Ingeniería inversa del sistema de archivos de DVRs PCBox

Silva, Gaston A.

Poder Judicial de Rio Negro

gsilva@jusrionegro.gov.ar

Abstract. La recuperación de videos de las grabadoras de video o DVRs dentro de la forensia digital, se ha transformado en una tarea dificultosa debido a la naturaleza modificada y falta de especificación de los sistemas de archivos que utilizan. Esta falta de especificación de la mayoría de los DVRs que se ofrecen en el mercado, impiden la recuperación y el análisis de los datos almacenados mediante las herramientas tradicionales utilizadas en la informática forense (por ej. Encase, FTK). El objetivo de este trabajo es analizar el sistema de archivos utilizado por los DVR marca PCBox que nos permita establecer un método forense confiable para la recuperación de los metadatos y los videos almacenados como así también la presentación del software desarrollado para la reconstrucción del sistema de archivos.

Keywords: Sistema de archivos DVR, ingeniería inversa, DVR PCBox, análisis metadatos, recuperación de videos.

1 Introducción

Los sistemas de detección y grabación de imágenes o DVR se han convertido en una herramienta útil para la identificación y esclarecimiento de delitos y/o accidentes.

Una amplia oferta de DVRs (Digital Video Recorder) se ofrecen en el mercado a precios accesibles que hacen posible su instalación en grandes y pequeños comercios como así también en viviendas familiares.

La mayoría de estos dispositivos almacenan los videos en discos rígidos utilizando sistemas de archivos propietarios [1] que dificultan su reconstrucción mediante el uso de herramientas ampliamente utilizadas en Informática Forense. Por ejemplo Encase, FTK y Autopsy no son capaces de reconocer la estructura modificada de los sistema de archivos de los DVRs.

Durante el año 2017 ingresaron al Laboratorio de Informática Forense causas que incluían DVRs entre los dispositivos a analizar en las cuales la recuperación de los videos era de gran importancia para esclarecer los hechos investigados. Las herramientas disponibles, no fueron capaces de recuperar los metadatos y los videos almacenados en los medios de almacenamiento utilizados por estas grabadoras de video.

1.1 Alternativas para la recuperación de videos y metadatos

La imposibilidad de recuperar la información utilizando las herramientas disponibles en el laboratorio de Informática Forense del Poder Judicial de Rio Negro ha generado la necesidad de analizar otras alternativas para lograr la extracción de los videos almacenados en los DVRs:

- Incorporación de herramientas forenses específicas.
- Ingreso a la interface gráfica del dispositivo.
- Ingeniería inversa del sistema de archivos para la reconstrucción de los videos y sus metadatos.

Incorporación de herramientas forenses específicas

Existen en el mercado herramientas que permiten identificar y recuperar los metadatos y los videos de varias marcas de DVRs. Algunas de las más conocidas son DVR Examiner y HX Recovery.

Contar con este tipo de herramientas agiliza el proceso de análisis ante la presencia de DVRs entre los dispositivos secuestrados.

Como principal desventaja podemos encontrar el alto costo para la adquisición de estas herramientas.

Ingreso a la interface gráfica del dispositivo

Esta metodología requiere realizar una copia forense bit a bit del disco del DVR, conectarlo al equipo, encenderlo, ingresar un usuario y clave válidos para luego acceder a la interface gráfica de visualización y recuperación de videos. Una vez finalizado este proceso, se debe apagar el DVR y volver a conectar el disco original.

El encendido de los dispositivos no es una práctica forense recomendable ya que puede producir cambios en la información almacenada en el disco rígido. En el caso de los DVRs se recomienda ponerlos en marcha sin cámaras conectadas para evitar que las mismas envíen las imágenes capturadas al medio de grabación.

Aunque se desconecten las cámaras, igualmente hay posibilidades que se produzcan cambios en los datos del disco rígido ya que muchos de los sistemas operativos de los DVRs guardan la información de eventos en un área específica del disco. Estas modificaciones, pueden ser documentadas y justificadas como cambios controlados que no afectan los metadatos ni los videos y así darle validez a la información recuperada a partir de este método.

Sin embargo en muchas ocasiones no tendremos disponibles un usuario y clave válidos, siendo poco probable el acceso al dispositivo.

Ingeniería inversa del sistema de archivos

Para el caso particular del sistema de archivos de los DVRs PCBox, no existe documentación y/o especificación del mismo haciendo indispensable la aplicación de ingeniería inversa.

La ingeniería inversa persigue el objetivo de obtener la mayor cantidad de información técnica de un producto, del cual no se tiene la más mínima información de su diseño, construcción y funcionamiento, de modo que se debe partir de un todo para comprender cada pieza del sistema.

Como resultado obtendremos una especificación detallada del funcionamiento del sistema de archivos bajo estudio, que nos permitirá la identificación y recuperación de los videos almacenados y de sus metadatos, pudiendo dar certeza que el proceso de recuperación cumple con todas las etapas de la metodología forense aplicada en nuestro laboratorio.

Según [2] el término ingeniería inversa se refiere al proceso de analizar la estructura, funcionamiento, características y, en general, los fundamentos técnicos de un sistema o dispositivo ya sea mecánico o electrónico, e incluso un programa computacional (software). La actividad de ingeniería inversa usualmente requiere examinar, desarmar y analizar los componentes del dispositivo para crear otro dispositivo que pueda ya sea replicar o mejorar su funcionamiento, o bien que pueda interactuar ("conversar") con el dispositivo analizado. En el caso de un programa de software, este proceso usualmente involucra examinar el programa compilado (o ejecutable) e incluso ejecutarlo bajo condiciones controladas. También puede incluir un análisis del código fuente, esto es, el programa correspondiente escrito en un lenguaje de programación de alto nivel. Intuitivamente, la ingeniería inversa es una técnica que – cuando es exitosa -- permite a un investigador o profesional determinar "cómo" opera un programa y sus características.

En nuestro caso, no contamos con los códigos fuentes del sistema de archivo por lo cual nuestro trabajo se basará en el análisis de la estructura y funcionamiento del sistema de archivos utilizado por los DVRs PCBox que a partir de ahora denominaremos QFAT File System.

1.2 Funcionamiento de un DVR

Un DVR es un dispositivo electrónico que almacena videos en formato digital en un medio de almacenamiento (generalmente un disco rígido). El grado de especificidad de estos dispositivos hace que la utilización de un sistema de archivos tradicional (NTFS, EXT2, EXT3, etc) [3] sea una sobrecarga.

La utilización de un sistema de archivos tradicional implica una mayor demanda de memoria, y dada la acotada disponibilidad de RAM que poseen y la necesidad de realizar las acciones de escritura y lectura lo más eficientes posibles han llevado a la implementación de sistemas de archivos específicos que optimicen la grabación y la recuperación de videos. En verdad, los sistemas de archivos de los DVRs son sencillos ya que implementan un conjunto acotado de funcionalidades necesarias para el almacenamiento y recuperación de videos, no siendo necesarias, por ejemplo, una

gestión de permisos de usuarios, una estructura de árbol con carpetas anidadas ni la posibilidad borrar archivos de video ni renombrarlos.

Además de las funciones de grabación y recuperación de videos, los DVRs cuentan con un sistema de LOGS que permite almacenar cronológicamente los eventos acontecidos a partir del arranque del sistema y durante su funcionamiento.

2 Análisis del medio de almacenamiento

Basandonos en el análisis en capas propuesto por Brian Carrier [4] se abordó el análisis en los niveles de volúmnes, sistema de archivos y aplicaciones.

Partiendo de un disco vacío, se procedió a conectarlo. El DVR PCBox modelo PCB-DVR9008 detectó el HDD aunque sin una estructura conocida y nos permitió darle formato. Una vez formateado y sin tener conectada ninguna cámara para evitar que se inicie el proceso de grabación, apagamos el equipo y retiramos el disco.

Este primer paso resultó de gran importancia para el análisis a nivel de volúmenes y, lo que Carrier denomina contenido y Sistema de archivo, dentro del nivel de sistemas de archivos

Para realizer el análisis de los metadatos y los videos (dentro de la capa de sistemas de archivos) y la capa de aplicaciones, se conectaron las cámaras al DVR, se configuró la cámara 1 con modalidad de grabación en “detección de movimiento” con un frame rate de 25. La cámara 2 con modalidad de grabación en “modo continuo” y frame rate de 2. Se dejó el DVR en funcionamiento registrando la fecha configurada en el dispositivo.

.

Para la realización de estas tareas se hizo uso de las siguientes herramientas:

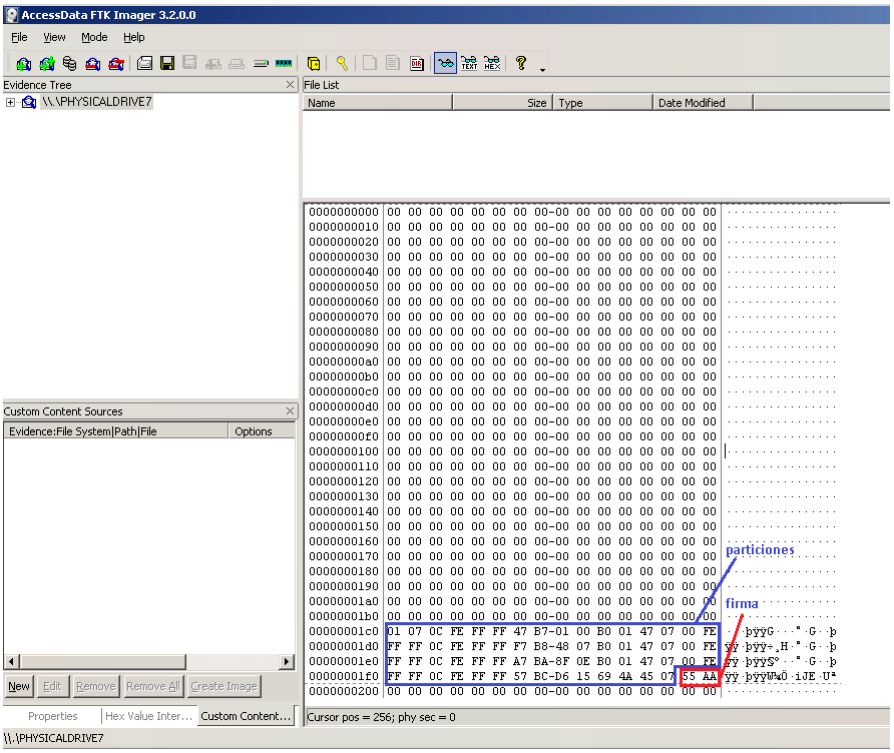
- Bloqueador de escritura Tableau eSATA Forensic Bridge: el montado de la unidad para el análisis de los datos requiere un bloqueo que evite cualquier modificación de la información almacenada
- FTK Imager 3.2.0.0: nos permite el montado del disco, reconocer particiones, la lectura y localización de sectores del disco, la visualización en modo texto y hexadecimal de la información contenida, búsqueda por palabras claves y desplazamientos absolutos desde el comienzo del disco o relativos a una posición particular.
- Calculadora Hexadecimal (https://es.calcuworld.com/calculadoras-matematicas/calculadora-hexadecimal/ : para la conversión de valores hexadecimal a decimal haciendo más fácil la interpretación de la información a descifrar.
- Convertidor de estampillas de tiempo UNIX (https://www.epochconverter.com/): convierte una estampilla de tiempo en formato UNIX a un formato legible por el humano

2.1 Análisis de Volúmenes

Utilizando el bloqueador Tableau eSATA Forensic Bridge y FTK Imager se analizó el primer sector del disco.

Se pudo observar una firma digital de booteo (Boot Signature) (/xAA/x55) que sugiere que estamos en presencia de un MBR (Master Boot Record) [5]. Su estructura no coincide con la de MBRs conocidos ni tiene código de Booteo.

Se pudo descifrar la existencia de cuatro particiones donde se detalla el sector de inicio y el tamaño en sectores de cada una de ellas.



FTK Imager, al montar el disco, reconoce la existencia de 4 particiones exFAT aunque no puede reconocer el sistema de archivos de las mismas.

2.2 Análisis del Sistema de Archivos

Teniendo decodificadas las direcciones de comienzo de cada partición, comienza la tarea de interpretación del tipo de sistema de archivos de las mismas.

Para el caso de estudio, se pudo determinar que las particiones generadas son del mismo tamaño a excepción de la última cuyo tamaño es ligeramente inferior. Analizando el primer sector de cada partición, (Partition Boot Sector) y basados en la especificación de particiones FAT [6] parecemos estar en presencia de sistemas de ar-

chivos FAT. La firma OEM “mkdosfs” indica que la partición fue creada con la herramienta mkdosfs (aplicación utilizada para crear sistemas de archivos DOS bajo el sistema operativo Linux).

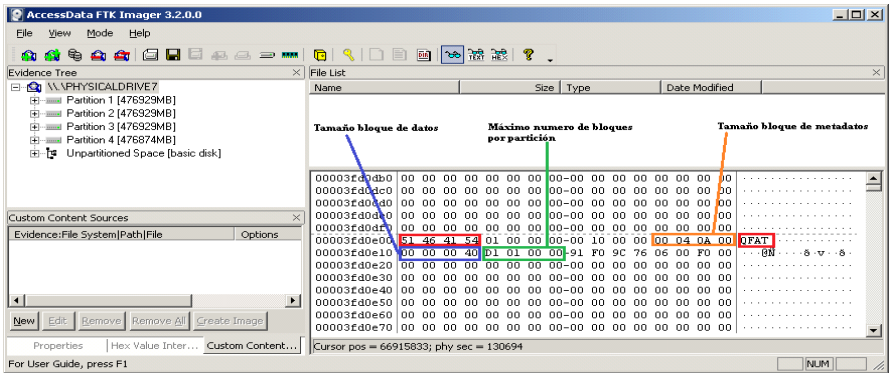
Desplazándonos a la posición de la Tabla de Asignación de Archivos (FAT) [6] no encontramos una estructura que se corresponda con este tipo de sistema de archivos.

Buscando datos que puedan revelar algo de información del tipo de sistema de archivos de las particiones generadas luego del formateo, encontramos un sector cuyos primeros 4 bytes eran la palabra “QFAT”.

Este sector contiene la siguiente información:

- Tamaño de los bloques de metadatos: del byte 12 al 15
- Tamaño de los bloques de datos (Videos): del byte 16 al 19.
- Máximo número de bloques: del byte 20 al 23

Los datos numéricos están almacenados en formato Little Endian [7]



Ocho sectores más adelante comienza el primer bloque de metadatos de la partición.

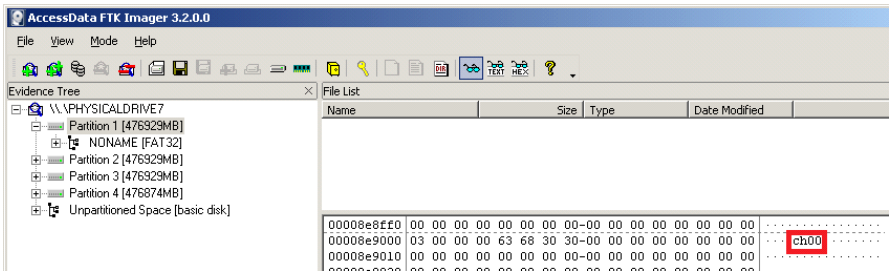
Para llegar al comienzo del primer bloque de videos, se debe multiplicar el tamaño de un bloque de metadatos por la cantidad de bloques de metadatos y sumarlo al inicio de la partición.

2.3 Análisis de Metadatos, organización del sistema de archivos, indexado de datos y nombres de archivos

Como señalamos anteriormente, el comienzo del área de metadatos esta 8 sectores por debajo del primer sector de QFAT de cada partición.

Se puso en funcionamiento el DVR, se conectaron las cámaras y se inició el proceso de grabación. Se documentó la fecha establecida en el sistema, los canales y los tiempos de grabación.

El primer dato de importancia encontrado en el primer bloque de metadatos fue la identificación del canal de grabación con la cadena de caracteres “chXX” donde XX es un número de dos dígitos que señala el canal de grabación al que corresponde el bloque de metadatos.



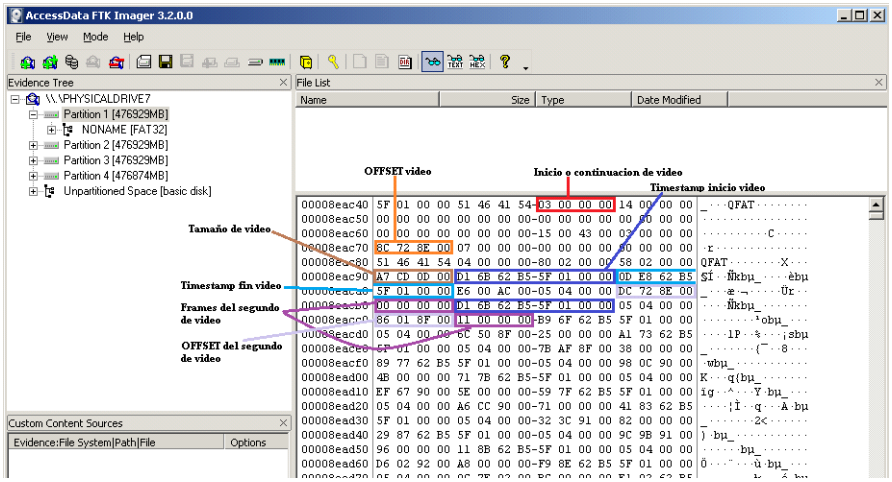
Desplazándonos al siguiente bloque de metadatos, se observó otro canal de grabación.

La reiteración y sucesión de bloques analizados nos permitió determinar que cada arranque de grabación de un dispositivo de captura (cámara fija, domo, etc) era identificado con un nuevo bloque de metadatos. Los metadatos se guardan de manera secuencial en cada bloque hasta que su espacio o el del bloque de datos (videos) se agota y el sistema de archivos le asigna el siguiente bloque vacío disponible.

El siguiente paso fue descifrar el significado de los metadatos. En esta etapa nos encontramos nuevamente con la utilización de la palabra “QFAT” como separador de información. El mismo término fue descubierto como delimitador dentro del área de datos y de aquí surge la denominación QFAT File System.

Para cada archivo de video grabado se almacena la siguiente información:

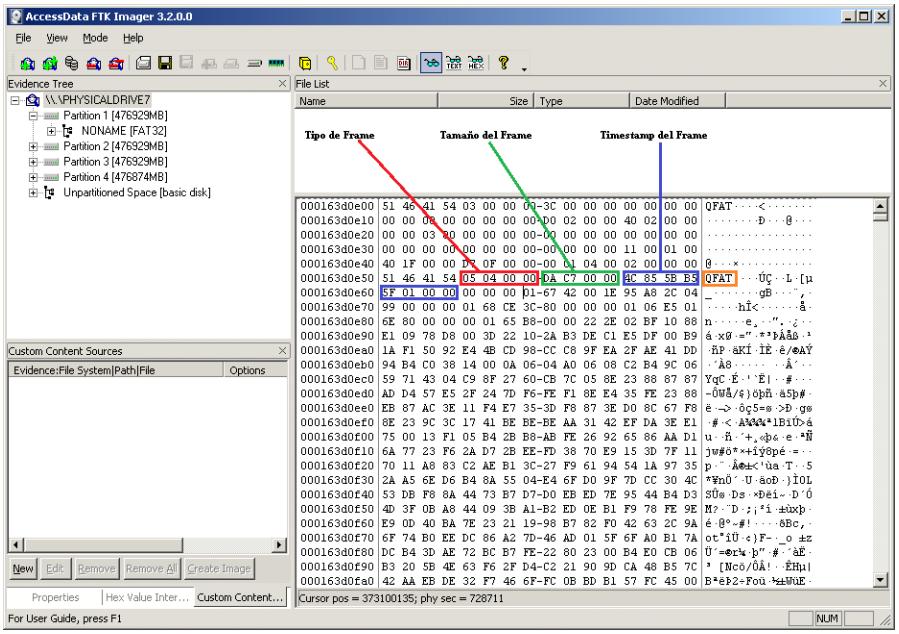
- Un valor que indica si el video es continuación de un video que se comenzó a grabar en algún bloque anterior o si es el inicio de grabación.
- El desplazamiento del video dentro del bloque de datos
- El tamaño en bytes del video
- Dos timestamp en formato UNIX [8] que indican la fecha y hora de inicio y fin de la grabación.
- Para cada segundo de grabación se indica su timestamp, su desplazamiento relativo dentro del bloque de video y su cantidad de Frames generados por el estándar de grabación de video H264 [9]



2.4 Análisis a nivel aplicaciones

Como explicamos en la sección anterior, conocemos el desplazamiento relativo de cada segundo de video y la cantidad de Frames.

Cada Frame está separado por la palabra “QFAT” y está formado por un timestamp que indica el momento exacto que representa dentro de la grabación, un valor que define el tipo de Frame (Predictive Inter Frame, Bi Predictive Inter Frame o Intra Frame) [10], el tamaño del frame en bytes y por último su codificación.



Hay una correspondencia uno a uno entre los bloques de metadatos y los bloques de Video. Si en una partición hay X bloques de metadatos entonces hay X bloques de Video,

Si el espacio de un bloque de metadatos se agota durante la grabación de un canal CHXX, el sistema de archivos le asigna a ese canal el próximo bloque de metadatos disponible hasta agotar el máximo número de bloques definido durante el formateo del disco. El cambio de bloque de metadatos hace que también se asigne un nuevo bloque de Videos que se corresponde secuencialmente con el de metadatos.

Las acciones anteriores se repiten si el que se agota primero es el espacio de un bloque de Videos.

Si no hay bloques disponibles en una partición entonces se comienzan a utilizar los bloques de la siguiente partición.

Si no quedan disponibles bloques en ninguna de las cuatro particiones, entonces si el modo de grabación es cíclico se comienza a sobreescribir la partición con grabaciones más viejas.

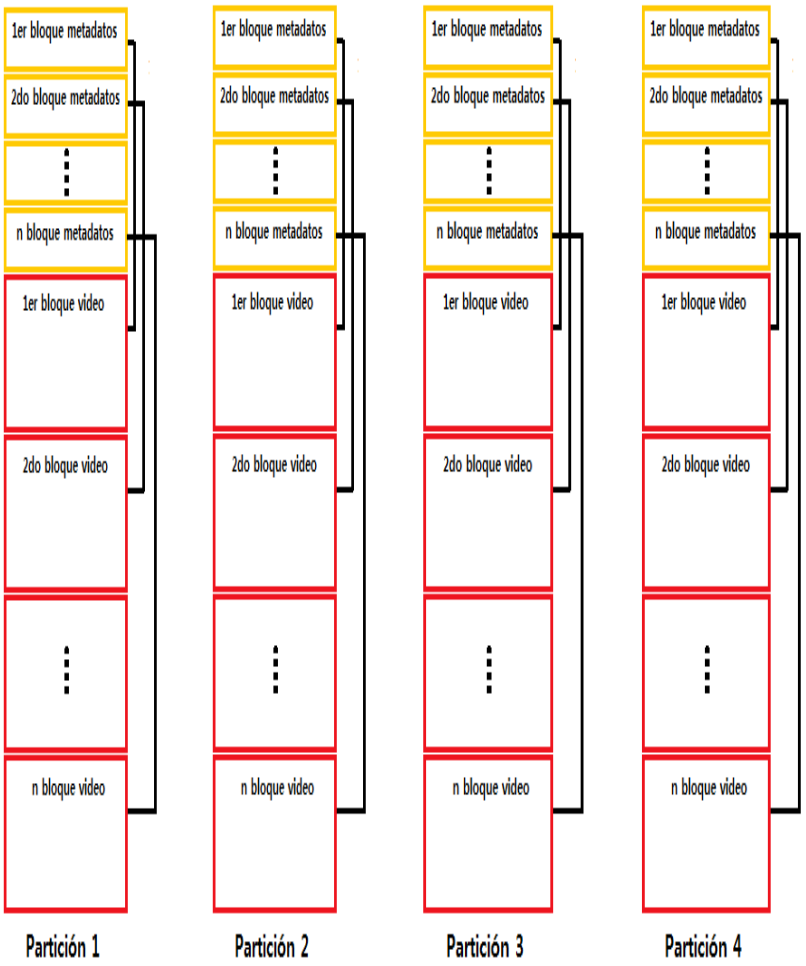


Figura . Las 4 particiones creadas por el DVR y la correspondencia de los bloques de metadatos y de videos

2.5 Búsqueda de Registros de Logs

Los registros de logs [11] identifican todos los eventos del sistema. Para las ciencias forenses puede formar una fuente de información importante que nos permita determinar posibles acciones intencionales tales como el formateo intencional del disco para eliminar evidencias, cambio de horarios y fechas del sistema o anulación del envío de capturas de las cámaras al medio de grabación.

En el caso particular del sistema de logs de los DVRs PCBox el primer paso fue intentar determinar el lugar físico donde se guardan los registros. Las dos alternativas posibles abordadas fueron:

- Algún sector del disco rígido
- Algún sector de la memoria interna del DVR

La segunda alternativa es la más fácil de comprobar dado que si desconectamos el disco rígido, ingresamos al sistema de gestión del DVR y consultamos el log, debería mostrarnos los registros de actividades que sucedieron mientras estuvo en funcionamiento.

Efectivamente el resultado de este proceso nos arrojó el detalle de los eventos sucedidos por lo cual se deduce que los logs son guardados en la memoria interna del DVR.

Como ventaja de esta implementación podemos decir que es más difícil su modificación ya que debemos ingresar al sistema operativo para tener acceso al área reservada para el resguardo de los registros. Se intentó ingresar a través del servicio de TELNET pero el puerto de servicio no está habilitado.

Una posible desventaja es la limitación en espacio de la memoria interna del DVR que pondría un límite a la cantidad de registros que podrían resguardarse.

3 Software PCBox FS Recovery V1.0

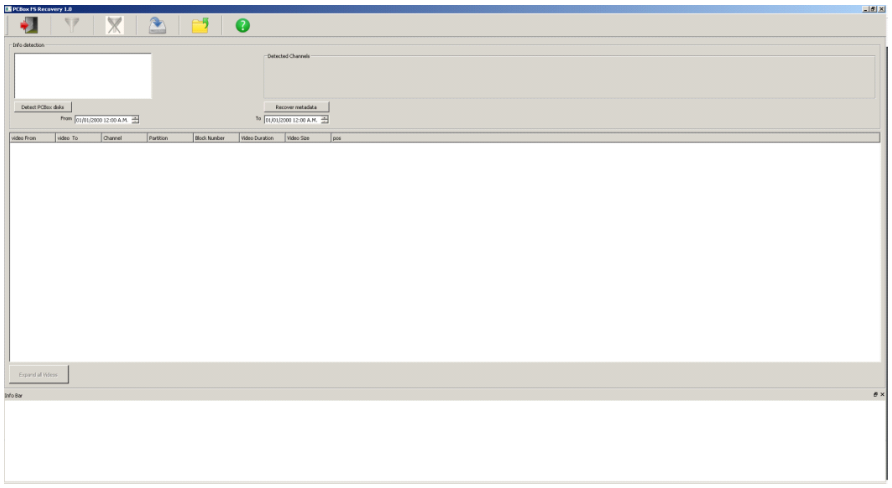
El software creado permite detectar los discos rígidos con sistema de archivos QFAT File System, reconstruir y visualizar los metadatos de los videos y filtrar y seleccionar los videos que se quieren recuperar.

La interfaz gráfica fue desarrollada con PyQt (es un binding de la biblioteca gráfica Qt para el lenguaje de programación Python)

La lógica para la reconstrucción del sistema de archivos se desarrolló en el lenguaje de programación Python utilizando el paradigma de Programación Orientada a Objetos.

3.1 Interface Gráfica

La ejecución del sistema se realiza desde la línea de comandos con la instrucción “python PCBox.py” y funciona bajo el sistema operativo Windows



Se recomienda conectar el disco a descifrar utilizando un bloqueador de escritura para evitar posibles modificaciones de la información contenida en el mismo.

3.2 Menu

- Presionando este botón se sale del sistema
- El botón de filtro se encuentra deshabilitado al inicio de la ejecución del programa. Se habilita una vez que se han detectado la existencia de metadatos. Al presionar el botón de filtrado, la visualización de los metadatos de videos representados por la fecha de inicio y fin de cada video, se limitaran a aquellos que estén entre el rango de fechas especificados en los campos “From” y “To” y de los canales de grabación seleccionados en los checkboxes “Detected Channels”
- Presionando este botón se eliminan los filtros aplicados.
- Este botón permite grabar los videos seleccionados en el árbol de visualización de metadatos de videos. Antes de comenzar la grabación se debe elegir la ubicación donde serán recuperados los archivos de video.

  Si previamente no se seleccionó una ubicación, aparecerá un recuadro donde se consulta si quiere seleccionarla.

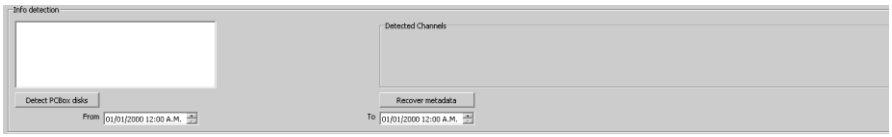
  Si ya se especificó una ubicación, entonces se grabaran todos los videos seleccionados en el árbol de metadatos.

  El nombre de los archivos se compone con la fecha y hora de inicio y la fecha y hora de finalización de la grabación. La extensión de los archivos es .h264. Para visualizarlos se puede utilizar el reproductor VLC (debe tener habilitado los codecs h264).

En caso que la cantidad de frames por segundo de grabación sea muy baja, el sistema mostrará en la barra de información (en la parte inferior de la ventana principal) como puede convertirse el archivo recuperado para una correcta visualización. En caso de no convertirlo, la reproducción se verá a mayor velocidad.

- Presionando este botón aparecerá un cuadro de dialogo que le permitirá elegir la ubicación donde se grabaran los videos.
- Al presionar este botón aparecerá un cuadro de ayuda e información del sistema.

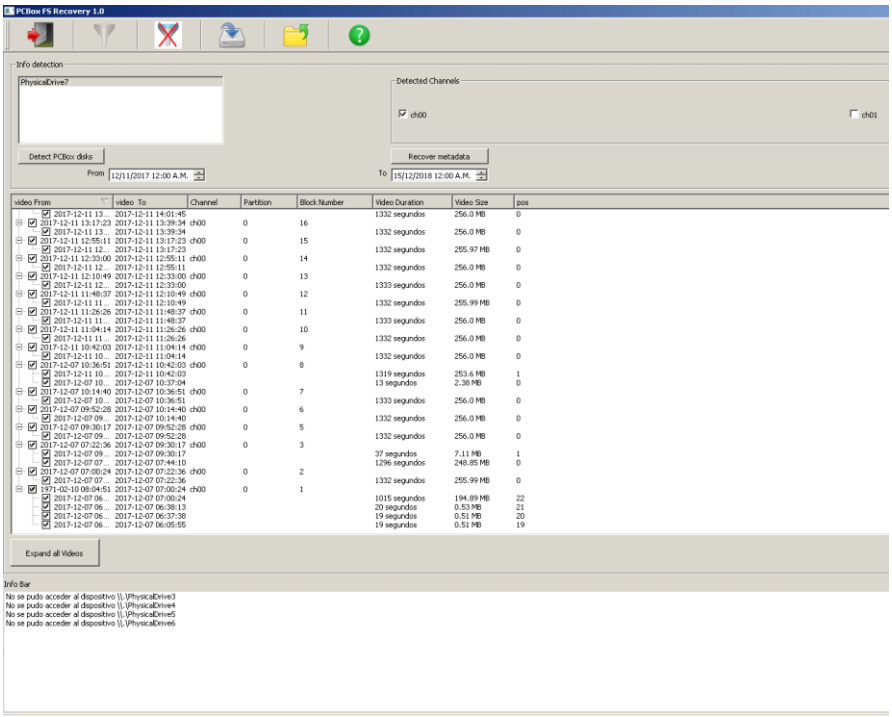
3.3 Detección de información



Para comenzar a utilizar las funciones del sistema primero hay que detectar el o los discos que pertenecen a algún DVR PCBox. Para ello se debe presionar el botón “Detect PCBox disks”. El sistema recorrerá todos los dispositivos físicos conectados a la PC donde se está ejecutando la aplicación y listará los nombres de aquellos que cumplan la condición.

Al hacer click sobre alguno de ellos y seguidamente presionamos el botón “Recover metadata” se recorrerá el sistema de archivos QFAT File System en busca de los canales de grabación que han capturado imágenes y los rangos de fechas que hay en cada bloque de metadatos, los cuales serán listados en el cuadro “metadata info”.

El botón “Expand all Videos” recupera los metadatos de cada video y los muestra en forma de árbol.



Se pueden limitar los resultados mostrados utilizando los filtros de fechas y de canales.

Cada archivo tiene un checkbox. Aquellos videos que estén marcados manualmente haciendo click en el check y/o mediante el uso de filtros serán los recuperados al presionar el botón “save” que se encuentra en la barra de menú.

3.4 Barra de información

Aquí se muestra información relacionadas con las acciones o inconvenientes durante el uso del sistema. Por ejemplo, se listan los dispositivos que no pudieron ser accedidos, los videos con bajo frame rate y la manera que pueden convertirse para una correcta visualización.

4 Conclusiones

La falta de especificación del sistema de archivos de la mayoría de los DVRs que se ofrecen en el mercado, impiden la recuperación y el análisis de los datos almacenados mediante las herramientas tradicionales utilizadas en la informática forense (por ej. Encase, FTK).

La utilización de la ingeniería inversa nos permitió determinar en forma detallada el funcionamiento del sistema de archivos utilizado por los DVRs marca PCBox posibilitando el desarrollo del sistema PCBox FS Recovery para la reconstrucción de los metadatos y de los videos almacenados en cualquier disco conectado a uno de estos equipos.

El grado de detalle logrado en el proceso de ingeniería inversa nos va a permitir desarrollar a futuro un sistema de recuperación de videos (video carver) en aquellos casos en los que la estructura de metadatos se encuentre dañada ya sea por sectores defectuosos o al darle formato al disco desde el DVR.

Más allá de los buenos resultados obtenidos, cabe destacar que este método requiere de mucho tiempo de análisis y pruebas, siendo poco probable utilizarlo en casos de urgencia que requieran descifrar sistemas de archivos desconocidos utilizados por otras marcas de DVRs.

Referencias

1. Richard Gomm, Nhien-An Le-Khac, Mark Scanlon and M-Tahar Kechadi, “An Analytical Approach to the Recovery of Data from 3rd Party Proprietary CCTV File Systems”
2. Dr. Alejandro Hevia, “La Ingeniería Inversa y su Rol en la Seguridad Informática” https://users.dcc.uchile.cl/~ahevia/ing-reversa.pdf
3. Brian Carrier, File System Forensic Analysis. Capítulos 11 y 14.
4. Brian Carrier, Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.14.9813&rep=rep1&type=pdf
5. Brian Carrier, File System Forensic Analysis pag. 66-73.
6. White Paper - Microsoft Extensible Firmware Initiative FAT32 File System Specification https://download.microsoft.com/download/1/6/1/161ba512-40e2-4cc9-843a-23143f3456c/fatgen103.doc
7. Endianness White Paper - http://www.pascal-man.com/navigation/faq-javabrowser/jython/endian.pdf
8. Timestamps en Unix - https://www.unixtimestamp.com/
9. ITU-T. H.264, advanced video coding for generic audiovisual services (2004). http:// www.itu.int/
10. White Paper – H264 video compression standard – AXIS Communicatios, https://www.axis.com/files/whitepaper/wp_h264_31669_en_0803_lo.pdf
11. Cano, Jeimy. Computación Forense. Descubriendo los Rastros Informáticos. Alfaomega. Méjico. (2009), p.313-316