
    6BAA virtual size
    1000 virtual address (00401000 to 00407BA9)
    6C00 size of raw data
     400 file pointer to raw data (00000400 to 00006FFF)
       0 file pointer to relocation table
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
60000020 flags
         Code
         Execute Read

SECTION HEADER #2
  .rdata name
    2262 virtual size
    8000 virtual address (00408000 to 0040A261)
    2400 size of raw data
    7000 file pointer to raw data (00007000 to 000093FF)
       0 file pointer to relocation table
```

```
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
40000040 flags
         Initialized Data
         Read Only

SECTION HEADER #3
   .data name
    2BAC virtual size
    B000 virtual address (0040B000 to 0040DBAB)
     E00 size of raw data
    9400 file pointer to raw data (00009400 to 0000A1FF)
       0 file pointer to relocation table
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
C0000040 flags
         Initialized Data
         Read Write

SECTION HEADER #4
  .reloc name
     B94 virtual size
    E000 virtual address (0040E000 to 0040EB93)
     C00 size of raw data
    A200 file pointer to raw data (0000A200 to 0000ADFF)
       0 file pointer to relocation table
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
42000040 flags
         Initialized Data
Discardable
         Read Only

  Summary

        3000 .data
        3000 .rdata
        1000 .reloc
        7000 .text

> dumpbin /all hello.exe
```

Este comando es parecido al anterior nos muestra la misma información con la diferencia que nos muestra la parte hexadecimal de cada una de las cabeceras disponible pero no nos muestra el código desensamblado.

```
Microsoft (R) COFF/PE Dumper Version 10.00.30319.01
Copyright (C) Microsoft Corporation.  All rights reserved.


Dump of file hello.exe

PE signature found
```

```
File Type: EXECUTABLE IMAGE

FILE HEADER VALUES
             14C machine (x86)
               4 number of sections
        4FAF2D84 time date stamp Sat May 12 22:41:56 2012
               0 file pointer to symbol table
               0 number of symbols
              E0 size of optional header
             102 characteristics
                   Executable
                   32 bit word machine

OPTIONAL HEADER VALUES
             10B magic # (PE32)
           10.00 linker version
            6C00 size of code
            5C00 size of initialized data
               0 size of uninitialized data
            125B entry point (0040125B)
            1000 base of code
            8000 base of data
          400000 image base (00400000 to 0040EFFF)
            1000 section alignment
             200 file alignment
            5.01 operating system version
            0.00 image version
            5.01 subsystem version
               0 Win32 version
            F000 size of image
             400 size of headers
               0 checksum
               3 subsystem (Windows CUI)
            8140 DLL characteristics
                   Dynamic base
                   NX compatible
                   Terminal Server Aware
          100000 size of stack reserve
            1000 size of stack commit
          100000 size of heap reserve
            1000 size of heap commit
               0 loader flags
              10 number of directories
               0 [       0] RVA [size] of Export Directory
            9CA4 [      28] RVA [size] of Import Directory
               0 [       0] RVA [size] of Resource Directory
               0 [       0] RVA [size] of Exception Directory
               0 [       0] RVA [size] of Certificates Directory
            E000 [     6E4] RVA [size] of Base Relocation Directory
               0 [       0] RVA [size] of Debug Directory
               0 [       0] RVA [size] of Architecture Directory
               0 [       0] RVA [size] of Global Pointer Directory
               0 [       0] RVA [size] of Thread Storage Directory
            9980 [      40] RVA [size] of Load Configuration Directory
               0 [       0] RVA [size] of Bound Import Directory
            8000 [     100] RVA [size] of Import Address Table Directory
               0 [       0] RVA [size] of Delay Import Directory
               0 [       0] RVA [size] of COM Descriptor Directory
               0 [       0] RVA [size] of Reserved Directory
```

```
SECTION HEADER #1
   .text name
    6BAA virtual size
    1000 virtual address (00401000 to 00407BA9)
    6C00 size of raw data
     400 file pointer to raw data (00000400 to 00006FFF)
       0 file pointer to relocation table
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
60000020 flags
         Code
         Execute Read

RAW DATA #1
00401000: 55 8B EC 68 40 80 40 00 E8 07 00 00 00 83 C4 04  U.ìh@.@.è.....Ä.

00401010: 33 C0 5D C3 53 56 57 BE 80 80 40 00 56 E8 0F 02  3À]ÃSVW¾..@.Vè..

00401020: 00 00 8B F8 8D 44 24 18 50 FF 74 24 18 56 E8 50  ...ø.D$.Pÿt$.VèP

00401030: 03 00 00 56 57 8B D8 E8 7D 02 00 00 83 C4 18 5F  ...VW.Øè}....Ä._

00401040: 5E 8B C3 5B C3 83 3D E8 86 40 00 02 74 05 E8 F6  ^.Ã[Ã.=è.@..t.èö

00401050: 0E 00 00 FF 74 24 04 E8 76 0D 00 00 68 FF 00 00  ...ÿt$.èv...hÿ..

00401060: 00 FF 15 50 80 40 00 59 59 C3 6A 18 68 D8 60 40  .ÿ.P.@.YYÃj.hØ`@

00401070: 00 E8 12 17 00 00 BF 94 00 00 00 8B C7 E8 5E 18  .è....¿.....Çè^.

00401080: 00 00 89 65 E8 8B F4 89 3E 56 FF 15 08 60 40 00  ...eè.ô.>Vÿ..`@.

00401090: 8B 4E 10 89 0D 04 87 40 00 8B 46 04 A3 10 87 40  .N.....@..F.£..@

004010A0: 00 8B 56 08 89 15 14 87 40 00 8B 76 0C 81 E6 FF  ..V.....@..v..æÿ

004010B0: 7F 00 00 89 35 08 87 40 00 83 F9 02 74 0C 81 CE  ....5..@..ù.t..Î

004010C0: 00 80 00 00 89 35 08 87 40 00 C1 E0 08 03 C2 A3  .....5..@.Áà..Â£

004010D0: 0C 87 40 00 33 FF 57 FF 15 00 60 40 00 66 81 38  ..@.3ÿWÿ..`@.f.8

004010E0: 4D 5A 75 1F 8B 48 3C 03 C8 81 39 50 45 00 00 75  MZu..H<.È.9PE..u

004010F0: 12 0F B7 41 18 3D 0B 01 00 00 74 1F 3D 0B 02 00  ..·A.=....t.=...

00401100: 00 74 05 89 7D E4 EB 27 83 B9 84 00 00 00 0E 76  .t..}äë'.¹.....v

00401110: F2 33 C0 39 B9 F8 00 00 00 EB 0E 83 79 74 0E 76  ò3À9¹ø...ë..yt.v

00401120: E2 33 C0 39 B9 E8 00 00 00 0F 95 C0 89 45 E4 57  â3À9¹è.....À.EäW

00401130: E8 02 16 00 00 59 85 C0 75 21 83 3D E8 86 40 00  è....Y.Àu!.=è.@.

00401140: 02 74 05 E8 01 0E 00 00 6A 1C E8 83 0C 00 00 68  .t.è....j.è....h
```

```
00401150: FF 00 00 00 E8 DE 0A 00 00 59 59 E8 35 15 00 00  ÿ...èÞ...YYè5...

00401160: 89 7D FC E8 82 13 00 00 85 C0 7D 08 6A 1B E8 D2  .}üè.....À}.j.èÒ

00401170: FE FF FF 59 FF 15 04 60 40 00 A3 84 9C 40 00 E8  þÿÿYÿ..`@.£..@.è

00401180: 44 12 00 00 A3 E0 86 40 00 E8 98 11 00 00 85 C0  D...£à.@.è.....À

00401190: 7D 08 6A 08 E8 AC FE FF FF 59 E8 54 0F 00 00 85  }.j.è¬þÿÿYèT....

004011A0: C0 7D 08 6A 09 E8 9B FE FF FF 59 6A 01 E8 B5 0A  À}.j.è.þÿÿYj.èµ.

004011B0: 00 00 59 89 45 DC 3B C7 74 07 50 E8 85 FE FF FF..Y.EÜ;Çt.Pè.þÿÿ

004011C0: 59 A1 24 87 40 00 A3 28 87 40 00 50 FF 35 1C 87  Y¡$.@.£(.@.Pÿ5..

004011D0: 40 00 FF 35 18 87 40 00 E8 23 FE FF FF 83 C4 0C  @.ÿ5..@.è#þÿÿ.Ä.

004011E0: 8B F0 89 75 D8 39 7D E4 75 06 56 E8 A2 0B 00 00  .ð.uØ9}äu.Vè¢...

004011F0: E8 BF 0B 00 00 EB 2B 8B 45 EC 8B 08 8B 09 89 4D  è¿...ë+.Eì.....M

SECTION HEADER #2
  .rdata name
    2262 virtual size
    8000 virtual address (00408000 to 0040A261)
    2400 size of raw data
    7000 file pointer to raw data (00007000 to 000093FF)
       0 file pointer to relocation table
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
40000040 flags
         Initialized Data
         Read Only

RAW DATA #2
00406000: 84 6E 00 00 98 6E 00 00 AA 6E 00 00 BA 6E 00 00  .n...n..ªn..ºn..

00406010: C8 6E 00 00 DA 6E 00 00 EE 6E 00 00 02 6F 00 00  Èn..Ún..în...o..

00406020: 0E 6F 00 00 1E 6F 00 00 34 6F 00 00 50 6F 00 00  .o...o..4o..Po..

00406030: 6A 6F 00 00 82 6F 00 00 9C 6F 00 00 B2 6F 00 00  jo...o...o..²o..

00406040: C2 6F 00 00 DC 6F 00 00 EE 6F 00 00 FC 6F 00 00  Âo..Üo..îo..üo..

00406050: 0E 70 00 00 1C 70 00 00 2A 70 00 00 38 70 00 00  .p...p..*p..8p..

00406060: 44 70 00 00 50 70 00 00 60 70 00 00 6A 70 00 00  Dp..Pp..`p..jp..

00406070: 76 70 00 00 82 70 00 00 92 70 00 00 A0 70 00 00  vp...p...p.. p..

00406080: AC 70 00 00 C2 70 00 00 D2 70 00 00 E6 70 00 00  ¬p..Âp..Òp..æp..

00406090: F8 70 00 00 12 71 00 00 22 71 00 00 38 71 00 00  øp...q.."q..8q..

004060A0: 4E 71 00 00 68 71 00 00 74 71 00 00 84 71 00 00  Nq..hq..tq...q..

004060B0: 9A 71 00 00 AA 71 00 00 BC 71 00 00 CE 71 00 00  .q..ªq..¼q..Îq..
```

```
004060C0: DE 71 00 00 EC 71 00 00 FE 71 00 00 10 72 00 00  Þq..ìq..þq...r..
004060D0: 00 00 00 00 00 00 00 00 FF FFFFFF F7 11 40 00  ........ÿÿÿÿ÷.@.
004060E0: 0B 12 40 00 00 00 00 00 06 00 00 06 00 01 00 00  ..@.............
004060F0: 10 00 03 06 00 06 02 10 04 45 45 45 05 05 05 05  .........EEE....
00406100: 05 35 30 00 50 00 00 00 00 20 28 38 50 58 07 08  .50.P.... (8PX..
00406110: 00 37 30 30 57 50 07 00 00 20 20 08 00 00 00 00  .700WP...  .....
00406120: 08 60 68 60 60 60 60 00 00 70 70 78 78 78 78 08  .`h````..ppxxxx.
00406130: 07 08 00 00 07 00 08 08 08 00 00 08 00 08 00 07  ................
00406140: 08 00 00 00 28 00 6E 00 75 00 6C 00 6C 00 29 00  ....(.n.u.l.l.).
00406150: 00 00 00 00 28 6E 75 6C 6C 29 00 00 43 6F 72 45  ....(null)..CorE
00406160: 78 69 74 50 72 6F 63 65 73 73 00 00 6D 73 63 6F  xitProcess..msco
00406170: 72 65 65 2E 64 6C 6C 00 72 75 6E 74 69 6D 65 20  ree.dll.runtime
00406180: 65 72 72 6F 72 20 00 00 0D 0A 00 00 54 4C 4F 53  error ......TLOS
00406190: 53 20 65 72 72 6F 72 0D 0A 00 00 00 53 49 4E 47  S error.....SING
004061A0: 20 65 72 72 6F 72 0D 0A 00 00 00 00 44 4F 4D 41   error......DOMA
004061B0: 49 4E 20 65 72 72 6F 72 0D 0A 00 00 00 00 00 00  IN error........
004061C0: 52 36 30 32 39 0D 0A 2D 20 54 68 69 73 20 61 70  R6029..- This ap
004061D0: 70 6C 69 63 61 74 69 6F 6E 20 63 61 6E 6E 6F 74  plicationcannot
004061E0: 20 72 75 6E 20 75 73 69 6E 67 20 74 68 65 20 61   run using the a
004061F0: 63 74 69 76 65 20 76 65 72 73 69 6F 6E 20 6F 66  ctive version of
00406200: 20 74 68 65 20 4D 69 63 72 6F 73 6F 66 74 20 2E   the Microsoft .
00406210: 4E 45 54 20 52 75 6E 74 69 6D 65 0A 50 6C 65 61  NET Runtime.Plea
00406220: 73 65 20 63 6F 6E 74 61 63 74 20 74 68 65 20 61  se contact the a
00406230: 70 70 6C 69 63 61 74 69 6F 6E 27 73 20 73 75 70  pplication's sup
00406240: 70 6F 72 74 20 74 65 61 6D 20 66 6F 72 20 6D 6F  port team for mo
00406250: 72 65 20 69 6E 66 6F 72 6D 61 74 69 6F 6E 2E 0D  re information..
00406260: 0A 00 00 00 52 36 30 32 38 0D 0A 2D 20 75 6E 61  ....R6028..- una
00406270: 62 6C 65 20 74 6F 20 69 6E 69 74 69 61 6C 69 7A  bletoinitializ
004071A0: 70 53 74 72 69 6E 67 57 00 00 B2 01 47 65 74 53  pStringW..².GetS
004071B0: 74 72 69 6E 67 54 79 70 65 41 00 00 B5 01 47 65  tringTypeA..µ.Ge
```

```
004071C0: 74 53 74 72 69 6E 67 54 79 70 65 57 00 00 2A 03  tStringTypeW..*.

004071D0: 53 65 74 53 74 64 48 61 6E 64 6C 65 00 00 2E 00  SetStdHandle....

004071E0: 43 6C 6F 73 65 48 61 6E 64 6C 65 00 6C 01 47 65  CloseHandle.l.Ge

004071F0: 74 4C 6F 63 61 6C 65 49 6E 66 6F 41 00 00 79 03  tLocaleInfoA..y.

00407200: 56 69 72 74 75 61 6C 50 72 6F 74 65 63 74 00 00  VirtualProtect..

00407210: BB 01 47 65 74 53 79 73 74 65 6D 49 6E 66 6F 00  ».GetSystemInfo.

00407220: 4B 45 52 4E 45 4C 33 32 2E 64 6C 6C 00 00        KERNEL32.dll..


Section contains the following imports:

    KERNEL32.dll
                408000 Import Address Table
                409CCC Import Name Table
                     0 time date stamp
                     0 Index of first forwarder reference

                  186 GetCommandLineA
                  2D3 HeapSetInformation
                   EE EnterCriticalSection
                  339 LeaveCriticalSection
                   CA DecodePointer
                  4D3 UnhandledExceptionFilter
                  4A5 SetUnhandledExceptionFilter
                  300 IsDebuggerPresent
                   EA EncodePointer
                  4C0 TerminateProcess
                  1C0 GetCurrentProcess
                  245 GetProcAddress
                  218 GetModuleHandleW
                  119 ExitProcess
                  525 WriteFile
                  264 GetStdHandle
                  214 GetModuleFileNameW
                  213 GetModuleFileNameA
                  161 FreeEnvironmentStringsW
                  511 WideCharToMultiByte
                  1DA GetEnvironmentStringsW
                  46F SetHandleCount
                  2E3 InitializeCriticalSectionAndSpinCount
                  1F3 GetFileType
                  263 GetStartupInfoW
                   D1 DeleteCriticalSection
                  4C5 TlsAlloc
                  4C7 TlsGetValue
                  4C8 TlsSetValue
                  4C6 TlsFree
                  2EF InterlockedIncrement
                  473 SetLastError
                  1C5 GetCurrentThreadId
                  202 GetLastError
                  2EB InterlockedDecrement
                  2CD HeapCreate
```

```
                  3A7 QueryPerformanceCounter
                  293 GetTickCount
                  1C1 GetCurrentProcessId
                  279 GetSystemTimeAsFileTime
                  4B2 Sleep
                  2CF HeapFree
                  172 GetCPInfo
                  168 GetACP
                  237 GetOEMCP
                  30A IsValidCodePage
                  418 RtlUnwind
                  33F LoadLibraryW
                  2CB HeapAlloc
                  2D2 HeapReAlloc
                  19A GetConsoleCP
                  1AC GetConsoleMode
                  157 FlushFileBuffers
                  32D LCMapStringW
                  367 MultiByteToWideChar
                  269 GetStringTypeW
                  466 SetFilePointer
                  304 IsProcessorFeaturePresent
                  2D4 HeapSize
                   52 CloseHandle
                  524 WriteConsoleW
                  487 SetStdHandle
                   8F CreateFileW

  Section contains the following load config:

            00000048 size
                   0 time date stamp
                0.00 Version
                   0 GlobalFlags Clear
                   0 GlobalFlags Set
                   0 Critical Section Default Timeout
                   0 Decommit Free Block Threshold
                   0 Decommit Total Free Threshold
            00000000 Lock Prefix Table
                   0 Maximum Allocation Size
                   0 Virtual Memory Threshold
                   0 Process Heap Flags
                   0 Process Affinity Mask
                   0 CSD Version
                0000 Reserved
            00000000 Edit list
            0040B410 Security Cookie
            004099D0 Safe Exception Handler Table
                   3 Safe Exception Handler Count

    Safe Exception Handler Table

          Address
          --------
          00402450
          00404D20
          00406EA0

SECTION HEADER #3
   .data name
```

```
    2BAC virtual size
    B000 virtual address (0040B000 to 0040DBAB)
     E00 size of raw data
    9400 file pointer to raw data (00009400 to 0000A1FF)
       0 file pointer to relocation table
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
C0000040 flags
         Initialized Data
         Read Write

RAW DATA #3
00408000: 00 00 00 00 42 4B 40 00 00 00 00 00 00 00 00 00  ....BK@.........

00408010: 7D 1B 40 00 5C 2F 40 00 6E 36 40 00 00 00 00 00  }.@.\/@.n6@.....

00408020: 00 00 00 00 23 1C 40 00 00 00 00 00 00 00 00 00  ....#.@.........

00408030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................

00408040: 48 65 6C 6C 6F 20 57 6F 72 6C 64 21 0A 00 00 00  Hello World!....

00408050: A3 1D 40 00 01 00 00 00 54 61 40 00 44 61 40 00  £.@.....Ta@.Da@.

00408060: 80 8C 40 00 00 00 00 00 80 8C 40 00 01 01 00 00  ..@.......@.....

00408070: 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00  ................

00408080: 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00  ................

00408090: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................

004080A0: 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00  ................

004080B0: 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................


SECTION HEADER #4
  .reloc name
     B94 virtual size
    E000 virtual address (0040E000 to 0040EB93)
     C00 size of raw data
    A200 file pointer to raw data (0000A200 to 0000ADFF)
       0 file pointer to relocation table
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
42000040 flags
Initialized Data
Discardable
ReadOnly

RAW DATA #4
0040E000: 00 10 00 00 88 00 00 00 04 30 17 30 BC 30 C7 30  .........0.0¼0Ç0

0040E010: D8 30 FD 30 0A 31 17 31 23 31 2F 31 35 31 47 31  Ø0ý0.1.1#1/151G1

0040E020: 4F 31 5A 31 A1 31 A6 31 B0 31 EA 31 EF 31 F6 31  O1Z1¡1¦1°1ê1ï1ö1
```

```
0040E030: FC 31 66 32 6C 32 86 32 95 32 A2 32 AE 32 BE 32  ü1f2l2.2.2¢2®2¾2
0040E040: C5 32 D4 32 E0 32 ED 32 11 33 23 33 31 33 46 33  Å2Ô2à2í2.3#313F3
0040E050: 50 33 76 33 A9 33 B8 33 C1 33 E5 33 14 34 56 34  P3v3©3¸3Á3å3.4V4
0040E060: 68 34 14 35 1C 35 31 35 3C 35 24 36 BC 36 DA 36  h4.5.515<5$6¼6Ú6
0040E070: 00 37 60 37 6F 37 8A 37 D8 3A C8 3B 13 3D 56 3D  .7`7o7.7Ø:È;.=V=
0040E080: 82 3D A3 3D 83 3F 00 00 00 20 00 00 CC 00 00 00  .=£=.?... ..Ì...
0040E090: A4 31 A8 31 AC 31 B0 31 B4 31 B8 31 BC 31 C0 31  ¤1¨1¬1°1´1¸1¼1À1
0040EB60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0040EB70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0040EB80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0040EB90: 00 00 00 00                                     ....
```

```
BASE RELOCATIONS #4
    1000 RVA,       88 SizeOfBlock
4  HIGHLOW              0040B000
17  HIGHLOW             004099F0
BC  HIGHLOW             0040B410
C7  HIGHLOW             0040BDE0
D8  HIGHLOW             0040BDEC
FD  HIGHLOW             00409A10
10A  HIGHLOW            0040DBA8
117  HIGHLOW            00408004
123  HIGHLOW            00400000
12F  HIGHLOW            0040003C
135  HIGHLOW            00400000
147  HIGHLOW            00400018
14F  HIGHLOW            00400074
15A  HIGHLOW            004000E8
1A1  HIGHLOW            00408000
1A6  HIGHLOW            0040DBA4
```

```
1B0  HIGHLOW          0040BDE4
1EA  HIGHLOW          0040BE10
1EF  HIGHLOW          0040BE14
1F6  HIGHLOW          0040BE08
1FC  HIGHLOW          0040BE04
266  HIGHLOW          0040B018
26C  HIGHLOW          0040DBA0
286  HIGHLOW          0040DBA0
295  HIGHLOW          0040CB9C
2A2  HIGHLOW          0040DBA0
2AE  HIGHLOW          0040CB9C
2BE  HIGHLOW          0040B018
2C5  HIGHLOW          0040CB9C
2D4  HIGHLOW          0040B298
2E0  HIGHLOW          0040B028
2ED  HIGHLOW          0040CA80
311  HIGHLOW          0040B088
323  HIGHLOW          0040BE28
331  HIGHLOW          0040CB9C
346  HIGHLOW          0040B018
350  HIGHLOW          0040B278
376  HIGHLOW          00408008
3A9  HIGHLOW          00408008
3B8  HIGHLOW          0040B018
3C1  HIGHLOW          0040B278
3E5  HIGHLOW          0040800C
414  HIGHLOW          0040800C
456  HIGHLOW          0040BDF0
468  HIGHLOW          0040BDF4
514  HIGHLOW          0040BCE8
```

```
51C  HIGHLOW           0040BAA0
531  HIGHLOW           0040B9A8
53C  HIGHLOW           0040BAA0
2000 RVA,          CC SizeOfBlock
1A4  HIGHLOW           0040198F
1A8  HIGHLOW           0040178E
1AC  HIGHLOW           004017BE
1B0  HIGHLOW           0040181C
1B4  HIGHLOW           00401868
1B8  HIGHLOW           00401873
1BC  HIGHLOW           004018B9
1C0  HIGHLOW           004019EA
1CD  HIGHLOW           0040BDFC
1DF  HIGHLOW           0040B410
2BF  HIGHLOW           0040801C
2C9  HIGHLOW           00408018
2D6  HIGHLOW           00408014
314  HIGHLOW           00408028
31B  HIGHLOW           00408024
328  HIGHLOW           0040BDFC
32E  HIGHLOW           00408010
36B  HIGHLOW           0040B2A0
387  HIGHLOW           0040B2A4
3AA  HIGHLOW           0040B408
3BD  HIGHLOW           0040B40C
3F1  HIGHLOW           00402450
40E  HIGHLOW           0040B410
462  HIGHLOW           0040B410
53C  HIGHLOW           0040CB98
544  HIGHLOW           0040CB98
```

```
55C  HIGHLOW            0040CB98
577  HIGHLOW            0040B410
5CE  HIGHLOW            0040B410
622  HIGHLOW            004025DF
628  HIGHLOW            0040801
635  HIGHLOW            004081C4
63B  HIGHLOW            00408030
3000 RVA,           150 SizeOfBlock
23  HIGHLOW             00408048
2F  HIGHLOW             00408048
49  HIGHLOW             00408060
6F  HIGHLOW             0040CA80
75  HIGHLOW             0040CA64
9F  HIGHLOW             0040CA80
E4  HIGHLOW             0040CA64
EB  HIGHLOW             0040CA84
100  HIGHLOW            0040CA64
147  HIGHLOW            0040CA64
151  HIGHLOW            0040CA64
17C  HIGHLOW            0040805C
194  HIGHLOW            0040CA80
1B2  HIGHLOW            00408058
1D6  HIGHLOW            0040CA80
206  HIGHLOW            0040803C
218  HIGHLOW            0040805C
246  HIGHLOW            00408058
269  HIGHLOW            0040CA64
26F  HIGHLOW            00408054
283  HIGHLOW            004099E0
288  HIGHLOW            004099E0
```

```
2A9  HIGHLOW            004099E8
2AE  HIGHLOW            004099E8
2CF  HIGHLOW            00408020
2D6  HIGHLOW            00408068
2E2  HIGHLOW            0040B45C
2E8  HIGHLOW            0040806C
2F4  HIGHLOW            0040C56C
2FA  HIGHLOW            00408010
303  HIGHLOW            0040B45C
309  HIGHLOW            00408070
312  HIGHLOW            0040B458
31E  HIGHLOW            0040C574
324  HIGHLOW            00408010
32C  HIGHLOW            0040B458
332  HIGHLOW            0040B45C
33E  HIGHLOW            00408074
344  HIGHLOW            0040B45C
4000 RVA,           A4 SizeOfBlock
0  HIGHLOW              0040B9A8
9  HIGHLOW              0040B9A8
13  HIGHLOW             00408078
47  HIGHLOW             0040C6D0
52  HIGHLOW             0040C6D0
5C  HIGHLOW             004080B0
75  HIGHLOW             0040C6D0
7F  HIGHLOW             004080AC
92  HIGHLOW             0040C6D0
B6  HIGHLOW             0040B410
ED  HIGHLOW             0040B9B0
122  HIGHLOW            004080B4
```

```
135  HIGHLOW           004080A8
1A5  HIGHLOW           0040B9C0
1C2  HIGHLOW           0040B9AC
20B  HIGHLOW           0040B9B4
27A  HIGHLOW           0040C6D0
299  HIGHLOW           00409B28
30E  HIGHLOW           00408088
31A  HIGHLOW           0040B580
32D  HIGHLOW           00408078
33F  HIGHLOW           0040BAA0
35A  HIGHLOW           0040C6E0
362  HIGHLOW           0040C6E4
36A  HIGHLOW           0040C6E8
381  HIGHLOW           0040C6D4
39A  HIGHLOW           0040B7A0
3B6  HIGHLOW           0040B8A8
3BF  HIGHLOW           0040B9A8
3C5  HIGHLOW           00408088
3CE  HIGHLOW           0040B9A8
6000 RVA,          AC SizeOfBlock
37  HIGHLOW            00408038
56  HIGHLOW            00408084
F3  HIGHLOW            00409C08
125  HIGHLOW           0040CA64
14D  HIGHLOW           0040CA80
1C7  HIGHLOW           00409C28
1F1  HIGHLOW           0040CA64
211  HIGHLOW           0040CA80
247  HIGHLOW           004080D0
251  HIGHLOW           00408084
```

```
2C6  HIGHLOW            0040B410
30F  HIGHLOW            004080D8
3A8  HIGHLOW            004080D4
478  HIGHLOW            0040804C
4F2  HIGHLOW            0040B410
515  HIGHLOW            004080D8
5AE  HIGHLOW            004080DC
999  HIGHLOW            0040BD28
9AB  HIGHLOW            0040BD2C
9BD  HIGHLOW            0040BD30
9CF  HIGHLOW            0040BD58
9E1  HIGHLOW            0040BD5C
A07  HIGHLOW            0040BD34
A19  HIGHLOW            0040BD38
A2B  HIGHLOW            0040BD3C
A3D  HIGHLOW            0040BD40
A4F  HIGHLOW            0040BD44
A61  HIGHLOW            0040BD48
A73  HIGHLOW            0040BD4C
A85  HIGHLOW            0040BD60
A97  HIGHLOW            0040BD64
AA9  HIGHLOW            0040BD68
ABB  HIGHLOW            0040BD6C
ACD  HIGHLOW            0040BD70
9000 RVA,           48 SizeOfBlock
8E8  HIGHLOW            0040C730
8EC  HIGHLOW            0040C788
9BC  HIGHLOW            0040B410
9C0  HIGHLOW            004099D0
A08  HIGHLOW            004010A8
```

```
A24  HIGHLOW           0040121D
A28  HIGHLOW           00401231
A48  HIGHLOW           0040289D
A68  HIGHLOW           004033EA
A74  HIGHLOW           004033F9
A90  HIGHLOW           004035AC
A9C  HIGHLOW           004035B8
AB8  HIGHLOW           004039A4
AD8  HIGHLOW           00403B2E
AE4  HIGHLOW           00403AFA
B00  HIGHLOW           00403CB1
B20  HIGHLOW           00404025
B40  HIGHLOW           004043F7
B60  HIGHLOW           0040477B
B7C  HIGHLOW           00404F0B
B80  HIGHLOW           00404F1E
B9C  HIGHLOW           00404F5C
BA0  HIGHLOW           00404F60
BC0  HIGHLOW           00405149
BE0  HIGHLOW           004052FD
C00  HIGHLOW           004059E8
C20  HIGHLOW           004061B9
C40  HIGHLOW           00406292
C60  HIGHLOW           00406C54
C80  HIGHLOW           004074D9
CA0  HIGHLOW           0040783B
0  ABS
B000 RVA,          114 SizeOfBlock
18  HIGHLOW            0040CBA0
20  HIGHLOW            0040CBA0
```

```
298  HIGHLOW           00408150
29C  HIGHLOW           00408140
9A8  HIGHLOW           0040B580
AA8  HIGHLOW           00409004
AAC  HIGHLOW           00409000
AB0  HIGHLOW           00408FFC
AB4  HIGHLOW           00408FF8
AB8  HIGHLOW           00408FF4
ABC  HIGHLOW           00408FF0
AC0  HIGHLOW           00408FEC
AC4  HIGHLOW           00408FE4
AC8  HIGHLOW           00408FDC
ACC  HIGHLOW           00408FD4
AD0  HIGHLOW           00408FC8
AD4  HIGHLOW           00408FBC
AD8  HIGHLOW           00408FB4
ADC  HIGHLOW           00408FA8
AE0  HIGHLOW           00408FA4
AE4  HIGHLOW           00408FA0
AE8  HIGHLOW           00408F9C
AEC  HIGHLOW           00408F98
AF0  HIGHLOW           00408F94
AF4  HIGHLOW           00408F90
AF8  HIGHLOW           00408F8C
AFC  HIGHLOW           00408F88
B00  HIGHLOW           00408F84
B04  HIGHLOW           00408F80
B08  HIGHLOW           00408F7C
B0C  HIGHLOW           00408F78
B10  HIGHLOW           00408F70
```

```
B14  HIGHLOW            00408F64

B18  HIGHLOW            00408F5C

B1C  HIGHLOW            00408F54

B20  HIGHLOW            00408F94

B24  HIGHLOW            00408F4C

B28  HIGHLOW            00408F44

B2C  HIGHLOW            00408F3C

B30  HIGHLOW            00408F30

B34  HIGHLOW            00408F28

B38  HIGHLOW            00408F1C

B3C  HIGHLOW            00408F10

Summary

        3000 .data
        3000 .rdata
        1000 .reloc
        7000 .text
```

4.5.5 Revisión de las cadenas de caracteres ASCII y Unicode

El siguiente comando que vamos a mostrar es el strings. El funcionamiento de strings consta de mostrar por pantalla las cadenas de caracteres ASCII contenidas en el archivo binario. Por defecto solamente busca en las variables globales o estáticas inicializadas y las secciones con información para cargar el proceso.

El strings no identifica el programa solo hace referencia a KERNELL32.dll que se trata de las librerías del S.O. de Windows y además hace referencia a un par de funciones.

Lo ejecutamos y obtenemos lo siguiente:

```
# strings hello.exe

uNSW
@u^V
t%HHt
HHtXHHt
HHty+
RPSW
90tW
?If90t
PPPPP
h0$@
Y__^[
9csm
8csm
uTVWh
j h0
PPPPP
<v*V
^SSSSS
t?VSP
Y[_^
PPPPP
>"u&
<tK<   tG
wf93t
f90u
f90u
VVV+
@PSVV
t*VV
j@j ^V
SWf9M
j@j
hu4@
u,9E
~,WPV
98t^
tVPV
t'Ou
woVW
GetCommandLineA
HeapSetInformation
EnterCriticalSection
LeaveCriticalSection
DecodePointer
UnhandledExceptionFilter
SetUnhandledExceptionFilter
IsDebuggerPresent
EncodePointer
TerminateProcess
GetCurrentProcess
GetProcAddress
GetModuleHandleW
ExitProcess
WriteFile
GetStdHandle
GetModuleFileNameW
GetModuleFileNameA
FreeEnvironmentStringsW
```

```
WideCharToMultiByte
GetEnvironmentStringsW
SetHandleCount
InitializeCriticalSectionAndSpinCount
GetFileType
GetStartupInfoW
DeleteCriticalSection
TlsAlloc
TlsGetValue
TlsSetValue
TlsFree
InterlockedIncrement
SetLastError
GetCurrentThreadId
GetLastError
InterlockedDecrement
HeapCreate
QueryPerformanceCounter
GetTickCount
GetCurrentProcessId
GetSystemTimeAsFileTime
Sleep
HeapFree
GetCPInfo
GetACP
GetOEMCP
IsValidCodePage
RtlUnwind
LoadLibraryW
HeapAlloc
HeapReAlloc
GetConsoleCP
GetConsoleMode
FlushFileBuffers
LCMapStringW
MultiByteToWideChar
GetStringTypeW
SetFilePointer
IsProcessorFeaturePresent
HeapSize
CloseHandle
WriteConsoleW
SetStdHandle
CreateFileW
KERNEL32.dll
Hello World!
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
1#1/151G1O1Z1
1f2l2
3#313F3P3v3
4V4h4
9E9R9W9e9@:c:n:
:';.;8;J;a;o;u;
&010;0T0^0q0
1Y2x2
393A3I3`3y3
4"464
```

```
5m506^6
7:7j8q8
=h>m>
?V?\?a?o?t?y?~?
0Q0V0]0b0i0n0|0
1I2N2W2f2
3&31373G3L3]3e3k3u3{3
4!4;4=6D6J6A7p7v7
1'212
:/:A:S:e:w:
; ;9;W;
=#=-=6=A=M=R=b=g=m=s=
=T>Y>l>
>U?o?x?
,0D0K0S0X0\0`0
0:1@1D1H1L1
272i2p2t2x2|2
2X3^3{3
454]4
6L7t7
8<8J8
1(1,1d:l:t:|:
:$:(:H:h:t:
; ;@;`;|;
<<@<`<
; ;$;(;,;0;4;8;<;@;D;H;L;P;`;d;h;l;p;t;x;|;
<h<x<
=(=,=0=4=8=<=@=D=H=L=X=\=`=d=h=l=p=t=x=|=
```

4.5.6 Editor Hexadecimal

Aunque el strings no mostraba bastante información sobre el binario, el visualizador hexadecimal nos permitirá examinar el archivo entero. En este caso usaremos la siguiente la herramienta WinHex, mostraremos una porción del archivo hello.exe.

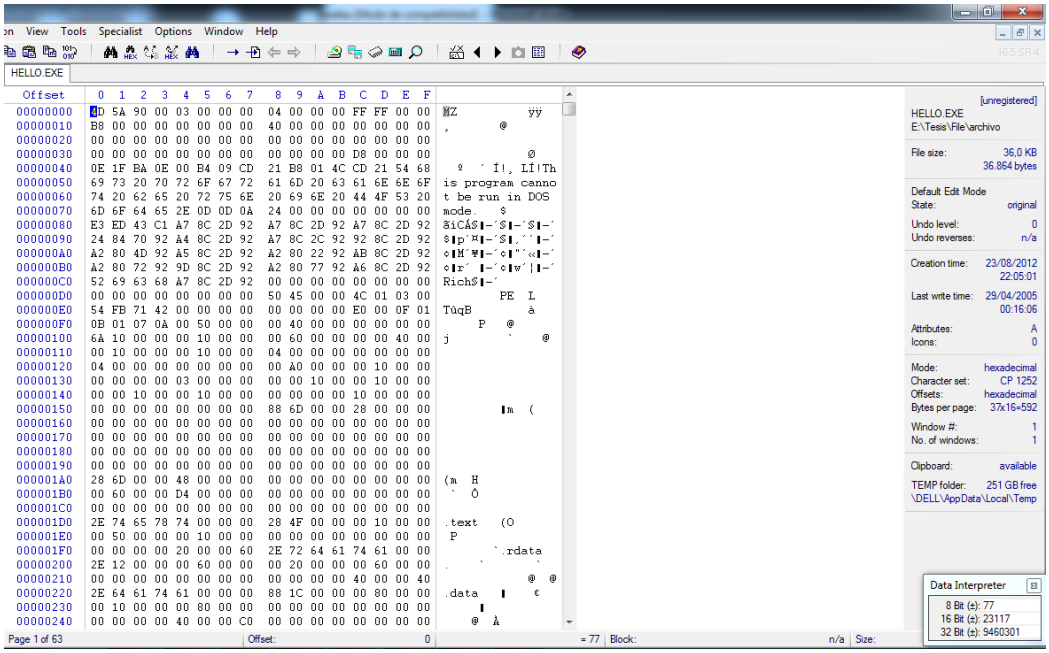


Figura 8.- Abriendo el archivo con el WinHex

```
00000000  4d 5a 90 00 03 00 00 00  04 00 00 00 ffff 00 00 |MZ..............|
00000010  b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00|........@.......|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 d8 00 00 00|................|
00000040  0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68|........!..L.!Th|
00000050  69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  |isprogramcanno|
00000060  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  |t be run in DO|
00000070  6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00|mode....$.......|
00000080  e3 ed 43 c1 a7 8c 2d 92  a7 8c 2d 92 a7 8c 2d 92  |..C...-...-...|
00000090  24 84 70 92 a4 8c 2d 92  a7 8c 2c 92 92 8c 2d 92  |$.p...-...,...|
000000a0  a2 80 4d 92 a5 8c 2d 92  a2 80 22 92 ab 8c 2d 92  |..M...-..."...|
000000b0  a2 80 72 92 9d 8c 2d 92  a2 80 77 92 a6 8c 2d 92  |..r...-...w...|
000000c0  52 69 63 68 a7 8c 2d 92  00 00 00 00 00 00 00 00  |Rich..........|
000000d0  00 00 00 00 00 00 00 00  50 45 00 00 4c 01 03 00|........PE..L...|
000000e0  54 fb 71 42 00 00 00 00  00 00 00 00 e0 00 0f 01|T.qB............|
000000f0  0b 01 07 0a 00 50 00 00  00 40 00 00 00 00 00 00|.....P...@......|
```

```
00000100  6a 10 00 00 00 10 00 00  00 60 00 00 00 00 40 00|j........`....@.|
00000110  00 10 00 00 00 10 00 00  04 00 00 00 00 00 00 00|................|
00000120  04 00 00 00 00 00 00 00  00 a0 00 00 00 10 00 00|................|
00000130  00 00 00 00 03 00 00 00  00 00 10 00 00 10 00 00|................|
00000140  00 00 10 00 00 10 00 00  00 00 00 00 10 00 00   |................|
00000150  00 00 00 00 00 00 00 00  88 6d 00 00 28 00 00 00|.........m..(...|
00000160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
000001a0  28 6d 00 00 48 00 00 00  00 00 00 00 00 00 00 00|(m..H...........|
000001b0  00 60 00 00 d4 00 00 00  00 00 00 00 00 00 00 00|.`..............|
000001c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
000001d0  2e 74 65 78 74 00 00 00  28 4f 00 00 00 10 00 00|.text...(O......|
000001e0  00 50 00 00 00 10 00 00  00 00 00 00 00 00 00 00|.P..............|
000001f0  00 00 00 00 20 00 00 60  2e 72 64 61 74 61 00 00  |.....`.rdata..|
00000200  2e 12 00 00 00 60 00 00  00 20 00 00 00 60 00 00  |.....`.....`..|
00000210  00 00 00 00 00 00 00 00  00 00 00 00 40 00 00 40|............@..@|
00000220  2e 64 61 74 61 00 00 00  88 1c 00 00 00 80 00 00|.data...........|
00000230  00 10 00 00 00 80 00 00  00 00 00 00 00 00 00 00|................|
00000240  00 00 00 00 40 00 00 c0  00 00 00 00 00 00 00 00|....@...........|
00000250  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00000260  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00000270  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00000280  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00000290  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
000002a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
000002b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
000002c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00008f40  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
```

```
00008f50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00008f60  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00008f70  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00008f90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00008fa0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00008fb0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00008fc0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00008fd0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00|................|
00009000  48 45 4c 4c 4f 2e 45 58  45 3a 20 50 45 33 32 20  |HELLO.EXE: PE3|
00009010  65 78 65 63 75 74 61 62  6c 65 20 66 6f 72 20 4d  |executable foM|
00009020  53 20 57 69 6e 64 6f 77  73 20 28 63 6f 6e 73 6f  |S Window(conso|
00009030  6c 65 29 20 49 6e 74 65  6c 20 38 30 33 38 36 20  |le) Intel 8038|
00009040  33 32 2d 62 69 74 0a                              |32-bit.|
```

El primer campo de esta estructura, en el desplazamiento 0000, hay dos caracteres: "MZ", que indican que se trata de un archivo ejecutable .EXE. Además MZ son las iniciales de Mark Zbikowski el cual fue el diseñador del formato de archivo ejecutable DOS.

Si se trata de un archivo con un programa W32, este campo apunta a dos caracteres: "PE" (Portable Ejecutable), el formato elegido por M$ para los archivos con programas W32.

El formato de PE es una estructura de datos que encapsula la información necesaria para el cargador del SO Windows para administrar el código ejecutable. El trozo de DOS sigue a la cabecera DOS y es responsable del

mensaje thisisprogramcannot be run in DOS mode. Para la compatibilidad con los anteriores sistemas operativos, el nuevo formato PE mantuvo la estructura original de la cabecera DOS.

4.5.7 PE Explorer

Una herramienta que nos será de mucha ayuda es el programa PE Explorer el cual analizará el archivo y nos mostrará un resumen de la información del encabezado PE y todos los recursos contenidos en el archivo PE y nos permitirá explorar los elementos específicos dentro de un archivo ejecutable.

A continuación observaremos la cabecera del archivo el cual nos indica que es un archivo PE trabaja en entorno Windows con arquitectura x86.

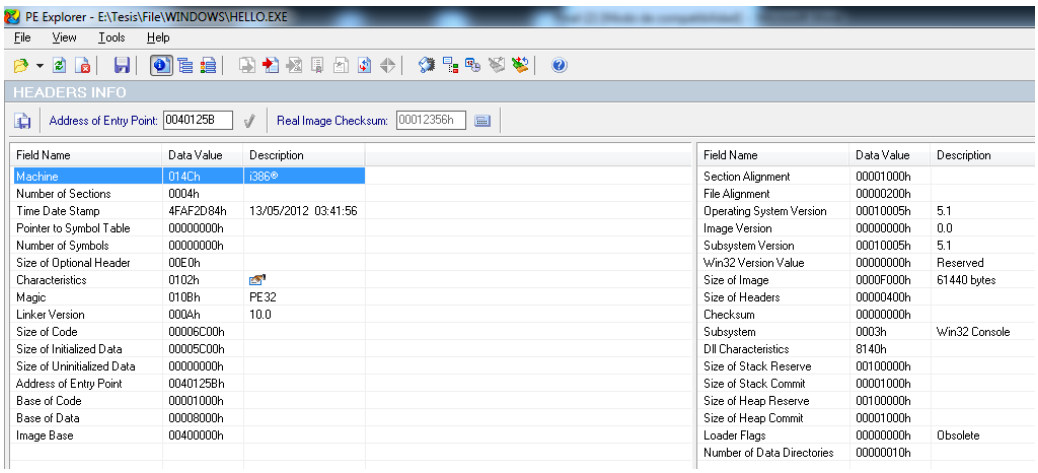


Figura 9.- Información de la cabecera del archivo

4.5.7.1 Dependencias

A continuación vamos a observar las dependencia eso quiero decir que vamos a observar todos los módulos a los que está vinculado estáticamente el

archivo PE y los que están cargados con demora, y nos va a mostrar en una estructura jerárquica de árbol, donde se muestra hasta dónde abarca el archivo ejecutable. Además vemos las listas de todas las funciones que exportan dicho módulo y cuáles de estas funciones son actualmente utilizadas por otros módulos del sistema y observamos el conjunto mínimo de archivos requeridos para un módulo en concreto con una información detallada de cada uno de estos archivos requeridos como la ruta en el sistema o el número de versión.

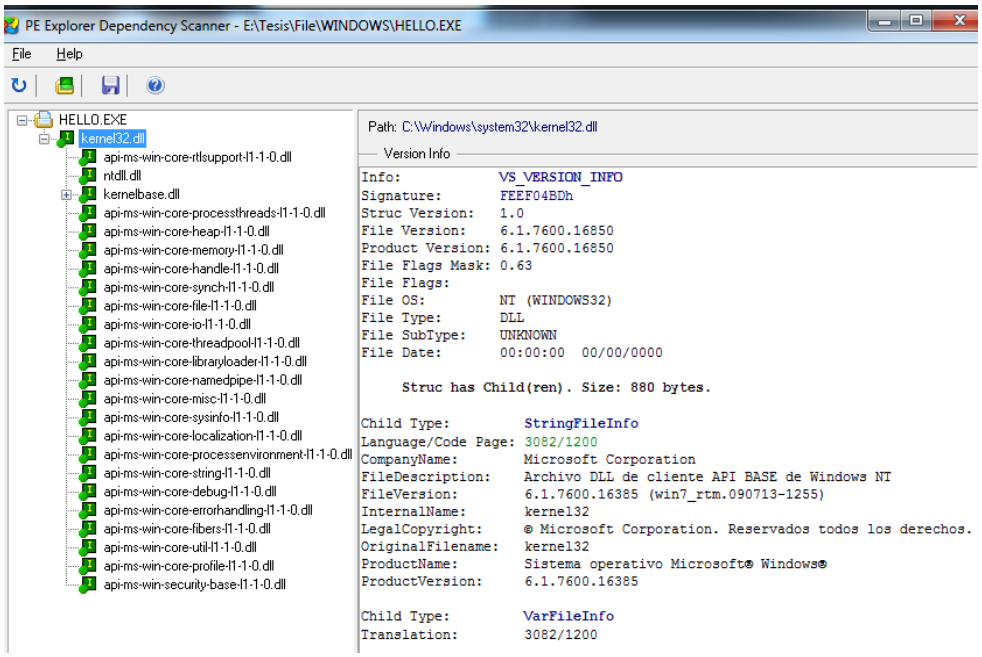


Figura 10.- Dependencias del archivo

4.5.8 Desensamblador IDA

Lo siguiente que vamos a realizar es utilizar un desensamblador para ello utilizaremos la herramienta IDA que es un desensamblador empleado para

ingeniería inversa, primeramente abriremos el programa y nos mostrara un cuadro en nuestro caso le daremos click al botón Previous con el cual se nos abrirá uno de las archivos de la lista de archivos recientes que se encuentra directamente debajo del botón. La lista de archivos usados recientemente se rellena con los valores ida.reg en plataformas que no sean Windows.

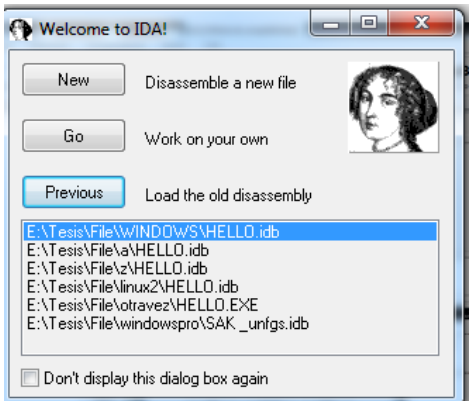


Figura 11.- Abriendo el achivo en IDA

Al elegir para abrir un nuevo archivo, se nos presentará un cuadro de dialogo, IDA genera una lista de tipos de archivo posibles y muestra la lista en la parte superior del cuadro del diálogo. Esta lista representa a los cargadores del IDA que son más adecuados para hacer frente al archivo seleccionado.

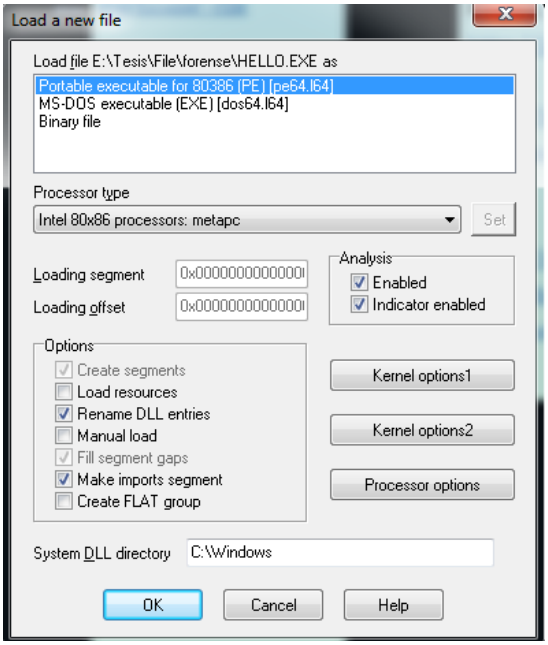


Figura 12.- Cargando el nuevo archivo en el IDA

Luego de esto se nos abrirá la ventana de texto que es la visualización tradicional utilizada para ver y manipular el archivo generado. La pantalla de texto presenta el listado completo del desmontaje de un programa y nos proporciona el único medio para visualizar las regiones de datos de un binario.

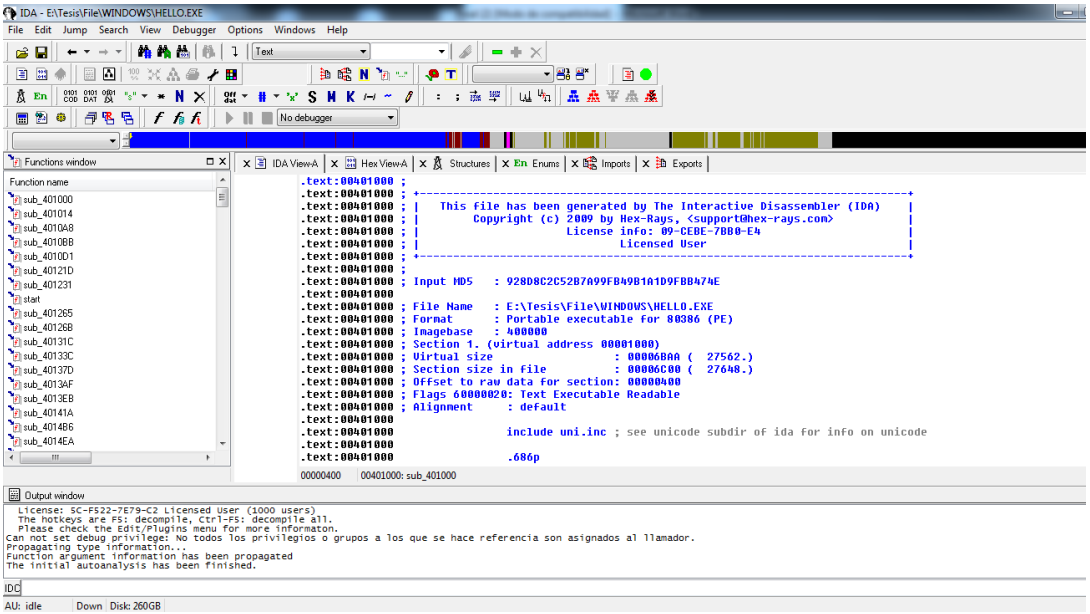


Figura 13.- Visualización del archivo binario

A continuación mostraremos una parte del texto de lo que nos mostró al analizar el archivo hello.exe

```
.text:00401000 ; +-------------------------------------------------------------
---------------+
.text:00401000 ;
.text:00401000 ; Input MD5   : 928D8C2C52B7A99FB49B1A1D9FBB474E
.text:00401000
.text:00401000 ; File Name   : E:\Tesis\File\WINDOWS\HELLO.EXE
.text:00401000 ; Format      : Portable executable for 80386 (PE)
.text:00401000 ;Imagebase    : 400000
.text:00401000 ; Section 1. (virtual address 00001000)
.text:00401000 ; Virtual size                  : 00006BAA (  27562.)
.text:00401000 ; Section size in file          : 00006C00 (  27648.)

.text:00401000 ; Offset to raw data for section: 00000400
.text:00401000 ; Flags 60000020: Text Executable Readable
.text:00401000 ; Alignment     : default
.text:00401000
.text:00401000                 include uni.inc ; see unicodesubdir of ida
for info on unicode
.text:00401000
.text:00401000                 .686p
.text:00401000                 .mmx
.text:00401000                 .model flat
.text:00401000
.text:00401000 ;
===========================================================================
.text:00401000
```

```
.text:00401000 ; Segment type: Pure code
.text:00401000 ; Segment permissions: Read/Execute
.text:00401000 _text           segment para public 'CODE' use32
.text:00401000                 assume cs:_text
.text:00401000                 ;org 401000h
.text:00401000                 assume es:nothing, ss:nothing, ds:_data,
fs:nothing, gs:nothing
.text:00401000
.text:00401000 ; =============== S U B R O U T I N E
=======================================
.text:00401000
.text:00401000 ; Attributes: bp-based frame
.text:00401000
.text:00401000 sub_401000      proc near               ; CODE XREF: start-
5Bp
.text:00401000                 push    ebp
.text:00401001                 movebp, esp
.text:00401003                 push    offset aHelloWorld ; "Hello World!\n"
.text:00401008                 call    sub_401014
.text:0040100D                 add     esp, 4
.text:00401010                 xoreax, eax
.text:00401012                 pop     ebp
.text:00401013                 retn
.text:00401013 sub_401000      endp
.text:00401013
.text:00401014
.text:00401014 ; =============== S U B R O U T I N E
=======================================
.text:00401014
.text:00401014
.text:00401014 sub_401014      proc near               ; CODE XREF:
sub_401000+8p
.text:00401014                 push    0Ch
.text:00401016                 push    offset unk_4099F0
.text:0040101B                 call    sub_4023F0
.text:00401020                 xoreax, eax
.text:00401022                 xoresi, esi
.text:00401024                 cmp     [ebp+8], esi
.text:00401027                 setnz   al
.text:0040102A                 cmpeax, esi
.text:0040102C                 jnz     short loc_401043
.text:0040102E                 call    sub_4023A0
.text:00401033                 movdwordptr [eax], 16h
.text:00401039                 call    sub_40234E
.text:0040103E                 or      eax, 0FFFFFFFFh
.text:00401041                 jmp     short loc_4010A2
```

4.6 Análisis Dinámico

Este tipo de análisis se centra en cómo se comporta el código cuando es ejecutado el código malicioso y el uso de utilidades para ver cómo el proceso interactúa con el

sistema de archivos, el registro, la interfaces de programación de aplicaciones, y el sistema operativo.

4.6.1 Debugger OllyDBG

En nuestro caso vamos a utilizar el depurador OllyDbg, al abrir nuestro depurador nos aparecerá un cuadro de dialogo avisándonos que la DLL que está en la carpeta de OLLYDBG es más antigua que la de sistema, si apretamos SI, borrara la antigua de la carpeta del OLLY usara la de sistema, en este caso voy a elegir No, significa que usara la propia antes del sistema, ya que fue concebido con esa dll.

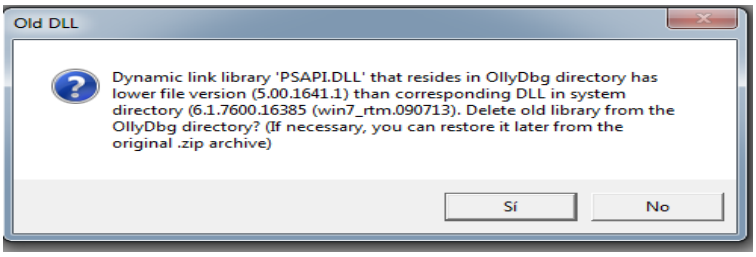


Figura 14.- Elección del DLL

Se abrirá la ventana para que busquemos el archivo a debuggear en este caso es el hello.exe

A lo que se nos abre el programa aplastaremos F9 para que corra el programa, nos daremos cuenta que está dividido en cuatro secciones analizaremos cada una de esas secciones.

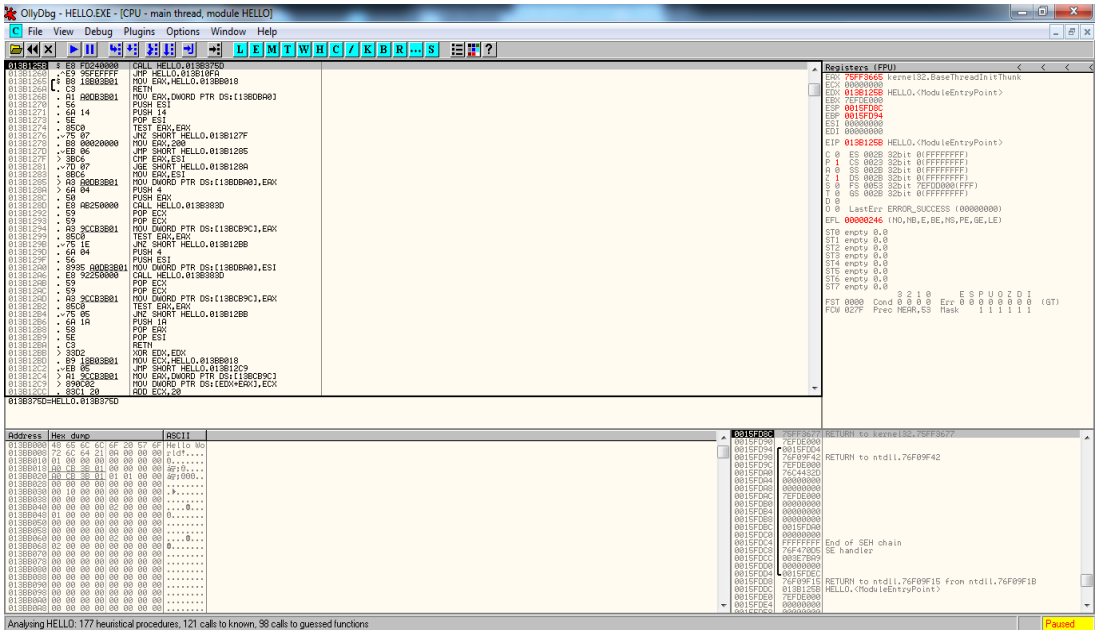


Figura 15.- Visualización del archivo hello.exe en OllyDbg

La primera ventana nos mostrara el listado desensamblado del programa que vamos a debuggear.

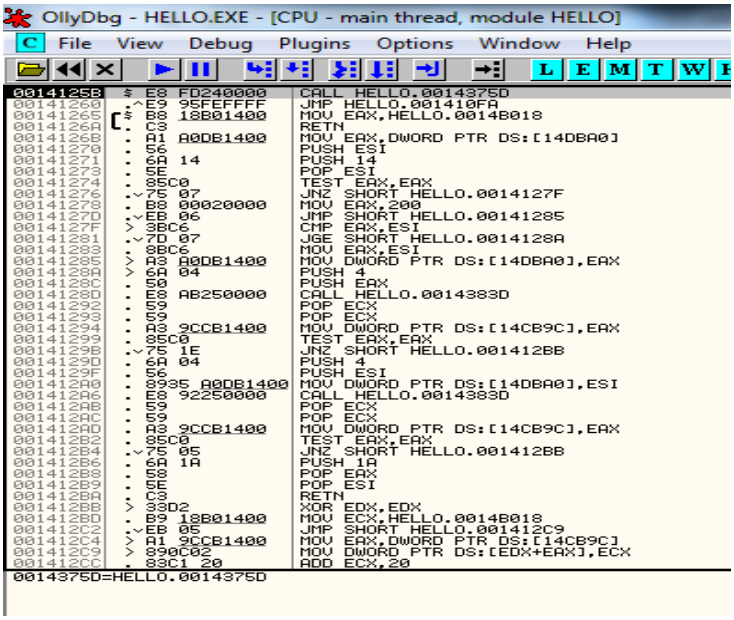


Figura 16.- Visualización del programa a Debuggear

En la segunda ventana nos mostrara los registros ya que el procesador necesita asistentes en su tarea de ejecutar los programas, los registros nos ayudan en ello. Los otros registros pueden tomar valores variables y sirven para asistir al procesador en las ejecuciones de las instrucciones.

Vemos que son EAX, ECX, EDX, EBX, ESP, EBP, ESI, EDI y EIP

Esos son los llamados registros de 32 bits

Debajo de los registros se encuentran los flags vemos que son C P A Z S T D y O.

Solo pueden tener valores de cero o uno, que nos advierten que al ejecutar determinada instrucción, ha ocurrido algo, según el flag que sea.

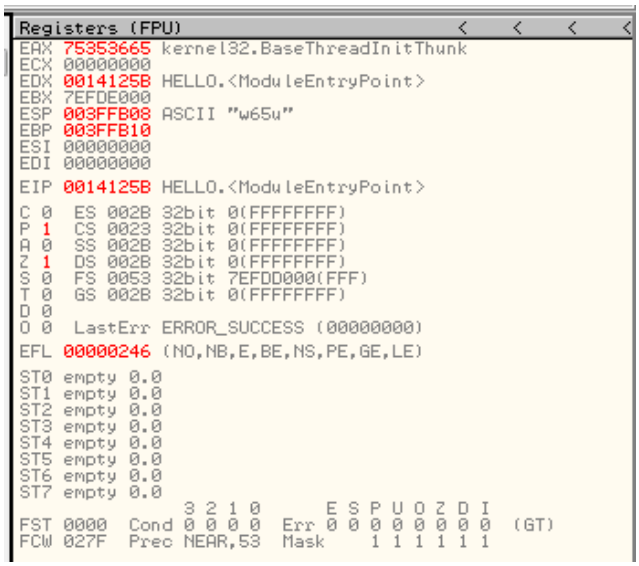


Figura 17.- Registros del programa

En la tercera ventana nos mostrara el stack o pila esta es una zona de la memoria, en la cual se van guardando datos que más adelante deben ser

recuperados.

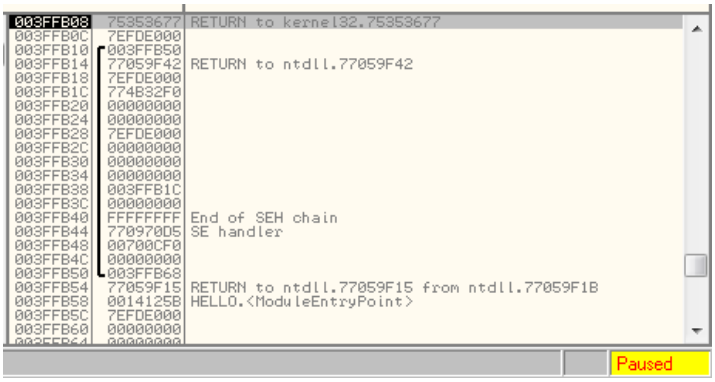


Figura 18.- Stack del programa

Y la última ventana a mostrar es el dump que por default nos mostrara la visualización hexadecimal del programa ejecutado.

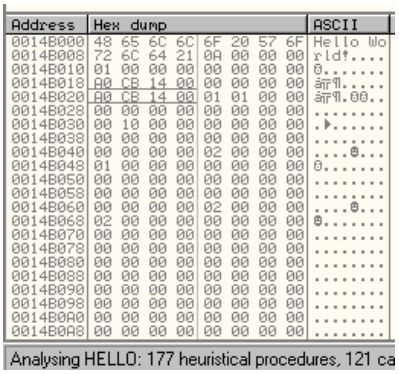


Figura 19.- Visualización del hexadecimal del programa

A continuación con la ayuda de la opción E nos mostrara el listado de los ejecutables que utiliza el programa, en nuestro caso observamos que esta utilizando el .exe y el .dll

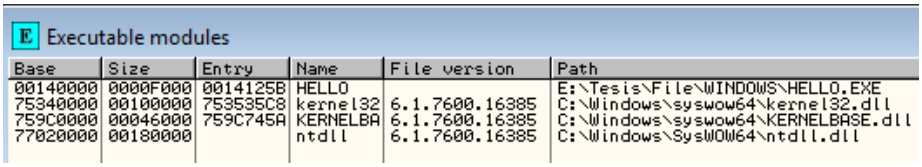


Figura 20.- Listado de los ejecutables

Con la opción M nos mostrara la memoria ocupada por nuestro programa, se observa las diversas secciones allocadas por el sistema además de las secciones del ejecutable, y las dlls que utiliza el proceso.

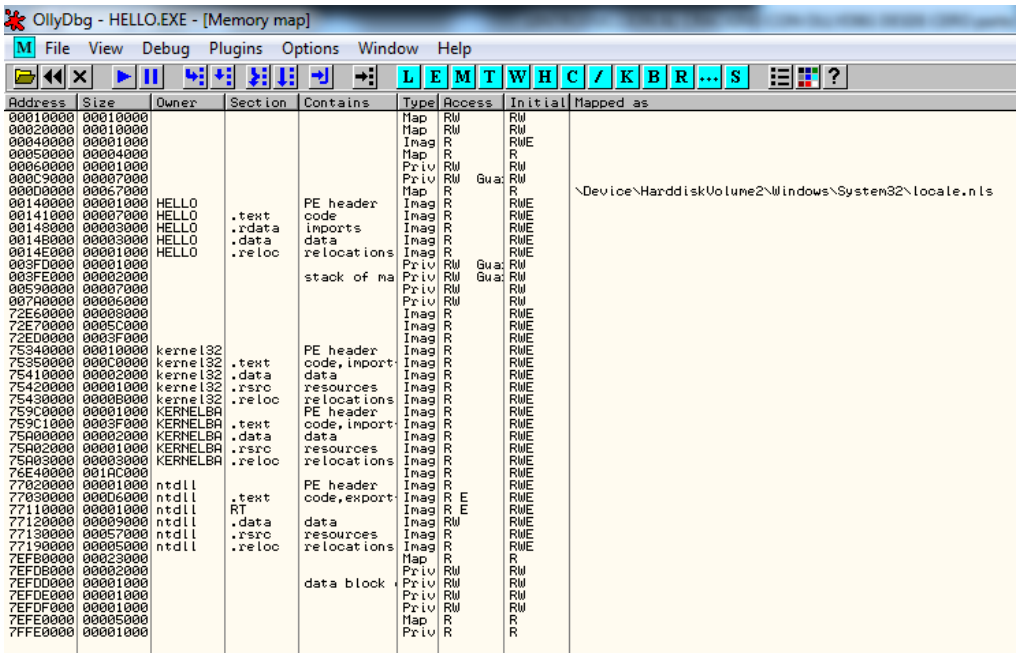
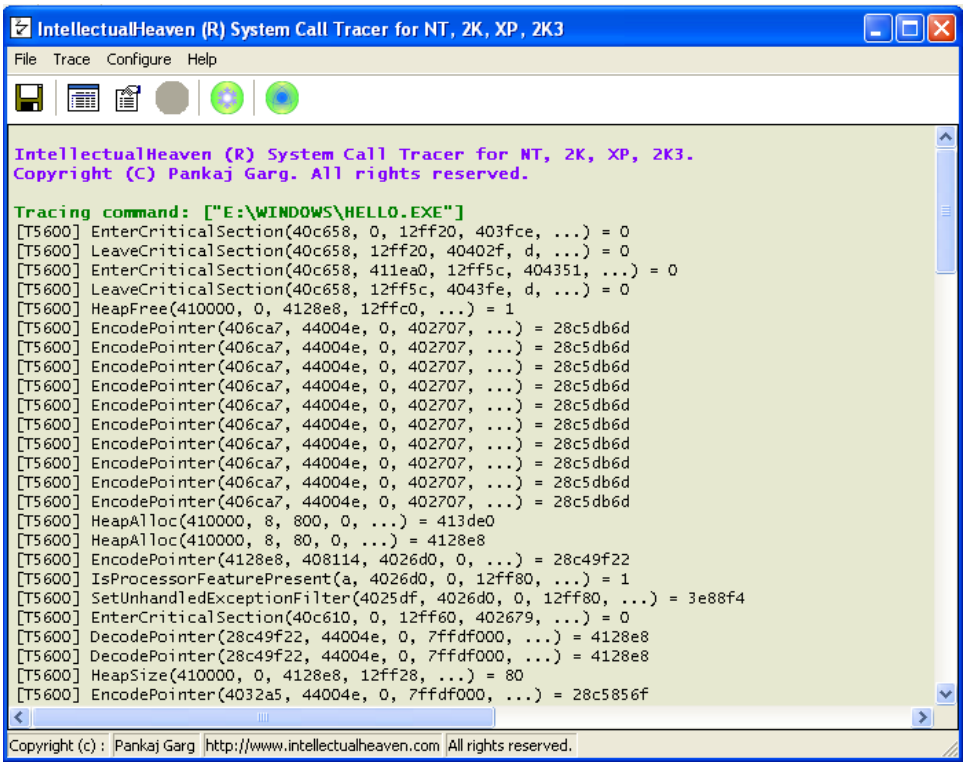


Figura 21.- Memoria del programa

4.6.2 Usando StraceNT

El siguiente programa que utilizaremos nos ayuda a rastrear el uso de las llamadas del sistema por un proceso ejecutado, es esencialmente una intervención telefónica entre un programa y el sistema operativo. Nos va a mostrar información sobre el acceso a archivos, acceso a redes, acceso de memoria.



```
IntellectualHeaven (R) System Call Tracer for NT, 2K, XP, 2K3.
Copyright (C) Pankaj Garg. All rights reserved.

Tracing command: ["E:\WINDOWS\HELLO.EXE"]
[T5600] EnterCriticalSection(40c658, 0, 12ff20, 403fce, ...) = 0
[T5600] LeaveCriticalSection(40c658, 12ff20, 40402f, d, ...) = 0
[T5600] EnterCriticalSection(40c658, 411ea0, 12ff5c, 404351, ...) = 0
[T5600] LeaveCriticalSection(40c658, 12ff5c, 4043fe, d, ...) = 0
[T5600] HeapFree(410000, 0, 4128e8, 12ffc0, ...) = 1
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] HeapAlloc(410000, 8, 800, 0, ...) = 413de0
[T5600] HeapAlloc(410000, 8, 80, 0, ...) = 4128e8
[T5600] EncodePointer(4128e8, 408114, 4026d0, 0, ...) = 28c49f22
[T5600] IsProcessorFeaturePresent(a, 4026d0, 0, 12ff80, ...) = 1
[T5600] SetUnhandledExceptionFilter(4025df, 4026d0, 0, 12ff80, ...) = 3e88f4
[T5600] EnterCriticalSection(40c610, 0, 12ff60, 402679, ...) = 0
[T5600] DecodePointer(28c49f22, 44004e, 0, 7ffdf000, ...) = 4128e8
[T5600] DecodePointer(28c49f22, 44004e, 0, 7ffdf000, ...) = 4128e8
[T5600] HeapSize(410000, 0, 4128e8, 12ff28, ...) = 80
[T5600] EncodePointer(4032a5, 44004e, 0, 7ffdf000, ...) = 28c5856f
```

Figura 22.- Visualización del programa StraceNT

```
IntellectualHeaven (R) System Call Tracer for NT, 2K, XP, 2K3.
Copyright (C) Pankaj Garg. All rights reserved.

Tracing command: ["E:\WINDOWS\HELLO.EXE"]
[T5600] EnterCriticalSection(40c658, 0, 12ff20, 403fce, ...) = 0
[T5600] LeaveCriticalSection(40c658, 12ff20, 40402f, d, ...) = 0
[T5600] EnterCriticalSection(40c658, 411ea0, 12ff5c, 404351, ...) = 0
[T5600] LeaveCriticalSection(40c658, 12ff5c, 4043fe, d, ...) = 0
[T5600] HeapFree(410000, 0, 4128e8, 12ffc0, ...) = 1
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
```

```
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] EncodePointer(406ca7, 44004e, 0, 402707, ...) = 28c5db6d
[T5600] HeapAlloc(410000, 8, 800, 0, ...) = 413de0
[T5600] HeapAlloc(410000, 8, 80, 0, ...) = 4128e8
[T5600] EncodePointer(4128e8, 408114, 4026d0, 0, ...) = 28c49f22
[T5600] IsProcessorFeaturePresent(a, 4026d0, 0, 12ff80, ...) = 1
[T5600] SetUnhandledExceptionFilter(4025df, 4026d0, 0, 12ff80, ...) = 3e88f4
[T5600] EnterCriticalSection(40c610, 0, 12ff60, 402679, ...) = 0
[T5600] DecodePointer(28c49f22, 44004e, 0, 7ffdf000, ...) = 4128e8
[T5600] DecodePointer(28c49f22, 44004e, 0, 7ffdf000, ...) = 4128e8
[T5600] HeapSize(410000, 0, 4128e8, 12ff28, ...) = 80
[T5600] EncodePointer(4032a5, 44004e, 0, 7ffdf000, ...) = 28c5856f
[T5600] EncodePointer(4128ec, 44004e, 0, 7ffdf000, ...) = 28c49f26
[T5600] LeaveCriticalSection(40c610, 12ff60, 402682, 8, ...) = 0
[T5600] EnterCriticalSection(40c6a0, 0, 12ff30, 401393, ...) = 0
[T5600] HeapAlloc(410000, 0, 1000, 40bdf4, ...) = 4145f8
[T5600] GetLastError(40b000, 12fccc, 403483, 12fccc, ...) = 7f
[T5600] TlsGetValue(1, 12fccc, 403419, 2, ...) = 7c8097e0
[T5600] SetLastError(7f, 40b000, 12fccc, 403483, ...) = 7ffde000
[T5600] EnterCriticalSection(41211c, 86e865ab, 40ca80, 40, ...) = 0
[T5600] GetLastError(40, 1, 403483, 1, ...) = 7f
[T5600] TlsGetValue(1, 1, 403419, 2, ...) = 7c8097e0
[T5600] SetLastError(7f, 40, 1, 403483, ...) = 7ffde000
[T5600] GetConsoleMode(7, 12e3cc, 1, 40ca80, ...) = 1
[T5600] WriteFile(7, 12e3f4, e, 12e3d4, ...) = 1
[T5600] LeaveCriticalSection(41211c, 12fef0, 4061c2, 1, ...) = 0
[T5600] LeaveCriticalSection(40c6a0, 12ff2c, 40140b, 11, ...) = 0
```

```
[T5600] EnterCriticalSection(40c610, 0, 12ff6c, 402785, ...) = 0
[T5600] DecodePointer(28c49f22, 86e86473, 44004e, 0, ...) = 4128e8
[T5600] DecodePointer(28c49f26, 86e86473, 44004e, 0, ...) = 4128ec
[T5600] EncodePointer(0, 4027e9, 86e86473, 44004e, ...) = 2885b7ca
[T5600] DecodePointer(28c5856f, 86e86473, 44004e, 0, ...) = 4032a5
[T5600] EncodePointer(0, 4027fc, 86e86473, 44004e, ...) = 2885b7ca
[T5600] DecodePointer(28c49f22, 86e86473, 44004e, 0, ...) = 4128e8
[T5600] DecodePointer(28c49f26, 86e86473, 44004e, 0, ...) = 4128ec
[T5600] EnterCriticalSection(40c598, 450038, 12ff18, 403a78, ...) = 0
[T5600] EnterCriticalSection(40c688, 0, 12fed4, 401393, ...) = 0
[T5600] LeaveCriticalSection(40c688, 12fed0, 40140b, 10, ...) = 0
[T5600] EnterCriticalSection(40c6a0, 1, 12fed4, 401393, ...) = 0
[T5600] LeaveCriticalSection(40c6a0, 12fed0, 40140b, 11, ...) = 0
[T5600] EnterCriticalSection(40c6b8, 2, 12fed4, 401393, ...) = 0
[T5600] LeaveCriticalSection(40c6b8, 12fed0, 40140b, 12, ...) = 0
[T5600] LeaveCriticalSection(40c598, 12ff18, 403b35, 1, ...) = 0
[T5600] HeapFree(410000, 0, 413de0, 12ff6c, ...) = 1
[T5600] LeaveCriticalSection(40c610, 12ff6c, 402894, 8, ...) = 0
[T5600] GetModuleHandleW(4081c4, 12ff20, 402667, 0, ...) = 0
[T5600] ExitProcess(0, 12ff6c, 40289d, 0, ...) [T5600] ReadProcessMemory(10,
7ffdf00c, 12f2fc, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241eb4, 12f300, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241ee0, 12f288, 50, ...) = 1
[T5600] ReadProcessMemory(10, 241f48, 12f288, 50, ...) = 1
[T5600] ReadProcessMemory(10, 242010, 12f288, 50, ...) = 1
[T5600] ReadProcessMemory(10, 2420e0, 12f288, 50, ...) = 1
[T5600] ReadProcessMemory(10, 2421a0, 12f288, 50, ...) = 1
[T5600] ReadProcessMemory(10, 7ffdf00c, 12f2b4, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241eb4, 12f2b8, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241ee0, 12f2d0, 50, ...) = 1
```

```
[T5600] ReadProcessMemory(10, 209da, 12f344, 14, ...) = 1
[T5600] ReadProcessMemory(10, 7ffdf00c, 12f280, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241eb4, 12f284, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241ee0, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 7ffdf00c, 12f2b4, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241eb4, 12f2b8, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241ee0, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 241f48, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 7c93040c, 12f344, 14, ...) = 1
[T5600] ReadProcessMemory(10, 7ffdf00c, 12f280, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241eb4, 12f284, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241ee0, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 241f48, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 7ffdf00c, 12f2b4, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241eb4, 12f2b8, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241ee0, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 241f48, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 242010, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 241fd8, 12f344, 1a, ...) = 1
[T5600] ReadProcessMemory(10, 7ffdf00c, 12f280, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241eb4, 12f284, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241ee0, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 241f48, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 242010, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 7ffdf00c, 12f2b4, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241eb4, 12f2b8, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241ee0, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 241f48, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 242010, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 2420e0, 12f2d0, 50, ...) = 1
```

```
[T5600] ReadProcessMemory(10, 2420ba, 12f344, c, ...) = 1
[T5600] ReadProcessMemory(10, 7ffdf00c, 12f280, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241eb4, 12f284, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241ee0, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 241f48, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 242010, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 2420e0, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 7ffdf00c, 12f2b4, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241eb4, 12f2b8, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241ee0, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 241f48, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 242010, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 2420e0, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 2421a0, 12f2d0, 50, ...) = 1
[T5600] ReadProcessMemory(10, 242170, 12f344, 14, ...) = 1
[T5600] ReadProcessMemory(10, 7ffdf00c, 12f280, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241eb4, 12f284, 4, ...) = 1
[T5600] ReadProcessMemory(10, 241ee0, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 241f48, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 242010, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 2420e0, 12f2a8, 50, ...) = 1
[T5600] ReadProcessMemory(10, 2421a0, 12f2a8, 50, ...) = 1
Target process has been terminated. Exit Code = 0.
```

4.7 Análisis de los archivos Sak.exe

(SAK.EXE, SAK_OL~1.EXE, SAK_UN~1.EXE, SAK_UN~2.EXE)

4.7.1 Información general de los archivos a analizar

Debido a que realizaremos los primeros análisis de los archivos SAK.EXE, SAK_OL~1.EXE, SAK_UN~1.EXE, SAK_UN~2.EXE, están en un archivo WINDOWS.rar (comprimido WINRAR), se llevara a cabo un proceso para su extracción y análisis.

Se procede al análisis del archivo SAK.EXE, será descompreso usando un ambiente LINUX CAINE.

Comandos para análisis en entrono LINUX.

Descargar descompresor en CAINE: -apt –get install rar unrar.

Creamos las siguientes carpetas: windows, textoanalisis, imagenanalisis.

En la carpeta asignada textoanalisis enviaremos archivos de textos con las salidas de los comandos ejecutados.

En la carpeta asignada imagenanalisis enviaremos de imagen con las salidas de los comandos ejecutados.

Descomprimir archivo WINDOWS en la nueva carpeta en el mismo directorio nombrada windows:

unrar e WINDOWS.rar ./windows

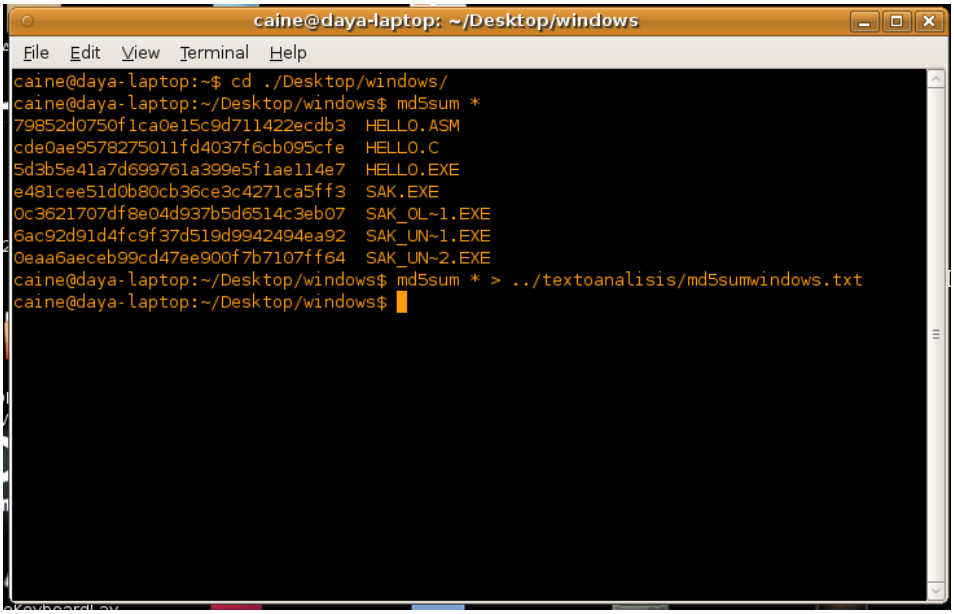


Figura 23.- Información general de los archivos a analizar

Para generar un MD5 Hash de todos los archivos en la carpeta windows y crear con esta información una archivo de texto y enviarlo al directorio. /textoanalisis.

cd ./windows

md5sum *

md5sum * >...//textoanalisis/md5sumwindows.txt

Revisamos el tamaño, permisos y fecha de creación de los archivos en el fichero windows:

la - l *

la -l * > ../textoanalisis/lalswindows.txt

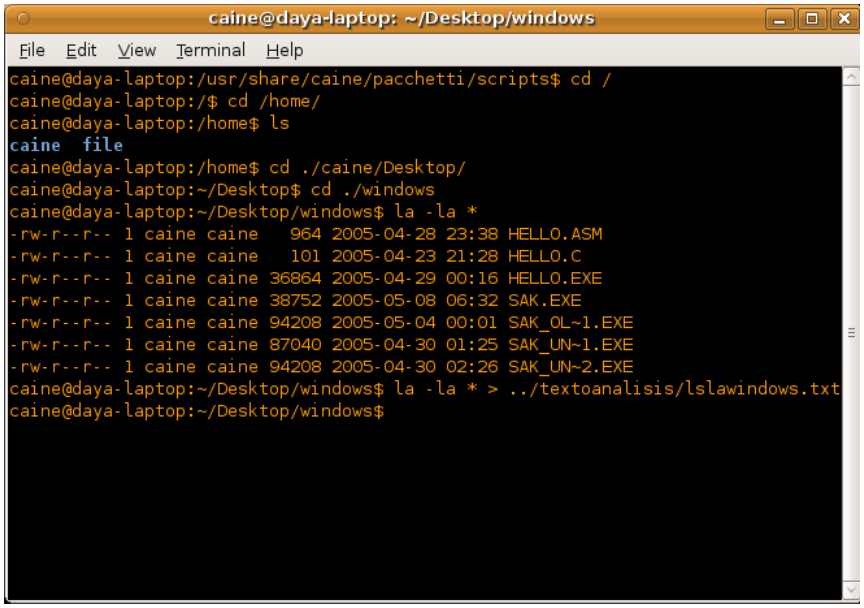


Figura 24.- Información general de los archivos

Borramos los Ficheros nombrados HELLO, ya que con anterioridad se analizaron.

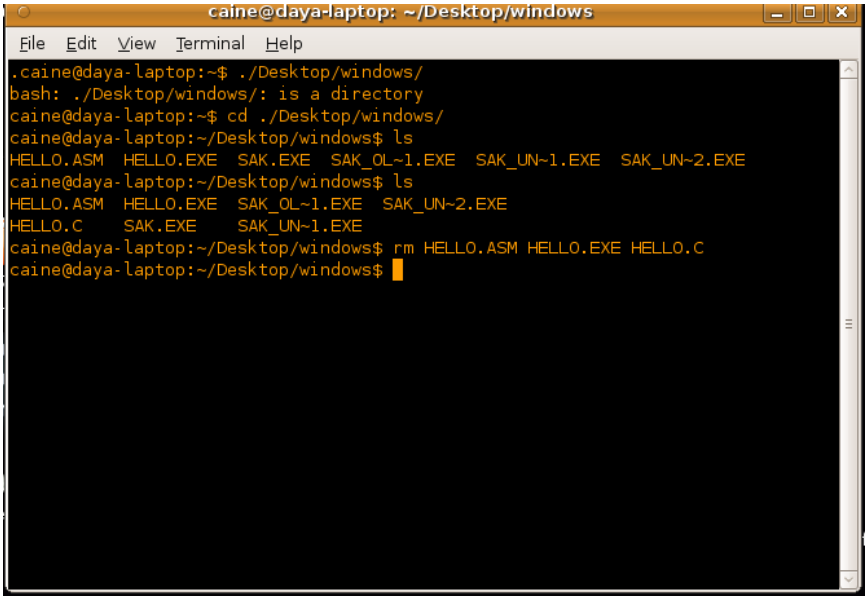


Figura 25.- Eliminación de los archivos que ya han sido analizados

Para revisar las cadenas de caracteres imprimibles que contengan los ficheros,

útil para visualizar ficheros que no sean, o que no se sepa que son de texto plano, ejecutaremos el comando STRING para cada uno de los ficheros SAK.

Strings SAK.EXE > ../textoanalisis/stringsak.txt

Strings SAK_OL~1.EXE > ../textoanalisis/stringsak_ol.txt

Strings SAK_UN~1.EXE > ../textoanalisis/stringsak_un1.txt

Strings SAK_UN~2.EXE > ../textoanalisis/stringsak_un2.txt

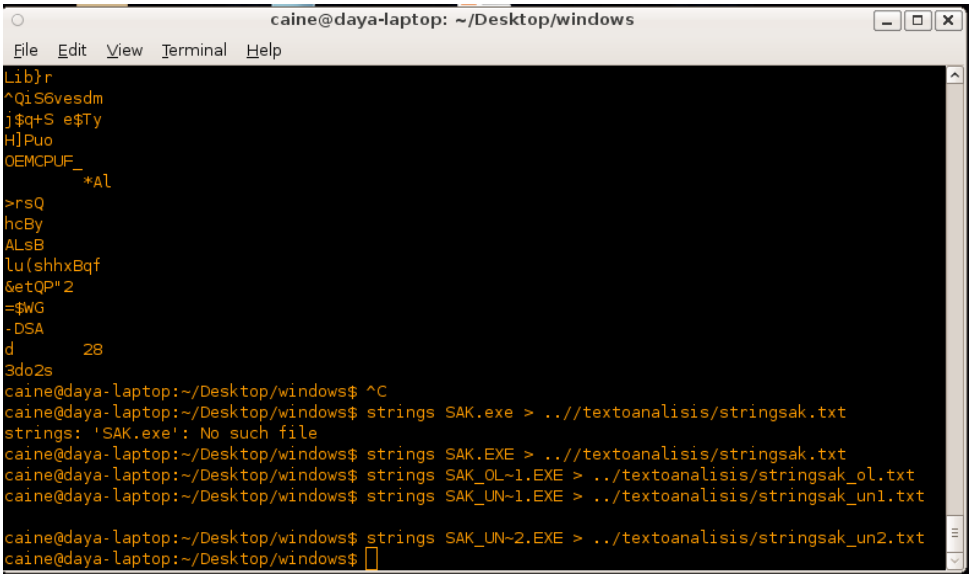


Figura 26.- Ejecución del comando string

4.7.1.1 Archivos a analizar

stringsak.txt

Observamos las siguientes salidas del comando donde solo nos certifica que es un archivo ejecutable, hace referencia a KERNEL32-dll y LOADLIBRARY GETPROCADDRESS.

stringsak_ol.txt

Aquí observamos más funciones con la excepción, es una variación de SAK.EXE con código y una leyenda de Desempaquetado con ProcDump 32.

stringsak_un1.txt

El mismo código que el archivo SAK_OL~1.EXE pero sin la leyenda de desempaquetado

stringsak_un2.txt

Observamos código adicional al desempaquetado. Ejecutamos el comando file *

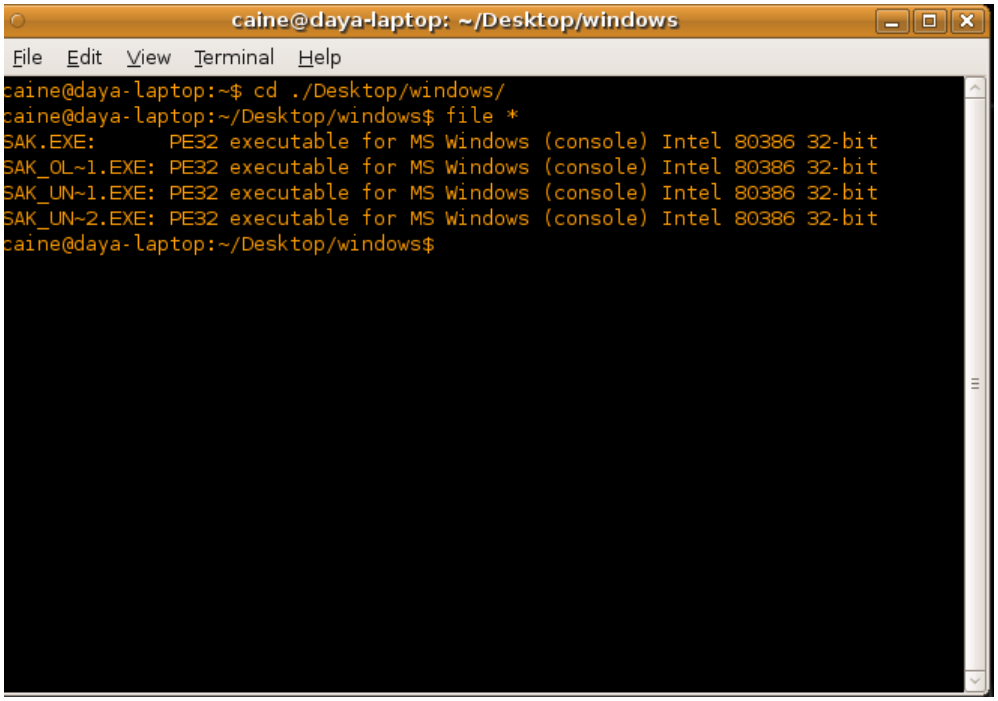


Figura 27.- Ejecución del comando file

Entendiendo que son archivos ejecutables Windows procederemos a realizar un análisis dentro de su entorno en una PC con Windows 7.

4.8 Análisis Estático

Una vez que se intenta descomprimir con el antivirus AVAST se presentan los siguientes mensajes de alerta contra los archivos.

Figura 28.- Análisis con el programa Avast

4.8.1 Análisis SAK.EXE

4.8.1.1 Análisis en dirección WEB ANUBIS de Archivos SAK

```
[########################################################################]
    Analysis Report for unknown2.exe
                    MD5: e481cee51d0b80cb36ce3c4271ca5ff3
[########################################################################]

Summary:
    - Performs Registry Activities:
        The executable reads and modifies registry values. It also creates
and
        monitors registry keys.

[========================================================================]
    Table of Contents
[========================================================================]

- General information
- unknown2.e.exe
  a) Registry Activities
  b) File Activities
```

```
[############################################################################]
    1. General Information
[############################################################################]
[============================================================================]
    Information about Anubis' invocation
[============================================================================]
        Time needed:        241 s
        Report created:     06/10/10, 20:48:30 UTC
        Termination reason: Timeout
        Program version:    1.74.2865


[############################################################################]
    2. unknown2.e.exe
[############################################################################]
[============================================================================]
    General information about this executable
[============================================================================]
        Analysis Reason: Primary Analysis Subject
        Filename:        unknown2.e.exe
        MD5:             e481cee51d0b80cb36ce3c4271ca5ff3
        SHA-1:           64d55255658b5deacfb62c9e3395c8e15b4ab08d
        File Size:       38752 Bytes
        Command Line:    "C:\unknown2.e.exe"
        Process-status
        at analysis end: alive
        Exit Code:       0

[============================================================================]
    Load-time Dlls
[============================================================================]
        Module Name: [ C:\WINDOWS\system32\ntdll.dll ],
               Base Address: [0x7C900000 ], Size: [0x000AF000 ]
        Module Name: [ C:\WINDOWS\system32\kernel32.dll ],
               Base Address: [0x7C800000 ], Size: [0x000F6000 ]

[============================================================================]
    Run-time Dlls
[============================================================================]
        Module Name: [ C:\WINDOWS\system32\WS2HELP.dll ],
               Base Address: [0x71AA0000 ], Size: [0x00008000 ]
        Module Name: [ C:\WINDOWS\system32\WS2_32.dll ],
               Base Address: [0x71AB0000 ], Size: [0x00017000 ]
        Module Name: [ C:\WINDOWS\system32\WSOCK32.dll ],
               Base Address: [0x71AD0000 ], Size: [0x00009000 ]
        Module Name: [ C:\WINDOWS\system32\msvcrt.dll ],
               Base Address: [0x77C10000 ], Size: [0x00058000 ]
        Module Name: [ C:\WINDOWS\system32\ADVAPI32.dll ],
               Base Address: [0x77DD0000 ], Size: [0x0009B000 ]
        Module Name: [ C:\WINDOWS\system32\RPCRT4.dll ],
               Base Address: [0x77E70000 ], Size: [0x00092000 ]
        Module Name: [ C:\WINDOWS\system32\Secur32.dll ],
               Base Address: [0x77FE0000 ], Size: [0x00011000 ]

[============================================================================]
    SigBuster Output
[============================================================================]
        FSG V1.0 SN: 1716
FSG V1.0-1.2 SN: 1717
```

```
[==========================================================================]
    Ikarus Virus Scanner
[==========================================================================]
        Backdoor.Win32.Agobot (Sig-Id: 19228740)

[==========================================================================]
    Program output
[==========================================================================]
        Stdout:
Enter Password:

[==========================================================================]
    2.a) unknown2.e.exe - Registry Activities
[==========================================================================]
[--=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-]
    Registry Values Read:
[--=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-]
        Key: [
HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers ],
             Value Name: [ TransparentEnabled ], Value: [ 1 ], 1 time
        Key: [ HKLM\System\CurrentControlSet\Control\Terminal Server ],
             Value Name: [ TSUserEnabled ], Value: [ 0 ], 1 time
        Key: [ HKLM\System\CurrentControlSet\Services\WinSock2\Parameters ],
             Value Name: [ WinSock_Registry_Version ], Value: [ 2.0 ], 2
times
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5 ],
             Value Name: [ Num_Catalog_Entries ], Value: [ 3 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5 ],
             Value Name: [ Serial_Access_Num ], Value: [ 4 ], 2 times
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000001 ],
             Value Name: [ DisplayString ], Value: [ Tcpip ], 4 times
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000001 ],
             Value Name: [ Enabled ], Value: [ 1 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000001 ],
             Value Name: [ LibraryPath ], Value: [
%SystemRoot%\System32\mswsock.dll ], 2 times
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000001 ],
             Value Name: [ ProviderId ], Value: [
0x409d05229e7ecf11ae5a00aa00a7112b ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000001 ],
             Value Name: [ StoresServiceClassInfo ], Value: [ 0 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000001 ],
             Value Name: [ SupportedNameSpace ], Value: [ 12 ], 1 time
```

```
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000001 ],
             Value Name: [ Version ], Value: [ 0 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000002 ],
             Value Name: [ DisplayString ], Value: [ NTDS ], 4 times
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000002 ],
             Value Name: [ Enabled ], Value: [ 1 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000002 ],
             Value Name: [ LibraryPath ], Value: [
%SystemRoot%\System32\winrnr.dll ], 2 times
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000002 ],
             Value Name: [ ProviderId ], Value: [
0xee37263b80e5cf11a55500c04fd8d4ac ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000002 ],
             Value Name: [ StoresServiceClassInfo ], Value: [ 0 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000002 ],
             Value Name: [ SupportedNameSpace ], Value: [ 32 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000002 ],
             Value Name: [ Version ], Value: [ 0 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000003 ],
             Value Name: [ DisplayString ], Value: [ Network Location
Awareness (NLA) Namespace ], 4 times
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000003 ],
             Value Name: [ Enabled ], Value: [ 1 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000003 ],
             Value Name: [ LibraryPath ], Value: [
%SystemRoot%\System32\mswsock.dll ], 2 times
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000003 ],
             Value Name: [ ProviderId ], Value: [
0x3a244266a83ba64abaa52e0bd71fdd83 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000003 ],
             Value Name: [ StoresServiceClassInfo ], Value: [ 0 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000003 ],
```

```
            Value Name: [ SupportedNameSpace ], Value: [ 15 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5\Catalog_Entries\000000000003 ],
            Value Name: [ Version ], Value: [ 0 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
],
            Value Name: [ Next_Catalog_Entry_ID ], Value: [ 1012 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
],
            Value Name: [ Num_Catalog_Entries ], Value: [ 11 ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
],
            Value Name: [ Serial_Access_Num ], Value: [ 4 ], 2 times
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
\Catalog_Entries\000000000001 ],
            Value Name: [ PackedCatalogItem ], Value: [
%SystemRoot%\system32\mswsock. ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
\Catalog_Entries\000000000002 ],
            Value Name: [ PackedCatalogItem ], Value: [
%SystemRoot%\system32\mswsock. ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
\Catalog_Entries\000000000003 ],
            Value Name: [ PackedCatalogItem ], Value: [
%SystemRoot%\system32\mswsock. ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
\Catalog_Entries\000000000004 ],
            Value Name: [ PackedCatalogItem ], Value: [
%SystemRoot%\system32\rsvpsp.d ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
\Catalog_Entries\000000000005 ],
            Value Name: [ PackedCatalogItem ], Value: [
%SystemRoot%\system32\rsvpsp.d ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
\Catalog_Entries\000000000006 ],
            Value Name: [ PackedCatalogItem ], Value: [
%SystemRoot%\system32\mswsock. ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
\Catalog_Entries\000000000007 ],
            Value Name: [ PackedCatalogItem ], Value: [
%SystemRoot%\system32\mswsock. ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
\Catalog_Entries\000000000008 ],
            Value Name: [ PackedCatalogItem ], Value: [
%SystemRoot%\system32\mswsock. ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
\Catalog_Entries\000000000009 ],
```

```
            Value Name: [ PackedCatalogItem ], Value: [
%SystemRoot%\system32\mswsock. ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
\Catalog_Entries\000000000010 ],
            Value Name: [ PackedCatalogItem ], Value: [
%SystemRoot%\system32\mswsock. ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
\Catalog_Entries\000000000011 ],
            Value Name: [ PackedCatalogItem ], Value: [
%SystemRoot%\system32\mswsock. ], 1 time

[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-]
    Monitored Registry Keys:
[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-]
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog
5 ],
            Watch subtree: [ 0 ], Notify Filter: [ Key Change ], 1 time
        Key: [
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
],
            Watch subtree: [ 0 ], Notify Filter: [ Key Change ], 1 time


[==========================================================================]
    2.b) unknown2.e.exe - File Activities
[==========================================================================]
[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-]
    Memory Mapped Files:
[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-]
        File Name: [ C:\WINDOWS\system32\WS2HELP.dll ]
        File Name: [ C:\WINDOWS\system32\WS2_32.dll ]
        File Name: [ C:\WINDOWS\system32\WSOCK32.dll ]



[##########################################################################]
                       International Secure Systems Lab
                            http://www.iseclab.org

Vienna University of Technology     Eurecom France            UC Santa
Barbara
http://www.tuwien.ac.at          http://www.eurecom.fr
http://www.cs.ucsb.edu

                          Contact: anubis@iseclab.org
```

4.8.2 Análisis Virus Total SAK.EXE

Figura 29.- Análisis con Virus Total

4.8.2.1 Informe Virus Total

Antivirus	Result	Update
AhnLab-V3	Win32/IRCBot.worm.variant	20120329
AntiVir	Worm/AgoBot.PAJ.3	20120330
Antiy-AVL	-	20120330
Avast	Win32:Trojan-gen	20120330
AVG	Worm/Agobot.GLE	20120330
BitDefender	Packer.FSG.A	20120330
ByteHero	-	20120328
CAT-QuickHeal	(Suspicious) - DNAScan	20120330
ClamAV	-	20120330
Commtouch	W32/SuspPack.DH.gen!Eldorado	20120330
Comodo	Backdoor.Win32.Agobot.paj	20120330
DrWeb	Tool.Netcat.91	20120330
Emsisoft	Backdoor.Win32.Agobot!IK	20120330
eSafe	Win32.WormAgoBot.Paj	20120328
eTrust-Vet	-	20120330
F-Prot	W32/SuspPack.DH.gen!Eldorado	20120330
F-Secure	Packer.FSG.A	20120330
Fortinet	W32/Heuri.D!tr.bdr	20120330
GData	Packer.FSG.A	20120330
Ikarus	Backdoor.Win32.Agobot	20120330

Jiangmin	Backdoor/Agobot.ebh	20120329
K7AntiVirus	Riskware	20120329
Kaspersky	Backdoor.Win32.Agobot.paj	20120330
McAfee	W32/Gaobot.worm	20120330
McAfee-GW-Edition	Heuristic.LooksLike.Win32.Suspicious.F	20120330
Microsoft	-	20120330
NOD32	a variant of Win32/RemoteAdmin.NetCat.AB	20120330
Norman	W32/Packed_FSG.A	20120330
nProtect	Backdoor/W32.AgoBot.38752	20120330
Panda	W32/Gaobot.OXI.worm	20120330
PCTools	Net-Worm.Agobot.B!rem	20120326
Rising	Trojan.Win32.Generic.11EB77F0	20120330
Sophos	Mal/Packer	20120330
SUPERAntiSpyware	-	20120329
Symantec	W32.HLLW.Gaobot.gen	20120330
TheHacker	Backdoor/Agobot.paj	20120330
TrendMicro	TROJ_GEN.R99C1DI	20120330
TrendMicro-HouseCall	TROJ_GEN.R99C1DI	20120330
VBA32	-	20120330
VIPRE	Trojan.Win32.Generic!BT	20120330
ViRobot	-	20120330
VirusBuster	Packed/FSG	20120330

Tabla I.- Análisis con Virus Total

	SAK.EXE	**SAK_OL~1.EXE**	**SAK_UN~2.EXE**	**SAK_UN~1.EXE**
a-squared		Backdoor.Win32.Agobot!IK	Backdoor.Win32.Agobot!IK	Backdoor.Win32.Agobot!IK
AhnLab-V3	Win32/IRCBot.worm.variant	Win32/IRCBot.worm.variant	Win32/IRCBot.worm.variant	Win32/IRCBot.worm.variant
AntiVir	Worm/AgoBot.PAJ.3	TR/Crypt.PEPM.Gen	TR/Crypt.PEPM.Gen	TR/Crypt.PEPM.Gen
Antiy-AVL	-	Backdoor/Win32.Agobot	-	-
Avast	Win32:Trojan-gen	-	Win32:Trojan-gen	-
Authentium		W32/BackdoorX.AYWP	W32/BackdoorX.BACW	-
AVG	Worm/Agobot.GLE	Worm/Agobot.GLE	Worm/Agobot.GLE	Worm/Agobot.GLE
BitDefender	Packer.FSG.A	Backdoor.Bot.70938	Trojan.Generic.47154	Trojan.Generic.47154

ByteHero	-			
CAT-QuickHeal	(Suspicious) – DNAScan	Backdoor.Agobot.paj	Backdoor.Agobot.paj	Backdoor.Agobot.paj
ClamAV	-	-	Trojan.Agent-126464	
Commtouch	W32/SuspPack.DH.gen!Eldorado			
Comodo	Backdoor.Win32.Agobot.paj	-	-	
DrWeb	Tool.Netcat.91	Tool.Netcat.91	Win32.HLLW.Agobot.69	
Emsisoft	Backdoor.Win32.Agobot!IK			
ESafe	Win32.WormAgoBot.Paj		Win32.Agobot.paj	
eTrust-Vet	-	Win32.Agobot.paj	-	
F-Prot	W32/SuspPack.DH.gen!Eldorado	-	W32/BackdoorX.BACW	
F-Secure	Packer.FSG.A	W32/BackdoorX.AYWP	Trojan.Generic.47154	Trojan.Generic.47154
Fortinet	W32/Heuri.D!tr.bdr	Backdoor.Bot.70938	PossibleThreat	
GData	Packer.FSG.A	W32/AgoBot.PAJ!tr.bdr	Trojan.Generic.47154	Trojan.Generic.47154
Ikarus	Backdoor.Win32.Agobot	Backdoor.Bot.70938	Backdoor.Win32.Agobot	Backdoor.Win32.Agobot
Jiangmin	Backdoor/Agobot.ebh	Backdoor.Win32.Agobot	Backdoor/Agobot.dex	Backdoor/Agobot.dex
K7AntiVirus	Riskware	Backdoor/Agobot.dex	Backdoor.Win32.Agobot	Backdoor.Win32.Agobot.paj
Kaspersky	Backdoor.Win32.Agobot.paj	Backdoor.Win32.Agobot.paj	Backdoor.Win32.Agobot.paj	Backdoor.Win32.Agobot.paj
McAfee	W32/Gaobot.worm	Backdoor.Win32.Agobot.paj	W32/Gaobot.worm	-
McAfee+Artemis		W32/Gaobot.worm	W32/Gaobot.worm	Artemis!0EAA6AECEB99
McAfee-GW-Edition	Heuristic.LooksLike.Win32.Suspicious.F	W32/Gaobot.worm	Heuristic.LooksLike.Win32.Suspicious.L!93	Heuristic.LooksLike.Win32.Suspicious.L!93
Microsoft	-	Heuristic.LooksLike.Win32.Suspicious.L!93	Backdoor:Win32/Ursap!rts	-
NOD32	a variant of Win32/RemoteAdmin.NetCat.AB	Backdoor:Win32/Ursap!rts	probably a variant of Win32/Agobot	-
Norman	W32/Packed_FSG.A	-	W32/Gaobot.PVY	W32/Gaobot.PVX
nProtect	Backdoor/W32.AgoBot.38752	W32/Gaobot.PVX	-	-
Panda	W32/Gaobot.OXI.worm	Backdoor/W32.AgoBot.94208.B	W32/Gaobot.OXI.worm	W32/Gaobot.OXI.worm

PCTools	Net-Worm.Agobot.B!rem	W32/Gaobot.OXI.worm	Net-Worm.Agobot	-
Prevx		Net-Worm.Agobot	-	-
Rising	Trojan.Win32.Generic.11EB77F0	Medium Risk Malware	-	-
Sophos	Mal/Packer	-	Mal/Generic-A	-
SUPER AntiSpyware		Mal/Generic-A	Trojan.Win32.Generic!BT	Backdoor.Agobot
Symantec	W32.HLLW.Gaobot.gen	Backdoor.Agobot	W32.HLLW.Gaobot.gen	-
TheHacker	Backdoor/Agobot.paj	W32.HLLW.Gaobot.gen	Backdoor/Agobot.paj	-
TrendMicro	TROJ_GEN.R99C1DI	Backdoor/Agobot.paj	Cryp_Xed-3	Cryp_Xed-3
TrendMicro-HouseCall	TROJ_GEN.R99C1DI	Mal_Xed-3		
VBA32	-	Backdoor.Win32.Agobot.paj	Backdoor.Win32.Agobot.paj	Backdoor.Win32.Agobot.paj
VIPRE	Trojan.Win32.Generic!BT			
ViRobot	-		Backdoor.Win32.Agobot.87040	Backdoor.Win32.Agobot.87040
VirusBuster	Packed/FSG	Backdoor.Win32.Agobot.87040	Worm.Agobot.WQAC	Worm.Agobot.WQBS

Tabla II.- Análisis de todos los archivos con Virus Total

Después de analizar archivo sak.exe en los enlaces web se obtiene que SAK.EXE:

- Es ejecutable lee y modifica los valores del registro. También crea y controla las claves de registro.
- Carga las Librerías: ntdll.dll y kernel32.dll
- ntdll.dll es un módulo que contiene funciones de sistema del NT.
- Es un proceso del sistema necesario para que su sistema de funcione correctamente. No debe eliminarse.

kernel32.dll es el Microsoft Windows Kernel más importante. Las funciones que tratan la mayor parte de funciones de las ventanas se conectan a este DLL del núcleo de cierta manera.

En su mayoría los programas antivirus lo reconocen como:

- Un ejecutable empaquetado con FSG.
- Una modificación de NETCAT.
- Un backdoor clásico para controlar el ordenador infectado.

Descargarnos y ejecutamos el programa Stud_PE, con estos datos creamos una tabla comparativa de los ficheros analizados.

Una tabla Comparativa creada con resultados del Sotware Stud_PE

PE Structure	SAK.EXE	SAK_OL~1.EXE	SAK_UN~2.EXE	SAK_UN~1.EXE
COFF File Header				
Signature	4550(PE)	4550(PE)	4550(PE)	4550(PE)
Machine	014C	014C	014C	014C
NumberOfSections	3	4	4	4
TimeDateStamp	0	0	0	0
PointerToSymbolTable	0	0	0	0
NumberOfSymbols	0	0	0	0
SizeOfOptionalHeader	0	0	0	0
Characteristics	010F	010F	010F	010F
Optional Header [PE32]				
Magic	010B	010B	010B	010B
MajorLinkerVersion	0	0	0	0
MinorLinkerVersion	0	0	0	0
SizeOfCode	10000	10000	10000	10000
SizeOfInitializedData	8000	8000	8000	8000
SizeOfUninitializedData	0	0	0	0
AddressOfEntryPoint	22000	00005AFD	00005AFD	00005AFD
BaseOfCode	1000	1000	1000	1000

BaseOfData	11000	11000	11000	11000
ImageBase	400000	400000	400000	400000
SectionAlignment	1000	1000	1000	1000
FileAlignment	1000	1000	1000	1000
MajorOSVersion	4	4	4	4
MinorOSVersion	0	0	0	0
MajorImageVersion	0	0	0	0
MinorImageVersion	0	0	0	0
MajorSubsystemVersion	4	4	4	4
MinorSubsystemVersion	0	0	0	0
Reserved	0	0	0	0
SizeOfImage	23000	19000	19000	19000
SizeOfHeaders	1000	1000	1000	1000
CheckSum	0	0	0	0
Subsystem	3	3	3	3
DLL Characteristics	0	0	0	0
SizeOfStackReserve	100000	100000	100000	100000
SizeOfStackCommit	1000	1000	1000	1000
SizeOfHeapReserve	100000	100000	100000	100000
SizeOfHeapCommit	1000	1000	1000	1000
LoaderFlags	0	0	0	0
NumberOfRvaAndSizes	10	10	10	10
Data_Directories				
Export Table	0	0	0	0
Import Table	0000006B000220F4	0000003C000184F8	0000003C000184F8	0000003C000184F8
Resource Table	0	0	0	0
Exception Table	0	0	0	0
Certificate Table	0	0	0	0
Base Relocation Table	0	0	0	0
Debug	0	0	0	0
Architecture	0	0	0	0
Global Ptr	0	0	0	0
TLS Table	0	0	0	0
Load Config Table	4800013218	4800013218	4800013218	4800013218
Bound Import	0	0	0	0
IAT	0	0	0	000002040001827C
Delay Import Descriptor	0	0	0	0

COM+ Runtime Header	0	0	0	0
Reserved	0	0	0	0

Tabla III.- Tabla comparativa con el Software Stud_PE

Analizaremos si es un programa empaquetado con Fast Small good.

Verificamos la firma y encontramos que SAK.EXE se encuentra empaquetado bajo FGS 1.0.

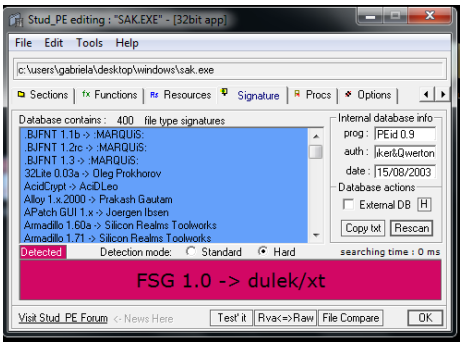


Figura 30.- Análisis con el programa FSG

Buscamos una herramienta para proceder a desempaquetar SAK.EXE, revisamos el hash presentado en Stud_PE, para asegurarnos de que el análisis no está afectando la integridad del fichero. Ejecutamos el comando descargado ms5deep –l z * para la revisión de la integridad de los archivos.

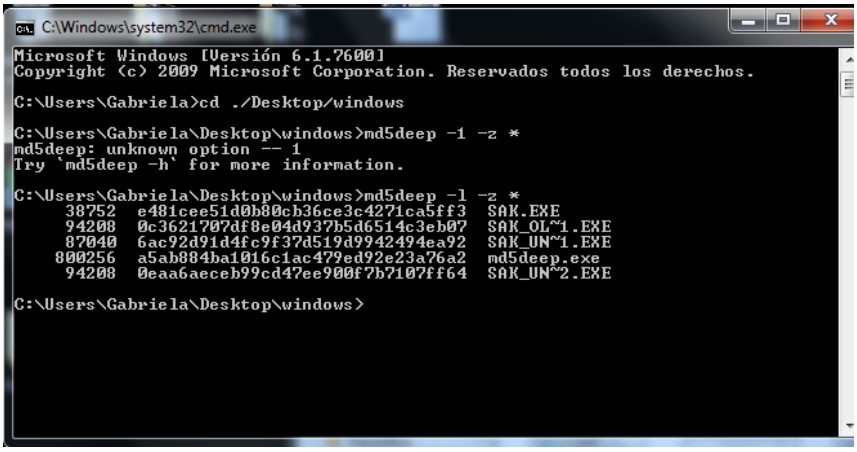


Figura 31.- Hash de los archivos a analizar

Con RDG Packer Detector podemos obtener datos más precisos del empaquetado de SAK.EXE

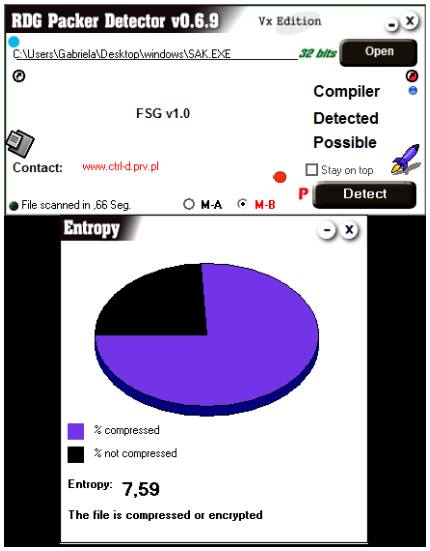


Figura 32.- Análisis con RDG Packer Detector

Se utiliza el programa UNFGS para desempaquetar el fichero SAK.EXE

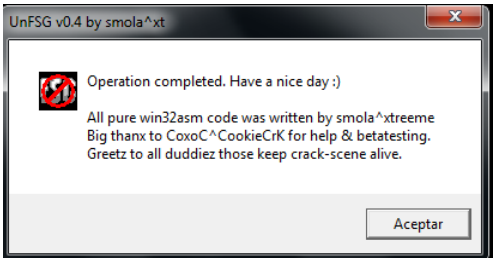


Figura 33.- Desempaquetado del archivo

Y se guarda el archivo con el nombre de UNFSGSAK.EXE

Se realiza una verificación de los archivos:

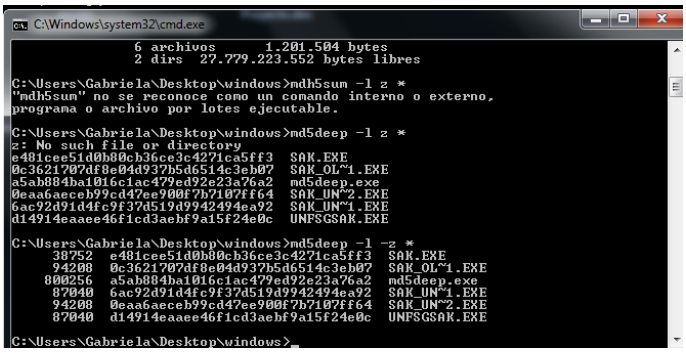


Figura 34.- Verificación de los archivos

Los archivos no han sufrido ningún cambio, pero el archivo creado UNFGS.EXE y SAK_UN~1.EXE tienen el mismo tamaño 87040.

El archivo SAK.EXE está desempaquetado de FSG, con la utilidad BinText, revisamos la estructura de los archivos SAK.EXE, UNFSGSAK.EXE y SAK_UN~1.EXE.

4.8.3 Archivo generado por BIN TEXT

SAK.EXE	SAK_UN~1.EXE			UNFSGSAK.EXE		
File pos **Mem pos**	**File pos** ========	**Mem pos** =======	**ID Text** ==	**File pos** ========	**Mem pos** =======	**ID Text** ==

ID Text	====	====
======== ======= == ====	00000000004D 00000040004D 0 !Windows Program	00000000004D 00000040004D 0 !Windows Program
00000000004D 00000040004D 0 !Windows Program	000000000158 000000400158 0 0000F97D	000000000158 000000400158 0 0000F97D
00000000022F 00000040022F 0 @.data	000000000180 000000400180 0 000026F6	000000000180 000000400180 0 000026F6
000000000258 000000400258 0 .idata	0000000001A8 0000004001A8 0 00001258	0000000001A8 0000004001A8 0 00001258
000000000F34 0000004221340 KERNEL32.dll	0000000001D0 0000004001D0 0 00000C2B	0000000001D0 0000004001D0 0 00000C2B
000000000F42 0000004221420 LoadLibraryA	00000000114E 00000040114E 0 ~xUV;	00000000114E 00000040114E 0 ~xUV;
000000000F50 0000004221500 GetProcAddress	0000000012EB 0000004012EB 0 t$$t	0000000012EB 0000004012EB 0 t$$t
000000001049 0000004190490 D ~E-	000000001637 000000401637 0 ;D$$}	000000001637 000000401637 0 ;D$$}
00000000108D 00000041908D 0 ~xUV;	0000000016CE 0000004016CE 0 t$(t!	0000000016CE 0000004016CE 0 t$(t!
0000000010DC 0000004190DC 0 "e0B1	0000000017E9 0000004017E9 0 ;l$$uM9	0000000017E9 0000004017E9 0 ;l$$uM9
00000000125A 00000041925A 0 w8d.9C	000000001B05 000000401B05 0 PVVVj	000000001B05 000000401B05 0 PVVVj
000000001315 0000004193150 RPht%	000000001B30 000000401B30 0 VVVVVj	000000001B30 000000401B30 0 VVVVVj
0000000013A7 0000004193A70 PQhW	000000001BF9 000000401BF9 0 L$ QR	000000001BF9 000000401BF9 0 L$ QR
0000000013C1 0000004193C10 YCc(;	000000001C6A 000000401C6A 0 D$$PQ	000000001C6A 000000401C6A 0 D$$PQ
00000000142C 00000041942C0 5|o}A	000000001D84 000000401D84 0 L$$QR	000000001D84 000000401D84 0 L$$QR
000000001457 000000419457	000000001E7A 000000401E7A 0 u#PPPPPj	000000001E7A 000000401E7A 0 u#PPPPPj
	000000001F9C 000000401F9C 0 D$4Vh	000000001F9C 000000401F9C 0 D$4Vh
	000000001FC5 000000401FC5 0 u9SSSSSj	000000001FC5 000000401FC5 0 u9SSSSSj
	000000002019 000000402019 0 uDSSSSSj	000000002019 000000402019 0 uDSSSSSj
	000000002086 000000402086 0 StWHtBHt*SSSSj	000000002086 000000402086 0 StWHtBHt*SSSSj
	0000000026DF 0000004026DF 0 PQhlKA	0000000026DF 0000004026DF 0 PQhlKA
	000000002B7F 000000402B7F 0 f9=,UA	000000002B7F 000000402B7F 0 f9=,UA
	000000002D94 000000402D94 0 f9=8UA	000000002D94 000000402D94 0 f9=8UA
	000000003678 000000403678 0 .BENu	000000003678 000000403678 0 .BENu
	0000000037A2 0000004037A2 0 $SUVW	0000000037A2 0000004037A2 0 $SUVW
	00000000382E 00000040382E 0	00000000382E 00000040382E 0

0 Hv_,E	tsf9=hKA	tsf9=hKA
000000001512	0000000038CC 0000004038CC 0	0000000038CC 0000004038CC 0
000000419512	D$8RP	D$8RP
0 C66_C	000000003935 000000403935 0	000000003935 000000403935 0
000000001524	T$,Rj	T$,Rj
000000419524	000000003995 000000403995 0	000000003995 000000403995 0
0 1bNzC	|$8QW	|$8QW
000000001570	000000003C0D 000000403C0D 0	000000003C0D 000000403C0D 0
000000419570	L$8PQ	L$8PQ
0 0"DD@<	000000003E76 000000403E76 0	000000003E76 000000403E76 0
0000000015C7	SVh\ A	SVh\ A
0000004195C7	000000003E97 000000403E97 0	000000003E97 000000403E97 0
0 h lX(4|	D$\PhX A	D$\PhX A
00000000161D	000000003F4A 000000403F4A 0	000000003F4A 000000403F4A 0
00000041961D	D$ Ph	D$ Ph
0 6vgv$9	000000004183 000000404183 0	000000004183 000000404183 0
0000000017B5	tuBI;	tuBI;
0000004197B5	000000004636 000000404636 0	000000004636 000000404636 0
0 \oM,+TV	f9=<UA	f9=<UA
00000000187F	00000000464B 00000040464B 0	00000000464B 00000040464B 0
00000041987F	QRhlKA	QRhlKA
0 tWHlB	000000004836 000000404836 0	000000004836 000000404836 0
000000001957	f9-<UA	f9-<UA
000000419957	0000000048AA 0000004048AA 0	0000000048AA 0000004048AA 0
0 ddP2<	f9|$(	f9|$(
0000000019E9	0000000048D7 0000004048D7 0	0000000048D7 0000004048D7 0
0000004199E9	f95<UA	f95<UA
0 C"IDOU	0000000048F5 0000004048F5 0	0000000048F5 0000004048F5 0
0000000019F2	PQh|!A	PQh|!A
0000004199F2	0000000054A2 0000004054A2 0	0000000054A2 0000004054A2 0
0 a$gHm	C =02CVu	C =02CVu
000000001A4F	0000000057B9 0000004057B9 0	0000000057B9 0000004057B9 0
000000419A4F	B 02CV	B 02CV
0 0"6D<B	000000005D9E 000000405D9E 0	000000005D9E 000000405D9E 0
000000001A58	QQSV3	QQSV3
000000419A58	000000005DBA 000000405DBA	000000005DBA 000000405DBA
0 N$THZ	0 VVVVj	0 VVVVj
000000001B70	00000000681F 00000040681F 0	00000000681F 00000040681F 0
000000419B70	95$[A	95$[A
0 VhLj9	000000006869 000000406869 0	000000006869 000000406869 0
000000001B96	95$[A	95$[A
000000419B96	00000000699F 00000040699F 0	00000000699F 00000040699F 0
0 rt?@I	Yu+Vj	Yu+Vj
000000001C45	000000007E63 000000407E63 0	000000007E63 000000407E63 0
000000419C45	SVWUj	SVWUj
0 HPj(H	000000007ECC 000000407ECC 0	000000007ECC 000000407ECC 0
000000001CD6	t.;t$$t(	t.;t$$t(
000000419CD6	000000008A42 000000408A42 0	000000008A42 000000408A42 0
0 P$yhR	oG<-uK	oG<-uK
000000001D09	000000008A50 000000408A50 0	000000008A50 000000408A50 0
000000419D09	]t@G:	]t@G:
0 NVHPT	000000008C91 000000408C91 0	000000008C91 000000408C91 0
000000001D9F	YYj0[	YYj0[

000000419D9F 0 ;,0;f9=l,e	000000009774 000000409774 0 QQSVW3	000000009774 000000409774 0 QQSVW3
000000001DBF 000000419DBF 0 %yf$G	000000009890 000000409890 0 @PVSS	000000009890 000000409890 0 @PVSS
000000001E47 000000419E47 0 !P%lj	0000000098AE 0000004098AE 0 t#SSUP	0000000098AE 0000004098AE 0 t#SSUP
000000001F71 000000419F71 0 u7L}BH	0000000098B5 0000004098B5 0 t$$VSS	0000000098B5 0000004098B5 0 t$$VSS
000000002083 00000041A083 0 R;5Po	000000009984 000000409984 0 VC20XC00U	000000009984 000000409984 0 VC20XC00U
000000002240 00000041A240 0 p%u[A	000000009AE9 000000409AE9 0 j@h 'A	000000009AE9 000000409AE9 0 j@h 'A
00000000228E 00000041A28E 0 BizJsTM&#n	000000009B10 000000409B10 0 PVPWW	000000009B10 000000409B10 0 PVPWW
000000002326 00000041A326 0 }'A|"	000000009B8E 000000409B8E 0 9} u	000000009B8E 000000409B8E 0 9} u
000000002332 00000041A332 0 zg_>aD	**File pos Mem pos ID Text**	**File pos Mem pos ID Text**
00000000233A 00000041A33A 0 Af @X	======== ======= == ====	======== ======= == ====
0000000023A0 00000041A3A0 0 .BEN7u	00000000A37A 00000040A37A 0 tSj=V	00000000A37A 00000040A37A 0 tSj=V
0000000023A9 00000041A3A9 0 xJ&dS	00000000A53E 00000040A53E 0 R95dWA	00000000A53E 00000040A53E 0 R95dWA
0000000023B1 00000041A3B1 0 Dza/|	00000000A64B 00000040A64B 0 v N+D$	00000000A64B 00000040A64B 0 v N+D$
0000000023B7 00000041A3B7 0 y$--h	00000000AE40 00000040AE40 0 wHVSU	00000000AE40 00000040AE40 0 wHVSU
00000000243E 00000041A43E 0 BO!t/N	00000000AF86 00000040AF86 0 SVWse	00000000AF86 00000040AF86 0 SVWse
0000000024B3 00000041A4B3 0 P9 >t	00000000B2A2 00000040B2A2 0 ;5$[A	00000000B2A2 00000040B2A2 0 ;5$[A
0000000024C7 00000041A4C7 0 0I (s	00000000B829 00000040B829 0 LSVWj	00000000B829 00000040B829 0 LSVWj
00000000268A 00000041A68A 0 ~D60DUtJ	00000000B916 00000040B916 0 VWumh	00000000B916 00000040B916 0 VWumh
	00000000C1F9 00000040C1F9 0 WWWWVSW	00000000C1F9 00000040C1F9 0 WWWWVSW
	00000000C21E 00000040C21E 0 t2WWVPVSW	00000000C21E 00000040C21E 0 t2WWVPVSW
	00000000C2A2 00000040C2A2 0 u8SS3	00000000C2A2 00000040C2A2 0 u8SS3
	00000000C4A0 00000040C4A0 0 t!SS9]	00000000C4A0 00000040C4A0 0 t!SS9]
	00000000C8C7 00000040C8C7 0 ;=$[A	00000000C8C7 00000040C8C7 0 ;=$[A
	00000000CC90 00000040CC90 0 ;=$[A	00000000CC90 00000040CC90 0 ;=$[A
	00000000D367 00000040D367 0 s"95(RA	00000000D367 00000040D367 0 s"95(RA
	000000010A00 000000411000 0 POSIXLY_CORRECT	000000010A00 000000411000 0 POSIXLY_CORRECT

000000002693	000000010A14 000000411014 0	000000010A14 000000411014 0
00000041A693	%s: invalid option -- %c	%s: invalid option -- %c
0 FBVQA%	000000010A34 000000411034 0	000000010A34 000000411034 0
000000002748	%s: illegal option -- %c	%s: illegal option -- %c
00000041A748	000000010A54 000000411054 0	000000010A54 000000411054 0
0 (ht.E	%s: option requires an argument -- %c	%s: option requires an argument -- %c
00000000275F	000000010A84 000000411084 0	000000010A84 000000411084 0
00000041A75F	%s: unrecognized option	%s: unrecognized option
0 @LgxhX	000000010A9D 00000041109D 0	000000010A9D 00000041109D 0
000000002889	%c%s'	%c%s'
00000041A889	000000010AAC 0000004110AC	000000010AAC 0000004110AC
0 XN)"H	0 %s: unrecognized option	0 %s: unrecognized option
0000000028F8	000000010AC5 0000004110C5 0	000000010AC5 0000004110C5 0
00000041A8F8	--%s'	--%s'
0 Mwl;B	000000010AD4 0000004110D4 0	000000010AD4 0000004110D4 0
000000002910	%s: option	%s: option
00000041A910	000000010AE0 0000004110E0 0	000000010AE0 0000004110E0 0
0 duXK"	%s' requires an argument	%s' requires an argument
000000002920	000000010B04 000000411104 0	000000010B04 000000411104 0
00000041A920	%s: option	%s: option
0 h "A	000000010B10 000000411110 0	000000010B10 000000411110 0
00000000295F	%c%s' doesn't allow an argument	%c%s' doesn't allow an argument
00000041A95F	000000010B3C 00000041113C 0	000000010B3C 00000041113C 0
0 tuB1$	%s: option	%s: option
000000002AD7	000000010B48 000000411148 0	000000010B48 000000411148 0
00000041AAD7	--%s' doesn't allow an argument	--%s' doesn't allow an argument
0 (]XIa	000000010B74 000000411174 0	000000010B74 000000411174 0
000000002B7A	%s: option	%s: option
00000041AB7A	000000010B80 000000411180 0	000000010B80 000000411180 0
0 tJ\[Bh	%s' is ambiguous	%s' is ambiguous
	000000010B9C 00000041119C 0	000000010B9C 00000041119C 0
File pos	Failed to execute shell, error = %s	Failed to execute shell, error = %s
Mem pos	000000010BC8 0000004111C8 0	000000010BC8 0000004111C8 0
ID Text	SessionReadShellThreadFn exitted,	SessionReadShellThreadFn exitted,
========	error = %s	error = %s
=======	000000010C08 000000411208 0	000000010C08 000000411208 0
== ====	Failed to execute shell	Failed to execute shell
	000000010C24 000000411224 0	000000010C24 000000411224 0
000000002C59	Failed to create shell stdin pipe, error	Failed to create shell stdin pipe, error
00000041AC59	= %s	= %s
0 ~//*	000000010C5C 00000041125C 0	000000010C5C 00000041125C 0
000000002DEA	Failed to create shell stdout pipe, error	Failed to create shell stdout pipe, error
00000041ADEA	= %s	= %s
0 2hPt#@	000000010C94 000000411294 0	000000010C94 000000411294 0
000000002E5E	WaitForMultipleObjects error: %s	WaitForMultipleObjects error: %s
00000041AE5E	000000010CBC 0000004112BC 0	000000010CBC 0000004112BC 0
0	Failed to create ReadShell session	Failed to create ReadShell session
pD[JV)EP?C"6	thread, error = %s	thread, error = %s
000000002EA9	000000010CFC 0000004112FC 0	000000010CFC 0000004112FC 0
00000041AEA9	unknown socket error	unknown socket error
0 !&C2]	000000010D18 000000411318 0	000000010D18 000000411318 0
i$uH	NO_DATA	NO_DATA
000000002F2E	000000010D2C 00000041132C 0	000000010D2C 00000041132C 0

00000041AF2E	NO_RECOVERY	NO_RECOVERY
0 Dd@2<	000000010D40 000000411340 0	000000010D40 000000411340 0
000000002FDD	TRY_AGAIN	TRY_AGAIN
00000041AFDD	000000010D54 000000411354 0	000000010D54 000000411354 0
0 Np@HVj	HOST_NOT_FOUND	HOST_NOT_FOUND
0000000030E4	000000010D68 000000411368 0	000000010D68 000000411368 0
00000041B0E4	DISCON	DISCON
0 &<7u#	000000010D7C 00000041137C 0	000000010D7C 00000041137C 0
000000003172	NOTINITIALISED	NOTINITIALISED
00000041B172	000000010D90 000000411390 0	000000010D90 000000411390 0
0 _{i$f	VERNOTSUPPORTED	VERNOTSUPPORTED
0000000031DB	000000010DA4 0000004113A4 0	000000010DA4 0000004113A4 0
00000041B1DB	SYSNOTREADY	SYSNOTREADY
0 6Gx?u;	000000010DB8 0000004113B8 0	000000010DB8 0000004113B8 0
0000000032DD	REMOTE	REMOTE
00000041B2DD	000000010DCC 0000004113CC 0	000000010DCC 0000004113CC 0
0 8bI?<J	STALE	STALE
000000003378	000000010DE0 0000004113E0 0	000000010DE0 0000004113E0 0
00000041B378	DQUOT	DQUOT
0 zpFrU	000000010DF4 0000004113F4 0	000000010DF4 0000004113F4 0
0000000035BF	USERS	USERS
00000041B5BF	000000010E08 000000411408 0	000000010E08 000000411408 0
0 Bz(@/	PROCLIM	PROCLIM
00000000379E	000000010E1C 00000041141C 0	000000010E1C 00000041141C 0
00000041B79E	NOTEMPTY	NOTEMPTY
0 "2j{!	000000010E30 000000411430 0	000000010E30 000000411430 0
0000000037D6	HOSTUNREACH	HOSTUNREACH
00000041B7D6	000000010E44 000000411444 0	000000010E44 000000411444 0
0 c'yt D	HOSTDOWN	HOSTDOWN
000000003858	000000010E58 000000411458 0	000000010E58 000000411458 0
00000041B858	NAMETOOLONG	NAMETOOLONG
0 4Y8q$!Jpg7	000000010E6C 00000041146C 0	000000010E6C 00000041146C 0
000000003898	LOOP	LOOP
00000041B898	000000010E80 000000411480 0	000000010E80 000000411480 0
0 {B2v)	connection refused	connection refused
00000000392E	000000010E98 000000411498 0	000000010E98 000000411498 0
00000041B92E	TIMEDOUT	TIMEDOUT
0 +Kp~Z	000000010EAC 0000004114AC 0	000000010EAC 0000004114AC 0
000000003A65	TOOMANYREFS	TOOMANYREFS
00000041BA65		
0 t!RD	**File pos Mem pos ID Text**	**File pos Mem pos ID Text**
000000003C30	======== ======= ==	======== ======= ==
00000041BC30	====	====
0 hP (l		
000000003D3E	000000010EC0 0000004114C0 0	000000010EC0 0000004114C0 0
00000041BD3E	SHUTDOWN	SHUTDOWN
0 }HpVPt	000000010ED4 0000004114D4 0	000000010ED4 0000004114D4 0
000000003D7D	NOTCONN	NOTCONN
00000041BD7D	000000010EE8 0000004114E8 0	000000010EE8 0000004114E8 0
0 E3D=7	ISCONN	ISCONN
000000003E77	000000010EFC 0000004114FC 0	000000010EFC 0000004114FC 0
00000041BE77	NOBUFS	NOBUFS
0 "rIf	000000010F10 000000411510 0	000000010F10 000000411510 0

000000003FF0	CONNRESET	CONNRESET
00000041BFF0	000000010F24 000000411524 0	000000010F24 000000411524 0
0 QfV05)	CONNABORTED	CONNABORTED
000000004022	000000010F38 000000411538 0	000000010F38 000000411538 0
00000041C022	NETRESET	NETRESET
0 ~-"]P	000000010F4C 00000041154C 0	000000010F4C 00000041154C 0
0000000040F3	NETUNREACH	NETUNREACH
00000041C0F3	000000010F60 000000411560 0	000000010F60 000000411560 0
0 p;9P5j}	NETDOWN	NETDOWN
0000000042C3	000000010F74 000000411574 0	000000010F74 000000411574 0
00000041C2C3	ADDRNOTAVAIL	ADDRNOTAVAIL
0 h!CD	000000010F88 000000411588 0	000000010F88 000000411588 0
000000004491	ADDRINUSE	ADDRINUSE
00000041C491	000000010F9C 00000041159C 0	000000010F9C 00000041159C 0
0 L;u	AFNOSUPPORT	AFNOSUPPORT
00000000452F	000000010FB0 0000004115B0 0	000000010FB0 0000004115B0 0
00000041C52F	PFNOSUPPORT	PFNOSUPPORT
0 +xaQiu~	000000010FC4 0000004115C4 0	000000010FC4 0000004115C4 0
00000000460D	OPNOTSUPP	OPNOTSUPP
00000041C60D	000000010FD8 0000004115D8 0	000000010FD8 0000004115D8 0
0 B0M 7E|C@	SOCKTNOSUPPORT	SOCKTNOSUPPORT
0000000047C1	000000010FEC 0000004115EC 0	000000010FEC 0000004115EC 0
00000041C7C1	PROTONOSUPPORT	PROTONOSUPPORT
0 <;'jv8	000000011000 000000411600 0	000000011000 000000411600 0
000000004812	NOPROTOOPT	NOPROTOOPT
00000041C812	000000011014 000000411614 0	000000011014 000000411614 0
0 pJw'to:	PROTOTYPE	PROTOTYPE
00000000482B	000000011028 000000411628 0	000000011028 000000411628 0
00000041C82B	MSGSIZE	MSGSIZE
0 y"KsH{	00000001103C 00000041163C 0	00000001103C 00000041163C 0
00000000494C	DESTADDRREQ	DESTADDRREQ
00000041C94C	000000011050 000000411650 0	000000011050 000000411650 0
0 ?~4lX	NOTSOCK	NOTSOCK
0000000049D2	000000011064 000000411664 0	000000011064 000000411664 0
00000041C9D2	ALREADY	ALREADY
0 |k13W	000000011078 000000411678 0	000000011078 000000411678 0
000000004C1C	INPROGRESS	INPROGRESS
00000041CC1C	00000001108C 00000041168C 0	00000001108C 00000041168C 0
0 HTjw%	WOULDBLOCK	WOULDBLOCK
000000004D0B	0000000110A0 0000004116A0 0	0000000110A0 0000004116A0 0
00000041CD0B	MFILE	MFILE
0 &IZK/	0000000110B4 0000004116B4 0	0000000110B4 0000004116B4 0
000000004F48	INVAL	INVAL
00000041CF48	0000000110C8 0000004116C8 0	0000000110C8 0000004116C8 0
0 9%s")	FAULT	FAULT
000000004FAF	0000000110DC 0000004116DC 0	0000000110DC 0000004116DC 0
00000041CFAF	ACCES	ACCES
0 dCSb-	0000000110F0 0000004116F0 0	0000000110F0 0000004116F0 0
000000004FB8	BADF	BADF
00000041CFB8	000000011104 000000411704 0	000000011104 000000411704 0
0 :5 1X	INTR	INTR
000000005231	000000011124 000000411724 0	000000011124 000000411724 0
00000041D231	punt!	punt!

0 XundN 00000000527C	000000001112C 00000041172C 0 spurious timer interrupt!	000000001112C 00000041172C 0 spurious timer interrupt!
00000041D27C 0 52\5T	000000001114C 00000041174C 0 Hmalloc %d failed	000000001114C 00000041174C 0 Hmalloc %d failed
0000000052B0 00000041D2B0	000000011164 000000411764 0 DNS fwd/rev mismatch: %s != %s	000000011164 000000411764 0 DNS fwd/rev mismatch: %s != %s
0 vH)T+ 00000000531F	000000001118C 00000041178C 0 Warning: forward host lookup failed	000000001118C 00000041178C 0 Warning: forward host lookup failed
00000041D31F 0 (dP2l'	for %s: h_errno %d 0000000111D0 0000004117D0 0	for %s: h_errno %d 0000000111D0 0000004117D0 0
00000000558A 00000041D58A	%s: inverse host lookup failed: h_errno %d	%s: inverse host lookup failed: h_errno %d
0 u|l8l 0000000055B1	000000011204 000000411804 0 Warning: inverse host lookup failed	000000011204 000000411804 0 Warning: inverse host lookup failed
00000041D5B1 0 1e t NE	for %s: h_errno %d 000000011248 000000411848 0	for %s: h_errno %d 000000011248 000000411848 0
00000000569E 00000041D69E	%s: forward host lookup failed: h_errno %d	%s: forward host lookup failed: h_errno %d
0 P>9]! 0000000056E4	000000001127C 00000041187C 0 gethostpoop fuxored	000000001127C 00000041187C 0 gethostpoop fuxored
00000041D6E4 0 c{(uw	000000011294 000000411894 0 Can't parse %s as an IP address	000000011294 000000411894 0 Can't parse %s as an IP address
0000000058C6 00000041D8C6	0000000112C0 0000004118C0 0 Warning: port-bynum mismatch, %d	0000000112C0 0000004118C0 0 Warning: port-bynum mismatch, %d
0 "INrB 0000000058D5	!= %d 0000000112F0 0000004118F0 0	!= %d 0000000112F0 0000004118F0 0
00000041D8D5 0 p%t{4\!	loadports: bogus values %d, %d 000000011318 000000411918 0	loadports: bogus values %d, %d 000000011318 000000411918 0
0000000059DE 00000041D9DE	loadports: no block?! 000000011334 000000411934 0	loadports: no block?! 000000011334 000000411934 0
0 u>fe\ 000000005A29	Warning: source routing unavailable on this machine, ignoring	Warning: source routing unavailable on this machine, ignoring
00000041DA29 0 .t' pi#	000000011380 000000411980 0 Can't grab %s:%d with bind	000000011380 000000411980 0 Can't grab %s:%d with bind
000000005A33 00000041DA33	0000000113A0 0000004119A0 0 retrying local %s:%d	0000000113A0 0000004119A0 0 retrying local %s:%d
0 K7,:T 000000005C7F	0000000113BC 0000004119BC 0 nnetfd reuseaddr failed	0000000113BC 0000004119BC 0 nnetfd reuseaddr failed
00000041DC7F 0 ?B bC	0000000113D8 0000004119D8 0 Can't get socket	0000000113D8 0000004119D8 0 Can't get socket
000000005D2F 00000041DD2F	0000000113EC 0000004119EC 0 connect to [%s] from %s [%s] %d	0000000113EC 0000004119EC 0 connect to [%s] from %s [%s] %d
0 K>=0> 000000005DDF	000000011414 000000411A14 0 invalid connection to [%s] from %s	000000011414 000000411A14 0 invalid connection to [%s] from %s
00000041DDDF 0 G[q$5	[%s] %d 000000011448 000000411A48 0	[%s] %d 000000011448 000000411A48 0
000000005E90 00000041DE90	post-rcv getsockname failed 00000001146C 000000411A6C 0	post-rcv getsockname failed 00000001146C 000000411A6C 0
0 \I8rJ 000000005E9C	] %d ... 00000001147C 000000411A7C 0	] %d ... 00000001147C 000000411A7C 0
00000041DE9C 0 K-\n:	listening on [000000011490 000000411A90 0	listening on [000000011490 000000411A90 0
000000005EDA	local getsockname failed	local getsockname failed

00000041DEDA 0 lVQ%0 000000006005 00000041E005 0 VC20X 00000000605C 00000041E05C 0 5?xH< **File pos** **Mem pos** **ID Text** ======== ======= == ==== 0000000060BB 00000041E0BB 0 KX=zg 0000000062A6 00000041E2A6 0 <tf.S N 0000000062DE 00000041E2DE 0] !W> 0000000062F5 00000041E2F5 0 p~tRI 0000000063C0 00000041E3C0 0 Q506VJ 000000006415 00000041E415 0 _8[jJ 0000000064DB 00000041E4DB 0 :>$;#i 000000006568 00000041E568 0 "K0@(v 00000000660F 00000041E60F 0 "WZP! 0000000066A0 00000041E6A0 0 tSj|=, 000000006749 00000041E749 0 DE{V 000000006763 00000041E763 0 H*dQt	0000000114B0 000000411AB0 0 local listen fuxored 0000000114CC 000000411ACC 0 UDP listen needs -p arg 0000000114E8 000000411AE8 0 udptest first write failed?! errno %d 000000011518 000000411B18 0 ofd write err 000000011528 000000411B28 0 %8.8x 000000011530 000000411B30 0 oprint called with no open fd?! **File pos Mem pos ID Text** ======== ======= == ==== 000000011558 000000411B58 0 too many output retries 000000011574 000000411B74 0 net timeout 000000011584 000000411B84 0 select fuxored 000000011598 000000411B98 0 Preposterous Pointers: %d, %d 0000000115BC 000000411BBC 0 port numbers can be individual or ranges: m-n [inclusive] 000000011608 000000411C08 0 -u UDP mode 000000011616 000000411C16 0 -v verbose [use twice to be more verbose] 000000011642 000000411C42 0 -w secs timeout for connects and final net reads 000000011675 000000411C75 0 -z zero-I/O mode [used for scanning] 0000000116BC 000000411CBC 0 -t answer TELNET negotiation 0000000116E8 000000411CE8 0 -g gateway source- routing hop point[s], up to 8 000000011719 000000411D19 0 -G num source- routing pointer: 4, 8, 12, ... 000000011748 000000411D48 0 -h this cruft 000000011758 000000411D58 0 -i secs delay interval for lines sent, ports scanned	0000000114B0 000000411AB0 0 local listen fuxored 0000000114CC 000000411ACC 0 UDP listen needs -p arg 0000000114E8 000000411AE8 0 udptest first write failed?! errno %d 000000011518 000000411B18 0 ofd write err 000000011528 000000411B28 0 %8.8x 000000011530 000000411B30 0 oprint called with no open fd?! **File pos Mem pos ID Text** ======== ======= == ==== 000000011558 000000411B58 0 too many output retries 000000011574 000000411B74 0 net timeout 000000011584 000000411B84 0 select fuxored 000000011598 000000411B98 0 Preposterous Pointers: %d, %d 0000000115BC 000000411BBC 0 port numbers can be individual or ranges: m-n [inclusive] 000000011608 000000411C08 0 -u UDP mode 000000011616 000000411C16 0 -v verbose [use twice to be more verbose] 000000011642 000000411C42 0 -w secs timeout for connects and final net reads 000000011675 000000411C75 0 -z zero-I/O mode [used for scanning] 0000000116BC 000000411CBC 0 -t answer TELNET negotiation 0000000116E8 000000411CE8 0 -g gateway source- routing hop point[s], up to 8 000000011719 000000411D19 0 -G num source- routing pointer: 4, 8, 12, ... 000000011748 000000411D48 0 -h this cruft 000000011758 000000411D58 0 -i secs delay interval for lines sent, ports scanned

000000006769 00000041E769 0 &4d{,U	00000001178F 000000411D8F 0 -l listen mode, for inbound connects	00000001178F 000000411D8F 0 -l listen mode, for inbound connects
000000006791 00000041E791 0 8P1R*A	0000000117B6 000000411DB6 0 -L listen harder, re-listen on socket close	0000000117B6 000000411DB6 0 -L listen harder, re-listen on socket close
0000000067E6 00000041E7E6 0 AR959	0000000117E4 000000411DE4 0 -n numeric-only IP addresses, no DNS	0000000117E4 000000411DE4 0 -n numeric-only IP addresses, no DNS
000000006889 00000041E889 0 v N+23	00000001180B 000000411E0B 0 -o file hex dump of traffic	00000001180B 000000411E0B 0 -o file hex dump of traffic
0000000068CA 00000041E8CA 0 wN=4u	000000011829 000000411E29 0 -p port local port number	000000011829 000000411E29 0 -p port local port number
0000000069A2 00000041E9A2 0 I,R.&	000000011845 000000411E45 0 -r randomize local and remote ports	000000011845 000000411E45 0 -r randomize local and remote ports
0000000069B0 00000041E9B0 0 $h6$)?7=	00000001186B 000000411E6B 0 -s addr local source address	00000001186B 000000411E6B 0 -s addr local source address
000000006AA8 00000041EAA8 0 d PHd	0000000118E0 000000411EE0 0 -e prog inbound program to exec [dangerous!!]	0000000118E0 000000411EE0 0 -e prog inbound program to exec [dangerous!!]
000000006AC2 00000041EAC2 0 x|3y;.	00000001191C 000000411F1C 0 -d detach from console, background mode	00000001191C 000000411F1C 0 -d detach from console, background mode
000000006D66 00000041ED66 0 @qSJA#p	000000011950 000000411F50 0 [v1.10 NT]	000000011950 000000411F50 0 [v1.10 NT]
000000006DC9 00000041EDC9 0 H0/[Z	00000001195B 000000411F5B 0 connect to somewhere: nc [-options] hostname port[s] [ports] ...	00000001195B 000000411F5B 0 connect to somewhere: nc [-options] hostname port[s] [ports] ...
000000006E89 00000041EE89 0 hPy=9O@3	00000001199D 000000411F9D 0 listen for inbound: nc -l -p port [options] [hostname] [port]	00000001199D 000000411F9D 0 listen for inbound: nc -l -p port [options] [hostname] [port]
	0000000119DB 000000411FDB 0 options:	0000000119DB 000000411FDB 0 options:
000000006ED5 00000041EED5 0 '\R<'	000000011A04 000000412004 0 You entered an Incorrect Password. Exiting...	000000011A04 000000412004 0 You entered an Incorrect Password. Exiting...
000000007231 00000041F231 0 w~*9E>	000000011A40 000000412040 0 Password accepted!	000000011A40 000000412040 0 Password accepted!
0000000072EF 00000041F2EF 0 s-y<<<	000000011A5C 00000041205C 0 Enter Password:	000000011A5C 00000041205C 0 Enter Password:
000000007312 00000041F312 0 Q+@P&	000000011A70 000000412070 0 no port[s] to connect to	000000011A70 000000412070 0 no port[s] to connect to
000000007339 00000041F339 0 58!ha	000000011A90 000000412090 0 no destination	000000011A90 000000412090 0 no destination
00000000745A	000000011AA4 0000004120A4 0 no connection	000000011AA4 0000004120A4 0 no connection
	000000011AB4 0000004120B4 0 invalid port %s	000000011AB4 0000004120B4 0 invalid port %s
	000000011AC8 0000004120C8 0	000000011AC8 0000004120C8 0

00000041F45A	can't open %s	can't open %s
0 (" D	000000011AD8 0000004120D8 0	000000011AD8 0000004120D8 0
00000000753E	nc -h for help	nc -h for help
00000041F53E	000000011AEC 0000004120EC 0	000000011AEC 0000004120EC 0
0 TE@F;	invalid wait-time %s	invalid wait-time %s
000000007568	000000011B08 000000412108 0	000000011B08 000000412108 0
00000041F568	too many -g hops	too many -g hops
0 9VZ(E?	000000011B1C 00000041211C 0	000000011B1C 00000041211C 0
000000007579	invalid hop pointer %d, must be	invalid hop pointer %d, must be
00000041F579	multiple of 4 <= 28	multiple of 4 <= 28
0 ".,8x2	000000011B5C 00000041215C 0	000000011B5C 00000041215C 0
000000007774	all-A-records NIY	all-A-records NIY
00000041F774	000000011B74 000000412174 0	000000011B74 000000412174 0
0 KP'sz(K	wrong	wrong
00000000796B	000000011B7C 00000041217C 0	000000011B7C 00000041217C 0
00000041F96B	sent %d, rcvd %d	sent %d, rcvd %d
0 4"PQA	000000011B90 000000412190 0	000000011B90 000000412190 0
0000000079F8	%s [%s] %d (%s)	%s [%s] %d (%s)
00000041F9F8	000000011BA4 0000004121A4 0	000000011BA4 0000004121A4 0
0 Unt>K	%s [%s] %d (%s) open	%s [%s] %d (%s) open
000000007B3C	000000011BC0 0000004121C0 0	000000011BC0 0000004121C0 0
00000041FB3C	invalid local port %s	invalid local port %s
0 -;=h%	000000011BDC 0000004121DC	000000011BDC 0000004121DC
000000007B52	0 invalid interval time %s	0 invalid interval time %s
00000041FB52	000000011BFC 0000004121FC 0	000000011BFC 0000004121FC 0
0 HD0Ii	ade:g:G:hi:lLno:p:rs:tuvw:z	ade:g:G:hi:lLno:p:rs:tuvw:z
000000007BD4	000000011C20 000000412220 0	000000011C20 000000412220 0
00000041FBD4	Cmd line:	Cmd line:
0 <d@2D	000000011C30 000000412230 0	000000011C30 000000412230 0
000000007C9F	CorExitProcess	CorExitProcess
00000041FC9F	000000011C40 000000412240 0	000000011C40 000000412240 0
0 k@Aq;1	mscoree.dll	mscoree.dll
000000007D3E	000000011C81 000000412281 0	000000011C81 000000412281 0
00000041FD3E	(8PX	(8PX
0 4=dW)	000000011C89 000000412289 0	000000011C89 000000412289 0
000000007E57	700WP	700WP
00000041FE57	000000011CA1 0000004122A1 0	000000011CA1 0000004122A1 0
0 6/)#7	ppxxxx	ppxxxx
000000008334	000000011CCC 0000004122CC 0	000000011CCC 0000004122CC 0
000000420334	(null)	(null)
0 t"wQB)Gu	000000011D14 000000412314 0	000000011D14 000000412314 0
0000000083C9	runtime error	runtime error
0000004203C9	000000011D28 000000412328 0	000000011D28 000000412328 0
0 a@}>m52	TLOSS error	TLOSS error
00000000845F	000000011D38 000000412338 0	000000011D38 000000412338 0
00000042045F	SING error	SING error
0 OSIXLY_C	000000011D48 000000412348 0	000000011D48 000000412348 0
000000008474	DOMAIN error	DOMAIN error
000000420474	000000011D58 000000412358 0	000000011D58 000000412358 0
0 inval	R6029	R6029
00000000848B	000000011D5F 00000041235F 0	000000011D5F 00000041235F 0
00000042048B	- This application cannot run using the	- This application cannot run using the
0 dN l&egD	active version of the Microsoft .NET	active version of the Microsoft .NET

000000008506 000000420506 0 u>{=shf 00000000851F 00000042051F 0 wR=ad 00000000852B 00000042052B 0 Fnw7itt 00000000855B 00000042055B 0 ptF,M;ul 000000008593 000000420593 0 NO_DAT 0000000085AB 0000004205AB 0 _AGEIN,(H 0000000085B5 0000004205B5 0 T6T_Z 0000000085BB 0000004205BB 0 yFwURD 0000000085C2 0000004205C2 0 w7ISt 0000000085D0 0000004205D0 0 AeL:E6(0000000085FA 0000004205FA 0 DQhUP 000000008629 000000420629 0 AMETO 000000008654 000000420654 0 MANbY **File pos** **Mem pos** **ID Text** ======== ======= == ==== 00000000865E 00000042065E 0)HU|R 00000000867F 00000042067F 0 h<SBD'	Runtime **File pos Mem pos ID Text** ======== ======= == ==== 000000011DB4 0000004123B4 0 Please contact the application's support team for more information. 000000011DFC 0000004123FC 0 R6028 000000011E03 000000412403 0 - unable to initialize heap 000000011E24 000000412424 0 R6027 000000011E2B 00000041242B 0 - not enough space for lowio initialization 000000011E5C 00000041245C 0 R6026 000000011E63 000000412463 0 - not enough space for stdio initialization 000000011E94 000000412494 0 R6025 000000011E9B 00000041249B 0 - pure virtual function call 000000011EBC 0000004124BC 0 R6024 000000011EC3 0000004124C3 0 - not enough space for _onexit/atexit table 000000011EF4 0000004124F4 0 R6019 000000011EFB 0000004124FB 0 - unable to open console device 000000011F20 000000412520 0 R6018 000000011F27 000000412527 0 - unexpected heap error 000000011F44 000000412544 0 R6017 000000011F4B 00000041254B 0 - unexpected multithread lock error 000000011F74 000000412574 0 R6016 000000011F7B 00000041257B 0 - not enough space for thread data 000000011FA2 0000004125A2 0 This application has requested the Runtime to terminate it in an unusual way. 000000011FF0 0000004125F0 0	Runtime **File pos Mem pos ID Text** ======== ======= == ==== 000000011DB4 0000004123B4 0 Please contact the application's support team for more information. 000000011DFC 0000004123FC 0 R6028 000000011E03 000000412403 0 - unable to initialize heap 000000011E24 000000412424 0 R6027 000000011E2B 00000041242B 0 - not enough space for lowio initialization 000000011E5C 00000041245C 0 R6026 000000011E63 000000412463 0 - not enough space for stdio initialization 000000011E94 000000412494 0 R6025 000000011E9B 00000041249B 0 - pure virtual function call 000000011EBC 0000004124BC 0 R6024 000000011EC3 0000004124C3 0 - not enough space for _onexit/atexit table 000000011EF4 0000004124F4 0 R6019 000000011EFB 0000004124FB 0 - unable to open console device 000000011F20 000000412520 0 R6018 000000011F27 000000412527 0 - unexpected heap error 000000011F44 000000412544 0 R6017 000000011F4B 00000041254B 0 - unexpected multithread lock error 000000011F74 000000412574 0 R6016 000000011F7B 00000041257B 0 - not enough space for thread data 000000011FA2 0000004125A2 0 This application has requested the Runtime to terminate it in an unusual way. 000000011FF0 0000004125F0 0

0000000086D2	Please contact the application's	Please contact the application's
0000004206D2	support team for more information.	support team for more information.
0 IZEy\	000000012038 000000412638 0	000000012038 000000412638 0
0000000086FD	R6009	R6009
0000004206FD	00000001203F 00000041263F 0	00000001203F 00000041263F 0
0 ~,xFLI	- not enough space for environment	- not enough space for environment
000000008743	000000012064 000000412664 0	000000012064 000000412664 0
000000420743	R6008	R6008
0 ~pF!L	00000001206B 00000041266B 0	00000001206B 00000041266B 0
000000008809	- not enough space for arguments	- not enough space for arguments
000000420809	000000012090 000000412690 0	000000012090 000000412690 0
0 k$?!0TLs	R6002	R6002
000000008822	000000012097 000000412697 0	000000012097 000000412697 0
000000420822	- floating point not loaded	- floating point not loaded
0 i\(D|	0000000120B8 0000004126B8 0	0000000120B8 0000004126B8 0
000000008853	Microsoft Visual C++ Runtime	Microsoft Visual C++ Runtime
000000420853	Library	Library
0 B$F<\:	0000000120E4 0000004126E4 0	0000000120E4 0000004126E4 0
00000000885A	Runtime Error!	Runtime Error!
00000042085A	0000000120F4 0000004126F4 0	0000000120F4 0000004126F4 0
0 tfd\F7R	Program:	Program:
000000008881	000000012104 000000412704 0	000000012104 000000412704 0
000000420881	<program name unknown>	<program name unknown>
0 r?38$p	00000001265C 000000412C5C 0	00000001265C 000000412C5C 0
0000000088B0	GetProcessWindowStation	GetProcessWindowStation
0000004208B0	000000012674 000000412C74 0	000000012674 000000412C74 0
0 kEB B:I5	GetUserObjectInformationA	GetUserObjectInformationA
0000000088E9	000000012690 000000412C90 0	000000012690 000000412C90 0
0000004208E9	GetLastActivePopup	GetLastActivePopup
0 !%8.Ox	0000000126A4 000000412CA4 0	0000000126A4 000000412CA4 0
000000008953	GetActiveWindow	GetActiveWindow
000000420953	0000000126B4 000000412CB4 0	0000000126B4 000000412CB4 0
0 om-Xa6cl	MessageBoxA	MessageBoxA
00000000898C	0000000126C0 000000412CC0 0	0000000126C0 000000412CC0 0
00000042098C	user32.dll	user32.dll
0]Ywho=c	000000012704 000000412D04 0	000000012704 000000412D04 0
0000000089A7	Program:	Program:
0000004209A7	000000012710 000000412D10 0	000000012710 000000412D10 0
0 s7gz\:	A buffer overrun has been detected	A buffer overrun has been detected
0000000089CA	which has corrupted the program's	which has corrupted the program's
0000004209CA	000000012755 000000412D55 0	000000012755 000000412D55 0
0 TENL	internal state. The program cannot	internal state. The program cannot
0000000089ED	safely continue execution and must	safely continue execution and must
0000004209ED	00000001279C 000000412D9C 0	00000001279C 000000412D9C 0
0 R"b[b	now be terminated.	now be terminated.
000000008A05	0000000127B0 000000412DB0 0	0000000127B0 000000412DB0 0
000000420A05	Buffer overrun detected!	Buffer overrun detected!
0 (Tf4X8	0000000127D0 000000412DD0 0	0000000127D0 000000412DD0 0
000000008A2F	A security error of unknown cause has	A security error of unknown cause has
000000420A2F	been detected which has	been detected which has
0 ls?(,	00000001280E 000000412E0E 0	00000001280E 000000412E0E 0
000000008A4D	corrupted the program's internal state.	corrupted the program's internal state.
000000420A4D	The program cannot safely	The program cannot safely

0 RA+L'	000000012851 000000412E51 0	000000012851 000000412E51 0
000000008A6F	continue execution and must now be	continue execution and must now be
000000420A6F	terminated.	terminated.
0 :lJy9M	000000012884 000000412E84 0	000000012884 000000412E84 0
000000008AD4	Unknown security failure detected!	Unknown security failure detected!
000000420AD4	000000012C04 000000413204 0	000000012C04 000000413204 0
0 zYd%Lh	CONIN$	CONIN$
000000008AFB	000000012C0C 00000041320C 0	000000012C0C 00000041320C 0
000000420AFB	CONOUT$	CONOUT$
0 [v1r.	000000013D50 000000414B50 0	000000013D50 000000414B50 0
000000008B3C	(UNKNOWN)	(UNKNOWN)
000000420B3C	000000013D6C 000000414B6C 0	000000013D6C 000000414B6C 0
0 VKCDA	sent %d, rcvd %d	sent %d, rcvd %d
000000008BC5	000000013D80 000000414B80 0	000000013D80 000000414B80 0
000000420BC5	0123456789abcdef	0123456789abcdef
0 sN0X!	000000014D38 000000418738 0	000000014D38 000000418738 0
000000008BDD	KERNEL32.dll	KERNEL32.dll
000000420BDD	000000014D46 000000418746 0	000000014D46 000000418746 0
0 <= 286	GetLastError	GetLastError
000000008BE5	000000014D54 000000418754 0	000000014D54 000000418754 0
000000420BE5	CloseHandle	CloseHandle
0 zN-AR	000000014D61 000000418761 0	000000014D61 000000418761 0
000000008C75	CreateProcessA	CreateProcessA
000000420C75	000000014D71 000000418771 0	000000014D71 000000418771 0
0 !501<	DuplicateHandle	DuplicateHandle
000000008D35	000000014D82 000000418782 0	000000014D82 000000418782 0
000000420D35	GetCurrentProcess	GetCurrentProcess
0 P1s1T	000000014D95 000000418795 0	000000014D95 000000418795 0
000000008D3F	ExitThread	ExitThread
000000420D3F	000000014DA1 0000004187A1 0	000000014DA1 0000004187A1 0
0 q@!aF'	Sleep	Sleep
000000008E11	000000014DA8 0000004187A8 0	000000014DA8 0000004187A8 0
000000420E11	ReadFile	ReadFile
0 :!hIA8		
000000008E18	**File pos Mem pos ID Text**	**File pos Mem pos ID Text**
000000420E18	======== ======= ==	======== ======= ==
0 &.<_N*9	====	====
000000008E29		
000000420E29	000000014DB2 0000004187B2 0	000000014DB2 0000004187B2 0
0 \,#8Z~#	PeekNamedPipe	PeekNamedPipe
000000008F08	000000014DC1 0000004187C1 0	000000014DC1 0000004187C1 0
000000420F08	WriteFile	WriteFile
0 IYZfA	000000014DCC 0000004187CC 0	000000014DCC 0000004187CC 0
000000008F18	CreatePipe	CreatePipe
000000420F18	000000014DD8 0000004187D8 0	000000014DD8 0000004187D8 0
0 Popu*	DisconnectNamedPipe	DisconnectNamedPipe
000000008F20	000000014DED 0000004187ED 0	000000014DED 0000004187ED 0
000000420F20	TerminateProcess	TerminateProcess
0 !G81M	000000014DFF 0000004187FF 0	000000014DFF 0000004187FF 0
0000000090BD	WaitForMultipleObjects	WaitForMultipleObjects
0000004210BD	000000014E17 000000418817 0	000000014E17 000000418817 0
0 pepE@	TerminateThread	TerminateThread
000000009152	000000014E28 000000418828 0	000000014E28 000000418828 0

000000421152	CreateThread	CreateThread
0	000000014E36 000000418836 0	000000014E36 000000418836 0
V)h$\#"upzQZ	GetStdHandle	GetStdHandle
00000000918B	000000014E44 000000418844 0	000000014E44 000000418844 0
00000042118B	FreeConsole	FreeConsole
0 p82,!<	000000014E51 000000418851 0	000000014E51 000000418851 0
00000000919E	WriteConsoleA	WriteConsoleA
00000042119E	000000014E60 000000418860 0	000000014E60 000000418860 0
0 u"nrY	CreateFileA	CreateFileA
000000009294	000000014E6D 00000041886D 0	000000014E6D 00000041886D 0
000000421294	GetNumberOfConsoleInputEvents	GetNumberOfConsoleInputEvents
0 (UNK#OW	000000014E8C 00000041888C 0	000000014E8C 00000041888C 0
0000000092AA	PeekConsoleInputA	PeekConsoleInputA
0000004212AA	000000014E9F 00000041889F 0	000000014E9F 00000041889F 0
0 sent	GetConsoleMode	GetConsoleMode
0000000092B4	000000014EAF 0000004188AF 0	000000014EAF 0000004188AF 0
0000004212B4	SetConsoleMode	SetConsoleMode
0 r;cvl	000000014EBF 0000004188BF 0	000000014EBF 0000004188BF 0
0000000092BD	ReadConsoleInputA	ReadConsoleInputA
0000004212BD	000000014ED2 0000004188D2 0	000000014ED2 0000004188D2 0
0 12345678	GetCurrentProcessId	GetCurrentProcessId
0000000092C6	000000014EE7 0000004188E7 0	000000014EE7 0000004188E7 0
0000004212C6	GetCurrentThreadId	GetCurrentThreadId
0 9abcdef	000000014EFB 0000004188FB 0	000000014EFB 0000004188FB 0
000000009316	GetTickCount	GetTickCount
000000421316	000000014F09 000000418909 0	000000014F09 000000418909 0
0 % @dt	QueryPerformanceCounter	QueryPerformanceCounter
000000009342	000000014F22 000000418922 0	000000014F22 000000418922 0
000000421342	LCMapStringW	LCMapStringW
0 H$yH8	000000014F30 000000418930 0	000000014F30 000000418930 0
00000000942C	LCMapStringA	LCMapStringA
00000042142C	000000014F3E 00000041893E 0	000000014F3E 00000041893E 0
0 GC)P4	GetLocaleInfoA	GetLocaleInfoA
00000000949F	000000014F4E 00000041894E 0	000000014F4E 00000041894E 0
00000042149F	InterlockedExchange	InterlockedExchange
0 JetgasCEr	000000014F63 000000418963 0	000000014F63 000000418963 0
0000000094B9	LoadLibraryA	LoadLibraryA
0000004214B9	000000014F71 000000418971 0	000000014F71 000000418971 0
0 y}tgP.c	VirtualQuery	VirtualQuery
0000000094C6	000000014F7F 00000041897F 0	000000014F7F 00000041897F 0
0000004214C6	GetSystemInfo	GetSystemInfo
0 upliz$3	000000014F8E 00000041898E 0	000000014F8E 00000041898E 0
0000000094DD	VirtualProtect	VirtualProtect
0000004214DD	000000014F9E 00000041899E 0	000000014F9E 00000041899E 0
0	GetStringTypeW	GetStringTypeW
Th8md7VBwp	000000014FAE 0000004189AE 0	000000014FAE 0000004189AE 0
0000000094EA	GetStringTypeA	GetStringTypeA
0000004214EA	000000014FBE 0000004189BE 0	000000014FBE 0000004189BE 0
0 3FiYS	HeapSize	HeapSize
0000000094F6	000000014FC8 0000004189C8 0	000000014FC8 0000004189C8 0
0000004214F6	SetStdHandle	SetStdHandle
0 ?P p7ZrP	000000014FD6 0000004189D6 0	000000014FD6 0000004189D6 0
00000000954E	SetFilePointer	SetFilePointer

00000042154E	000000014FE6 0000004189E6 0	000000014FE6 0000004189E6 0
0 3Numb	SetEnvironmentVariableA	SetEnvironmentVariableA
000000009555	000000014FFF 0000004189FF 0	000000014FFF 0000004189FF 0
000000421555	GetOEMCP	GetOEMCP
0 Of	000000015009 000000418A09 0	000000015009 000000418A09 0
gIbpuA#vW	HeapFree	HeapFree
0000000095BB	000000015013 000000418A13 0	000000015013 000000418A13 0
0000004215BB	HeapAlloc	HeapAlloc
0]Exfh	00000001501E 000000418A1E 0	00000001501E 000000418A1E 0
0000000095C7	ExitProcess	ExitProcess
0000004215C7	00000001502B 000000418A2B 0	00000001502B 000000418A2B 0
0 Lib}r	GetProcAddress	GetProcAddress
0000000095D6	00000001503B 000000418A3B 0	00000001503B 000000418A3B 0
0000004215D6	GetModuleHandleA	GetModuleHandleA
0 QiS6vesdm	000000015053 000000418A53 0	000000015053 000000418A53 0
0000000095E4	GetSystemTimeAsFileTime	GetSystemTimeAsFileTime
0000004215E4	00000001506C 000000418A6C 0	00000001506C 000000418A6C 0
0 j$q+S e$Ty	GetCommandLineA	GetCommandLineA
	00000001507D 000000418A7D 0	00000001507D 000000418A7D 0
File pos	GetVersionExA	GetVersionExA
Mem pos	00000001508C 000000418A8C 0	00000001508C 000000418A8C 0
ID Text	WideCharToMultiByte	WideCharToMultiByte
========	0000000150A1 000000418AA1 0	0000000150A1 000000418AA1 0
=======	SetHandleCount	SetHandleCount
== ====	0000000150B1 000000418AB1 0	0000000150B1 000000418AB1 0
	GetFileType	GetFileType
0000000095FF	0000000150BE 000000418ABE 0	0000000150BE 000000418ABE 0
0000004215FF	GetStartupInfoA	GetStartupInfoA
0 H]Puo	0000000150CF 000000418ACF 0	0000000150CF 000000418ACF 0
000000009619	HeapDestroy	HeapDestroy
000000421619	0000000150DC 000000418ADC	0000000150DC 000000418ADC
0 OEMCPUF_	0 HeapCreate	0 HeapCreate
00000000969E	0000000150E8 000000418AE8 0	0000000150E8 000000418AE8 0
00000042169E	VirtualFree	VirtualFree
0 ALsB	0000000150F5 000000418AF5 0	0000000150F5 000000418AF5 0
0000000096AC	VirtualAlloc	VirtualAlloc
0000004216AC	000000015103 000000418B03 0	000000015103 000000418B03 0
0 lu(shhxBqf	HeapReAlloc	HeapReAlloc
0000000096F1	000000015110 000000418B10 0	000000015110 000000418B10 0
0000004216F1	IsBadWritePtr	IsBadWritePtr
0 &etQP"2	00000001511F 000000418B1F 0	00000001511F 000000418B1F 0
000000009748	FlushFileBuffers	FlushFileBuffers
000000421748	000000015131 000000418B31 0	000000015131 000000418B31 0
0 3do2s	RtlUnwind	RtlUnwind
00000000004D	00000001513C 000000418B3C 0	00000001513C 000000418B3C 0
00000040004D	GetModuleFileNameA	GetModuleFileNameA
0 !Windows	000000015150 000000418B50 0	000000015150 000000418B50 0
Program	UnhandledExceptionFilter	UnhandledExceptionFilter
00000000022F	00000001516A 000000418B6A 0	00000001516A 000000418B6A 0
00000040022F	FreeEnvironmentStringsA	FreeEnvironmentStringsA
0 @.data	000000015183 000000418B83 0	000000015183 000000418B83 0
000000000258	GetEnvironmentStrings	GetEnvironmentStrings
000000400258		

0 .idata 000000000F34 000000422134 0	**File pos Mem pos ID Text** ======== ======= == ====	**File pos Mem pos ID Text** ======== ======= == ====
KERNEL32.dll 000000000F42 000000422142 0	00000001519A 000000418B9A 0 FreeEnvironmentStringsW 0000000151B3 000000418BB3 0 GetEnvironmentStringsW	00000001519A 000000418B9A 0 FreeEnvironmentStringsW 0000000151B3 000000418BB3 0 GetEnvironmentStringsW
LoadLibraryA 000000000F50 000000422150 0	0000000151CB 000000418BCB 0 CompareStringA 0000000151DB 000000418BDB 0 MultiByteToWideChar	0000000151CB 000000418BCB 0 CompareStringA 0000000151DB 000000418BDB 0 MultiByteToWideChar
GetProcAddress 000000001049 000000419049 0 D ~E-	0000000151F0 000000418BF0 0 GetCPInfo 0000000151FB 000000418BFB 0 CompareStringW	0000000151F0 000000418BF0 0 GetCPInfo 0000000151FB 000000418BFB 0 CompareStringW
00000000108D 00000041908D 0 ~xUV;	00000001520B 000000418C0B 0 GetACP 000000015213 000000418C13 0	00000001520B 000000418C0B 0 GetACP 000000015213 000000418C13 0
0000000010DC 0000004190DC 0 "e0B1	SetEndOfFile 000000015220 000000418C20 0 WSOCK32.dll	SetEndOfFile 000000015220 000000418C20 0 WSOCK32.dll
00000000125A 00000041925A 0 w8d.9C	000000011CBC 0000004122BC 0 (null) 000000012B1F 00000041311F 0	000000011CBC 0000004122BC 0 (null) 000000012B1F 00000041311F 0
000000001315 000000419315 0 RPht%	j>Wak?Xbl@YcmAZdnB[eoC\fpD]gq 00000000004D 00000040004D 0 !Windows Program	j>Wak?Xbl@YcmAZdnB[eoC\fpD]gq 00000000004D 00000040004D 0 !Windows Program
0000000013A7 0000004193A7 0 PQhW	000000000158 000000400158 0 0000F97D 000000000180 000000400180 0	000000000158 000000400158 0 0000F97D 000000000180 000000400180 0
0000000013C1 0000004193C1 0 YCc(;	000026F6 0000000001A8 0000004001A8 0 00001258	000026F6 0000000001A8 0000004001A8 0 00001258
00000000142C 00000041942C 0 5|o}A	0000000001D0 0000004001D0 0 00000C2B 00000000114E 00000040114E 0	0000000001D0 0000004001D0 0 00000C2B 00000000114E 00000040114E 0
000000001457 000000419457 0 Hv_,E	~xUV; 0000000012EB 0000004012EB 0 t$$t	~xUV; 0000000012EB 0000004012EB 0 t$$t
000000001512 000000419512 0 C66_C	000000001637 000000401637 0 ;D$$} 0000000016CE 0000004016CE 0	000000001637 000000401637 0 ;D$$} 0000000016CE 0000004016CE 0
000000001524 000000419524 0 1bNzC	t$(t! 0000000017E9 0000004017E9 0 ;l$$uM9	t$(t! 0000000017E9 0000004017E9 0 ;l$$uM9
000000001570 000000419570 0 0"DD@<	000000001B05 000000401B05 0 PVVVj 000000001B30 000000401B30 0	000000001B05 000000401B05 0 PVVVj 000000001B30 000000401B30 0
0000000015C7 0000004195C7 0 h lX(4|	VVVVVj 000000001BF9 000000401BF9 0 L$ QR	VVVVVj 000000001BF9 000000401BF9 0 L$ QR
00000000161D	000000001C6A 000000401C6A 0	000000001C6A 000000401C6A 0

00000041961D	D$$PQ	D$$PQ
0 6vgv$9	000000001D84 000000401D84 0	000000001D84 000000401D84 0
0000000017B5	L$$QR	L$$QR
0000004197B5	000000001E7A 000000401E7A 0	000000001E7A 000000401E7A 0
0 \oM,+TV	u#PPPPPj	u#PPPPPj
00000000187F	000000001F9C 000000401F9C 0	000000001F9C 000000401F9C 0
00000041987F	D$4Vh	D$4Vh
0 tWHlB	000000001FC5 000000401FC5 0	000000001FC5 000000401FC5 0
000000001957	u9SSSSSj	u9SSSSSj
000000419957	000000002019 000000402019 0	000000002019 000000402019 0
0 ddP2<	uDSSSSSj	uDSSSSSj
0000000019E9	000000002086 000000402086 0	000000002086 000000402086 0
0000004199E9	StWHtBHt*SSSSj	StWHtBHt*SSSSj
0 C"IDOU	0000000026DF 0000004026DF 0	0000000026DF 0000004026DF 0
0000000019F2	PQhlKA	PQhlKA
0000004199F2	000000002B7F 000000402B7F 0	000000002B7F 000000402B7F 0
0 a$gHm	f9=,UA	f9=,UA
000000001A4F	000000002D94 000000402D94 0	000000002D94 000000402D94 0
000000419A4F	f9=8UA	f9=8UA
0 0"6D<B	000000003678 000000403678 0	000000003678 000000403678 0
000000001A58	.BENu	.BENu
000000419A58	0000000037A2 0000004037A2 0	0000000037A2 0000004037A2 0
0 N$THZ	$SUVW	$SUVW
000000001B70	00000000382E 00000040382E 0	00000000382E 00000040382E 0
000000419B70	tsf9=hKA	tsf9=hKA
0 VhLj9	0000000038CC 0000004038CC 0	0000000038CC 0000004038CC 0
000000001B96	D$8RP	D$8RP
000000419B96	000000003935 000000403935 0	000000003935 000000403935 0
0 rt?@I	T$,Rj	T$,Rj
000000001C45	000000003995 000000403995 0	000000003995 000000403995 0
000000419C45	|$8QW	|$8QW
0 HPj(H	000000003C0D 000000403C0D 0	000000003C0D 000000403C0D 0
000000001CD6	L$8PQ	L$8PQ
000000419CD6	000000003E76 000000403E76 0	000000003E76 000000403E76 0
0 P$yhR	SVh\ A	SVh\ A
000000001D09	000000003E97 000000403E97 0	000000003E97 000000403E97 0
000000419D09	D$\PhX A	D$\PhX A
0 NVHPT	000000003F4A 000000403F4A 0	000000003F4A 000000403F4A 0
000000001D9F	D$ Ph	D$ Ph
000000419D9F	000000004183 000000404183 0	000000004183 000000404183 0
0 ;,0;f9=l,e	tuBI;	tuBI;
000000001DBF	000000004636 000000404636 0	000000004636 000000404636 0
000000419DBF	f9=<UA	f9=<UA
0 %yf$G	00000000464B 00000040464B 0	00000000464B 00000040464B 0
000000001E47	QRhlKA	QRhlKA
000000419E47	000000004836 000000404836 0	000000004836 000000404836 0
0 !P%lj	f9-<UA	f9-<UA
000000001F71	0000000048AA 0000004048AA 0	0000000048AA 0000004048AA 0
000000419F71	f9|$(	f9|$(
0 u7L}BH	0000000048D7 0000004048D7 0	0000000048D7 0000004048D7 0
000000002083	f95<UA	f95<UA
00000041A083	0000000048F5 0000004048F5 0	0000000048F5 0000004048F5 0
0 R;5Po	PQh|!A	PQh|!A

000000002240	0000000054A2 0000004054A2 0	0000000054A2 0000004054A2 0
00000041A240	C =02CVu	C =02CVu
0 p%u[A	0000000057B9 0000004057B9 0	0000000057B9 0000004057B9 0
00000000228E	B 02CV	B 02CV
00000041A28E	000000005D9E 000000405D9E 0	000000005D9E 000000405D9E 0
0 BizJsTM&#n	QQSV3	QQSV3
000000002326	000000005DBA 000000405DBA	000000005DBA 000000405DBA
00000041A326	0 VVVVj	0 VVVVj
0 }'A|"	00000000681F 00000040681F 0	00000000681F 00000040681F 0
000000002332	95$[A	95$[A
00000041A332	000000006869 000000406869 0	000000006869 000000406869 0
0 zg_>aD	95$[A	95$[A
00000000233A	00000000699F 00000040699F 0	00000000699F 00000040699F 0
00000041A33A	Yu+Vj	Yu+Vj
0 Af @X	000000007E63 000000407E63 0	000000007E63 000000407E63 0
0000000023A0	SVWUj	SVWUj
00000041A3A0	000000007ECC 000000407ECC 0	000000007ECC 000000407ECC 0
0 .BEN7u	t.;t$$t(	t.;t$$t(
0000000023A9		
00000041A3A9	**File pos Mem pos ID Text**	**File pos Mem pos ID Text**
0 xJ&dS	======== ======= ==	======== ======= ==
0000000023B1	====	====
00000041A3B1		
0 Dza/|	000000008A42 000000408A42 0	000000008A42 000000408A42 0
0000000023B7	oG<-uK	oG<-uK
00000041A3B7	000000008A50 000000408A50 0	000000008A50 000000408A50 0
0 y$--h	]t@G:	]t@G:
00000000243E	000000008C91 000000408C91 0	000000008C91 000000408C91 0
00000041A43E	YYj0[	YYj0[
0 BO!t/N	000000009774 000000409774 0	000000009774 000000409774 0
0000000024B3	QQSVW3	QQSVW3
00000041A4B3	000000009890 000000409890 0	000000009890 000000409890 0
0 P9 >t	@PVSS	@PVSS
0000000024C7	0000000098AE 0000004098AE 0	0000000098AE 0000004098AE 0
00000041A4C7	t#SSUP	t#SSUP
0 0I (s	0000000098B5 0000004098B5 0	0000000098B5 0000004098B5 0
00000000268A	t$$VSS	t$$VSS
00000041A68A	000000009984 000000409984 0	000000009984 000000409984 0
0 ~D60DUtJ	VC20XC00U	VC20XC00U
000000002693	000000009AE9 000000409AE9 0	000000009AE9 000000409AE9 0
00000041A693	j@h 'A	j@h 'A
0 FBVQA%	000000009B10 000000409B10 0	000000009B10 000000409B10 0
000000002748	PVPWW	PVPWW
00000041A748	000000009B8E 000000409B8E 0	000000009B8E 000000409B8E 0
0 (ht.E	9} u	9} u
00000000275F	00000000A37A 00000040A37A 0	00000000A37A 00000040A37A 0
00000041A75F	tSj=V	tSj=V
0 @LgxhX	00000000A53E 00000040A53E 0	00000000A53E 00000040A53E 0
000000002889	R95dWA	R95dWA
00000041A889	00000000A64B 00000040A64B 0	00000000A64B 00000040A64B 0
0 XN)"H	v N+D$	v N+D$
	00000000AE40 00000040AE40 0	00000000AE40 00000040AE40 0
File pos	wHVSU	wHVSU

Mem pos **ID Text**	00000000AF86 00000040AF86 0 SVWse	00000000AF86 00000040AF86 0 SVWse
======== =======	00000000B2A2 00000040B2A2 0 ;5$[A	00000000B2A2 00000040B2A2 0 ;5$[A
== ==== 0000000028F8	00000000B829 00000040B829 0 LSVWj 00000000B916 00000040B916 0	00000000B829 00000040B829 0 LSVWj 00000000B916 00000040B916 0
00000041A8F8 0 Mwl;B	VWumh 00000000C1F9 00000040C1F9 0	VWumh 00000000C1F9 00000040C1F9 0
000000002910 00000041A910	WWWWVSW 00000000C21E 00000040C21E 0	WWWWVSW 00000000C21E 00000040C21E 0
0 duXK" 000000002920	t2WWVPVSW 00000000C2A2 00000040C2A2 0	t2WWVPVSW 00000000C2A2 00000040C2A2 0
00000041A920 0 h "A	u8SS3 00000000C4A0 00000040C4A0 0	u8SS3 00000000C4A0 00000040C4A0 0
00000000295F 00000041A95F	t!SS9] 00000000C8C7 00000040C8C7 0	t!SS9] 00000000C8C7 00000040C8C7 0
0 tuB1$ 000000002AD7	;=$[A 00000000CC90 00000040CC90 0	;=$[A 00000000CC90 00000040CC90 0
00000041AAD7 0 (]XIa	;=$[A 00000000D367 00000040D367 0	;=$[A 00000000D367 00000040D367 0
000000002B7A 00000041AB7A	s"95(RA 000000010A00 000000411000 0	s"95(RA 000000010A00 000000411000 0
0 tJ\[Bh 000000002C59	POSIXLY_CORRECT 000000010A14 000000411014 0	POSIXLY_CORRECT 000000010A14 000000411014 0
00000041AC59 0 ~//*	%s: invalid option -- %c 000000010A34 000000411034 0	%s: invalid option -- %c 000000010A34 000000411034 0
000000002DEA 00000041ADEA	%s: illegal option -- %c 000000010A54 000000411054 0	%s: illegal option -- %c 000000010A54 000000411054 0
0 2hPt#@ 000000002E5E	%s: option requires an argument -- %c 000000010A84 000000411084 0	%s: option requires an argument -- %c 000000010A84 000000411084 0
00000041AE5E 0	%s: unrecognized option 000000010A9D 00000041109D 0	%s: unrecognized option 000000010A9D 00000041109D 0
pD[JV)EP?C"6 000000002EA9	%c%s' 000000010AAC 0000004110AC	%c%s' 000000010AAC 0000004110AC
00000041AEA9 0 !&C2]	0 %s: unrecognized option 000000010AC5 0000004110C5 0	0 %s: unrecognized option 000000010AC5 0000004110C5 0
i$uH 000000002F2E	--%s' 000000010AD4 0000004110D4 0	--%s' 000000010AD4 0000004110D4 0
00000041AF2E 0 Dd@2<	%s: option 000000010AE0 0000004110E0 0	%s: option 000000010AE0 0000004110E0 0
000000002FDD 00000041AFDD	%s' requires an argument 000000010B04 000000411104 0	%s' requires an argument 000000010B04 000000411104 0
0 Np@HVj 0000000030E4	%s: option 000000010B10 000000411110 0	%s: option 000000010B10 000000411110 0
00000041B0E4 0 &<7u#	%c%s' doesn't allow an argument 000000010B3C 00000041113C 0	%c%s' doesn't allow an argument 000000010B3C 00000041113C 0
000000003172 00000041B172	%s: option 000000010B48 000000411148 0	%s: option 000000010B48 000000411148 0
0 _{i$f 0000000031DB	--%s' doesn't allow an argument 000000010B74 000000411174 0	--%s' doesn't allow an argument 000000010B74 000000411174 0
00000041B1DB 0 6Gx?u;	%s: option 000000010B80 000000411180 0	%s: option 000000010B80 000000411180 0

0000000032DD	%s' is ambiguous	%s' is ambiguous
00000041B2DD	000000010B9C 00000041119C 0	000000010B9C 00000041119C 0
0 8bI?<J	Failed to execute shell, error = %s	Failed to execute shell, error = %s
000000003378	000000010BC8 0000004111C8 0	000000010BC8 0000004111C8 0
00000041B378	SessionReadShellThreadFn exitted,	SessionReadShellThreadFn exitted,
0 zpFrU	error = %s	error = %s
0000000035BF	000000010C08 000000411208 0	000000010C08 000000411208 0
00000041B5BF	Failed to execute shell	Failed to execute shell
0 Bz(@/	000000010C24 000000411224 0	000000010C24 000000411224 0
00000000379E	Failed to create shell stdin pipe, error	Failed to create shell stdin pipe, error
00000041B79E	= %s	= %s
0 "2j{!	000000010C5C 00000041125C 0	000000010C5C 00000041125C 0
0000000037D6	Failed to create shell stdout pipe, error	Failed to create shell stdout pipe, error
00000041B7D6	= %s	= %s
0 c'yt D	000000010C94 000000411294 0	000000010C94 000000411294 0
000000003858	WaitForMultipleObjects error: %s	WaitForMultipleObjects error: %s
00000041B858	000000010CBC 0000004112BC 0	000000010CBC 0000004112BC 0
0 4Y8q$!Jpg7	Failed to create ReadShell session	Failed to create ReadShell session
000000003898	thread, error = %s	thread, error = %s
00000041B898	000000010CFC 0000004112FC 0	000000010CFC 0000004112FC 0
0 {B2v)	unknown socket error	unknown socket error
00000000392E	000000010D18 000000411318 0	000000010D18 000000411318 0
00000041B92E	NO_DATA	NO_DATA
0 +Kp~Z	000000010D2C 00000041132C 0	000000010D2C 00000041132C 0
000000003A65	NO_RECOVERY	NO_RECOVERY
00000041BA65	000000010D40 000000411340 0	000000010D40 000000411340 0
0 t!RD	TRY_AGAIN	TRY_AGAIN
000000003C30	000000010D54 000000411354 0	000000010D54 000000411354 0
00000041BC30	HOST_NOT_FOUND	HOST_NOT_FOUND
0 hP (l	000000010D68 000000411368 0	000000010D68 000000411368 0
000000003D3E	DISCON	DISCON
00000041BD3E	000000010D7C 00000041137C 0	000000010D7C 00000041137C 0
0 }HpVPt	NOTINITIALISED	NOTINITIALISED
000000003D7D	000000010D90 000000411390 0	000000010D90 000000411390 0
00000041BD7D	VERNOTSUPPORTED	VERNOTSUPPORTED
0 E3D=7	000000010DA4 0000004113A4 0	000000010DA4 0000004113A4 0
000000003E77	SYSNOTREADY	SYSNOTREADY
00000041BE77	000000010DB8 0000004113B8 0	000000010DB8 0000004113B8 0
0 "rIf	REMOTE	REMOTE
000000003FF0	000000010DCC 0000004113CC 0	000000010DCC 0000004113CC 0
00000041BFF0	STALE	STALE
0 QfV05)		
000000004022	**File pos Mem pos ID Text**	**File pos Mem pos ID Text**
00000041C022	======== ======= ==	======== ======= ==
0 ~-"]P	====	====
0000000040F3		
00000041C0F3	000000010DE0 0000004113E0 0	000000010DE0 0000004113E0 0
0 p;9P5j}	DQUOT	DQUOT
0000000042C3	000000010DF4 0000004113F4 0	000000010DF4 0000004113F4 0
00000041C2C3	USERS	USERS
0 h!CD	000000010E08 000000411408 0	000000010E08 000000411408 0
000000004491	PROCLIM	PROCLIM
00000041C491	000000010E1C 00000041141C 0	000000010E1C 00000041141C 0

0 L;u	NOTEMPTY	NOTEMPTY
00000000452F	000000010E30 000000411430 0	000000010E30 000000411430 0
00000041C52F	HOSTUNREACH	HOSTUNREACH
0 +xaQiu~	000000010E44 000000411444 0	000000010E44 000000411444 0
00000000460D	HOSTDOWN	HOSTDOWN
00000041C60D	000000010E58 000000411458 0	000000010E58 000000411458 0
0 B0M 7E|C@	NAMETOOLONG	NAMETOOLONG
0000000047C1	000000010E6C 00000041146C 0	000000010E6C 00000041146C 0
00000041C7C1	LOOP	LOOP
0 <;'jv8	000000010E80 000000411480 0	000000010E80 000000411480 0
000000004812	connection refused	connection refused
00000041C812	000000010E98 000000411498 0	000000010E98 000000411498 0
0 pJw'to:	TIMEDOUT	TIMEDOUT
00000000482B	000000010EAC 0000004114AC 0	000000010EAC 0000004114AC 0
00000041C82B	TOOMANYREFS	TOOMANYREFS
0 y"KsH{	000000010EC0 0000004114C0 0	000000010EC0 0000004114C0 0
00000000494C	SHUTDOWN	SHUTDOWN
00000041C94C	000000010ED4 0000004114D4 0	000000010ED4 0000004114D4 0
0 ?~4lX	NOTCONN	NOTCONN
0000000049D2	000000010EE8 0000004114E8 0	000000010EE8 0000004114E8 0
00000041C9D2	ISCONN	ISCONN
0 |k13W	000000010EFC 0000004114FC 0	000000010EFC 0000004114FC 0
000000004C1C	NOBUFS	NOBUFS
00000041CC1C	000000010F10 000000411510 0	000000010F10 000000411510 0
0 HTjw%	CONNRESET	CONNRESET
000000004D0B	000000010F24 000000411524 0	000000010F24 000000411524 0
00000041CD0B	CONNABORTED	CONNABORTED
0 &IZK/	000000010F38 000000411538 0	000000010F38 000000411538 0
000000004F48	NETRESET	NETRESET
00000041CF48	000000010F4C 00000041154C 0	000000010F4C 00000041154C 0
0 9%s")	NETUNREACH	NETUNREACH
000000004FAF	000000010F60 000000411560 0	000000010F60 000000411560 0
00000041CFAF	NETDOWN	NETDOWN
0 dCSb-	000000010F74 000000411574 0	000000010F74 000000411574 0
000000004FB8	ADDRNOTAVAIL	ADDRNOTAVAIL
00000041CFB8	000000010F88 000000411588 0	000000010F88 000000411588 0
0 :5 1X	ADDRINUSE	ADDRINUSE
000000005231	000000010F9C 00000041159C 0	000000010F9C 00000041159C 0
00000041D231	AFNOSUPPORT	AFNOSUPPORT
0 XundN	000000010FB0 0000004115B0 0	000000010FB0 0000004115B0 0
00000000527C	PFNOSUPPORT	PFNOSUPPORT
00000041D27C	000000010FC4 0000004115C4 0	000000010FC4 0000004115C4 0
0 52\5T	OPNOTSUPP	OPNOTSUPP
0000000052B0	000000010FD8 0000004115D8 0	000000010FD8 0000004115D8 0
00000041D2B0	SOCKTNOSUPPORT	SOCKTNOSUPPORT
0 vH)T+	000000010FEC 0000004115EC 0	000000010FEC 0000004115EC 0
00000000531F	PROTONOSUPPORT	PROTONOSUPPORT
00000041D31F	000000011000 000000411600 0	000000011000 000000411600 0
0 (dP2l'	NOPROTOOPT	NOPROTOOPT
00000000558A	000000011014 000000411614 0	000000011014 000000411614 0
00000041D58A	PROTOTYPE	PROTOTYPE
0 u|l8l	000000011028 000000411628 0	000000011028 000000411628 0
0000000055B1	MSGSIZE	MSGSIZE

00000041D5B1 0 1e t NE	00000001103C 00000041163C 0 DESTADDRREQ	00000001103C 00000041163C 0 DESTADDRREQ
00000000569E 00000041D69E 0 P>9]!	000000011050 000000411650 0 NOTSOCK 000000011064 000000411664 0 ALREADY	000000011050 000000411650 0 NOTSOCK 000000011064 000000411664 0 ALREADY
0000000056E4 00000041D6E4 0 c{(uw	000000011078 000000411678 0 INPROGRESS	000000011078 000000411678 0 INPROGRESS
0000000058C6 00000041D8C6 0 "INrB	00000001108C 00000041168C 0 WOULDBLOCK 0000000110A0 0000004116A0 0 MFILE	00000001108C 00000041168C 0 WOULDBLOCK 0000000110A0 0000004116A0 0 MFILE
0000000058D5 00000041D8D5 0 p%t{4\!	0000000110B4 0000004116B4 0 INVAL	0000000110B4 0000004116B4 0 INVAL
0000000059DE 00000041D9DE 0 u>fe\	0000000110C8 0000004116C8 0 FAULT 0000000110DC 0000004116DC 0 ACCES	0000000110C8 0000004116C8 0 FAULT 0000000110DC 0000004116DC 0 ACCES
000000005A29 00000041DA29 0 .t' pi#	0000000110F0 0000004116F0 0 BADF	0000000110F0 0000004116F0 0 BADF
000000005A33 00000041DA33 0 K7,:T	000000011104 000000411704 0 INTR 000000011124 000000411724 0 punt!	000000011104 000000411704 0 INTR 000000011124 000000411724 0 punt!
000000005C7F 00000041DC7F 0 ?B bC	00000001112C 00000041172C 0 spurious timer interrupt!	00000001112C 00000041172C 0 spurious timer interrupt!
000000005D2F 00000041DD2F 0 K>=0>	00000001114C 00000041174C 0 Hmalloc %d failed 000000011164 000000411764 0 DNS fwd/rev mismatch: %s != %s	00000001114C 00000041174C 0 Hmalloc %d failed 000000011164 000000411764 0 DNS fwd/rev mismatch: %s != %s
File pos **Mem pos** **ID Text**	00000001118C 00000041178C 0 Warning: forward host lookup failed for %s: h_errno %d	00000001118C 00000041178C 0 Warning: forward host lookup failed for %s: h_errno %d
======== ======= == ====	0000000111D0 0000004117D0 0 %s: inverse host lookup failed: h_errno %d	0000000111D0 0000004117D0 0 %s: inverse host lookup failed: h_errno %d
000000005DDF 00000041DDDF 0 G[q$5	000000011204 000000411804 0 Warning: inverse host lookup failed for %s: h_errno %d 000000011248 000000411848 0 %s: forward host lookup failed: h_errno %d	000000011204 000000411804 0 Warning: inverse host lookup failed for %s: h_errno %d 000000011248 000000411848 0 %s: forward host lookup failed: h_errno %d
000000005E90 00000041DE90 0 \I8rJ	00000001127C 00000041187C 0 gethostpoop fuxored	00000001127C 00000041187C 0 gethostpoop fuxored
000000005E9C 00000041DE9C 0 K-\n:	000000011294 000000411894 0 Can't parse %s as an IP address	000000011294 000000411894 0 Can't parse %s as an IP address
000000005EDA 00000041DEDA 0 lVQ%0	0000000112C0 0000004118C0 0 Warning: port-bynum mismatch, %d != %d	0000000112C0 0000004118C0 0 Warning: port-bynum mismatch, %d != %d
000000006005 00000041E005 0 VC20X	0000000112F0 0000004118F0 0 loadports: bogus values %d, %d 000000011318 000000411918 0 loadports: no block?!	0000000112F0 0000004118F0 0 loadports: bogus values %d, %d 000000011318 000000411918 0 loadports: no block?!
00000000605C		

00000041E05C	000000011334 000000411934 0	000000011334 000000411934 0
0 5?xH<	Warning: source routing unavailable	Warning: source routing unavailable
0000000060BB	on this machine, ignoring	on this machine, ignoring
00000041E0BB	000000011380 000000411980 0	000000011380 000000411980 0
0 KX=zg	Can't grab %s:%d with bind	Can't grab %s:%d with bind
0000000062A6	0000000113A0 0000004119A0 0	0000000113A0 0000004119A0 0
00000041E2A6	retrying local %s:%d	retrying local %s:%d
0 <tf.S N	0000000113BC 0000004119BC 0	0000000113BC 0000004119BC 0
0000000062DE	nnetfd reuseaddr failed	nnetfd reuseaddr failed
00000041E2DE	0000000113D8 0000004119D8 0	0000000113D8 0000004119D8 0
0] !W>	Can't get socket	Can't get socket
0000000062F5	0000000113EC 0000004119EC 0	0000000113EC 0000004119EC 0
00000041E2F5	connect to [%s] from %s [%s] %d	connect to [%s] from %s [%s] %d
0 p~tRI		
0000000063C0	**File pos Mem pos ID Text**	**File pos Mem pos ID Text**
00000041E3C0	======== ======= ==	======== ======= ==
0 Q506VJ	====	====
000000006415		
00000041E415	000000011414 000000411A14 0	000000011414 000000411A14 0
0 _8[jJ	invalid connection to [%s] from %s	invalid connection to [%s] from %s
0000000064DB	[%s] %d	[%s] %d
00000041E4DB	000000011448 000000411A48 0	000000011448 000000411A48 0
0 :>$;#i	post-rcv getsockname failed	post-rcv getsockname failed
000000006568	00000001146C 000000411A6C 0	00000001146C 000000411A6C 0
00000041E568	] %d ...	] %d ...
0 "K0@(v	00000001147C 000000411A7C 0	00000001147C 000000411A7C 0
00000000660F	listening on [	listening on [
00000041E60F	000000011490 000000411A90 0	000000011490 000000411A90 0
0 "WZP!	local getsockname failed	local getsockname failed
0000000066A0	0000000114B0 000000411AB0 0	0000000114B0 000000411AB0 0
00000041E6A0	local listen fuxored	local listen fuxored
0 tSj|=,	0000000114CC 000000411ACC 0	0000000114CC 000000411ACC 0
000000006749	UDP listen needs -p arg	UDP listen needs -p arg
00000041E749	0000000114E8 000000411AE8 0	0000000114E8 000000411AE8 0
0 DE{V	udptest first write failed?! errno %d	udptest first write failed?! errno %d
	000000011518 000000411B18 0	000000011518 000000411B18 0
000000006763	ofd write err	ofd write err
00000041E763	000000011528 000000411B28 0	000000011528 000000411B28 0
0 H*dQt	%8.8x	%8.8x
000000006769	000000011530 000000411B30 0	000000011530 000000411B30 0
00000041E769	oprint called with no open fd?!	oprint called with no open fd?!
0 &4d{,U	000000011558 000000411B58 0	000000011558 000000411B58 0
000000006791	too many output retries	too many output retries
00000041E791	000000011574 000000411B74 0	000000011574 000000411B74 0
0 8P1R*A	net timeout	net timeout
0000000067E6	000000011584 000000411B84 0	000000011584 000000411B84 0
00000041E7E6	select fuxored	select fuxored
0 AR959	000000011598 000000411B98 0	000000011598 000000411B98 0
000000006889	Preposterous Pointers: %d, %d	Preposterous Pointers: %d, %d
00000041E889	0000000115BC 000000411BBC 0	0000000115BC 000000411BBC 0
0 v N+23	port numbers can be individual or	port numbers can be individual or
0000000068CA	ranges: m-n [inclusive]	ranges: m-n [inclusive]
00000041E8CA	000000011608 000000411C08 0	000000011608 000000411C08 0

0 wN=4u	-u UDP mode	-u UDP mode
0000000069A2	000000011616 000000411C16 0	000000011616 000000411C16 0
00000041E9A2	-v verbose [use	-v verbose [use
0 I,R.&	twice to be more verbose]	twice to be more verbose]
0000000069B0	000000011642 000000411C42 0	000000011642 000000411C42 0
00000041E9B0	-w secs timeout for	-w secs timeout for
0 $h6$)?7=	connects and final net reads	connects and final net reads
000000006AA8	000000011675 000000411C75 0	000000011675 000000411C75 0
00000041EAA8	-z zero-I/O	-z zero-I/O
0 d PHd	mode [used for scanning]	mode [used for scanning]
000000006AC2	0000000116BC 000000411CBC 0	0000000116BC 000000411CBC 0
00000041EAC2	-t answer	-t answer
0 x|3y;.	TELNET negotiation	TELNET negotiation
000000006D66	0000000116E8 000000411CE8 0	0000000116E8 000000411CE8 0
00000041ED66	-g gateway source-	-g gateway source-
0 @qSJA#p	routing hop point[s], up to 8	routing hop point[s], up to 8
000000006DC9	000000011719 000000411D19 0	000000011719 000000411D19 0
00000041EDC9	-G num source-	-G num source-
0 H0/[Z	routing pointer: 4, 8, 12, ...	routing pointer: 4, 8, 12, ...
000000006E89	000000011748 000000411D48 0	000000011748 000000411D48 0
00000041EE89	-h this cruft	-h this cruft
0 hPy=9O@3	000000011758 000000411D58 0	000000011758 000000411D58 0
	-i secs delay	-i secs delay
000000006ED5	interval for lines sent, ports scanned	interval for lines sent, ports scanned
00000041EED5	00000001178F 000000411D8F 0	00000001178F 000000411D8F 0
0 '\R<'	-l listen mode,	-l listen mode,
000000007231	for inbound connects	for inbound connects
00000041F231	0000000117B6 000000411DB6 0	0000000117B6 000000411DB6 0
0 w~*9E>	-L listen	-L listen
0000000072EF	harder, re-listen on socket close	harder, re-listen on socket close
00000041F2EF	0000000117E4 000000411DE4 0	0000000117E4 000000411DE4 0
0 s-y<<<	-n numeric-	-n numeric-
000000007312	only IP addresses, no DNS	only IP addresses, no DNS
00000041F312	00000001180B 000000411E0B 0	00000001180B 000000411E0B 0
0 Q+@P&	-o file hex dump	-o file hex dump
000000007339	of traffic	of traffic
00000041F339	000000011829 000000411E29 0	000000011829 000000411E29 0
0 58!ha	-p port local port	-p port local port
00000000745A	number	number
00000041F45A	000000011845 000000411E45 0	000000011845 000000411E45 0
0 (" D	-r randomize	-r randomize
00000000753E	local and remote ports	local and remote ports
00000041F53E	00000001186B 000000411E6B 0	00000001186B 000000411E6B 0
0 TE@F;	-s addr local source	-s addr local source
000000007568	address	address
00000041F568	0000000118E0 000000411EE0 0	0000000118E0 000000411EE0 0
0 9VZ(E?	-e prog inbound	-e prog inbound
000000007579	program to exec [dangerous!!]	program to exec [dangerous!!]
00000041F579	00000001191C 000000411F1C 0	00000001191C 000000411F1C 0
0 ".,8x2	-d detach from	-d detach from
000000007774	console, background mode	console, background mode
00000041F774	000000011950 000000411F50 0	000000011950 000000411F50 0
0 KP'sz(K	[v1.10 NT]	[v1.10 NT]

00000000796B 00000041F96B 0 4"PQA	00000001195B 000000411F5B 0 connect to somewhere: nc [-options] hostname port[s] [ports] ...	00000001195B 000000411F5B 0 connect to somewhere: nc [-options] hostname port[s] [ports] ...
0000000079F8 00000041F9F8 0 Unt>K	00000001199D 000000411F9D 0 listen for inbound: nc -l -p port [options] [hostname] [port]	00000001199D 000000411F9D 0 listen for inbound: nc -l -p port [options] [hostname] [port]
000000007B3C 00000041FB3C 0 -;=h%	0000000119DB 000000411FDB 0 options:	0000000119DB 000000411FDB 0 options:
000000007B52 00000041FB52 0 HD0Ii	000000011A04 000000412004 0 You entered an Incorrect Password. Exiting...	000000011A04 000000412004 0 You entered an Incorrect Password. Exiting...
000000007BD4 00000041FBD4 0 <d@2D	000000011A40 000000412040 0 Password accepted!	000000011A40 000000412040 0 Password accepted!
000000007C9F 00000041FC9F 0 k@Aq;1	000000011A5C 00000041205C 0 Enter Password:	000000011A5C 00000041205C 0 Enter Password:
000000007D3E 00000041FD3E 0 4=dW)	000000011A70 000000412070 0 no port[s] to connect to	000000011A70 000000412070 0 no port[s] to connect to
000000007E57 00000041FE57 0 6/)#7	000000011A90 000000412090 0 no destination	000000011A90 000000412090 0 no destination
000000008334 000000420334 0 t"wQB)Gu	000000011AA4 0000004120A4 0 no connection	000000011AA4 0000004120A4 0 no connection
0000000083C9 0000004203C9 0 a@}>m52	000000011AB4 0000004120B4 0 invalid port %s	000000011AB4 0000004120B4 0 invalid port %s
00000000845F 00000042045F 0 OSIXLY_C	000000011AC8 0000004120C8 0 can't open %s	000000011AC8 0000004120C8 0 can't open %s
000000008474 000000420474 0 inval	000000011AD8 0000004120D8 0 nc -h for help	000000011AD8 0000004120D8 0 nc -h for help
00000000848B 00000042048B 0 dN l&egD	000000011AEC 0000004120EC 0 invalid wait-time %s	000000011AEC 0000004120EC 0 invalid wait-time %s
000000008506 000000420506 0 u>{=shf	000000011B08 000000412108 0 too many -g hops	000000011B08 000000412108 0 too many -g hops
00000000851F 00000042051F 0 wR=ad	000000011B1C 00000041211C 0 invalid hop pointer %d, must be multiple of 4 <= 28	000000011B1C 00000041211C 0 invalid hop pointer %d, must be multiple of 4 <= 28
00000000852B 00000042052B 0 Fnw7itt	000000011B5C 00000041215C 0 all-A-records NIY	000000011B5C 00000041215C 0 all-A-records NIY
00000000855B 00000042055B 0 ptF,M;ul	000000011B74 000000412174 0 wrong	000000011B74 000000412174 0 wrong
000000008593 000000420593	000000011B7C 00000041217C 0 sent %d, rcvd %d 000000011B90 000000412190 0 %s [%s] %d (%s) 000000011BA4 0000004121A4 0 %s [%s] %d (%s) open 000000011BC0 0000004121C0 0 invalid local port %s 000000011BDC 0000004121DC 0 invalid interval time %s 000000011BFC 0000004121FC 0 ade:g:G:hi:lLno:p:rs:tuvw:z 000000011C20 000000412220 0 Cmd line: 000000011C30 000000412230 0	000000011B7C 00000041217C 0 sent %d, rcvd %d 000000011B90 000000412190 0 %s [%s] %d (%s) 000000011BA4 0000004121A4 0 %s [%s] %d (%s) open 000000011BC0 0000004121C0 0 invalid local port %s 000000011BDC 0000004121DC 0 invalid interval time %s 000000011BFC 0000004121FC 0 ade:g:G:hi:lLno:p:rs:tuvw:z 000000011C20 000000412220 0 Cmd line: 000000011C30 000000412230 0

0 NO_DAT 0000000085AB 0000004205AB 0 _AGEIN,(H 0000000085B5 0000004205B5 0 T6T_Z **File pos** **Mem pos** **ID Text** ======== ======= == ==== 0000000085BB 0000004205BB 0 yFwURD 0000000085C2 0000004205C2 0 w7ISt 0000000085D0 0000004205D0 0 AeL:E6(0000000085FA 0000004205FA 0 DQhUP 000000008629 000000420629 0 AMETO 000000008654 000000420654 0 MANbY 00000000865E 00000042065E 0)HU|R 00000000867F 00000042067F 0 h<SBD' 0000000086D2 0000004206D2 0 IZEy\ 0000000086FD 0000004206FD 0 ~,xFLI 000000008743 000000420743 0 ~pF!L 000000008809 000000420809 0 k$?!0TLs 000000008822 000000420822	**CorExitProcess** **File pos Mem pos ID Text** ======== ======= == ==== 000000011C40 000000412240 0 mscoree.dll 000000011C81 000000412281 0 (8PX 000000011C89 000000412289 0 700WP 000000011CA1 0000004122A1 0 ppxxxx 000000011CCC 0000004122CC 0 (null) 000000011D14 000000412314 0 runtime error 000000011D28 000000412328 0 TLOSS error 000000011D38 000000412338 0 SING error 000000011D48 000000412348 0 DOMAIN error 000000011D58 000000412358 0 R6029 000000011D5F 00000041235F 0 - This application cannot run using the active version of the Microsoft .NET Runtime 000000011DB4 0000004123B4 0 Please contact the application's support team for more information. 000000011DFC 0000004123FC 0 R6028 000000011E03 000000412403 0 - unable to initialize heap 000000011E24 000000412424 0 R6027 000000011E2B 00000041242B 0 - not enough space for lowio initialization 000000011E5C 00000041245C 0 R6026 000000011E63 000000412463 0 - not enough space for stdio initialization 000000011E94 000000412494 0 R6025 000000011E9B 00000041249B 0 - pure virtual function call 000000011EBC 0000004124BC 0 R6024	**CorExitProcess** **File pos Mem pos ID Text** ======== ======= == ==== 000000011C40 000000412240 0 mscoree.dll 000000011C81 000000412281 0 (8PX 000000011C89 000000412289 0 700WP 000000011CA1 0000004122A1 0 ppxxxx 000000011CCC 0000004122CC 0 (null) 000000011D14 000000412314 0 runtime error 000000011D28 000000412328 0 TLOSS error 000000011D38 000000412338 0 SING error 000000011D48 000000412348 0 DOMAIN error 000000011D58 000000412358 0 R6029 000000011D5F 00000041235F 0 - This application cannot run using the active version of the Microsoft .NET Runtime 000000011DB4 0000004123B4 0 Please contact the application's support team for more information. 000000011DFC 0000004123FC 0 R6028 000000011E03 000000412403 0 - unable to initialize heap 000000011E24 000000412424 0 R6027 000000011E2B 00000041242B 0 - not enough space for lowio initialization 000000011E5C 00000041245C 0 R6026 000000011E63 000000412463 0 - not enough space for stdio initialization 000000011E94 000000412494 0 R6025 000000011E9B 00000041249B 0 - pure virtual function call 000000011EBC 0000004124BC 0 R6024

0 i\(D|	000000011EC3 0000004124C3 0	000000011EC3 0000004124C3 0
000000008853	- not enough space for _onexit/atexit	- not enough space for _onexit/atexit
000000420853	table	table
0 B$F<\:	000000011EF4 0000004124F4 0	000000011EF4 0000004124F4 0
00000000885A	R6019	R6019
00000042085A	000000011EFB 0000004124FB 0	000000011EFB 0000004124FB 0
0 tfd\F7R	- unable to open console device	- unable to open console device
000000008881	000000011F20 000000412520 0	000000011F20 000000412520 0
000000420881	R6018	R6018
0 r?38$p	000000011F27 000000412527 0	000000011F27 000000412527 0
0000000088B0	- unexpected heap error	- unexpected heap error
0000004208B0	000000011F44 000000412544 0	000000011F44 000000412544 0
0 kEB B:I5	R6017	R6017
0000000088E9	000000011F4B 00000041254B 0	000000011F4B 00000041254B 0
0000004208E9	- unexpected multithread lock error	- unexpected multithread lock error
0 !%8.Ox	000000011F74 000000412574 0	000000011F74 000000412574 0
000000008953	R6016	R6016
000000420953	000000011F7B 00000041257B 0	000000011F7B 00000041257B 0
0 om-Xa6cl	- not enough space for thread data	- not enough space for thread data
00000000898C	000000011FA2 0000004125A2 0	000000011FA2 0000004125A2 0
00000042098C	This application has requested the	This application has requested the
0]Ywho=c	Runtime to terminate it in an unusual	Runtime to terminate it in an unusual
0000000089A7	way.	way.
0000004209A7	000000011FF0 0000004125F0 0	000000011FF0 0000004125F0 0
0 s7gz\:	Please contact the application's	Please contact the application's
0000000089CA	support team for more information.	support team for more information.
0000004209CA	000000012038 000000412638 0	000000012038 000000412638 0
0 TENL	R6009	R6009
0000000089ED	00000001203F 00000041263F 0	00000001203F 00000041263F 0
0000004209ED	- not enough space for environment	- not enough space for environment
0 R"b[b	000000012064 000000412664 0	000000012064 000000412664 0
000000008A05	R6008	R6008
000000420A05	00000001206B 00000041266B 0	00000001206B 00000041266B 0
0 (Tf4X8	- not enough space for arguments	- not enough space for arguments
000000008A2F	000000012090 000000412690 0	000000012090 000000412690 0
000000420A2F	R6002	R6002
0 ls?(,	000000012097 000000412697 0	000000012097 000000412697 0
000000008A4D	- floating point not loaded	- floating point not loaded
000000420A4D	0000000120B8 0000004126B8 0	0000000120B8 0000004126B8 0
0 RA+L'	Microsoft Visual C++ Runtime	Microsoft Visual C++ Runtime
000000008A6F	Library	Library
000000420A6F	0000000120E4 0000004126E4 0	0000000120E4 0000004126E4 0
0 :lJy9M	Runtime Error!	Runtime Error!
000000008AD4	0000000120F4 0000004126F4 0	0000000120F4 0000004126F4 0
000000420AD4	Program:	Program:
0 zYd%Lh	000000012104 000000412704 0	000000012104 000000412704 0
000000008AFB	<program name unknown>	<program name unknown>
000000420AFB	00000001265C 000000412C5C 0	00000001265C 000000412C5C 0
0 [v1r.	GetProcessWindowStation	GetProcessWindowStation
000000008B3C	000000012674 000000412C74 0	000000012674 000000412C74 0
000000420B3C	GetUserObjectInformationA	GetUserObjectInformationA
0 VKCDA	000000012690 000000412C90 0	000000012690 000000412C90 0
000000008BC5	GetLastActivePopup	GetLastActivePopup

000000420BC5	0000000126A4 000000412CA4 0	0000000126A4 000000412CA4 0
0 sN0X!	GetActiveWindow	GetActiveWindow
000000008BDD	0000000126B4 000000412CB4 0	0000000126B4 000000412CB4 0
000000420BDD	MessageBoxA	MessageBoxA
0 <= 286	0000000126C0 000000412CC0 0	0000000126C0 000000412CC0 0
000000008BE5	user32.dll	user32.dll
000000420BE5	000000012704 000000412D04 0	000000012704 000000412D04 0
0 zN-AR	Program:	Program:
000000008C75	000000012710 000000412D10 0	000000012710 000000412D10 0
000000420C75	A buffer overrun has been detected	A buffer overrun has been detected
0 !501<	which has corrupted the program's	which has corrupted the program's
000000008D35	000000012755 000000412D55 0	000000012755 000000412D55 0
000000420D35	internal state. The program cannot	internal state. The program cannot
0 P1s1T	safely continue execution and must	safely continue execution and must
000000008D3F	00000001279C 000000412D9C 0	00000001279C 000000412D9C 0
000000420D3F	now be terminated.	now be terminated.
0 q@!aF'	0000000127B0 000000412DB0 0	0000000127B0 000000412DB0 0
000000008E11	Buffer overrun detected!	Buffer overrun detected!
000000420E11	0000000127D0 000000412DD0 0	0000000127D0 000000412DD0 0
0 :!hIA8	A security error of unknown cause has	A security error of unknown cause has
000000008E18	been detected which has	been detected which has
000000420E18	00000001280E 000000412E0E 0	00000001280E 000000412E0E 0
0 &.<_N*9	corrupted the program's internal state.	corrupted the program's internal state.
000000008E29	The program cannot safely	The program cannot safely
000000420E29	000000012851 000000412E51 0	000000012851 000000412E51 0
0 \,#8Z~#	continue execution and must now be	continue execution and must now be
000000008F08	terminated.	terminated.
000000420F08	000000012884 000000412E84 0	000000012884 000000412E84 0
0 IYZfA	Unknown security failure detected!	Unknown security failure detected!
000000008F18	000000012C04 000000413204 0	000000012C04 000000413204 0
000000420F18	CONIN$	CONIN$
0 Popu*	000000012C0C 00000041320C 0	000000012C0C 00000041320C 0
000000008F20	CONOUT$	CONOUT$
000000420F20	000000013D50 000000414B50 0	000000013D50 000000414B50 0
0 !G81M	(UNKNOWN)	(UNKNOWN)
0000000090BD		
0000004210BD	**File pos Mem pos ID Text**	**File pos Mem pos ID Text**
0 pepE@	======== ======= ==	======== ======= ==
000000009152	====	====
000000421152		
0	000000013D6C 000000414B6C 0	000000013D6C 000000414B6C 0
V)h$\#"upzQZ	sent %d, rcvd %d	sent %d, rcvd %d
00000000918B	000000013D80 000000414B80 0	000000013D80 000000414B80 0
00000042118B	0123456789abcdef	0123456789abcdef
0 p82,!<	000000014D38 000000418738 0	000000014D38 000000418738 0
00000000919E	KERNEL32.dll	KERNEL32.dll
00000042119E	000000014D46 000000418746 0	000000014D46 000000418746 0
0 u"nrY	GetLastError	GetLastError
000000009294	000000014D54 000000418754 0	000000014D54 000000418754 0
000000421294	CloseHandle	CloseHandle
0 (UNK#OW	000000014D61 000000418761 0	000000014D61 000000418761 0
0000000092AA	CreateProcessA	CreateProcessA
0000004212AA	000000014D71 000000418771 0	000000014D71 000000418771 0

0 sent	DuplicateHandle	DuplicateHandle
0000000092B4	000000014D82 000000418782 0	000000014D82 000000418782 0
0000004212B4	GetCurrentProcess	GetCurrentProcess
0 r;cvl	000000014D95 000000418795 0	000000014D95 000000418795 0
0000000092BD	ExitThread	ExitThread
0000004212BD	000000014DA1 0000004187A1 0	000000014DA1 0000004187A1 0
0 12345678	Sleep	Sleep
0000000092C6	000000014DA8 0000004187A8 0	000000014DA8 0000004187A8 0
0000004212C6	ReadFile	ReadFile
0 9abcdef	000000014DB2 0000004187B2 0	000000014DB2 0000004187B2 0
000000009316	PeekNamedPipe	PeekNamedPipe
000000421316	000000014DC1 0000004187C1 0	000000014DC1 0000004187C1 0
0 % @dt	WriteFile	WriteFile
000000009342	000000014DCC 0000004187CC 0	000000014DCC 0000004187CC 0
000000421342	CreatePipe	CreatePipe
0 H$yH8	000000014DD8 0000004187D8 0	000000014DD8 0000004187D8 0
00000000942C	DisconnectNamedPipe	DisconnectNamedPipe
00000042142C	000000014DED 0000004187ED 0	000000014DED 0000004187ED 0
0 GC)P4	TerminateProcess	TerminateProcess
00000000949F	000000014DFF 0000004187FF 0	000000014DFF 0000004187FF 0
00000042149F	WaitForMultipleObjects	WaitForMultipleObjects
0 JetgasCEr	000000014E17 000000418817 0	000000014E17 000000418817 0
0000000094B9	TerminateThread	TerminateThread
0000004214B9	000000014E28 000000418828 0	000000014E28 000000418828 0
0 y}tgP.c	CreateThread	CreateThread
0000000094C6	000000014E36 000000418836 0	000000014E36 000000418836 0
0000004214C6	GetStdHandle	GetStdHandle
0 upliz$3	000000014E44 000000418844 0	000000014E44 000000418844 0
0000000094DD	FreeConsole	FreeConsole
0000004214DD	000000014E51 000000418851 0	000000014E51 000000418851 0
0	WriteConsoleA	WriteConsoleA
Th8md7VBwp	000000014E60 000000418860 0	000000014E60 000000418860 0
0000000094EA	CreateFileA	CreateFileA
0000004214EA	000000014E6D 00000041886D 0	000000014E6D 00000041886D 0
0 3FiYS	GetNumberOfConsoleInputEvents	GetNumberOfConsoleInputEvents
0000000094F6	000000014E8C 00000041888C 0	000000014E8C 00000041888C 0
0000004214F6	PeekConsoleInputA	PeekConsoleInputA
0 ?P p7ZrP	000000014E9F 00000041889F 0	000000014E9F 00000041889F 0
	GetConsoleMode	GetConsoleMode
File pos	000000014EAF 0000004188AF 0	000000014EAF 0000004188AF 0
Mem pos	SetConsoleMode	SetConsoleMode
ID Text	000000014EBF 0000004188BF 0	000000014EBF 0000004188BF 0
========	ReadConsoleInputA	ReadConsoleInputA
=======	000000014ED2 0000004188D2 0	000000014ED2 0000004188D2 0
== ====	GetCurrentProcessId	GetCurrentProcessId
	000000014EE7 0000004188E7 0	000000014EE7 0000004188E7 0
00000000954E	GetCurrentThreadId	GetCurrentThreadId
00000042154E	000000014EFB 0000004188FB 0	000000014EFB 0000004188FB 0
0 3Numb	GetTickCount	GetTickCount
000000009555	000000014F09 000000418909 0	000000014F09 000000418909 0
000000421555	QueryPerformanceCounter	QueryPerformanceCounter
0 Of	000000014F22 000000418922 0	000000014F22 000000418922 0
gIbpuA#vW	LCMapStringW	LCMapStringW

0000000095BB	000000014F30 000000418930 0	000000014F30 000000418930 0
0000004215BB	LCMapStringA	LCMapStringA
0]Exfh	000000014F3E 00000041893E 0	000000014F3E 00000041893E 0
0000000095C7	GetLocaleInfoA	GetLocaleInfoA
0000004215C7	000000014F4E 00000041894E 0	000000014F4E 00000041894E 0
0 Lib}r	InterlockedExchange	InterlockedExchange
0000000095D6	000000014F63 000000418963 0	000000014F63 000000418963 0
0000004215D6	LoadLibraryA	LoadLibraryA
0 QiS6vesdm	000000014F71 000000418971 0	000000014F71 000000418971 0
0000000095E4	VirtualQuery	VirtualQuery
0000004215E4	000000014F7F 00000041897F 0	000000014F7F 00000041897F 0
0 j$q+S e$Ty	GetSystemInfo	GetSystemInfo
0000000095FF	000000014F8E 00000041898E 0	000000014F8E 00000041898E 0
0000004215FF	VirtualProtect	VirtualProtect
0 H]Puo	000000014F9E 00000041899E 0	000000014F9E 00000041899E 0
000000009619	GetStringTypeW	GetStringTypeW
000000421619	000000014FAE 0000004189AE 0	000000014FAE 0000004189AE 0
0 OEMCPUF_	GetStringTypeA	GetStringTypeA
00000000969E	000000014FBE 0000004189BE 0	000000014FBE 0000004189BE 0
00000042169E	HeapSize	HeapSize
0 ALsB	000000014FC8 0000004189C8 0	000000014FC8 0000004189C8 0
0000000096AC	SetStdHandle	SetStdHandle
0000004216AC	000000014FD6 0000004189D6 0	000000014FD6 0000004189D6 0
0 lu(shhxBqf	SetFilePointer	SetFilePointer
0000000096F1	000000014FE6 0000004189E6 0	000000014FE6 0000004189E6 0
0000004216F1	SetEnvironmentVariableA	SetEnvironmentVariableA
0 &etQP"2	000000014FFF 0000004189FF 0	000000014FFF 0000004189FF 0
000000009748	GetOEMCP	GetOEMCP
000000421748	000000015009 000000418A09 0	000000015009 000000418A09 0
0 3do2s	HeapFree	HeapFree
	000000015013 000000418A13 0	000000015013 000000418A13 0
	HeapAlloc	HeapAlloc
	00000001501E 000000418A1E 0	00000001501E 000000418A1E 0
	ExitProcess	ExitProcess
	00000001502B 000000418A2B 0	00000001502B 000000418A2B 0
	GetProcAddress	GetProcAddress
	00000001503B 000000418A3B 0	00000001503B 000000418A3B 0
	GetModuleHandleA	GetModuleHandleA
	000000015053 000000418A53 0	000000015053 000000418A53 0
	GetSystemTimeAsFileTime	GetSystemTimeAsFileTime
	00000001506C 000000418A6C 0	00000001506C 000000418A6C 0
	GetCommandLineA	GetCommandLineA
	00000001507D 000000418A7D 0	00000001507D 000000418A7D 0
	GetVersionExA	GetVersionExA
	00000001508C 000000418A8C 0	00000001508C 000000418A8C 0
	WideCharToMultiByte	WideCharToMultiByte
	0000000150A1 000000418AA1 0	0000000150A1 000000418AA1 0
	SetHandleCount	SetHandleCount
	0000000150B1 000000418AB1 0	0000000150B1 000000418AB1 0
	GetFileType	GetFileType
	0000000150BE 000000418ABE 0	0000000150BE 000000418ABE 0
	GetStartupInfoA	GetStartupInfoA
	0000000150CF 000000418ACF 0	0000000150CF 000000418ACF 0

	HeapDestroy **File pos Mem pos ID Text** ======== ======= == ==== 0000000150DC 000000418ADC 0 HeapCreate 0000000150E8 000000418AE8 0 VirtualFree 0000000150F5 000000418AF5 0 VirtualAlloc 000000015103 000000418B03 0 HeapReAlloc 000000015110 000000418B10 0 IsBadWritePtr 00000001511F 000000418B1F 0 FlushFileBuffers 000000015131 000000418B31 0 RtlUnwind 00000001513C 000000418B3C 0 GetModuleFileNameA 000000015150 000000418B50 0 UnhandledExceptionFilter 00000001516A 000000418B6A 0 FreeEnvironmentStringsA 000000015183 000000418B83 0 GetEnvironmentStrings 00000001519A 000000418B9A 0 FreeEnvironmentStringsW 0000000151B3 000000418BB3 0 GetEnvironmentStringsW 0000000151CB 000000418BCB 0 CompareStringA 0000000151DB 000000418BDB 0 MultiByteToWideChar 0000000151F0 000000418BF0 0 GetCPInfo 0000000151FB 000000418BFB 0 CompareStringW 00000001520B 000000418C0B 0 GetACP 000000015213 000000418C13 0 SetEndOfFile 000000015220 000000418C20 0 WSOCK32.dll 000000011CBC 0000004122BC 0 (null) 000000012B1F 00000041311F 0 j>Wak?Xbl@YcmAZdnB[eoC\fpD]gq	**HeapDestroy** **File pos Mem pos ID Text** ======== ======= == ==== 0000000150DC 000000418ADC 0 HeapCreate 0000000150E8 000000418AE8 0 VirtualFree 0000000150F5 000000418AF5 0 VirtualAlloc 000000015103 000000418B03 0 HeapReAlloc 000000015110 000000418B10 0 IsBadWritePtr 00000001511F 000000418B1F 0 FlushFileBuffers 000000015131 000000418B31 0 RtlUnwind 00000001513C 000000418B3C 0 GetModuleFileNameA 000000015150 000000418B50 0 UnhandledExceptionFilter 00000001516A 000000418B6A 0 FreeEnvironmentStringsA 000000015183 000000418B83 0 GetEnvironmentStrings 00000001519A 000000418B9A 0 FreeEnvironmentStringsW 0000000151B3 000000418BB3 0 GetEnvironmentStringsW 0000000151CB 000000418BCB 0 CompareStringA 0000000151DB 000000418BDB 0 MultiByteToWideChar 0000000151F0 000000418BF0 0 GetCPInfo 0000000151FB 000000418BFB 0 CompareStringW 00000001520B 000000418C0B 0 GetACP 000000015213 000000418C13 0 SetEndOfFile 000000015220 000000418C20 0 WSOCK32.dll 000000011CBC 0000004122BC 0 (null) 000000012B1F 00000041311F 0 j>Wak?Xbl@YcmAZdnB[eoC\fpD]gq

Tabla IV.- Archivo generado por BinText

El Archivo SAK.EXE esta compreso mientras que los archivos UNFSG.EXE y SAK_UN~1.EXE son idénticos.

Se revisará el archivo con un software de Ingeniería Inversa para analizar los comandos que se presentan en este archivo modificado y descompreso de SAK.EXE

4.8.4 Análisis del archivo con IDA PRO

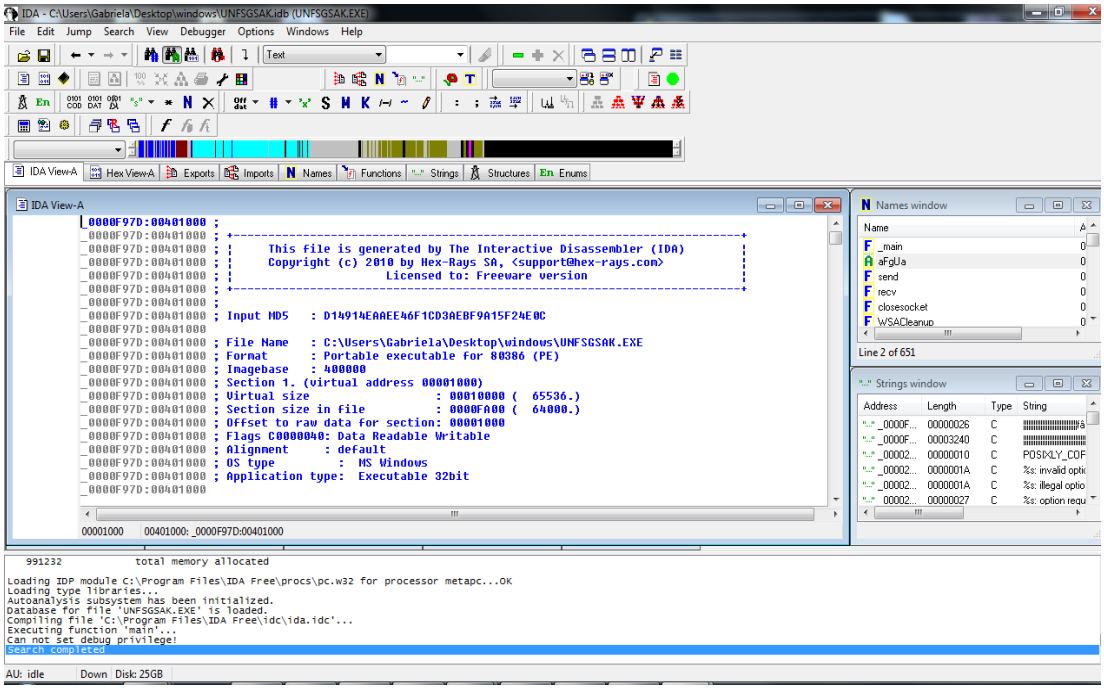


Figura 35.- Análisis con el programa IDA PRO

Con las opciones de buscar, encontramos la línea donde pide una contraseña:

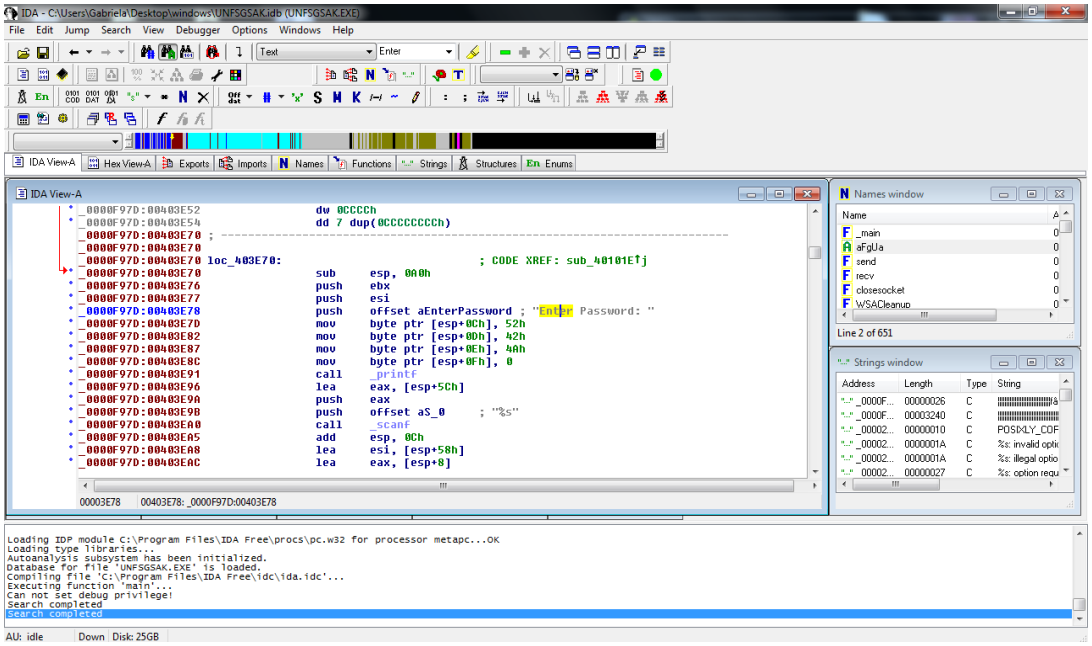


Figura 36.- Password encontrado con el programa IDA

Encontramos el texto seleccionado, que es el valor que se ingresa para acceder a este ejecutable.

4.8.4.1 Expresiones del lenguaje ensamblador

Expresión de MASM	Expresión del depurador	Expresión de C++
BYTE PTR [bx]	BY ebx	*(unsigned char) ebx

Tabla V.- Expresiones del lenguaje ensamblador

ESP: Stack es, en el mejor de los casos, un concepto difícil de entender. Sin embargo, la comprensión de la pila es esencial para ingeniería reversa.

El registro de stack, esp, es básicamente un registro que apunta a una ubicación arbitraria en memoria llamada " stack". Stack es sólo una sección

muy grande de memoria temporal en donde los datos pueden ser almacenados y recuperados. Cuando se llama a una función, un poco de espacio del stack se asigna a la función, y cuando una función devuelve el stack debe estar en el mismo estado en que comenzó.

En esta función conserva los valores para compararlos, dentro del Código ASCII:

52h R
42h B
4Ah J
0

Esta cadena de Valores vendría a ser la que se solicita al ejecutar el archivo.

4.9 Análisis Dinámico

Se ejecuta el archivo SAK.EXE y se ingresa la cadena de valores encontrada en el análisis estático.

RBJ

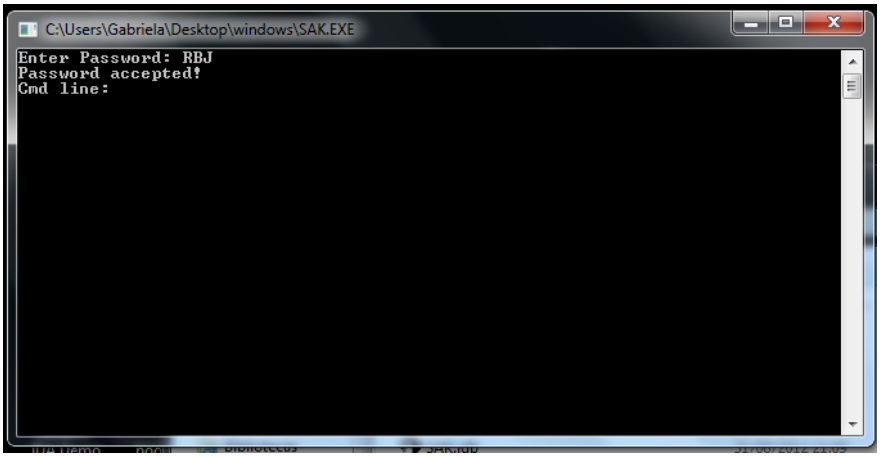


Figura 37.- Ejecución del password encontrado

Si ejecuta el archivo UNFSGSAK.EXE, no se ejecuta debido a que no es un archivo ejecutable. Con la aplicación LORDPE podemos ejecutar este archivo como el fichero en análisis sin que este empaquetado.

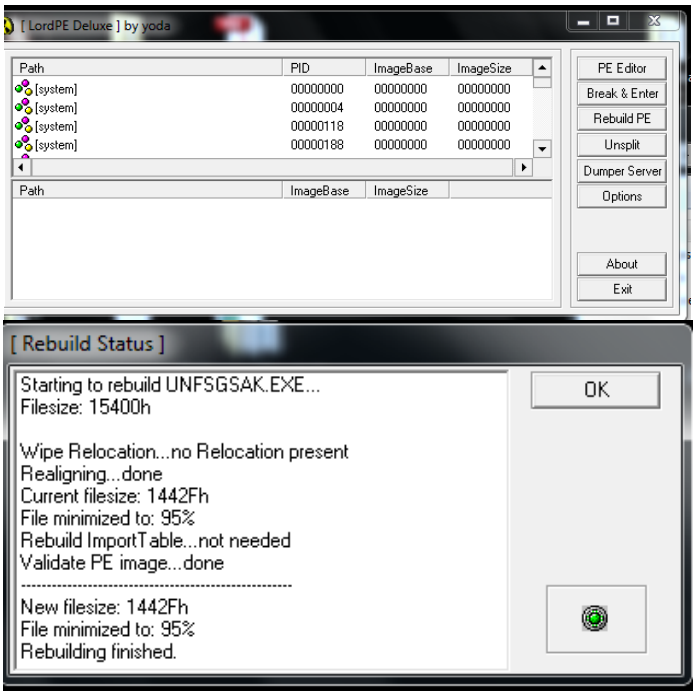


Figura 38.- Análisis con el programa Lordpe

En un principio gracias a la información generada por los enlaces Web que analizaron los archivos, entendimos que puede ser:

- Una modificación de NETCAT.
- Un backdoor clásico para controlar el ordenador infectado

Si ejecutamos las Aplicaciones se puede ingresar comandos disponibles en NETC

CONCLUSIONES

1.- Después de haber realizado el análisis respectivo hemos determinado que el archivo SAK.EXE es un archivo ejecutable y los archivos SAK_OL~1.EXE, SAK_UN~1.EXE, SAK_UN~2.EXE son una variación de este, además al aplicar las herramientas open source (Caine, VirtualBox, StraceNT, Winhex, OllyDbg, Anubi, Procdump, Fsg, Netcat, Unfsg, Virus Total) necesarias rectificamos que se reconoce a los cuatro archivos como un virus caballo de troya Win32: Trojan-gen.

2.-Realizadas las pruebas pertinentes concluimos que el archivo SAK.EXE modifico los registros principales de WINDOWS, además de estar empaquetado con FSG este es un backdoor clásico que controla el ordenador infectado, adicionalmente el archivo ejecutable usa una contraseña para controlar su aplicación y concluimos que el archivo es una versión literalmente modificada de netcat.

3.-Después de haber analizado el archivo **hello.exe** con los dos tipos de análisis, el estático y el dinámico empleando las herramientas necesarias, se pudo determinar que el archivo no presenta ninguna amenaza para los sistemas, sólo contiene una función de usuario principal para poder mostrar el mensaje "HelloWorld!" y luego se detiene.

4.-Se ha intentado destacar la necesidad imperiosa de aplicar metodologías y procedimientos específicos con el fin de poder lograr un mejor análisis además de que podemos disponer de herramientas que nos pueden ayudar en el análisis del ejecutable y así poder encontrar el propósito de este y garantizar la calidad de las evidencias durante todo el proceso forense, haciendo hincapié en la recopilación y custodia de las evidencias.

5.-Terminando el estudio respectivo de este proyecto concluimos que la informática forense debe ser una política de seguridad necesaria en la organización y que la misma debe ser orientada específicamente a encontrar las respuestas a los incidentes informáticos que ocurren de forma anormal, teniendo presente que a medida que evoluciona la tecnología, también evolucionan los métodos de ataque y delitos informáticos de los cuales las empresas están propensas a sufrirlos si no se toma las medidas de seguridad respectivas.

6.-Al termino del proceso investigativo hemos logrado conocer que existe una gran variedad de herramientas de libre distribución y propietarias que están consolidadas en el medio para realizar este tipo de procedimientos, las mismas que mantienen los preceptos forenses y otorgan resultados altamente confiables.

RECOMENDACIONES

En lo referente a la realización del análisis es importante tomar ciertas consideraciones:

1.- Utilizar herramientas de análisis adecuadas puede ayudar a la organización a prevenir futuros ataques, determinar el grado de compromiso, y determinar el número y tipo de intrusos, esto es extremadamente útil durante las fases de limpieza y contención de respuesta a incidentes, también después de identificar el tipo, el nombre y la ubicación de las herramientas, puede escanear la red para otros acontecimientos de la misma herramienta.

2.- Disponer de una correcta gestión de parches y actualizaciones de su hardware y software, ya que gran parte de los ataques se basan en explotar un número reducido de vulnerabilidades en sistemas y aplicaciones.

3.- Formar e informar a sus usuarios para que conozcan, acepten y sean capaces de aplicar las directrices de su política de seguridad. Hacerles ver lo que ha ocurrido en otras organizaciones o entidades, cómo ha afectado un incidente a sus actividades. Informando y formando a los usuarios se reducirá la frecuencia de los incidentes, sobre todo aquellos que impliquen la ejecución de código malicioso, o el saltarse la política de uso adecuado de los sistemas.

4.- Disponer de una base de conocimientos sobre incidentes, basta algo tan sencillo como enlaces a páginas de software antivirus, o empresas y organizaciones especializadas en seguridad informática, así como suscribirse a sus listas e-mail de notificaciones de alertas y vulnerabilidades.

5.- Ejecutar e instalar únicamente aquellos archivos de los que conocemos cabalmente su origen y funcionamiento, va a permitir que se mantenga el equipo de cómputo en condiciones óptimas de rendimiento, nunca ejecutar un archivo o programa sin estar plenamente seguros de su finalidad, o documentarnos previamente para saber de qué se trata.

GLOSARIO DE TERMINOS

Cadena de Custodia: Es el procedimiento de control que se emplea para los indicios materiales afines al delito, desde su ubicación, hasta que son valorados por los diferentes funcionarios encargados de su análisis, normalmente peritos, y que tiene como finalidad no viciar el manejo que de ellos se haga, y así evitar la contaminación, alteración, daños, reemplazos, contaminación o destrucción.

DLL (*dynamic-link library)* Es el término con el que se refiere a los archivos con código ejecutable que se cargan bajo demanda de un programa por parte del sistema operativo. Esta denominación es exclusiva a los sistemas operativos Windows siendo ".dll" la extensión con la que se identifican estos ficheros, aunque el concepto existe en prácticamente todos los sistemas operativos modernos.

Depurador: (*debugger*), Es un programa usado para probar y depurar (eliminar los errores) de otros programas (el programa "objetivo").

Checksum: Es una función hash que tienen como propósito principal detectar cambios accidentales en una secuencia de datos para proteger la integridad de datos, verificando que no haya discrepancias.

Shell: Es el término usado en informática para referirse a un intérprete de comandos, el cual consiste en la interfaz de usuario tradicional de los sistemas operativos basados en Unix y similares como GNU/Linux.

ELF: (*Executable and Linkable Format*) es un formato de archivo para ejecutables, código objeto, bibliotecas compartidas y volcados de memoria. Es el formato ejecutable usado mayoritariamente en los sistemas tipo UNIX como GNU/Linux, BSD, Solaris, Irix.

API: (*Application Programming Interface*) es el conjunto de funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción. Son usadas generalmente en las bibliotecas (también denominadas vulgarmente "librerías").

ASCII: (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange — *Código Estándar Estadounidense para el Intercambio de Información*), es un código de caracteres basado en el alfabeto latino, tal como se usa en inglés moderno y en otras lenguas occidentales. El código ASCII utiliza 7 bits para representar los caracteres

Hash: Es una cadena de letras y números que resulta del cálculo sobre una cadena de origen. La idea es que el algoritmo provea distintas firmas (o hashes MD5) para

distintos orígenes. El cálculo es irreversible y de una sóla vía, es decir que a partir de un hash es muy difícil calcular la cadena original que lo formó a través del algoritmo MD5.

ntdll.dll: Es un módulo que contiene funciones de sistema del NT, es un proceso del sistema necesario para que el sistema funcione correctamente.

Backdoor: En un sistema informático es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema. Aunque estas puertas pueden ser utilizadas para fines maliciosos y espionaje no siempre son un error, pueden haber sido diseñadas con la intención de tener una entrada secreta.

BIBLIOGRAFÍA

(1) HeavenTools Software. (2000). Obtenido de http://www.heaventools.com/overview.htm

(2) Arquillo, J. (Septiembre de 2007). *Herramienta de Apoyo para el Analisis Forense*.

Obtenido de http://books.openlibra.com/pdf/Herramienta-de-Apoyo-para-el-analisis-forense

de-computadoras.pdf

(3) Carrera, E., & Elser, D. (2004). *OllyDbg Plugins*. Obtenido de http://www.openrce.org/downloads/details/108/OllyDump

(4) Casey, E. (2004). *Digital Evidencie and Computer Crime.* Academy Press.

(5) Chenette, S. (2006). *Downloader Analysis*. Obtenido de http://securitylabs.websense.com/content/Blogs/2546.aspx

(6) Cyberec. (2007). *Olly Debugger en Español*. Obtenido de http://olly-dbg.blogspot.com/

(7) Eagle, C. (2011). *The IDA Pro Book.* Canada.

(8) Ferreira, A. (2008). *Programación basica en lenguaje ensamblador*. Obtenido de http://learnassembler.com/binutilesp.html

(9) Jones, D., Alvarez, P., & Harris, M. (s.f.). *md5deep and hashdeep*. Obtenido de http://md5deep.sourceforge.net/

(10) Kolbitsch, C., Lindorfer, M., & Milani, P. (s.f.). *Anubis: Analyizing Unknow Binaries*.

Obtenido de http://anubis.iseclab.org/?action=home

(11) Lithiumly. (2008). *Translated from vietnamese and complied to AdobePDF*. Obtenido

De http://es.scribd.com/doc/29395283/RCE-Unpacking-eBook-Translated-by-LithiumLi Unprotected

(12) Mandia, K., Prosise, C., & Pepe, M. (2003). *Incident Reponse & Computer Forensics,*

Second Edition. Estados Unidos.

(13) Martin. (s.f.). *Welcome to Reverse Engineering with LX*. Obtenido de http://myweb.tiscali.co.uk/reverseengineering/index.html

(14) Microsoft. (2008). *Expresiones del lenguaje ensamblador*. Obtenido de http://msdn.microsoft.com/es-es/library/56638b75(v=vs.80).aspx

(15) Microsoft. (s.f.). *MSDN*. Obtenido de http://msdn.microsoft.com/es es/library/756as972.aspx

(16) Mignolo, a. (2009). *Análisis básico de ejecutables*. Obtenido de http://seguinfo.wordpress.com/2009/01/13/analisis-basico-de-ejecutables/

(17) Radier. (2004). *Manual unpacking FSG 1.0*. Obtenido de http://comcrazy.net76.net/REA/Manual%20unpacking%20FSG%201.0.htm

(18) Rojodos. (2003). *El hacker,net*. Obtenido de http://foro.elhacker.net/tutoriales_documentacion/el_netcat_la_navaja_suiza_de_los_

hacker_y_administradores-t15859.0.html;msg83196

(19) Shihary, N., & Franke, K. (2008). *Computational Forensics.* Springer.

(20) Spears, A. (2007). *Overview of PE file format*. Obtenido de http://in4k.untergrund.net/various%20web%20articles/Iczelion_s_PE_Tutorial_1_Overvie_of_PE_File_Format.htm

(21) *Reverse Engineering*. (2007). Obtenido de http://reversengineering.wordpress.com/hugecollection/rea-unpacking-ebook-by-kienmanowa/

(22) Contreras Vega, G., & Ochoa, C. (2004). Obtenido de http://observatoriodelacapacitacion.stps.gob.mx/oc/PDF/cursos_en_linea/Seguridad_Internet_SE.pdf

(23) Contreras, F. (Abril de 2009). *Monografias.com*. Obtenido de http://www.monografias.com/trabajos74/herramientas-computacion-forense-control-digital/herramientas-computacion-forense-control-digital.shtml

(24) Cruz Allende, D. (2007). Obtenido de http://es.scribd.com/doc/90149118/Fases-y-metodologi%CC%81a-del-ana%CC%81lisis-forense

(25) Fisher, B. (s.f.). *Techniques of Crime Scene Investigation.* ISBN 0-8493-8119-3.

(26) Giacobbi, G. (s.f.). *The GNU Netcat project*. Obtenido de http://netcat.sourceforge.net/

(27) Gomez, A., & Monserrat, F. (Septiembre de 2001). Obtenido de http://www.rediris.es/cert/doc/pdf/hades.pdf

(28) Kruse, W., & Wesly, A. (2002). *Computer Forensic Incident Response*

Essentials.

(29) Lopez, M. (2007). Obtenido de http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

(30) Mandia, K., Prosise, C., & Pepe, M. (2003). *Incident Reponse & Computer Forensics, Second Edition.* Estados Unidos.

(31) Microsoft. (s.f.). *MSDN*. Obtenido de http://support.microsoft.com/kb/177429/es

(32) Sarkisov, E., & Dittrich, D. (2000). Obtenido de http://es.tldp.org/Presentaciones/200211hispalinux/odisho/analisisforense.html

(33) *Virus Total*. (s.f.). Obtenido de https://www.virustotal.com

(34)AVAST. (s.f.). Obtenido de http://www.avast.com/es-ww/index

(35) Gomez Cardenas, R. (s.f.). Obtenido de http://www.cryptomex.org/SlidesForensia/ForensiaMalware.pdf

(36) Jones, R. (2005). *Internet Forensics.* O'Reilly Media, Inc.

(37) Prats, J. (s.f.). *systemadmin.es*. Obtenido de http://systemadmin.es/2011/10/resumen-de-llamadas-al-sistema-con-strace

(38)*RCE Tool Library*. (s.f.). Obtenido de http://www.woodmann.com/collaborative/tools/index.php/LordPE

(39) Gonzalez, J. (Marzo de 2006). Obtenido de http://www.seguridad.unam.mx/eventos/reto/r3_tecnico6.pdf

(40) Silverhack. (2006). *Scribd.* Obtenido de http://www.elhacker.net