Universidad Luterana Salvadoreña

Análisis de Sistema 2017

Catedrático: José Luis Alvarado Aguilar

Instalación y uso de bulk_extractor

Integrantes: Xavier Edenilson Hernández Lovos

Denis Emerson Zamora

INTRODUCCIÓN

El aumento progresivo de la tecnología, en lo referente a equipos informáticos y de telecomunicaciones con acceso a Internet, ha traído como consecuencia que se incremente de manera significativa los incidentes de seguridad informática. Aquí es donde entra a jugar un papel importante la informática forense, la cual se enfoca en a búsqueda de posibles autores de delitos informáticos. La informática forense aplica una serie de técnicas y métodos de investigación que permiten reconstruir, lo más fielmente posible, la secuencia de eventos que tuvieron lugar en uno o en varios equipos informáticos, o en toda una plataforma tecnológica, para la ejecución exitosa de un incidente de seguridad informático.

Este trabajo se centraliza en la instalación, demostración, uso e importancia de bulk_extractor como herramienta de informática forense. Mediante el cual se analizan y extrae información de dispositivos electrónicos como computadoras, Smartphone, discos duros etc. que estén involucrados en un delito informático

JUSTIFICACIÓN

El análisis informático forense es un área de la seguridad informática que evoluciona en forma constante con los avances tecnológicos y en paralelo con el perfeccionamiento de los ataques informáticos. Es un área que se apoya sustancialmente en el software para el cumplimiento de sus objetivos, para lo cual existe una amplia gama de aplicativos que permiten investigar un incidente desde muchas perspectivas.

A través del presente trabajo se tratará de presentar de la forma más objetiva, clara, detallada la efectividad y aplicabilidad de una de las herramientas de software más representativas del mercado encaminadas a la investigación informática forense bulk_extractor

OBJETIVO GENERAL

•Conocer el funcionamiento del software bulk_extractor y cuáles son sus aportes a la informática forense.

OBJETIVOS ESPECÍFICOS

•Mostrar como instalar el software de informática forense bulk_extractor

•Identificar las ventajas y desventajas que ofrece bulk_extractor

•Realizar pruebas con la utilización del software de informática forense

ANTECEDENTES

El campo de la informática forense se inició en la década de 1980, poco después de que las computadoras personales se convirtieran en una opción viable para los consumidores. En 1984, fue creado un programa del FBI. Conocido por un tiempo como el Programa de Medios Magnéticos, que ahora se conoce como CART (CART, del inglés computer analysis and response team), o análisis de informática y equipo de respuesta. Poco después, el hombre al que se le atribuye ser el "padre de la informática forense", comenzó a trabajar en este campo. Su nombre era Michael Anderson, y era un agente especial de la División de Investigación Criminal del IRS. Anderson trabajó para el gobierno en esta capacidad hasta mediados de 1990, tras lo cual fundó New Technologies, Inc., un equipo que lleva la firma forense.

En las próximas décadas, e incluso hoy en día, esta área ha tenido una gran expansión. La policía y las fuerzas militares siguen marcando una fuerte presencia en las áreas de seguridad de la información y la informática forense.

Más recientemente, el sector privado ha analizado la necesidad de realizar investigaciones forenses en las disputas legales de carácter civil. El campo de la informática forense continúa creciendo diariamente. Cada vez más investigadores privados en investigación informática forense y privados son cada vez un nivel más amplio de conocimientos en este campo.

Las compañías de software continúan produciendo programas forenses nuevos y más robusto de software, y el nivel de las fuerzas de la ley y la policía, existe una búsqueda continua para identificar y capacitar a aumentar su plantilla en respuesta a los delitos relacionados con la tecnología.

¿Qué es bulk_extractor?

Es una herramienta informática forense que escanea una imagen de disco, un archivo o un directorio de archivos y extrae información útil sin analizar el sistema de archivos ni las estructuras del sistema de archivos. Los resultados se pueden inspeccionar, analizar o procesar fácilmente con herramientas automatizadas. bulk_extractor también crea un histograma de las características que encuentra, ya que las características que son más comunes tienden a ser más importantes. El programa se puede usar para aplicaciones de aplicación de la ley, defensa, inteligencia e investigación cibernética.

¿Cómo funciona?

bulk_extractor se distingue de otras herramientas forenses por su velocidad y minuciosidad. Debido a que ignora la estructura del sistema de archivos, bulk_extractor puede procesar diferentes partes del disco en paralelo. En la práctica, el programa divide el disco en páginas de 16MiByte y procesa una página en cada núcleo disponible. Esto significa que las máquinas de 24 núcleos procesan un disco aproximadamente 24 veces más rápido que una máquina de 1 núcleo. bulk_extractor también es minucioso. Esto se debe a que bulk_extractor automáticamente detecta, descomprime y vuelve a procesar recursivamente los datos comprimidos que se comprimen con una variedad de algoritmos. Nuestras pruebas han demostrado que existe una cantidad significativa de datos comprimidos en las regiones no asignadas de los sistemas de archivos que se pasan por alto por la mayoría de las herramientas forenses que comúnmente se usan hoy en día.

Otra ventaja de ignorar los sistemas de archivos es que bulk_extractor se puede usar para procesar cualquier medio digital. Hemos utilizado el programa para procesar discos duros, SSD, medios ópticos, tarjetas de cámara, teléfonos celulares, volcados de paquetes de red y otros tipos de información digital

Archivos de características de salida

bulk_extractor ahora crea un directorio de salida que incluye:

- **ccn.txt:** Números de tarjeta de crédito
- **ccn_track2.txt:** Información de la "pista 2" de la tarjeta de crédito
- **domain.txt:** dominios de Internet que se encuentran en la unidad de disco, incluidas las direcciones de punto y coma encontradas en el texto.
- **email.txt:** Direcciones de correo electrónico
- **ether.txt:** Direcciones MAC de Ethernet encontradas a través del paquete de IP tallado de archivos de intercambio y archivos de hibernación del sistema comprimido y fragmentos de archivo.
- **exif.txt:** EXIFs de JPEG y segmentos de video. Este archivo de características contiene todos los campos EXIF, expandidos como registros XML.
- **find.txt:** Los resultados de las solicitudes de búsqueda de expresiones regulares específicas.
- **ip.txt:** Direcciones IP encontradas a través del tallado de paquetes IP.
- **telephone.txt:** Números de teléfono de EE. UU. e internacionales.
- **url.txt :** Url que generalmente se encuentran en cachés del navegador, mensajes de correo electrónico y pre compilados en ejecutables.
- **url_searches.txt:** Un histograma de términos utilizados en las búsquedas en Internet de servicios como Google, Bing, Yahoo y otros.
- **wordlist.txt:** una lista de todas las "palabras" extraídas del disco, útiles para el descifrado de contraseñas.
- **lista de palabras** _ ***.** : La lista de palabras con duplicados eliminados, formateados en una forma que se puede importar fácilmente a un popular programa de descifrado de contraseñas.
- **zip.txt:** Un archivo que contiene información sobre cada componente de archivo ZIP encontrado en los medios. Esto es excepcionalmente útil ya que los archivos ZIP contienen una estructura interna y ZIP es cada vez más el formato de archivo compuesto de elección para una variedad de productos como Microsoft Office.

Para cada uno de los anteriores, se pueden crear dos archivos adicionales:

- _**stopped.txt:** bulk_extractor admite una lista de detención, o una lista de elementos que no es necesario señalar a la atención del usuario. Sin embargo, en lugar de simplemente suprimir esta información, que podría causar la ocultación de algo crítico, las entradas detenidas se almacenan en los archivos detenidos.
- _**histogram.txt:** bulk_extractor también puede crear histogramas de características. Esto es importante, ya que la experiencia ha demostrado que las direcciones de correo electrónico, los nombres de dominio, las URL y otra información que aparece con mayor frecuencia en un disco duro o en la memoria de un teléfono celular se pueden usar para crear rápidamente un patrón de informe de vida.

El extractor masivo también crea un archivo que captura la procedencia de la ejecución:

- **report.xml:** Un informe XML forense digital que incluye información sobre los medios de origen, cómo se compiló y ejecutó el programa bulk_extractor, el tiempo para procesar la evidencia digital y un meta informe de la información que se encontró.

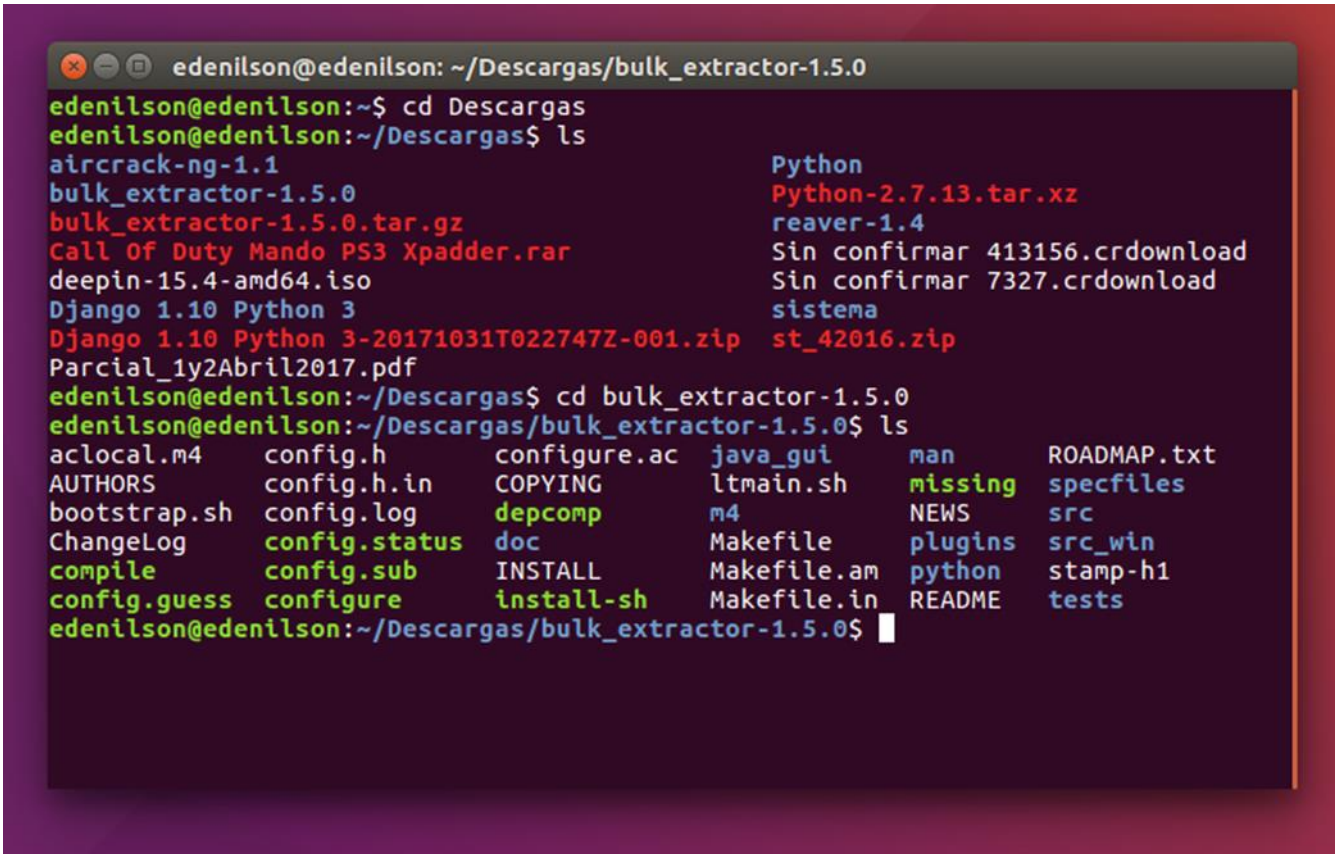
INSTALACIÓN DE BULK_EXTRACTOR EN DEBÍAN Y UBUNTU

1- Descargue el último archivo bulk_extractor.tar.gz desde:

http://downloads.digitalcorpora.org/downloads/bulk_extractor/

2-Descomprimir el archivo en la carpeta descargas

3-Entramos a la terminal del sistema, nos dirigimos a la carpeta descarga y luego a la raíz del software



3-Instalamos Bulk_extractor con los siguientes comandos:

•./configure

•make

•sudo make install

```
edenilson@edenilson: ~/Descargas/bulk_extractor-1.5.0
edenilson@edenilson:~/Descargas/bulk_extractor-1.5.0$ ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether to enable maintainer-specific portions of Makefiles... no
checking for prefix by checking for bulk_extractor... /usr/local/bin/bulk_extrac
tor
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking for g++... g++
checking whether we are using the GNU C++ compiler... yes
```

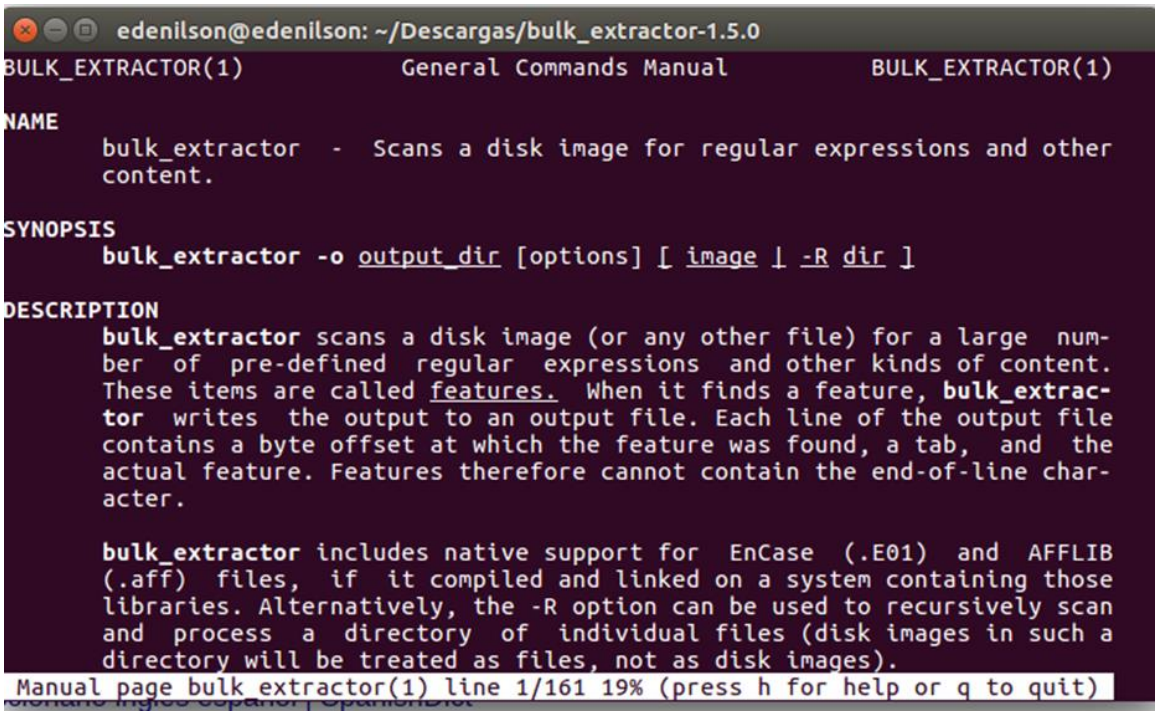
Y listo bulk_extractor fue instalado con éxito

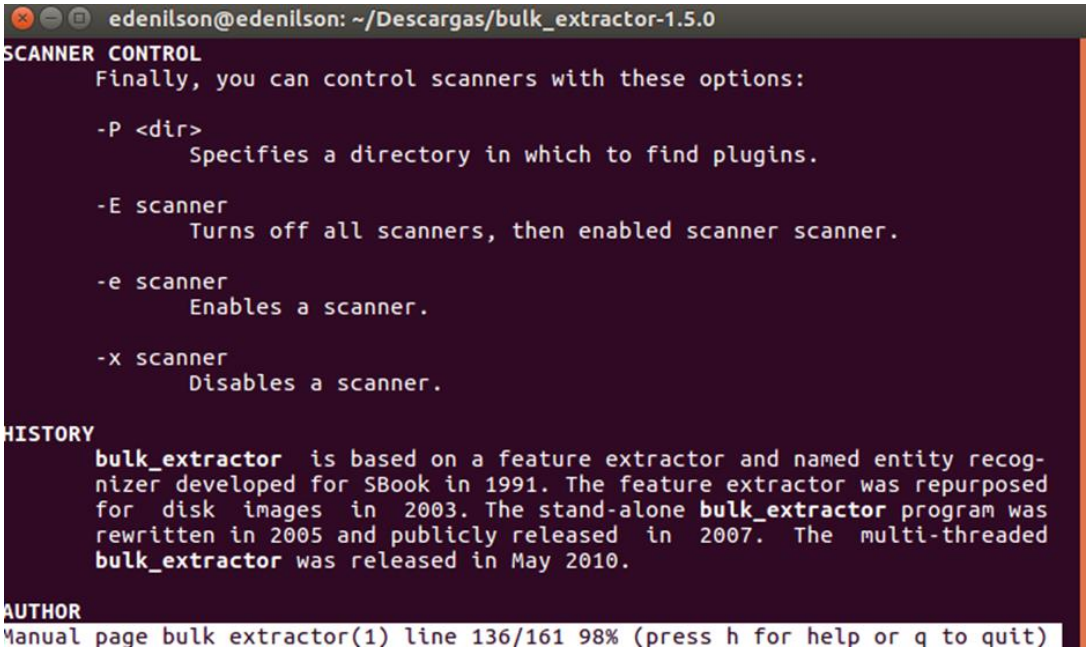
```
edenilson@edenilson: ~/Descargas/bulk_extractor-1.5.0
BULK_EXTRACTOR(1)           General Commands Manual          BULK_EXTRACTOR(1)

NAME
       bulk_extractor  -  Scans a disk image for regular expressions and other
       content.

SYNOPSIS
       bulk_extractor -o output_dir [options] [ image | -R dir ]

DESCRIPTION
       bulk_extractor scans a disk image (or any other file) for a large  num-
       ber  of  pre-defined  regular  expressions  and other kinds of content.
       These items are called features.  When it finds a feature, bulk_extrac-
       tor  writes  the output to an output file. Each line of the output file
       contains a byte offset at which the feature was found, a tab,  and  the
       actual feature. Features therefore cannot contain the end-of-line char-
       acter.

       bulk_extractor includes native support for  EnCase  (.E01)  and  AFFLIB
       (.aff)  files,  if  it compiled and linked on a system containing those
       libraries. Alternatively, the -R option can be used to recursively scan
       and  process  a  directory  of  individual files (disk images in such a
       directory will be treated as files, not as disk images).
 Manual page bulk_extractor(1) line 1/161 19% (press h for help or q to quit)
```

EJEMPLO DEL USO DE LA HERRAMIENTA BULK_EXTRACTOR

1- Desde la raíz de bulk_extractor entramos a la herramienta para extraer toda la información del disco duro con el comando: **man bulk_extractor**

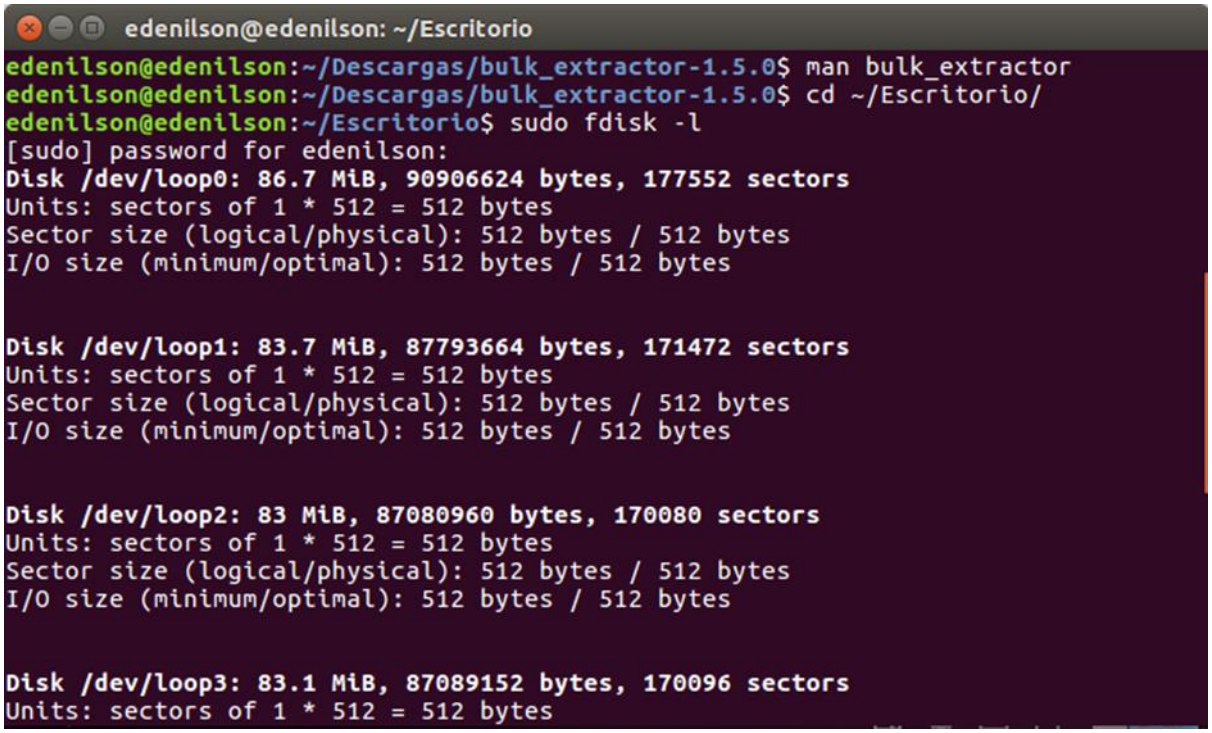
La herramienta nos brinda una descripción de los procesos que podemos realizar y un manual general de comandos

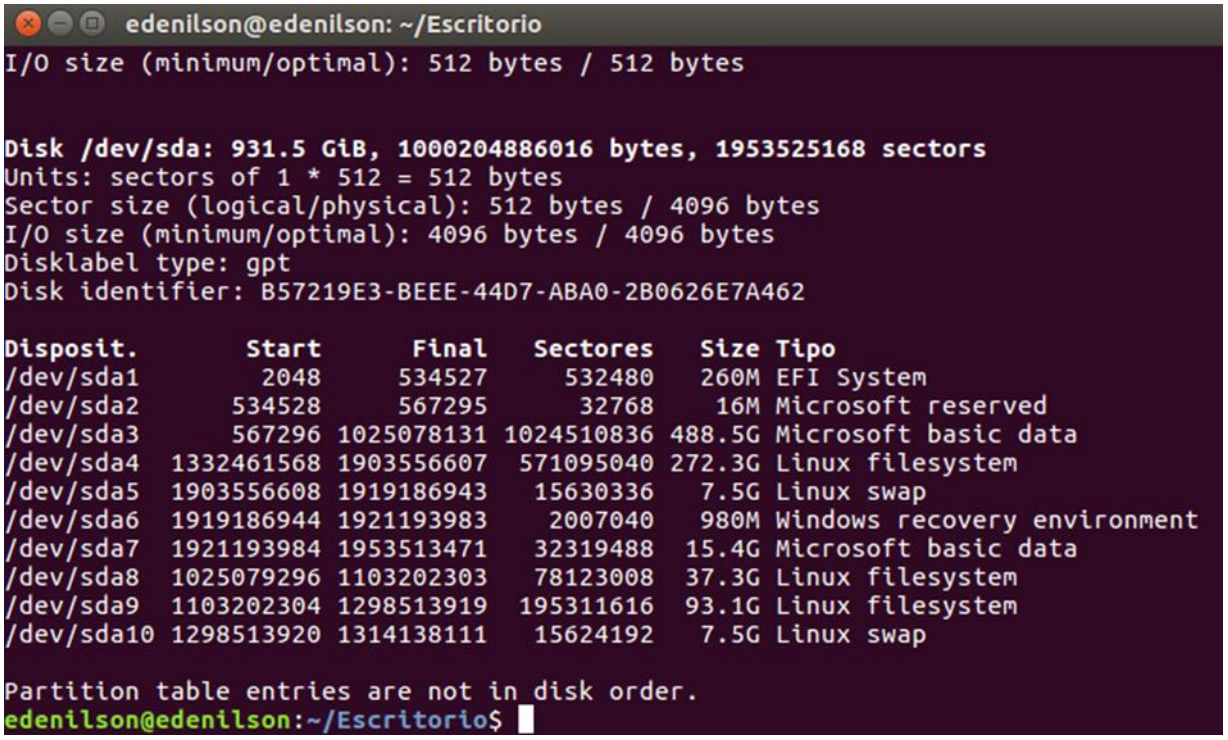




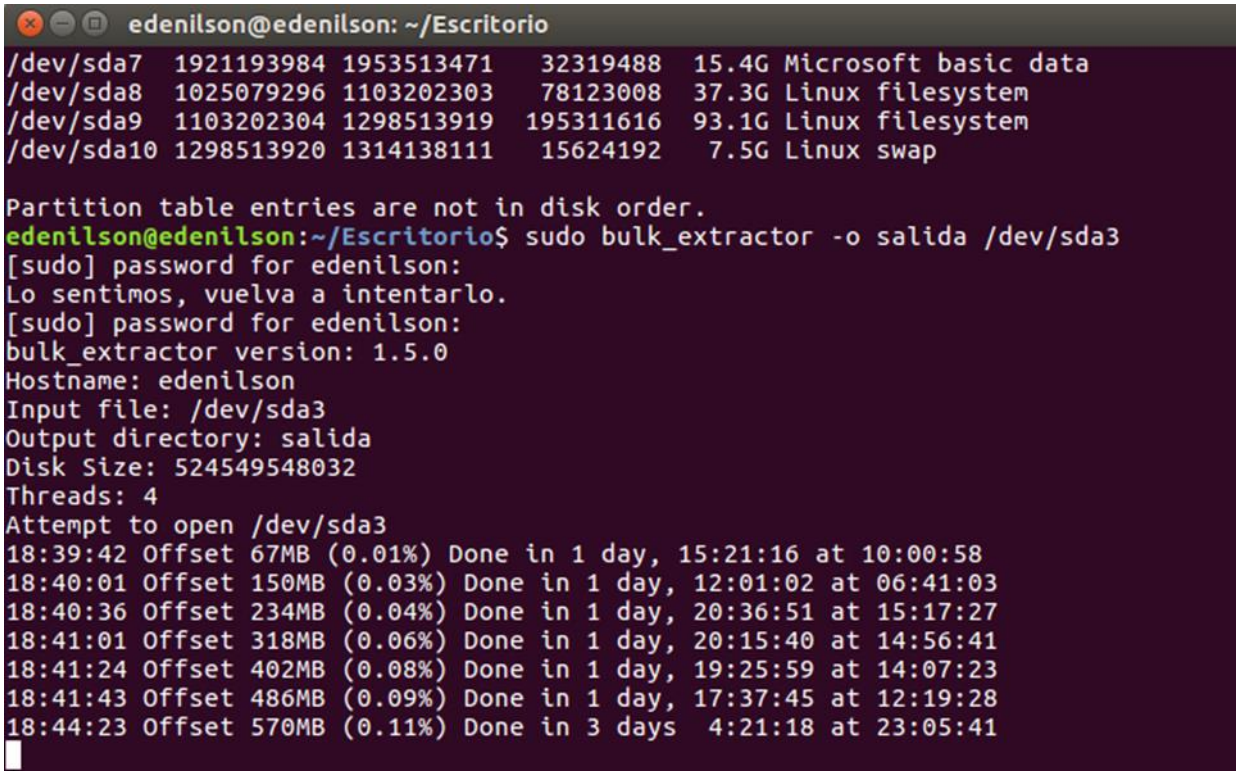
2- Luego de inspeccionar las opciones de la herramienta presionamos **Q** para salir. Nos dirigimos al directorio de salida donde queremos que se cree la carpeta que muestre los resultados del análisis del disco duro, elegimos en el escritorio **~/Escritorio/**

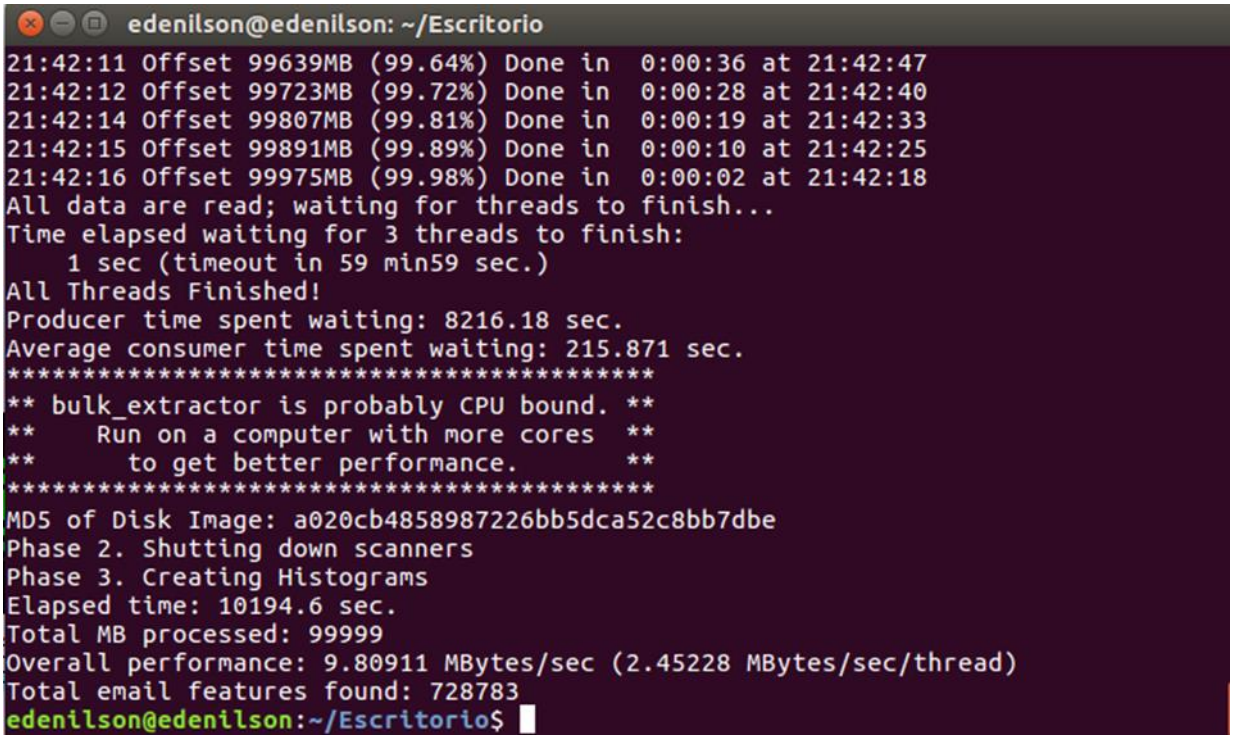
Después examinamos las particiones que tiene el equipo con el comando **sudo fdisk –l**



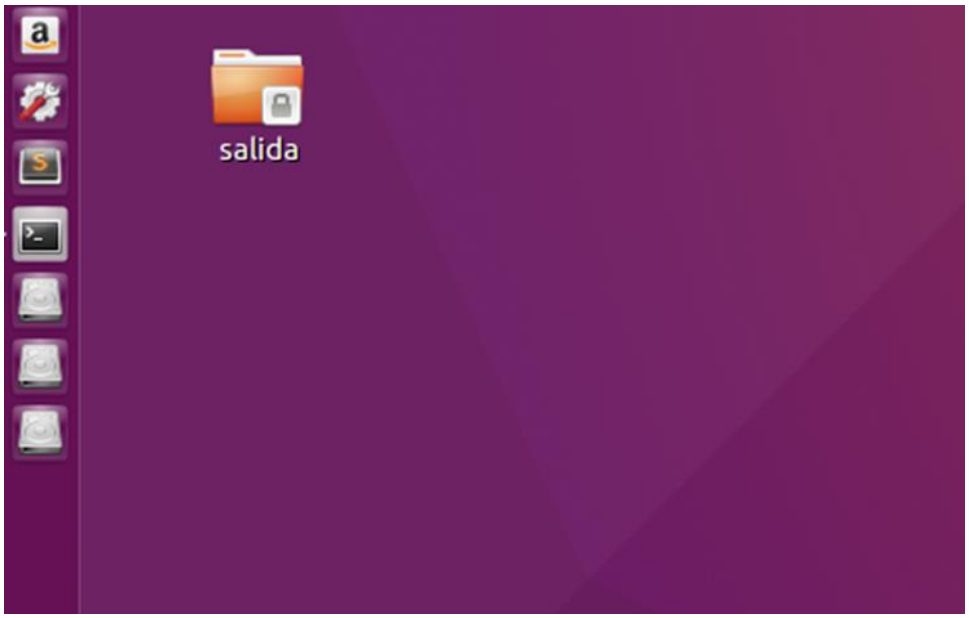


3-Después de escoger cual partición quiere extraer la información, Digitamos el comando: **sudo bulk_extractor -o salida /dev/sda9/** y comenzara el proceso de extracción de la información

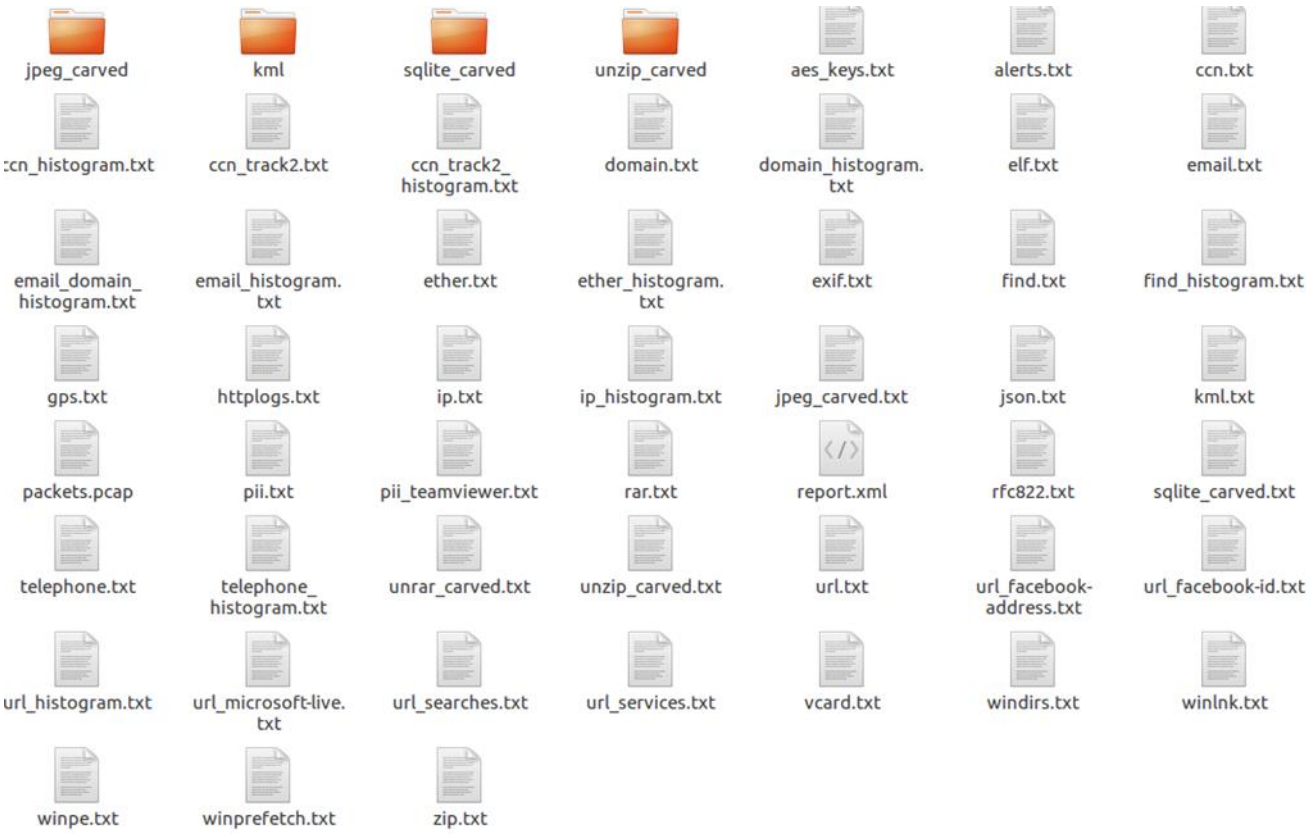




4- Al finalizar se crea la carpeta **SALIDA** en el escritorio mostrando el resultado de toda la información extraída del disco duro analizado.



Entramos a la carpeta y podemos observar todos los datos obtenidos del disco duro analizado



CONCLUSIÓN

El programa se puede usar para aplicaciones de aplicación de la ley, defensa, inteligencia e investigación cibernética. Mediante el cual se analizan y extrae información de dispositivos electrónicos como computadoras, Smartphone, discos duros etc. que estén involucrados en un delito informático.

BIBLIOGRAFÍA

http://www.forensicswiki.org/wiki/Bulk_extractor

https://www.youtube.com/watch?v=QVfYOvhrugg

http://simson.net/ref/2012/2012-08-08%20bulk_extractor%20Tutorial.pdf