# Actividad Extra Distribución Agave.

Sausedo Zarate Mariana-N.L.20

2 de Diciembre de 2015.

## 1. Actividades a realizar:

## 2. Utilizando las herramientas Multihasher (sección "Adquirir - Duplicar - Preservar") y HxD (sección "Utilidades").

a) Descargue una imagen y verifique el hash que le proporciona Multihasher.
b) Cambie alguno de los bytes con HxD y guarde la imagen con un nombre diferente. Verifique nuevamente el hash de la imagen.
c)¿ Es el mismo hash?

No es el mismo hash tiene la misma longitud pero no es el mismo,para verificar que la integridad de una imagen ISO, lo que se hace es comprobar lo que se denomina el hash del archivo descargado, para luego compararlo con el HASH original que le corresponde a la imagen. En caso de no se hayan producido errores de descarga, las dos funciones hash deben coincidir.

d) Como experto forense, ¿ cómo le pueden ayudar éstas herramientas?
El hash es una función algorítmica que permite identificar una entrada, ya sea una imagen ISO, un archivo de texto, una contraseña, etc., mediante un conjunto de caracteres únicos para esa entrada. Existen diferentes algoritmos de

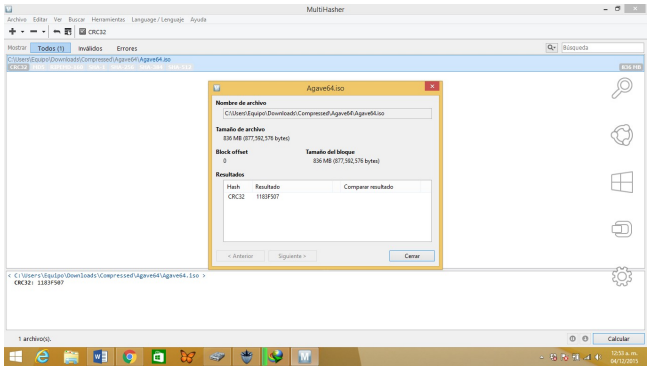


Figura 1: Hash original de ISO.

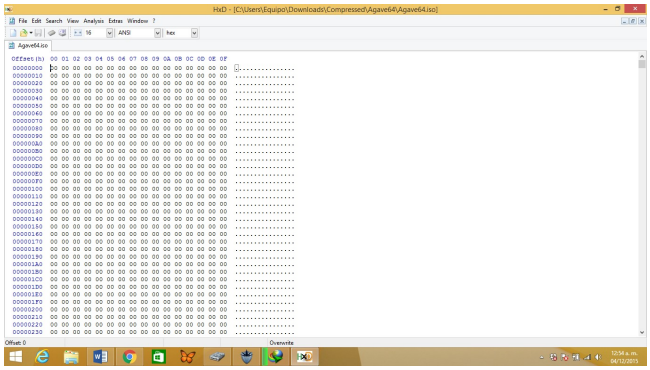

Figura 2: Tabla de bytes original.

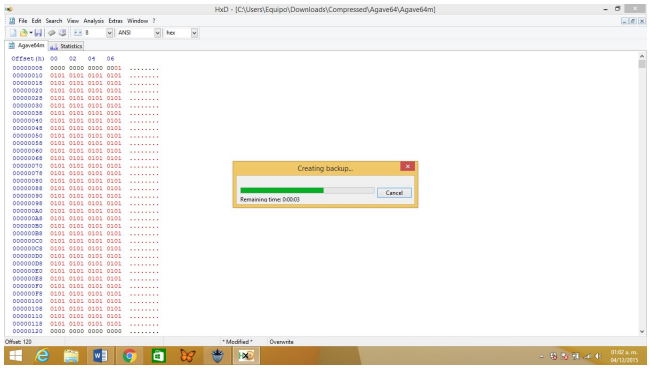

Figura 3: Cambio de bytes de ISO original.

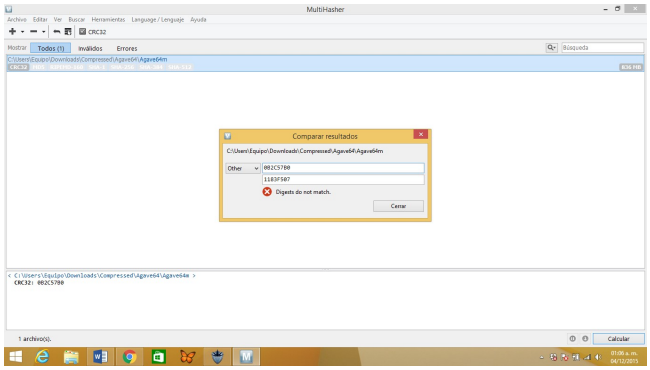

Figura 4: Comparación de HASH con bytes alterados.

funciones hash, pero quizá los más utilizados a nivel práctico sean el MD5 y el SHA-1
El uso de funciones hash está ampliamente extendido en el ámbito de la seguridad informática, ya que es una manera de comprobar la integridad de datos o contraseñas, a la vez que se puede usar como firma digital. Para nuestro caso, nos va a servir para comprobar la integridad de una imagen ISO que nos hayamos descargado.

## 3.En la sección "Analizar Bitácoras", explique la diferencia entre ChromeHistoryView, MozillaHistoryView y MyLastSearch.Como experto forense, ¿ qué beneficios le proporciona utilizar las tres herramientas?

Una bitácora puede registrarmucha información acerca de eventos relacionados con el sistema que la genera los cuales pueden ser:

- Fecha y hora.
- Direcciones IP origen y destino.
- Dirección IP que genera la bitácora.
- Usuarios.
- Errores.

La importancia de las bitácoras es la de recuperar información ante incidentes de seguridad, detección de comportamiento inusual, información para resolver problemas, evidencia legal, es de gran ayuda en las tareas de cómputo forense.
Las Herramientas de análisis de bitácoras mas conocidas son las siguientes:

- Para UNIX, Logcheck, SWATCH.
- Para Windows, LogAgent

Las bitácoras contienen información crítica es por ello que deben ser analizadas, ya que están teniendo mucha relevancia, como evidencia en aspectos legales.
El uso de herramientas automatizadas es de mucha utilidad para el análisis de bitácoras, es importante registrar todas las bitácoras necesarias de todos los sistemas de cómputo para mantener un control de las mismas.

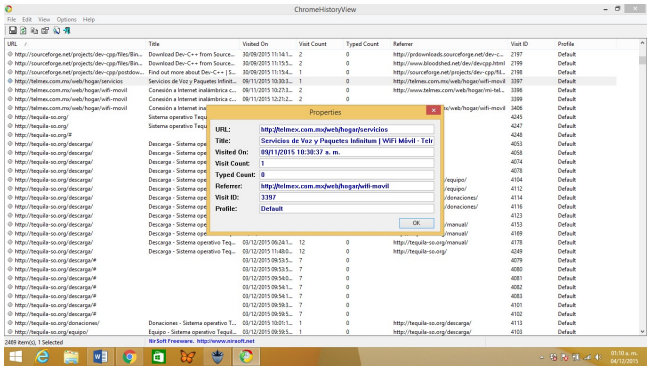

Figura 5: Herramienta ChromeHistoryView.

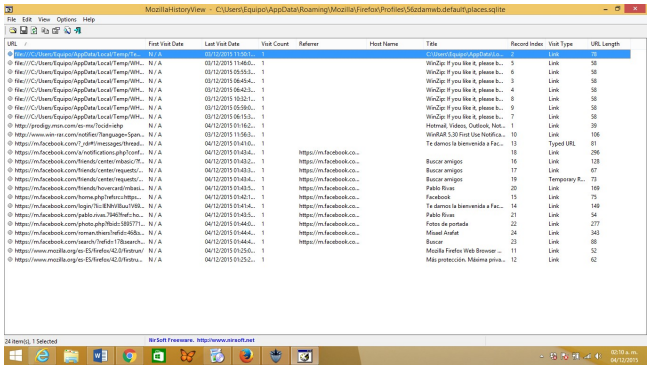

Figura 6: Herramienta MozillaHistoryView.

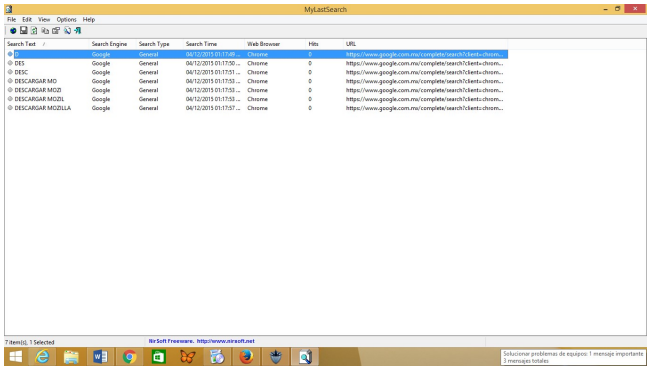

Figura 7: Herramienta MyLastSearch.

## 4.Ejecutar todas las herramientas de la sección "Reconocimiento de Sistema", describiendo que realiza cada una. Como experto forense, seleccione tres de ellas que le permitan describir, cuál fue probablemente el hueco de seguridad que permitió tener acceso al equipo

- Herramienta CurrProcess: Esta herramienta nos indica la fecha de creación ya se de una imagen, documento de texto, etc; también la ejecución de algún software descargado, así como la versión, carpeta donde se encuentra alojado y el número de proceso.

- Herramienta DiskCountersView: Esta herramienta muestra los contadores del sistema de cada unidad de disco en su sistema, incluyendo el número total de operaciones de lectura / escritura y el número total de lectura / escritura bytes. También muestra información de la unidad en general, como el nombre del disco, número de partición, ubicación partición, y así sucesivamente.

- Herramienta DriveLetterView: Esta herramienta es una utilidad simple que permite que usted vea la lista de todas las asignaciones de la letra de impulsión en su sistema, incluyendo impulsiones locales, red alejada conduce, el CD o DVD conduce, y las impulsiones del USB - aunque no se tapan actualmente. También le permite cambiar fácilmente una letra de unidad de los dispositivos USB y acciones remotas de la red, así como para eliminar una letra de unidad del dispositivo USB no está conectado.

- Herramienta LastActivityView: Es una herramienta para el sistema operativo Windows que recopila información de varias fuentes en un sistema en funcionamiento, y muestra un registro de las acciones realizadas por el usuario y los eventos ocurridos en este equipo.

  La actividad desplegada por LastActivityView incluye: Running archivo .exe, apertura abierta de cuadro de diálogo / guardar, archivo / carpeta de apertura desde el Explorador o cualquier otro software, instalación de software, el apagado del sistema / start, aplicación o fallo del sistema, red de conexión / desconexión y más.

  Usted puede exportar esta información en csv archivo html / delimitado por tabuladores / xml / o copiar al portapapeles y luego pegarlo en Excel u otro software.

- Herramienta MyEventView: Es una herramienta de alternativa sencilla para el visor de sucesos estándar de Windows. A diferencia de visor de sucesos de Windows, MyEventViewer le permite ver varios registros de eventos en una lista, así como la descripción del evento y los datos se muestran en la ventana principal, en lugar de abrir una nueva.

  También, con MyEventViewer puede seleccionar fácilmente los artículos múltiples eventos y luego guardarlas en archivos HTML / Texto / XML, o copiarlos al portapapeles (Ctrl + C) y luego pegarlas en Excel.

- Herramienta RecentFilesView: Cada vez que usted abre un archivo desde el Explorador de Windows o desde un estándar abierto de diálogo caja / guardar, el nombre del archivo que abrió es registrada por el sistema operativo. Algunos de los nombres se guardan en la carpeta de 'reciente'. Otros se guardan en el registro.

  Esta utilidad muestra la lista de todos los archivos abiertos recientemente, y le permite borrar las entradas de nombre de archivo deseados. También puede guardar la lista de archivos en texto / html / xml.

- Herramienta USBDeview: Es una pequeña utilidad que lista todos los dispositivos USB que actualmente conectados a su ordenador, así como todos los dispositivos USB que utilizó anteriormente.

  Para cada dispositivo USB, se muestra información ampliada: Nombre del dispositivo / descripción, tipo de dispositivo, número de serie (para dispositivos de almacenamiento masivo), la fecha / hora se añadió ese dispositivo, IdProveedor, ProductID, y mucho más .

  USBDeview también permite des-instalar los dispositivos USB que utilizó anteriormente, dispositivos USB de desconexión que están actualmente conectados a su ordenador, así como deshabilitar y habilitar dispositivos USB.

  También puede utilizar USBDeview en un equipo remoto, siempre y cuando se conecte a la computadora con el usuario ADMIN.

- Herramienta WhatInStartUp: Esta herramienta muestra la lista de todas las aplicaciones que se cargan automáticamente cuando se inicia Windows. Para cada aplicación, se muestra la siguiente información:

  Tipo de inicio (Registro de carpetas / De inicio), la línea de comandos de cuerdas, nombre del producto, versión, nombre de compañía, la ubicación en el sistema de registro o archivo, y más archivos.

  Se le permite deshabilitar fácilmente o eliminar programas no deseados que se ejecutan en su arranque de Windows. Se puede utilizar en su instancia actualmente en ejecución de Windows, así como usted puede utilizarlo en la instancia externa de Windows en otra unidad.

  WhatInStartup también es compatible con una característica especial Ïnhabilitación permanente Si un programa que ha desactivado previamente se sumó de nuevo a la lista de inicio de Windows, WhatInStartup detectará automáticamente el cambio y desactivar de nuevo.

- Herramienta WinAudit: Esta herramienta puede hacer una auditoría completa de tu ordenador, exportando a un archivo cada aspecto de su configuración.

  Genera una consulta general de cada rincón de nuestro ordenador, desde información tan simple como qué sistema operativo usamos hasta parámetros de seguridad y detalles sobre el hardware. No importa qué plataforma Windows se posea o qué tan antiguo sea el ordenador, WinAudit puede saber qué es lo que tiene, y salvarlo.

  WinAudit realiza un sumario muy amplio, el cual puede exportarse bajo diferentes formatos. Entre las opciones más interesantes, la información

puede guardarse en formato HTML, o incluso exportarse a un documento PDF.

- Herramienta WinLister: Esta utilidad muestra la lista de las ventanas abiertas en el sistema. Para cada ventana, se muestra información útil: el título, la manija de la ventana, la ubicación, tamaño, nombre de la clase, número de proceso, el nombre del programa que creó la ventana, y más .

  Además, se puede fácilmente ocultar, mostrar o cerrar las ventanas seleccionadas, o guardar la lista de ventanas en el texto o archivo HTML.

# 4. De la sección "Redes", ¿ en qué le puede ayudar la herramienta CurrPorts.

CurrPorts realiza un exhaustivo análisis de tu sistema, mostrando posteriormente en su interfaz una detallada lista con todos los puertos que están activos en ese momento.

Puedes seleccionar exactamente los datos que quieres visualizar, a elegir de elementos tales como dirección del puerto, nombre del puerto, nombre del proceso, ruta completa, dirección IP local, estado del puerto, usuario, etc.

La herramienta te permite seleccionar un puerto o un proceso concreto y cerrarlos, así como generar un informe en HTML a partir de los datos obtenidos en el análisis.

# 5. De la sección Utilidades:

- a)¿ Cuál será el propósito de tener un Command Prompt como parte de las herramientas proporcionadas por Agave?

  Como sabes un símbolo del sistema es un punto de entrada para las órdenes de ordenador en la ventana del símbolo del sistema. Al escribir comandos en el símbolo del sistema, puede realizar tareas en el ordenador sin necesidad de utilizar la interfaz gráfica de Windows.

  Tener uno propio que es la posibilidad que nos brinda Agave, es de mucha utilidad ya que sólo tú tendrás ese "permiso",para realizar tareas sobre tu sistema.

- b) Utilice la herramienta index.dat Viewer ¿Qué información almacena el archivo index.dat ? ¿ en qué sistemas operativos se utiliza este archivo?

  El archivo index.dat es un archivo de datos. Es un repositorio de información como URLs, búsquedas y archivos abiertos recientemente. Su propósito es el de permitir rápido acceso a los datos usados por Internet Explorer. Por ejemplo, cada dirección de Internet visitada es archivada en este archivo, permitiendo a Internet Explorer autocompletar rápidamente mientras el usuario tipea la dirección web. El archivo index.dat es específico del usuario y es abierto mientras el usuario está registrado. Existen archivos separados para historial de Internet Explorer, cache y cookies.

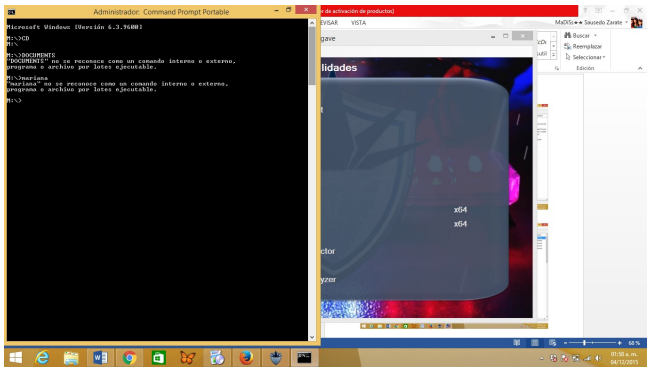


Figura 8: Herramienta Command Prompt.

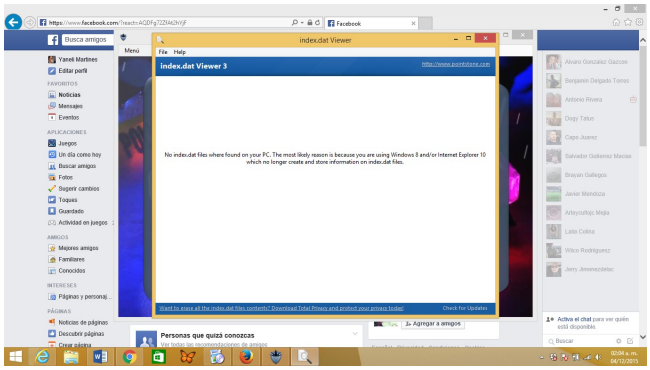


Figura 9: Herramienta IndEX.dat.

El archivo index.dat nunca es removido o redimensionado. Un archivo index.dat demasiado grande puede perjudicar el rendimiento.

Nota: La extensión .dat es generalmente usada para archivos de datos (archivos que no son legibles por humanos). Es posible encontrar archivos 'index.dat' que no son usados por Internet Explorer.En mi caso no pude ejecutar la herramienta.

- c) ¿ Qué utilidad tiene la herramienta USB WriteProtector?

  USB Write Protector es una herramienta de muy fácil uso que permite activar o desactivar la protección contra escritura de todos los dispositivos de almacenamiento USB que se conectan al ordenador. Una vez que se activa la protección, no será posible transferir datos a los dispositivos USB.la protección.

  Su uso es muy sencillo, solo es necesario ejecutar el programa y elegir entre ON y OFF para activar o desactivar la protección.

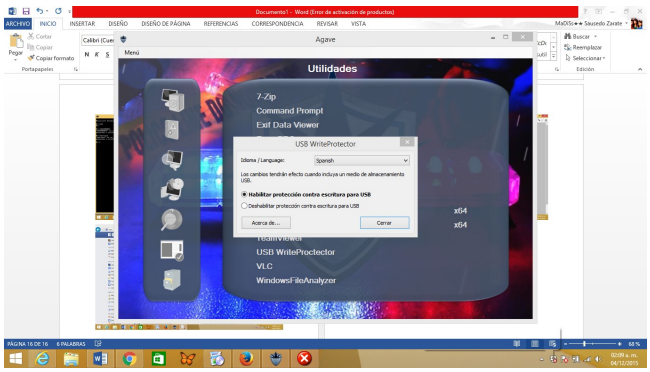


Figura 10: Herramienta USB Write.

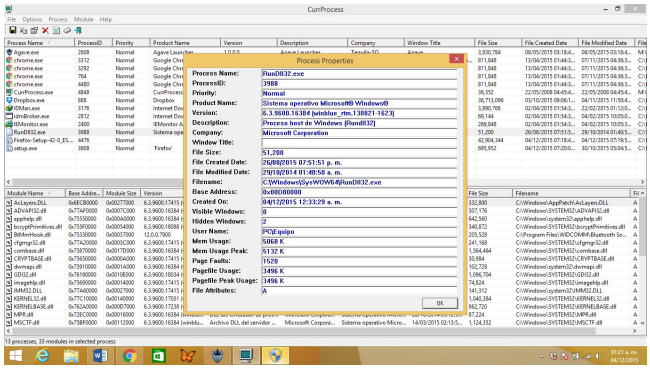


Figura 11: Herramienta CurrProcess.

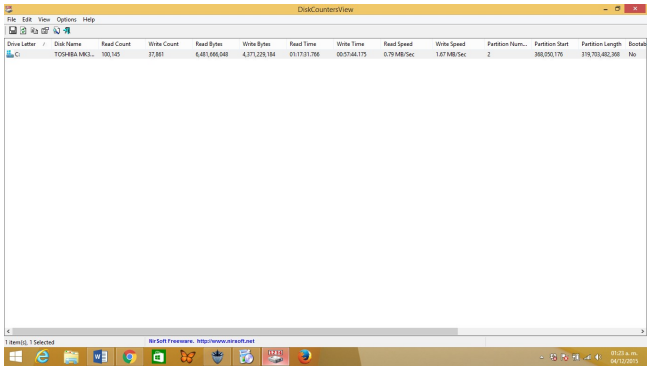


Figura 12: Herramienta DiskCountersView.

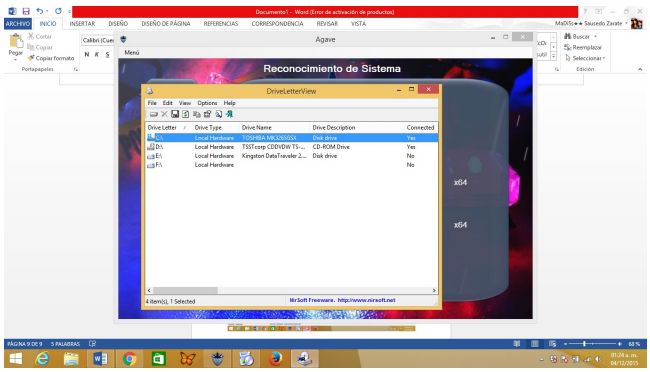


Figura 13: Herramienta DriveLetterView.

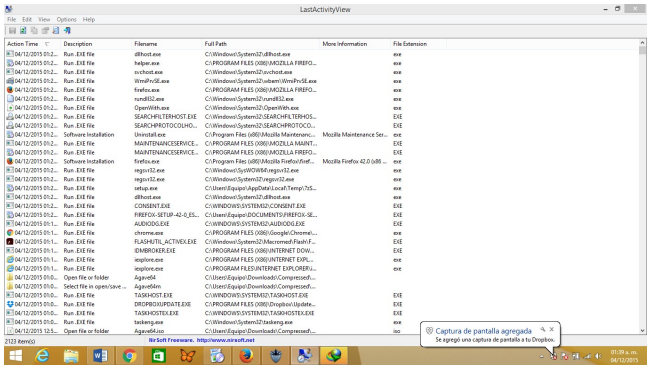


Figura 14: Herramienta LastActivityView.

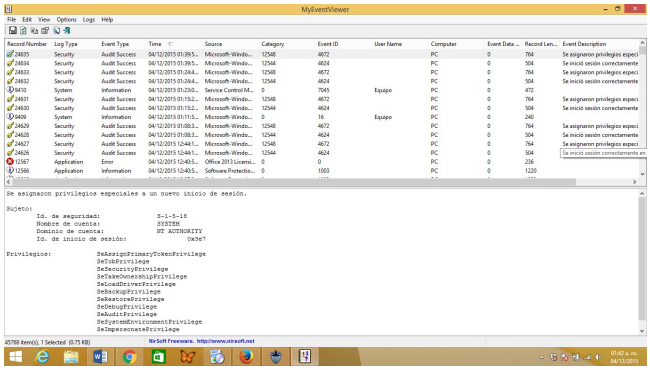


Figura 15: Herramienta MyEventViewer.

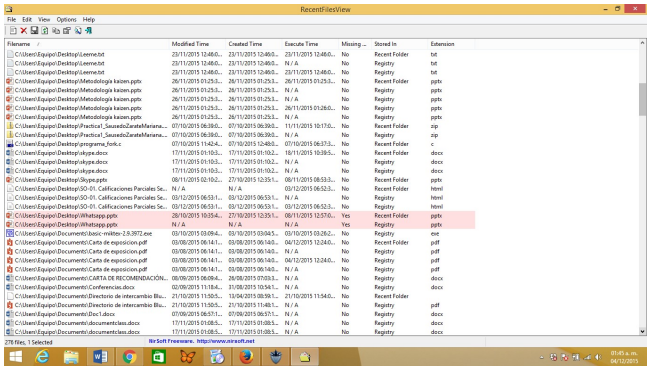

Figura 16: Herramienta RecentFilesView.

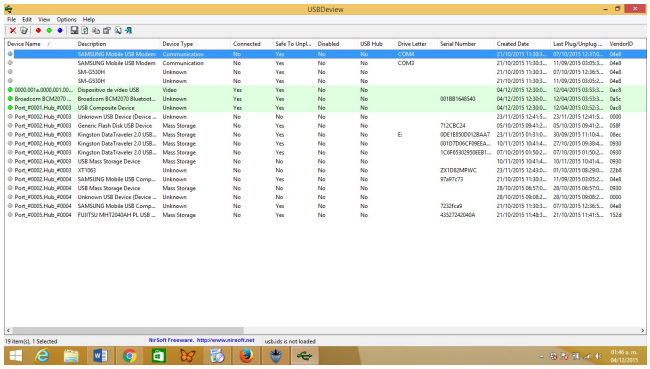

Figura 17: Herramienta USBDeview.

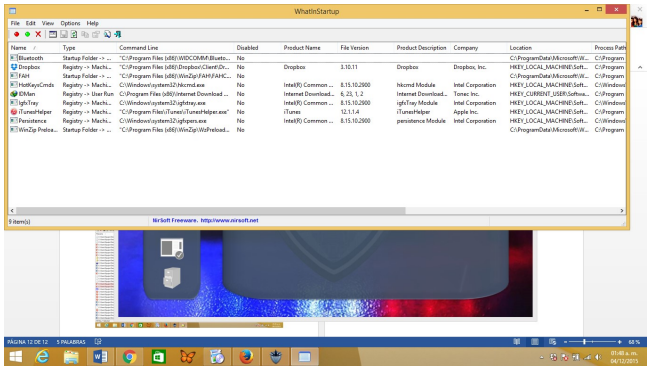

Figura 18: Herramienta WhatInStartUp.

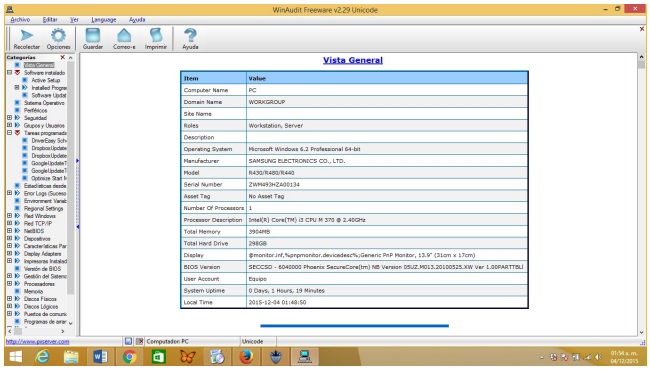


Figura 19: Herramienta WinAudit.

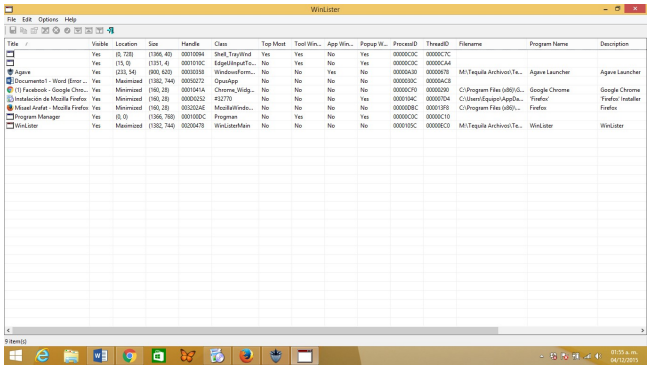


Figura 20: Herramienta WinLister.

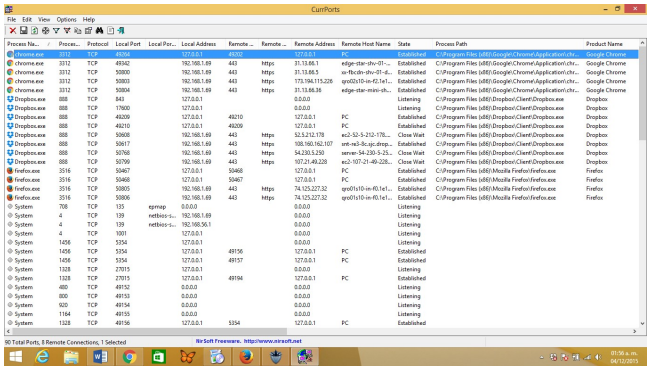


Figura 21: Herramienta CurrPorts.

# 2. Bibliografía


- Available at: http://tequila-so.org/descarga/ [Accessed 1 de Diciembre 2015]
- Available at: http://www.nirsoft.net/ [Accessed 2 de Diciembre 2015]
- Available at: http://proporcionasoporte.blogspot.es/ [Accessed 2 Diciembre 2015].
- Available at: http://es.ccm.net/download/descargar-29479-usb-write-protector [Accessed 2 Diciembre 2015].