GESTIÓN DE EVIDENCIA DIGITAL EN ESCENARIOS CONVENCIONALES E IOT

Tiffany Estupiñan Londoño, Karen Mora Merchán

Programa de Ingeniería de Sistemas

Escuela Colombiana de Ingeniería Julio Garavito

Director:

Msc. Claudia Santiago Cely

Proyecto de Grado

2018-2 / 2019-1

Tabla de contenido

1 RESUMEN 6

2 PLANTEAMIENTO DEL PROBLEMA 6

2.1 **DEFINICIÓN DEL PROYECTO** 6

2.2 **DESCRIPCIÓN DEL PROBLEMA** 6

3 JUSTIFICACIÓN 6

4 OBJETIVOS 7

4.1 Objetivo General 7

4.2 Objetivos Específicos 7

5 MARCO TEÒRICO 7

5.1 Informática Forense 8

5.1.1 Usos de la Informática Forense 9

5.2 Evidencia Digital 10

5.2.1 Clasificación de la evidencia digital 10

5.2.2 Criterios de admisibilidad de la evidencia digital 10

5.2.3 Manipulación de la evidencia digital 11

5.3 Definiciones 11

5.3.1 Datos 11

5.3.2 Datos Volátiles 11

5.3.3 Datos No Volátiles 11

5.3.4 Volcado de Memoria 12

5.3.5 Cadena de Custodia 12

5.3.6 Perito Informático Forense 12

5.3.7 Peritaje 12

5.3.8 Informe Pericial 12

5.3.9 Contraperitaje 13

5.3.10 Meta peritaje 13

5.3.11 Tanatología 13

5.4 Marco Legal 13

5.4.1 Marco Legal Colombiano 13

5.4.2 Marco Legal Internacional 15

5.5 Delitos Informáticos 15
5.6 Gestión de la Evidencia Digital 16
5.6.1 Recolección de datos volátiles 16
5.6.2 Recolección de datos NO volátiles 17
5.6.3 Cadena de custodia- Procedimiento 17
5.6.4 Volcado de memoria- Procedimiento 18
5.6.5 Recuperación de datos 19
6 Gestión de la evidencia digital 19
6.1 Mapa de conceptos 19
6.2 Memoria 20
6.2.1 Copia forense 26
6.2.2 Imagen forense 26
6.2.3 Recopilación de evidencia 26
6.2.3.1 Windows 26
6.2.3.1.1 Experimento 27
6.2.3.2 Linux 38
6.2.3.2.1 Experimento 39
6.2.3.3 Mac OS 44
6.2.3.3.1 Experimento 44
6.2.3.4 Dispositivos moviles 49
6.2.3.4.1 Android 51
6.2.3.5 Retos y conclusiones 53
6.3 Ossim 54
6.3.1 Herramientas 55
6.3.1.1 Pasivas 55
6.3.1.2 Activas 56
6.3.2 Secciones 56
6.3.2.1 Tableros 56
6.3.2.2 Análisis 57
6.3.2.3 Ambientes 57
6.3.2.4 Reportes 57
6.3.3 Actividad 57
6.3.4 Conclusión y reporte final 59

6.4 Red Forense 59
6.4.1 Tipos 60
6.4.1.1 Catch-it-as-you-can-system 60
6.4.1.2 Stop,look and listen 60
6.4.2 Procedimiento 61
6.4.3 Ataques comunes 61
6.4.4 Herramientas 62
6.4.5 Ejercicio 62
6.5 IoT 65
6.6 Nuggets DLS 68
6.6.1 Linux 72
6.7 Plataformas IoT 75
6.7.1 Samsung Artik 75
6.7.2 Amazon IoT 76
6.7.3 IBM Watson IoT 78
6.7.4 SiteWhere 78
6.7.5 Node red 78
6.7.6 GreenWave 82
6.7.7 Macchina.io 82
6.7.8 Thinger 83
6.8 Sistemas de archivos 83
6.8.1 Clasificación 84
6.8.1.1 Categoría de sistema de archivos 84
6.8.1.2 Categoría de metadato 84
6.8.1.3 Categoría de nombre de archivo 84
6.8.1.4 Categoría de contenido 85
6.8.1.5 Categoría de aplicación 85
6.8.2 FAT 85
6.8.3 NTFS 85
6.8.4 EXT 86
6.8.5 Actividad 86
6.8.6 Conclusión 86
6.9 Virtualizadores en la Forensia digital 86

6.9.1 Hipervisor: Definición 86
6.9.1.1 Hipervisor tipo 1 (bare metal) 87
6.9.1.2 Hipervisor tipo 2 (Host) 87
6.9.1.3 Hipervisores híbridos 87
6.9.2 Seguridad en hipervisores 88
6.9.2.1 Ataques a hipervisores 91
6.9.3 Forensia en Hipervisores 91
6.9.3.1 Experimento 95
6.10 Herramientas utilizadas 116
6.10.1 Helix 116
6.10.2 Deft 116
6.10.3 Hirens boot 117
6.10.4 Santoku 117
6.10.5 Dlc boot 117
6.10.6 EnCase 117
6.10.7 Katana 117
6.10.8 Koon-Boot 117
6.10.9 WireShark 117
6.10.10 WhatsApp Extractor 117
6.10.11 My lan Viewer 118
7 CONCLUSIONES 118
8 AGRADECIMIENTOS 119

1 RESUMEN

Los criminales cada vez más aprovechan la tecnología para cometer delitos y eludir a las autoridades. Este hecho ha obligado a los gobiernos a reglamentar y establecer unos parámetros y directrices de buenas prácticas que deban llevarse a cabo en la gestión de evidencias digitales, de manera que puedan ser usadas como pruebas válidas ante un juzgado, teniendo en cuenta que la prueba dentro de un proceso judicial es de especial importancia. Por lo tanto, la obtención de Información se considera hoy en día en una de las actividades primordiales en una investigación forense. De ahí, la necesidad de que se actúe en el manejo de evidencia, en pro de evitar acciones que puedan invalidar las evidencias digitales ante un proceso judicial.

2 PLANTEAMIENTO DEL PROBLEMA

A causa del rápido avance tecnológico, se hace evidente la necesidad de capacitar a las empresas e instituciones a responder frente a un incidente tecnológico, que le permita obtener una primera impresión de lo que pudo haber ocurrido en sus sistemas, como ocurrió y que información pudo obtener. Es por esto que en este proyecto se busca utilizar y analizar las metodologías existentes en forensia digital y así mismo comparar el procedimiento usado con la forensia en cloud e IoT para de esta manera determinar su similitud o diferencia.

2.1 DEFINICIÓN DEL PROYECTO

El proyecto busca ampliar el conocimiento del porque es importante la gestión de la evidencia digital en escenarios convencionales e IoT, apropiándose de herramientas y de procedimientos para generar una guía de primeros auxilios para saber cómo reaccionar frente a in incidente mientras llegan las entidades correspondientes a realizar el respectivo trabajo.

2.2 DESCRIPCIÓN DEL PROBLEMA

Se identifica la falta de conocimiento de las empresas y personas sobre la importancia de la forensia digital en general, por lo que se busca crear un documento que sirva de guía como primera respuesta ante un incidente digital para las empresas. Así mismo se pretende crear contenido que sea fácil de entender y permita generar interés en el tema.

3 JUSTIFICACIÓN

La tecnología está cada vez más inmersa en la vida cotidiana de las personas, es por eso que han tomado conciencia al respecto y buscan proteger su información, aunque no cuenten con la pericia para esto. Gracias a este hecho, adherido al uso indiscriminado de mecanismos de anonimato y a las dificultades para la obtención de información digital es la razón por la cual creemos que es una temática interesante cuyo objetivo es difundir la información sobre la gestión de evidencia digital,

así como sus buenas prácticas logrando mitigar la desinformación y la dificultad para la investigación con evidencia digital. Todo esto por medio del conocimiento y uso de herramientas de software utilizadas para la investigación informática forense de manera que se pueda presentar de forma objetiva, clara y detallada su efectividad y aplicabilidad.

Actualmente se encuentra con más frecuencia casos de delito informático, violación de sistemas y dispositivos, fraude informático e incidentes de seguridad de la información y privacidad de los datos. Como parte de lo que se requiere en estos casos, es poder determinar qué fue lo que paso, cómo ocurrieron los hechos, cómo evaluar los rastros o huellas que dejaron los atacantes en los sistemas para determinar cómo proceder legalmente, defenderse y protegerse. Y ahora, con los dispositivos IoT en todas partes, también es importante revisar cómo aplicar las mismas o nuevas soluciones de gestión de evidencia digital en este nuevo escenario.

4 OBJETIVOS

4.1 Objetivo General

Generar una propuesta para la gestión de evidencia digital aplicada a escenarios convencionales y de internet de las cosas que incluya herramientas, metodologías y procedimientos requeridos para que pueda ser utilizado dentro de procesos legales en la generación, análisis y control de evidencia digital.

4.2 Objetivos Específicos

- Conocer la problemática de la gestión de evidencia digital y la informática forense en diferentes escenarios
- Estudiar metodologías y recomendaciones sobre la gestión de evidencia digital
- Identificar similitudes y diferencias entre escenarios convencionales e IoT
- Apropiar herramientas de gestión de evidencia digital y mecanismo de interacción entre diferentes herramientas
- Generar material de apoyo que permita profundizar en estas temáticas en cursos del programa de ingeniería de Sistemas

5 MARCO TEÒRICO

Dado que este trabajo tiene como enfoque la gestión de evidencia digital, es necesario conocer sus antecedentes. En vista que en la actualidad es común escuchar el término de informática forense creemos fundamental conocer su historia y el trasfondo de su significado. La informática forense tiene sus inicios en la década de los 70 con la aparición de los transistores, utilizados para la innovación de las computadoras. Dado el rápido avance de la tecnología el interés por el estudio en el ámbito de la informática forense se hizo evidente en 1980, después de que las computadoras personales empezaron a transformarse en opciones para los usuarios.

Gracias al rápido avance de las computadoras en los 80’s surgieron aficionados por la programación, muchos de ellos pertenecientes a importantes entidades gubernamentales de los

Estados Unidos entre quienes estaba Michael Anderson quien junto con Danny Mares y Andy Fried de la IRS; Ron Peters y Jack Lewis del servicio secreto de los Estados Unidos; Jim Christy y Karen Matthews del departamento de defensa; Tom Seiffert, Roland Lascola y Sandy Mapstone de las agencias locales de aplicación de la ley de los estados unidos ; y los canadienses, Gord Hama y Steve Choy fundaron la primera organización dedicada a la forensia digital, llamada International Association of computer Investigation Specialist (IACIS). Anderson trabajó para el gobierno en la división de investigación criminal hasta mediados de 1990 y a raíz de la IACISl es considerado el padre de la informática forense [1].

A partir de esta década se dieron importantes pasos en la informática forense. El primero de ellos en 1993 cuando se celebró la primera conferencia sobre la recopilación de pruebas en equipos, la cual tenía como propósito reunir expertos en el tema con el fin de socializar prácticas e intercambiar herramientas, experiencia e información. Gracias a este primer encuentro, en 1996 se creó la IOCE (International Organization on Computer Evidence) con la intención de compartir las prácticas de informática forense en todo el mundo. Para 1998 a la IOCE se le encargó la tarea de desarrollar una serie de principios aplicables a los procedimientos entre las naciones para garantizar la fiabilidad del uso de las pruebas digitales recogidas por un estado para ser utilizadas en tribunales de justicia. En el cambio del milenio se analizó por parte del FBI alrededor de 2000 casos a través del análisis de 17 terabytes de datos lo que dio lugar a la creación del primer laboratorio regional de Informática Forense del FBI. Gracias a toda esta labor para el año 2003 los casos analizados por el FBI exceden los 6500 a través del análisis de 782 terabytes de datos [1].

Colombia no es la excepción, para el año 1999 aunque el delito informático no está explícitamente definido en el código penal, la Legislación si incluye en forma explícita el concepto de Evidencia Digital y reglamenta los requerimientos para que la misma sea permitida en un procedimiento jurídico con la Ley 527 de 1999. Sin embargo, para el año 2004 apareció el término "informática forense" cuando en el código de procedimiento penal colombiano en el artículo 236 (Recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes.) otorga permiso sobre el fiscal a recopilar componentes tecnológicos como computadoras, servidores y demás medios de almacenamiento físico que considere son pieza clave en una investigación [2] [3].

5.1 Informática Forense

Según el FBI, la informática (o computación) forense "es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional" [4].

La ***informática forense*** fue creada para ayudar a capturar a los intrusos en la red con motivo de hacer daño a terceros. Esta ciencia abarca las siguientes disciplinas [5]:

La ***computación forense*** encargada de resolver y analizar la información ubicada en los medios informáticos y de esta forma crear hipótesis de acuerdo a la información recopilada [6].

La ***forensia en redes*** tiene como función revisar los protocolos, configuraciones e infraestructura de comunicaciones con el fin de hallar datos precisos como la ruta tomada por el intruso y los rastros que pudo dejar en un tiempo particular [7].

La ***forensia digital*** encargada de tomar el conocimiento de la criminalística tradicional para aplicarlo en los medios informáticos

La informática forense tiene 3 objetivos, a saber:

1. La compensación de los daños causados por los criminales o intrusos.
2. La persecución y procesamiento judicial de los criminales.
3. La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, la principal de ellas es la recolección de evidencia [8], además son enfocados en dar garantía y respaldo al usuario. Es por esto que un experto en este campo está capacitado en redactar pautas acerca del uso de los sistemas informáticos para un ente específico, con el fin de mantener la máxima seguridad en cada uno de los equipos evitando que sean comprometidos y que exponga datos o cualquier otra información de valor.

5.1.1 Usos de la Informática Forense

Los usos de la informática forense varían según la aplicación pues proporciona una de las mejores rutas para hacer una investigación cuando se sospeche o exista una mala conducta digital.

Ya que por medio de una investigación informática forense es posible acceder a áreas en el espacio más remoto de almacenamiento de una computadora y de este modo extraer evidencia e información útil incriminatoria usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil. Convirtiéndose en una ciencia de alta demanda y gran contribución a la aplicación de la ley, así mismo se está usando para reabrir y resolver casos que se han congelado en el tiempo y dada la velocidad en que la tecnología avanza, del mismo modo lo han hecho las técnicas y formas de recopilación de datos.

Sin embargo, no es el único uso dado en la actualidad pues existen muchos servicios de investigación privada enfocada a los roles tanto empresariales como personales con el fin buscar evidencia para la prevención o tratamiento de algún incidente digital y de esta forma descubrir si se ha tratado de una infidelidad, fraude, discriminación, acoso, o divorcio como es el caso de los servicios personales, o por el contrario para temas corporativos puede ser recolectada información en casos sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial [9].

5.2 Evidencia Digital

Es un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales [10]. Una definición más general propuesta por Brian Carrier es definir la evidencia digital como datos digitales que soportan o refutar una hipótesis acerca de un evento o estado de datos digitales [11].
La evidencia digital es un medio válido para usarse como prueba en la legislación colombiana tomando en cuenta que abarca cualquier tipo de información extraída de un medio o de un dispositivo digital. Puede ser de distintos tipos como por ejemplo el contenido de un archivo, metadatos, datos de log, información de medios de almacenamiento no visible como archivos eliminados [12].

5.2.1 Clasificación de la evidencia digital

Se clasifica en tres categorías:

- Registros almacenados en el equipo informático: son aquellos generados por una persona y que son almacenados en el computador, lo importante con este tipo de archivos es importante demostrar que las afirmaciones humanas son reales.
- Registros generados por un equipo informático: son aquellos generados mediante la programación de un computador, estos son inalterables por las personas llamados log estos son utilizados como pruebas para demostrar el correcto registro generado por el computador.
- Registros híbridos: son aquellos generados por una combinación entre una persona y un computador, solo sirven como prueba si cumplen los dos requisitos anteriores [10].

5.2.2 Criterios de admisibilidad de la evidencia digital

Existen cuatro criterios para analizar a la hora de tener en cuenta la admisibilidad de la evidencia, estas son:

- Autenticidad: con el fin de demostrar que toda la información es precisa y verídica confirmando que la evidencia no ha sido modificada y que proviene de una fuente identificada. Para asegurar su cumplimiento se requiere que una arquitectura entregue mecanismos que certifiquen la integridad de los archivos [7] [10] [13].

- Confiabilidad: establece si realmente los medios que se están probando son de fuentes confiables, creíbles y verificables. Para comprobar esto se debe contar con una arquitectura que demuestra que los logs que genera son confiables y que pueden ser identificados, recolectados, almacenados y verificados [14].

- Completitud o suficiencia: demuestra que la prueba está completa, para asegurarlo debe garantizar la integridad, sincronización y centralización logrando obtener una vista completa de toda la situación realizando una completa correlación de eventos ya sea manual o sistematizada.

- Apogeo y respeto por las leyes y las reglas del poder judicial: la evidencia digital debe cumplir con todos los códigos de los procedimientos y disposiciones legales del sistema jurídico del respectivo país en este caso en Colombia.

5.2.3 Manipulación de la evidencia digital

Para esta investigación es fundamental diferenciar entre evidencia y prueba, la evidencia digital es la recopilada por un perito y la prueba es aquella evidencia involucrada en una investigación. Se deben tener en cuenta algunos, requisitos para cumplir con la manipulación de la evidencia digital es por eso que a continuación se listaran cada uno de ellos:

- Se debe manejar un buen uso de los medios forenses estériles en cuanto a las copias de la información.
- Se debe controlar y mantener la integridad de todos los medios originales recopilados, lo que significa que al momento de realizar la recolección se debe verificar que nunca cambie la evidencia.
- Solo un profesional forense puede tener acceso a la evidencia digital
- Todas las copias de los datos obtenidos deben estar correctamente marcadas, controladas y preservadas y deben estar siempre disponibles para la revisión de la misma manera que los resultados.
- cuando la evidencia digital esté en manos de una persona, éste será responsable de absolutamente todas las acciones tomadas durante su poder.

Son las agencias las encargadas de llevar de manera responsable los procesos de recolección y análisis de la evidencia garantizando el cumplimiento de los anteriores numerales [14].

5.3 Definiciones

5.3.1 Datos

Desde este punto de vista los datos son pulsos eléctricos a través de la combinación de circuitos y pueden ser representados por la computadora como tipo numérico, alfabético o simbólico, encargados de describir objetos, condiciones o situaciones, para la toma de decisiones.

5.3.2 Datos Volátiles

Son aquellos datos que quedan almacenados de forma temporal en la memoria volátil del sistema como lo es la memoria RAM o la memoria caché que se podrían perder si el equipo se apaga o se reinicia [15] [7] [16].

5.3.3 Datos No Volátiles

También llamados datos persistentes, son aquellos que se encuentran almacenados en el disco duro u otros dispositivos de almacenamiento que normalmente no se pierden al apagar o reiniciar el equipo.

5.3.4 Volcado de Memoria

Es la abstracción reproducida en binario de los datos que se encuentran en la memoria RAM y en la memoria virtual. Para los sistemas Windows se manejan tres tipos de volcado de memoria mini, kernel y full. El mini se caracteriza por recuperar la información de los procesos y la memoria tal como se estaba ejecutando, mientras, el tipo kernel contiene al mini y adicionalmente al núcleo del sistema operativo, el estado de los registros y el ciclo de vida de los procesos. Finalmente, el tercer tipo de volcado corresponde al vaciado completo de la memoria RAM y virtual del equipo. Por otro lado, en los sistemas operativos Unix y derivados existen dos tipos de volcados, el tipo Core que contiene la información de una aplicación cuando ocurre un error en su ejecución y el otro tipo completo que corresponde a la información total del sistema [6] [17].

5.3.5 Cadena de Custodia

La cadena de custodia es un proceso controlado que busca brindar soporte a la prueba digital ante un juez con el fin de garantizar la veracidad de las pruebas recopiladas. En el caso particular de evidencia digital, la información se puede encontrar en diferentes estados, almacenada estáticamente (información persistente), almacenada dinámicamente
(información volátil), en tránsito o desplazamiento (en la red en forma de paquete de información) [14] [18].

5.3.6 Perito Informático Forense

Es el profesional que se encarga de realizar los procedimientos de recopilación de pruebas y exámenes detallados sobre equipos involucrados en un ataque, dividiendo su labor de análisis en tres ramas computadores y dispositivos, redes y evidencia digitales. Sin embargo, su labor incluye también el componente preventivo con el fin de evitar espionajes, fraudes, robos de información, manipulación de datos y programas, etc., que pueden ocasionar grandes pérdidas a las compañías. Su análisis permite responder las preguntas básicas de una hipótesis: quién, cómo, dónde, cuándo y por qué [5] [14] [18].

5.3.7 Peritaje

Es una disciplina encaminada a las actividades que se presentarán en un litigio de hechos basados en evidencias formales. Utilizando técnicas de informática forense para dar puntos de vista y aportar consideraciones sobre los factores de la actividad pericial, teniendo una visión netamente probática de los indicios, extrayendo los hechos complejos y de alto nivel de las evidencias obtenidas [14] [18].

5.3.8 Informe Pericial

Es un documento que enmarca el protocolo legal y técnico de la recopilación de evidencia, donde el perito expone el resultado de los análisis realizados. Donde inicialmente el perito analiza la situación planteada por el juez y determina el procedimiento a seguir para la intervención de acuerdo a lo solicitado por la justicia.
Se debe detallar todo el procedimiento realizado explicando detalladamente las operaciones que se llevaron a cabo. Debe ser claro y objetivo, así como demostrar suficiencia de conocimiento científico del perito [14] [18] [19] [20].

5.3.9 Contraperitaje

Es la revisión crítica de un informe pericial informática con el fin de buscar fallos en las metodologías y protocolos usados para recopilación de evidencia, de tal manera que se pueda refutar la conclusión emitida por el perito firmante del informe original.
"El Contraperitaje, por regla general, no es más que una pericia que se realiza a un objeto que ya fue periciado con anterioridad y que es realizada por un perito distinto del primero, ya sea, durante el mismo litigio o de forma privada. Entendiendo que siempre el contra peritaje va a ser un segundo, tercer o cuarto peritaje practicado a un mismo objeto." [21] [22].

5.3.10 Meta peritaje

Tiene como objetivo encontrar concordancia en los procesos, omisiones o errores que haya tenido el perito al realizar su informe pericial. Sin embargo, no es considerado un informe pericial, aunque debe contener los apartados o ítems respectivos a la estructura de un informe pericial para que tenga un orden lógico y cronológico [21] [22] [23].

5.3.11 Tanatología

Creada para realizar el análisis de flujo de red, captura de paquetes, evaluación de registro, control de firewall entre otros, permitiendo conocer y dar un análisis de los fenómenos observados dando una explicación del impacto generado por el ataque del sistema específico. El tanatólogo digital (perito) es el encargado de la recuperación de las arquitecturas, seguimiento e identificación de piratas para poder establecer cuál fue el delito informático [4].

5.4 Marco Legal

5.4.1 Marco Legal Colombiano

Teniendo en cuenta las definiciones descritas anteriormente en esta investigación, es necesario tener presente que para que tal evidencia sea válida como prueba ante un juez, debe fundamentarse no sólo en el correcto procedimiento de recolección como también en lo establecido por la ley.

Enmarcando la perspectiva legal en Colombia se considera que la primera ley que incluye temáticas digitales fue la Ley 527 de 1999, denominada "Ley de Comercio Electrónico", la cual reconoció como prueba válida a los mensajes de datos, otorgándoles la fuerza probatoria establecida en el Código de Procedimiento Civil. Los artículos de esta Ley especifican como debe ser tratada la evidencia, teniendo en cuenta la integridad, la admisibilidad y fuerza probatoria de los mensajes de datos, así como el criterio para valorar probatoriamente el mismo, incluye además las recomendaciones para la conservación de los mensajes de datos y documentos a través de tercero.

Sin embargo, La ley 527 dio paso a muchas regulaciones relacionadas al tratamiento de la información empezando con la ley 594 de 2000, la cual es, la ley general de archivos y criterios de seguridad, que da a conocer los conceptos sobre los distintos tipos de archivos, exponiendo la elaboración del documento hasta su eliminación o conservación permanente que se genera dentro de una entidad u empresa [3].

Para 2007 se da la Circular 052 de la Superintendencia Financiera de Colombia, donde se establecen los requerimientos mínimos de calidad y seguridad en el manejo de información a

través de canales y medios de distribución de productos y servicios para clientes y usuarios. De igual manera en 2008 se establece, la ley estatutaria 1266 la cual regula el manejo de la información contenida en bases de datos personales, principalmente la financiera, comercial, crediticia, de servicios y la proveniente de otros países, e igualmente se establecen las disposiciones legales relacionadas con el hábeas data.

En 2009 se reglamentó la ley 1273 por medio de la cual se modifica el Código Penal, estableciendo la protección de la información y de los datos. Esta ley penaliza todo acto que atente contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. En este mismo año se da la ley 1341 en la cual se establecen los conceptos y principios de la sociedad de la información, la organización de las TIC y la creación de la Agencia Nacional de Espectro (ANE), con el fin de establecer las obligaciones de los proveedores de redes y servicios de telecomunicaciones en relación a la seguridad de la información y la inviolabilidad de las comunicaciones.

No obstante, existen artículos penales que, aunque no tienen relación explícita con las evidencias digitales, si se aplica a su uso en una investigación. Es así como el Código de Procedimiento Penal colombiano asume algunas facultades de la Fiscalía relacionadas con la obtención de evidencia, pues en el artículo 235 sostiene que "el fiscal podrá ordenar de manera fundada y por escrito la interceptación de comunicaciones que contengan información de interés para la investigación. Los órganos encargados de cumplir con la orden tienen la obligación de realizar la tarea inmediatamente después de haber sido notificados y de guardar la debida reserva" [24]. Por otro lado, el art. 236 "faculta al fiscal a ordenar el secuestro de computadoras, servidores y otros dispositivos de almacenamiento para que luego sean analizados por expertos en informática forense. El secuestro será autorizado cuando haya motivos razonablemente fundados de que existió transmisión de información relevante y se limitará exclusivamente al tiempo necesario para la captura de la información contenida" [24] [25].

En los dos supuestos, el fiscal deberá comparecer dentro de las 24 horas de realizada la medida ante el juez de control de garantías para que se desarrolle la audiencia de control de legalidad. Durante el trámite de la audiencia sólo podrán asistir, además del fiscal, los funcionarios de la policía judicial y los testigos o peritos que prestaron declaraciones juradas con el fin de obtener la orden respectiva.

Cabe resaltar que, de todas las leyes y artículos presentados, especialmente la ley 1273 de 2009 y la Ley 527 de 1999, son empleadas para la administración de la justicia en un caso donde interviene como medio probatorio la evidencia digital [26].

5.4.2 Marco Legal Internacional

En cuanto a el marco legal internacional es conveniente destacar los esfuerzos de los países latinoamericanos, por ponerse a la par de los países europeos en cuanto a leyes contra la ciberdelincuencia.

El sistema penal mundial se ha enfrentado a un desafío constante desde el surgimiento y reconocimiento de los delitos informáticos, dando así la necesidad de hacer adecuaciones normativas con el fin de tipificar y penalizar correctamente tales delitos. Sin embargo, dado que el sistema de pruebas fue fundamentado en la evidencia física muchas veces es necesario aplicar normas que regulan este tipo de evidencia a la evidencia digital, creando en algunos casos brechas jurídicas.

Si bien se han dado importantes pasos en este campo, cabe resaltar que existen falencias de capacitación y conocimiento del tema, dando lugar a una ineficiente utilización de las herramientas disponibles, así como generando inconvenientes en la penalización ante tribunales.

Caso contrario se presenta en Europa, pues a pesar de llevar una lucha constante contra la ciberdelincuencia, son quienes llevan la delantera en el ámbito legal creando de esta forma un punto de referencia para Latinoamérica. Es así como se estableció una Directiva Europea, la Directiva 2016/1148, que contiene las medidas para garantizar un elevado nivel de seguridad en las redes y sistemas de información comunes para los miembros de la Unión Europea [27], todo esto con el compromiso de que los mismos cumplan y adopten las medidas adecuadas para minimizar, reducir o prevenir el riesgo planteado.

De igual manera, uno de los puntos de esta directiva plantea que ante cualquier tipo de incidente informático los miembros están en el deber de notificar inmediatamente a la autoridad competente de cada país, entiéndase como el CERT (del inglés Computer Emergency Response Team**)** para que con su oportuno apoyo se puedan tomar medidas de prevención y control, no solo a nivel institucional sino a nivel nacional.

Cabe resaltar, que mientras en Latinoamérica la gran brecha es la falta de capacitación de las personas frente a un incidente de seguridad, en Europa existe mayor capacitación convirtiéndolo en una fortaleza que les permite ser puntos de referencia para las demás naciones incluyendo a Norte America. Hitos como lo fue el convenio sobre Ciberdelincuencia (conocido como el convenio de Budapest) convirtiéndose en el primer tratado internacional que busca hacer frente a los delitos informáticos con la creación de leyes nacionales, así como la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones; y aunque fue elaborado por el consejo europeo tuvo colaboración de varios países de Asia y América.

5.5 Delitos Informáticos

El convenio de Budapest con el fin de definir un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea propone una clasificación de los delitos informáticos en tres grupos [28]:

- *Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos en los que se contempla*:

- Acceso Ilícito, que constituye acceso malintencionado a una parte o todo el sistema sin autorización.
- Interceptación Ilícita de datos, hacia, desde o dentro de un sistema.
- Interferencia de datos, que es la eliminación, alteración o daño intencional de datos sin autorización.
- Interferencia en el funcionamiento del sistema, obstaculizando su buen desempeño introduciendo, transmitiendo, dañando, borrando o alterando sus datos.
- Mal uso de dispositivos, que facilite el propósito de cometer delitos.

Entre los delitos más reconocidos están el hacking que se conoce porque el perpetrador intenta acceder a un sistema o a un computador sin la debida autorización con la intención de cometer delitos desde el mismo.

- *Delitos asistidos por computadora:* entiéndase que son crímenes tradicionales donde la computadora es únicamente una herramienta para cometerlos.
  - Delitos relacionados con la informática: contempla realizar fraude o transferencias de dinero o valor monetario con el objetivo de obtener un beneficio económico no autorizado mediante la alteración, introducción, eliminación o acceso ilícito de datos en un sistema.
  - Delitos relacionados con dispositivos: contempla la alteración de dispositivos informáticos adaptados para hacer, recibir, obtener, vender o transferir información con el fin de su falsificación o uso fraudulento.
- *Delitos relacionados al contenido:* son similares a los delitos asistidos por computadora con la diferencia que el objetivo de ataque es el contenido como es el impulso y apoyo de la pornografía infantil, grooming, falsa información, racismo o xenofobia.

Entre otros actos relacionados al crimen informático, se encuentran la infracción al copyright o derechos de autor pues dada la sobre explotación de información que se encuentra en la internet es un delito difícil de controlar. Así mismo, se encuentra el ciberbullying pues no existe una legislación específica que lo penalice, lo cual lo convierte en un debate político y social.

5.6 Gestión de la Evidencia Digital

Gestionar la evidencia digital no es más que tener el conocimiento de cómo utilizar, trabajar o manipular la evidencia física, son los pasos para seguir al momento de analizar la evidencia con las herramientas y técnicas presentadas a continuación.

5.6.1 Recolección de datos volátiles

Para la recolección de los datos volátiles, se debe evitar la contaminación de los dispositivos sospechosos a toda costa, sin embargo, es bastante complicado controlarlo pues se puede hacer uso de herramientas y comandos que causan graves efectos en la posible evidencia cómo cambiar las fechas y horarios originales de los accesos a los archivos, utilizar bibliotecas compartidas o de archivos DLL, activar un software malicioso o en el peor de los escenarios forzar un reinicio lo que causaría la pérdida de todos los datos volátiles.

Teniendo en cuenta la naturaleza de estos datos, antes de comenzar su recolección es necesario acordonar el área, así como desconectar el dispositivo de internet con el fin de evitar que sea interceptado, además es necesario tener en cuenta las siguientes consideraciones [7] [13] [15] [16]:

- Ejecutar un intérprete de comandos confiable, que usualmente será la terminal del sistema operativo, a menos que se especifique lo contrario.
- Registrar la fecha, hora del sistema, zona horaria en que se realiza la recopilación.
- Determinar quién o quienes se encuentran con una sesión abierta, ya sea usuarios locales o remotos.
- Registrar los tiempos de creación, modificación y acceso de todos los archivos.
- Verificar y registrar todos los puertos de comunicación abiertos.
- Registrar las aplicaciones relacionadas con los puertos abiertos.
- Registrar todos los procesos activos.
- Verificar y registrar las conexiones de redes actuales y recientes.
- Registrar la fecha y hora del sistema.
- Verificar la integridad de los datos.
- Documentar todas las tareas y comandos efectuados durante la recolección
- Examinar y extraer los registros de eventos.
- Examinar la base de datos o los módulos del núcleo del sistema operativo.
- Verificar la legitimidad de los comandos del sistema operativo.
- Examinar y extraer los archivos de claves del sistema operativo.
- Obtener y examinar los archivos de configuración relevantes del sistema operativo.
- Obtener y examinar la información contenida en la memoria RAM del sistema

Esto es posible mediante el uso de herramientas forenses disponibles en los kits usados durante la investigación de este proyecto. La más adecuada para este tipo de información en el caso de Windows es D.A.R.T disponible en el kit DEFT que permite hacer el levantamiento de información volátil accediendo a la pestaña “Forensics” permitiendo la adquisición de información volátil necesaria para la investigación. Cabe destacar que existen además muchos comandos que permiten hacer la copia forense, sin embargo, con esto se corre el riesgo de alterar la información, por otra parte, el uso de herramientas forenses permite generar informes de auditoría válidos frente a una corte.

5.6.2 Recolección de datos NO volátiles

En cuanto a datos No volátiles se le debe dar un buen manejo a los dispositivos para evitar la contaminación, aunque dado el caso que el dispositivo se contamine esta se puede controlar mediante técnicas, herramientas y una metodología. Una de las herramientas más común es dd.exe desarrollada por George Garner, esta herramienta tiene la capacidad de crear una copia bit a bit del disco duro del dispositivo sospechoso, con el fin de que ningún dato sea alterado.

5.6.3 Cadena de custodia- Procedimiento

La cadena de custodia es un procedimiento basado en el principio de la “mismidad” para garantizar la autenticidad e integridad de las evidencias, asegurar que lo mismo que se revisó es lo que se le entrega al tribunal penal o a la entidad correspondiente. Estos mecanismos buscan probar que la evidencia recolectada no sea alterada, a continuación, se presentan los pasos mínimos que se

manejan en una cadena de custodia y para la elaboración del procedimiento de recolección y gestión de evidencia forense [7] [8] [9] [14] [18] [11] [29]:

- se debe llevar una hoja de ruta en la cual se escriben los datos principales sobre la evidencia como fechas, horas, custodios, identificaciones, firma y cargo de quien recibe y entrega la evidencia y demás datos que considere importante
- Adjuntar todos los recibos personales de todos los custodios (con datos similares a los que tiene la hoja de ruta)
- pegar rótulos o etiquetas a todos los empaques de las evidencias como las bolsas, sobres de papel, frascos, cajas, entre otros.
- mantener un libro de registro físico o virtual de entradas y salidas para los laboratorios o los despachos de los fiscales e investigadores

Estos pasos se realizan con el fin de brindar confianza a las personas que reciban las evidencias y certificar que la información es íntegra, que no ha sido alterada o modificada.

5.6.4 Volcado de memoria- Procedimiento

Hoy en día el volumen de los discos es muy amplio por lo que el proceso puede resultar costoso en cuanto a tiempo y a recursos [17]. Los volcados de memoria son una representación binaria que tienen los sistemas, estas están contenidas en la memoria RAM y virtual del sistema operativo. Se debe tener bien claro qué tipo de volcado se va a realizar, y es posible clasificarlos en 3 tipos:

- *Crear una copia bit stream de disco a imagen*: es el método más habitual y más rápido. Además, permite realizar tantas copias como sea necesario de una manera fácil y sencilla para la fase de análisis.
- *Crear una copia bit stream de disco a disco*: es el método utilizado en el caso de que no sea posible realizar una copia bit stream de disco a imagen. Del mismo modo que el método anterior se puede realizar tantas copias como sean necesarias. La realización de un clonado mediante un dispositivo hardware conlleva una mayor fiabilidad y rapidez.
- *Creación de una copia de datos dispersos de una carpeta o archivo*: es decir, realizar una copia selectiva, ya que en muchas ocasiones dependiendo del tipo de incidente puede no ser necesario volcar todo el disco y sea suficiente copiar ciertas carpetas o ficheros.

Adicionalmente es necesario tener en cuenta algunos datos complementarios en el proceso del volcado de memoria:

- En caso de que se requiera hacer una copia sectorizada (como es el caso de incidentes de malware, para posteriormente analizar qué sectores se encuentran infectados) del disco es necesario usar el método, Master Boot Record que hace referencia al primer sector, sector 0, de un dispositivo de almacenamiento de datos. Posee un tamaño de 512 bytes y almacena información relativa a cómo iniciar el sistema, qué tipo de particiones hay en el dispositivo y el tamaño de las mismas, etc. En cierto tipo de incidentes, principalmente relacionados con malware, puede resultar de interés extraerlo para que en un posterior análisis determinar si está infectado.
- Si lo que se requiere es una información más detallada de los ficheros y carpetas se usa el método Master File Table (MFT) la cual es una tabla que almacena información relevante de todos los ficheros y carpetas de una unidad o disco. Contiene, entre otra, información como nombre, tamaño, fecha, hora, o permisos, incluso de ficheros que hayan sido eliminados hasta el momento en el que dicho espacio sea necesario y se sobrescribe.

5.6.5 Recuperación de datos

Es un proceso utilizado para recuperar archivos de manera legal, recuperando archivos que fueron dañados, corrompidos o eliminados de forma ilegal, es por eso que antes de utilizar la herramienta se debe tener en cuenta los siguientes pasos [12].

- la identificación de los equipos informáticos para determinar los datos a recopilar y analizar
- Analizar el dispositivo para realizar la recuperación mediante el análisis de los discos duros y extracción de información sobre que causo la perdida de los archivos para poder eliminar el ransomware del equipo.
- Elaboración del informe con todos los resultados obtenidos, dando el análisis detallado de los datos recogidos, también se deben explicar los procedimientos que se realizaron para recuperar los archivos.

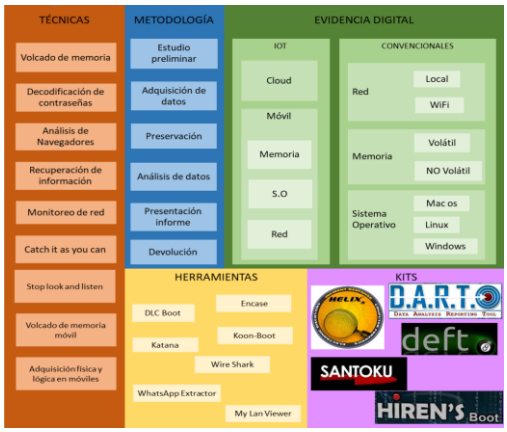
6 Gestión de la evidencia digital

A continuación, se encuentra el trabajo realizado durante el proyecto aplicando la metodología y técnicas a las diferentes herramientas investigadas. Adicionalmente se establece el marco de información con el que se pretende tener una guía de lo que se debe tener en cuenta durante la gestión de evidencia digital.

6.1 Mapa de conceptos

La imagen encontrada a continuación es el primer producto realizado como proyecto de grado, es un mapa de bloques sobre el enfoque general para el proyecto el cual esta distribuido de la siguiente manera:

La sección verde es la clasificación de los dispositivos para el alcance del proyecto que en este caso es los equipos convenciones como los computadores o routers y los dispositivos IoT como lo son los celulares, SmartWatch, smartTv a los cuales se analizaron mediante unas técnicas como las que se observan en la sección azul, estas técnicas son importantes a la hora de entreagar la evidencia ya que si no cumple con la metodología apropiada no será admisible ante la corte por lo que es muy importante el bloque naranja en donde se tienen todas las herramientas utilizadas en el proyecto para la recolección de evidencia ya sea en la sección de red, memoria o sistema operativo, como también para móvil o cloud, estas técnicas se realizan con la ayudad de herramientas y kits forenses los cuales son open source y son fácil de usar para la recolección porque cuentan con las características y principios que deben tener las pruebas para ser validas ante la corte.



6.2 Memoria

La memoria, como componente principal de un dispositivo que genera y almacena datos, es el objetivo principal de los ataques informáticos. Por ende, es fundamental conocer su significado, su importancia, los seis niveles de memoria existentes entregando una explicación de cada uno y las técnicas que son aplicadas en cuanto a memoria como el volcado de memoria que es una representación binaria del contenido de la memoria RAM, conoceremos los 3 tipos de volcado de memoria los cuales están clasificados según la información que se desea recuperar o analizar [30] [31].

La memoria en informática es un dispositivo a base de circuitos que permite almacenar limitadamente la información de la computadora, muchas veces conteniendo información vital no solo para el propietario sino para el funcionamiento de la máquina como tal, pues son clave para el arranque de la computadora o la ejecución de instrucciones. Son diversos los tipos de memoria y de acuerdo a sus características, difieren sus funciones [32].
Entre las características principales se encuentra su capacidad pues compone un dato esencial para calibrar la potencia de un computador, la cual está medida en bytes, como dato esencial en cuanto mayor sea la cantidad de memoria que posea un dispositivo mejor será su rendimiento. Siendo parte de la arquitectura del dispositivo, como componente también posee su propia arquitectura que define los tipos de memoria existentes, así como el tipo de información que almacena [33].

Los niveles que componen la jerarquía de memoria habitualmente son [34]:

- Nivel 0: Registros del microprocesador o CPU
- Nivel 1: Memoria caché
- Nivel 2: Memoria primaria (RAM)
- Nivel 3: Memorias flash
- Nivel 4: Disco duro (con el mecanismo de memoria virtual)
- Nivel 5: Cintas magnéticas (consideradas las más lentas, con mayor capacidad, de acceso secuencial)
- Nivel 6: Redes (actualmente se considera un nivel más de la jerarquía de memorias).

Se realizará entonces un análisis trivial sobre cada uno de los niveles, para dar un mejor entendimiento sobre la memoria en sí. En el nivel 0 se encuentran los registros del procesador que ofrecen un nivel de memoria más rápido y pequeño que la memoria principal, que permite a los

usuarios conocedores del lenguaje de ensamble acceder a estos registros y hacer uso óptimo de la memoria principal. Así mismo contiene registros utilizados por el procesador para el sistema operativo para controlar la ejecución de programas. En el nivel 1, se encuentra la memoria caché (caché, que proviene del francés y significa escondite) la cual almacena datos de rápido acceso con información volátil lo que le permite ser de apoyo para la memoria principal y de esta manera mejorar la capacidad de procesamiento [35].

Su funcionamiento a simple vista es bastante sencillo, cuando un dato es accedido por primera vez una copia del acceso es guardada en caché haciendo más rápido su posterior acceso, razón por la cual se renueva constantemente.
A su vez, la memoria caché se encuentra organizada en diferentes niveles según sea su proximidad al núcleo del procesador. Un elemento a considerar es el tamaño de la memoria caché, si bien el punto de equilibrio depende del tipo de programas ejecutados, por esto existirá una cierta cantidad de memoria a partir de la cual el incremento del rendimiento obtenido no compensa el costo adicional de agregar más memoria caché. En la actualidad los procesadores indican que usan 3 niveles de caché: L1 de 10KB a 20 KB, L2 de 128KB a 512KB y L3 de 4M a 12MB [36].

La memoria caché L1, es un tipo de memoria pequeña y rápida que está en la unidad de procesamiento central, utilizada para acceder a datos importantes de uso frecuente. Es el tipo más rápido y de mayor costo integrado en el equipo.
La memoria caché L2, es utilizada para almacenar información reciente fue diseñado para reducir el tiempo de acceder a datos que han sido usados anteriormente. Por su parte la memoria caché L2 es secundaria a la CPU y es más lenta que la memoria caché L1. La memoria caché L2 es la más unificada, lo que significa que se usa para almacenar los datos e instrucciones de programas.
La memoria caché L3 es una memoria que está integrada en la placa madre. Se utiliza para alimentar a la memoria caché L2, y generalmente es más rápida que la memoria principal del sistema, pero todavía más lenta que la memoria caché L2 [36].

Indudablemente las ventajas son claras pues representa un aumento de la velocidad, sin embargo, también tiene desventajas puesto que si no se borra la caché o se refresca periódicamente se podría estar accediendo a datos no actualizados. En el nivel 2 se encuentra la memoria RAM (Random Access Memory) la cual es considerada como uno de los componentes más importantes de la CPU puesto que es la encargada de almacenar y ejecutar todas las instrucciones asignadas por el procesador, así como las órdenes de otros componentes tales como la tarjeta gráfica, el disco duro e incluso aplicaciones que se ejecuten en el equipo.
Gracias al avance tecnológico, este componente ha tenido numerosas versiones a medida que se ha optimizado su rendimiento.

Algunos de los modelos de memoria Ram volátiles más utilizados actualmente son [37]:

- VRAM o Video Random Access Memory que puede ser accedida por dos dispositivos simultáneamente.
- DRAM o Dynamic Random Access Memory, ya que requiere constante actualización, este tipo de memoria ya no se utiliza.

- SRAM Static Random Access Memory, aunque son muy rápidas, son difíciles de conseguir pues ya no se comercializan.
- DDR RAM surge como reemplazo a la SRAM, pues además de ser más rápida está constantemente sincronizada y funciona enviando datos de redundancia cada ciclo de reloj.
- DDR2 DDR3 y DDR4 son las más utilizadas en la actualidad con mucho mejor rendimiento y menor consumo de energía.
- RAMBUS a nivel de rendimiento es de las mejores pero debido a su alto costo no tuvo mucho éxito en las ventas.

De esta manera cuanta más memoria ram tenga un dispositivo más posibilidades tiene de poder abrir varios programas informáticos al tiempo, pues incluso aunque no lo parezca, el entorno gráfico, el fondo de pantalla o el uso del ratón funciona a traves de RAM. Como ya se ha dicho con anterioridad, la memoria RAM es utilizada para almacenar programas y datos que usa el procesador en tiempo real, esto hace que la información almacenada desaparezca cuando se apaga el dispositivo [38].
Curiosamente muchas veces es confundida con la memoria ROM (Read Only Memory), la cual no es volátil lo que hace su acceso más lento pues como su nombre lo indica es de solo lectura. A su vez la memoria ROM se descompone en diferentes tipos [39]:

- MaskROM es la que se escribe durante el proceso de fabricación de la memoria y no puede modificarse.
- PROM (Programmable Read-Only Memory) Similar a la Mask ROM, pero los datos pueden ser introducidos después de fabricar el chip para luego no poder ser modificados.
- EPROM: (Erasable Programmable Read Only Memory) similar a la anterior, con la diferencia que sólo permite borrar contenido si este se expone a luz ultravioleta de alta intensidad.
- EEPROM: (Electrically Erasable Programmable Read-only Memory) permite eliminar los datos de manera electrónica, y pueden reescribirse los datos escritos en ellas un número limitado de veces.

La memoria flash es una manera avanzada desarrollada de EEPROM que permite que múltiples áreas de memoria sean escritas o borradas en una misma operación, y esta es la que utilizan en la actualidad la mayoría de dispositivos con memoria flash como las memorias USB, tarjetas SD y más recientemente los SSD [40].

Es así como llegamos al nivel 3, memorias Flash, de las cuales anteriormente ya se ha hablado. Sin embargo, cabe destacar algunas de sus características más importantes. Iniciamos con la resistencia a los golpes, pues al no incluir elementos mecánicos en su interior puede moverse con mayor libertad lo que la hace ideal para dispositivos móviles. Adicionalmente esto lo hace mucho más silencioso, de bajo consumo y de tamaño reducido. No obstante, no todo son ventajas, puesto que solo permite una cantidad finita de escrituras y borrados, generalmente entre 10.000 y 1 millón), lo que hacen los controladores de estos dispositivos es ir añadiendo datos nuevos a partes que nunca se han usado para así no quemarlas demasiado pronto.
Inicialmente almacenaban 8 MB, pero actualmente almacenan más de 64 GB, con una velocidad de hasta 20 MB/s [41].

Con estas grandes capacidades de almacenamiento alcanzamos el nivel 4 de la arquitectura de memoria que son los discos duros, también llamado, hard disk. o HDD. Es un dispositivo de almacenamiento magnético que aloja de forma permanente la información del ordenador, incluyendo el sistema operativo y las aplicaciones [42]. Este funciona por medio de un sistema de grabación magnética y está compuesto por uno o màs discos que se unen y giran a gran velocidad, sin embargo, actualmente existen los discos duros de estado sólido que usan procesos químicos para grabar la información, lo que lo hace mucho más resistente a daños y golpes, así como representa una mejora en velocidad de lectura y escritura, comparado con el disco magnético.

Dentro de este nivel es muy común hablar de memoria virtual [43], pues es una técnica que ayuda a la memoria física para que la memoria principal parezca más grande que su tamaño físico, por lo que permite ejecutar programas más grandes que la memoria física disponible mientras que la memoria principal actúa como cache de la memoria secundaria (disco duro). La combinación entre hardware especial y el sistema operativo hace uso de la memoria principal y la secundaria para hacer parecer que el ordenador tiene mucha más memoria principal (RAM) que la que realmente posee.
Aunque la memoria virtual podría estar implementada por el software del sistema operativo, en la práctica casi siempre se usa una combinación de hardware y software, dado el esfuerzo extra que implicaría para el procesador.

Para los últimos niveles de la jerarquía es importante destacar que son los usados para hacer copias de seguridad o de soporte. La cinta magnética es un tipo de soporte de almacenamiento de información que permite grabar datos sobre una banda de material magnético, que son usualmente utilizadas para hacer backups. Aunque podría creerse que se encuentran en desuso, Sony anunció en 2014 que han conseguido una cinta magnética que puede almacenar 148 Gbit por pulgada cuadrada o 23 Gbit por cm^2, permitiendo que en una cinta se almacenen 185 TB (185000 GB). En tanto en mayo de 2014 la empresa Fujifilm anunció que desarrolló un cartucho que almacena 154 TB.

Por otra parte, en el último nivel se encuentran los sistemas de almacenamiento de red, la cual es una arquitectura de almacenamiento a nivel de archivos en la que uno o más servidores almacenan datos en discos dedicados y los comparte, lo que hace que los datos sean más accesibles entre los dispositivos de una red [44].
Los tres principales sistemas de almacenamiento usados son [45]:

- SAN: (Storage Area Network), consiste en conectar discos a una controladora que con la suma de sus capacidades forma un espacio de almacenamiento global, junto con un servidor es posible gestionar los datos y permitir una conexión a una red local.
- DAS (Direct Attached Storage) es almacenamiento conectado directamente a una computadora individual, habilitando una capacidad extra de almacenamiento de esta.
- NAS: (Network Attached Storage) es el más utilizado por quienes buscan centralizar los archivos y copias de seguridad, dado que este sistema incorpora su propio sistema de conexión y recepción de peticiones de acceso a los datos, elimina a los servidores del proceso.

Con esto en mente, es posible hablar de almacenamiento en la nube, el cual Según el IEEE Computer Society la computación en la nube es: "un paradigma en el que la información se almacena de manera permanente en servidores de Internet y se envía a cachés" [46].

Permite almacenar y acceder a datos transfiriéndose a través de internet o de otra red a un sistema de almacenamiento externo que se contrata por medio de un tercero quien administra y opera el almacenamiento en la nube como un servicio. Estos sistemas de almacenamiento pueden ser escalables y adaptables a las necesidades de almacenamiento, accesibles desde cualquier lugar y desde cualquier dispositivo. Esto le otorga agilidad, escala global y durabilidad a la información.

Las empresas disponen de tres modelos principales para elegir: un servicio de almacenamiento en nube pública, adecuado para datos no estructurados; un servicio de almacenamiento en nube privada, que puede estar protegido detrás de un firewall de la compañía para tener más control sobre los datos; y un servicio de almacenamiento en nube híbrida, que combina servicios de almacenamiento en nube pública y privada para ofrecer una mayor flexibilidad [46].

Sin embargo, no todo son ventajas, pues el uso de este tipo de tecnología crea cierta dependencia de los proveedores de este tipo de servicio confiando en su tecnología y funcionamiento, sin tener acceso a los servidores físicos en caso de necesitarlo. Por otro lado, puede existir una sobrecarga en los servidores si el número de usuarios es muy alto o no se sigue una política de uso adecuada y a pesar de requerir una mínima inversión e infraestructura ya que solo es necesario contar con una plataforma en la nube y no hay que instalar ningún software, puede llegar a generar altos costos según el espacio requerido de almacenamiento [46].

Para un correcto análisis, existen técnicas de recolección de datos que son procedimientos especiales utilizados para obtener y evaluar las evidencias necesarias, suficientes y competentes que le permitan formar un juicio profesional y objetivo, que facilite la calificación de los hallazgos detectados en la materia examinada. La recolección debe ser realizada por un perito profesional en informática forense, dicha recolección representa un esfuerzo considerable por su parte. Si este procedimiento se hace correctamente es mucho más útil para atrapar al delincuente y representa una oportunidad mucho mayor en ser admitida como hecho en un juicio.
Como parte del análisis de la recolección, se deben considerar varios factores entre estos se encuentran la evaluación de escena, herramientas y equipamientos, dispositivos electrónicos, el tipo de información que se quiere recolectar, almacenamiento y transporte, análisis de la información obtenida y el reporte de resultados [47].

En todos y cada uno de los casos analizados se debe tener en cuenta el procedimiento adecuado para realizar la recopilación de la información. Para este procedimiento es necesario comenzar por llevar una orden de recopilación de información dando la posibilidad de ser admitidos en un proceso judicial. Luego se debe determinar el tipo de evidencia que se busca en la investigación, lo que ayuda a determinar la relevancia de los datos. Una vez se ha establecido el tipo de información que se busca y lugares probables donde encontrarlos, por lo que es necesario fijar qué

dispositivos son volátiles y pueden contener información sensible, necesaria para la investigación [48].

Para comenzar el proceso de recopilación, se debe eliminar la interferencia externa, establecer las herramientas necesarias, así como documentar todas las acciones realizadas para validar el proceso de recolección de evidencia. Finalmente es necesario hacer el análisis de la evidencia, el cual se dará por terminado cuando se descubra cómo fue realizado el delito, el porqué, quien o quienes lo cometieron, bajo qué circunstancias, cuál era el objetivo del ataque y qué daños causaron.

Por otro lado, hoy en día el volumen de los discos es muy amplio por lo que el proceso puede resultar costoso en cuanto a tiempo y a recursos.
Los volcados de memoria son una representación binaria que tienen los sistemas, estas están contenidas en la memoria RAM y virtual del sistema operativo. Se debe tener bien claro qué tipo de volcado se va a realizar, y es posible clasificarlos en 3 tipos [49]:

a. El primero es creando una copia bit stream de disco a imagen: es el método más habitual y más rápido. Además, permite realizar tantas copias como sea necesario de una manera fácil y sencilla para la fase de análisis.
b. Como segunda instancia se puede crear una copia bit stream de disco a disco: este método es utilizado en caso de que no sea posible realizar una copia bit stream de disco a imagen. Del mismo modo que el método anterior se puede realizar tantas copias como sean necesarias. La realización de un clonado mediante un dispositivo hardware conlleva una mayor fiabilidad y rapidez.
c. Por último, tenemos la creación de una copia de datos dispersos de una carpeta o archivo: es decir, realizar una copia selectiva, ya que en muchas ocasiones dependiendo del tipo de incidente puede no ser necesario volcar todo el disco y sea suficiente copiar ciertas carpetas o ficheros.

Adicionalmente es necesario tener en cuenta algunos datos complementarios en el proceso del volcado de memoria:
En caso de que se requiera hacer una copia sectorizada (como es el caso de incidentes de malware, para posteriormente analizar qué sectores se encuentran infectados) del disco es necesario usar el método, Master Boot Record [50] que hace referencia al primer sector, sector 0, de un dispositivo de almacenamiento de datos. Posee un tamaño de 512 bytes y almacena información relativa a cómo iniciar el sistema, qué tipo de particiones hay en el dispositivo y el tamaño de las mismas, etc. En cierto tipo de incidentes, principalmente relacionados con malware, puede resultar de interés extraerlo para que en un posterior análisis determinar si está infectado.

Si lo que se requiere es una información más detallada de los ficheros y carpetas se usa el método Master File Table (MFT) [51] la cual es una tabla que almacena información relevante de todos los ficheros y carpetas de una unidad o disco. Contiene, entre otra, información como nombre, tamaño, fecha, hora, o permisos, incluso de ficheros que hayan sido eliminados hasta el momento en el que dicho espacio sea necesario y se sobrescribe.

6.2.1 Copia forense

El clonado forense o también conocido como copia forense de discos duros, se realiza con el fin de certificar y mantener la cadena de custodia de las evidencias, ya que, de no hacerse correctamente, las pruebas recolectadas quedarían invalidadas. Esta técnica consiste en copiar todo el contenido de un disco duro, bit a bit, en otro dispositivo de almacenamiento con una herramienta que permita generar una firma hash de los bits leídos durante el proceso. obteniendo de eta forma, una copia exacta a bajo nivel de todo el contenido del disco duro además de certificar su contenido con la firma hash [52].

Es deber del perito informático certificar la cadena de custodia, esto es, que las evidencias permanecen inalteradas desde el momento en que son intervenidas, pudiendo certificar su originalidad en cualquier momento posterior a la intervención.

6.2.2 Imagen forense

Es una técnica particular que permitirá crear una copia exacta del dispositivo o equipo original en uno nuevo. Esto significa que el original y la copia serán idénticos al momento preciso en que se hizo la imagen, al grado que incluso, de ambas se pueda recuperar información borrada a través de técnicas, tan sencillas con herramientas especializadas en cómputo forense o de técnicas más tediosas como el análisis manual de archivos en hexadecimal [53].

La imagen forense cumple entonces con los conceptos básicos del cómputo forense: identificar, preservar, recuperar, analizar y presentar hechos y opiniones, por tanto, al **preservar** todos los atributos del origen permiten que los hechos y opiniones puedan presentarse en tribunales [54].

6.2.3 Recopilación de evidencia

6.2.3.1 Windows

Por lo general el equipo se puede encontrar en 2 posibles estados, encendido, con procesos en ejecución, conectado a la red y con informacion de interes en medios como la memoria volátil y muerto, en que el dispositivo se encuentra desconectado, sin procesos activos y con información no volátil.

Basados en estos estados, si el dispositivo está vivo lo más recomendable es volcar la memoria RAM. Sin embargo, se debe tener en cuenta que algunos computadores usan contraseña de administrador para acceder al sistema operativo, en caso de que esto sucediera, es necesario usar herramientas adicionales a las mencionadas en el artículo. Luego es necesario hacer una copia bit a bit de los medios de almacenamiento para lo que se recomienda el uso de herramientas tipo LIVECD como DEFT con lo que se genera el correspondiente Hahs en MD5 y SHA-1 para garantizar la integridad de los datos adquiridos [55].

A Continuación, es necesario analizar la imagen por medio de la misma herramienta es posible hacerlo, pues la mayoría de las suites permiten montar de manera segura la imagen para poder recorrer directorios y ficheros con mayor facilidad, usualmente se usa una herramienta como dd2vmdk para crea un disco virtual de la imagen y poder analizarla sin correr riesgos.
Expertos en la materia aseguran que manejar de esta manera la evidencia trae varias ventajas en la investigación:

"Cuando se revive un entorno virtualizado, la copia bit a bit, tenemos las siguientes ventajas:

- se puede aislar totalmente el sistema para evitar la comunicación con el mundo exterior.
- se puede ejecutar herramientas gratuitas que permitan extraer la información gráfica y automáticamente sin comprometer un entorno real.
- se tiene la posibilidad de sacar snapshots del sistema sin tener comprometido el segundo original.
- se puede ver el entorno real que tenía el usuario.
- se puede buscar información de una manera más rápida y fácil, ya que la navegación por el sistema será más intuitiva."

En la fase de análisis de Datos se realiza el análisis temporal, la búsqueda de contenido, recuperar los binarios y documentos borrados o corruptos, búsqueda de archivos ocultos o no usuales, búsqueda de procesos en ejecución, busqueda de cuentas de usuario. todo esto con el objetivo de encontrar evidencia relacionada al caso.

6.2.3.1.1 Experimento

Para el caso de prueba de herramientas en Windows se hizo una prueba específica en la recopilación de datos en una memoria flash, más específicamente en una memoria usb. Con el uso de herramientas como Helix y Deft, con el fin de conocer la línea de tiempo de la información registrada en la memoria.

Realizaremos la imagen de una USB de 1GB, para conocer la línea de tiempo de los archivos que han estado en la memoria entregándo información sobre qué archivos han sido creados, modificados o eliminados.

Para comenzar con esta auditoría se solicitó autorización para el uso de la USB otorgando al dueño la información pertinente de lo que se realizaría. De manera que se procede a insertar la USB en el computador y se revisa el dispositivo a inspeccionar, en donde se encuentran 8 archivos, entre ellos unos archivos de word, pdf, html y una grabación, todos en perfecto estado. Después de eso se ejecuta la aplicación de Helix la cual de manera paralela crea un pdf en donde queda registrando la hora de inicio de la aplicación como se puede observar en la figura 2 y junto con ello todas las acciones que se realizan durante la ejecución de la aplicación como se observa en la imagen en la figura 3, con lo que al terminar la ejecución de la aplicación entrega un reporte final con las notas finales y la hora de finalización de la aplicación como aparece en la figura 4, el cual únicamente se obtiene al final de la ejecución.

```
Helix Iniciado en: 09/17/2018 en 15:48:07
==========
---------- SYSTEM INFORMATION --------
Sistema Operativo:
Operating System Version: 6.2.9200
User Information:
Administrador: Windows User
Organización:
Admin: No
Admin Rights: Yes
Información de Red:
Nombre-Red: REDES107
Usuario: Redes
IP: 192.168.37.1
NIC: 005056c00001
Domain:
Unidades Detectadas:
C:\ (Unidad lógica)
D:\ (Unidad lógica)
E:\ (Unidad lógica)
F:\ (Unidad lógica)
G:\ (Unidad de CD/DVD-ROM)
H:\ (Unidad de CD/DVD-ROM)
----------
```

Fig. 2 Acciones realizadas

15:48:15 - Helix desplegó la página Acerca de...
15:48:44 - Helix desplegó la página 1 de Información del Sistema.
15:49:00 - Helix desplegó la página 2 de Información del Sistema.
15:49:33 - Helix desplegó la página 1 de Adquisición "Live".
16:00:23 - El botón Adquirir fue ejecutado.
16:00:39 - Helix desplegó la página 2 de Adquisición "Live".
16:00:43 - El programa FTK Imager fue ejecutado satisfactoriamente.
17:24:29 - Helix desplegó la página del Escaneo en búsqueda de Imágenes.
17:24:32 - Helix desplegó la página 1 de Información del Sistema.
17:24:32 - Helix desplegó la página 1 de Adquisición "Live".
17:24:33 - Helix desplegó la página 2 de Adquisición "Live".
17:24:34Live RAM Acquisition Page
17:24:36 - Helix desplegó la página 2 de Adquisición "Live".
17:24:37 - Helix desplegó la página 1 de Adquisición "Live".
17:24:39 - Helix desplegó la página 2 de Adquisición "Live".
17:24:40Live RAM Acquisition Page
17:24:43 - Helix desplegó la página 1 de Incident Response.
17:24:52 - Helix desplegó la página 2 de Incident Response.
17:24:56 - Helix desplegó la página 1 de Incident Response.
17:24:57 - Helix desplegó la página 2 de Incident Response.
17:24:59 - Helix desplegó la página 3 de Incident Response.
17:25:13 - The USBDeview program was executed.
17:28:09 - Helix desplegó la página 2 de Incident Response.
17:28:13 - Helix desplegó la página 3 de Incident Response.
17:28:21 - Helix desplegó la página de Examinar Contenidos.
17:29:05 - Helix desplegó la página del Escaneo en búsqueda de Imágenes.
17:30:19 - Helix desplegó la página de Notas de Investigación.

Fig. 3 Acciones realizadas

```
###################### INVESTIGATIVE NOTES ##############################
Investigator:
Case Number:
Agency:

#########################################################################

=========================================================================
Helix Detenido on: 09/17/2018 en 17:35:19
```

Fig. 4 Acciones realizadas

Toda esta informacion anterior se genera paralelamente al proceso de obtención de la información, la cual se hizo teniendo la debida precaución de no alterar la realización de la imagen. Para la recopilación de la imagen forense, fue necesario seguir los siguientes pasos en la herramienta Helix.

Dado que es una herramienta fácil e intuitiva fue necesario ingresar al icono (adquision) como se indica en la figura 5.

Fig. 5 Adquisicion de memoria

A continuación se selecciona el origen de la adquisicion, que en este caso es la memoria USB, asi como el destino por lo que lo más recommendable es que sea de tipo disco duro y finalmente un nombre que identifique la imagen forense que se va a adquirir tal como se observa en la figura 6.

Fig. 6 Adquisicion de memoria

Esto llevará a una pantalla que da informacion sobre la herramienta que se usará para la imagen tal como aparece en la figura 7.

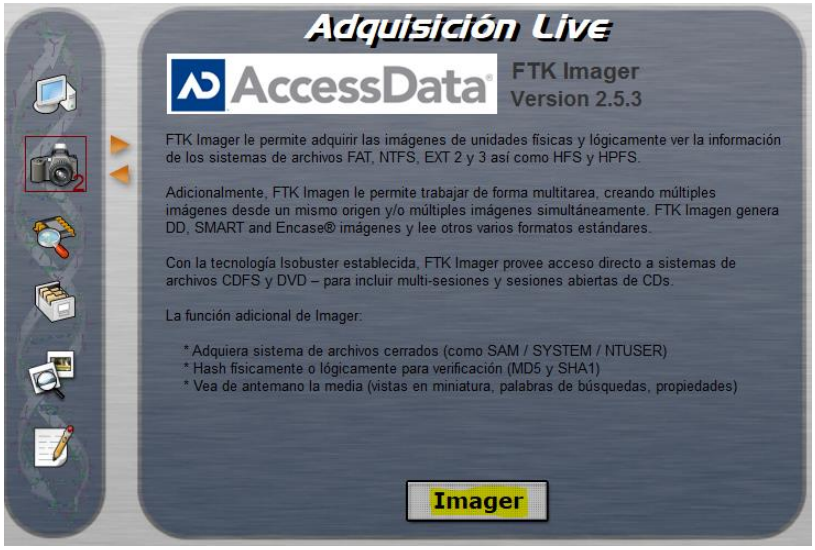


Fig. 7 Herramienta

Esto desplegará una nueva ventana que muestra la ejecución de la herramienta como tal, que para el ejercicio es FTK Imager de la figura 8.

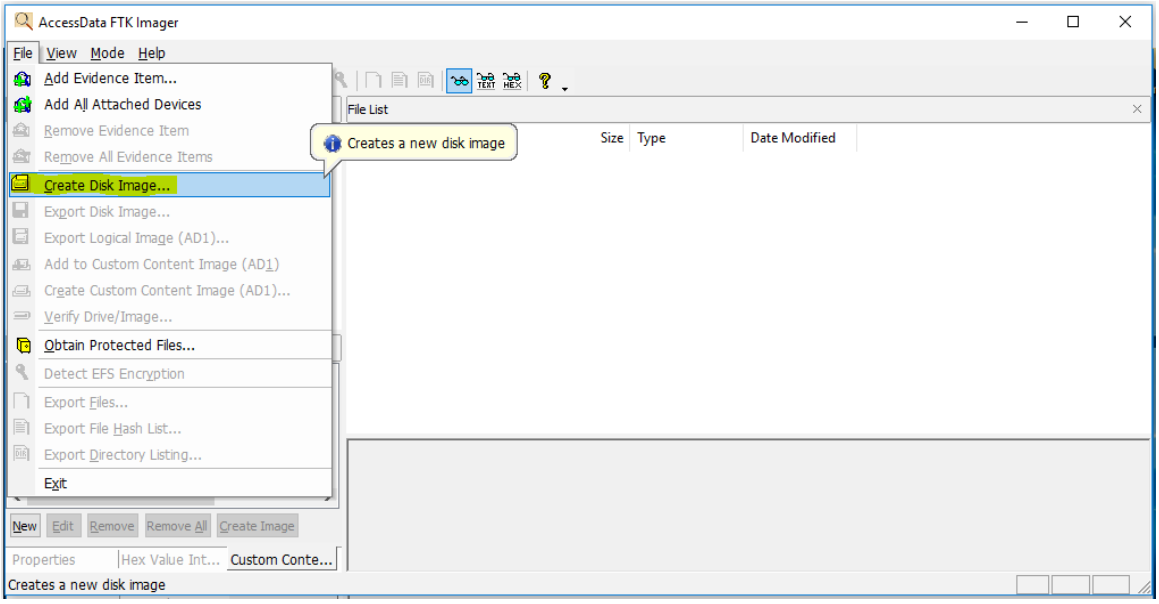


Fig. 8 FKT Imager

En FTK imager , solo queda buscar la opción de crear imagen para comenzar el proceso como aparece en la figura 8. Así pues, la herramienta solicitará l fuente de copia de la figura 9 y a continuación solicitará seleccionar de la lista que ofrece de acuerdo a la opción seleccionada como fuente, esto se puede apreciar en la figura 10, por lo que si se escoge un medio físico es muy importante de que está correctamente conectado .

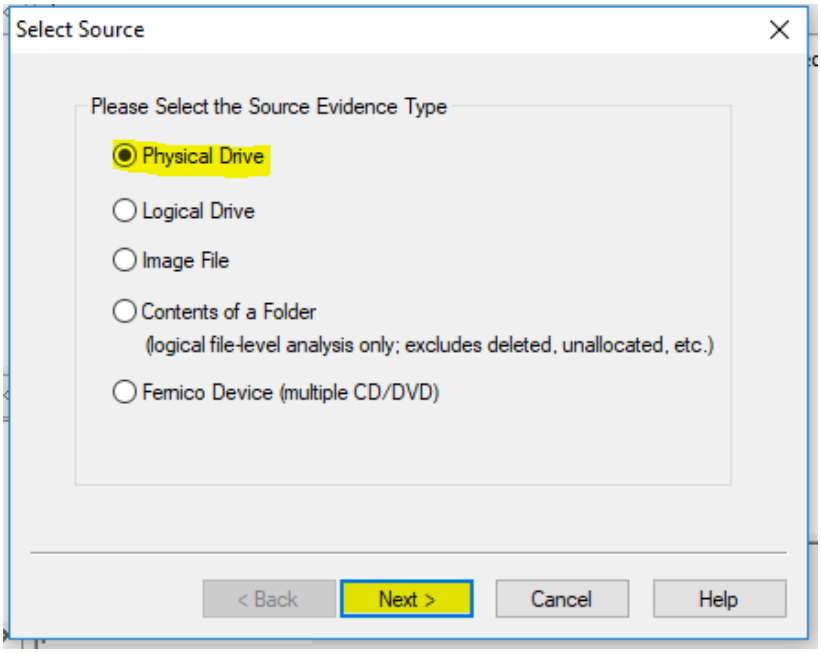


Fig. 9 Fuente

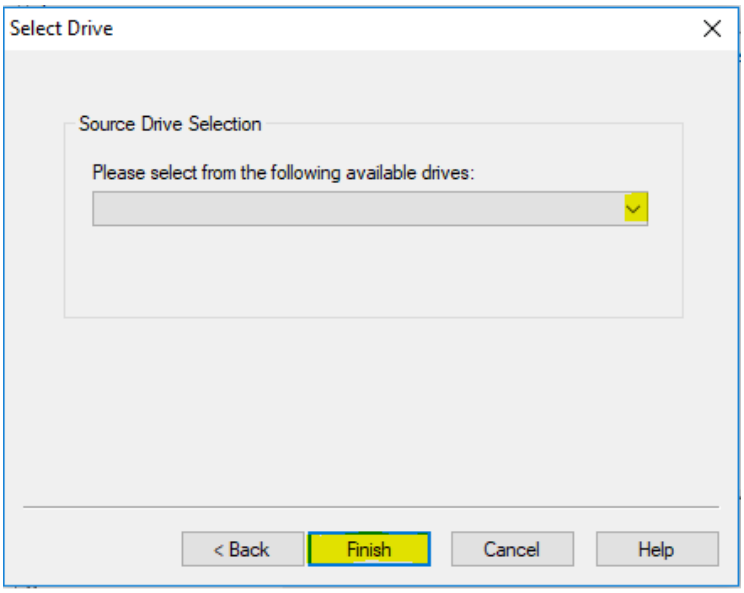


Fig. 10 Seleccionar Fuente

Ahora el software solicita elegir a cuál dispositivo le va a realizar la imagen, por lo que nuevamente debe escogerlo de una lista proporcionada por la herramienta como se aprecia en la figura 11.

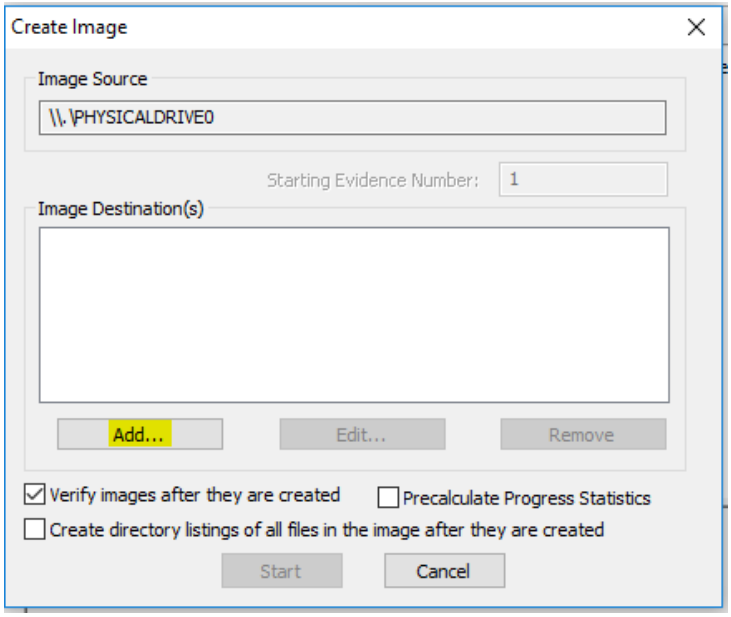


Fig. 11 Seleccionar copia

Para el siguiente paso es importante tener en cuenta el tipo de imagen en la que se espera que salga la copia, pues de esto depende su posterior lectura esto se puede ver en la figura 12. Lo más común y recommendable es escoger el tipo dd (raw) que al ser de los más conocidos, permite que casi cualquiera herramienta pueda tener acceso a él.

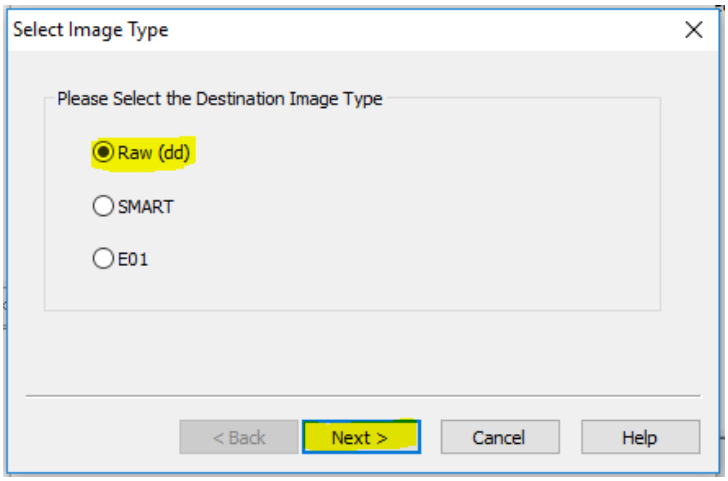


Fig. 12 Tipo de copia

Finalmente solicita unos datos pertinentes alcaso de investigacion que permitirán rotular correctamente toda la informacion que arroja la herramienta como se observa en la figura 13 , lo que para un perito resulta muy útil y hace que ante una corte sea admisible.

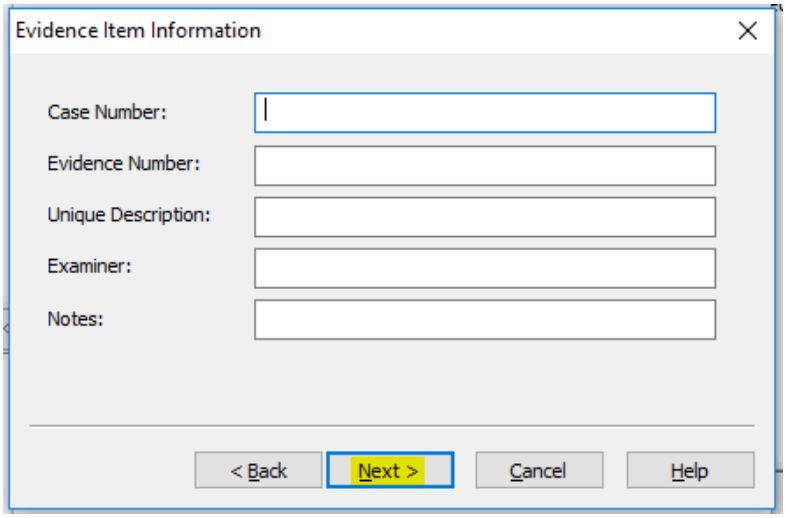


Fig. 13 Informacion adicional

Finalmente es momento de comenzar a generar la copia y para ello bastará con oprimir el boton start como se aprecia en la figura 14 y 15.

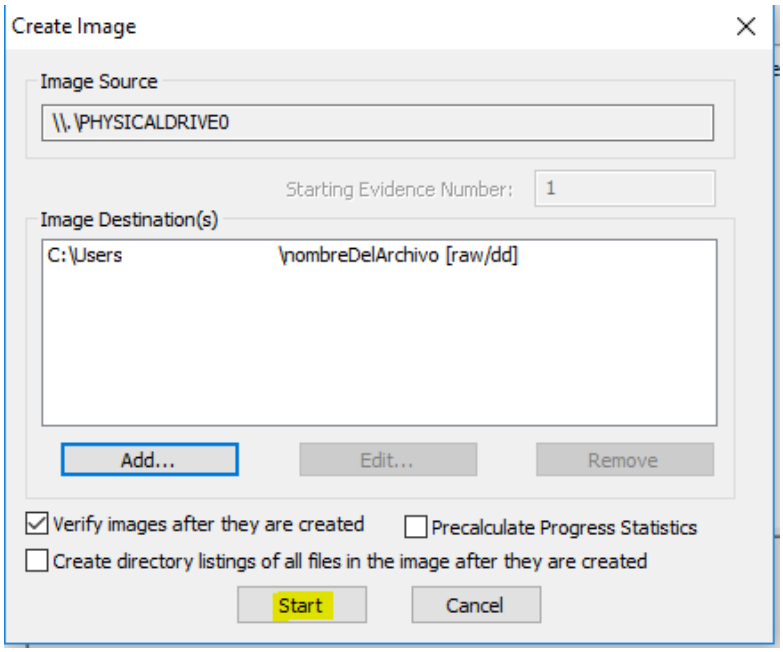


Fig. 14 Comienzo de Proceso

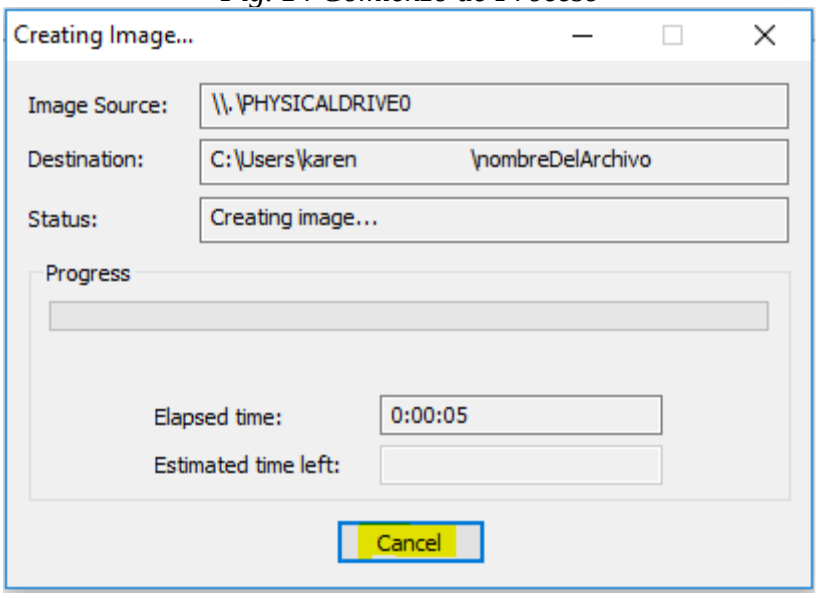


Fig. 15 Proceso

Para cuando termina la imagen, se debe llenar el final del reporte con los datos pertinentes, para ello debemos es necesario hacer click en la imagen de informe como aparece en la figura 16 y esto arroja un informe como se aprecia en la figura 17, 18.

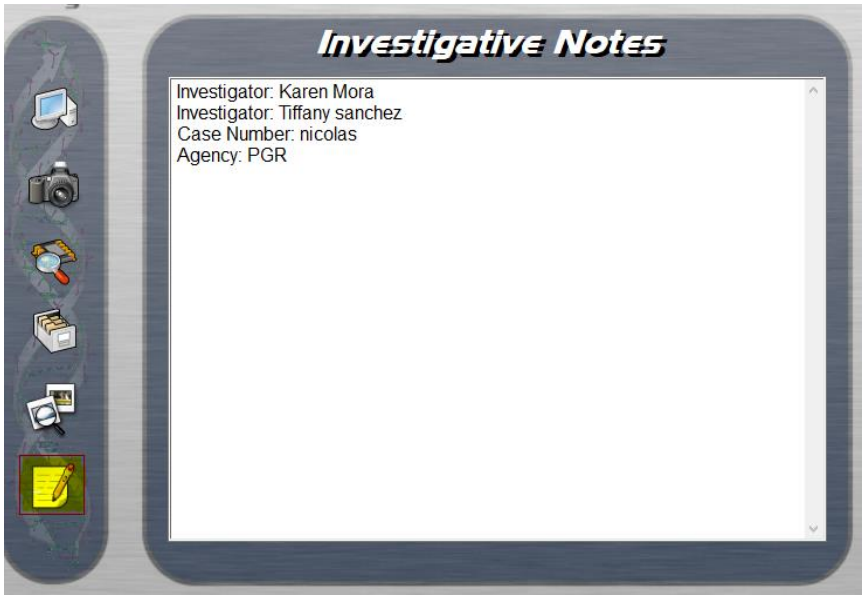


Fig. 16 generacion de informe

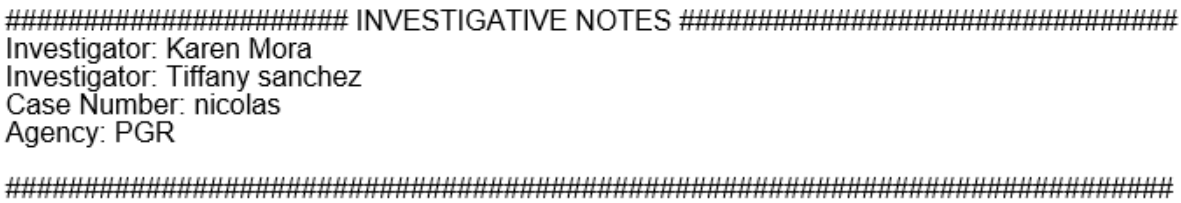


Fig. 17 Informe

Fig. 18 Informe de Investigacion

Al terminar la ejecución de Helix se almacenan en el computador, cuatro archivos de diferentes extensiones, como se explicó al comienzo del ejercicio. Al analizar cada uno de ellos se encuentra que todas las acciones realizadas han sido registradas y protegidas, por otro lado, en un archivo .txt contiene la información registrada del caso como aparece en la figura 19, toda la información que tiene el dispositivo que se está analizando de la figura 20, la información de la imagen como aparece en la figura 21 y la verificación de los resultados de la imagen mostrados respectivamente.

```
Created By AccessData® FTK® Imager 2.5.3.14 071018

Case Information:
Case Number: nicolas
Evidence Number: N002
Unique Description: D002
Examiner: tiffYkaren
```

Fig. 19 Archivo TXT

```
Physical Evidentiary Item (Source) Information:
[Drive Geometry]
 Cylinders: 127
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 2,047,998
[Physical Drive Information]
 Drive Model: JetFlash TS1GJF2A/120 USB Device
 Drive Serial Number: MJ20MWNI
 Drive Interface Type: USB
 Source data size: 999 MB
 Sector count:    2047998
[Computed Hashes]
 MD5 checksum:    d22de4dd2ca798921d41b9563d86fb13
 SHA1 checksum:
302830bf4f0e57c80859b409d41d8233ad7fddc1
```

Fig. 20 Información del Caso

```
Image Information:
 Acquisition started:   Mon Sep 17 17:06:01 2018
 Acquisition finished:  Mon Sep 17 17:07:55 2018
 Segment list:
  C:\Users\Redes\Downloads\nicolas\Nicolas.001
```

Fig. 21 Información del dispositivo

```
Image Verification Results:
 Verification started:  Mon Sep 17 17:07:55 2018
 Verification finished: Mon Sep 17 17:07:59 2018
 MD5 checksum:    d22de4dd2ca798921d41b9563d86fb13 :
verified
 SHA1 checksum:
302830bf4f0e57c80859b409d41d8233ad7fddc1 : verified
```

Fig. 22 Verificación de resultados

Entre los archivos arrojados, se encontró uno en formato .xls que contiene la informacion de los archivos hallados en la memoria flash, pero donde adicionalmente da informacion de tamaño, cuando fue creado, modificado, accedido y borrado como se aprecia en la figura 23.

A	B	C	D	E	F	G
Filename	Full Path	Size	Created	Modified	Accessed	Is Deleted
04 What happens tomorrow.wma	Partition 1\NONAME [FAT16]\[root]\04 What happens tomor	4001030	2006-May-19	2005-jul.-19 19	2006-jun.-29 0:0(	yes
04. Track 4.mp3	Partition 1\NONAME [FAT16]\[root]\04. Track 4.mp3	4292845	2006-May-19	2002-oct.-15 1(	2006-jun.-29 0:0(	yes
05 Green Day - Wake me up when september.wm	Partition 1\NONAME [FAT16]\[root]\05 Green Day - Wake m	4515058	2006-May-19	2005-jul.-19 19	2006-jun.-29 0:0(	yes
05. Track 5.mp3	Partition 1\NONAME [FAT16]\[root]\05. Track 5.mp3	4641423	2006-May-19	2002-oct.-15 1(	2006-jun.-29 0:0(	yes
06 Good charlotte - I just wanna live.wma	Partition 1\NONAME [FAT16]\[root]\06 Good charlotte - I jus	2710296	2006-May-19	2005-jul.-19 19	2006-jun.-29 0:0(	yes
06. Track 6.mp3	Partition 1\NONAME [FAT16]\[root]\06. Track 6.mp3	5132943	2006-May-19	2002-oct.-15 1(	2006-jun.-29 0:0(	yes
07 Maroon 5 - She will be loved.wma	Partition 1\NONAME [FAT16]\[root]\07 Maroon 5 - She will b	4162452	2006-May-19	2005-jul.-19 19	2006-jun.-29 0:0(	yes
07. Track 7.mp3	Partition 1\NONAME [FAT16]\[root]\07. Track 7.mp3	4651454	2006-May-19	2002-oct.-15 1(	2006-jun.-29 0:0(	yes
08 Moby - Lift me up.wma	Partition 1\NONAME [FAT16]\[root]\08 Moby - Lift me up.wm	3032966	2006-May-19	2005-jul.-19 19	2006-jun.-29 0:0(	yes
08. Track 8.mp3	Partition 1\NONAME [FAT16]\[root]\08. Track 8.mp3	4529201	2006-May-19	2002-oct.-15 1(	2006-jun.-29 0:0(	yes
09. Track 9.mp3	Partition 1\NONAME [FAT16]\[root]\09. Track 9.mp3	4205074	2006-May-19	2002-oct.-15 1(	2006-jun.-29 0:0(	yes
10 Pista 10.wma	Partition 1\NONAME [FAT16]\[root]\10 Pista 10.wma	4520884	2006-May-19	2005-jul.-19 19	2006-jun.-29 0:0(	yes
10. Track 10.mp3	Partition 1\NONAME [FAT16]\[root]\10. Track 10.mp3	4191283	2006-May-19	2002-oct.-15 1(	2006-jun.-29 0:0(	yes
11 Avril LAvinge - She wasn't.wma	Partition 1\NONAME [FAT16]\[root]\11 Avril LAvinge - She w	2847728	2006-May-19	2005-jul.-19 19	2006-jun.-29 0:0(	yes
11. Track 11.mp3	Partition 1\NONAME [FAT16]\[root]\11. Track 11.mp3	5233256	2006-May-19	2002-oct.-15 1(	2006-jun.-29 0:0(	yes
Diana Krall - Live In Paris - 11 - A Case Of You.mp	Partition 1\NONAME [FAT16]\[root]\Diana Krall - Live In Pari	16966490	2006-May-19	2002-Dec-08 0	2006-jun.-29 0:0(	yes
S-5-3-42-2819952290-8240758988-879315005-3(	Partition 1\NONAME [FAT16]\[root]\RECYCLER\S-5-3-42-2(	16384	2009-May-18	2009-my.-18 1(	2018-mzo.-05 0:(	no
fwqkvsq.vmx	Partition 1\NONAME [FAT16]\[root]\RECYCLER\S-5-3-42-2(	81760	2004-Aug-20	2004-Aug-20 0	2009-oct.-12 0:0(	yes

Fig. 23 Archivo Excel

Al revisar con detenimiento el documento es posible apreciar que registra archivos creados desde el 2008 y que fueron eliminados tiempo después, por otro lado también registra archivos como.java, imágenes, documentos de word, powerpoint o excel, también audios y videos.

Ahora como complemento a la investigación se utiliza la herramienta llamada Deft. Que permite la recuperación de los archivos y ayuda concluir que la gran mayoría de archivos que aparecen eliminados en el Excel proporcionado por Dart se recuperaron de forma satisfactoria, sin embargo, algunas imágenes y audios no se recuperaron completamente. Lo que demuestra que cuando un espacio en memoria ha sido utilizado varias veces, la información, aunque se puede recuperar no siempre se recupera completa.

Con este primer acercamiento, se dio paso a un experimento mucho más completo realizado en un equipo de cómputo donde se buscaba recopilar la mayor cantidad posible de actividades realizadas por un estudiante común en la Escuela Colombiana de Ingeniería Julio Garavito. Esto se llevó acabo en 3 diferentes puntos de concentración de estudiantes: biblioteca, sala decanatura de sistemas y sala de inglés. Para los escenarios de la biblioteca y la sala de decanatura de sistemas, se hicieron pruebas muy similares comenzando con un volcado de memoria que arrojaba los mismos resultados que en el experimento con la memoria USB, pero además se experimentó con las herramientas de tráfico de red, sin embargo, no se obtuvieron datos concluyentes. Por lo que finalmente, se decide ir a una sala con mayor afluencia como lo es la sala de inglés, donde se procuró hacer un uso más exhaustivo de las herramientas disponibles, para lo que se usó DART que viene disponible con la distribución de DEFT.

Para este escenario se obtuvieron muchos más resultados, comenzando por la herramienta WinAudit disponible en la opción Incident Response el cual genera un archivo pdf de la figura 24 con todas las especificaciones de la máquina evaluada.

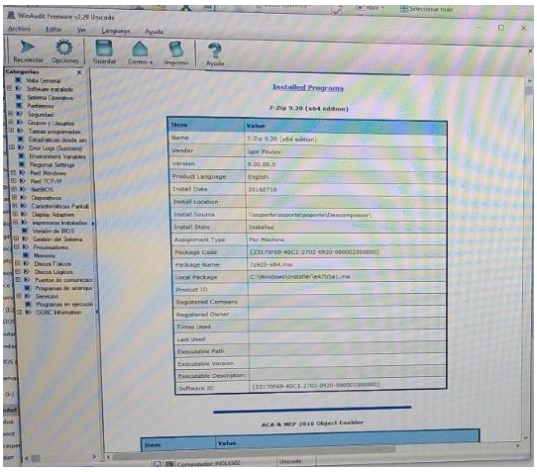


Fig. 24 Especificaciones Maquina

Luego se procede a usar la herramienta forensic – browser forensic tool para detectar todas aquellas búsquedas realizadas en el PC como se observa en la figura 25, que de acuerdo a una clasificación predeterminada puede escoger el tipo de búsquedas como redes sociales, pornografía, hacking entre otras.

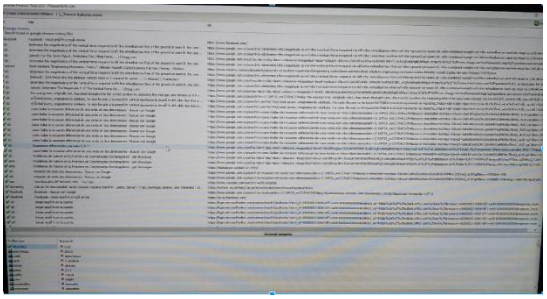


Fig. 25 Busquedas Realizadas

Sin embargo, si el dispositivo se encuentra apagado estas mismas herramientas pueden usarse desde el arranque de la máquina lo que significa modificar el arranque del dispositivo y acceder a las herramientas sin alterar el estado de la máquina.

6.2.3.2 Linux

Existen múltiples herramientas forenses, aún más para Linux que para cualquier sistema operativo, que por su facilidad de ser de código abierto permite su fácil adaptabilidad a las necesidades del peritaje en cada caso concreto.

Expertos aseguran que Linux es la mejor opción para construir entornos específicos para el análisis forense que pueden ser iniciados desde discos externos (LIVE CD) o en máquinas virtuales. De esta manera permite utilizar las herramientas para extraer y analizar las evidencias procedentes de otros sistemas operativos.

Entre sus mayores ventajas se encuentra que al ser de libre distribución supone un ahorro para los peritos la hace compatible con muchos de los sistemas analizados. Adicionalmente existen multitud de distribuciones que proporcionan conjuntos de herramientas forenses listas para usar,

usualmente en LIVE CD lo que permite acceder a los sistemas a analizar sin modificar el contenido del mismo.

Sin embargo, también presenta desventajas y dificultades, siendo la principal de todo el reto que significa usar y configurar estas herramientas en el ambiente de Linux. Por otra parte, ya que es menos conocido puede generar inseguridad entre los agentes legales frente a una investigación. No obstante, es un sistema que ofrece varias utilidades nativas que permite hacer la recopilación de evidencia sin alterar, por accidente, la información con la instalación de herramientas externas. Es el caso del comando "dd" (Dataset Definition) [56] el cual permite la creación bit a bit de particiones del disco o del disco completo. El uso de este comando es simple, sin embargo, existen varias consideraciones a tener en cuenta; Lo primero es conocer las particiones / discos duros que tiene el sistema, algo que se puede conocer fácilmente con el comando "sudo fdisk -l" [57] o con algún programa gráfico de particiones como gparted, pero esto último es poco recomendable, pues podría alterar los registros del dispositivo. Aunque no es un comando difícil de usar y su información se puede consultar con el comando "man dd" e "info dd", se recomienda usarlo con precaución pues, así como copia la información de un disco, así mismo la puede eliminar si se usa una instrucción mal.

Otra consideración a tener en cuenta, es que, por ser un comando reservado, no es posible visualizar su proceso de ejecución por lo que muchas veces se usa acompañado del comando "pv" que permite obtener en el terminal una especie de barra de progreso, la información sobre bytes transferidos, el tiempo que lleva ejecutándose y la tasa de transferencia, todo esto en tiempo real.

Otros comandos de interés nativos que ofrece linux son "uname -a" y "lsb_release -a" nos mostrarán las principales características del sistema, como pueden ser la versión de kernel y la distribución del sistema operativo. Por otra parte, como se mencionó de manera sutil anteriormente el comando "fdisk -lu /dev/sda" permitirá obtener las diferentes particiones existentes en el disco duro /dev/sda, así como los sectores de inicio y fin de cada una de ellas. Esto también nos servirá para comprobar el *hash* de las imágenes de cada partición en caso de ser necesario

Básicamente linux, permite desde su propio sistema por medio de comandos obtener información y pues más allá de las prestaciones que pueda ofrecer una herramienta implementada en el mismo sistema operativo, muchas veces será más útil y eficaz hacerlo directamente.

6.2.3.2.1 Experimento

Al igual que en investigaciones anteriores, lo primero a tener en cuenta es verificar el estado de la máquina, en caso de que se encuentre apagada, será útil el uso de herramientas como deft o Helix en modo boot.

Por otra parte, si la máquina se encuentra encendida lo primero a hacer es realizar el volcado de memoria o la copia bit a bit del disco, que como se mencionó con anterioridad se puede realizar usando el comando dd.

Sin embargo, antes de recopilar la evidencia de memoria es necesario obtener información sobre el disco y sus particiones. Para lo que se usa el comando fdisk .

Para listar todas las particiones existentes en nuestro sistema pasaremos el argumento "-l", que hará que se listen ordenadas por el nombre del dispositivo esto se puede apreciar en la figura 26.

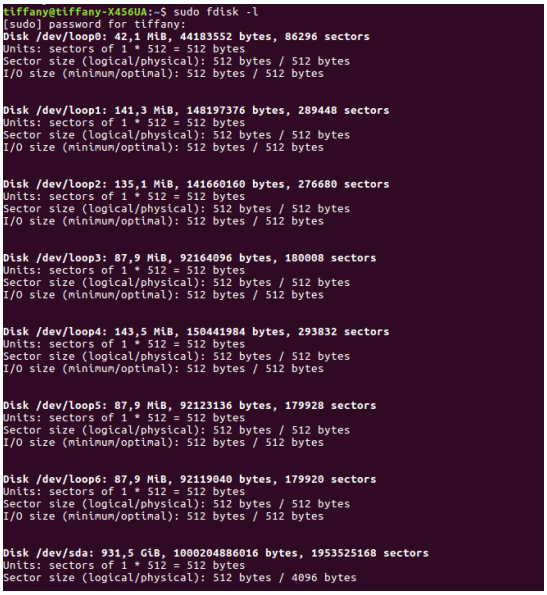


Fig. 26 Listado de Particiones

Para efectos de la investigación, no basta con mostrarlo en pantalla por lo que será necesario guardar el resultado en un archivo, lo que se puede hacer fácilmente con el comando de la figura 27:

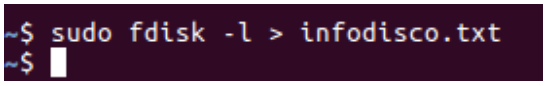


Fig. 27 particiones guardadas en un archivo

Esto creará el archivo "infodisco.txt" en la carpeta en la que estamos ubicados por defecto, donde el archivo contendrá la misma información mostrada en pantalla.
Cabe resaltar que el comando fdisk tiene muchas más utilidades, que, aunque son de gran importancia y utilidad, no se ejecutaron en la realización de este experimento.

Conociendo el disco y sus particiones, es posible realizar la copia (clonación de disco) bit a bit con el comando dd, mediante la instrucción "*# dd if=/dev/sdx of=/dev/sdy bs=1M "*

Donde if significa "input file=archivo de entrada ", es decir, lo que se quiere copiar y of significa "output file=archivo de salida ", o sea, el archivo destino (donde se van a copiar los datos); origen y destino pueden ser dispositivos (lectora de CD o DVD, disco duro,usb, partición, etc.), archivo de copia de seguridad o imagen de disco, etc, pero no carpetas o subcarpetas.

Cómo se explicó anteriormente, el comando es "ciego" por lo que no permite ver el progreso del proceso, para que esto sea posible se agrega un comando adicional, obteniendo como resultado una instrucción de la siguiente forma: "*# dd if=/dev/sdx |pv| of=/dev/sdy bs=1M "* como se observa en la figura 28.

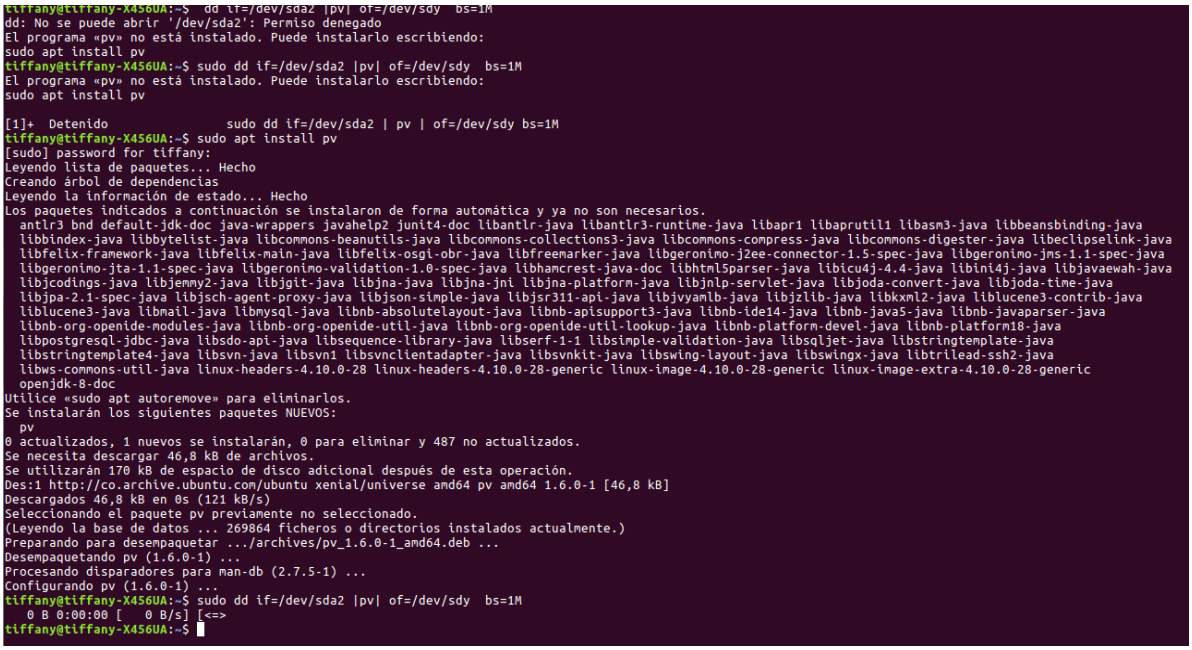


Fig. 28 visualizacion del proceso

En el experimento, se puede observar que el comando pv permite ver una barra de progreso de la copia. Así como para que esto sea posible, fue necesario instalar la instrucción pv, lo cual sería un riesgo a cambiar la información recolectada.

Otra información importante y fácil de recuperar por medio de los comandos de Linux son los procesos que corren en el momento de realizar la investigación. Para esto será necesario usar el comando “Ps” que permitirá visualizar todos los procesos que corren, de igual manera, si se quiere guardar esta información en un archivo de texto bastará con añadir “>procesos.txt” por lo que el comando completo sería como aparece en la figura 29: “*#ps -aux > procesos.txt”*

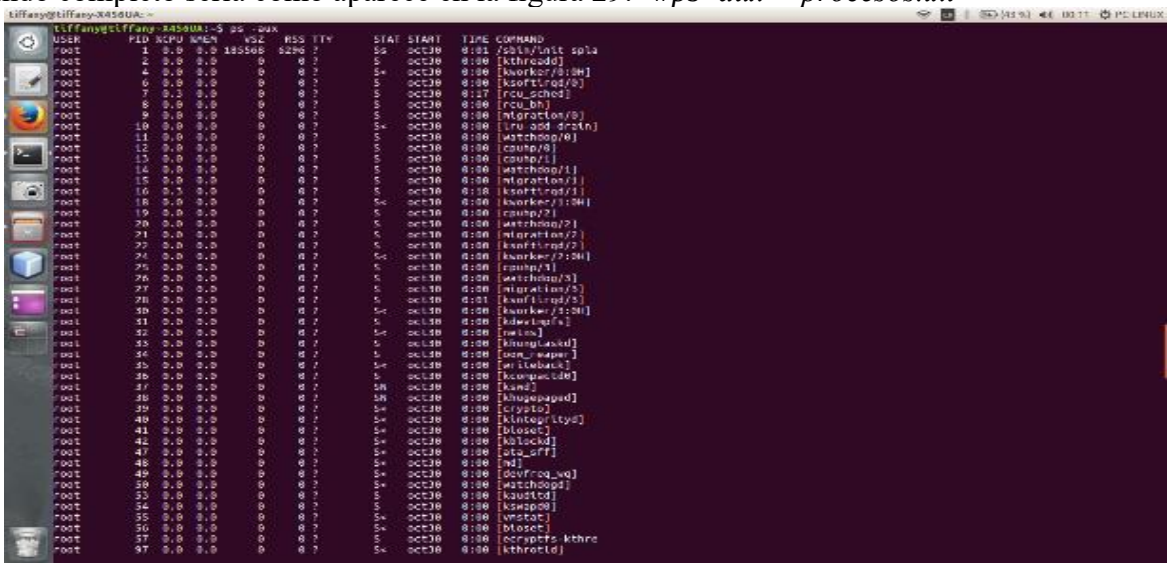


Fig. 29 Procesos

Este comando permitirá no solo visualizar los resultados sino guardarlos en un archivo para su posterior análisis como se muestra en la figura 30 .

```
ps -aux > procesos.txt
```

Fig. 30 comando de procesos

Obteniendo un archivo de texto con la misma información mostrada en terminal. Otro comando importante que nos ayudará en todo este proceso de la recopilación de información es "top" la cual nos ayuda a conocer los procesos de ejecución del sistema en tiempo real que se va a ir actualizando cada 3 segundos. Muestra un resumen del estado de nuestro sistema y la lista de procesos que se están ejecutando esto se puede ver en la figura 31.

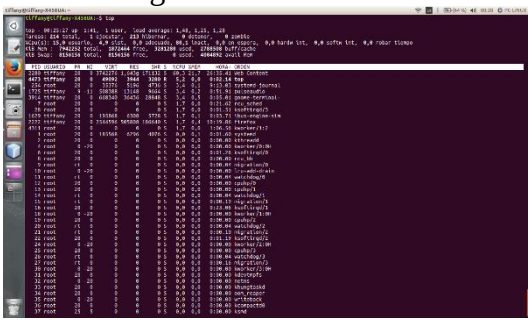


Fig. 31 Resumen de estado del sistema

Aunque es posible enviar esta información a un archivo de la misma manera que se ha hecho con los otros comandos, el archivo resultante no es del todo claro y su lectura es casi imposible. Además del hecho, que, por actualizarse cada 3 segundos, la copia al archivo podría nunca terminar y es necesario cancelarla para poder continuar. Sin embargo, es posible realizar el análisis con la información mostrada en pantalla de la figura 32:

```
top - 00:25:27 up  1:41,  1 user,  load average: 1,48, 1,25, 1,28
```

Fig. 32 Comando Top

En la primera línea es posible observar la hora actual,el tiempo que ha estado el sistema encendido, el número de usuarios y la carga media en intervalos de 5, 10 y 15 minutos respectivamente como se aprecia en la figura 33.

Fig. 33 Resultado comando top

La segunda línea muestra el total de tareas y procesos, los cuales pueden estar en diferentes estados: *ejecutar* son los procesos ejecutándose actualmente o preparados para ejecutarse, *hibernar* son procesos dormidos esperando para ejecutarse, *detener* ejecución de proceso detenida y *zombie*: el proceso no está siendo ejecutado. Son procesos se quedan en este estado cuando el proceso que los ha iniciado muere. Toda esta informacion se muestra en la figura 34.

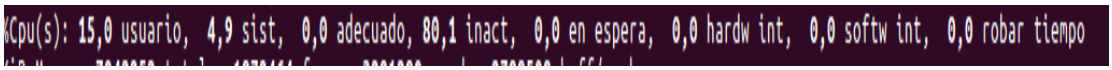


Fig. 34 Resultado comando top

Por otra parte, la tercera línea muestra los porcentajes de uso del procesador diferenciado por el uso que se le dé, donde *us* refiere al tiempo de CPU de usuario mientras que *sy* el tiempo de CPU del kernel, como se aprecia en la imagen 35.

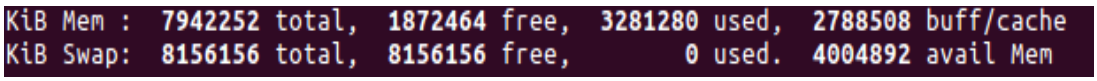


Fig. 35 Resultado comando top

Las dos últimas líneas hacen referencia al uso de memoria, tanto física como virtual. Las siguientes líneas de columnas son aún más sencillas de interpretar, sin embargo, si se considera necesitar más información al respecto solo debe usar el comando “man top”.

Finalmente, los últimos, pero no menos importante comando utilizado en la investigación fue “w” de la figura 36 y “last” de la figura 37, que hacen relación a los usuarios y accesos al sistema respectivamente. Por una parte “w” muestra qué usuarios están en nuestro sistema, y qué están ejecutando.

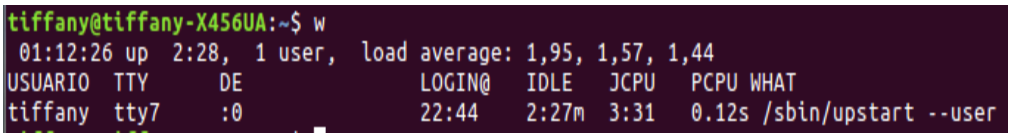


Fig. 36 W comando

Por otro lado, el comando “last” muestra un listado con los últimos accesos (login) al sistema.

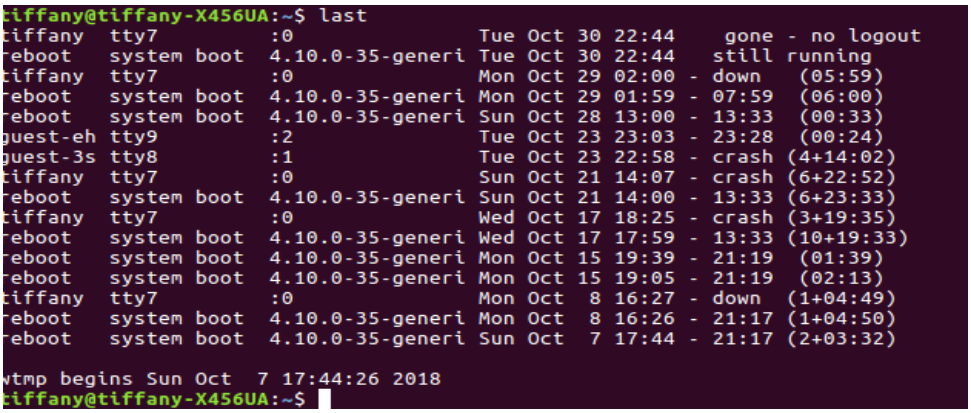


Fig. 37 Last comando

6.2.3.3 Mac OS

Muchas veces se ha escuchado decir que MacOS es muy seguro por no ser constantemente atacado por los ciberdelincuentes, sin embargo, no es del todo cierto pues, aunque el uso y acceso al sistema operativo es bastante complejo, en los últimos años se ha evidenciado el gran aumento de ataques a estos sistemas operativos. Es por esto que MacOS requiere una metodología única y especial para investigar ataques en sistemas de Apple, no obstante, las técnicas y herramientas forenses son muy escasas para este sistema.

Esto no quiere decir que hacer forensia en sistemas MacOS sea imposible, pues al igual que con Linux y Windows, solo se requiere el conocimiento básico del tipo de archivos y extensiones que maneja, con el fin de conocer dónde buscar y qué clase de información buscar.

Por otra parte, esta tarea se facilita aún más si el perito que realiza la investigación tiene conocimiento previo del sistema, pues no representará ningún problema al momento de ejecutar las herramientas forenses o en caso de ser necesario, ejecutar las herramientas desde arranque de la máquina.

6.2.3.3.1 Experimento

Para el caso de este experimento se usó una máquina con sistema operativo MAC con sistema operativo El capitán (10.11.3) del laboratorio de informática en la Escuela Colombiana de Ingeniería Julio Garavito.

Para este caso, se usó una de las herramientas más recomendadas por expertos para Mac que es Pac4Mac de código libre y fácil ejecución.

Esta herramienta se descarga directamente desde GitHub y contiene herramientas Python, las cuales basta con ejecutarlas desde la terminal para usarlas como se muestra en la figura.

Fig. 38 Ejecución de Pac4Mac

Aunque la herramienta indicaba que el sistema operativo no era compatible, esto no fue impedimento para permitir su uso. Las opciones que despliega hacen referencia al volcado de memoria sobre el equipo, por lo que es lo primero que se ejecuta.

El resultado de esto, es una carpeta llamada “Results” como se observa en la figura 39, donde se encuentra el volcado de la memoria y logs del sistema operativo. Presentado en diferentes carpetas, dentro de la cual se encuentra la información recuperada.

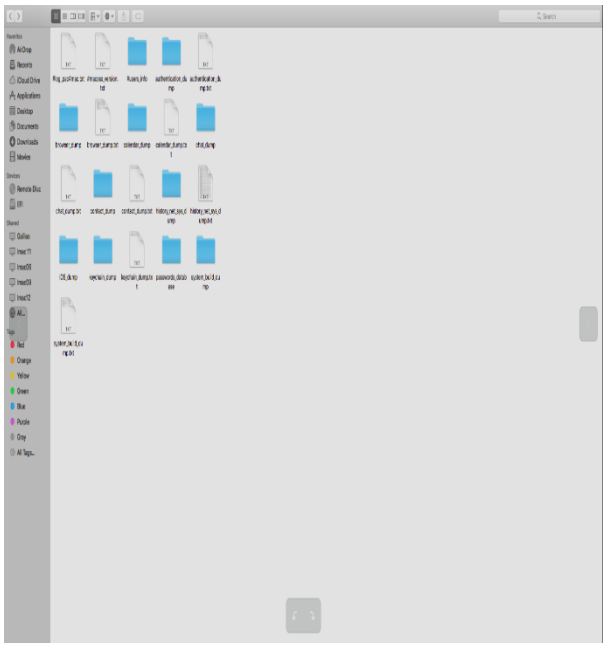


Fig. 39 Resultado ejecucion

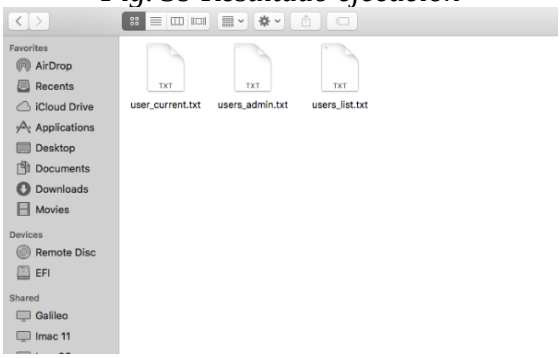


Fig. 40 Archivos Obtenidos

Se puede observar que la mayoría de los archivos recuperados son en el formato propio del sistema. plist. Acompañado de un archivo en .txt que indica la información recuperada.

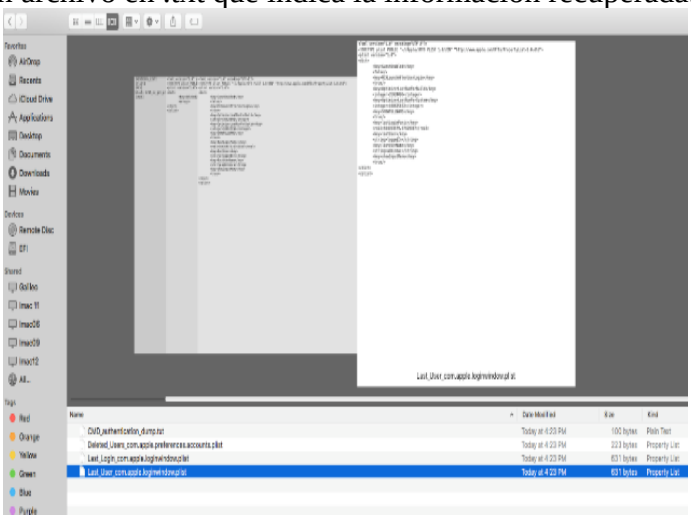


Fig. 41 Información recuperada

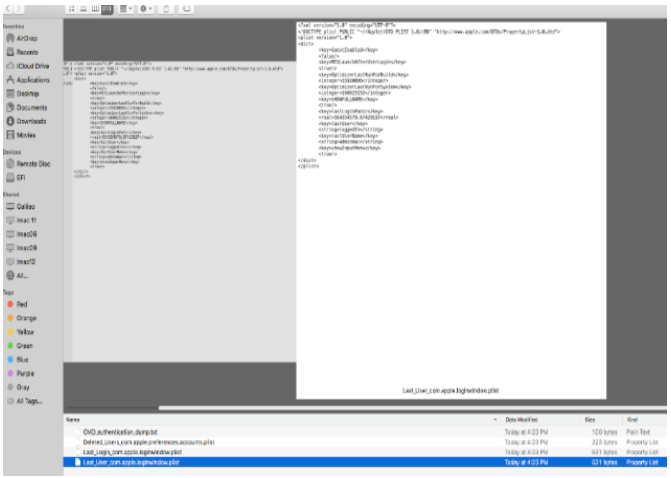


Fig. 42 Información recuperada

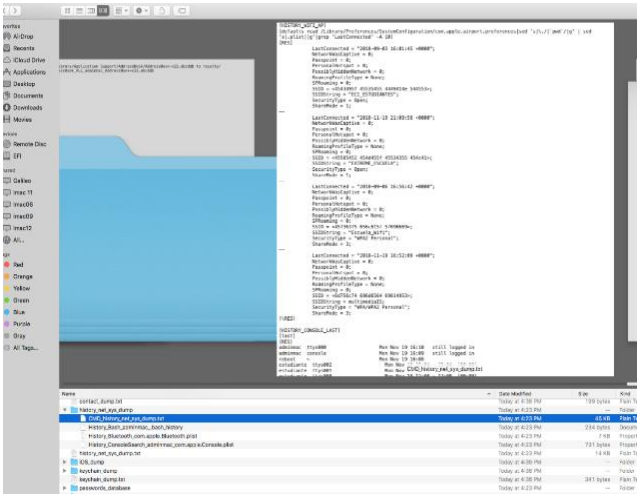


Fig. 43 Informacion recuperada

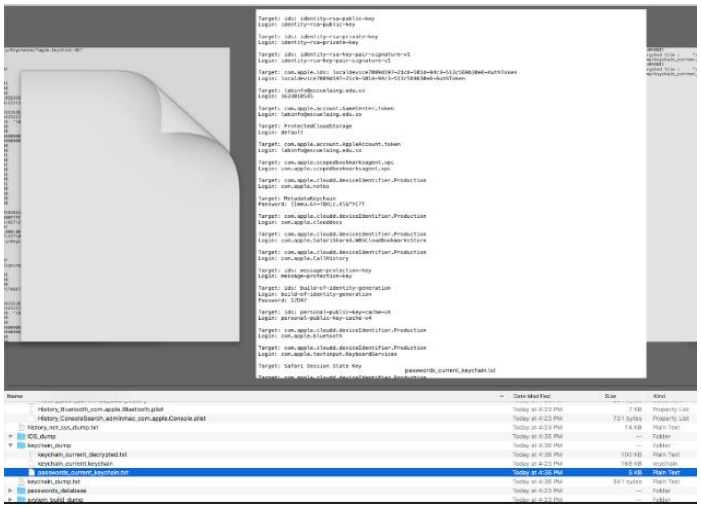


Fig. 44 Informacion recuerada

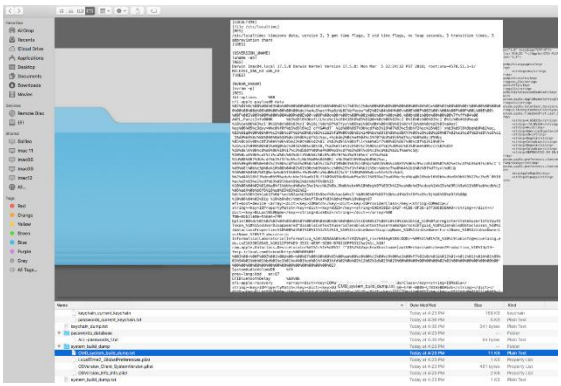


Fig. 45 Informacion recuperada

Fig. 46 Informacion recuperada

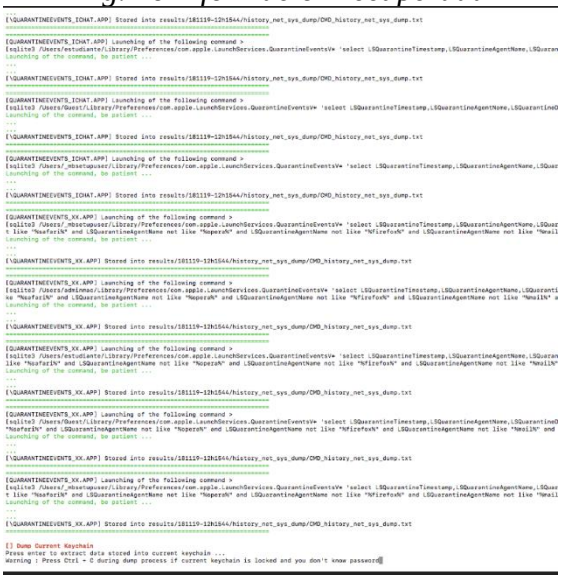


Fig. 47 Informacion recuperada

6.2.3.4 Dispositivos moviles

Ya que el dispositivo móvil hace es una parte importante en nuestra vida diaria, el enfoque de recopilación de evidencia digital no se puede sesgar únicamente a computadores, es necesario pensar también en la navaja suiza digital que representa un dispositivo móvil. Gracias a esto la información que guardan estos dispositivos es muy relevante y en caso de que se cometa algún delito puede llegar a ser de mucha utilidad y esto facilita algunos procesos judiciales, es entonces donde entra en juego el análisis forense de dispositivos móviles y las herramientas que existen a disposición para el objetivo.

Se presume que la información que se puede recopilar de este tipo de dispositivos es mucho más amplia que en un dispositivo convencional, pues se pueden recuperar historiales de llamadas, de mensajes, de emails, de navegación, así como, fotos, videos y en general cualquier tipo de archivo que haya sido almacenado o incluso borrado del dispositivo.
Hay que tener en cuenta que la mayoría de las terminales están bloqueados con algún tipo de patrón o contraseña (incluso aunque sean biométricos, tienen de contraseña de respaldo que permiten acceder al dispositivo) por eso es que lo primero que se debe hacer es tener herramientas que permitan desbloquear la contraseña. Sin embargo, una recomendación general que se hace respecto al punto anterior es clonar el dispositivo en caso de que se llegue al límite de intentos impuesto por el fabricante, de modo que al introducir varias veces la contraseña errónea no se bloquee y destruya la información que contiene.

Pese a que no existe una metodología estándar sobre la manera específica de hacer análisis forense de dispositivos móviles, hay una serie de guías que pueden servir de pauta a seguir para la correcta realización del proceso. Por un lado se encuentra el documento “Guidelines on Mobile Device Forensics” del NIST (National Institute of Standards and Technology) [58] en que habla a nivel general del dispositivo, la estructura de sus archivos, de la memoria, el tipo de conexión a internet que usa, mientras que a nivel de forensia habla de la clasificación de extracción que usan las herramientas disponibles (manual , lógica, JTAG, etc) , además de esto sugieren algunas herramientas y muestran sus utilidades de acuerdo a los niveles de adquisición lo que lo hace un documento con información muy completa a la hora de recopilar evidencia digital .

A la hora de realizar el proceso de extracción existe un número notable de herramientas que se deben tener en consideración. Dependiendo de su funcionamiento interno pueden ser catalogadas de diferentes maneras. Como base para su clasificación se puede utilizar la pirámide propuesta por Sam Brothers en la U.S. Cybercrime Conference de 2011 de la figura 48 [59].

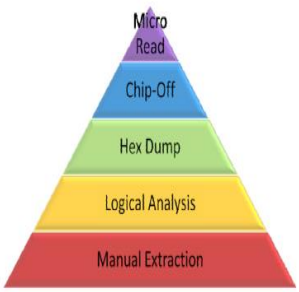


Fig. 48 Piramide de Sam Brohers

Por otro lado se encuentra el documento "Developing Process for Mobile Device Forensics" del SANS que realmente es un poco más general y habla específicamente de la metodología.

Sin embargo, la metodología general en dispositivos móviles no difiere mucho de la tecnología convencional, teniendo de esta forma la preservación, adquisición, análisis, documentación y presentación de la evidencia recopilada en móviles.

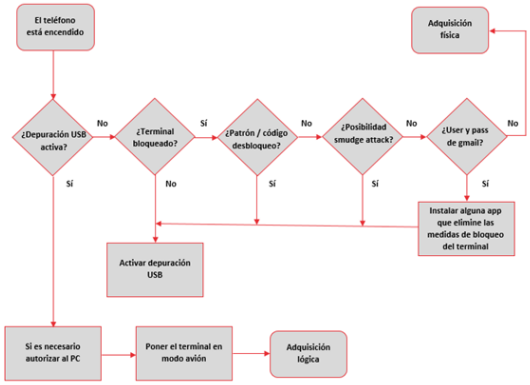


Fig. 49 Modelo de estudio en moviles

A la hora de seleccionar el método más adecuado, se tienen en cuenta multitud de aspectos como por ejemplo: el nivel de exhaustividad requerido, la limitación de tiempo para realizar el proceso, qué tipo de información es necesario obtener: información volátil, información que ha sido previamente eliminada, información de aplicaciones de terceros, etc.

Para poder seleccionar de la forma más adecuada se recomiendan algunas pautas, destacando diferentes aspectos necesarios como tener en cuenta si la depuración del USB está activa, si el dispositivo se encuentra bloqueado o tenemos acceso al mismo, entre otros:

Métodos para analizar dispositivos móviles:

- El teléfono está encendido.
- ¿Está la depuración del USB encendida?
    - No. ¿Está el terminal bloqueado?
        - Sí, sin posibilidad de desbloquearlo: Utilizar el método de adquisición física.
        - No: Activar depuración USB.

Sí, es necesario autorizar al PC: poner el dispositivo en modo avión y utilizar el método de adquisición lógica.

6.2.3.4.1 Android

Se hace uso de un celular Samsung J5 Prime sin permisos de root o bootloader. Haciendo uso del santoku con el celular conectado y habilitado a depuración por usb se hace uso herramienta AF logical OSE, el que desde la terminal permite recuperar llamadas, mensajes de texto, numeros de celular guardados. En caso de no reconocer el dispositivo se debe revisar que la depuración por usb está activa .

Fig. 50 Santoku

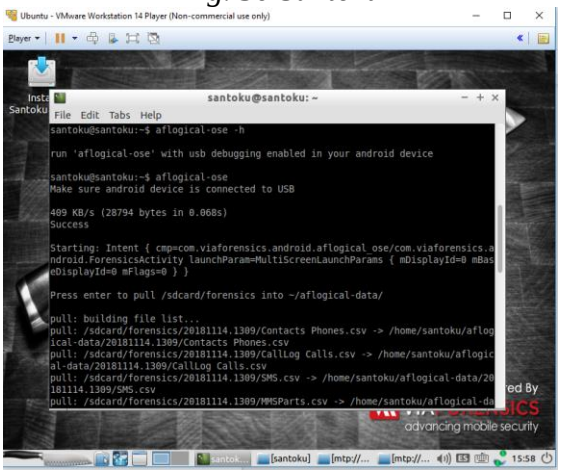


Fig. 51 Ejecución herramienta

Esta herramienta ejecutará una apk en el cellular que permite recolectar la informacion del equipo y almacena la informacion recolectada en el computador como se observa en la figura 52.

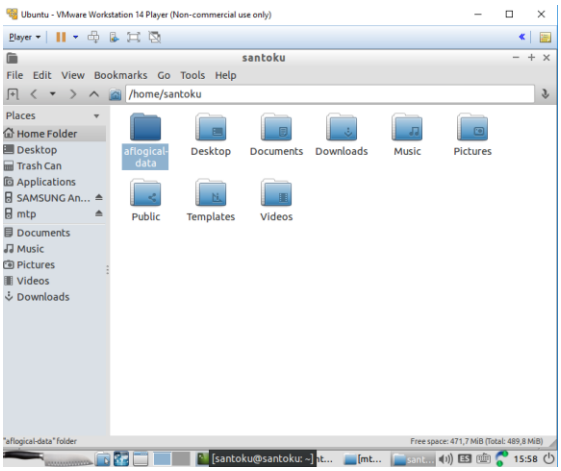


Fig. 52 Resultado de ejecucion

Dentro de la cual se encuentra informacion sobre llamadas y mensajes de texto asi como los contactos almacenados en la memoria del equipo como se muestra en la figura 53.

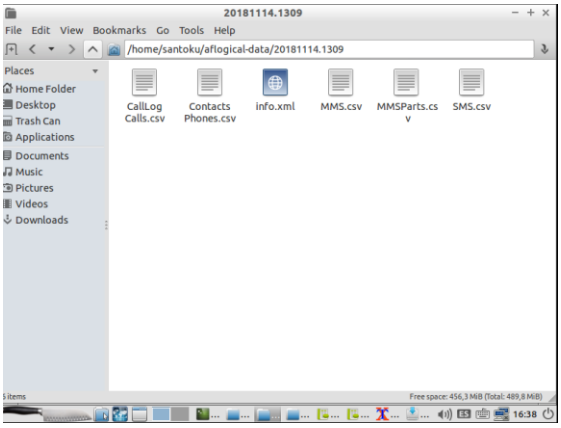


Fig. 53 Resultado Obtenido

Cada uno de los archivos generados muestra informacion en texto plano , sobre llamadas, contactos y mensajes recientes que permiten rastrear la actividad del objetivo , todo esto se muestra en las figuras 54, 55,56.

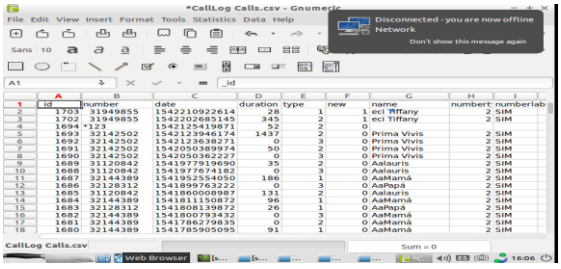


Fig. 54 Listado de llamadas

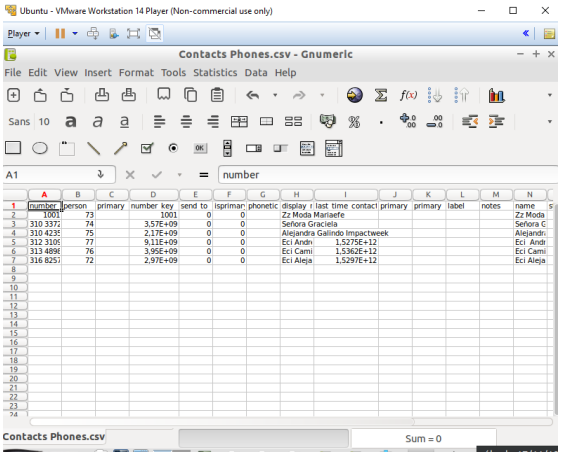


Fig. 55 Listado Mensajes

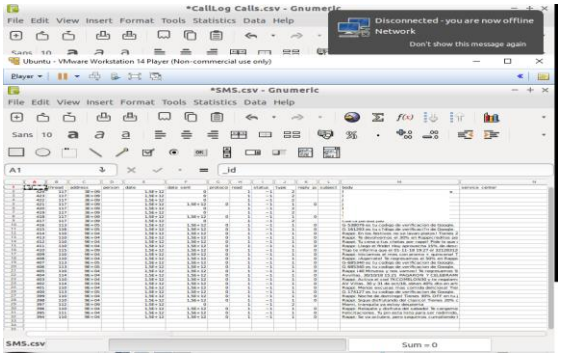


Fig. 56 Listado mensajes

6.2.3.5 Retos y conclusiones

Son muchas las recomendaciones a tener en cuenta en el momento de realizar una recopilación de evidencia en los componentes de memoria, sin embargo, la principal de todas es tener muy en cuenta el sistema operativo al que se enfrenta.

Teniendo esto en mente, se puede decir que Windows no constituye gran reto para un perito al momento de realizar una recopilación de evidencia, pues por ser un SO tan popular se encuentra amplia variedad, de todos los colores y sabores, de herramientas que permiten realizar la tarea de recuperar la información. Herramientas que además de ser de gran utilidad y confiabilidad, son ampliamente reconocidas por la parte legal del tema, dándole de esta forma mayor fiabilidad a la evidencia recolectada.

Por otra parte, los sistemas operativos Linux por ser de baja demanda entre los usuarios comunes, son aprovechados ampliamente por los hackers, lo que representa ventajas y desventajas por igual para el perito. Esto a causa de que la mayoría de herramientas se encuentran desarrolladas en base a linux, lo que permite obtener más fácilmente la evidencia, no obstante, de la misma manera es posible borrar el rastro completamente del sistema haciendo más complicado el trabajo del perito y llevando a que frente a una corte, las pruebas no puedan tener tanta validez como es requerido.

Finalmente, para el caso de Mac OS, cabe destacar que no es nada fácil su manejo como sistema operativo y esto dificulta el uso de las pocas herramientas existentes para el peritaje, por lo que podría considerarse de los mayores retos enfrentados en esta investigación.

Dado que la investigación en su mayoría se llevó a cabo en los laboratorios de informática de la Escuela Colombiana de Ingeniería Julio Garavito, representó un gran reto el enfrentarse a la hardenizacion que estos equipos tenían, lo que impedía el uso de las herramientas y nos hizo recurrir a investigar mucho más con el fin de encontrar aquellas brechas de seguridad que nos permitieran usar las herramientas necesarias para la recopilación de la información.

Así pues de esta parte de la investigación fue posible generar un artículo titulado "La importancia de la memoria como evidencia digital en la informática forense" publicado en la conferencia LACCEI 2019 y que tiene como resumen la figura 57.

Resumen- ***La presente investigación plantea la importancia que tiene la relación entre la memoria y la gestión de evidencia digital frente a una indagación forense, mediante el análisis de técnicas, metodologías y herramientas que permiten hacer la recopilación forense de la información en este componente disponible en cada dispositivo. Considerando los diferentes factores que deben tenerse en cuenta, así como los tipos de memoria existentes, para de esta manera llegar a la conclusión de su importancia frente a los procesos legales y escenarios forenses en los que se analizan.***

Palabras Clave - forense, memoria, evidencia, información

Fig. 57 La importancia de la memoria como evidencia digital en la informatica forense

6.3 Ossim

En la actualidad la seguridad informática está en auge, y gracias a eso se han creado grandes plataformas otorgando la disponibilidad de conectarse entre redes y es por esto que es importante contar con una herramienta para visualizar en tiempo real el funcionamiento de la red y poder verificar las anomalías generadas por usuarios o atacantes a la red y los servidores. Es por esto que se necesita una herramienta que colabore a la toma de decisiones de manera oportuna para favorecer y mantener el correcto funcionamiento de la organización.

Por ello existen múltiples herramientas para ayudar en la administración y la gestión de eventos de seguridad mediante un motor de correlación y una herramienta open source o paga creadas para tener a la vista de aspectos relativos a la seguridad y la infraestructura. Bajo esta premisa, la Escuela Colombiana de Ingeniería Julio Garavito maneja Open Source Security Information Management o en español Herramienta de Código Abierto para la Gestión de Seguridad de la información la cual es comúnmente conocida como **OSSIM**, esta máquina provee una máquina de correlación con distintos niveles de interfaces, reportes y herramientas para el manejo de incidentes [60].

Esta herramienta actúa como un Sistema para prevención de intrusos, realizando filtros en la red para tener exclusivamente la información requerida por el usuario en cuestión. Cuenta con numerosos elementos, como lo son ***Short*** que es un Sistema de detección de intrusos, ***Spade*** utilizado para la detectar anomalías en los paquetes e identificar paquetes sin firma, ***Arpwatch*** que es utilizado para detectar las anomalías en las direcciones MAC, ***Openvas*** para la evaluación del sistema de detección de intrusos y el Escáner de Vulnerabilidad, ***Tcptrack*** para conocer información de las sesiones, ***Ntop*** el cual construye una impresionante base de datos con la información de la red para la detección de cambios en el comportamiento, ***Nagios***, utilizado para monitorear la disponibilidad de los hosts y de los servicios. ***nfSen*** encargado de la visualización de los flujos de red para la detección de anomalías de red, ***Osiris*** y ***OSEC*** son sistemas de detección de intrusos basados en host, Snare, colecciona los logs en Windows. Aparte de estas, OSSIM maneja sus propias herramientas logrando ser el motor más importante de correlación brindando soporte e integridad a los logs con plugins [61] [62].

6.3.1 Herramientas

OSSIM es un conjunto que integra diversas herramientas unidas en un solo programa para el análisis, visualización y gestión de los eventos que ocurren en la organización.

Esta herramienta maneja dos tipos de herramientas, las activas y las pasivas y cada una de ellas maneja respectivamente:

6.3.1.1 Pasivas

- ***Snort*** encargado de analizar en tráfico de red mediante el uso de firmas generando eventos de seguridad, realza escaneo de puertos, gusanos, malware, violaciones de política como P2P, mensajería, pornografía entre otros.
- ***Ntop*** es un monitor de red y de uso que analiza el tráfico de red ofreciendo datos en tiempo real en forma de estadísticas, matrices de tiempo y actividad, también brinda información sobre los activos como las sesiones y la detección de alteración de la red.
- ***NFSen*** su función es recolectar y procesar los datos mediante comandos, permitiendo la visualización y la gestión de lo recolectado.
- ***Kismet*** funciona como un sniffer y un detector de intrusos en redes Wireless, cuenta con distintos rangos para rastrear tráfico, cumpliendo con la normativa PCI.
- ***P0f***, su función es la detección de anomalías en el sistema operativo mediante un análisis de tráfico por los activos de la red, detectando cambios en el sistema operativo, realizando gestión de inventario y revisando los accesos no autorizados a la red.
- ***Pads*** encargado de la detección de anomalías en los servicios a partir del análisis de tráfico generado por los activos, realizando la gestión de inventario, detectando cambio en los servicios y violaciones de las políticas.
- ***Arpwatch*** verifica y encuentra las discrepancias en las direcciones MAC mediante el análisis de tráfico de red de los activos, identificando cambios en las direcciones asociadas a cada dirección IP.

- ***Tcptrack*** realiza el monitoreo de las sesiones mostrando información sobre las conexiones TCP que se encuentran activas en la red mostrando cosas como la duración de la conexión y los datos transferidos.
- ***Nepenthes*** es el encargado de emular los servicios y las vulnerabilidades para recolectar la información de los atacantes, cosas como los patrones de ataque, ficheros, entre otros. Entre sus funciones está la de conocer los equipos infectados, la creación de firmas según los ataques identificados y la colección de malware.

6.3.1.2 Activas

- ***OCS***, esta herramienta es utilizada para la gestión del inventario, realizando inventario para hardware y software, también realiza búsquedas que tengan violaciones de las políticas con gestión de vulnerabilidades y un control de hardware.
- ***Nagios*** es un motor de disponibilidad encargado de monitorear la disponibilidad de los activos y servicios ya sea mediante la comprobación del puerto de que MySQL está levantado, verificar que si se está escuchando un servidor MySQL o mediante la realización de una consulta al servidor y su respectiva comprobación.
- ***OpenVas*** su función principal es el escaneo de vulnerabilidades mediante una serie de firmas para prevenir los ataques, brindando la posibilidad de realizar los escaneos de forma remota.
- ***OSVDB*** es una base de datos que almacena las vulnerabilidades, entre sus funciones está la creación de reglas de correlación y relacionar los identificadores de cada vulnerabilidad.
- ***OSSEC*** se encarga de analizar los logs y comprobar la integridad del sistema, como también monitorear el registro y la detección de sistemas rootkit, toda su función es a nivel de host, sus principales funciones son la recolección de eventos en sistemas Windows y Unix, recolección de eventos de aplicaciones y la monitorización de carpetas, ficheros y registros.
- ***Nmap*** es el encargado del escáner de los puertos, la realización del escaneo permite realizar configuraciones de elementos como la precisión, la velocidad o el grado de intrusión. Descubre activos, identifica puertos abiertos y determina qué sistema operativo se está utilizando junto con los servicios que se están ejecutando.

6.3.2 Secciones

La interfaz OSSIM cuenta con 5 ventanas, Dashboards, Analysis, Environment, Reports y configuration, cada una de ellas maneja herramientas especializadas para el monitoreo de red, escaneo de vulnerabilidades, generación de reportes, entre otros.

6.3.2.1 Tableros

Es el primer menú que aparece cuando ingresamos al sistema, en esta sección se realiza el monitoreo y análisis de la seguridad mostrando de manera general las actividades y métricas de la red, también cuenta con espacio para conocer el estado de la implementación, observar mapas de riesgo y OTX para visualizar las amenazas de forma gráfica, con una interfaz como se puede observar en la figura58 y la figura59 [63] [64].

6.3.2.2 Análisis

En este menú se encuentran servicios para analizar la seguridad de la red como alarmas, eventos de seguridad(SIEM), registros sin procesar y tickets. cada uno de ellos muestra un seguimiento de los eventos junto con un reporte detallado.

6.3.2.3 Ambientes

En este menú encontramos opciones como assets & groups, vulnerabilities, netflow, traffic capture, availability, detection, donde podemos realizar cosas como encontrar los activos que están conectados al sistema, conocer las vulnerabilidades que han tenido los host, capturar el tráfico de la red, etc.

6.3.2.4 Reportes

En esta sección podemos encontrar todos los informes de alarmas, detalles de los activos, disponibilidad, geográfico, eventos SIEM, base de datos y vulnerabilidades, estado de las entradas, actividad de todos o de cada usuario, entre otros.

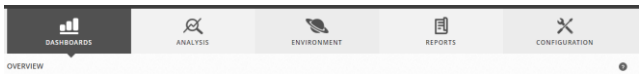


Fig. 58

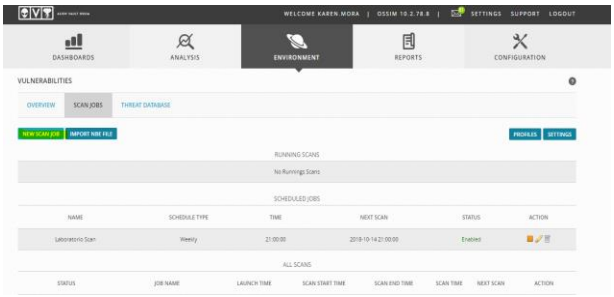


Fig. 59

6.3.3 Actividad

Respecto a la implementación realizaremos un escaneo de red y para ello ingresamos en ambientes, vulnerabilidades y click en nuevo trabajo de escaneo. Solo puede ejecutar hasta 5 exploraciones simultáneas, teniendo en cuenta el perfil que se usa (defecto, profundo y último) para este informe se decide usar el perfil por defecto, que es completo, pero no destructivo. Así mismo, se usa el método de programación, tiene múltiples formas de programación, pero para efectos de la investigación se usa de tipo inmediato. En configuraciones avanzadas se habilita el envío de correo electrónico, al usuario. Se seleccionaron las direcciones ip a escanear, disponibles dentro de una lista generada automáticamente como se observa en las figuras 60 y 61.

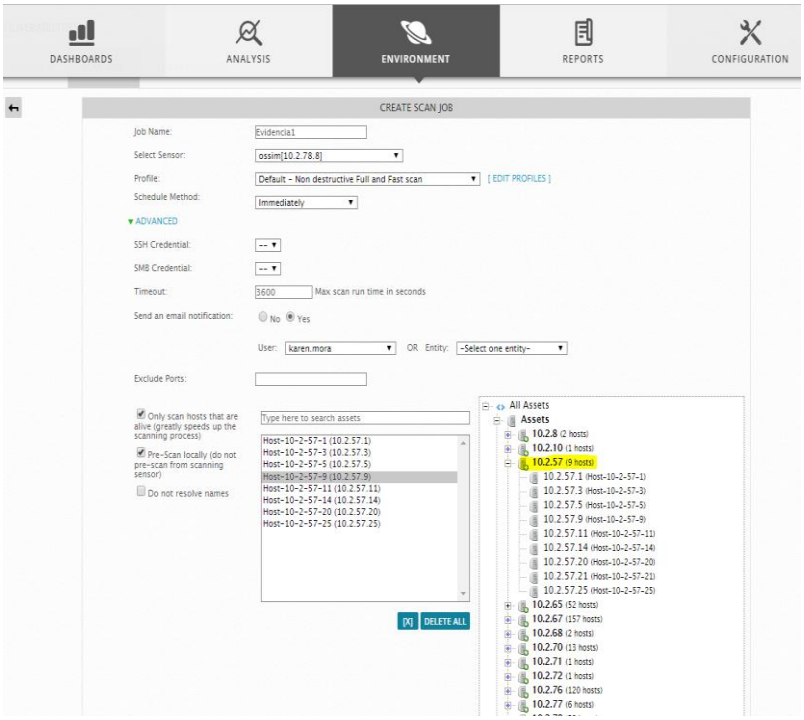


Fig. 60

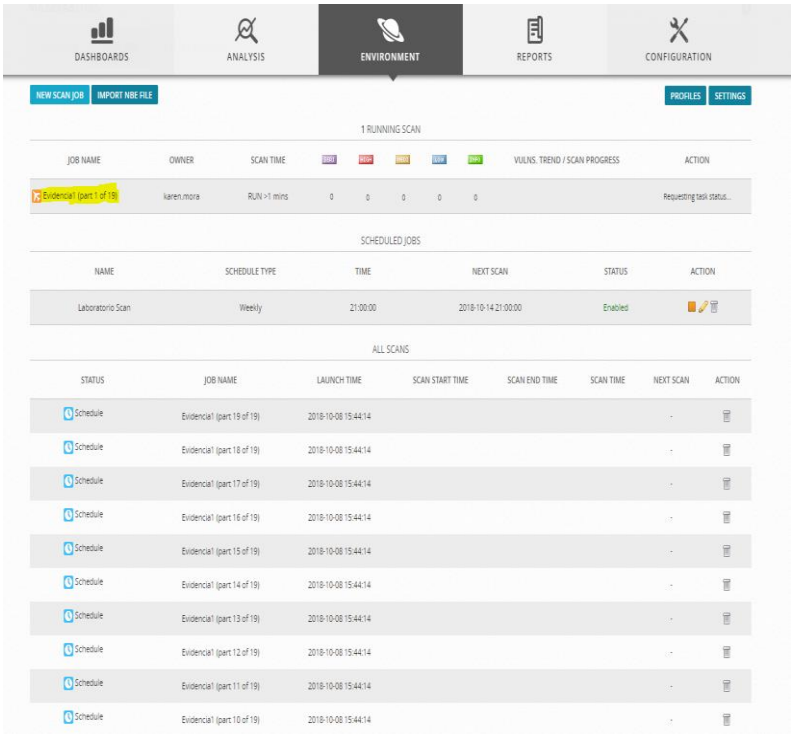


Fig. 61

La realización del escaneo tiene como finalidad encontrar si hay cambios en los hosts, en los servicios del sistema operativo pero al final no obtenemos el reporte ni respuesta del escaneo

realizado por ende procedemos a averiguar qué pasa. para nuestra sorpresa el poder tener los logs debemos tener la máquina paga USM [65] [66].

6.3.4 Conclusión y reporte final

Se realizaron búsquedas para poder acceder a la gestión de forensia digital que ofrece alienvault pero culminando sin éxito ya que toda esa parte es paga y sólo es ofrecida por la máquina SIN anywhere, nos colocamos en contacto con ellos para ver si había alguna posibilidad de obtener una versión free de la gestión para manejarla en la máquina y conocer su funcionamiento, lo cual fue imposible de acuerdo a las políticas de las empresa.

Es una lástima no poder observar cómo funciona la parte forense de alienVault pero obtuvimos un completo acompañamiento de la compañía para el proceso de buscar una solución. OSSIM es una máquina impresionante que ayuda a jerarquizada las vulnerabilidades y ataques del sistema y aunque maneja alarmas no es suficiente para obtener un análisis forense.

para concluir con la parte de OSSIM podemos decir que es una máquina impresionante que ayuda a jerarquizada las vulnerabilidades y ataques del sistema y aunque maneja alarmas no es suficiente para obtener un análisis forense. También tiene un análisis de vulnerabilidades con distintos filtros para conocer qué clase de ataques está recibiendo la empresa y aprender a reaccionar ante ellos.

6.4 Red Forense

En cuanto a la sección de red tenemos una rama completa llamada red forense encargada de monitorear la red mediante la ayuda de kits o herramientas para recolectar, analizar, correlacionar datos y generar informes que sean admisibles en los juzgados.

la forensia en redes es la rama de la informática forense encarga de capturar, registrar y analizar los eventos de la red para descubrir los atacantes, fallos en seguridad o incidentes, la cual debe recolectar la información necesaria para ser presentarda como evidencia legal o para detección de intrusos o vulnerabilidades en un hogar o lugar de trabajo.

El monitoreo en redes se realiza para detectar anomalías o modificaciones y poder conocer el tipo de ataque generado como también trazar la ruta de este mediante los rastros que se capturen en el momento, mediante la captura, preservación y análisis de datos [67].

Este análisis contiene distintas actividades que se realizan según la evidencia encontrada y el tipo de investigación que se debe realizar, algunas de las actividades son

- Reensamblar paquetes
- Extraer contenido del tráfico
- Examinar flujo de tráfico
- Inspeccionar encabezados de paquetes

La información que recolecta esta rama es la volátil y dinámica ya que circula por internet de manera muy rápida lo que causa que la información se pierda de manera eficaz después de que se transmite, o el dispositivo deja de recibir impulsos eléctricos es por ello que una de las técnicas en realizar un monitoreo constante para evitar la pérdida de información porque generalmente los incidentes se descubren después de que ya lo realizaron y si no se almacena la información es probable que se pierda información importante de quien realizo el ataque y que hizo, entre otras cosas.

La forensia en redes analiza el historial de tráfico de datos para investigar los ataques a la seguridad, reconstruyendo en secuencia las evidencias recopiladas, permitiendo de esta forma recuperar mensajes, el tráfico de la red, correos electrónicos y demás información, mediante la recolección de los paquetes de datos.

El análisis de red utiliza distintas técnicas como lo son los mensajes de alera de los IDS, examinar los eventos de una alarma, examinar el encabezado de los protocolos de un paquete, determinar si el evento es un virus, escaneo, etc.

6.4.1 Tipos

Los tipos de forensia en la red son Catch-it-as-you-can-system y Stop,look and listen que tienen como finalidad ayudar a encontrar la fuente del ataque.

6.4.1.1 Catch-it-as-you-can-system

El cual es utilizado en el momento que ocurre el ataque, por eso requiere de gran espacio para almacenar toda la información del sistema, ya que se deben capturar todos los paquetes que pasen por ese punto del tráfico y ser escritos en algún medio para posteriormente analizarlos.

6.4.1.2 Stop,look and listen

Esta técnica se basa en realizar un monitoreo constante de la red y sólo se captura cierta información la cual es almacenada para un análisis futuro, por tanto no requiere tanto almacenamiento pero si requiere un procesador más veloz para no perder paquetes.

Gracias a la realización de estas técnicas podemos conocer el momento en el que el atacante ingresó al sistema, como también la duración y el protocolo usado para ingresar.

Algunas de las ventajas de la forensia en redes es que esta no produce ningún impacto en el end-point, no modifica o altera las plataformas, funciona en los distintos sistemas operativos y logra hallar información de un host.

Gracias a esta rama de la forensia podemos conocer con quién se comunica el atacante y que transferencias realizó, además de lograr la recuperación de evidencia como documentos, conocer si borro el backdoor, si realizaron modificaciones al servidor, entre otras.

6.4.2 Procedimiento

El proceso para la gestión de evidencia en redes es el siguiente:

- Captura, en donde se realiza la obtención de los paquetes que viajan en medio.
- Registro, proceso encargado de almacenar los paquetes capturados.
- Análisis, proceso encargado de analizar cada uno de los paquetes.
- Objetivos, encargado de conocer porque se realizó ataque y realizar la forensia de host.

Gracias a las distintas técnicas o procedimientos se pueden capturar de manera eficaz paquetes como los de TCP/IP, ICMP, NTP, LLMNR, entre otros.

- El protocolo TCP es el encargado de proporcionar un comunicación segura entre el emisor y el receptor para realizar transferencia de datos de manera segura, revisando si existe duplicidad en los datos ya que si encuentra un duplicado lo em una de manera inmediata.

- El protocolo ICMP es el encargado de verificar que los paquetes si lleguen a su destino mediante una comunicación entre las ip y las distintas maquinas, se comunica mediante mensajes informativos en caso de encontrar un error si encuentra un problema.

- El protocolo NTP es el encargado de la sincronización de la red y las distintas maquinas, encargado de monitorear y detectar las fallas en los relojes internos.

- El protocolo LLMNR encargado de resolver los nombres de los sistemas informáticos cercanos funciona sobre IPv4 e IPv6 con registros similares a los del DNS.

6.4.3 Ataques comunes

Los paso a paso más comunes a la hora del ataque son los siguientes:

- Realizar un mensaje de alerta de un IDS.
- Analizar y examinar el evento.
- Reconstruir la sesión.
- Examinar el paquete.
- Determinar el tipo de evento.
- Escalar el evento.

Un aporte importante para la gestión de la evidencia es la realización de una copia forense la cual es difícil conseguir por la velocidad que la red maneja además se debe tener en cuenta el alcance y la privacidad, la copia forense maneja cadena de evidencia, formas digitales y controles de acceso.

Se debe tener en cuenta diferentes aspectos, uno de ellos es la obtención de los datos porque estos pueden ser muchos y puede llegar a ser complicado el manejo de estos, además estos deben cumplir con el protocolo de privacidad y legalidad, y si por el contrario no son muchos datos los obtenidos estos pueden no ser suficientes para considerarse como evidencia.

6.4.4 Herramientas

Los espacios más comunes para capturar datos son:

- Hub, porque otorga facilidad al momento de adquirir la información y son muy ineficientes.
- Switch, porque es posible habilitar el spanning en algún puerto.

Las herramientas utilizadas para la gestión de la evidencia en redes deben cumplir con unos requisitos como:

- Integridad de los datos.
- Permitir la reconstrucción de la sesión de.manera automática.
- Extraer archivos de un paquete.
- Realizar reproducciones vi a telnet, ftp e IRC.

Algunas de las herramientas más comunes son

- Xplico
- NertworkMiner
- Payags
- Bro-IDS
- Tcpxtract
- Tcpow
- Chaosreader
- WireShark
- foremost

6.4.5 Ejercicio

Para la realización de las pruebas utilizamos WireShark y MyLanViewer, donde conseguimos cosas como el nombre y los eventos de los computadores que están en la misma red, conocer que sesiones se han iniciado en un computador específico, realizamos ping a las máquinas, conocemos cuál es la ip externa, el historial y el traceroute de una ip, en la captura de paquetes podemos capturar usuarios y contraseñas, detección de fallos o intrusos.

Con la ayuda de la herramienta MyLanViewer obtuvimos los resultados como un scaner completo del rango indicado como se muestra en la figura62, también está la posibilidad de acceder al folder como la figura63.

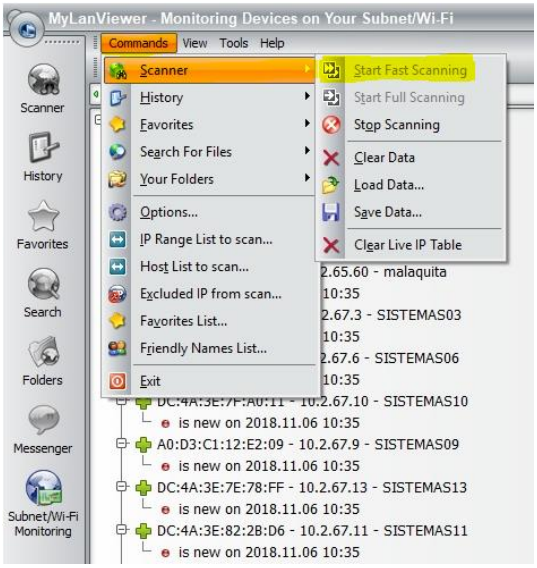


Fig. 62

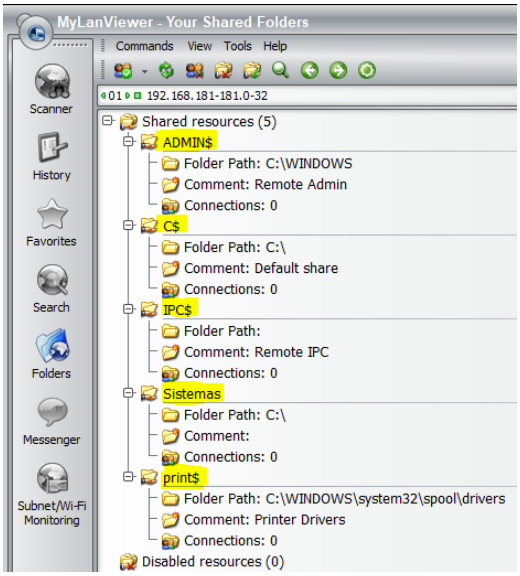


Fig. 63

Otra de las funciones que se usaron fue la del trace rout a un host específico para saber si se puede llegar hasta ella como se muestra en la figura64, los datos encontrados gracias a la herramienta se pueden almacenar y exportar de la manera portable como se obtiene en la figura 65 donde obtenemos todos los datos del host al que se le está realizando el seguimiento.

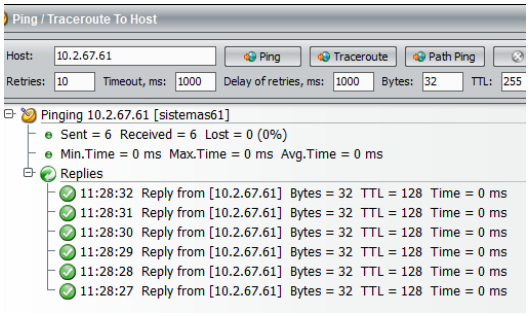


Fig. 64

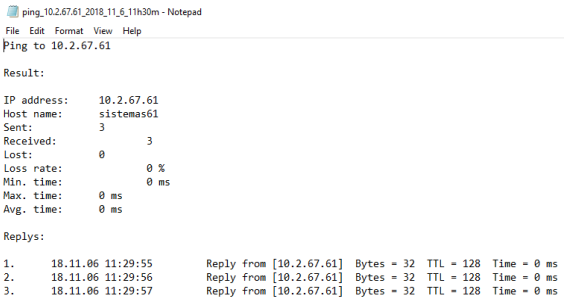


Fig. 65

Otra de las funciones que provee la herramienta es la posibilidad de conocer quién es el dueño de una IP, junto con datos de la ip como esta en la figura66.

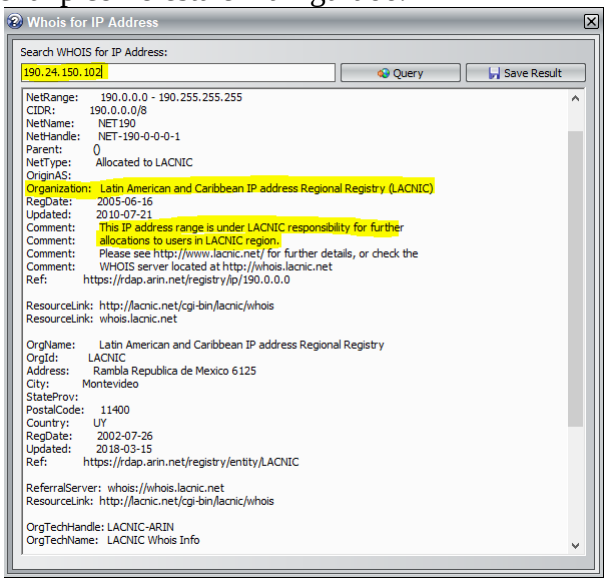


Fig. 66

Gracias a la realización de la gestión de la evidencia en la red podemos resolver dudas como qué fue lo que Paso, donde paso, cuando paso, porque paso, quien y como lo hizo [68].

Toda la investigación realizada dio paso a la realizacion de un articulo llamado "Importancia de la Forensia en Redes para la Recopilación de Evidencia Digital" el cual será publicado en la conferencia LACCEI 2019, a continuación el abstract del articulo

Abstract– Network Forensics is a sub-branch of digital forensics responsible for the collection of data that passes through the network, through techniques that perform IP tracking, network monitoring technique, packet capture and compilation of documents. All these techniques are carried out with different programs, for this article MyLanViewer and WireShark are used because they provide tools for network monitoring, packet capture, IP tracking, IP recognition and are free, throughout the article will be deepened in the architecture of the network, the typologies and topologies that exist according to the needs of the network. Keywords-- forensic network, protocols, digital evidence.

Resumen– Red forense es una subrama de forense digital responsable de la recopilación de datos que pasa a través de la red, a través de técnicas que realizan el seguimiento de IP, la técnica de monitoreo de red, la captura de paquetes y la recopilación de documentos. Todas estas técnicas se llevan a cabo con diferentes programas, para este artículo se utilizó MyLanViewer y WireShark porque proporcionan herramientas para realizar monitoreo de red, captura de paquetes, seguimiento de IP, reconocimiento de IP y son gratuitos, a lo largo del artículo se profundizará en la arquitectura de la red, las tipologías y topologías que existen según las necesidades de la red. Palabras clave-- red forense, protocolos, evidencia digital.

6.5 IoT

Internet of things (Iot) o más conocido como el internet de las cosas, según SAP es una red de objetos físicos como carros, maquinas, electrodomesticos, etc. los cuales utilizan sensores y APIs para conectarse y poder realizar un intercambio de datos por internet. todo esto con la premisa de hacer más fácil la vida de las personas.

Aunque las IoT son tendencia en estos momentos, ese término surgió a finales de 1990 por Kevin Ashton, quien fue parte de los que resolvió el como conectar los objetos con las etiquetas RFID. aunque la primera vez que uso la frase" internet de las cosas" fue para una presentación en 1999 solo hasta los estos últimos años se ha apreciado gran parte de su potencial gracias a que las redes inalámbricas están más inmersas, los sensores que están integrados son más refinados y las personas usan la tecnología como una herramienta más personal y profesional.

Gracias a las iot tenemos soluciones como

- lograr realizar redes eléctricas inteligentes que están conectadas de manera más eficiente.
- realización de sensores de monitoreo para una máquina de cualquier tipo para que monitoreen y diagnostican mediante lo realización de predicciones para la solución de problemas a corto plazo.

- recibir alertas de los electrodomésticos comentando que le falta a la nevera para entregar el recordatorio de pasar a la tienda por más leche.
- creacion y realizacion de un sistema de seguridad residencial, para que se pueda realizar un monitoreo y control remoto de las cerraduras, calefacción, ventanas, etc.

Cisco como muchas empresas predicen que para el 2020 habrá 5’0.000 millones de objetos conectados y funcionando bajo las IoT, otros como Gartner predecían 26.000 millones y otros tantos decían 30.000 millones, pero eso quizá sea solo una fracción de lo que realmente sucederá, ya que es el siguiente paso en la evolución de las tecnologías.

Aunque todos estos aportes son muy significativos al momento se facilitar la vida de las personas, pero como todo no es bueno, esta nueva tecnología debe encargarse de la seguridad ya que maneja mucha información en tiempo real y puede ser utilizada de formas negativas para perjudicar a las personas, es por eso que no todo es color de rosa por eso también se debe tener cuidado al momento de la utilización de esta tecnología ya que debemos tener claridad en la autonomía que se le está entregando al dispositivo que se está conectando, ya que puede realizar cosas sin preguntar por la confusión de los datos que obtenga, otro de los riesgos y quizá el más importante es la seguridad informática ya que en el momento que realicen un ataque no solo pueden recopilar datos personales, también pueden interceptar para realizar ataques u otro tipo de cosas y es por eso que existe la rama IoT forense.

La forensia digital se encarga de la identificación, recopilación, análisis y presentación de pruebas digitales de dispositivos convencionales para que sean admisibles ante la corte en el momento de delitos informáticos o incidentes de seguridad, gracias al aumento de dispositivos IoT se ha registrado un aumento en el número de incidentes de seguridad cibernética en estos dispositivos, es por eso que se creó florencia en IoT, que es una subdivisión de la forensia digital pero enfocada a dispositivos IoT encargada de recopilación y análisis de información en un rango más amplio de fuentes como sensores, dispositivos de comunicación, almacenamiento en la nube entre otros y también en la realización de pruebas en dispositivos para validar la veracidad de los resultados. En cuanto a la parte de jurisdicción y propiedad, ambas técnicas son iguales, ya que maneja personas, empresas, gobiernos, etc.

Existe gran variedad en los dispositivos iot por eso no existe un estandar unico para la identificación, recopilación y análisis de datos en estos dispositivos, pero si se maneja un tipo de estándar global para los mismos, este se basa en tres aspectos:

- Análisis forense en dispositivos
  - en cuanto a la parte de convencionales se refiere a la recolección de la evidencia en dispositivos como gráficos, audios, video, etc, como cámaras de CCTV o audios de amazon Eco.
- Análisis forense en red
  - para este ámbito se incluyen todos los tipos de red que son utilizados por los dispositivos para enviar y recibir la información, como lo son las redes, PAN, LAN,

WAN, MAN, etc, también las pruebas de hardware y software que proporcionen la comunicación entre los dispositivos como pc, dispositivos moviles, IPS, IDS y firewalls.

- Análisis forense en cloud
    - En la actualidad la mayoría de dispositivos utilizan internet para compartir sus recursos en la nube, lo que la convirtió en el lugar más popular para los atacantes, el inconveniente es que que para la forensia convencional el perito trabaja bajo un dispositivo de forma física para extraer toda la evidencia en cambio la nube es otro escenario completamente diferente ya que la evidencia podría ser separada en múltiples ubicaciones lo que dificulta la adquisición de los datos, también se tiene un control limitado para el acceso al momento de la adquisición de los datos ya que se debe solicitar una orden al proveedor con los datos del titular para poder acceder a ella y como esta dispersos no se pueden embargar o retener de manera rápida, otro de los problemas es la utilización de máquinas virtuales como servidores ya que estas al no estar sincronizadas con los dispositivos la información volátil puede ser borrada. en este grupo se incluye las pruebas encontradas en hardware y software, nubem redes sociales, proveedores del servicio de internet, redes móviles e identidades virtuales.

En donde la recopilación de evidencia puede ser obtenida de un dispositivo iot, un sensor, una red interna o externa, como un enrutador en el caso de la interna y una aplicación como caso de la externa. La razón de ser de esta sub-rama es la de identificar, obtener e identificar la evidencia digital de los dispositivos iot para fines legales o para realizar investigaciones.

A continuación, se enumeran los desafíos que tiene esta rama para la recolección de datos:

- Localización de los datos: muchos de los datos están distribuidos en lugares que no controla el usuario como la nube donde pueden estar en otros países lo que limita la búsqueda según las regulaciones de los distintos países.

- VIda útil: gracias a la limitación en el almacenamiento de los dispositivos, la vida útil de los datos es corta ya que se realiza una sobreescritura con los nuevos datos lo que causa la pérdida de la información, aunque muchos datos llegan a la nube mediante la transferencia de datos, es bastante complicado asegurar la cadena de custodia y para demostrar la veracidad de la información.

- Servicio en la nube: gran parte de las cuentas son anónimas ya que este servicio no verifica información, ya que cualquier persona puede ingresar datos falsos para crear una cuenta lo que no garantiza la identificación del atacante

- Seguridad: la falta de seguridad podría dar pie para que se modifique la evidencia, por ende si genera dudas esta no será admisible ante la corte.

- Tipo de dispositivo: en la forensia convencional la evidencia es un pc, o un móvil pero en iot la evidencia puede ser una nevera o una lavadora inteligente, lo que causa un mayor reto a la hora de la extracción de la información porque este está configurado según el fabricante y estos pueden utilizar distintas plataformas, sistemas operativos y hardware según deseen.

6.6 Nuggets DLS

Es denominado como un lenguaje de dominio específico enfocado a la forensia digital dedicado a resolver un problema en particular, siendo un lenguaje opuesto a Java o lenguajes de modelado como UML [69].

Por lo tanto, es recomendable que sea usado por un experto en el tema al que hace referencia el dominio, sin embargo, se considera un lenguaje limitado pues al intentar hacer cosas más generales se perderán los beneficios específicos por lo que algunos expertos han atinado a denominarlo como un “sql forense”

Se creó al ver la necesidad que tienen los investigadores forenses, pues se han convertido en parte desarrolladores, lo cual no es precisamente su trabajo pues ellos deben enfocarse en entender el caso, entender y analizar la evidencia [70].

La pagina oficial de Nugget [71] como se observa en la figura 67, indica que para poder comenzar a hacer uso de este lenguaje tienen disponible un docker y un repositorio en github donde permite descargar el código fuente y comenzar a trabajar en el lenguaje. El proyecto incluye como tal un analizador sintáctico que a su vez contiene un parser el cual recibe una sucesión de instrucciones que permiten el procesamiento del lenguaje.

Como lo indican en [72] docker es un contenedor de software que inicialmente sólo se encontraba disponible en Linux sin embargo es posible instalarlo en Windows. Para hacer uso de los comandos iniciales que indican en la página oficial de nugget es necesario descargar desde este contenedor la herramienta. Pero no es tarea fácil pues requiere permisos de virtualización lo que puede llevar a que no funcione correctamente.

Siguiendo los pasos indicados en la url de arriba es muy sencilla la instalación, sin embargo cuando se intenta correr el comando de nugget indica que docker no está corriendo. De igual manera cuando se pone a correr el contenedor, presenta un mensaje de error que indica que la virtualización no está activa como se observa en la figura 69.

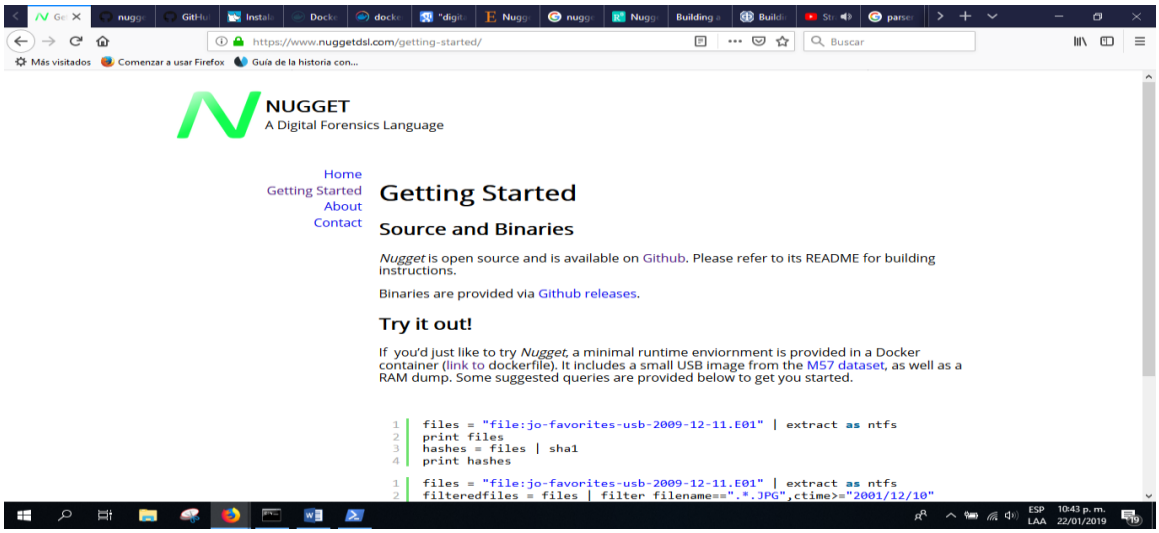


Fig. 67 Nugget Oficial

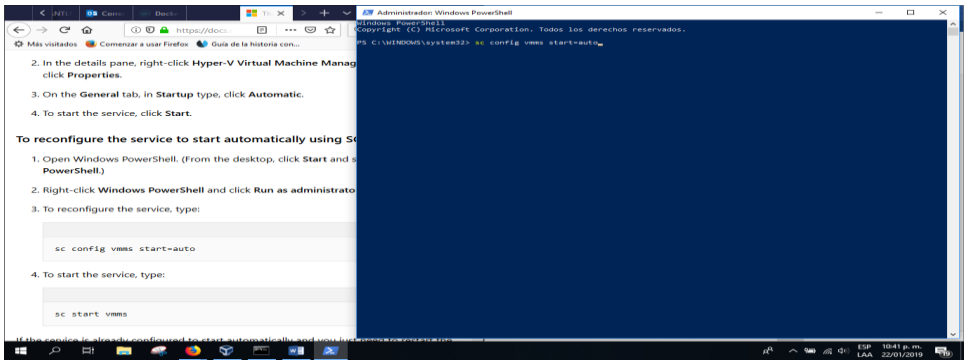


Fig. 68 Nugget Docker

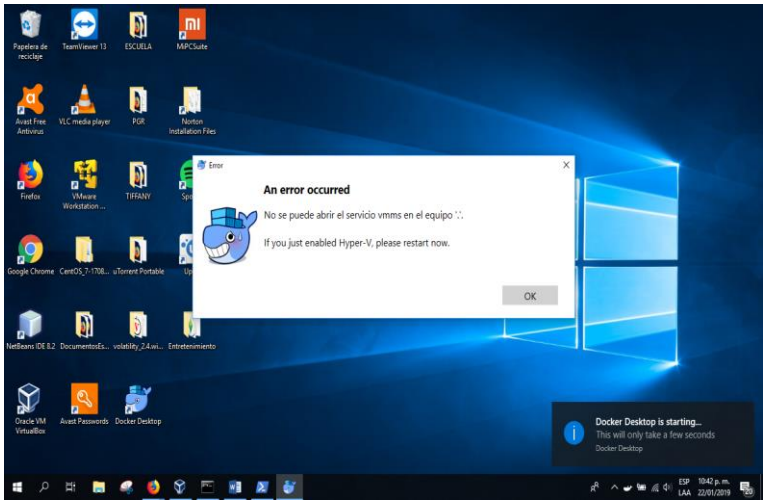


Fig. 69 Error Docker

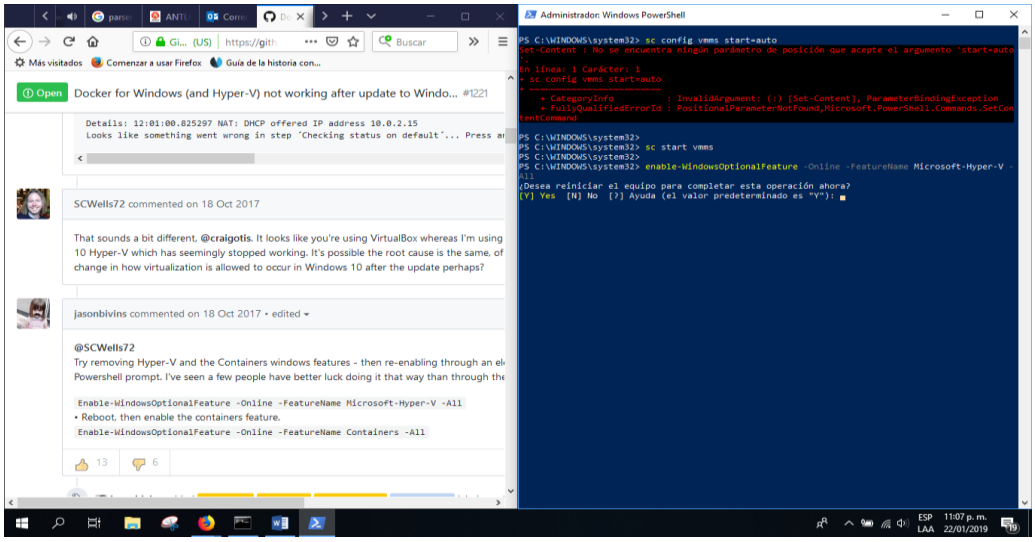
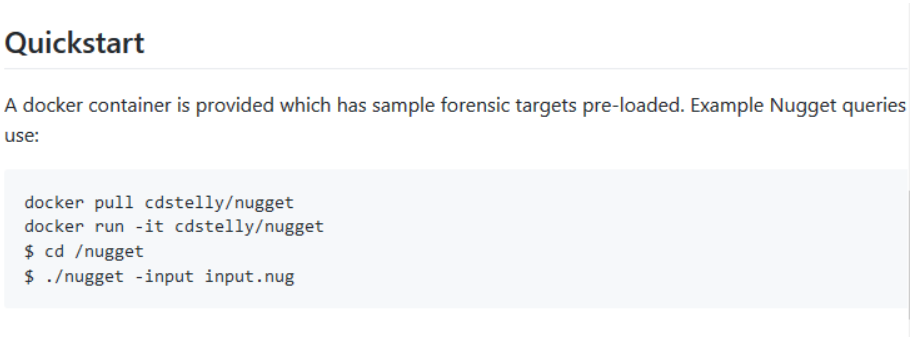


Fig. 70 Solucion Docker

Después de varios intentos y reinicios, finalmente el docker es activado y corre con normalidad. Fue solucionado gracias a un foro encontrado en internet como se muestra en la imagen 70.



Quickstart

A docker container is provided which has sample forensic targets pre-loaded. Example Nugget queries use:

```
docker pull cdstelly/nugget
docker run -it cdstelly/nugget
$ cd /nugget
$ ./nugget -input input.nug
```

Fig. 71 Uso de docker

Siguiendo las indicaciones encontradas en la página oficial de la figura 71, se corren algunos comandos en el docker como se observa en la figura 72.

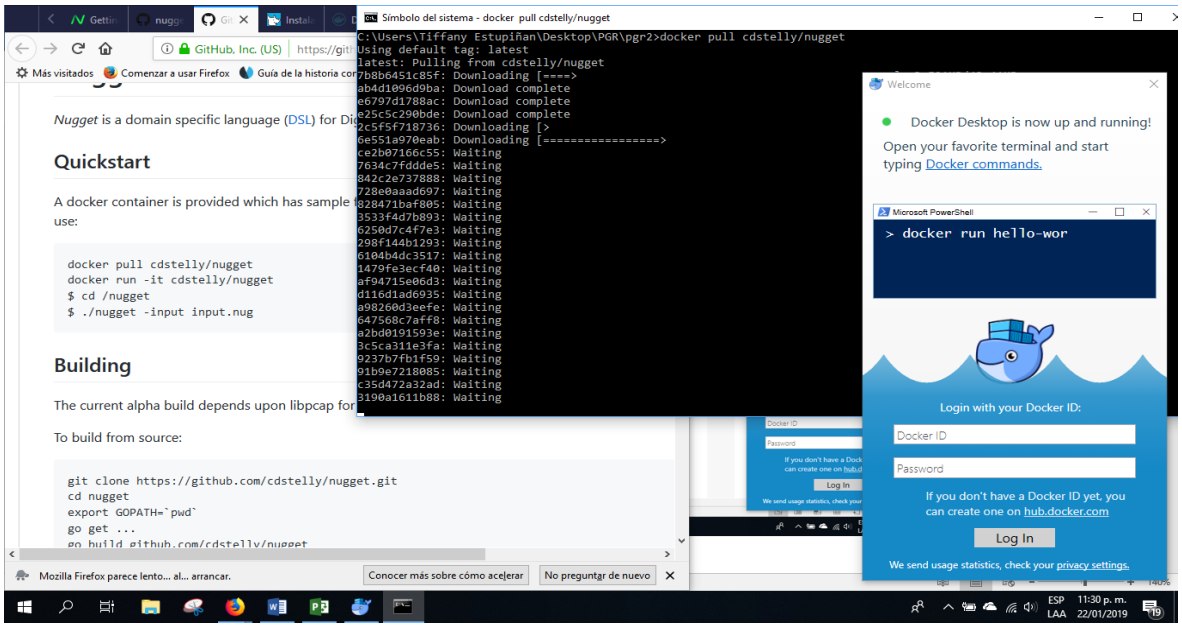


Fig. 72 Nugget en funcionamiento

Incluso a primera vista, la mayoría de los profesionales forenses reconocerían fácilmente la consulta anterior como una instancia de filtrado de archivos conocidos; en este caso, se aplica a todos los archivos pdf extraídos de la fuente target.dd, y se crea después del 1 de enero de 2017. Los puntos principales aquí son:

- el experto en dominios no necesitaba aprender un lenguaje de programación de propósito general para comprender la intención de la consulta (y podría aprender rápidamente a escribir otros similares);

- esta es una especificación formal que puede traducirse fácilmente en código ejecutable;

- la consulta solo especifica lo que se debe hacer, y no cómo se debe realizar; existen numerosas implementaciones posibles, incluidas las que emplean el recurso de un grupo de computadoras.

- La consulta en sí documenta de forma inequívoca el proceso forense y permite la prueba, verificación y reproducción automatizadas de los resultados.

En otras palabras, nugget busca hacer para la computación forense lo que SQL hizo para las bases de datos relacionales: establecer una interfaz de consulta estándar que sea lo suficientemente completa e intuitiva para que los expertos en dominios puedan comprenderla fácilmente, al tiempo que proporciona una especificación formal de la computación que debe llevarse a cabo. afuera. SQL permitió la coexistencia de numerosas implementaciones en competencia, lo que permitió un desarrollo rápido, una ejecución optimizada y un desarrollo de GUI autónomo.

Es importante ubicar este esfuerzo en un contexto más amplio y reconocer que el DSL nugget es un componente de un esfuerzo de investigación más amplio para abordar de manera integral un conjunto de problemas relacionados con la reproducibilidad, el rendimiento y la escalabilidad. Como se muestra en la Fig. 73, el lenguaje es una interfaz entre la capa UI (textual o gráfica) y el entorno de ejecución y el administrador de recursos. El DSL presenta un medio unificado para ejecutar cálculos forenses (utilizando el conjunto de herramientas disponibles), organizarlos en tuberías de procesamiento y almacenar / devolver los resultados según sea necesario

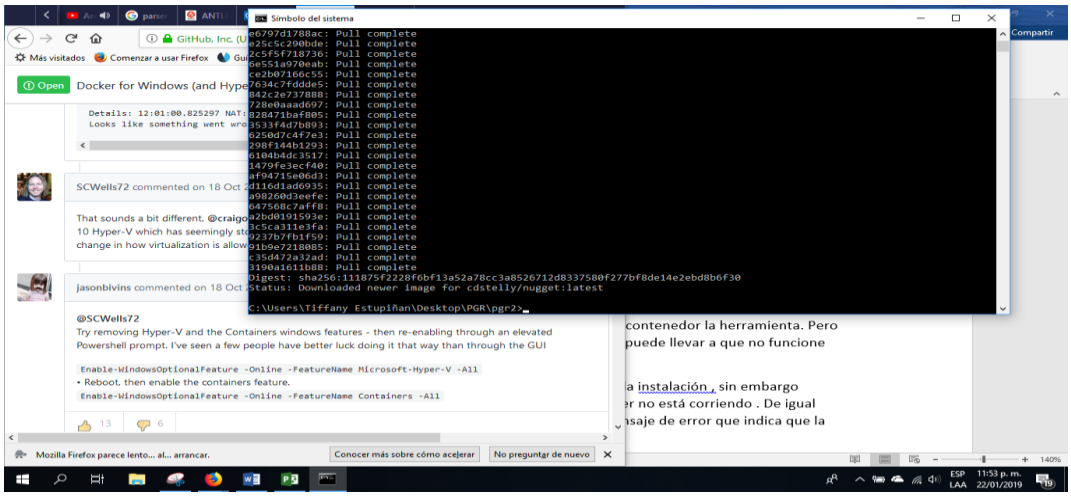


Fig. 73 Nugget en funcionamiento

Cuando se corre el nugget.exe no hace nada, abre un bash y vuelve a cerrarse. cuando se abre por consola indica como indica la figura 74.

```
C:\Users\Redes\Downloads>nugget.exe
panic: open input.nug: The system cannot find the file specified.

goroutine 1 [running]:
main.main()
        C:/Users/drew/GoglandProjects/nugget/nugtest.go:461 +0x70a

C:\Users\Redes\Downloads>
```

Fig. 74 Error Nugget

Sin embargo, a pesar de que en el docker nugget funciona correctamente, no fue posible reproducir el mismo comportamiento fuera del docker . Por lo que con eso se procede a acceder desde el sistema operativo linux que permite hacer las ejecuciones de manera mas nativa.

6.6.1 Linux

En linux se supone que docker es nativo por lo que no hay que instalarlo sin embargo si hay que correr un comando como se ve en la figura 75 para permitir que funcione correctamente [73] luego de esto se reinicia el equipo y docker comienza la descarga del proyecto

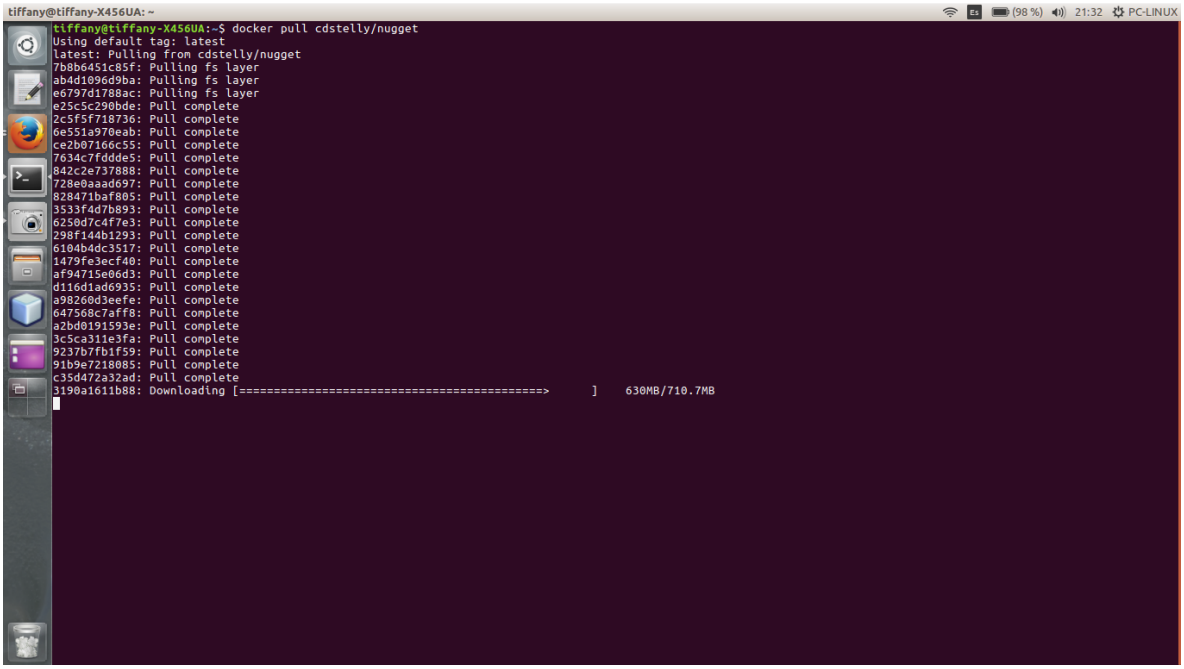


Fig. 75 Docker en Linux

Se siguen los comandos descritos en la página de nugget como se observa en la figura 76, anteriormente referenciados.

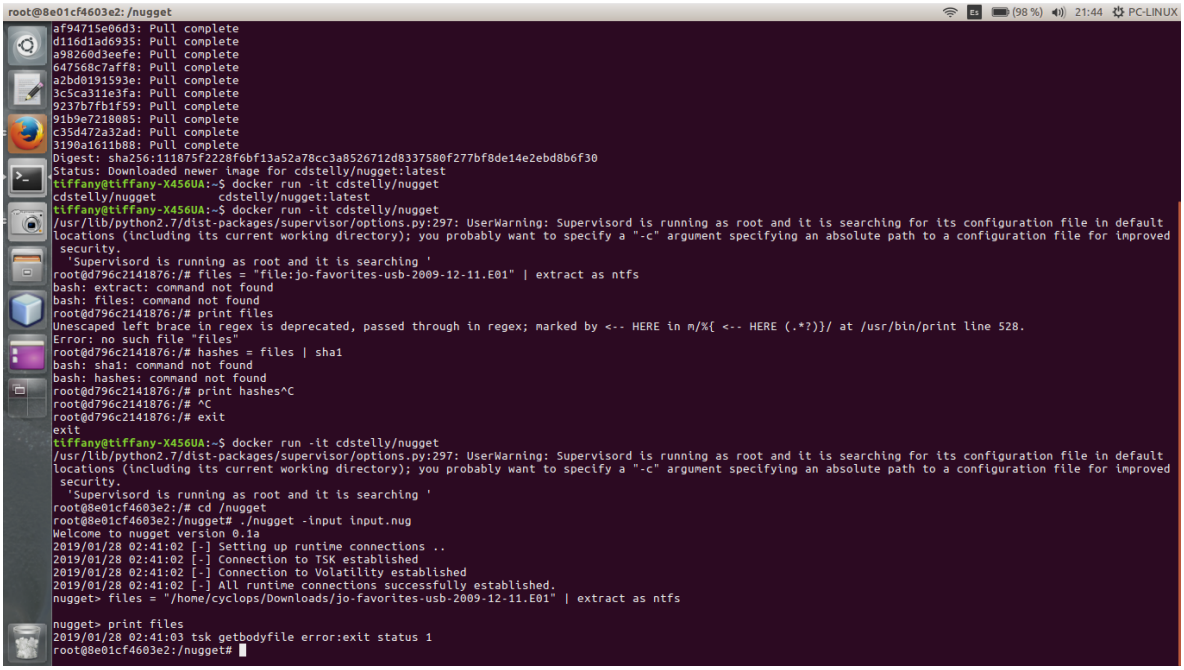


Fig. 76 Nugget en Docker Linux

Ya que no se conoce mucho del tema y no hay casi documentación de la misma, se procede a mirar que traen por dentro los archivos de muestra, se evidencian sentencias al estilo sql pero al intentar reproducirlas no dan el mismo efecto como se muestra en la fig.

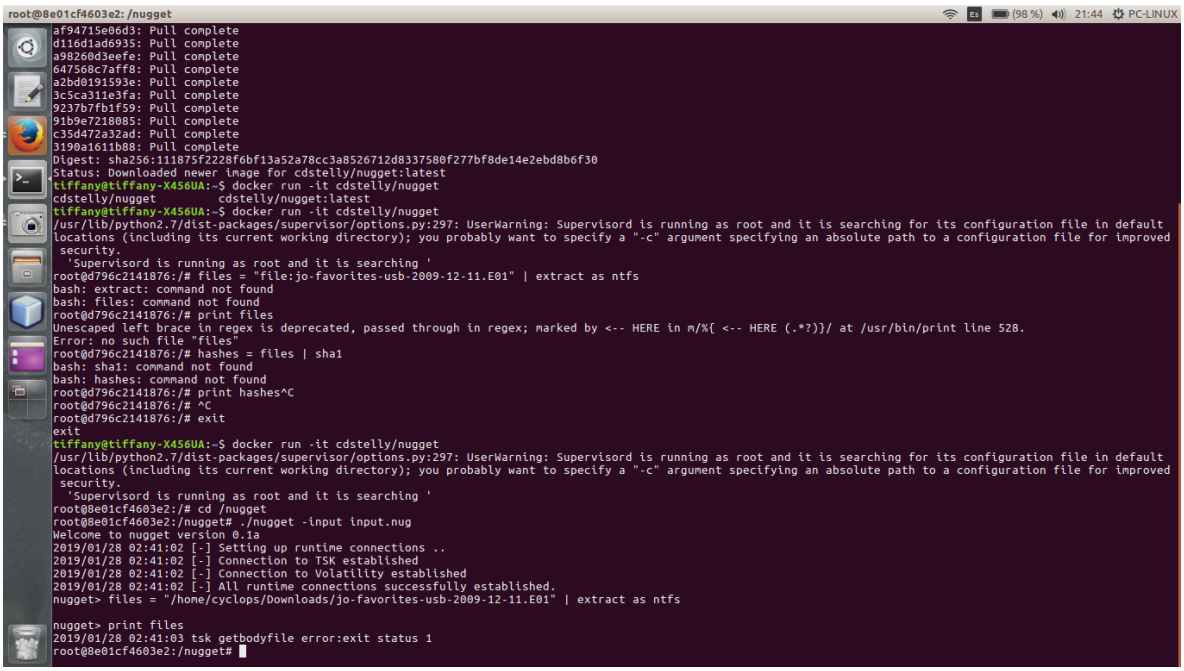


Fig. 77 Ejecución Nugget

Como se evidencia en la figura 78 y 79 se realizaron varios intentos de ejecución que no resultaron exitosos, por lo que la investigación al respecto finaliza ahí.

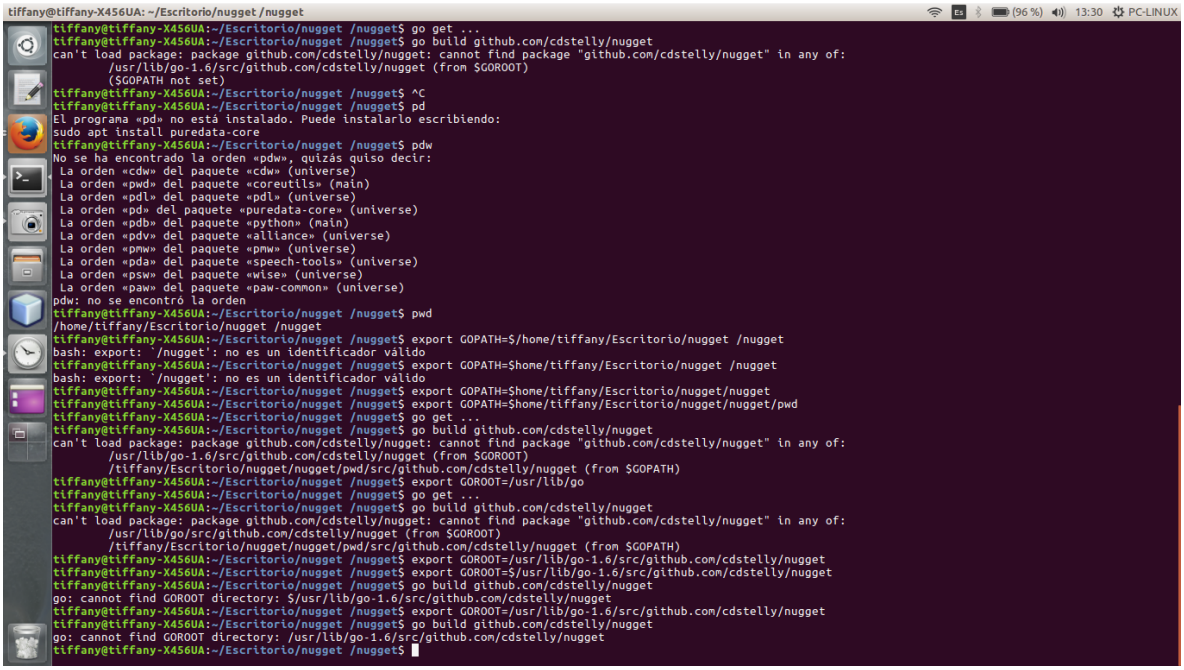


Fig. 78 Ejecución Nugget

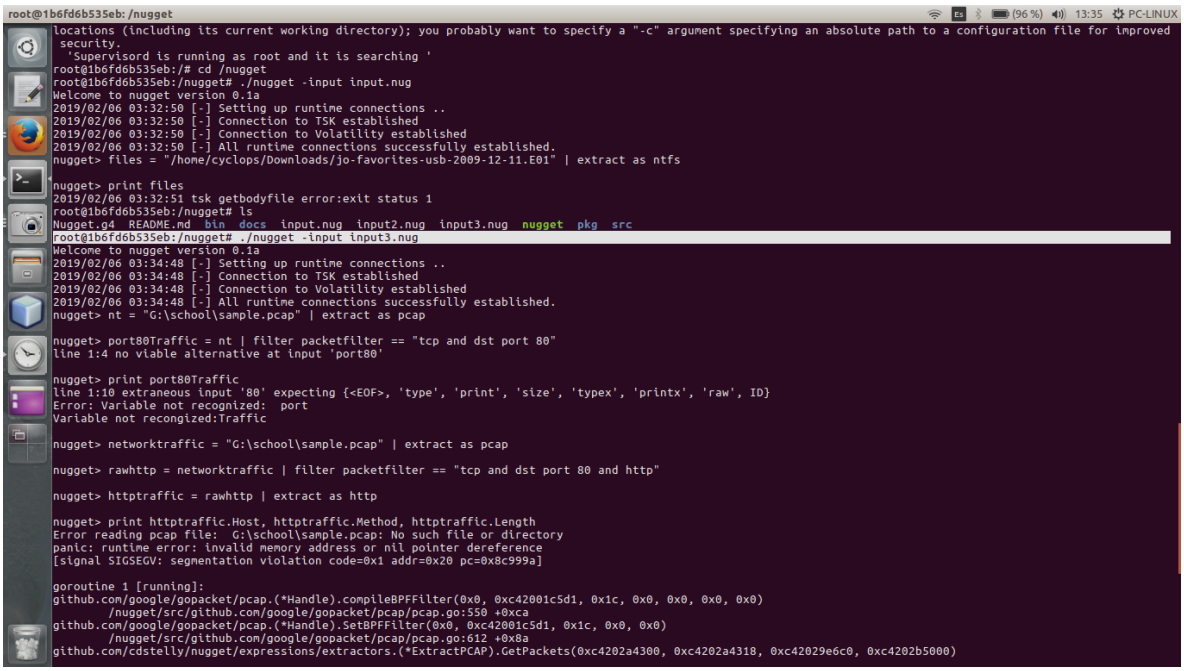


Fig. 79 Ejecucion Nugge

6.7 Plataformas IoT

6.7.1 Samsung Artik

Artik es una plataforma de Iot integrada que proporciona el camino más rapido para productos y servicios iot interoperables y sguros, pues unifica el hardware, software y l seguridad en un solo ambiente que queda centralizado en la plataforma cloud que ellos proporcionan . Los clientes pueden acceder y agregar informacion de diferentes fuentes (big data) teniendo asi completo control sobre sus datos .

En cuanto a forensia no ofrece mucho pues apesar de que tiene completo control de la informacion, ellos prometen que en un futuro la API podria incluir más trazabilidad de actividad de los usuarios. Adicionalmente al conectar un dispositivo permite obtener la informacion que se está recopilando en tiempo real y tambien obtener los dataLogs que permiten ver los mensajes que envia el dispositivo al ArtikCloud lo que permite visualizar la informacon, sin embargo, no es claro si se puede ver el historial de la informacion del dispositvo y si es asi que tanto tiempo se puede ver esta informacion. Desde el punto de vista forense se puede considerar que a lo mucho se puede rastrear o detectar un comportamiento inusual en el o los dispositivos, pero como tal recopilar información de quien o como accedio al dispositivo , no es posible; además una de las cosas que más recomienda Artik samsung es mantener los dispositivos seguros pues como tal lo único que ellos aseguran es la comunicacion de mensajes y conexion con el dispositivo a traves de tokens y sockets, maneja una interfaz amigable como se observa en la figura 80, figura 81 y figura 82. [74]

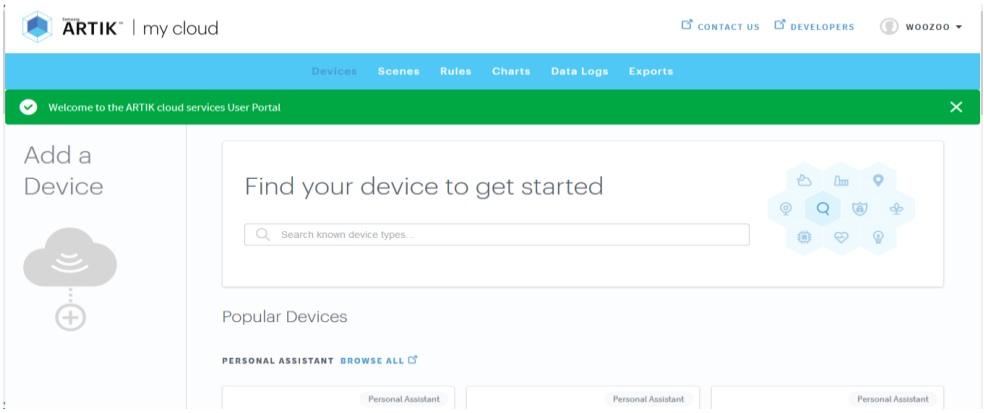


Fig. 80 Artik

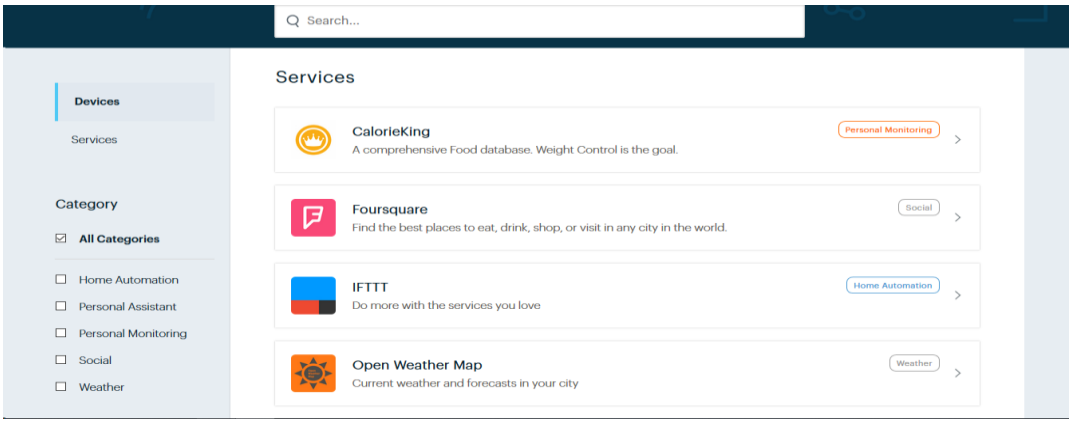


Fig. 81 Servicios Artik

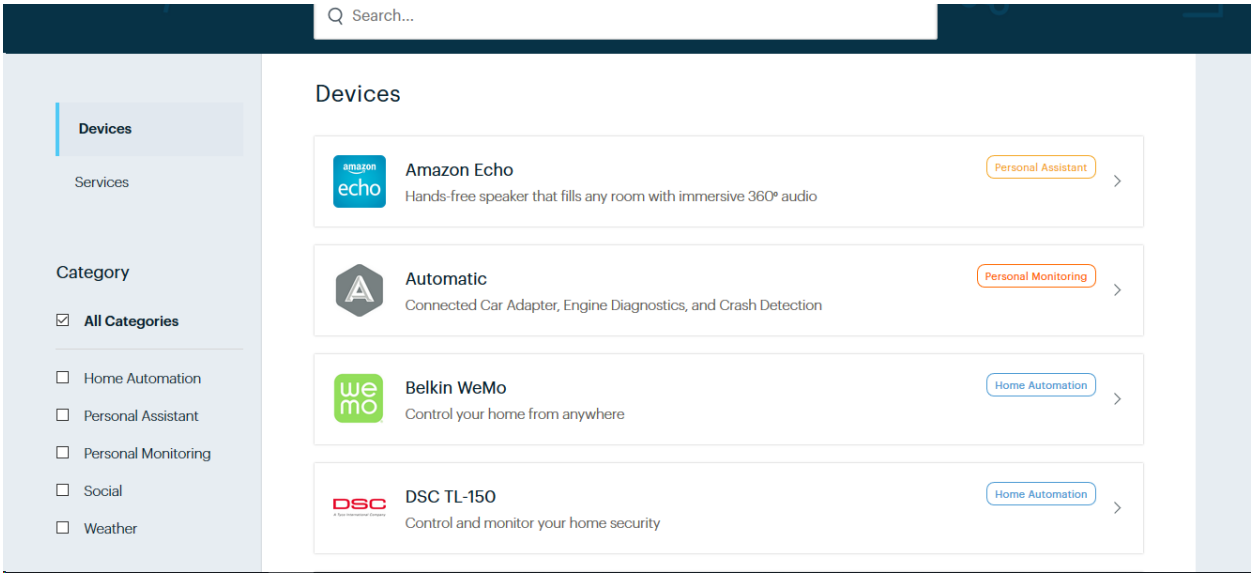


Fig. 82 Dispositivos Artik

6.7.2 Amazon IoT

AWS IoT brinda funcionalidad amplia y profunda que amplía el borde hasta la nube, de tal manera que puede crear soluciones IoT para casi cualquier fin en una amplia variedad de dispositivos.

AWS IoT también ofrece las funciones de seguridad más completas para que pueda crear políticas preventivas de seguridad y responder inmediatamente a posibles problemas de seguridad [75] [76].

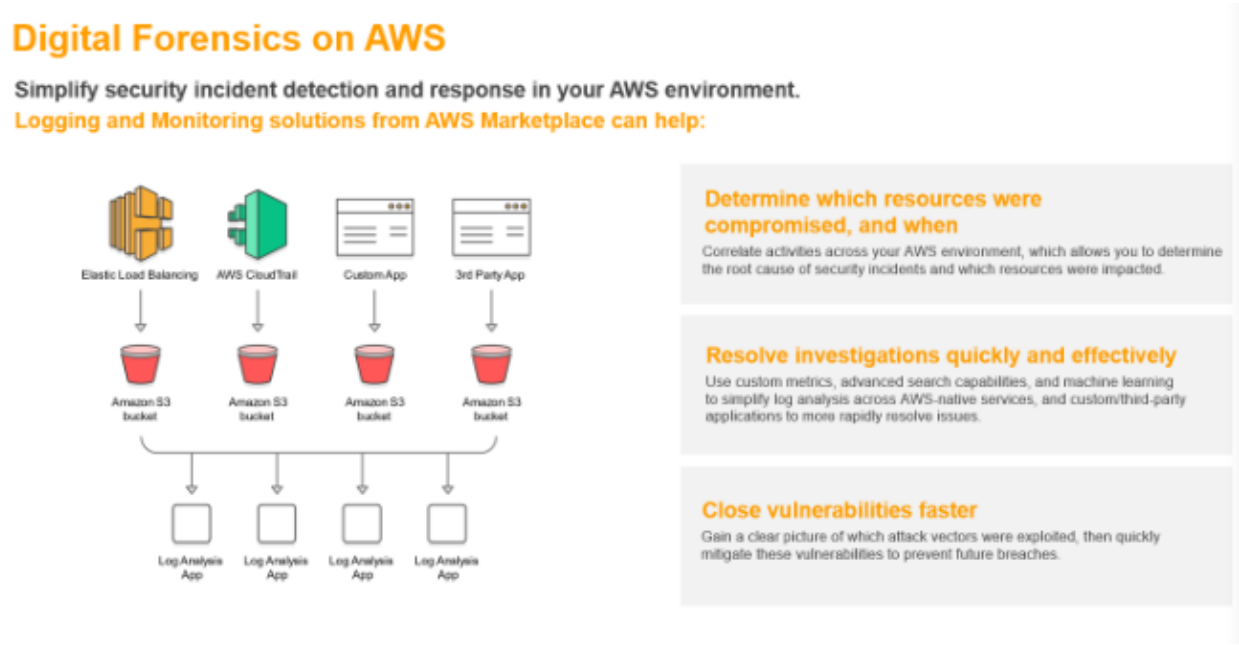


Fig. 83 AWS

AWS de la figura 83, tiene un mercado que ofrece la integración que permiten aumentar la seguridad de OS, plataformas, aplicaciones y datos. Sin embargo, son pagos y el pago debe ser por hora y de acuerdo a la cantidad de uso que le de al servicio, pero este servicio solo está disponible para aplicaciones y servicios, lo que permite conectarlo con los otros servicios Iot que ofrece AWS como lo es IOT core. En esta se intenta crear una cuenta para comprender la integración de aplicaciones con Iot core,WS IoT Core es un servicio en la nube administrado que permite a los dispositivos conectados interactuar de manera fácil y segura con las aplicaciones en la nube y otros dispositivos. AWS IoT Core admite miles de millones de dispositivos y billones de mensajes, y es capaz de procesarlos y direccionarlos a puntos de enlace de AWS y a otros dispositivos de manera fiable y segura. Con AWS IoT Core, sus aplicaciones pueden realizar un seguimiento de todos los dispositivos y comunicarse con ellos en todo momento, incluso cuando no están conectados., pero a pesar de que indica que es gratuito durante el registro solicita ingresar una tarjeta de crédito.

Otra aplicación disponible es AWS IoT Device Defender, que permite la auditoria de configuraciones de los dispositivos monitoreando las métricas de seguridad integrado con IOT Core con el fin de detectar comportamientos inusuales generando una alerta para tomar medidas a tiempo. Si se desea que automáticamente tome las medidas correspondientes entonces se puede integrar con otro servicio iot de Amazon que es el AWS IoT Device Management, no es muy claro en la documentación si permite guardar esta informacion recopilada y estas alertas de manera que permitan hacer una forensia completa , por lo tanto , es probable que por ser un servicio en la nube sea necesario hacer forensia en la nube y pueda presentar barreras. Por su puesto ellos (Amazon) ofrecen servicios pagos que permiten integrarse con sus plataformas y servicios que permiten hacer análisis de logs(Log Analytics) [77].

Pdevidence es un servicio web que permite manejar evidencia y tener un labotarorio forense portatil que está basasdo en AWS Cloud … me da la impresion que es más como para el papeleo de forensia tradicional pero no es muy clara la informacion .. es un alojamiento web para el manejo dl papeleo correspondiente.

6.7.3 IBM Watson IoT

IBM tiene un servicio llamado Qradar que permite capturar y analizar los incidentes forenses para de esta manera hacer un trackin de la conducta y ruta tomada por el posible atacante.Ayuda a mejorar la seguridad en la red haciendo captiras de paquetes en el dispositovo donde se encuentre desplegado. Es posible integrar Qradar con Watson y por medio de Inteligencia artifica [78] [79] [80] [81].

Qradar empodera el análisis de seguridad ayudando a hacer más eficiente la gestion y tomando decisiones mejores y más rapidas en casos de incidentes, junto con watson ayuda a tener retroalimentacion sobre las amenazas de Iot. Sin embargo, no muestra freetrial ni simulacion gratuita, unicamente se puede hacer cita para la compra directa. Por otra parte, watson por si solo no tiene documentacion que demuestre la presencia de herramientas que permitan el uso de forencia en el servicio.

6.7.4 SiteWhere

Es una plataforma opensource para desarrollar aplicaciones IoT cuenta con una infraestructura basada en microservicios los cuales implementan Kubernetes para poder realizar la implementación con cualquier proveedor en la nube, tambien cuenta con Apache Kalfka, Zookeeper y Hashicorp [82] [83].

6.7.5 Node red

Para empezar a utilizar esta plataforma disponible en Linux y Windows, la cual se realizó en Linux como se aprecia en la figura 84 y figura 85 la cual tiene el comando para empezar a instalación.

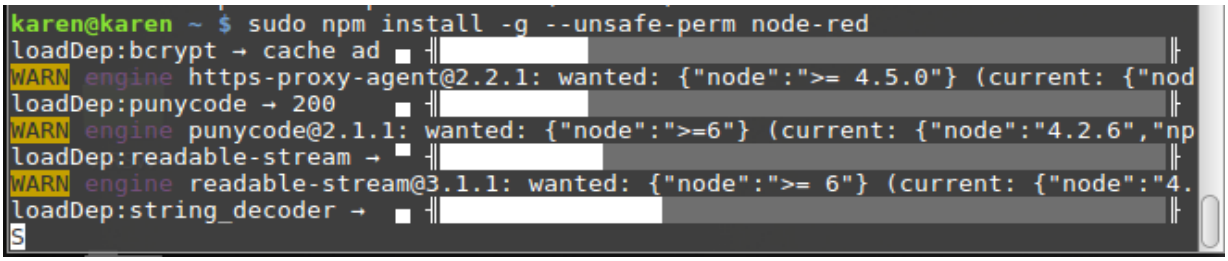


Fig. 84 Node Red

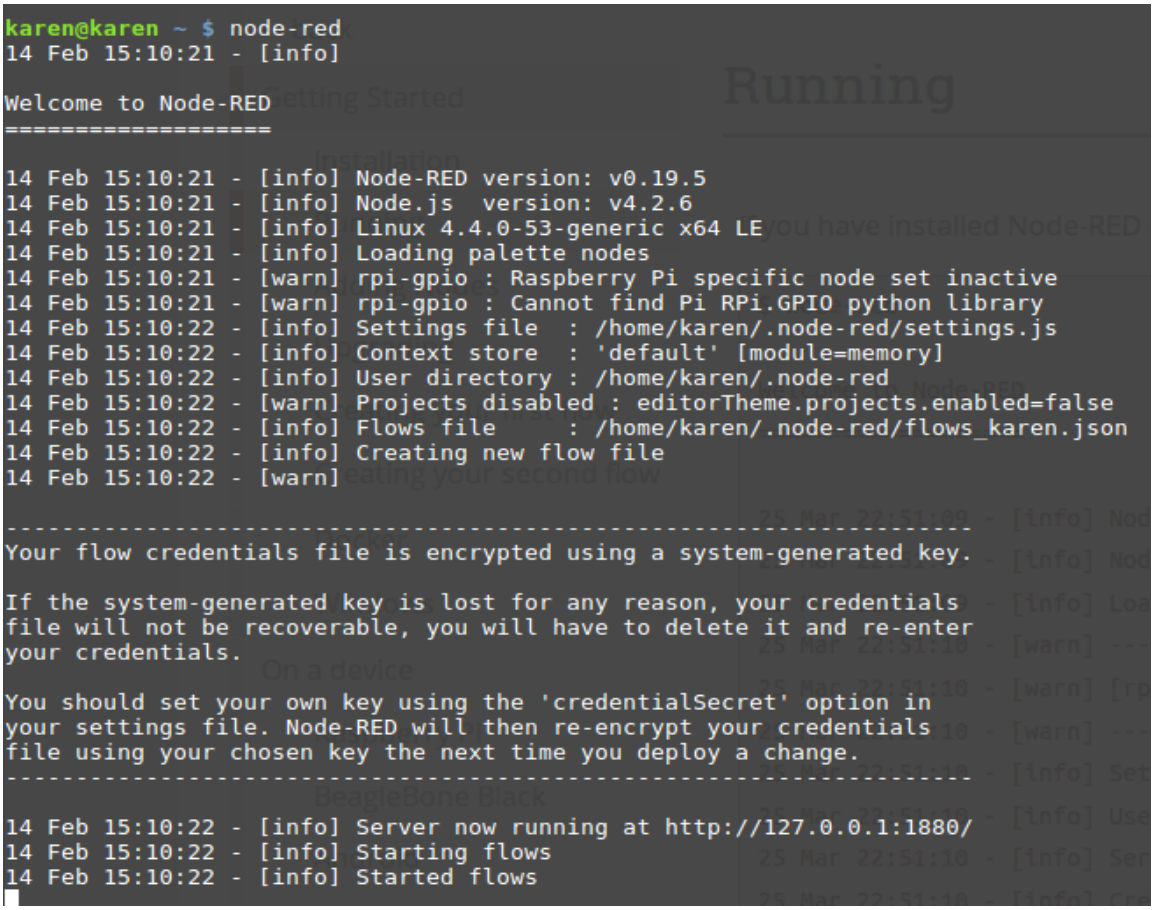


Fig. 85

Node red es una plataforma de programación donde se puedes conectar dispositivos, API y servicios en línea mediante un editor que facilita la integración y la conexión de los nodos que la herramienta otorga, esta basado en Node.js, se puede correr de manera local, en la nube o en un dispositivo, también cuenta con una función de JavaScript en donde se puede agregar el código que se necesite [84].

En la figura 86 hasta la figura 93 se observa la interacción de las dos plataformas, se creo una termómetro el cual notifica cuando es sistema captura un dato ya sea muy por encima o muy por debajo de los rangos colocados, en estas plataformas se pueden conectar los dispositivos IoT, se pueden sincronizar y monitorear

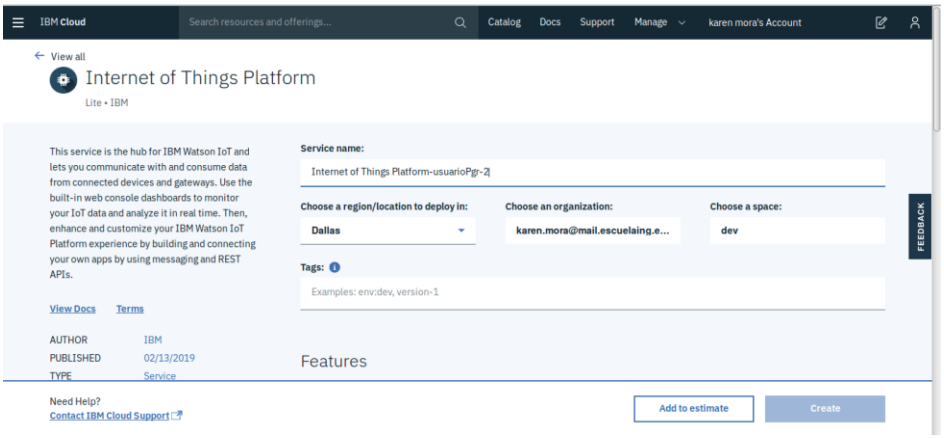


Fig. 86

Fig. 87

Fig. 88

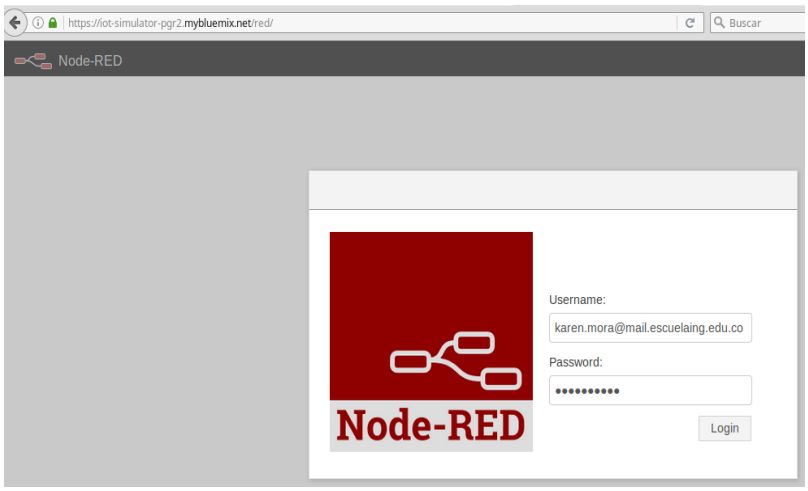


Fig. 89

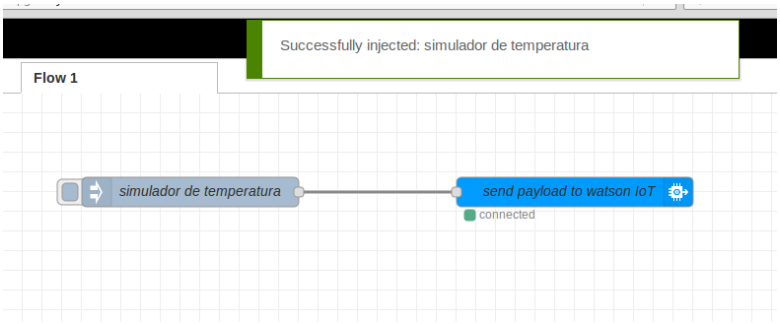


Fig. 90

Fig. 91

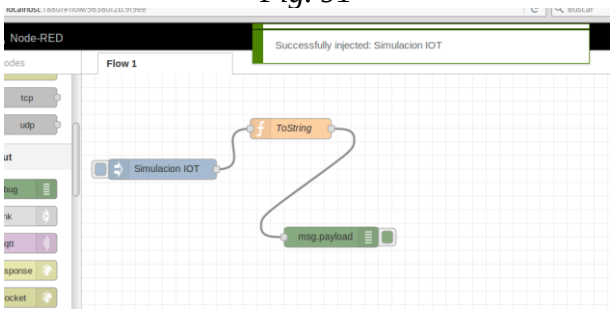


Fig. 92

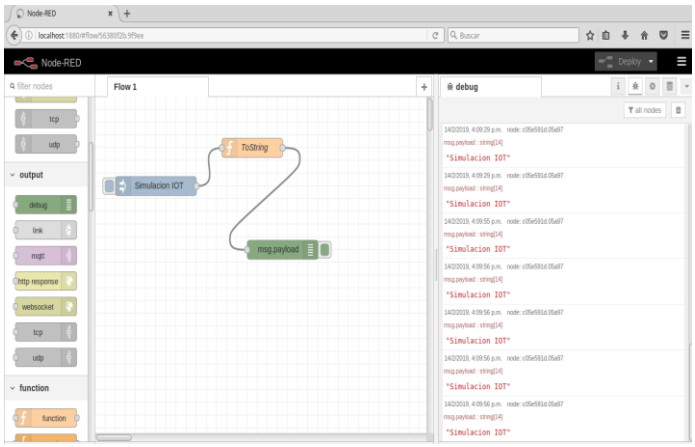


Fig. 93

6.7.6 GreenWave

Es una plataforma para administrar desde una sola fuente los dispositivos como, Puertas de enlace inalámbricas avanzadas, Enrutadores wifi, Aplicaciones de control móvil y / o mandos a distancia conectados, Controladores de pared conectados y tomas de corriente, Dispositivos habilitados para sensores (bombillas, altavoces inteligentes, sensores de movimiento y de ocupación, etc.). También funciona con dispositivos en la red entregando una infraestructura, en cuanto a los servicios de la nube, esta plataforma permite administrar, controlar y automatizar las funciones de las redes aunque no se pudo acceder a ello y solo se obtuvo respuesta como la que aparece en la figura 94 [85].

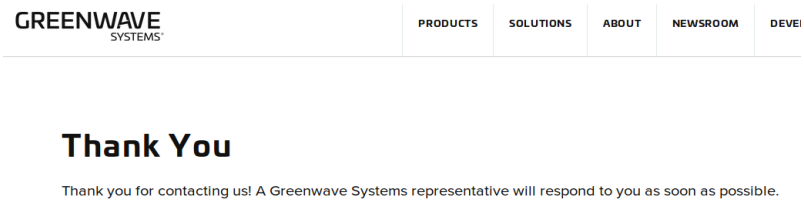


Fig. 94

6.7.7 Macchina.io

Plataforma de software para dispositivos, pasarelas de IoT y sistemas integrados que conectan sensores, actuadores, servicios en la nube, dispositivos móviles, etc. Brinda una plataforma para realizar un software confiable reduciendo costos en el desarrollo, riesgo y el tiempo. También proporciona un acceso seguro a través de la web, aplicaciones, ssh y vnc tanto para los usuarios finales como para los proveedores del servicio proporcionando una interfaz fácil de tratar como se observa en la figura 95.

Proporciona acceso de forma segura desde cualquier lugar con cualquier browser, cuenta con un administrador remoto con el cual las aplicaciones móviles o los asistentes como alexa de ios o android puedan acceder de forma segura al API REST del dispositivo. Todo esto mediante unos protocolos basados en TCP, incluidos SSH y VNc para brindar una administración remota segura y una correcta asistencia al usuario [86] [87].

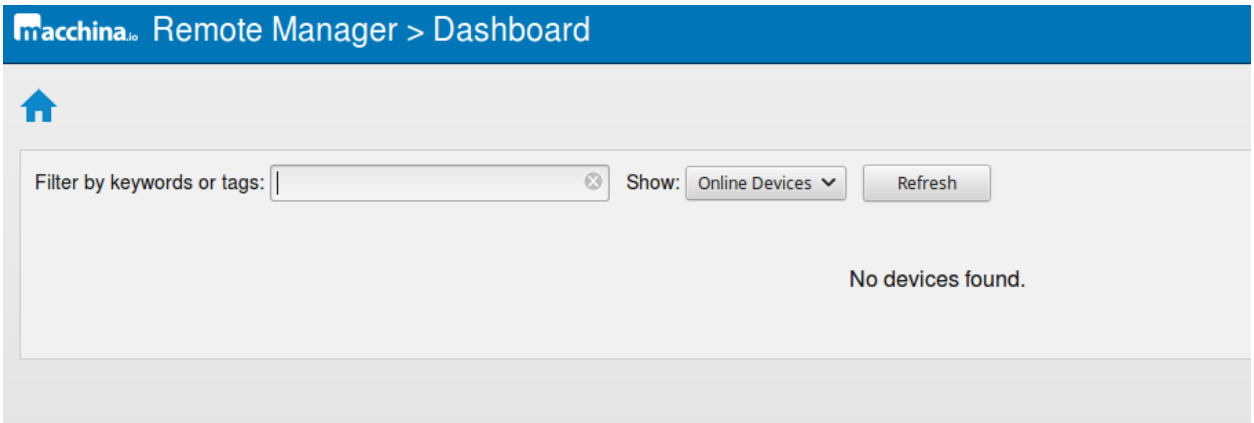


Fig. 95

6.7.8 Thinger

Es una plataforma que permite realizar Monitoreo y control de Variables, entregando un reporte de la transmisión de datos, permite registrar 3 dispositivos y durante el mes se pueden enviar 100mb peticiones. También cuenta con geolocalización de los dispositivos. Brinda soporte SSL y admite conexiones TLS para la plataforma,el diseño y la interfaz son como la figura 96 [88].

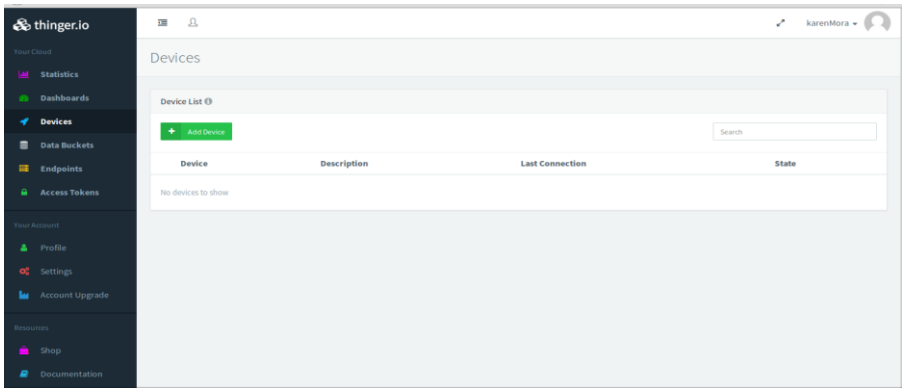


Fig. 96

6.8 Sistemas de archivos

Los sistemas de archivos son una estructura que usan los distintos sistemas operativos para mantener un seguimiento de los archivos y para almacenarlos de manera ordenada, los sistemas de archivo generalmente manejan un super bloque, un nodo, la ubicación de los datos, un bloque de datos y un bloque de indirección, que serán explicados más adelante con la especificación de cada sistema de archivos [89].

Gracias a los sistemas de archivos se pueden separar los datos en bloques diferentes y almacenar diferente información sobre estos datos, proporciona un índice para que el sistema operativo pueda conocer si el bloque esta ocupado o no.

El sistema de archivos FAT (File System Table) o en español tabla de localización de archivos, esta taba utiliza un mapa para conocer la ubicación de lo archivos que están almacenados [90].

Existen tres tipos de sistemas de archivo, los de disco, los de red y los de propósito especial. Los sistemas de archivo de disco son los encargados del almacenamiento con la utilización de los metadatos, la fecha de modificación y creación, su tamaño como también quien tiene acceso al archivo, existen distintos tipos de archivo pero os mas comunes son FAT, EXT y NTFS. Los sistemas de archivos de red son los que tienen acceso a la red de computadoras la cual tiene dos subgrupos, el primero es para los archivos distribuidos que son los que no proporcionan una entrada y salida y los archivos en paralelo que si las proporcionan [91]. y por ultimo están los sistemas de archivo de propósito especial que están compuestos por los otros sistemas de archivos que no entran en los anteriores grupos [89].

6.8.1 Clasificación

Los sistemas de archivo son importantes para la gestión de evidencia digital ya que gracias a ellos se puede conocer muchos de los datos, las creaciones, modificaciones, eliminación de archivos como también la recuperar información si se cuenta con metadatos para realizar la reconstrucción del archivo, existen distintos tipos de sistemas de archivo los cuales son distintos, pero se agrupan bajo cinco categorías que son la categoría de sistema de archivos, la categoría de contenido, la categoría de metadatos, la categoría de nombre de archivo y la categoría de aplicación.

6.8.1.1 Categoría de sistema de archivos

La categoría de sistema de archivos o file system category la cual contiene la información de los sistemas de archivos como la ubicación del archivo por si se elimina un archivo se debe ingresar a esta capa y reconstruir el archivo con la ayuda de un editor hexadecimal.

6.8.1.2 Categoría de metadato

La categoría de metadato o metadata category que contiene los datos que se encargan de la descripción de los archivos como también la ubicación del archivo, la hora y fecha de cuando se editaron o abrieron por ultima ves el archivo.

6.8.1.3 Categoría de nombre de archivo

La categoría de nombre de archivo o file name se pueden obtener los datos que proporciona el nombre del archivo y se encarga de realizar una traducción por así decirlo para convertir lo que escribe el usuario en un lenguaje que entienda el dispositivo para poder encontrar y acceder al archivo.

6.8.1.4 Categoría de contenido

La categoría de contenido tiene el contenido ”real” de los archivos en donde se manejan bloques que contienen un estado para conocer si esta asignado o no, conocer la ubicación del archivo, en el momento en el que elimina un archivo algunos sistemas operativos no sobre escriben los bloques por ende se puede recuperar completamente el archivo desde esta categoría.

6.8.1.5 Categoría de aplicación

La categoría de aplicación o application category la cual contiene datos que no son necesarios para realizar las acciones de lectura y escritura, mediante la utilización de un diario para guardar en un log las modificaciones realizadas [92].

6.8.2 FAT

El sistema de archivos FAT o tabla de asignación de archivos que incluyen los sistemas FAT12 que tiene un tamaño entre 512 bytes a 8 kilobytes , FAT16 que tiene un tamaño entre 512 bytes a 64 kilobytes y FAT32 que admite tamaños hasta de 2 terabytes. Los sistemas FAT manejan en el primer bloque el sistema de arranque que contiene la información de como esta particionado de manera lógica en el dispositivo de almacenamiento, cuenta con un área reservada que contiene un codijo ejecutable, un identificador OEM, el numero de FAT y un descriptor del sistema operativo, también contiene dos áreas de FAT’S para realizar un seguimiento de los bloques para conocer cuales están asignadas, cuales no están asignadas, conocer el inicio y el final del archivo y si el sector esta defectuoso seguido de un directorio raíz que contiene el nombre del archivo, el numero del bloque al que pertenece y el tamaño del archivo, la cual se modifica cada que se edita el archivo y por ultimo está el área de datos que es el área restante para almacenar los datos, en la siguiente imagen podemos observar la distribución de cada sector.

6.8.3 NTFS

El sistema de archivos NTFS (New Tecnology File System) o sistema de archivos de nueva tecnología en donde el nombre del archivo puede contener 255 caracteres, no es sensible a mayúsculas y minúsculas, cada una de las listas que maneja el sistema tiene una lista para realizar un control de acceso para cada archivo,

6.8.4 EXT

El sistema de archivos EXT es el sistema de archivos de unix o Linux cuyo tamaño es de 4 tera bytes reservando el 5 por ciento de los bloques para uso del administrador por si ocurre un proceso de sobrellenado, tiene eliminación segura de archivos ya que sobre escribe los datos [93].

6.8.5 Actividad

El trabajo realizado con los sistemas de archivo fue un escaner total del disco de un compurador, realizando busquedas para conocer la probabilidad que se tiene para poder recuperar un archivo completo, también se logró acceder a los bloques y ver su contenido escrito de manera exadecimal, en código binario entre otros. Al elegir que archivos se desea recuperar la herramienta pide una ubicación externa para almacenar el archivo recuperado y comprobamos que se puede obtener cien por ciento del archivo ya sea un documento de texto, una imagen, un video o una partición antigua.

6.8.6 Conclusión

Los sistemas de archivos son importantes ya que entregan una gran cantidad de datos que sirven como prueba ante la corte pero que por si solas no sirven como soporte, es por eso que este análisis debe ir acompañado de resultados de un monitoreo de red, recolección de una imagen forense, análisis de las bases de datos, recolección y análisis de toda la memoria junto con datos volátiles, no volátiles y toda la mayor cantidad de pruebas que sean admisibles ante la corte para asegurar la completitud de la evidencia ante la corte.

6.9 Virtualizadores en la Forensia digital

6.9.1 Hipervisor: Definición

El hipervisor también llamado monitor de máquina virtual (VMM) es un software utilizado para el control de la virtualización para usar al mismo tiempo diferentes sistemas operativos (SO) en el mismo equipo de cómputo [94].

Fueron desarrollados a principios de los años 70, con el objetivo principal de reducir costos. Usados originalmente como equipos de tiempo compartido para diferentes usuarios. Por esto los ingenieros de IBM en Cambridge, otorgaron a cada usuario una máquina virtual con un sencillo sistema operativo. El hipervisor permite consolidad con robustez y estabilidad varios sistemas operativos permitiendo el funcionamiento de cada uno por aparte sin interrupción aun cuando uno de los SO haya fallado [95].

La primera computadora diseñada específicamente para virtualización fue el mainframe IBM S/360 Modelo 67 en 1964, con el sistema operativo CP-40.7 Esta característica de virtualización ha sido un estándar de la línea que siguió IBM S/370 y sus sucesoras, incluyendo la serie actual.

Uno de los primeros hipervisores para PC fue VMware, desarrollado a finales de los años 1990. La arquitectura x86, usada en la mayoría de los sistemas de PC, es particularmente difícil de virtualizar. Pero los grandes fabricantes de microprocesadores, como AMD e Intel, desarrollaron

extensiones para tratar las partes de la arquitectura x86 que son más difíciles o ineficientes de virtualizar, proporcionando un apoyo adicional al hipervisor por parte del hardware. Esto permite un código de virtualización más simple y un mejor rendimiento para una virtualización completa.

6.9.1.1 Hipervisor tipo 1 (bare metal)

También denominado *nativo*, *unhosted* o *bare metal* (*sobre el metal desnudo*) [96], es software que se ejecuta directamente sobre el hardware, para ofrecer la funcionalidad descrita.
Algunos de los hipervisores tipo 1 más conocidos son los siguientes:

- Linux KVM[12].
- VMware ESXi.
- Xen.
- Citrix XenServer.
- Microsoft Hyper-V Server.
- Oracle VM Server para x86.[13]

Primero, con el software de virtualización basado en hipervisor, es posible actualizar las máquinas virtuales que se albergan en los servidores físicos sin ningún tipo de downtime. Segundo, es muy probable que la empresa ya esté virtualizando varios servidores físicos y quiera tener la opción de tener una gestión centralizada. Por último, un hipervisor bare metal siempre ofrece una mayor confiabilidad y rendimiento al no precisar de un sistema operativo Host, con lo cual se elimina un posible punto de fallo.

Sin embargo, la virtualización basada en hipervisor tiene un mayor rendimiento, mayor fiabilidad y estabilidad, mayor escalabilidad y mucha más funcionalidad.

6.9.1.2 Hipervisor tipo 2 (Host)

También denominado hosted, es software que se ejecuta sobre un sistema operativo para ofrecer la funcionalidad descrita. Algunos de los hipervisores tipo 2 más utilizados son los siguientes [97]:

- Oracle: Virtual Box.
- Virtual Box OSE (desde la v4.0 fusionado en Virtual Box).
- VMWare: Workstation (de pago).
- QEMU (varios sistemas operativos soportados).

En ellos el hipervisor se ejecuta en el contexto de un sistema operativo completo, que se carga antes que el hipervisor. Las máquinas virtuales se ejecutan en un tercer nivel, por encima del hipervisor. Son típicos de escenarios de virtualización orientada a la ejecución multiplataforma de software, como en el caso de CLR de .NET o de las máquinas virtuales de Java.

6.9.1.3 Hipervisores híbridos

En este modelo tanto el sistema operativo anfitrión como el hipervisor interactúan directamente con el hardware físico.
Las máquinas virtuales se ejecutan en un tercer nivel con respecto al hardware, por encima del hipervisor, pero también interactúan directamente con el sistema operativo anfitrión.

Los tipos de hipervisores anteriormente descritos se ven a mejor escala en la figura 98

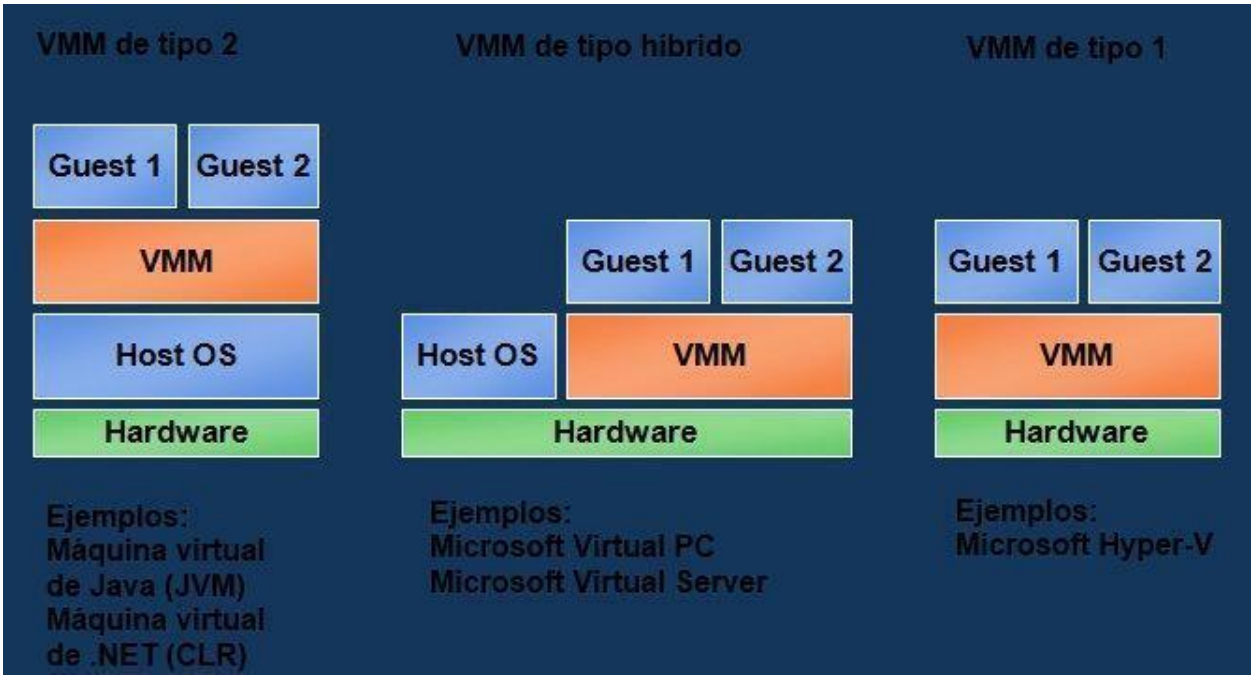


Fig. 98 Tipos Hipervisores

Algo a tener claro a la hora de virtualizar, es que necesitamos que la memoria RAM del equipo desde donde vamos a virtualizar, sea capaz de contener al sistema anfitrión (para VMM tipo 2) y a las MMVV. También deberíamos de disponer de bastante espacio en disco y además, que el procesador se haya construido pensando en la virtualización. Actualmente, cualquier ordenador puede virtualizar, pero es importante pensar en el microprocesador, la RAM y la capacidad de disco de la que se dispone.

Hoy en día, todos los nuevos microprocesadores traen instrucciones para ayudar a la virtualización. Esta característica puede que tenga que activarse en la BIOS del ordenador, concretamente es necesario para realizar virtualización de tipo I o de tipo II de Manager virtual Machine con sistema operativo de 64 bits sobre arquitecturas x86. En los microprocesadores de Intel se denomina *Intel VT-x* y en los de AMD su nombre es *AMD-V*.

6.9.2 Seguridad en hipervisores

La virtualización de servidores se ha establecido como una tecnología muy usual en la infraestructura de las empresas TI y de aquellas que ofrecen servicios cloud, para lograr una mejor utilización de los recursos hardware, reduciendo espacio físico y el consumo de recursos humanos y energéticos.
Teniendo en cuenta las funcionalidades base de un hipervisor es necesario detectar las potenciales amenazas y las contramedidas que pueden proporcionar seguridad contra la explotación de estas amenazas de seguridad [98]. A continuación, algunas de las funciones base de un hipervisor:

- Aislamiento de procesos VM: Aislamiento de procesos de máquinas virtuales: programación de máquinas virtuales para su ejecución, gestión de los procesos de

aplicación que se ejecutan en máquinas virtuales como CPU y gestión de memoria, cambio de contexto entre varios estados del procesador durante la ejecución de aplicaciones en máquinas virtuales, etc.

- Emulación de dispositivos y control de acceso: se combinan todos los dispositivos de red y almacenamiento (bloque) que esperan diferentes controladores nativos en máquinas virtuales, y que promueven el acceso a dispositivos físicos de diferentes máquinas virtuales.
- Ejecución de operaciones privilegiadas por el hipervisor para máquinas virtuales de tipo Host: ejecución de ciertas operaciones invocadas por el sistema operativo invitado por el hipervisor en lugar de ser ejecutadas directamente por el hardware del host debido a su naturaleza privilegiada. Se aplica a los hipervisores que han implementado para virtualización en lugar de completa virtualización
- Gestión del ciclo de vida de la máquina virtual todas las funciones, incluida la creación y administración de imágenes de la máquina virtual, control de estados de VM (Inicio, Pausa, Detener, etc.), migración de VM, toma de instantáneas, monitoreo de VM y política de ACCION.
- Gestión del hipervisor: definición de algunos artefactos y configuración de valores para varios parámetros de configuración en los módulos de software del hipervisor, incluidos aquellos para la configuración de un Virtual Red dentro del hipervisor y actualizaciones y parches a esos módulos.

Dado que el software del hipervisor tipo 2 , se encuentra en un host físico que está conectado a la red de la empresa tiene la capacidad de ser administrado de forma remota, al mismo tiempo soporta múltiples host virtuales (máquinas virtuales) que generalmente son nodos de una red virtual definida por software dentro de este host físico [94]. Con este escenario en mente es posible identificar las principales fuentes de amenaza para un hipervisor:

- Amenazas desde y atraves de la red empresarial en la cual el host del hipervisor reside (maquina física)
- Amenazas que surgen de máquinas virtuales mal intencionadas o comprometidas a través de canales como un hipervisor que comparte memoria y red virtual dentro del host del hipervisor
- Amenazas desde las interfaces web al DAEMON de administración de VM y las consolas de administración de hipervisores

EL hipervisor controla el acceso de la máquina virtual a los recursos físicos del hardware y proporciona aislamiento entra las máquinas virtuales. El acceso de la VM a los recursos de hardware, como la CPU y la memoria, está controlado directamente por el hipervisor mientras que el acceso a los recursos como la red y los dispositivos de almacenamiento controla a traes de módulos que residen en el kernel o en una VM de administración. El aislamiento de la red entre máquinas virtuales es proporcionado al asignar una dirección IP o MAC única a cada VM, definiendo redes de área local virtuales (VLAN) o superponer redes, y asignar el identificador de red apropiado a cada VM. La naturaleza de las amenazas las VM mal intencionadas o comprometidas puede manifestarse así [99]:

- Incumplimiento del aislamiento del proceso (VM escape): Las máquinas virtuales malintencionadas logran subvertir la función de aislamiento proporcionada por el manager Virtual Machine. Las VM comprometidas pueden acceder a áreas de memoria que pertenecen al hipervisor u otras máquinas virtuales y dispositivos de almacenamiento que no está autorizado a acceder. Las posibles razones de esta amenaza incluyen la instalación de rootkits o ataques en otras máquinas virtuales en el mismo host virtualizado.
- Incumplimiento del aislamiento de la red: las amenazas potenciales al aislamiento incluyen ataques como IP o MAC , la falsificación de direcciones por parte de una maquina virtual maliciosa y la indagación de tráfico , o la intercepción del tráfico de red virtual. El impacto de la subversión de estas redes permitiendo que algunas VM tengan acceso a información que no están autorizadas.
- Denegación de servicio: las máquinas virtuales mal configuradas o malintencionadas pueden consumir una cantidad desproporcionada de recursos del host, lo que da como resultado la denegación de servicio a otras máquinas virtuales en el host del hipervisor

Por otro lado, algunas vulnerabilidades potenciales de diseño que se relacionan con estas amenazas son [99]:

- Para programar adecuadamente las tareas de una máquina virtual individual (es decir, Las tareas de CPU, ya que a cada máquina virtual invitada se le asigna un conjunto de CPU virtuales), los estados de registro deben manejarse apropiadamente. Para habilitar el guardado y la carga del estado de cada CPU, el hipervisor utiliza datos Estructura denominada Estructura de Control de Máquina Virtual (VMCS). Implementación defectuosa de esta estructura de datos. Se ha sabido que causa pérdidas de memoria en el hipervisor.
- En plataformas de hardware que no proporcionan asistencia para virtualización, debe haber un mecanismo de software para descubrir instrucciones sensibles o críticas, enviar al VMM (hipervisor), y reemplácelos con instrucciones más seguras usando técnicas como binario Traducción antes de ejecutarlos en el hardware. Cualquier error al no atrapar las instrucciones críticas o la traducción defectuosa puede tener implicaciones de seguridad en la forma de un SO invitado que se le permita ejecutar instrucciones privilegiadas
- El hipervisor ejecuta una memoria basada en software. Unidad de administración (MMU) que asigna una tabla de página de la sombra para cada máquina virtual ya que las máquinas virtuales invitadas no pueden ser se le otorgó acceso directo a la MMU basada en hardware ya que potencialmente les permitiría acceder a la memoria que pertenece al hipervisor y otras máquinas virtuales co-alojadas (en algunas situaciones). Sin embargo, una implementación defectuosa de MMU basada en software podría llevar a la divulgación de datos en espacios de direcciones arbitrarios, como segmentos de memoria que pertenecen a la hipervisor y máquinas virtuales ubicadas, lo que da como resultado una violación del aislamiento de la memoria.
- El hipervisor aprovecha el hardware.
- La unidad de administración de memoria de E / S para imponer la separación de memoria para los controladores y procesos de dispositivos mediante el uso directo Acceso a memoria (DMA). Esta característica está incorporada en el hipervisor y habilitada en el hardware mediante un cambio de firmware Si no se usa, puede resultar en una vulnerabilidad por la cual el DMA podría potencialmente ser utilizado como un vector de ataque común por una

máquina virtual para sobrescribir la memoria física utilizada por otras máquinas virtuales y procesos.

6.9.2.1 Ataques a hipervisores

Los emuladores de máquinas virtuales tienen muchos usos donde los más conocidos son VirtualBox, Parallels, VMware, QEMU) . Para los investigadores de antimalware, el uso más común es colocar código desconocido dentro de un entorno virtual, y ver cómo se comporta Una vez completado el análisis, el medio ambiente puede ser destruido, esencialmente sin riesgo para el entorno real que lo alberga. Esta práctica proporciona un seguro manera de ver si una muestra puede ser maliciosa. Los ataques a máquinas virtuales pueden ir desde el más simple realizado con un código malicioso casi imposible de detectar hasta una denegación de servicio total lo que imposibilita el acceso total a la VM y finalmente el ataque que permite el escape desde una máquina virtual a la maquina física [100].

Los emuladores de máquinas virtuales vienen en dos formas: "hardwarebound" (también conocido como para-virtualización) y "puro software "(a través de la emulación de la CPU). El" hardware enlazado " La categoría se puede dividir en dos subcategorías: "hardwareassisted" y "guest de privilegio reducido" (o ring 1 guest) [101]. Ambas formas de la máquina virtual vinculada por hardware, se basan en la CPU real para ejecutar instrucciones no sensibles a una velocidad nativa. Logran un mejor rendimiento, por esta razón, en comparación con las implementaciones de software puro. Sin embargo, dado que ejecutan instrucciones en una CPU real, deben realizar algunos cambios en el entorno para poder compartir los recursos de hardware entre el sistema operativo invitado y el sistema operativo host. Algunos de estos cambios son visibles para las aplicaciones dentro del sistema operativo invitado, si las aplicaciones saben cómo se ven esos cambios.

6.9.3 Forensia en Hipervisores

El continuo y creciente uso de la virtualización es un obstáculo para la aplicación de técnicas forenses en la actualidad. Dado que dificulta la tarea de adquisión de memoria pues las herramientas existentes únicamente pueden acceder hasta donde el sistema operativo puede acceder porque lo que no sería posible accede a la memoria reservada por el administrador de la máquina virtual en sí. Por otro lado, cuando se adquiere una imagen física completa mediante hardware, las imágenes obtenidas no se pueden analizar adecuadamente [102].

Como bien se sabe la virtualización es uno de los pilares principales de la computación en la nube, estos escenarios plantean serios problemas para las investigaciones forenses, pues cualquier incidente que se presente como un intento de escape de la máquina virtual o comprometer el hipervisor en una infraestructura de nube se encuentra fuera del alcance de las actuales técnicas forenses.

Encontrar el hipervisor superior, es decir, el que tiene control total sobre la máquina, es ciertamente el objetivo principal de un análisis forense. Pero desde ahora, la mayoría de los hipervisores básicos admiten la virtualización anidada, al extraer también la jerarquía de hipervisores y máquinas virtuales anidadas podría ayudar a un analista a comprender mejor lo que se está ejecutando dentro del sistema.

En el peor de los casos, los campos podrían almacenarse en estructuras de datos complejas (como tablas hash) o guardarse en una forma codificada, lo que complica enormemente la tarea de ubicarlos en la memoria.

El NIST define la computación en la nube como "un modelo para habilitar el acceso a la red ubicuo, conveniente y a pedido a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionado y liberado con un mínimo esfuerzo de gestión o interacción del proveedor de servicios [103]. Este modelo de nube se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación ". Cloud forensics es un proceso aplicado a una implementación de este modelo.

Para todas las partes interesadas en el cloud forensic existen múltiples desafíos que podrían ser clasificados como técnicos, legales y organizativos pero que al compararse con los de forensia tradicional se considera que los de nube son exclusivos a su entorno

Se debe tener en cuenta que en la forensia tradicional los investigadores pueden tener control total sobre el equipo y sus componentes, de manera que la adquisición de información es mucho más sencilla, teniendo un fácil y directo acceso a los registros, a la memoria y a la red

Mientras que, en la computación en la nube, el hipevisor (como potencial artefacto forense) véase la figura 99, incrementa la complejidad que tiene la arquitectura del sistema obteniendo diferencias significativas en los sistemas operativos que trabajan bajo el mando del hipervisor por lo que además de que la búsqueda se haría uno por uno, entonces habría que hacerla con diferentes herramientas o comandos. Por lo tanto, la descentralización de los registros entre las diferentes capas, la accesibilidad del registro, la tenencia de las nubes y la preservación de la cadena de custodia hacen que el análisis de registros sea un desafío, además los registros obtenidos de hipervisores no son fáciles de comprender.

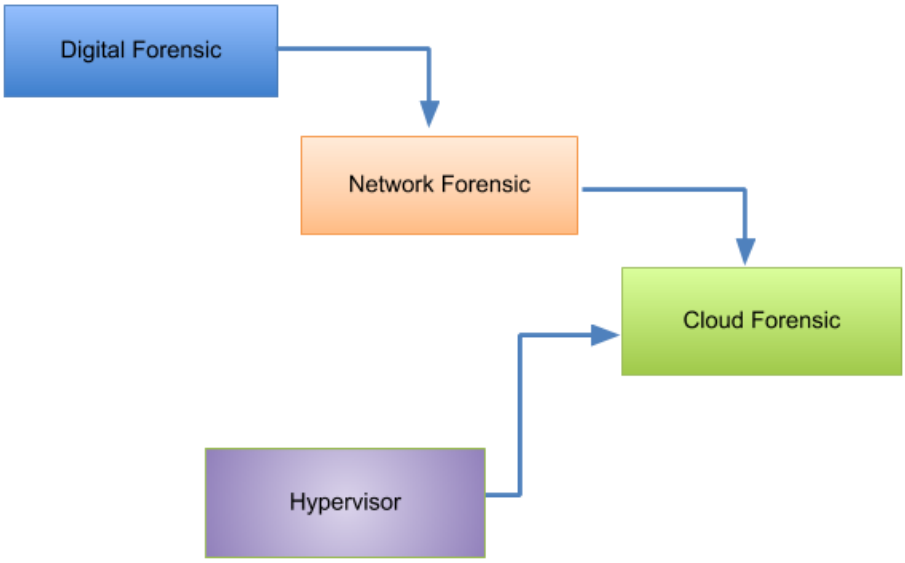


Fig. 99 Hipervisores En forensia digital

La identificación, recopilación y preservación de los medios puede ser particularmente desafiante en una nube. Entorno informático dado varios factores posibles, incluyendo [104]:

a. Identificación del proveedor de la nube y sus socios. Esto es necesario para entender mejor el medio ambiente y así abordar los siguientes factores
b. La capacidad de identificar de manera concluyente las cuentas correctas mantenidas en la nube por un consumidor, Especialmente si se utilizan diferentes personajes cibernéticos.
c. La capacidad del examinador forense para obtener acceso a los medios deseados.
d. Obtención de asistencia del personal de servicio del proveedor de infraestructura / aplicaciones en la nube.
e. Entender la topología, las políticas de propiedad y el sistema de almacenamiento dentro de la nube.
f. Una vez que se obtiene el acceso, la capacidad del examinador para completar una imagen de los medios con sonido forense.
g. El gran volumen de los medios de comunicación.
h. La capacidad de responder de manera oportuna a más de una ubicación física si es necesario.
i. Descubrimiento electrónico, colección de archivos de registro y derechos de privacidad dado un sistema de tenencia múltiple. (¿Cómo se hace recopilar el conjunto de archivos de registro aplicables para este asunto versus información extraña con posibles derechos de privacidad protecciones?)
j. Validación de la imagen forense.
k. La capacidad de realizar análisis en datos encriptados y la capacidad del recolector para obtener claves para descifrado
l. El sistema de almacenamiento ya no es local.

m. A menudo no hay forma de vincular la evidencia dada a un sospechoso en particular que no sea confiar en la nube palabra del proveedor

Una parte importante a analizar durante una investigación forense son los logs donde se registran todas las actividades realizadas por el SO durante su funcionamiento, no es nada diferente para las MV. Sin embargo, muchas veces pueden ser corruptos o difíciles de entender. Donde se puede encontrar diversa información sobre la actividad en general como se muestra a continuación:

- Inconsistencia en la actividad de la máquina virtual: Las líneas de tiempo pueden surgir porque los eventos de registro del kernel del hipervisor en la línea de tiempo están fuera de secuencia, o faltan los eventos de VM que deberían estar en la línea de tiempo.

- Logs en el Storage (acceso a bajo nivel): Los equipos de Storage tienen un acceso de Administración (usualmente web) y genera un log de las actividades de los usuarios que acceden. Los logs usualmente guardan:
    - Usuarios que accedieron
    - Direcciones IP orígenes de las conexiones
    - Actividad que realizaron
- Log en el Firewall interno: Si tenemos un Firewall interno que nos protege la red de administración, seguramente tendremos log en el Firewall que nos darán más información. En estos log tendremos.
    - Tráfico autorizado o no entre segmentos de red
    - Intentos de conexión
    - Direcciones IP orígenes / destino de las conexiones
    - Horarios de actividades

Un enfoque alternativo para un atacante es poner en peligro el sistema de virtualización, es explotar la máquina virtual que se ejecuta sobre el hipervisor, lo que puede ser posible si un atacante ejecuta código en una máquina virtual que permite que un sistema operativo que se ejecuta dentro del hipervisor se rompa e interactúe directamente con él. Este tipo de ataque podría permitirle al atacante acceder al sistema operativo del host, así como a todas las máquinas virtuales que se ejecutan en ese host. Esto se llama escape de la máquina virtual. Hay varios tipos de escape de máquinas virtuales que podrían ser posibles.

Las investigaciones de seguridad Tom Liston y Ed Skoudis demostraron varias herramientas que podrían desarrollarse para crear ataques de escape de VM [105]. Estas herramientas son:

- VMchat: este software de chat simple usó el canal de comunicación del hipervisor VMware como puerta trasera para enviar mensajes entre los sistemas operativos de los huéspedes o entre el sistema operativo de los huéspedes y el host. Este software simple hizo

  No requiere ningún código especial para ser instalado. Un ataque de inyección DLL puede explotar VMware en el sistema operativo del host, de modo que permite que la

aplicación se ejecute en el acceso del host a la memoria de la máquina VMware invitada. Cuando esto sucediera, el búfer de memoria se usará como canal de intercambio entre la máquina host y cliente como un búfer compartido. Esta herramienta no se escapa por completo de la máquina virtual; sin embargo, explote el límite entre la máquina host y VMware [105][105] [105].

- VMcat: esta extensión de la herramienta para que la idea de VMchat envíe resultados simples de (stdin) y (stdout) entre el canal de comunicación creado con VMchat, que se puede utilizar para hacer un túnel de un shell de comando entre los hosts y el invitado [105]

- VM Drag-n-Sploit: modificando el componente VMware en el invitado (VMwareService.exe), los investigadores lograron monitorear y cambiar todos los datos pasando por el canal de comunicación. Esto permitió ejecutar código en el SO huésped. eso podría permitir que un archivo que se arrastra y suelte sea reemplazado por un archivo arbitrario [105].

- VMft: un usuario en cualquier sistema operativo invitado con cualquier nivel de privilegio puede La lectura y escritura de datos en el sistema operativo host a través de la carpeta compartida está habilitada y una carpeta se comparte con una máquina virtual invitada [105].

6.9.3.1 Experimento

En cuanto a los hipervisores utilizados para la experimentación se usaron VMWare como primera medida tanto en Linux como en Windows con la intensión de conocer los tipos de log que pudiera generar el software como tal.
Para esto es necesario buscar la información en las carpetas de instalación como se observa en la figura 100.

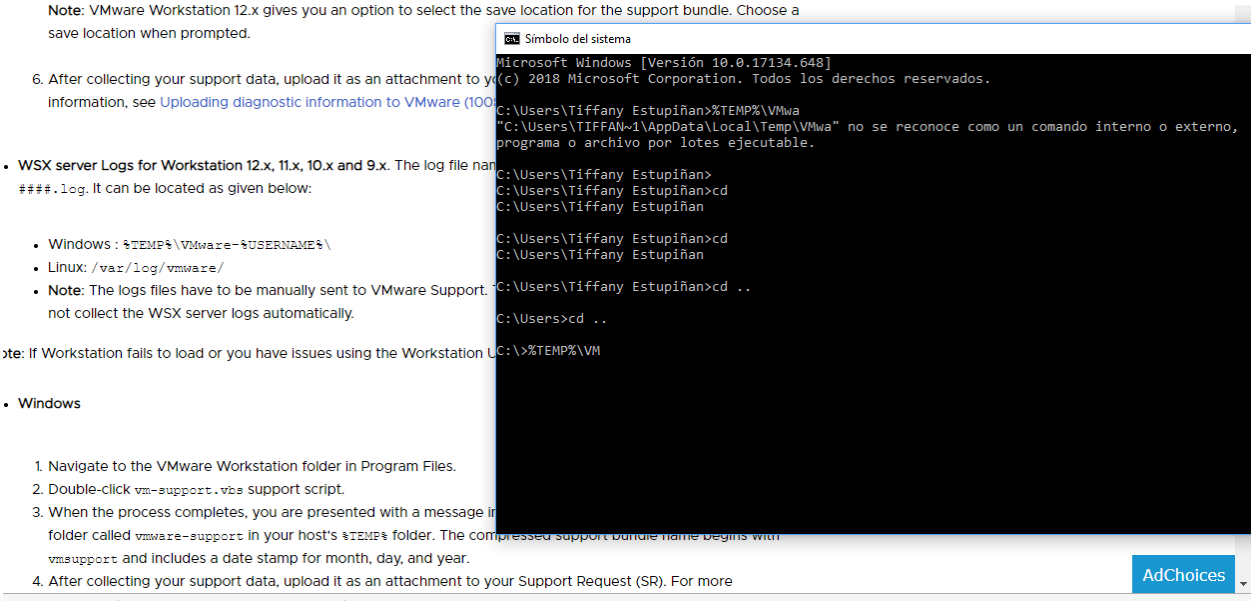


Fig 100 Accediendo al Hipervisor

Donde se podrá encontrar el archivo de soporte de la figura 101 de vmware que es el encargado de hacer la colecta automatica de logs.

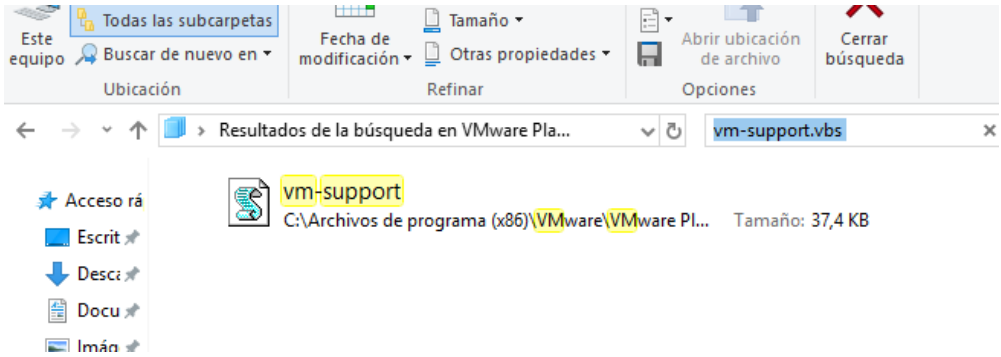


Fig 101 vm-support

Al ejecutar el script, comenzará automaticamente a generar los archivos y a correr el proceso como se evidencia en la figura 102. Los archivos son generados en un archivo de tipo .zip como se puede ver en la figura 103, donde al descomprimirlo se encontrará toda la informacion que puede entrega el hypervisor como tal .

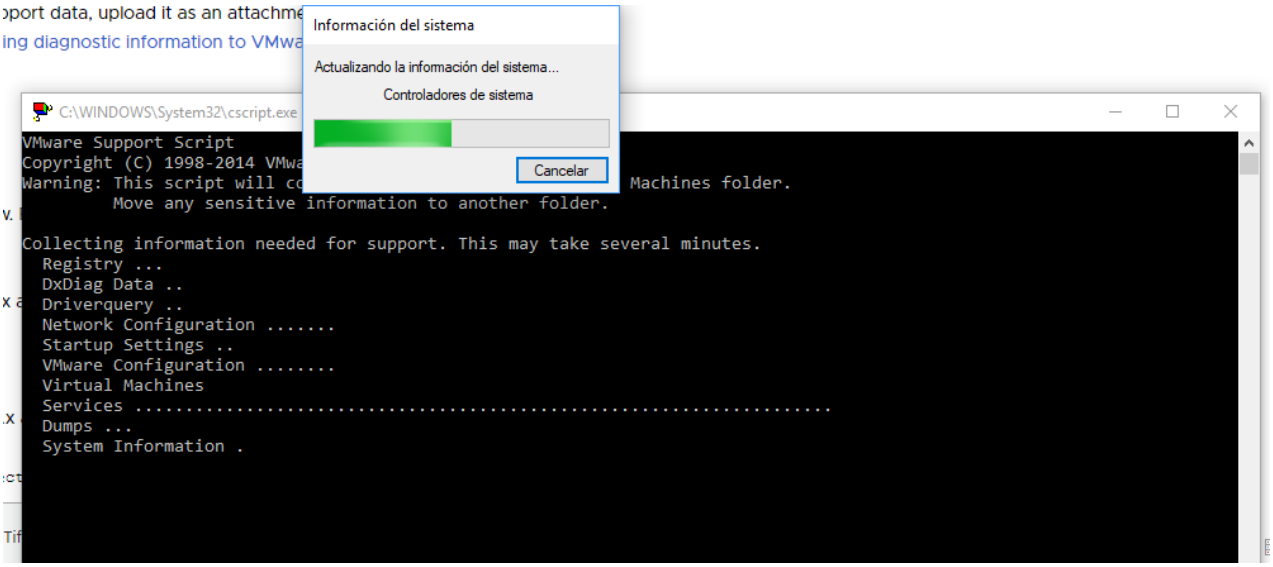


Fig 102 Generacion de archivos Log

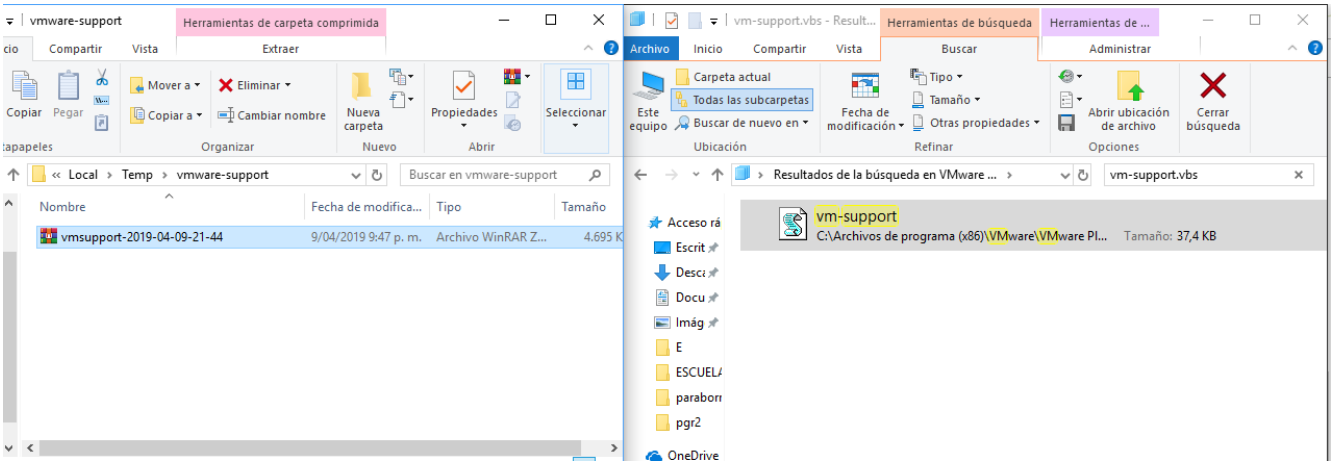


Fig 103 Zip de logs generados

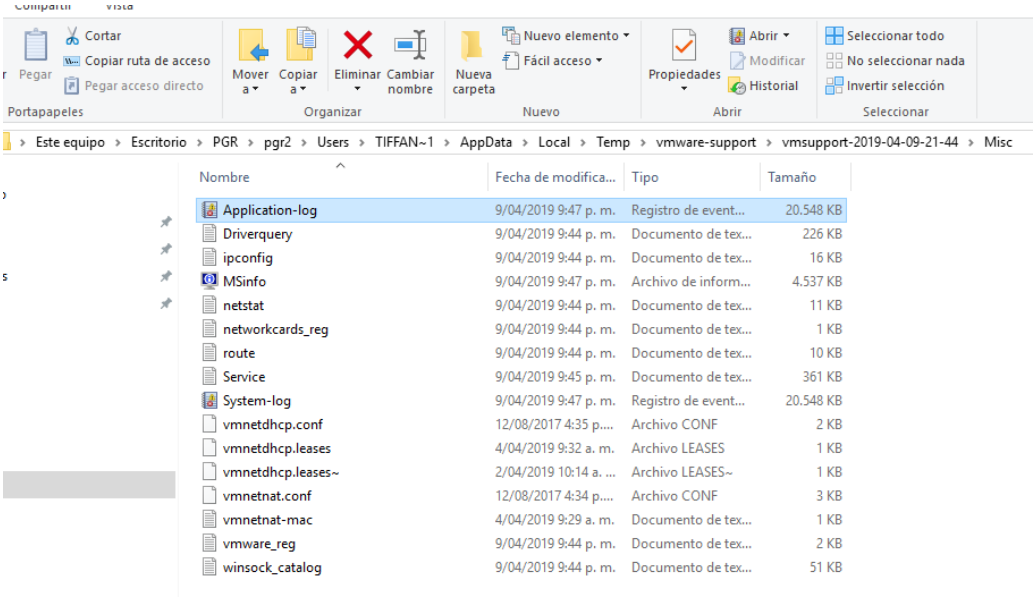


Fig 104 Logs recuperados

Estos logs entregados por el hipervisor permiten averiguar las veces que ha sido encendida o suspendida la maquina virtual, las conexiones de red que ha hecho y los recursos a los que ha tenido acceso tal como se evidencia en las figuras 105 a 115 .

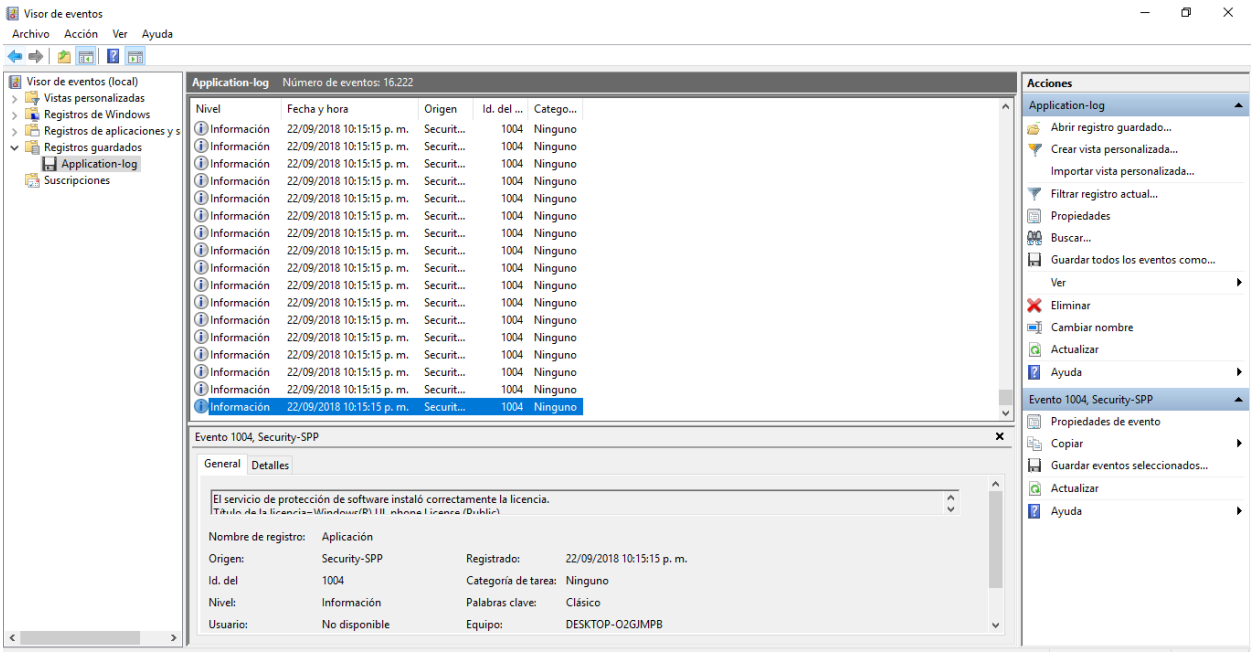


Fig 105 Información de Log

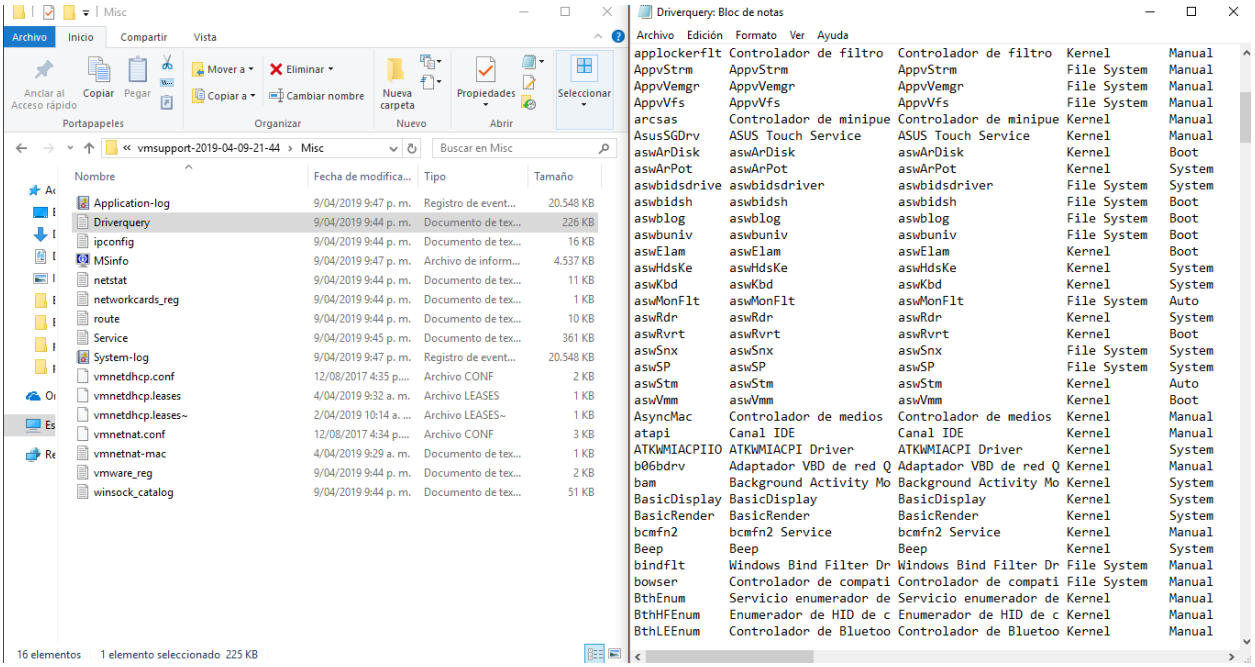


Fig 106 Drivers accedidos

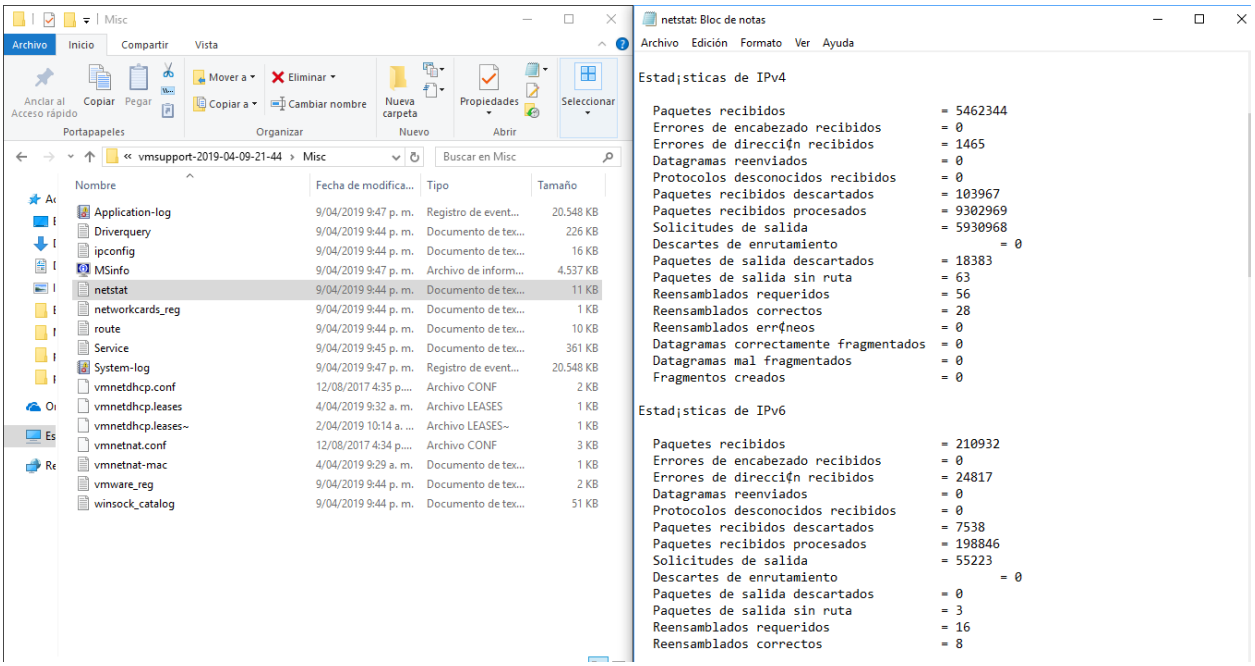


Fig 107 Estadisticas de Conexion

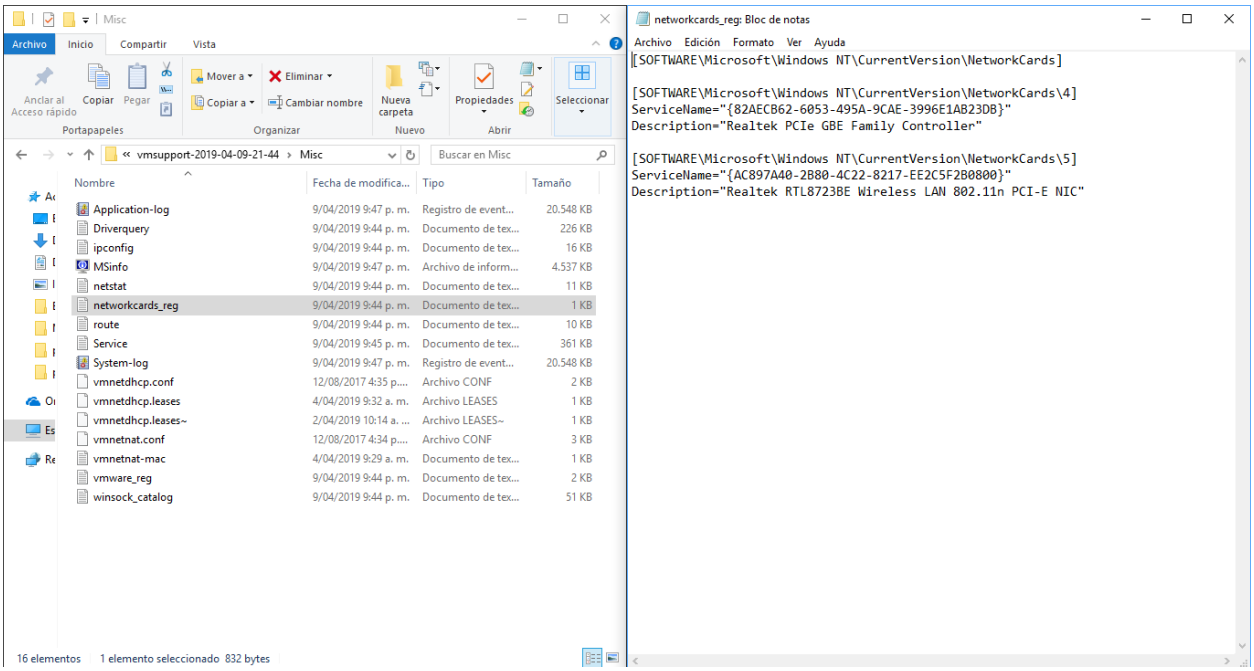


Fig 108 Acceso a recurso de red

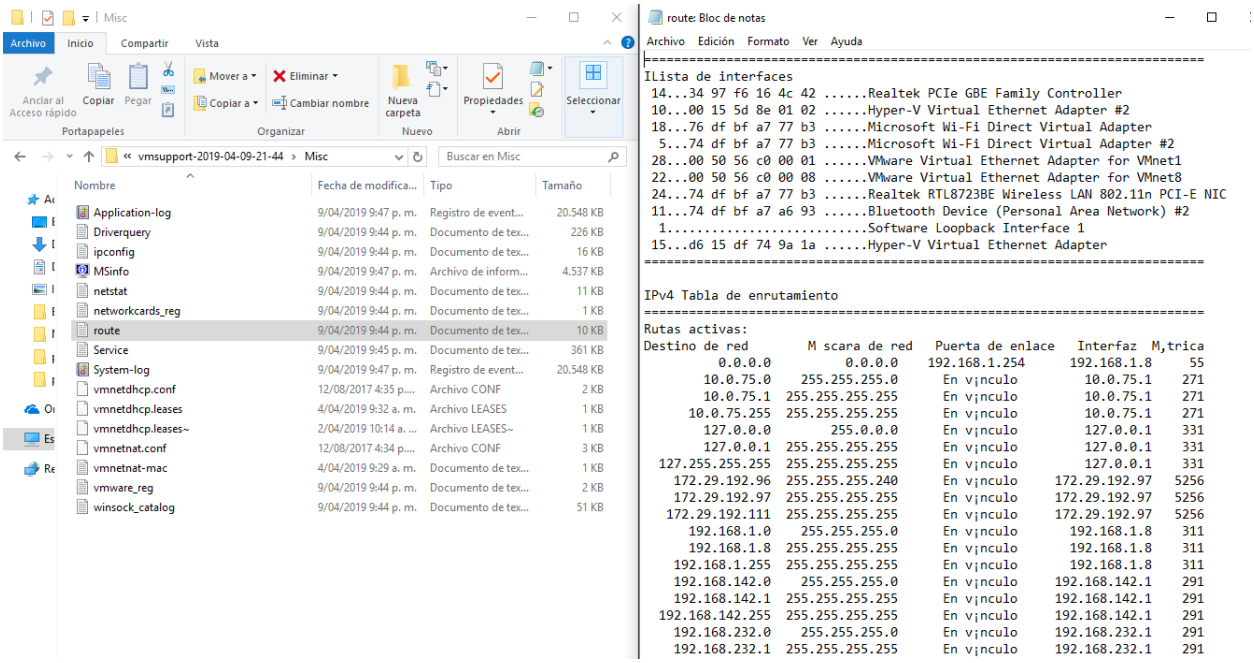


Fig 109 Conexiones realizadas

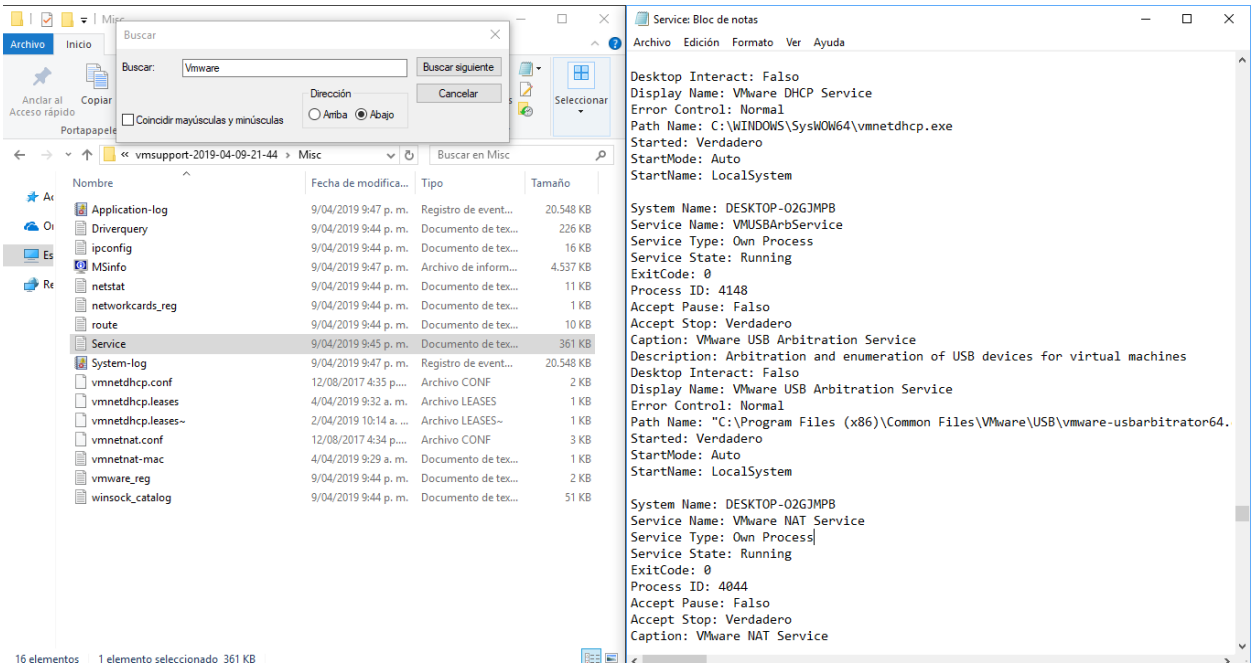


Fig 110 Listado de peticiones de Vmware

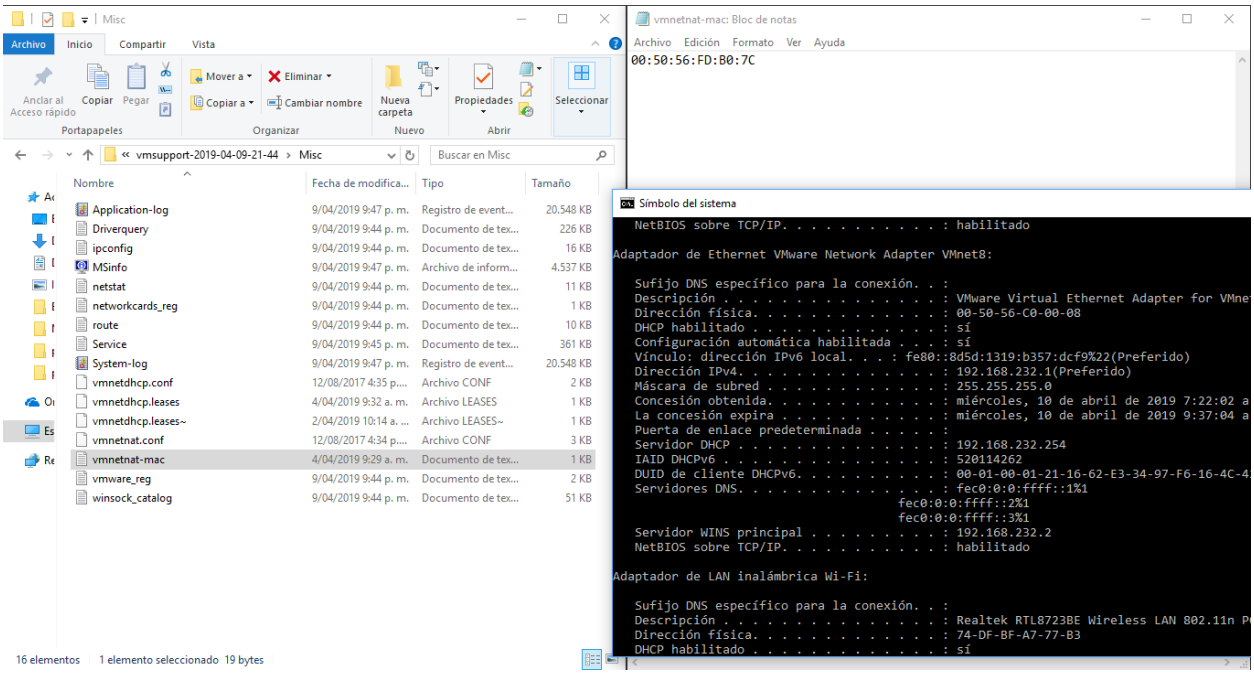


Fig 111 conexiones hechas por la maquina virtual basada en la MAC

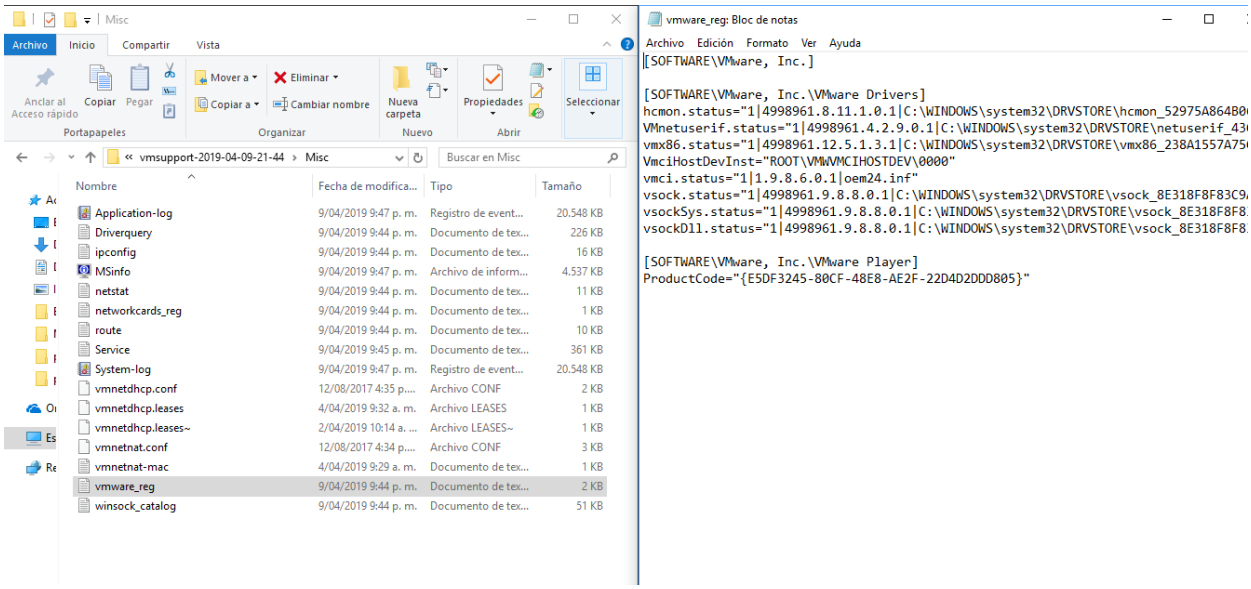


Fig 112 Registro de Uso

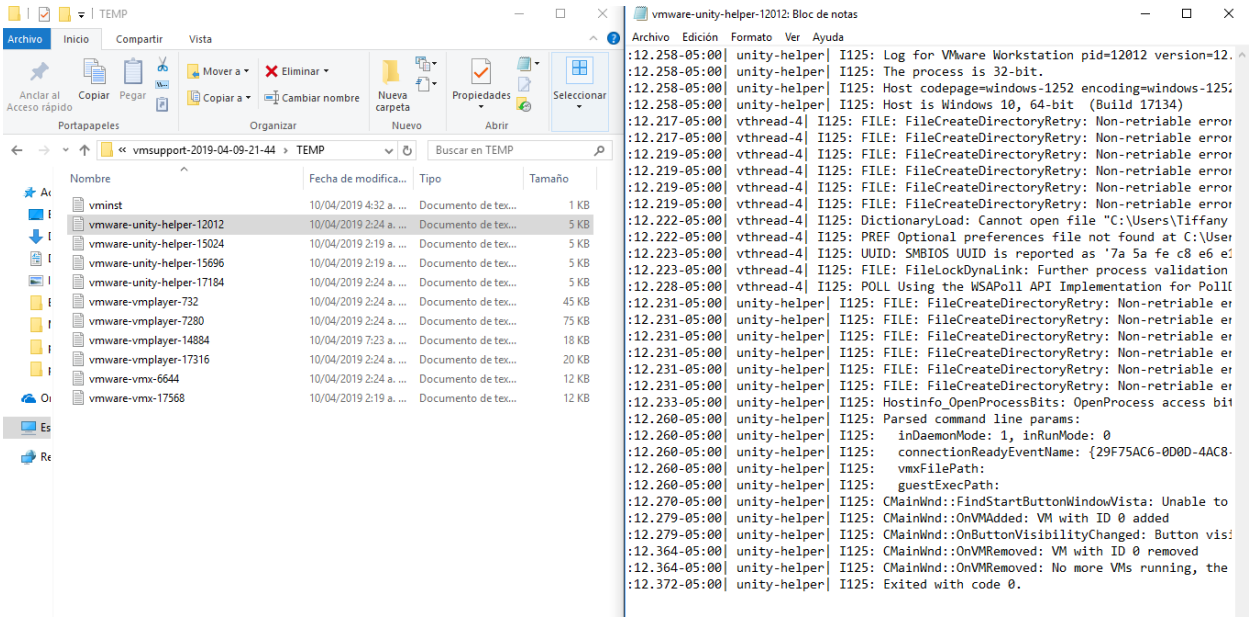


Fig 113 Log de VMWare

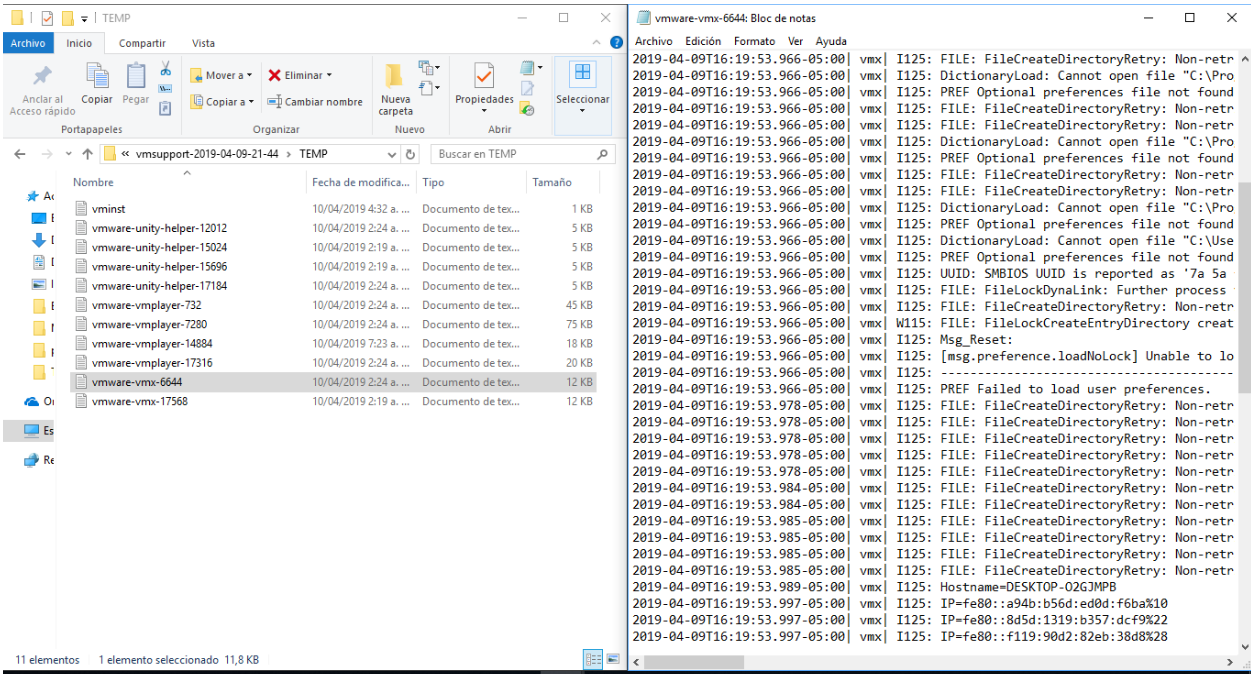


Fig 114 Log Vmware

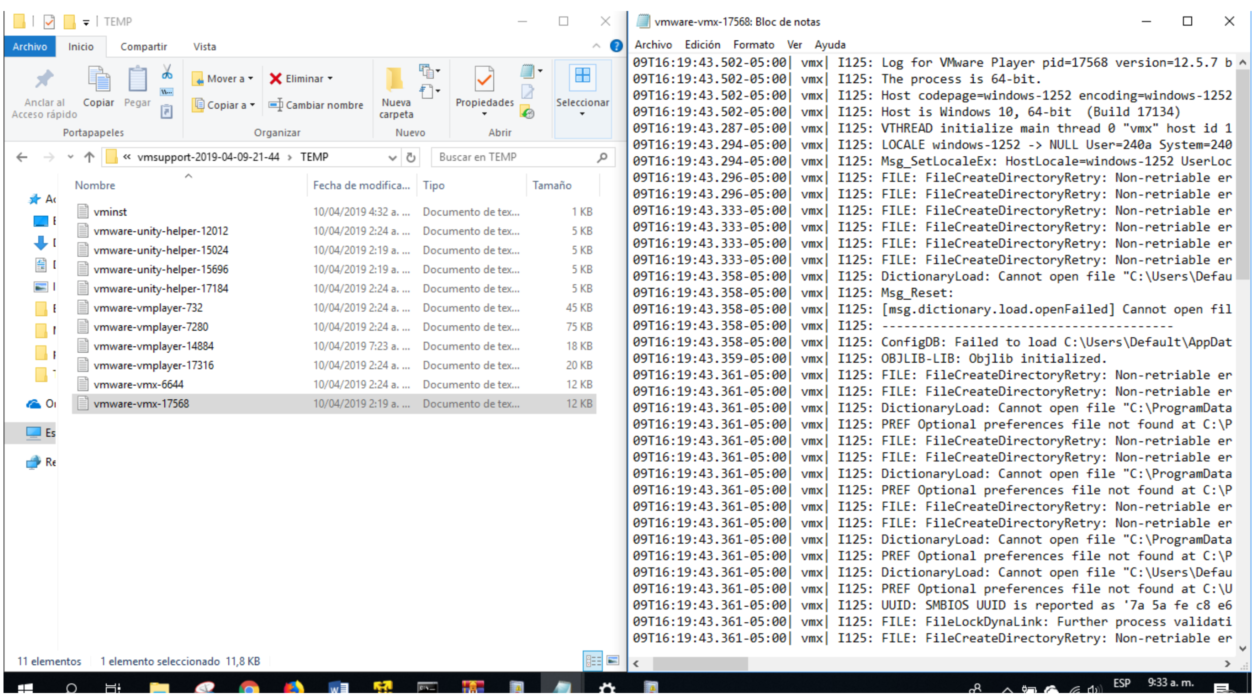


Fig 115 log VMWare

De igual manera se hizo la recopilacion de logs en linux con el virtualizador VMWare , donde se virtualizo un sistema operativo ligero como lo es Linux Puppy solo con el fin de obtener los logs que genere.

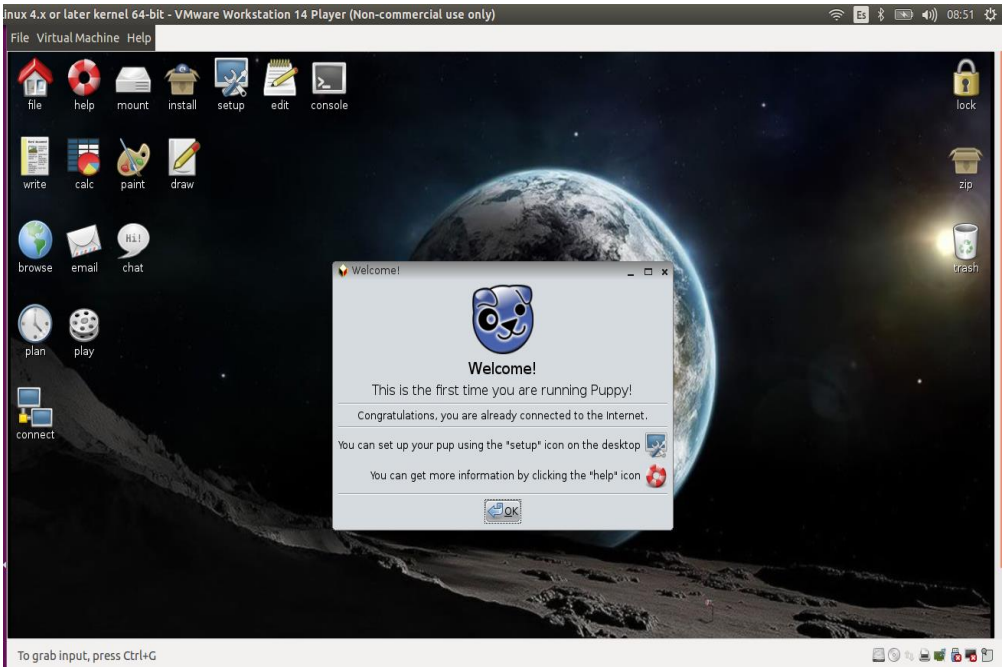


Fig 116 Linux Puppy virtualizado con VMWare

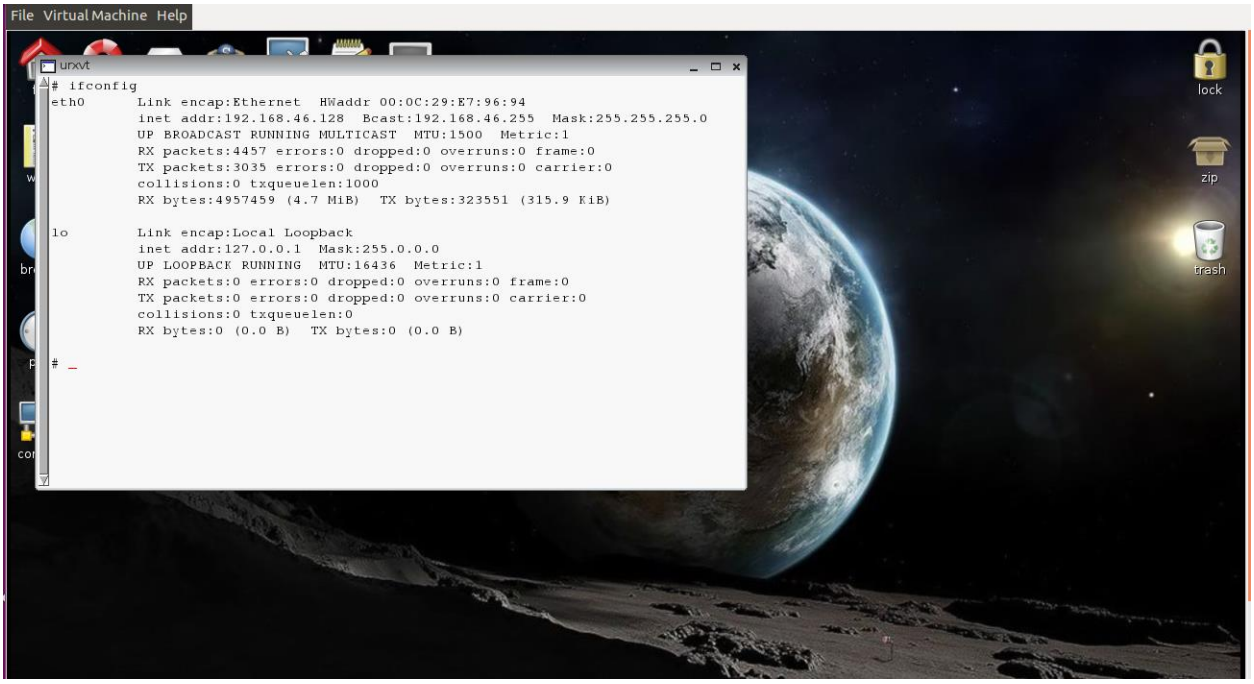


Fig 117 Configuraciones de red en Linux Puppy

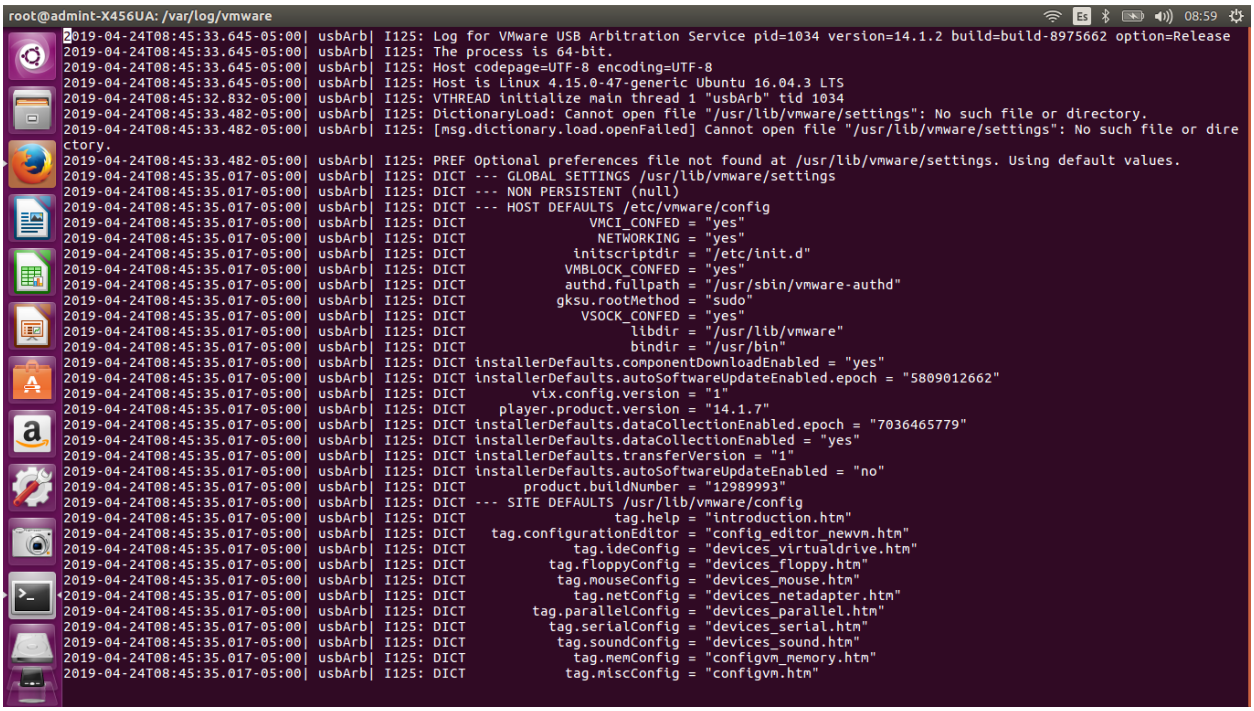


Fig 118 Logs de Vmware en Linux

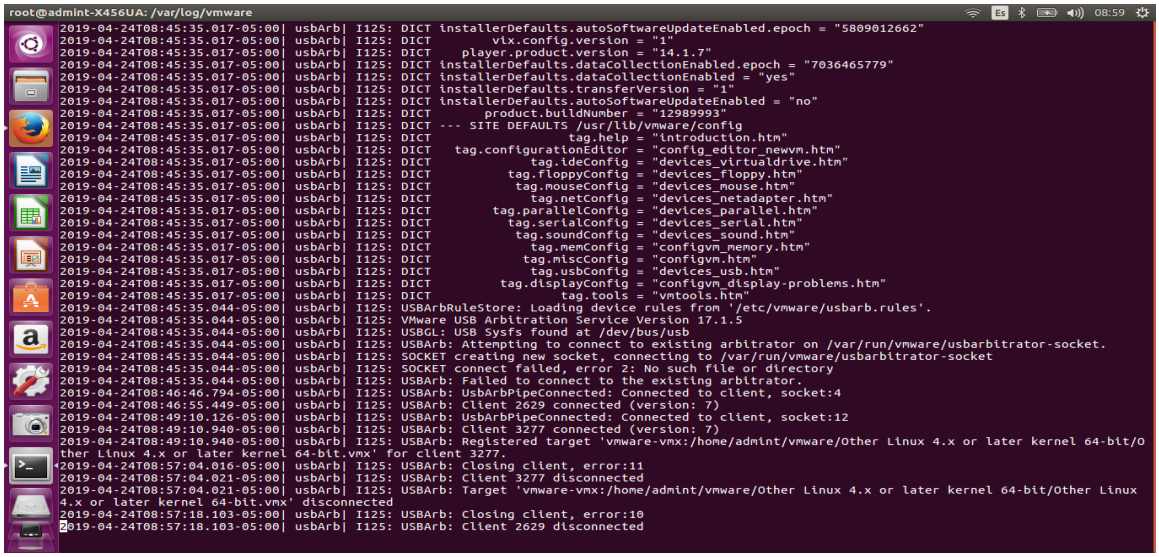


Fig 119 Logs de VMWare en Linux

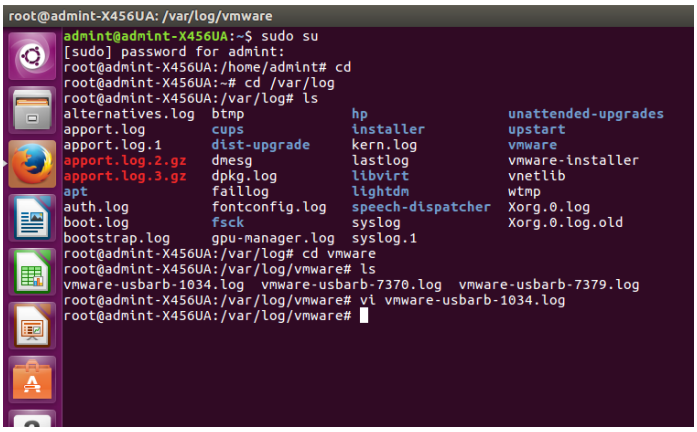


Fig 120 Logs de VMWare en Linux

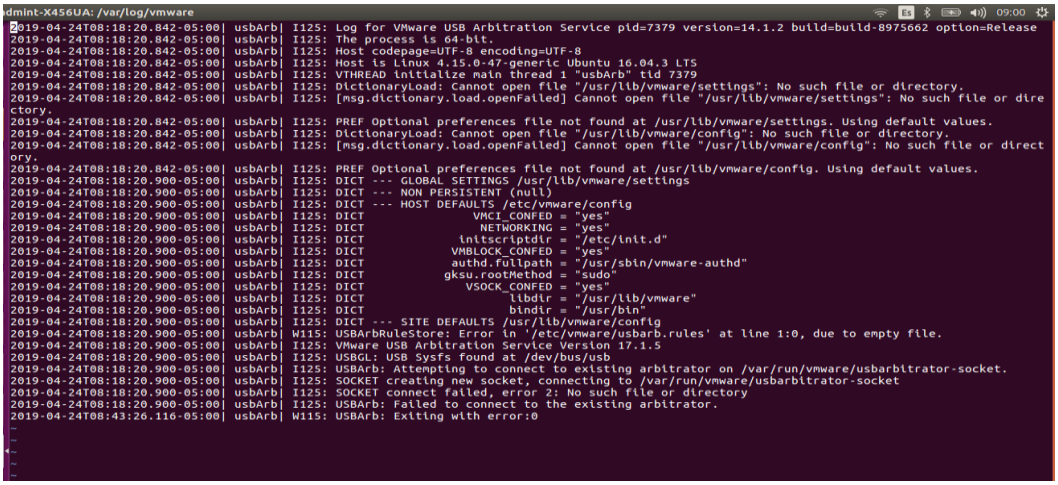


Fig 121 Logs de VMWare en Linux

- KVM (LINUX)/ QEMU

Otra parte de la investigación se llevó a cabo en el hipervisor de Linux , que permite la virtualización de máquinas virtuales de cualquiera tipo. Sin embargo, para el experimento como tal se usa una maquina ligera de distribución Linux como lo es puppy como se aprecia en la figura 122 con el simple objetivo de obtener los logs que pueda generar el virtualizador Qemu como se observa en la figura 123

Fig 122 Qemu virtualizando Linux Puppy

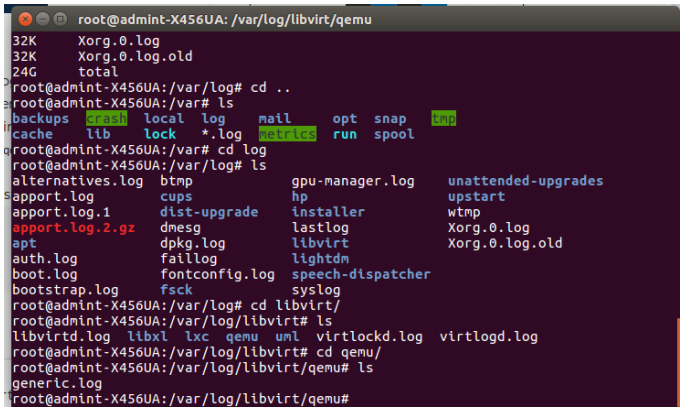


Fig 123 obteniendo Logs de Qemu

Accediendo al Sistema de logs de Linux se puede encontrar la carpeta de Qemu donde se encuentran los registros generados por el virtualizador como en la fig. 124.

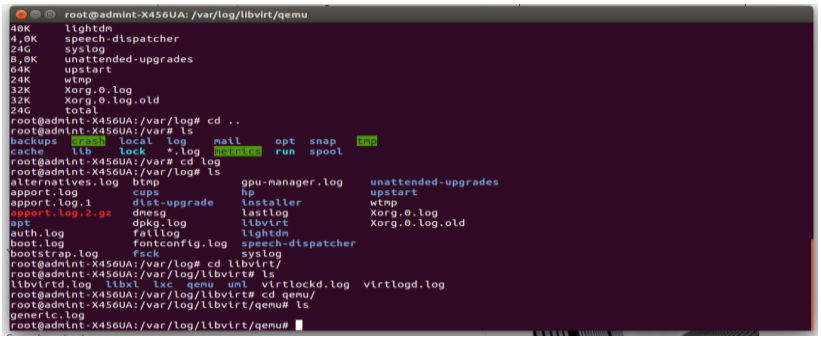


Fig 124 Acceso a logs de Qemu

Donde se aprecia un log general , que al acceder a este por consola (aunque tambien es posigle acceder por archivos) se evidencia todos los procesos y acciones realizadas por el virtualizador , incluso registra el momento de apagado de la maquina virtual como se evidencia en la figura 125 y 126 .

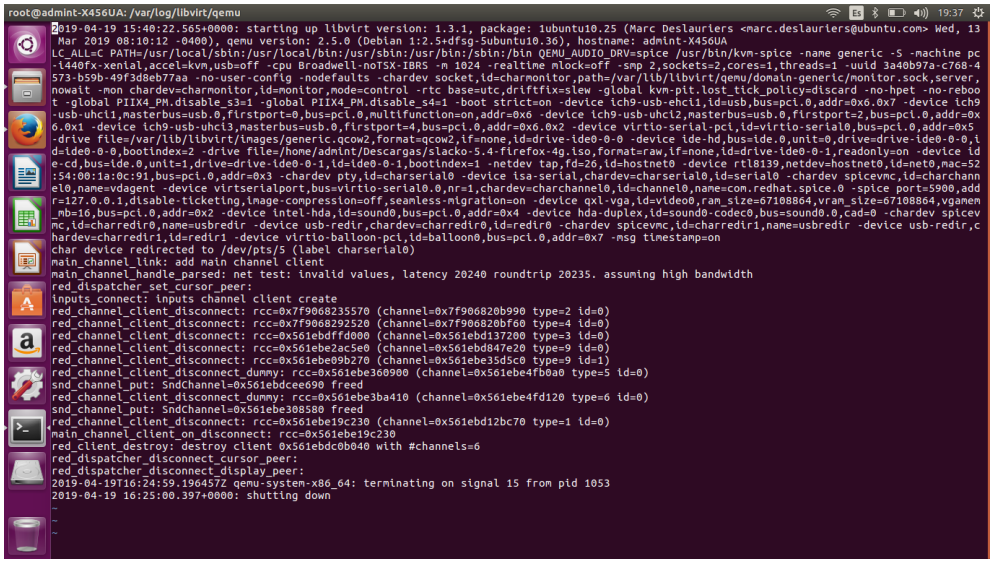


Fig 125 Log de Qemu

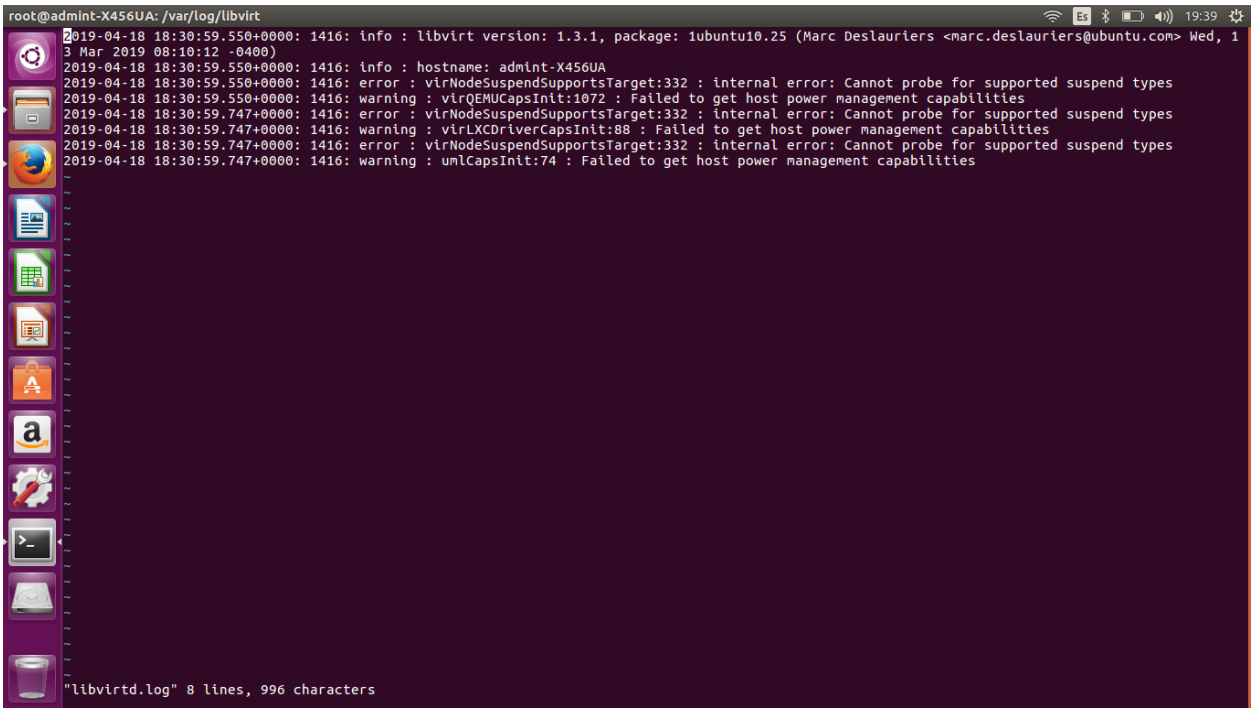


Fig 126 Log virtualizador

- VIRTUAL BOX

```
".VirtualBox" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Tiffany Estupiñan>cd .VirtualBox

C:\Users\Tiffany Estupiñan\.VirtualBox>find *.log
FIND: formato de parámetros incorrecto

C:\Users\Tiffany Estupiñan\.VirtualBox>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 18DD-000F

 Directorio de C:\Users\Tiffany Estupiñan\.VirtualBox

22/01/2019  10:42 p. m.    <DIR>          .
22/01/2019  10:42 p. m.    <DIR>          ..
22/01/2019  10:42 p. m.               928 selectorwindow.log
19/11/2018  10:16 a. m.               928 selectorwindow.log.1
22/01/2019  10:42 p. m.             4.680 VBoxSVC.log
19/11/2018  10:16 a. m.             3.690 VBoxSVC.log.1
05/10/2018  01:04 a. m.               866 VBoxSVC.log.2
05/10/2018  01:04 a. m.             2.132 VBoxSVC.log.3
04/10/2018  08:55 p. m.             5.599 VBoxSVC.log.4
20/05/2018  09:45 p. m.            13.750 VBoxSVC.log.5
22/01/2019  10:42 p. m.             2.270 VirtualBox.xml
22/01/2019  10:42 p. m.             2.171 VirtualBox.xml-prev
              10 archivos         37.014 bytes
               2 dirs  505.812.975.616 bytes libres

C:\Users\Tiffany Estupiñan\.VirtualBox>
```

Fig 127 Accediendo a Logs de VirutalBox

```
VirtualBox COM Server 5.2.12 r122591 win.amd64 (May  9 2018
10:42:46) release log
00:00:00.354635 main     Log opened
2018-11-19T15:15:59.588411300Z
00:00:00.354635 main     Build Type: release
00:00:00.354635 main     OS Product: Windows 10
00:00:00.354635 main     OS Release: 10.0.17134
00:00:00.354635 main     OS Service Pack:
00:00:00.457879 main     DMI Product Name: X456UA
00:00:00.470147 main     DMI Product Version: 1.0
00:00:00.470147 main     Host RAM: 8057MB (7.8GB) total, 2982MB
(2.9GB) available
00:00:00.544586 main     Executable: C:\Program Files\Oracle
\VirtualBox\VBoxSVC.exe
00:00:00.544586 main     Process ID: 14124
00:00:00.544586 main     Package type: WINDOWS_64BITS_GENERIC
00:00:00.547459          VirtualBox: object creation starts
00:00:00.548456          Home directory: 'C:\Users\Tiffany
EstupiÃ±an\.VirtualBox'
00:00:00.549453          Installed Drivers:
00:00:00.612398            C:\WINDOWS\system32\DRIVERS
\VBoxNetLwf.sys (Version: 5.2.12.22591)
00:00:00.675191            C:\WINDOWS\system32\DRIVERS
\VBoxUSBMon.sys (Version: 5.2.12.22591)
00:00:00.710211            C:\WINDOWS\system32\DRIVERS
\VBoxDrv.sys (Version: 5.2.12.22591)
00:00:01.141584          Loading settings file "C:\Users\Tiffany
EstupiÃ±an\.VirtualBox\VirtualBox.xml" with version "1.12-
windows"
00:00:01.352264          Getting USB descriptor failed with
```

Fig 128 Log de virtual Box

```
43:55:36.795736 MainPower Log continuation - Log started
2018-10-03T05:59:47.740520000Z
43:55:39.450477 dns-monitor HostDnsMonitor: old information
43:55:39.450477 dns-monitor   server 1: 190.157.8.33
43:55:39.450477 dns-monitor   server 2: 190.157.8.1
43:55:39.450477 dns-monitor   no domain set
43:55:39.450477 dns-monitor   no search string entries
43:55:39.450477 dns-monitor HostDnsMonitor: new information
43:55:39.450477 dns-monitor   no server entries
43:55:39.450477 dns-monitor   no domain set
43:55:39.450477 dns-monitor   no search string entries
43:55:39.450477 dns-monitor HostDnsMonitorProxy::notify
43:55:44.724804 dns-monitor HostDnsMonitor: old information
43:55:44.724804 dns-monitor   no server entries
43:55:44.730354 dns-monitor   no domain set
43:55:44.730354 dns-monitor   no search string entries
43:55:44.730354 dns-monitor HostDnsMonitor: new information
43:55:44.730354 dns-monitor   server 1: 190.157.8.33
43:55:44.730354 dns-monitor   server 2: 190.157.8.1
43:55:44.730354 dns-monitor   no domain set
43:55:44.730354 dns-monitor   no search string entries
43:55:44.730354 dns-monitor HostDnsMonitorProxy::notify
43:58:58.099937 USBPROXY Getting USB descriptor failed with
error 31
43:59:08.186123 USBPROXY Getting USB descriptor failed with
error 31
43:59:08.187333 USBPROXY Getting USB descriptor failed with
error 31
43:59:08.187333 USBPROXY USB: Unknown USB device detected
(idVendor: 0x04f2  idProduct: 0xb52b)
```

Fig 129 Log de encendido de VirtualBox

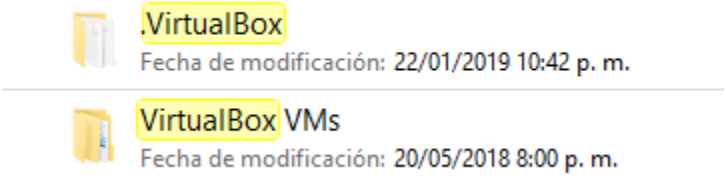


Fig 130 Acceso por archivos

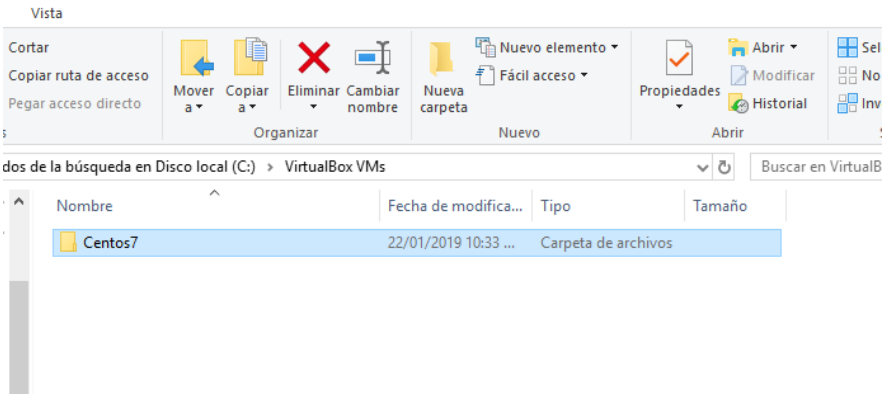


Fig 131 Maquina virtulizada en VirtualBox

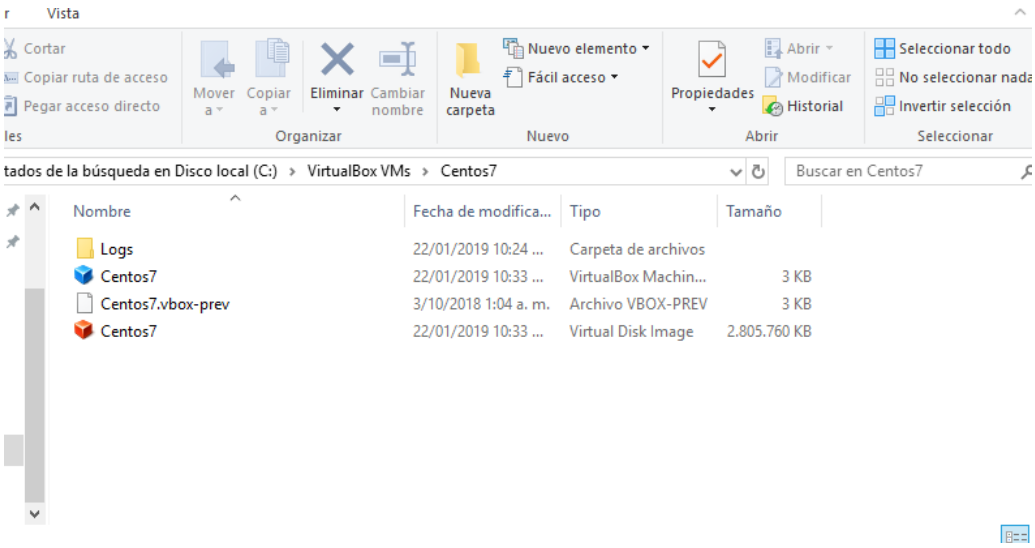


Fig 132 Logs correspondientes a la maquina virtualizada

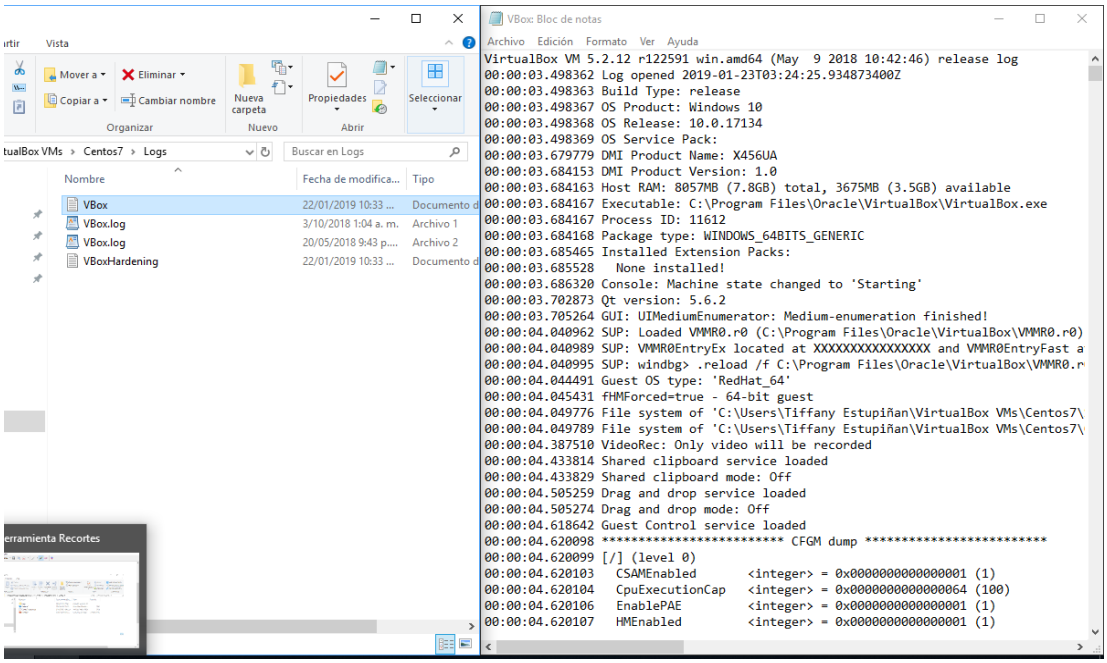


Fig 133 Contenido de los Logs de la maquina virtual

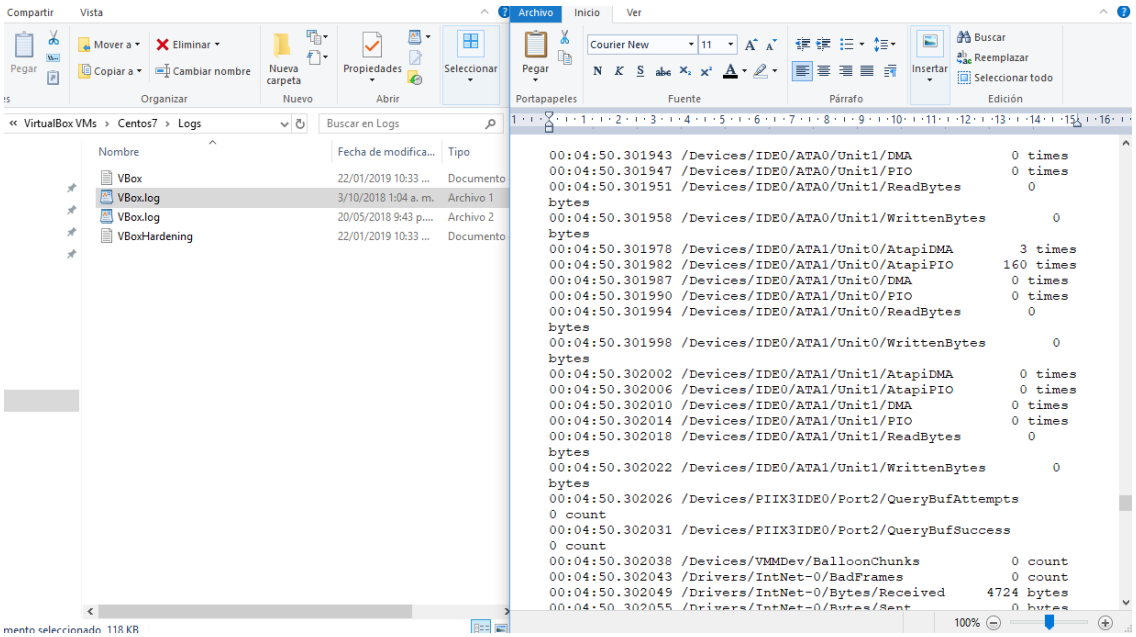


Fig 134 contenido de logs de maquina virtual

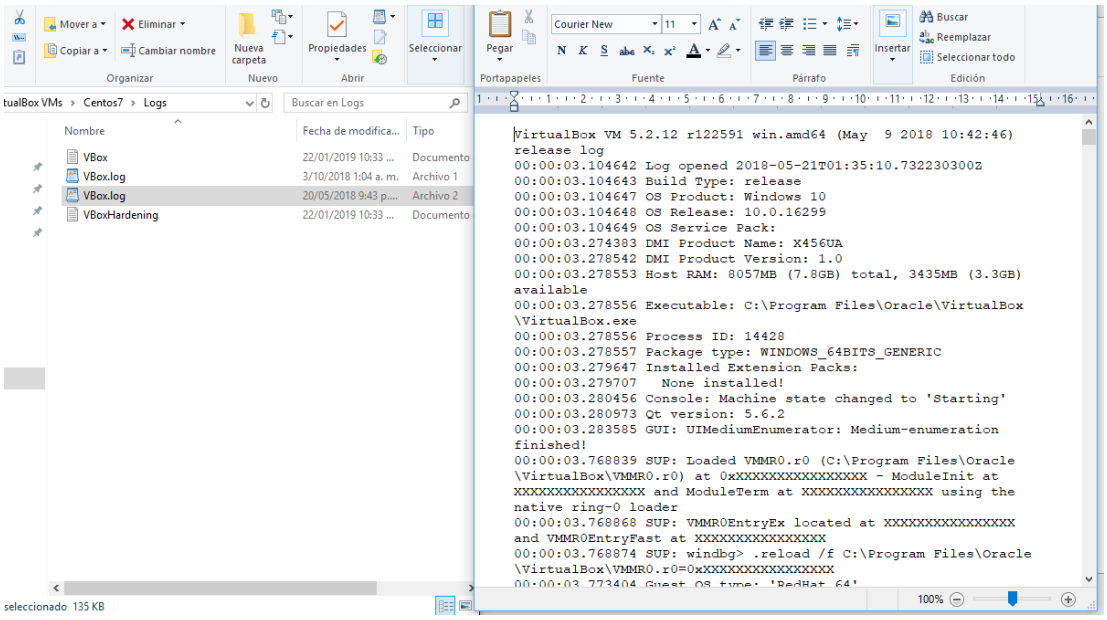


Fig 135 Contenido de los logs de maquina virtual

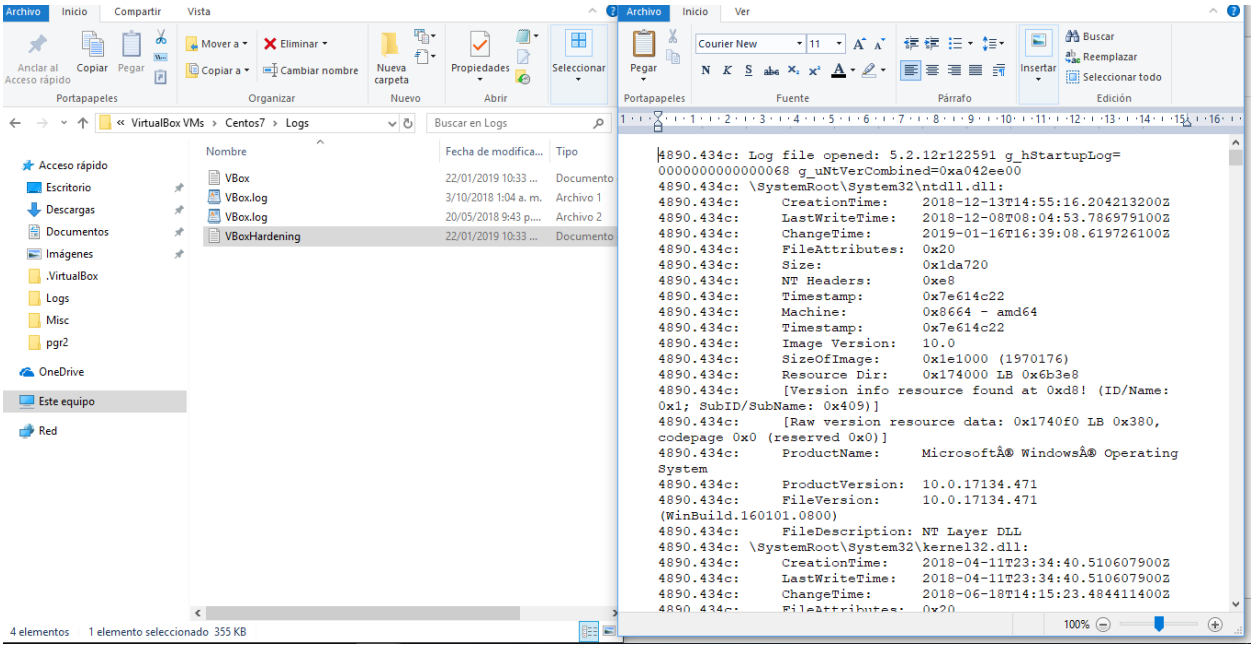


Fig 136 Log de maquina virtual

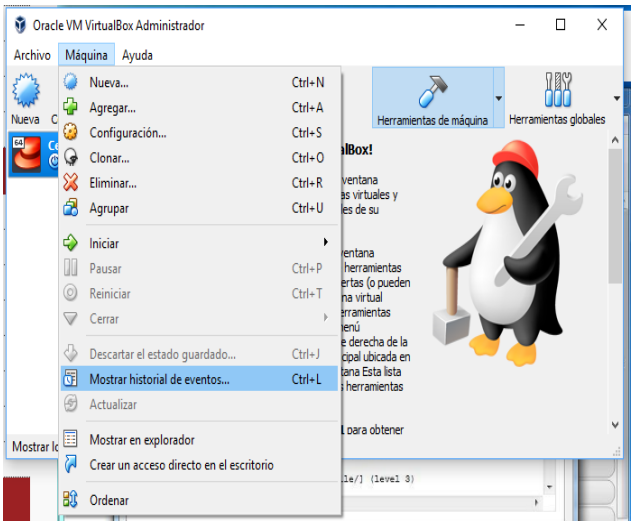


Fig 137 Logs desde virtual Box

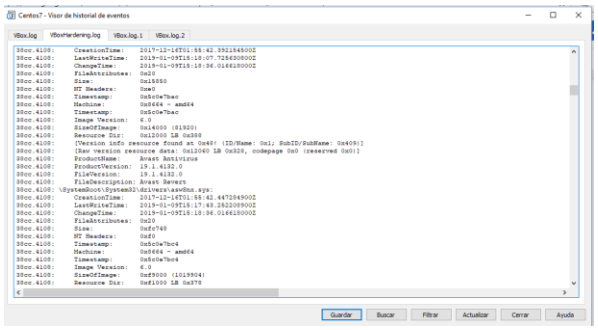


Fig 138 Log visualizado desde virtual box

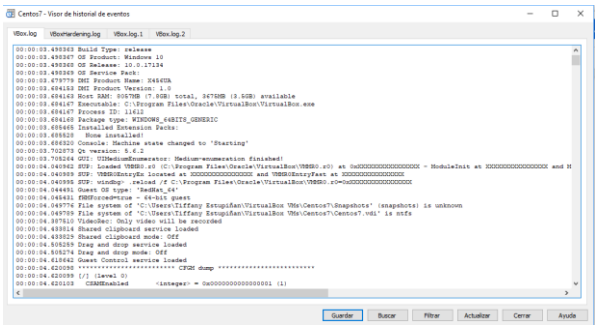


Fig 139 Log visualizado desde virtual box

De igual manera se quiso corroborar que la misma imformacion pudiera recopilarse con virtual box en linux , por lo que se ejecuto y se virtualizo lixuz puppy , y se procedio al hallazgo de los logs del virtualizador .

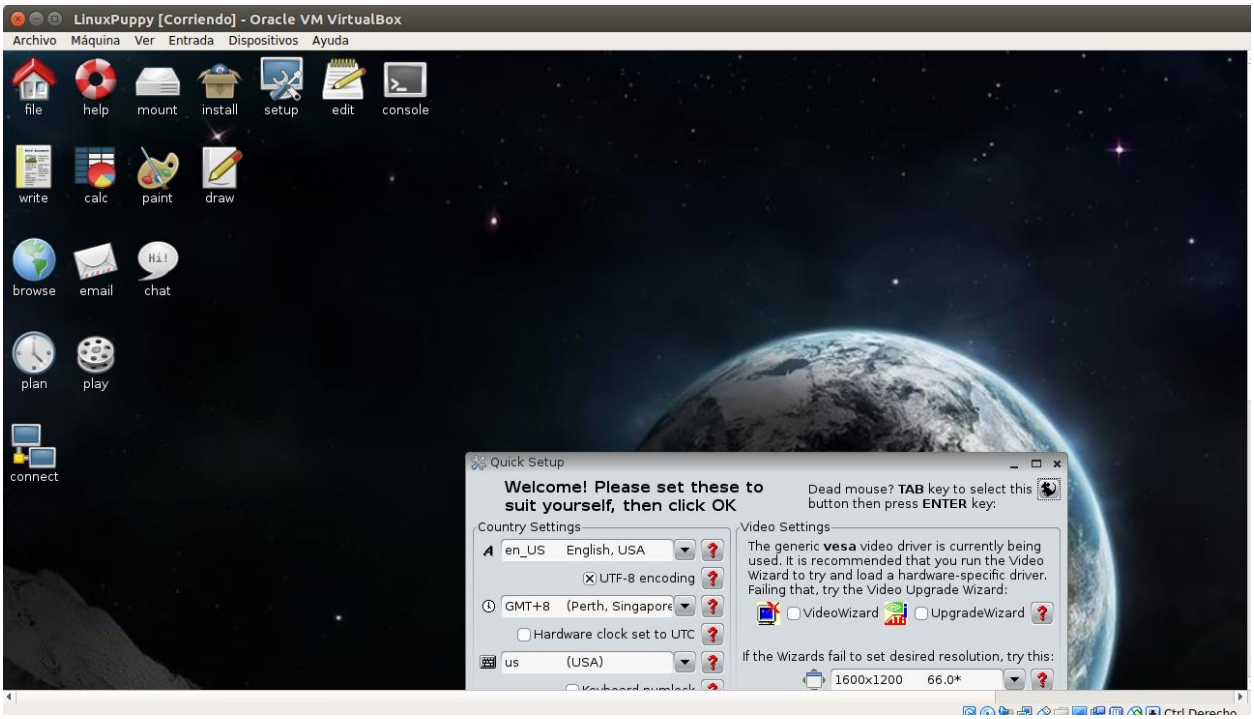


Fig 140 Linux Puppy virtualizado en Virtual Box en linux

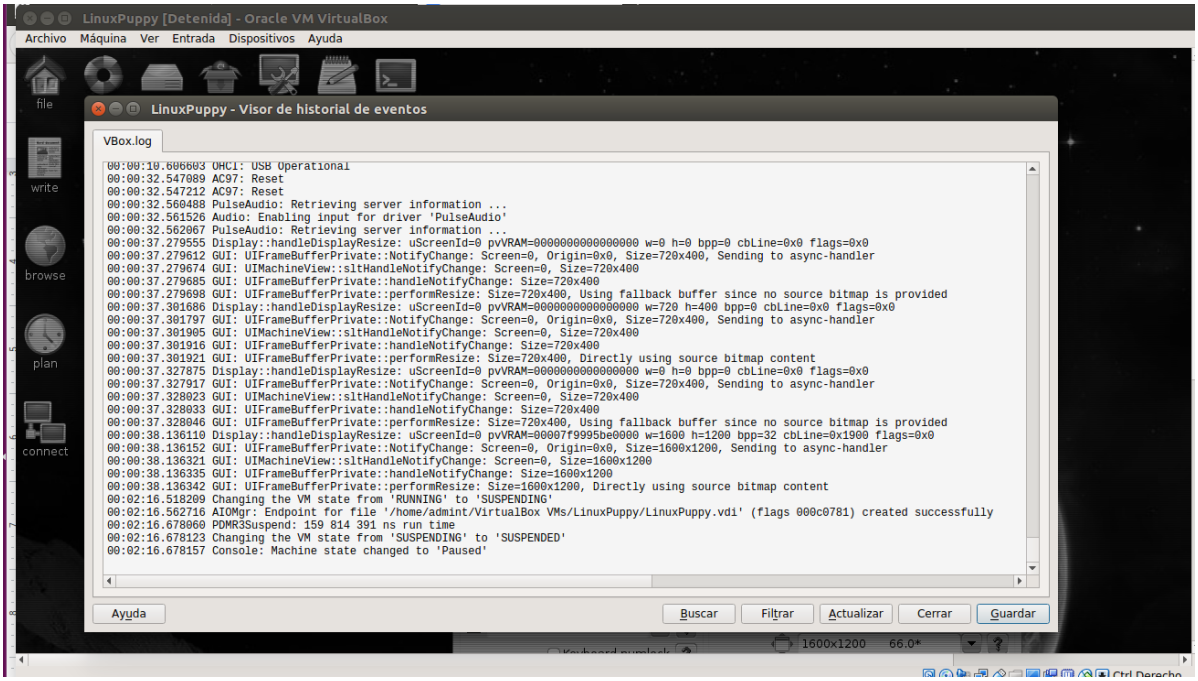


Fig 141 Logs visualizados desde virtual Box

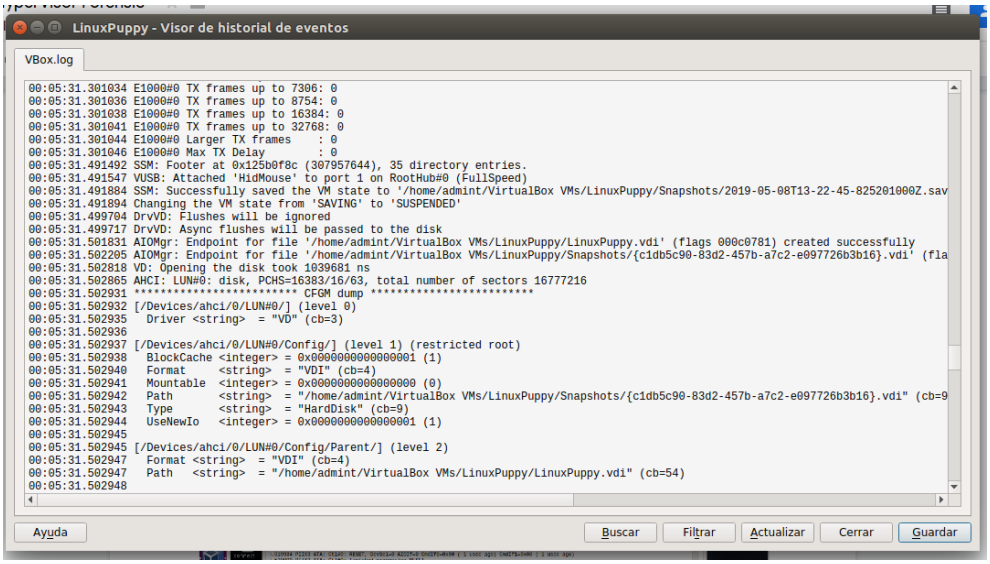


Fig 142 Logs visualizados desde virtual box

6.10 Herramientas utilizadas

Para la aplicación de toda la teoría en los distintos dispositivos, es necesario la utilización de herramientas, en nuestro caso decidimos usar kits para la gestión de forensia digital de open source o de uso público para la recolección de evidencia y la generación de los informes pertinentes de cada una de las pruebas realizadas. a continuación, se enuncian cada uno de los kits utilizados, y las herramientas que se utilizaron a lo largo de todo el proyecto.

6.10.1 Helix

Herramienta utilizada como solución a incidentes otorgando, análisis de forense, perfecto para la realización de imágenes forenses o copias forenses mediante la utilización de ftk imager. Se puede trabajar en entornos Mac OS X, Windows and Linux con un único interfaz [106].

- Hace imágenes de todos los dispositivos internos
- Hace una imagen de la memoria física
- Permite determinar si un disco está encriptado.
- Permite tener un dispositivo booteable, para cualquier sistema de x86
- Hace imágenes de todos los dispositivos internos
- Busca ficheros de tipos determinados (ej. Documentos .doc, .xls, .ppt, etc.)
- Contiene diversas aplicaciones de código abierto que nos permiten analizar datos, incluyendo los contenidos en teléfonos móviles.

6.10.2 Deft

Es una distribución para forensia digital y respuesta a incidentes, se ejecuta en vivo sin alterar o modificar los dispositivos a los que se le realiza la gestión, cuenta con una herramienta llamada DART que cuenta con herramientas para la realización de monitoreo de res, recuperación de contraseñas. revisión de historias entre otras, manejando interfaz para usuario y para administrador. En este proyecto se usó especialmente para la recuperación y el análisis de archivos, el sistema operativo se puede grabar tanto a un DVD como a una memoria USB y nos permite arrancar el sistema de 3 formas diferentes [107]:

- En modo interfaz cargado 100% en la memoria RAM (podemos extraer el DVD o USB cuando cargue).
- Con interfaz, pero en modo Live (cargando desde el medio).
- En modo texto para usarlo desde termina

6.10.3 Hirens boot

kit utilizado para solucionar el problema de arranque en los computadores, también cuenta con herramientas que permiten realizar cambio o eliminación de las contraseñas, recuperación de datos, otorga herramientas para la BIOS [108].

6.10.4 Santoku

cuenta con herramientas para la realización de la forensia en móviles de distintos fabricantes, permitiendo la adquisición y análisis de datos, como los contactos, imágenes, mensajes, entre otros [109].

6.10.5 Dlc boot

herramienta utilizada para quitar las contraseñas de acceso, también es utilizada para reparar los pc, limpiarlo de virus, realización de copias de seguridad, recuperación de datos, entre otras cosas [110].

6.10.6 EnCase

herramienta utilizada para hallar datos ocultos,, recolección de datos y realización de análisis, manejandolos de la manera correcta para poder ser admisibles ante la corte [111].

6.10.7 Katana

Es una distribución que recopila herramientas para realizar, penetracion, auditorías, análisis de redes, eliminación de virus, descifrar contraseñas, entre otras, puede ser ejecutada desde una usb [112].

6.10.8 Koon-Boot

Es una aplicación que permite acceder al computador sin tener la contraseña y si modificar ningún fichero del disco permitiendo un ilimitado acceso al dispositivo [113].

6.10.9 WireShark

Herramienta utilizada para el monitoreo de red, realizar captura de paquetes, analizar y solucionar problemas en la red [114].

6.10.10WhatsApp Extractor

Aplicación enfocada para Iphone mediante la recuperación de chats, fotos, videos y notas de voz de una cuenta de whatsApp, mediante la búsqueda de las copias de seguridad del dispositivo [115].

6.10.11 My lan Viewer

Es un escáner de red, mostrando todos los computadores que están en una red, otorgando los nombres de las máquinas, direcciones ip, direcciones MAC, especificaciones de cada computador, entre otras [116].

7 CONCLUSIONES

El rápido avance de la tecnologia, no afecta solo a los usuarios sino también a los expertos que deben estar al tanto de las vulnerabilidades que estas tecnologias conllevan y asi mismo la manera de hallarlas y contrarestarlas, esto permite no solo adelantarse a los hechos sino ademas adquirir la pericia para combatirlos en caso de ser necesario.

Siempre es necesario tener en cuanta que no solo avanzan las vulnerabilidades y tecnologias, sino también las herramientas utilizadas para la realización de una investigacion forense pues esto permitirá tener una mayor credibilidad frente a una corte.

Por otro lado, es importante resaltar la importancia de la memoria en cualquier dispositivo pues es alli es donde residen la gran mayoria de las acciones realizadas por el usuario y/o el atacante incluso aunque este haya borrados sus rastros, esto no solo se evidencia en el articulo “La importancia de la memoria como evidencia digital en la informatica forense” sino tambien en la investigacion realizada a los hipervisores pues la informacion requerida al respecto se halla en la memoria del equipo. Adicionalmente, en el caso de los hipervisores se require más tiempo y conocimiento del tema, pues es solo una parte de lo que la forensia puede analizar, ya que no se tuvieron en cuenta los contenedores como parte de la familia de virtualizadores.

Otra de las ramas importantes para la gestión de evidencia digital es la red forense, esta es una parte importante ya que se puede rastrear e camino del atcante como también saber que realizo, desde donde lo realizo, cuanto tiempo duro realianzolo, aunque se debe tener precaución ya que al capturar los datos en la red se pueden capturar paquetes que no corresponden a la investigación lo cual puede generar un delito al caturar información personal de otros usuarios, para esta técnica no solo se debe tener espaio para almacenar toda la información capturada, también se debe contar con una persona que sea capaz de leer y entender los datos lo suficientemente bien como para asegurar que es útil y que no a la hora de la investigación, esto esta explicado de manera mas detallada en el articulo “Importancia de la Forensia en Redes para la Recopilación de Evidencia Digital” donde se abordan temas como que información traen los distintos tipos de paquetes y las distintas herramientas que son de ayuda para los investigadores.

Para finalizar se indago mas afondo sobre que otro tipo de información se podía extraer y fue allí donde se empezó a trabajar con los sistemas de archivos para buscar otra manera de hallar información que sea adminible ante la corte en caso de una investigación, los sistemas de archivos pueden ser distintos dependiendo del sistema operativo en el que operen peo su base es general y consta de 5 capas en donde a cada una se le puede estraer distinta información de los archivos como también de si alguien manipulo el sistema y realizo acciones como sobreescritura, borrado de archivos, entre otras las cuales se explicaran mas afondo en el artículo “Importancia de los sistemas de archivo de disco para la recopilación y análisis de información” el cual fue realizado

gracias a toda la investigación realizada como parte de proyecto de grado de ingeniería de sistemas en la Escuela Colombiana de Ingenieria Julio Garavito.

Finalmente como conclusión más relacionada al Proyecto, es interesante y conveniente hacer este tipo de investigaciones dados nuestros intereses por la seguridad informatica, sin embargo, es necesario siempre tener un objetivo claro y una tematica acotada pues algunas veces el tema puede extenderse tanto que podria llegarse a perder la idea central del Proyecto.

También es importante ya que al realizar investigaciones de estos temas se difunde y genera conocimiento lo que a su ves se replica de maneras incontables logrando que mas gente conozcan no solo la importancia de sus datos si no como tomar medidas de primeros auxilios si algo ocurre y como actuar frente a ello, la temática del proyecto es actual e interesante es por eso que se debe monitorear un progreso y un enfoque para no ampliar el rango del alcance y perder el enfoque que se planteo al iniciar la investigación.

8 AGRADECIMIENTOS

Agradecemos a la Escuela Colombiana de Ingeniería Julio Garavito por la oportunidad de realizar esta investigación que aporta importante conocimiento en quienes apenas se empiezan a interesar en el tema, así como nos aportó a nosotras el conocimiento suficiente para despertar más curiosidad sobre los temas relacionados.

Por otro lado agradecemos especialmente a Claudia Santiago Cely que como directora de proyecto, siempre nos alentó a las nuevas búsquedas, a no conformarnos con los resultados obtenidos y nos guió en no perder el objetivo. Así mismo agradecemos a nuestros padres por la paciencia y consideración tenida durante todo el proceso de la carrera.

Finalmente pero no menos importante, agradecemos a los profesores Gerson Quintero, Daniel Díaz y Gerardo Ospina que con sus consejos y guías nos ayudaron a acotar los temas así como a entender un poco mejor la temática trabajada.

REFERENCIA

[1] M. Pollitt, "HAL Archives-ouvertes," 27 Noviembre 2017. [Online]. Available: https://hal.inria.fr/hal-01060606/document. [Accessed 12 septiembre 2018].

[2] E. C. d. Colombia, "docudigital," [Online]. Available: https://www.docudigital.com/wp-content/uploads/2016/11/LEY_527_DE_1999.pdf. [Accessed 13 Septiembre 2018].

[3] C. D. L. REPÚBLICA, "procuraduria," [Online]. Available: https://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/L-527-99.htm. [Accessed 15 Septiembre 2018].

[4] D. M. ARDILA CARRILLO and O. F. LOMBANA JIMÉNEZ, "unilibre.edu.co," 12 Mayo 2015. [Online]. Available: https://repository.unilibre.edu.co/bitstream/handle/10901/7969/Proyecto%20de%20grado.pdf?sequence=1. [Accessed 20 Agosto 2018].

[5] J. ANGUAS, "anguas," 12 Noviembre 2011. [Online]. Available: https://www.anguas.com/e1m6/Docs/01_Documentacion_Adicional_Curso_Peritaje_CPEIG.pdf. [Accessed 5 Septiembre 2018].

[6] A. Perez, "researchgate," Diciembre 2007. [Online]. Available: https://www.researchgate.net/publication/303822484_Analisis_Forense_de_la_Informacion_contenida_en_los_volcados_de_memoria. [Accessed 20 Septiembre 2018].

[7] G. A. ALVAREZ GUERRERO, "unipiloto," 2015. [Online]. Available: http://polux.unipiloto.edu.co:8080/00002643.pdf. [Accessed 27 Seotiembre 2018].

[8] L. Liu, "isaca," 2016. [Online]. Available: http://m.isaca.org/chapters12/costa-rica/events/Documents/Presentaciones%20congreso%20Isaca%202016/4.%20An%C3%A1lisis%20forense%20digital.pdf. [Accessed 30 Septiembre 2018].

[9] S. A. D. Pino, "oas.org," [Online]. Available: https://www.oas.org/juridico/english/cyb_pan_manual.pdf. [Accessed 17 Septiembre 2018].

[10] w. moura, "egov.ufsc.br," 22 Noviembre 2012. [Online]. Available: http://www.egov.ufsc.br/portal/conteudo/evidencia-digital-en-colombia-una-reflexi%C3%B3n-en-la-pr%C3%A1ctica. [Accessed 18 Septiembre 2018].

[11] mintic, "mintic.gov.co," 28 Marzo 2016. [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf. [Accessed 19 Septiembre 2018].

[12] P. J. Arnedo Blanco, "Universidad Internacional de la Rioja," 11 Marzo 2014. [Online]. Available: https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1. [Accessed 20 Seotiembre 2018].

[13] utn.edu.ec, "utn.edu.ec," [Online]. Available: http://repositorio.utn.edu.ec/bitstream/123456789/539/7/04%20ISC%20157%20CAPITULO%20II.pdf. [Accessed 22 Septiembre 2018].

[14] D. A. RAMÍREZ RIVEROS and E. F. CASTRO SERRATO, "UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”," 2018. [Online]. Available: https://repository.unad.edu.co/bitstream/10596/17370/1/86078250.pdf. [Accessed 12 Septiembre 2018].

[15] J. E. Castillo Guerra and J. A. Raquejo Romero, "Universidad Piloto de Colombia," [Online]. Available: http://polux.unipiloto.edu.co:8080/00000852.pdf. [Accessed 24 Septiemre 2018].

[16] dragonjar.org, "dragonjar.org," [Online]. Available: https://www.dragonjar.org/recogiendo-evidencias-analisis-forense-windows.xhtml. [Accessed 28 Septiembre 2018].

[17] D. E. B. Michelena, "REVISTA .SEGURIDAD," 2018. [Online]. Available: https://revista.seguridad.unam.mx/numero-17/an%C3%A1lisis-de-volcado-de-memoria-en-investigaciones-forenses-computacionales. [Accessed 27 Septiembre 2018].

[18] V. L. VIVAS, "UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA," 2017. [Online]. Available: https://repository.unad.edu.co/bitstream/10596/17473/1/1113665550.pdf. [Accessed 28 Septiembre 2018].

[19] Fude, "Fude," [Online]. Available: https://www.educativo.net/articulos/el-informe-pericial-y-sus-caracteristicas-135.html. [Accessed 26 Septiembre 2018].

[20] F. J. Tortosa López, "Asociacion Nacional de Tecnicos Universitarios en Documentoscopia," [Online]. Available: http://www.antud.org/El%20informe%20pericial.pdf. [Accessed 5 Octubre 2018].

[21] peritoinformaticocolegiado.es, "El contra-peritaje informático y el meta-peritaje informático," 18 Marzo 2015. [Online]. Available: https://peritoinformaticocolegiado.es/blog/el-contra-peritaje-informatico-y-el-meta-peritaje-informatico/. [Accessed 10 Octubre 2018].

[22] A. Navarro Navarro, "tics consulting," 10 Febrero 2011. [Online]. Available: http://www.ticsconsulting.es/blog/peritajes-contraperitajes-y-metaperitajes. [Accessed 10 Septiembre 2018].

[23] P. caligrafo, "Perito caligrafo documental," 2014. [Online]. Available: https://peritocaligrafo.webs.com/metaperitaje.htm. [Accessed 8 Septiembre 2018].

[24] C. d. P. Penal, "sherloc," 1 Septiembre 2004. [Online]. Available: https://sherloc.unodc.org/cld/en/legislation/col/codigo_de_procedimiento_penal/articulos_235_236_244/articulos_235_236_244.html?. [Accessed 12 Septiembre 2018].

[25] MinDefensa, "Soporte Legal de la Evidencia Digital en un Incidente Informático," [Online]. Available: http://www.colcert.gov.co/sites/default/files/evidencia_digital.pdf. [Accessed 22 Septiembre 2018].

[26] E. C. d. l. República, "hchr.org.co," 31 Agosto 2004. [Online]. Available: http://www.hchr.org.co/documentoseinformes/documentos/carceles/4_Nacionales/1_Normas_basicas/2_Regimen_penal_ejec_penas/Ley%20906%20de%202004,%20C%F3digo%20procedimiento%20penal.pdf. [Accessed 17 Septiembre 2018].

[27] P. EUROPEO, "boe," 6 Julio 2016. [Online]. Available: https://www.boe.es/doue/2016/194/L00001-00030.pdf. [Accessed 22 Septiembre 2018].

[28] oas.org, "oas.org," 23 Noviembre 2001. [Online]. Available: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf. [Accessed 19 Septiembre 2018].

[29] E. Perona, "security art work," 10 Febrero 2016. [Online]. Available: https://www.securityartwork.es/2016/02/10/analisis-forense-cadena-de-custodia-de-la-evidencia-digital/. [Accessed 22 Septiembre 2018].

[30] tallerinformatica, "Memoria," tallerinformatica, [Online]. Available: https://tallerinformatica.wordpress.com/memoria/. [Accessed 10 Septiembre 2018].

[31] memoriassinformaticas, "memoriassinformaticas," memoriassinformaticas, 28 Junio 2016. [Online]. Available: http://memoriassinformaticas.blogspot.com/2016/06/memoria-informatica-caracteristicas.html. [Accessed 10 Spetiembre 2018].

[32] caymans, "Tipos de memoria (informática) | Caracteristicas y funcionamiento," 247 Tecno, 17 Junio 2018. [Online]. Available: http://247tecno.com/tipos-de-memoria-informatica/. [Accessed 11 Septiembre 2018].

[33] ecured, "Memoria (informática)," ecured, [Online]. Available: https://www.ecured.cu/Memoria_(inform%C3%A1tica). [Accessed 11 Septiembre 2018].

[34] c. suazo, "Arquitectura de computadores," 27 Enero 2017. [Online]. Available: https://sites.google.com/site/arquitecturadecomputadoresis/jerarquia-de-memoria. [Accessed 28 Septiembre 2018].

[35] www.fing.edu.uy, "JERARQUÍA DE MEMORIA," www.fing.edu.uy, [Online]. Available: https://www.fing.edu.uy/tecnoinf/mvd/cursos/arqcomp/material/teo/arq-teo10.pdf. [Accessed 11 Septiembre 2018].

[36] S. C. Arango, "Memoria cache L1, L2 y L3," blogspot, 28 Abril 2013. [Online]. Available: sistop2013.blogspot.com/2013/04/memoria-cache-l1-l2-y-l3.html. [Accessed 13 Septiembre 2018].

[37] nextu, "nextu," nextu, [Online]. Available: https://www.nextu.com/blog/evolucion-memoria-ram/. [Accessed 16 Septiembre 2018].

[38] diffen, "diffen," diffen, [Online]. Available: https://es.diffen.com/tecnologia/RAM-vs-ROM. [Accessed 11 Septiembre 2018].

[39] umxprogramsis, "Arquitectura," umxprogramsis, [Online]. Available: https://umxprogramsis.wordpress.com/arquitectura/. [Accessed 13 Septiembre 2018].

[40] A. L. S. Iglesias, "Memoria Flash, definición y características.," aboutespanol, 05 Agosto 2014. [Online]. Available: https://www.aboutespanol.com/memoria-flash-definicion-y-caracteristicas-841286. [Accessed 13 Septiembre 2018].

[41] ingeniatic, "ingeniatic," ingeniatic , [Online]. Available: https://www.etsist.upm.es/estaticos/ingeniatic/index.php/tecnologias/item/511-memoria-flash.html. [Accessed 13 Septiembre 2018].

[42] alegsa, " DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA," alegsa, 2018. [Online]. Available: www.alegsa.com.ar/Dic/cinta_magnetica.php. [Accessed 13 Septiembre 2018].

[43] M. Virtual, "Memoria Virtual," Memoria Virtual , 28 Mayo 2012. [Online]. Available: systope.blogspot.com/2012/06/memoria-virtual.html. [Accessed 14 Septiembre 2018].

[44] redhat, "redhat," redhat, [Online]. Available: https://www.redhat.com/es/topics/data-storage/network-attached-storage#compare-das. [Accessed 14 Septiembre 2018].

[45] C. Miyachi, "What is “Cloud”? It is time to update the NIST definition?," ieeexplore.ieee.org, [Online]. Available: https://ieeexplore.ieee.org/document/8383652. [Accessed 14 Septiembre 2018].

[46] ictea, "ictea," Base de Conocimientos, [Online]. Available: www.ictea.com/cs/index.php?rp=/knowledgebase/215/What-is-Cloud-Computing.html. [Accessed 14 Septiembre 2018].

[47] PAOLINA, "Recolección de Evidencia Digital," cienciadigitalforense, [Online]. Available: http://cienciadigitalforense.blogspot.com/2014/11/recoleccion-de-evidencia-digital.html. [Accessed 13 Septiembre 2018].

[48] ninjasdelaweb, "ninjasdelaweb," ninjasdelaweb, [Online]. Available: ninjasdelaweb.com/metodologia-de-analisis-forense/. [Accessed 13 Septiembre 2018].

[49] revista.seguridad.unam.mx, "revista.seguridad.unam.mx," revista.seguridad.unam.mx, [Online]. Available: https://revista.seguridad.unam.mx/numero-17/análisis-de-volcado-de-memoria-en-investigaciones-forenses-computacionales. [Accessed 15 Septiembre 2018].

[50] norton, "Master Boot Record (MBR) (Registro de arranque maestro [MBR])," norton, [Online]. Available: https://mx.norton.com/online-threats/glossary/m/master-boot-record-mbr.html. [Accessed 14 Septiembre 2018].

[51] aprendizdesysadmin, "Informática Forense. Recuperación en la $MFT. Cuándo, cómo y a veces porque no se puede," 23 Septiembre 2016. [Online]. Available: https://aprendizdesysadmin.com/informatica-forense-recuperacion-en-la-mft-cuando-y-como/. [Accessed 14 Septiembre 2018].

[52] mattica, "mattica," mattica, 22 Marzo 2011. [Online]. Available: https://mattica.com/extraccion-o-imagen-forense/. [Accessed 13 Septiembre 2018].

[53] mattica, "¿Extracción o imagen forense?," mattica, 22 Marzo 2011. [Online]. Available: https://mattica.com/extraccion-o-imagen-forense/. [Accessed 14 Septiembre 2018].

[54] "Las imágenes forenses y su uso en procesos judiciales," ambitojuridico, 07 Noviembre 2018. [Online]. Available: https://www.ambitojuridico.com/noticias/tecnologia/tic/las-imagenes-forenses-y-su-uso-en-procesos-judiciales. [Accessed 26 Noviembre 2018].

[55] mintic, "Evidencia Digital," mintic, [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf. [Accessed 16 Septiembre 2018].

[56] unixtutorial, "dd command," unixtutorial, [Online]. Available: https://www.unixtutorial.org/commands/dd. [Accessed 10 octubre 2018].

[57] U. Manuals, "ubuntu," Ubunto Manuals, [Online]. Available: manpages.ubuntu.com/manpages/bionic/es/man8/fdisk.8.html. [Accessed 16 Octubre 2018].

[58] govinfo, "Archived NIST Technical Series Publication," govinfo, [Online]. Available: https://www.govinfo.gov/content/pkg/GOVPUB-C13-bd12c48cccb6fefb73982be53dea84c4/pdf/GOVPUB-C13-bd12c48cccb6fefb73982be53dea84c4.pdf. [Accessed 20 Octubre 2018].

[59] U. Veracruzana, "Herramientas para realizar análisis forenses a dispositivos móviles," 01 Marzo 2016. [Online]. Available: https://www.uv.mx/infosegura/general/noti_moviles-25/. [Accessed 25 Octubre 2018].

[60] Á. H. Bravo Bravo and Á. L. Villafuerte Quiroz, "Implantación De Una Herramienta Ossim Para El Monitoreo Y Gestión De," [Online]. Available: http://www.dspace.espol.edu.ec/bitstream/123456789/43765/1/BRAVO%20BRAVO%20%C3%81NGEL%20HERALDO%20Y%20VILLAFUERTE%20QUIROZ%20%C3%81LVARO%20LUIS.pdf. [Accessed 20 Octubre 2018].

[61] AlienVault, "AlienVaul," [Online]. Available: https://www.alienvault.com/documentation/usm-appliance/monitoring-analysis/viewing-dashboards.htm. [Accessed 20 Octubre 2018].

[62] AlienVault, "AlienVault," [Online]. Available: https://www.alienvault.com/documentation/usm-appliance/monitoring-analysis/analyzing-alarms-events.htm?tocpath=DOCUMENTATION%7CAlienVault%C2%AE%20USM%20Appliance%E2%84%A2%7CUser%20Guide%7CUSM%C2%A0Appliance%20Security%20Monitoring%20and%20Analysis%7C___2. [Accessed 20 Octubre 2018].

[63] AlienVault, "AlienVault," [Online]. Available: https://www.alienvault.com/documentation/usm-appliance/reports/ossim-report-types.htm. [Accessed 22 Octubre 2018].

[64] AlienVault, "AlienVault," [Online]. Available: https://www.alienvault.com/documentation/usm-appliance/reports/creating-custom-report-modules.htm?tocpath=DOCUMENTATION%7CAlienVault%C2%AE%20USM%20Appliance%E2%84%A2%7CUser%20Guide%7CUSM%C2%A0Appliance%20Reports%7C_____3. [Accessed 22 Octure 2018].

[65] J. M. Lorenzo, "slideshare," 12 Febrero 2010. [Online]. Available: https://es.slideshare.net/alienvault/alienvault-herramientas-integradas-en-ossim. [Accessed 25 Octubre 2018].

[66] AlienVault, "https://es.wikipedia.org/wiki/Open_Source_Security_Information_Management," [Online]. Available: https://es.wikipedia.org/wiki/Open_Source_Security_Information_Management. [Accessed 25 Octubre 2018].

[67] R. G. Cárdenas, "Computo forense redes," [Online]. Available: http://cryptomex.org/SlidesForensia/ForensiaRedes.pdf. [Accessed 25 Octubre 2018].

[68] D. MonDivakaran, "ScienceDirect," Marzo 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287617300452. [Accessed 26 Octubre 2018].

[69] nugget, "nugget," github, [Online]. Available: https://github.com/cdstelly/nugget. [Accessed 28 Enero 2019].

[70] ChristopherStelly, "Nugget: A digital forensics language," sciencedirect, 24 Marzo 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287618300380. [Accessed 30 Enero 2019].

[71] nuggetdsl, "nuggetdsl," nuggetdsl, 2018. [Online]. Available: https://www.nuggetdsl.co00000m/getting-started/. [Accessed 3 Marzo 2019].

[72] S. MACIAS, "en mi local funciona," santi macias, 16 Enero 2018. [Online]. Available: https://enmilocalfunciona.io/instalando-y-probando-docker-en-windows-10/. [Accessed 3 Marzo 2019].

[73] "tech over flow," tech over flow, 2019. [Online]. Available: https://techoverflow.net/2017/03/01/solving-docker-permission-denied-while-trying-to-connect-to-the-docker-daemon-socket/. [Accessed 8 Marzo 2019].

[74] artik, "artik," artik, [Online]. Available: https://artik.cloud/search/#stq=documentation&stp=1. [Accessed 7 Abril 2019].

[75] S. K. Mohiddin, "link springer," 31 Octubre 2018. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-13-1595-4_41. [Accessed 10 Febrero 2019].

[76] a. amazon, "Digital Forensics," [Online]. Available: https://aws.amazon.com/es/mp/scenarios/security/forensics/ . [Accessed 10 Febrero 2019].

[77] a. amazon, "PDEvidence Helps Solve Crimes Faster Using Automated AWS-Based System," [Online]. Available: https://aws.amazon.com/es/solutions/case-studies/pdevidence/. [Accessed 12 Febrero 2019].

[78] IBM, "Built with AI for the front-line Security Analyst," [Online]. Available: https://www.ibm.com/us-en/marketplace/cognitive-security-analytics. [Accessed 12 Febrero 2019].

[79] IBM, "Giving enterprises access to an ecosystem of collaborative defense," [Online]. Available: https://www.ibm.com/security/community/app-exchange. [Accessed 12 Febrero 2019].

[80] IBM, "Quickly conduct network forensics investigations," [Online]. Available: https://www.ibm.com/us-en/marketplace/ibm-qradar-incident-forensics?mhq=forensic%20&mhsrc=ibmsearch_a. [Accessed 12 Febrero 2018].

[81] IBM, "IBM QRadar Advisor with," [Online]. Available: https://public.dhe.ibm.com/common/ssi/ecm/24/en/24021824usen/c3444632-6845-449b-b5ad-d3268e69af88_24021824USEN.pdf. [Accessed 14 Fecbrero 2019].

[82] sitewhere, "sitewhere," [Online]. Available: https://sitewhere.io/docs/2.0.0/es/platform/#enfoque-arquitectonico. [Accessed 14 Febrero 2019].

[83] sitewhere, "sitewhere," 2018. [Online]. Available: https://github.com/sitewhere/sitewhere. [Accessed 13 Febrero 2019].

[84] Node-RED, "Node-RED," Node-RED, [Online]. Available: https://nodered.org/. [Accessed 7 Abril 2019].

[85] Greenwave, "Greenwave," [Online]. Available: https://greenwavesystems.com/contact-greenwave-systems/thank-you/?submissionGuid=12466286-9d6e-4cb0-b2cc-7fd35fc28fb2. [Accessed 14 Febrero 2019].

[86] macchina.io, "macchina," macchina.io, [Online]. Available: https://macchina.io/remote_signup.html. [Accessed 15 Febrero 2019].

[87] E. Foundation, "Eclipse Foundation," Eclipse Foundation, [Online]. Available: https://www.youtube.com/watch?v=aUkeAW91k4E. [Accessed 15 Febrero 2019].

[88] thinger, "thinger," thinger, [Online]. Available: https://thinger.io/. [Accessed 15 Febrero 2019].

[89] tldp.org, "Sistemas de archivos," tldp.org, [Online]. Available: http://www.tldp.org/pub/Linux/docs/ldp-archived/system-admin-guide/translations/es/html/ch06s08.html. [Accessed 10 Abril 2019].

[90] http://cidecame.uaeh.edu.mx, "Tipos de Sistemas de Archivos," http://cidecame.uaeh.edu.mx, [Online]. Available: http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro26/tipos_de_sistemas_de_archivos.html. [Accessed 17 Abril 2019].

[91] F. P. May, "tamps.cinvestav.mx," tamps.cinvestav.mx, Junio 2011. [Online]. Available: https://www.tamps.cinvestav.mx/~fpech/sd/files/introduccion.pdf. [Accessed 17 Abril 2019].

[92] T. Mohsin, "Infosec," Computer Forensics: Media & File System Forensics, [Online]. Available: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/media-file-system-forensics/#gref. [Accessed 20 Abril 2019].

[93] S. S. Khandare, "Computer Programming & Utilization," in *Computer Programming & Utilization*, Bogota, S. Chand Publishing, 2013, pp. 17-21.

[94] A. L. a. D. B. Mariano Graziano, "Hypervisor Memory Forensics," syssec-project.eu, [Online]. Available: http://www.syssec-project.eu/m/page-media/3/raid13_graziano.pdf. [Accessed 12 Marzo 2019].

[95] wikipedia, "Hipervisor," wikipedia, [Online]. Available: https://es.wikipedia.org/wiki/Hipervisor. [Accessed 17 Marzo 2019].

[96] J. M. Gonzalez, "Diferencias entre virtualización basada en hipervisor o en host," josemariagonzalez, 17 Noviembre 2011. [Online]. Available: https://www.josemariagonzalez.es/manuales-virtualizacion/diferencias-virtualizacion-basada-hipervisor-host.html. [Accessed 17 Marzo 2019].

[97] fpg.x10host.com, "Tipos de hipervisores," Tutorial de VirtualBox, [Online]. Available: fpg.x10host.com/VirtualBox/tipos_de_hipervisores.html. [Accessed 17 Marzo 2018].

[98] nvlpubs.nist.gov, "Archived NIST Technical Series Publication," nvlpubs.nist.gov, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125A.pdf. [Accessed 17 Marzo 2019].

[99] P. Ferrie, "Attacks on More Virtual Machine Emulators," Peter Ferrie, [Online]. Available: https://pdfs.semanticscholar.org/a72d/98d5a478efa62383a63862fc07dba831c8a5.pdf.. [Accessed 20 Marzo 2019].

[100] A. A. A. Ali, "virtual machine escapes," researchgate, Abril 2013. [Online]. Available: https://www.researchgate.net/publication/255791810_virtual_machine_escapes. [Accessed 22 Marzo 2019].

[101] J. C. Ardita, "Análisis forense técnico en entornos virtuales," [Online]. Available: m.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2015/CIGRAS-2015.09.10-02-Analisis%20Forense%20tecnico%20en%20Entornos%20Virtuales-Julio%20Ardita.pdf. [Accessed 25 Marzo 2019].

[102] N. Santos, "Cloud Forensics and Conclusions," Tecnico Lisboa, 2018. [Online]. Available: https://fenix.tecnico.ulisboa.pt/downloadFile/845043405479112/csf1718-3-09-cloud_forensics_and_conclusions.pdf. [Accessed 25 Marzo 2019].

[103] redhat, "¿Qué es una nube privada?," Red Hat, [Online]. Available: https://www.redhat.com/es/topics/cloud-computing/what-is-private-cloud. [Accessed 22 Marzo 2019].

[104] Paco, "Notas de seguridad Informatica," blogspot, 8 Junio 2017. [Online]. Available: notasdeseguridad.blogspot.com/2014/06/analisis-forense-en-maquinas-virtuales.html. [Accessed 22 Marzo 2019].

[105] A. Greenberg, "Virtualization's Dark Side," forbes, 9 Abril 2009. [Online]. Available: https://www.forbes.com/2008/04/09/virtualization-rsa-malware-tech-virtualization08-cx_ag_0409virtual.html#2d77f23d6871. [Accessed 23 Marzo 2019].

[106] H. Enterprise, "e-fense," e-fense, [Online]. Available: http://www.e-fense.com/h3-enterprise.php. [Accessed 10 Noviembre 2018].

[107] DEFT, " Def[t] DFIR Toolkit," DEFT, [Online]. Available: http://www.deftlinux.net/. [Accessed 17 Noviembre 2018].

[108] H. Boot, "Hiren's BootCD PE," Hiren's BootCD PE, [Online]. Available: https://www.hirensbootcd.org/. [Accessed 17 Noviembre 2018].

[109] Santoku, "Santoku," Santoku, [Online]. Available: https://santoku-linux.com/. [Accessed 17 Noviembre 2018].

[110] i. vitoria, "DLC Boot 2017, el pendrive indispensable que debes tener," informaticovitoria, 2 Junio 2017. [Online]. Available: https://www.informaticovitoria.com/dlc-boot-2016-el-pendrive-indispensable-que-debes-tener/. [Accessed 17 Noviembre 2018].

[111] guidancesoftware, "EnCase," guidancesoftware, [Online]. Available: https://www.guidancesoftware.com/encase-forensic. [Accessed 17 Noviembre 2018].

[112] katanaforensics, "katanaforensics," katanaforensics, [Online]. Available: https://katanaforensics.com/. [Accessed 18 Noviembre 2018].

[113] freedomprintssu, "freedomprintssu," freedomprintssu, [Online]. Available: https://freedomprintssu.weebly.com/home/kon-boot-usb-iso-download. [Accessed 18 Noviembre 2018].

[114] wireshark, "wireshark," wireshark, [Online]. Available: https://www.wireshark.org/docs/. [Accessed 18 Noviembre 2018].

[115] hatsapp-extracto and softonic, "softonic," softonic, [Online]. Available: https://whatsapp-extractor.softonic.com/?ex=BB-965.2. [Accessed 18 Noviembre 2018].

[116] m. l. viewer, "my lan viewer," MyLanViewer Network/IP Scanne, [Online]. Available: http://www.mylanviewer.com/. [Accessed 18 Noviembre 2018].

[117] golang, "github," golang, [Online]. Available: https://github.com/golang/go/wiki/SettingGOPATH . [Accessed 7 Marzo 2019].

[118] ZEOKAT, "voz idea," voz idea, 31 Mayo 2016. [Online]. Available: https://www.vozidea.com/instalar-go-windows-golang. [Accessed 7 Marzo 2019].

[119] U. Manuals, "Ubunto Manuals," Ubunto Manuals, [Online]. Available: manpages.ubuntu.com/manpages/bionic/es/man8/fdisk.8.html. [Accessed 17 octubre 2018].