Las limitaciones de la computación forense debido al uso de criptosistemas

Por:
Javier Fernando LEON CABRERA

Las limitaciones de la computación forense debido al uso de criptosistemas.

The limitations of forensic computing due to the use of cryptosystems

Javier Fernando Leon Cabrera[1]

Resumen

El presente trabajo muestra las limitaciones encontradas por el cómputo forense al momento de desarrollar una investigación sobre información que ha sido protegida con métodos de cifrado, con respecto a las técnicas y las herramientas disponibles para contrarrestar estos medios de protección. Para esto se estudiara los principales conceptos de la criptografía y el computo forense así como los métodos de cifrados más utilizados para la protección de una unidad de almacenamiento o de archivos de datos, de igual forma se nombrara los principales algoritmos utilizados por las diferentes aplicaciones que proporcionan el servicio de cifrado, para luego analizar los diferentes tipos de soluciones y técnicas utilizadas por la computación forense cuando encuentre con un escenario de este tipo. A partir del estudio realizado se puede concluir, que el computo forense encuentra muchas limitantes al dirigir su análisis en sistemas o unidades de disco que ha sido protegidos con un sistema de cifrado, mientras estas técnicas están cada vez están siendo desarrolladas de tal forma que no puedan ser descifradas, las técnicas forenses que se utilizan para intentar acceder a los datos, se basados principalmente en la información que el investigador pueda recolectar de la memoria RAM y otros archivos del sistema operativo y para esto deben contar siempre un escenario propicio, lo que en la mayoría de ocasiones no ocurre.

Palabras clave:	Computación forense, evidencia digital, encriptación, criptoanálisis, criptosistemas, algoritmo.

Abstract

This work shows the limitations encountered by forensic computer when developing research on information that has been protected with encryption methods with respect to the techniques and tools available to counter these means of protection. For this the main concepts of cryptography and computer forensics and methods of encryption most widely used for the protection of a storage unit or data files, just as the main algorithms used appointed it is studied by different applications They provide encryption service, and then analyze the different types of solutions and techniques used by forensic computer when you encounter a scenario of this type. From the study carried out can conclude that forensic computing finds many limitations to run their systems analysis or disk drives that have been protected with an encryption scheme, while these techniques are increasingly being developed so that no they can be deciphered, forensic techniques used to try to access data, mainly based on information that the researcher can collect RAM and other operating system files and this should always have a favorable scenario, which in most cases it does not occur.

Key words	Computer forensics, digital evidence, encryption, cryptanalysis, cryptosystems, algorithm.
Clasificación JEL JEL Classification	C63

[1]

INTRODUCCIÓN

El cifrado de archivos y de unidades de almacenamiento se ha tornado una práctica muy utilizada para proteger la información de observadores no autorizados, tanto que instigadores forenses dentro de sus trabajo de análisis encuentran muy comúnmente elementos con algún tipo de cifrado, creciendo la necesidad de conocer los contenidos que pueden ser una prueba relevante en el caso que se está investigando, debiendo aplicar varias herramientas y técnicas que trataran de descifrar la información, en este proceso el investigador forense encontrara varios problemas y limitaciones (Casey, 2012)

Para Halboob (2015) el uso de criptosistemas va de la mano de la preocupación sobre la privacidad de la información, la misma que puede verse amenazada cuando la información es accedida por terceras personas, lo que ha llevado a que las empresas y profesionales autónomos, generan aplicaciones basadas en algoritmos criptográficos que permitir cifrar la información protegiendo de tal forma que ninguna otra persona pueda acceder a sus contenidos. Igualmente menciona que estas soluciones orientadas a la privacidad son utilizados con otros fines como el del ocultamientos de datos, principalmente utilizados por usuarios, empresas, grupos terroristas, entidades de gobierno que de una u otra forma tiene información confidencial que no desean que sea expuesta y que en muchos de los casos los vincula con alguna actividad ilícita, por tal motivo utilizan medios criptográficos para cifrar sus archivos, sus discos duros, teléfonos celulares o comunicaciones, generando gran preocupación entre investigadores digitales porque esto trae graves inconvenientes en la aplicación del cómputo forense.

Es importante conocer las técnicas de cifrado utilizadas sobre unidades de almacenamiento y archivos, de esta forma sabremos con qué escenario se podrán enfrentar al momento de iniciar una investigación digital; y de encontrar algún medio encriptado será relevante poder reconocer que aplicativo fue utilizado para proteger la información, así como las técnicas de computo forense que pueden ser utilizadas para intentar romper el cifrado (Brown, 2015).

Este trabajo tiene como objetivo describir los diferentes tipos de criptosistemas utilizados para proteger la información de un usuario, así como detallar las técnicas de cómputo forense utilizadas para su descifrado y las limitaciones encontradas durante este proceso.

MARCO TEÓRICO

La Criptografía

La criptografía es una ciencia utilizada para crear diferentes funciones que son capaces de poder transformar mensajes de datos que normalmente son legibles por un usuario, a mensajes ilegibles o mensajes cifrados, es así que para poder llegar a una transformación de un mensaje legible a uno ilegible (cifrado) y viceversa (de cifrado a descifrado) solo pueden darse con el manejo y aplicación de una o más llaves que permitirán esta transformación (Paredes, 2008).

La criptografía tiene como principio el proteger la información y evitar así el acceso no autorizado de otras personas, pero este no es el único uso que se le da, también es utilizada para controlar y proteger la integridad de un mensaje y que no sufra alguna modificación en su recorrido (Rubí, 2011). Igualmente Travieso (2003) mencionana dice que es rama de las matemáticas que ingresa al mundo digital con el objeto de proporcionar una solución al problema de la confidencialidad y la autenticidad, teniendo como su principal propósito el prevenir problemas dentro de los sistemas de seguridad informática.

La Informática forense

Carrier (2002) indica que la informática forense es considerada una ciencia encargada de identificar, preservar, analizar y presentar información extraída de medios informáticos con la finalidad de que sean presentadas y aceptadas en un proceso legal, por esta razón el cómputo forense es una práctica llevada por casi todos los cuerpos de justicia del mundo con la finalidad de perseguir al delito. Asi mismo Cano (2004) manifiesta que el principal objetivo del cómputo forense es realizar análisis minucioso sobre sistemas operativos, programas, archivos, y hardware de almacenamiento en busca de evidencias digitales que aporten a un caso investigado, aplicando de forma correcta su metodología permitirá conservar la integridad de la información extraída, consiguiendo de esta forma la admisibilidad como prueba.

La metodología aplicada para una investigación digital forense recae en 4 pasos primordiales la cual inicia con la identificación del caso que permite al investigador recabar toda la información necesaria para iniciar su análisis, en esta parte metodológica podrá levantar el investigador una línea de tiempo previa que le permitirá enfocar su análisis en ventanas de

tiempo, además podrá saber con mayor certeza que software forense necesita para llevar adelante su trabajo (Mouhtaropoulos, Chang, & Grobler, 2014).

Continua con un segundo paso denominado preservación de evidencia, en el cual Amerini, Becarelli, Bertini & Caldell (2015) lo consideran muy crítico porque se trabaja con la evidencia misma, aquí se extrae imágenes bit a bit de las unidades de almacenamiento a ser analizadas con el fin de preservar el estado original de las evidencias, realizando el análisis sobre las copias generadas. Luego tenemos un tercer paso el de análisis de evidencias en el cual Luric (2012) manifiesta que es donde se aplican todas las técnicas y herramientas para descubrir y recabar las pruebas necesarias que serán presentadas en el informe final que se desarrolla en el cuarto paso de esta metodología, en donde forcht (2014) recomienda obtenerse de usar un lenguaje técnico que impida una correcta comprensión de personas poco conocedoras de términos técnicos.

Técnicas anti forenses

Día a día los investigadores forenses se enfrentan con retos que les exige un mayor esfuerzo al momento de buscar evidencias para la detección de un atacante informático, porque que la tecnología brinda a los ciberdleincuentes la oportunidad que incrementar sus prácticas de evasión utilizando herramientas que les permiten aplicar las llamadas técnicas anti-forenses, una práctica llevada a cabo para comprometer seriamente la disponibilidad de una evidencia digital, destruyéndola, manipulándola, eliminándola u ocultándola (Botero, Camero, & Cano, 2009).

Las principales técnicas anti-forenses utilizadas son el borrado de datos, la manipulación de metadatos, enmascarar una dirección IP, el uso de navegación anónima como Thor, el ocultamiento de información y el cifrado de datos (Kamal & Bassil , 2011). Stamm, Lyn, & Ray (2012) detallan que dentro de las técnicas de ocultamiento mas utilizadas esta la que se lo conoce con el nombre de esteganografía, una técnica que utiliza algoritmos matemáticos para ocultar un archivo dentro otro archivo de mayor tamaño, este proceso puede llevarse a cabo con la utilizando un simple comando copy hasta llegar a la utilización de software mucho mas sofisticado que hara que su detección sea mucho mas compleja. Asi mismo Stüttgen & Cohen (2013) dice que la practica del cifrado es conocida como la técnica anti forense mas utilizada debido a que se tiene fácil acceso a herramientas libres y de pago que no requieren altos conocimientos técnicos para ser utilizados, de tal manera que es utilizada para encriptar archivos y cualquier medio de almacenamiento, es así que Rekhis $ Boudriga (2013) dicen que para un analista forense es primordial dentro de sus primeros pasos ejecutados en la fase de preservación o de análisis de evidencias es determinar si el en el medio informático en el cual se esta trabajando, se ha ejecutado alguna técnica antiforense de cifrado sobre archivos o medios de almacenamiento, de esta forma podrán aplicar los procesos recomendados para tales casos.

Cifrado de Archivos

Muchas empresas han puesto a disposición soluciones de cifrado orientados a proteger la información contenida en archivos de datos, incluso los propios sistemas operativos cuentan con estas características que pueden ser utilizadas y configuradas por el usuario (Tseng, Huang, & Chang, 2014). Es asi que Ries (2015) dice que el sistema operativo Windows maneja un sistema denominado EFS (sistemas de cifrado de archivos) el cual trabaja combinando el cifrado simétrico con una clave para cifrar y poder descifrar los archivos, esta clave es protegida posteriormente con un cifrado asimétrico mediante la utilización de un certificado digital que lo generar dentro del proceso con el nombre del usuario, si es la primera vez que se realiza este proceso se genera una clave pasa uso del cifrado simétrico de la información a proteger con un algoritmos AES 256, a esta clave se la denomina File Encription Key o FEK, este FEK posteriormente se cifra utilizando la clave publica del usuario, el resultado de las utilización tanto de la clave publica como privada generan un certificado que se guardan en el almacén de certificados de este sistema pudiendo ser accesible por el mismo sistema, estos certificados tienen el nombre del usuario mas una extensión .msc (Ries, 2015)

Hanoymak (2013) manifiesta que usuarios también puede escoger entre un gran numero de herramientas gratuitas o de pago para solventar su necesidad de proteger sus archivos, dentro de estas soluciones predomina la utilización del algoritmo AES tanto de 128 y 256 bits, muy popular en la criptografía simétrica, siendo un cifrado generado por bloques no se ha encontrado aun un ataque exitoso sobre este algoritmo lo que lo hace muy seguro siendo utilizado por muchos gobiernos para garantizar la seguridad de su información clasificada; además de AES los aplicativos de protección utilizan otro tipo algoritmos también muy robustos como serpenter, TwoFish, BownFish y Ghost entre los que destaca.

En la tabla 1 veremos algunos programas para cifrado y el algoritmo que utilizan, asi como la plataforma en la que trabaja.

Tabla1

Programas utilizados para el Cifrado

Programa	Algoritmo que Utiliza	Plataforma
VeraCrypt	AES-256 Serpent, TwoFish	Win/Linux/Mac
AC-Crypt	AES-128	Win
CryptoForce	Blowfish-448 AES-256 Ghost 256	Win
FortFile Encryption	AES-256	Win
ECryptfs	AES-256	Linux
DiskCryptor	AES-256 Serpent TwoFish	Win
AES CRYPT	AES-256	Win/Linux/Mac

Nota: Listado Programas utilizados para el Cifrado de Archivos, donde se mmuestra el algoritmo que utiliza y la plataforma en la que funciona.

Otra forma de cifrado es el uso de programas de compresión de archivos, estas aplicaciones brindan la opción de encriptar la información, al momento de que se incluya una clave además de comprimir la información se cifrara, posteriormente será necesario introducir la misma clave para la descompresión y decifrado, estos aplicativos utilizan el algoritmo AES para asegurar la información (KARTIT & ELMARRAKI, 2015). En la tabla 2 veremos algunos programas de comprensión y que algoritmo utilizan, así como la plataforma en la que trabaja.

Tabla 2

Programas de compresion que usan cifrado

Programa	Algoritmo que Utiliza	Plataforma
WinRar	AES-128	Win/Linux
WinZip	AES 128-256	Windosw
7-ZIP	AES-256	Win/Linux

Nota: Programas de compresion que utilizan la opcion de cifrado, muetra los algoritomos que aplican y la plataforma donde trabaja.

Cifrado de Unidades de almacenamiento

Hanson & Tylor (2013) dicen que el sistema de cifrado orientado a unidades de almacenamiento garantiza que todo lo que se guarde en el dispositivo se cifre, siendo legible solamente cuando el usuario haya accedido al sistema y esté en funcionamiento caso contrario si alguien desea acceder a los datos con el equipo apagado accediendo al disco duro por otros métodos tendrá información ilegible, confusa y no podra visualizar ningún archivo real, cuando un disco duro se cifra por completo lo hace desde el primer bloque hasta el ultimo bloque de datos, desde el arranque al que normalmente se lo conoce como *pre-boot authentication o PBA,* que entra en funcionamiento cuando inicia el equipo.

Dell Corporation (2014) habla de la utilización de nuevas técnicas para el cifrado de discos duros, las versiones actuales de los equipos manejan una funcionalidad llamada trusted platform module o TPM, un microprocesador alojado en el *mainboard* del equipo, cuya característica es almacenar y autenticar las claves de cifrado del equipo, es decir que si el disco duro de un equipo es robado e instalado en otro equipo la información no será accesible, de esta forma trabaja el chip TPM como una puerta a la información; una de sus desventajas es que si se requiere el cambio del *mainboard* por avería, es muy probable que la información no sea accesible nuevamente, pero existen soluciones que también almacenan las claves de cifrado dentro de la misma unidad, así es como solventan este problema del TMP. Tanguy (2014) afirma que muchos fabricantes de unidades de almacenamiento traen el cifrado directamente en sus discos duros aplicando el estándar OPAL, que son especificaciones para los *self encrypting drives* (SED) o unidades de cifrado automáticos, lo que se hace mucho más sencillo el cifrado y la protección de los datos con estas unidades, pero además existen muchas herramientas de cifrado de discos, muchas son gratuitas y otras de pago, las comerciales normalmente enfocadas al mercado corporativo, y las gratuitas al personal, incluso algunas poderosas herramientas vienen incluidas dentro de los propios sistemas operativos que son cargados en nuestros equipos.

Microsoft (2012) indica que en sus sistemas operativos Windows viene instalada la aplicación BitLocker, una herramienta que utiliza un cifrado AES de 128 Bits, incorporada desde la versión 7 y posteriores, este software de cifrado trabaja con el chip TPM en el cual se almacena el PIN, al utilizar la cave directamente desde el TPM no se necesitara introducir un clave para acceder al equipo esta combinación de versatilidad permite la combinación del TPM y un PIN, pero al momento de su configuración puede marcarse y que si solicite el *password* al usuario antes de que inicie el sistema, adicionalmente BitLocker permite almacenar en una USB con las claves de acceso y que sin ella no podamos acceder al equipo, estos medios de acceso ya dependerá de la configuración inicial por parte del usuario.

Para la Plataforma de Apple OSX también se cuenta con soluciones para el cifrado de discos

duros dada las características que presenta la herramienta FileVault, este programa viene incluida en versiones y posteriores a Lion, todas las versiones son utilizan el algoritmo AES de 128 bit generando como es su características un cifrado muy robusto, de igual forma FileValut tiene varios aspectos particulares que son importantes destacar, en primer lugar si un usuario no tiene habilitado la opción de cifrado este aplicativo deja que inicie el sistemas hasta la pantalla de autenticación, pero deberá ser un usuario que tenga el cifrado activo e inicie sesión desbloqueando la unidad, un segundo aspecto particular que ya manejan otras aplicaciones es que este *software* genera una clave de recuperación que el usuario deberá almacenarla de forma segura o también permite generara una clave luego de responder varias preguntas previamente configuradas (Apple-Technical, 2013)

En los sistemas operativos Linux existe una variedad de herramientas que pueden ser utilizados con este fin, tanto para usuarios sin privilegios como para hacer cifrados completos del disco duro durante el arranque del equipo, para esto se utiliza el sistema de archivos EncFS (*Encrypt File System*) que viene a ser un directorio normal dentro del sistema en el cual contendrá los archivos cifrados mediante método hash, este directorio se encuentra dentro del directorio FUSE donde aparecerá la información de forma descifrada. (Lokhande & Avinash Wadhe, 2013)

El Cómputo forense y los sistemas FDE (*Full Disk Encryption*)

La inclusión del cifrado como parte de la seguridad los sistemas operativos han llevado a que los investigadores forenses tengan nuevos desafíos que cumplir al momento de la preservación y análisis de las evidencias digitales de un equipo informático, al encontrarse con un escenario de este tipo no podrá realizar su tares sin contar con las claves de acceso que permitirán acceder a los datos después de que un equipo de cómputo se encuentre apagado (Craiger & Swauger, 2013); por cuanto Fahd (2013) recomienda que al momento de encontrar un equipo encendido que ingresará dentro de un proceso de investigación forense, se verifique si la unidad maneja algún tipo de cifrado, de ser así, deberá realizarse una imagen forense de la unidad en vivo, con este tipo de adquisición se podrán manejar métodos de análisis factibles como le virtualización, que permitirán examinar de manera óptima un sistema FDE.

Shanmugam, Prashanthi, Sriram, & Krithika, (2015) manifiestan que durante el proceso de adquisición y preservación de evidencia donde se realiza el duplicado del disco duro se corre el riesgo de que el investigador no detecte que el disco se encuentre cifrado y luego de trasladar la información al laboratorio solo podrá ver datos de forma lógica, recomendando como parte de las buenas practicas durante este proceso, realizar un análisis previo en el sistema en busca de información que le permitirá verificar la existencia de un cargador de arranque FDE, así como constatar la falta de una estructura de carpetas muy comunes en estos sistemas de cifrado, de igual forma recalca que el método de adquisición deberá ser diferente al convencional donde se necesita sacar el disco duro y duplicarlo en los equipos especializados, aquí se deberá optar por generar imágenes forenses con el equipo encendido a nivel lógico, así como generar un volcado de la memoria RAM práctica muy recomendado para generar procesos de recuperación de claves, recalcando que el problema se presenta una vez apagado el equipo ya que no se tendrá acceso a la información del mismo hasta recuperar o encontrar las claves que permitirán acceder a los datos.

Es importante mencionar otro problema que conlleva la adquisición en vivo, los cambios que esta causa en la evidencia y que pueden ser un problema para el examinador que tendrá que detallar de forma específica el impacto que llevo su práctica sobre la evidencia digital, por ejemplo programas como FTK Imager Lite, OSforensic, o Encase Imager, generan una alteración a los datos volátiles cuando estos se cargan a la memoria, como al registro del sistema en donde se generan y se modifican entradas, es muy importante poder sustentar estos cambios sabiendo que en la parte legal juristas argumentan que las adquisiciones forenses no deberán alterar las evidencias originales por ningún concepto (Dykstra & Sherman, 2012).

Casey (2012) señala que muchos equipos de hardware orientados a la adquisición forenses presentan mensajes de error cuando se encuentran con disco duros cifrados con FDE, generando un problema para el investigador que de no encontrar la forma de solventar el problema deberá trabajar con las fuentes originales aplicando procedimientos que pueden alterar las fuentes originales al tratar de acceder a la información cifrada. De la misma forma recomienda que dentro de los primeros pasos al iniciar un análisis forense de sistemas FDE es identificar el tipo de cifrado que posee el disco, si se realiza una vista de los clúster con software forenses se podrá observar que no es fácil identificar cual producto fue utilizado, hay varios factores que intervienen en este proceso, primeramente es importante saber que al cifrar un disco se modifica el MBR (Master Boot Record o el VBR (Volumen Boot Record ya sea para ejecutar su código o los modifica con el objetivo de poder ejecutar el proceso de descifrado, en ambos casos la gran mayoría de soluciones de

cifrado generan unas firmas que identifican a cada producto.

Jenkins (2014) expone algunos ejemplos de firmas encontradas comúnmente en unidades de almacenamiento con sistemas FDE, utilizando el software de análisis forense Encase V7 muestra las ubicaciones de las firmas de algunas de las soluciones más comunes entre las cuales destacan el Check Point Full Disk Encryption en el cual se puede ser Localiza dentro del sector offset 90 en el VBR, la firma de este producto es "*Protect*" puede ser buscado con el valor hexadecimal "50 72 6F 74 65 63 74"

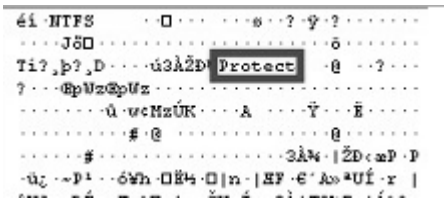

Figura 1. Firma FDE Generada con Check Point Full Disk Encryption
Fuente: Graham Jenkins Guidance Software, Spotting Full Disk, 2014 Encryption, 2014

También detalla el producto GuardianEdge Encryption Plus/Anywhere/Hard Disk Encryption and Symantec End point Encryption, en esta solución la encontramos en el sector offset 6 del MBR, la firma identificada es "PCGM" puede ser buscada con el siguiente valor hexadecimal "50 43 47 4D"

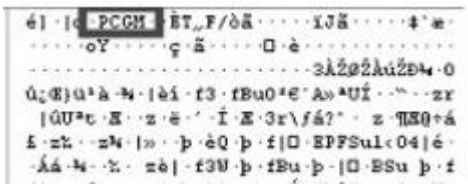

Figura 2. Firma FDE GuardianEdge Encryption Plus
Fuente: Graham Jenkins Guidance Software, Spotting Full Disk, 2014 Encryption, 2014

De igual forma hace mención al producto Sophos Safeguard Enterprise and Safeguard Easy de Safeguard Enterprise, donde describe al sector offset 119 del MBR, donde se almacena la firma cuyo identificador es "SGM400" y puede ser buscado con el valor hexadecimal "53 47 4D 34 30 30 3A"

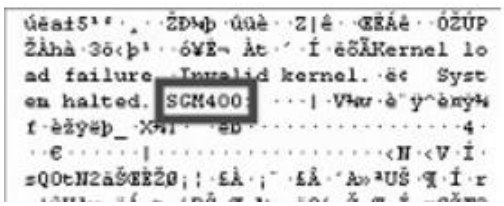

Figura 3. Firma FDE Sophos Safeguard Enterprise
Fuente: Graham Jenkins Guidance Software, Spotting Full Disk, 2014 Encryption, 2014

Técnica forense en cifrados de archivos

De acuerdo a Haoyang, Jiang, & Yuan (2013) conocer el tipo de cifrado con el cual está protegida la información es solamente el primer paso para planificar según los medios disponibles la aplicación de técnicas forenses para lograr acceder a la información, esto dependerá si es solo un archivo una carpeta o una unidad FDE. Menciona que dentro de estas técnicas forenses está la de utilizar las imágenes de las memoria RAM y archivos donde se alojan información generada y digitada por el usuario, en los sistemas operativos Windows tenemos a los archivos ntuser.dat, pagefile,sys, hiberfile.sys, el Linux podemos destacar la partición swap y el sistemas Mac a su archivo de intercambio de memoria, estos contenedores de información si bien son desconocidos por los usuarios almacenan gran cantidad de datos dentro de los cuales muy probablemente se encuentre las claves del cifrado de alguna carpeta , un archivo o un contenedor de datos creado con cifrado, con toda esta información varias aplicaciones forenses como AccesData Password Recovery, Elconsoff Password Recovery Bundle y Passware Kit se encargan de generar diccionarios de datos que será utilizados dentro del proceso que realizan denominado ataque por diccionario con la particularidad que serán palabras generadas por el mismo usuario lo que ha conseguido buenos resultados y mayor rapidez en el descifrado de archivos. Así mismo recalca que la intervención de un investigador forense sin experiencia puede cerrar la posibilidad de poder descifrar un archivo, el simple hecho de no generar una imagen de la memoria RAM antes de apagar el equipo se puede perder información sumamente valiosa e incluso la clave misma que pudo estar alojada de forma volatín dentro de este *hardware,* esto demuestra las pocas opciones disponibles que debe ser aprovechadas en este tipo de investigaciones.

Owens & Matthews (2013) mencionan que otro recurso para romper el cifrado dentro de una investigación digital es la utilización de *software* o *hardware* especializado en métodos ataque por fuerza bruta, que es el método en el cual se utilizan todas las combinaciones posibles de letras números y caracteres especiales. De la misma forma mencionan que este tipo de ataque consta de 4 aspectos vitales, primero un alfabeto para realizar las combinaciones que sean posibles, una longitud de palabra que nos permite determinar todas las posibles combinaciones, una palabra cifrada la cual se la requiere para realizar el proceso de ruptura del ciclo de interacciones en caso de localizar la palabra legible y por último un algoritmo de cifrado siendo indispensable para los procesos de fuerza bruta.

Cómputo forense y los criptosistemas

Walls & Neil Levine (2013) determinan que cuando se trabaja con medios electrónicos cifrados siempre se genera el riesgo de que los datos sufran alguna afectación o daño, para lo cual aconseja manejar un procedimientos para el manejo de evidencias digitales y que sean razonables, robustos y sobre todo defendibles es decir documentar de manera minuciosa los procesos realizados, determinando que la utilización de herramientas deben enfocarse a los estándares que se manejen en el medio forense digital, además menciona que la mayor preocupación en estas investigaciones es el descifrado de los datos o de la unidad en sí, que de acuerdo a los métodos utilizados pueden llevar varias horas, días o semanas lo que implica que mientras se trata de descifrar la información, la unidad está en constante trabajo lo que puede generar que esta falle, por lo tanto recomienda a los investigadores asegurarse de contar con respaldos de la fuente original y trabajar con herramientas forenses realmente compatibles con los datos de cifrado lo que permitirá generar un proceso más transparente y limpio que se verá reflejado en el trabajo menos forzado del disco en el proceso de descifrado.

Garfinkel (2014) menciona que una limitante que deben superar en la investigación de sistemas cifrados se encuentra en la parte legal ya que para iniciar el proceso de descifrado se requiere la autorización de un juez que en base a una presunción bien fundamentada autorice el proceso, normalmente en delitos graves como el terrorismo, pornografía infantil, asesinatos, tráfico de estupefacientes entre otras, dejando sin efecto la autorización en delitos de menor peso por temas de privacidad, esto hace que el uso de cifrado tanto en las comunicación como en el almacenamiento sea usado muy comúnmente, haciendo que la vida de los criminales y terroristas sea más fácil, mientras que para los investigadores forenses se torne muy difícil. De la misma forma comenta que los sistemas de cifrado se están implementado en las tecnologías de forma predeterminada sin que el usuario requiere instalar una aplicación o aceptar algunas condiciones, es así que encontramos Smartphone con sistemas integrados de cifrado así como Apple desde su versión IOS 8 establece cifrado de extremos a extremo al igual que G-mail. Menciona también que los sistemas operativos Windows desde la versión 8 y mejorada en la 10 utiliza el cifrado del disco duro por defecto.

Dingledine, Mathewson, & Murdoch (2014) dicen que el cifrado en las comunicaciones van de la mano con el anonimato que buscan las personas y esto desemboca en aplicaciones como TOR (the onion Router) muy popular para la navegación web anónima es un sistema simple que permite navegar por la web atreves de 7000 computadores vinculados de forma voluntaria, este software cifra los datos de forma automática de tal forma que no centra toda la información trasmitida en un solo computador sino en varios lo que hace muy difícil que sean investigados y localizados. De la misma forma que TOR, hace referencia a las aplicaciones utilizadas para la comunicación mediante dispositivos móviles que incluso son utilizadas de primera mano por los terroristas para planificar sus atentados, aplicaciones como Hiapp y Telegram especializadas para intercambiar mensajes cifrados e incluso que se auto destruyen luego de ser leídos, ha generado que sean muy utilizado en organizaciones delictivas. Indica también que Telegram es la favorita para ser usada en las comunicaciones por manejar un cifrado punto punto y una verificación de identidad del destinatario del mensaje, además maneja para su cifrado el algoritmo AES 256, generando de esta forma un mensaje que aunque sea interceptado sea indescifrable impidiendo que terceras personas puedan leer los mismos.

Badenhop (2016)**,** analiza el uso de los criptosistemas y la factibilidad de un análisis forense sobre estos y hace mención que el aumento del uso del cifrado genera un cambio en la metodología existente y que han sido adoptadas en muchos países como buenas prácticas en el manejo del cómputo forense, nos dice que la practica metodológica de desconectar el equipo de las fuentes eléctricas y proceder a la copia bit a bit de los discos duros ya no son viables, los investigadores que intervienen a incidentes de seguridad ven como la principal fuente de evidencia la localizada en la memoria RAM, siendo la primera el ser extraída, relegando en segundo plano a la unidades de discos duros; recalca que la memoria RAM contendrá información muy importante que nos permitirá investigar si tendemos archivos o particiones con cifrado dentro de la unidad, porque contendrá datos que nos permitan ejecutar procesos de descifrados así como otra información vital para una investigación.

CONCLUSIONES, LIMITACIONES Y TRABAJOS FUTUROS.

Para el computo forense encontrarse con métodos de cifrado genera grandes limitantes que se ven reflejadas en el desarrollo de la investigación, son pocas las probabilidades de lograr acceder a la información, y esto dependerá de las técnicas aplicadas por el investigador durante la recolección, y de un largo tiempo invertido, sin que esto asegure que se pueda conseguir el descifrado y el acceso a los datos.

Luego del análisis realizado sobre las limitaciones del cómputo forense y los criptosistemas, podemos determinar que existen una gran

variedad de aplicación que dan este servicio a los usuarios que en su gran mayoría utilizan el algoritmo AES de 128 o 256 bits para realizar un proceso un cifrado muy robusto tanto en archivos o unidades FDE, de igual forma se ha detallado que no existe regulación en el uso y distribución de estos sistemas que hasta las mismas corporaciones crean unidades de discos duros y sistemas operativos con un mecanismos de cifrado automático, es decir el usuario no tendrá que realizar ninguna aceptación al respecto, así también dentro del ámbito legal el computo forense encuentra sus limitantes en la cual se inicia una pugna legal de criterios, luego de que el juez conozca el pedido de autorizar la intervención de una unidad cifrada para lograr acceder a la información, su decisión en muchas ocasiones dependerá del peso del delito, que sea de interés nacional o sean graves para que acceda al petitorio, caso contrario dan paso a la protección de la privacidad de las personas negando la solicitud planteada, todos estos puntos generan un limitante en la práctica forense digital en termas de cifrado.

Existen muchas limitaciones que se encontraron durante el desarrollo de este trabajo, la gran cantidad soluciones que actualmente existen en el mercado tanto a nivel de software como de hardware para cifrado, esto no permitió realizar un análisis más específico de los mecanismos que utilizan cada uno, de igual forma en al campo del cómputo forense existen muy poca información con respecto a sistemas y técnicas utilizadas para el descifrado de archivos como de unidades FDE.

Es importante recomendar varios temas que pueden ser desarrollados en futuros trabajos, como la creación de diccionarios de datos a partir de la información de un usuario para la práctica de descifrado de archivos en la computación forense. De igual forma vemos que los criptosistemas también están dentro de las comunicaciones, sería importante realizar una investigación referente a la práctica del cómputo forense en navegadores anónimos como TOR. Igualmente se puede desarrollar un trabajado analice el el marco legal ecuatorianos referente a la posición que debe tomar un Juez al momento de negar o autorizar la intervención de un sistema cifrado con respecto a la privacidad y protección de datos de las personas.

BIBLIOGRAFÍA

Dingledine, R., Mathewson, N., & Murdoch, S. (2014). Tor: The Second-Generation Onion Router. *Computer University of Cambridge*.

Dykstra , D., & Sherman, K. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, 90-98.

Amerini, I., Becarelli, R., Bertini , B., & Caldell. (2015). Acquisition source identification through a blind image classification. *IET Image Processing 9,* , 329-337.

Apple. (2014). Best Practices for Deploying FileVault 2. *Deploying OS X Full Disk Encryption Technology*.

Apple-Technical. (2013). Best Practices for Deploying FileVault 2. *Apple Technical White Paper*.

Badenhop, C. W. (2016). Extraction and analysis of non-volatile memory of the ZW0301 module. *Digital Investigation Volumen 17*, 14-21.

Botero, A., Camero, I., & Cano, J. (2009). Técnicas Anti-Forenses en Informática: Ingeniería Reversa Aplicada a TimeStomp. *Departamento de Ingeniería de Sistemas, Pontificia Universidad Javeriana*.

Brown, C. S. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, 55–119.

Cano, J. J. (2004). INSEGURIDAD INFORMÁTICA: UN CONCEPTO DUAL EN SEGURIDAD INFORMÁTICA. *Revista De Ingeniería*, 44,49.

Carrier, B. (2002). Defining Digital Forensic Examination and Analisis Tools.

Casey, E. (2012). The Impact of Full Disk Encryption on Digital Forensics. *ACM SIGOPS Operating Systems Review* , 93 -98.

Corporation, D. (15 de 04 de 2014). *http://www.dell.com*. Obtenido de http://www.dell.com/support/article/us/en/04/SLN155364/es?c=us&l=en&s=bsd&cs=04#Hardware_encryption_versus_software_encryption

Craiger, P., & Swauger, J. (2013). Digital evidence obfuscation: recovery

techniques. *National Center for Forensic Science, University of Central Florida*.

Fahdi, M. A. (2013). Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions . *Information Security for South Africa*, 1 - 8.

forcht, K. A. (2004). Legal methods of using computer forensics techniques for computer crime analysis and investigation. *Issues Information System*.

Garfinkel,, S. (2014). he Prevalence of Encoded Digital Trace Evidence in the Nonfile Space of Computer Media. *Journal Of Forensic Sciences*, 1386-1393.

Halboob, W. (2015). Privacy Levels for Computer Forensics: Toward a More Efficient Privacy-preserving Investigation. *Procedia Computer Science Vol 56*, 370-375.

Hanoymak, T. (2013). On Provable Security of Cryptographic Schemes. *International Journal Of Information Security Science*, 44.56.

Haoyang Xie, Jiang, K., & Yuan, X. (2013). FORENSIC ANALYSIS OF WINDOWS REGISTRY AGAINST INTRUSION. *International Journal of Network Security & Its Applications (IJNSA)*, 121-134.

Henson, M., & Taylor, S. (2013). Beyond Full Disk Encryption: Protection on Security-Enhanced Commodity Processors. *Volume 7954 of the series Lecture Notes in Computer Science*, 307-321.

ISACA. (15 de 02 de 2012). *The Forensics Issues Raised by Full Disk Encryption*. Obtenido de http://www.isaca.org/chapters5/Ireland/Documents/2012%20Presentations/The%20Forensics%20Issues%20Raised%20by%20Full%20Disk%20Encryption.pdf

Jenkins, G. (18 de 04 de 2014). *Spotting Full Disk Encryption*. Obtenido de http://encase-forensic-blog.guidancesoftware.com/2014/04/version-7-tech-tip-spotting-full-disk.html

Kamal , D., & Bassil , M. (2011). The anti-forensics challenge. *ISWSA '11*.

KARTIT, Z., & ELMARRAKI, M. (2015). Applying Encryption Algorithm to Enhance Data Security in Cloud Storage. *Engineering Letters*, 277-282.

Lokhande , K., & Avinash Wadhe. (2013). Security in Android File System. *International Journal of Advanced Research in Computer Science and Software Engineering*.

Lukić, T. (2012). Digital Evidence. *Proceedings Of Novi Sad Faculty Of Law 46*, 177-192.

Microsoft. (02 de 07 de 2012). *BitLocker Drive Encryption Overview*. Obtenido de http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview

Mouhtaropoulos, A., Chang, T., & Grobler, M. (2014). Digital Forensic Readiness: Are We There Yet? *Journal of International Commercial Law & Technology*, 173-179.

Owens, J., & Matthews , J. (2013). A Study of Passwords and Methods Used in Brute-Force. *Department of Computer Science Clarkson University* .

Paredes, G. G. (2008). Introducción a la Criptografia. *Revista Digital Universitaria UNAM*.

Rekhis, S., & Boudriga, N. (2013). A System for Formal Digital Forensic Investigation. *IEEE Transactions on Information Forensics and Security*, 635-650.

Ries, D. G. (2015). Encryption: Basic security you should be using now. *Trends (15339556)*, 10,16.

Rubí, M. C. (2011). Teoría de números en criptografía y su debilidad ante la posible era de las computadoras cuánticas. *Ciencia Ergo Sum*.

Shanmugam, M., Prashanthi, K., Sriram, R., & Krithika, N. (2015). Proceedings of the 2015 International Conference on Advanced Research in Computer Science. *ACM New York*.

Stamm, M., Lin , S., & Ray , L. (2012). Forensics vs. anti-forensics: A decision and game theoretic framework. *2012 IEEE*

International Conference on Acoustics, Speech and Signal Processing (ICASSP), 1749 - 1752.

Stüttgen, J., & Cohen, M. (2013). Anti-forensic resilient memory acquisition. *Digital Investigation*, 105–115.

Tanguy, J. (2014). Self-Encrypting Drives. *Makron SSD Technical Marketing Engineer*.

Travieso, Y. M. (2003). La Criptografía como elemento de la seguridad informática. *ACIMED vol.11 no.6*.

Tseng, Y.-M., Huang, Y.-H., & Chang, H.-J. (2014). Privacy-preserving multireceiver ID-based encryption with provable security. *International Journal of Communication Systems*, 1034-1050.

Walls , R., & Neil Levine, B. (2013). Effective Digital Forensics Research is Investigator-Centric. *Dept. of Computer Science, University of Amherst, MA*.