EDP UNIVERSITY OF PUERTO RICO, INC.
RECINTO DE HATO REY
PROGRAMA DE MAESTRIA EN SISTEMAS DE INFORMACION
ESPECIALIDAD EN SEGURIDAD DE INFORMACION E
INVESTIGACION DE FRAUDE

CONSPIRACIÓN PARA ELUDIR LOS SISTEMAS DE PROTECCIÓN DE DERECHOS DE AUTOR Y TRÁFICO EN DISPOSITIVOS DE DESCIFRADO DE SATÉLITES

ANALISIS DEL CASO: UNITED STATES OF AMERICA VS ALNARDO VÁZQUEZ, AWILDO JIMENEZ, AND HIGINIO LAMBOY, NUMERO DE CASO: 18-670(ADC)

REQUISITO PARA LA MAESTRIA EN SISTEMAS DE INFORMACION
ESPECIALIDAD EN SEGURIDAD DE INFORMACION E
INVESTIGACION DE FRAUDE

MAYO, 2019

PREPARADO POR

WING SIANG NG ROSA

Sirva la presente para certificar que el Proyecto de investigación titulado:

CONSPIRACIÓN PARA ELUDIR LOS SISTEMAS DE PROTECCIÓN DE DERECHOS DE AUTOR Y TRÁFICO EN DISPOSITIVOS DE DESCIFRADO DE SATÉLITES

ANALISIS DEL CASO: UNITED STATES OF AMERICA VS ALNARDO VÁZQUEZ, AWILDO JIMENEZ, AND HIGINIO LAMBOY,

NUMERO DE CASO: 18-670(ADC)

PREPARADO POR:

WING SIANG NG ROSA

Ha sido aceptado como requisito parcial para el grado de:

Maestría en Sistemas de Información con Especialidad en Seguridad de Información e Investigación de Fraude

Mayo, 2019

Aprobado por:

Dr. Miguel Drouyn Marrero, Director

Tabla de Contenido

Tabla de Figuras

Sección 1: Introducción y Trasfondo

Introducción

El uso de satélites para el entretenimiento en los hogares ha tenido un incremento debido a que este servicio muestra más canales televisivos que la televisión conectado por antenas de tv con los canales locales. Las señales transmitidas por el satélite emisor al satélite receptor son encriptadas para evitar el hurto del dicho servicio. Al pasar el tiempo y con el avance tecnológico se ha descripta la señal para el uso en otro dispositivo no autorizado por el proveedor de servicio. El gobierno de Puerto Rico ha promovido leyes para combatir estos delitos hacia las compañías proveedoras. Según Cordero, (2013), se desarrolló una alianza contra la creciente piratería de señales digitales en una vista legislativa en la que las principales empresas dedicadas al negocio de televisión por cable o satélite apoyaron un proyecto de ley para combatir y penalizar esa práctica en Puerto Rico. Portavoces y directivos de las compañías Dish, Choice, Liberty Cablevision y DirecTV respaldaron la aprobación del Proyecto del Senado 410 para tipificar como delito la venta, instalación, interferencia, alteración o uso de equipo de recepción de servicios de cable televisión, televisión por satélite o servicios similares.

Descripción del caso

Numero de caso: 18-670(ADC)

Caso: United States of América VS Alnardo Vázquez, Awildo Jiménez Y Higinio Lamboy

Asunto: conspiración para eludir los sistemas de protección de derechos de autor, infringir derechos de autor y tráfico en el descifrado de satélite.

Partes en el caso:

Acusados:

- Alnado Vázquez, conocido como Naldo y Naldo Dish de edad 41 años
- Awildo Jiménez, conocido como Wildo, joselo626 y wildo20, de edad 36 años
- Higinio Lamboy, conocido como lngi, de edad 46 años

Entidades relacionadas al caso (victimas):

- Dish Network, Llc ("Dish")

Agente Investigador:

- Resultado de los esfuerzos de investigación por FBI.

Abogados:

- Manuel A. Morales

  Abogado de Armando Vázquez y Awildo Jiménez

- Eric A. Vos, Iván Santos Castaldo y Vivian I. Torralbas Halais

  Abogados de Higinio Lamboy

- Kebharu Smith

  Abogado litigante, División criminal.

Fiscales

- Nicholas W. Cannon

  Asistente del fiscal de los Estados Unidos Subjefe de inmigración, ciberdelitos y explotación infantil.

- José Capo Iriarte

  Asistente fiscal de los Estados Unidos Jefe, División criminal.

- Rosa Emilia Rodríguez Vélez jefa de la Fiscalía federal en Puerto Rico Abogada de los Estados Unidos.

Juez: Aida M. Delgado Colón, Juez de los Estados Unidos para distrito de Puerto Rico.

Trasfondo:

El señor Vázquez y Jiménez son los acusados de delito es poseer información ilícitamente para luego ser distribuida través usando servidor para lo cliente de los acusados. Ellos eran los propietarios y operadores de una organización que proporcionó los servicios pirateados a los clientes que pagaron una cuota mensual en efectivo para obtener el contenido

con derechos de autor entregados desde satélites DISH. Además, se identifica a Lamboy como su vendedor y reparador para el hardware que proporcionaron a sus clientes. La acusación describe un complejo esquema para hurtar el contenido protegido por derechos de autor para obtener beneficios financieros a través de la intercepción de señales de DISH cifradas que se distribuyeron para los clientes de DISH y descifrados a través de hardware emitido por DISH.

Descripción de los hechos:

Según los documentos del caso United States of América Vs Alnardo Vázquez, Awildo Jiménez, And Higinio Lamboy (2018), su reclamo fue por conspiración para eludir los sistemas de protección e infringir los de derechos de autor y tráfico en el descifrado de satélite.

El señor Vázquez junto Awildo Jiménez e Higinio Lamboy crearon una micro organización para obtener beneficios monetarios por uso de receptores de satélite programados con un software especial que permite a los receptores realizar una conexión directa a un servidor a través de Internet. Este servidor "internet key sharing" (IKS) elude la encriptación para poder descifrar la señal por uso de tarjeta originales del proveedor de servicio para tomar las llaves para ser distribuida por medio del internet. Los receptores no autorizados de los usuarios finales utilizan las llaves para descifrar las señales satelitales de DISH para obtener la programación de DISH sin autorización y sin el pago de una tarifa a DISH. El acceso a un servidor IKS generalmente está restringido para que un usuario final tenga que comprar una suscripción de un servicio pirata para obtener acceso al servidor "internet key sharing" (IKS).

Acusaciones, cargos y penalidades

Acusaciones

Título 17, Código de los Estados Unidos, 1201(a)(A) and (a)(2)

Tráfico de tecnología diseñada para eludir los sistemas de protección del derecho de autor. Según en el dictamen United States of América Vs Alnardo Vázquez, Awildo Jiménez, And Higinio Lamboy (2018) comenzó en un momento desconocido, y continuando hasta julio o alrededor de 2016, en el Distrito de Puerto Rico y en otros lugares, los acusados Alnardo Vázquez, Awildo Jiménez y Higinio Lamboy transforma la ventaja financiera en privada, en una tecnología, producto, servicio y dispositivo, específicamente software, sabiendo que la tecnología, el producto, el servicio y el dispositivo fueron diseñados y producidos principalmente con el propósito de eludir una medida tecnológica que controla eficazmente el acceso a una obra protegida por derechos de autor en virtud del Título 17 del Código de los Estados Unidos, a saber, un software privativo diseñado para funcionar y funcionar en un receptor de "Dish Networks".

Intencionalmente y con fines de tráfico de juegos financieros privados en una tecnología, producto, servicio y dispositivo que fue diseñado y producido principalmente con el propósito de eludir una medida tecnológica que controlaba eficazmente el acceso a una obra protegida en virtud del Título 17 del Código de los Estados Unidos. Para que sea intencional y a efectos de ganancias financieras privadas, infrinja un derecho de autor reproduciendo y distribuyendo, incluso por medios electrónicos, al menos diez copias de una o más obras protegidas por derecho

de autor, con un valor total al por menor superior a 2.500 dólares, durante un período de 180 días.

Además, fabricar, ensamblar, modificar, importar, exportar, vender y distribuir cualquier dispositivo y equipo electrónico, mecánico y de otro tipo, sabiendo y teniendo motivos para saber que el dispositivo y el equipo eran principalmente de ayuda en el descifrado no autorizado de Satélite. Programación cable y servicios de satélite directos a domicilio.

Título 18, Código de los Estados Unidos, Sección 371 y Sección 2

Por la conspiración fue comenzando en un momento desconocido y continuando en o alrededor de julio de 2016, en el Distrito de Puerto Rico, y en otros lugares, acusados Alnardo Vázquez, Awildo Jiménez y Higinio Lamboy a sabiendas estuvo de acuerdo, combinar, y conspirar para cometer delitos contra los Estados Unidos, es decir para eludir deliberadamente y a los efectos del beneficio financiero privado una medida tecnológica que controle eficazmente el acceso a una obra protegida en virtud del Título 17 del Código de los Estados Unidos.

El objetivo de la conspiración era que los Acusados y otros se enriquecieran proporcionando servicios de televisión por satélite pirateados a miles de clientes con fines privados de lucro. Los demandados, junto con otros, capturaron y obtuvieron las llaves de las tarjetas inteligentes asociadas con cuentas “DISH” que controlaban. Fue parte adicional de la conspiración que los Demandados, junto con otros, pusieran estas llaves asociadas con canales particulares de programación “DISH” en un servidor “Internet Key Sharing” (IKS) bajo su control. Más de la conspiración que los Demandados, junto con otros, proporcionaron receptores de satélite a los usuarios finales. Estos receptores fueron programados con un software especial que permitió a los receptores hacer una conexión directa a servidor a través de Internet al

servidor “Internet Key Sharing” (IKS) bajo el control de los Demandados con el fin de acceder a contraseña particulares para lograr Descifrado. Los receptores no autorizados de los usuarios finales utilizaron las contraseñas para descifrar las señales satelitales de “DISH” para obtener la programación de “DISH” sin autorización.

Los demandados junto con otros conspiraron a recolectaran pagos de suscripción sin la autorización de “DISH” y para su propio beneficio financiero privado. Además, parte de la conspiración fue que los demandados, junto con otros, instalaran y repararan estos receptores, así como los equipos conexos utilizados por los usuarios finales para obtener un servicio de televisión por satélite pirateado. Para llevar a cabo su objeto ilegal los demandados y otros solían ser cometerlo en los siguientes actos de vándalos en el Distrito de Puerto Rico y en otros lugares:

- el 11 de noviembre de 2014 o aproximadamente los demandados Vázquez y Jiménez hacían una copia de una factura por servicios de internet en un lugar en salinas, puerto rico.
- el 11 de enero de 2015, el demandado Vázquez y el demandado Jiménez transmitieron mensajes en línea entre sí relativos a la compra de servidores para operar la operación de piratería de internet key sharing (IKS) en salinas.
- el 15 de enero de 2015, el demandado Vázquez y el demandado Jiménez transmitieron mensajes en línea entre sí sobre el funcionamiento de los servidores de internet key sharing (IKS) en salinas, puerto rico y una interrupción del servicio local de puerto rico.
    - el 22 de enero de 2015, el demandado Vázquez y el demandado Jiménez transmitió mensajes en línea entre sí donde discuten las cuentas de súper

distribuidor y la eliminación de los usuarios que están re-compartiendo el servicio pirateado.

- El 30 de enero de 2015, el demandado Vázquez y el demandado Jiménez transmitieron mensajes en línea entre sí sobre problemas técnicos y otras cuestiones relacionadas con el funcionamiento de la piratería de (IKS).

- El 7 de febrero de 2015 o aproximadamente, el demandado Vázquez y el demandado Jiménez transmitieron mensajes en línea entre sí en puerto rico con respecto a la compra de enrutadores y otros equipos para utilizar para la piratería de internet key sharing (IKS).

- El 3 de noviembre de 2015, los demandados Jiménez y Vázquez poseían una gran cantidad de equipo relacionado con el servicio de televisión pirata dish satélite en un lugar en Salinas, Puerto Rico.

- El 5 de noviembre de 2015, el demandado Jiménez poseía una gran cantidad de equipos relacionados con el servicio de televisión por satélite de "dish" pirateado en su residencia en Salinas, Puerto Rico.

- El 17 de diciembre de 2015, el demandado Vázquez y el demandado Lamboy transmitieron mensajes en línea entre sí en puerto rico con respecto a la venta de equipos de piratería de (IKS).

- El 25 de enero de 2016, el demandado Vázquez y el demandado Lamboy se transmitieron mensajes en línea entre sí en puerto rico sobre el número de clientes y cuentas de internet key sharing (IKS) administrados por el demandado Vázquez.

- El 6 de julio de 2016, el demandado Lamboy poseía una gran cantidad de equipo relacionado con el servicio de televisión por satélite de (DISH) pirateado en su residencia en Mayagüez, Puerto Rico.

Definiciones de términos

- Derechos de autor- en inglés copyright ©, otorga al dueño varios derechos exclusivos para tener control la reproducción, importación y exportación de una obra de su autoría, por ejemplo, obra literaria, película, música, pintura entre otros, pero en el caso presentado el derecho es de software.
- Servidor- es un término que proviene del latín servitor y cuyo uso ha cambiado en los últimos años Los servidores suelen utilizarse para almacenar archivos digitales y proveer servicios como compartir información.
- Conspiración- de rigen en el latín conspiratĭo, el concepto de conspiración hace referencia al acto de conspirar, es decir, de aliarse contra un superior para arrebatarle el poder o contra un particular con el propósito de hacerle daño en bienes con el objetivo de llegar a un mismo objetivo.
- Card sharing- es un método por el cual receptores independientes (y externos) obtienen acceso simultáneo a una red de televisión de pago, usando una tarjeta de abonado de acceso condicional legítima.

- IKS- por sus siglas en inglés, internet key sharing en español es compartir llave a través de internet es el proceso de entregar mediante vía internet las llaves para abrir canales encriptados en Nagra 3.
- Piratería- es una actividad que desarrollan los piratas ya era un delincuente que abordaba embarcaciones en altamar para quedarse con sus riquezas en los siglos pasado. Hoy en día se utiliza ese término de piratería cuando ocurre copias o hurto de información para obtener un beneficio.

Sección 2: Revisión de literatura

Introducción

Según el artículo escrito por Zamorano (2019) en los años 90 era raro ver antenas parabólicas en una casa, sin embargo, hoy en día han aumentado el uso de ellas y no todas pagan a un proveedor de servicio. Es más frecuentemente las tiendas de electrónica ofrecen decodificadores para televisión satelital, las que usualmente se cree que están en una nebulosa jurídica ya que las señales van por el aire en vez de un cable coaxial. Por esto que no es así, ya que al igual que en Internet, la legalidad está en el uso que uno le da a una herramienta. Por ejemplo, la gran polémica del protocolo de Torrent uno lo puede usar tanto para descargar películas clásicas sin copyright de 1920 como para descargar contenido ilegal a través de The Pirate Bay o página web publiquen los en lace.

En el caso de la televisión satelital hay contenido protegido y contenido libre. Al decodificar un contenido protegido es ilegal, infringiendo el derecho de autor de las cadenas de televisión que transmiten por esas señales, mientras que hay canales que por diversos motivos son de acceso libre y no hay ninguna irregularidad en acceder a su contenido. Por ejemplo, los decodificadores piratas en ciertos lugares de importación de artículos electrónicos para ver los carteles exclusivos que ofrecen cientos de canales de televisión satelital por un precio fijo. Para saber si es ilegal, la gran mayoría de los canales de televisión por pago como “HBO” siempre su señal satelital es encriptada. Si te ofrecen ese canal junto al “Fox Sports Premium” o el “Playboy Channel”, por ejemplo, en síntesis, el servicio es ilegal.

El riesgo con este tipo de servicios aparte que es ilegal no te garantiza que funcionarán permanentemente, por ejemplo, que el sistema de encriptación de los canales fabricados por la

empresa ABC actualiza a su una nueva versión o interrupción de los servidores. Eso significa que mucha gente que compró este tipo de servicio o aparatos no tienen idea de cómo actualizarlos.

De todas formas cabe aclarar que el sistema ABC sí está crackeado, pero ahí la cosa se complica, pues el método tradicional de decodificación ya no funciona y se debe realizar a través de Internet para los receptores con esta capacidad, o con un receptor doble que decodifica la señal de un segundo satélite, lo que implica instalar dos antenas: Una para recoger la señal del satélite que tiene los canales de televisión encriptados, usualmente el Amazonas, y otra apuntando al satélite Telstar 12 que ayuda a decodificar la señal. Usualmente con lleva a una inversión mayor sin tener cuando durara esa tecnología implementada.

Figura 1 Pieza que se utiliza para eludir la señal satelital.

Como se ve en la foto, los aparatos para decodificar la señal de un segundo satélite son los ‘dongle’. Y en este punto de inflexión es cuando la complejidad de la piratería de una señal satelital se complica a tal grado que nos preguntamos si no es mejor dedicarse directamente a aprender sobre las opciones legales.

La televisión satelital gratis y legal existe conocida FTA (por las siglas en inglés de Free to Air) y son emisiones con carácter de libre acceso. Al principio la televisión satelital consistía en señales abiertas, pero luego las empresas productoras de material audiovisual iniciaron a proteger los derechos de autor por lo que comenzaron a codificar sus señales. Sin embargo, hay canales por su carácter estatal, cultural, por evitar los costos operativos de su codificación, porque eran de proyección política o religiosa, decidieron mantener sus señales libres.

Hay mucha confusión con el término FTA porque los distribuidores de decodificadores piratas usan el término para darle legitimidad a sus productos, pero numerosas autoridades gubernamentales han afirmado que no hay nada ilegal en recibir señales libres, pero capturar señales satelitales de televisión protegidas por derecho de autor está penado por la ley.

La siguiente foto corresponde a las antenas parabólicas que recogen la señal de varios satélites como AMC 6, Hispasat o Amazonas. Como se ven, son antenas de proveedores de televisión de pago pues es común encontrarlas por un precio muy económico en el mercado.

Figura 2 Posición de las antenas a distintos satélites.

Los receptores destinados al FTA no son nada barato, por lo que las comunidades incluso han desarrollado métodos para adaptar los decodificadores de la televisión de pago para recibir algunas señales libres que usualmente se encuentran en los satélites AMC6, Hispasat, Telstar 12 y 14, y Satmex 5 y 6. Para encontrar el listado de canales de cada satélite uno puede recurrir al sitio Lyngsat.com.

Este método sería el ideal para llevar la televisión a lugares remotos y comunidades rurales a muy bajo costo, aunque lamentablemente hay muchos canales de televisión abierta que

encriptan sus señales satelitales. Si realmente quisieran mejorar su cobertura ésta sería la opción más simple y rápida.

Fraudes involucrados

- Violaciones relativas a la elusión de las medidas tecnológicas de derecho de autor.
- Conspiración para cometer un delito a una organización.
- Accesoria para cometer y mantener operando el servicio pirata

Organización para vender servicios piratas

Los individuos se reúnen para organizarse para ejecutar sus funciones para ejecutar el servicio pirata. Aunque ya que estén violando el derecho de autor con el fin de beneficiarse con la intención de general un beneficio.

Leyes aplicables

- **18 U.S.C. *§371*-** Conspiración para cometer un delito o para defraudar a Estados Unidos

Si dos o más personas conspirar para cometer cualquier ofensa contra los Estados Unidos, o para defraudar a los Estados Unidos, o cualquier agencia de esta de cualquier manera o para cualquier propósito, y una o más de tales personas hacen cualquier acto para hacer efecto el objeto de la conspiración, cada uno de ellos será multado bajo este título o encarcelado no más de cinco años, o ambos. Sin embargo, la ofensa cuya comisión es objeto de la conspiración, es sólo un delito menor, el castigo por tal conspiración no excederá la pena máxima que se haya previsto para tal delito menor. (25 de junio de 1948, CH. 645, 62 stat. 701; Pub. L. 103 – 322, título XXXIII, § 330016 (1) (L), 13 de septiembre de 1994, 108 stat. 2147.)

18 U.S.C. ***§ 2***- La primera disposición que se encuentra en el título 18 del código de los Estados Unidos se refiere a los accesorios a la delincuencia. El título 18, código de los Estados Unidos § 2 ahora proporciona:

A. Quien cometa un delito contra los Estados Unidos o filantropía, coconspirador, consejos, órdenes, induce o adquiere su comisión, es castigado como un director.
B. Quien intencionalmente cause que se haga un acto que si es ejecutado directamente por él u otro sería una ofensa contra los Estados Unidos, es castigado como un director.

17 U.S. Code § 1201-) Violaciones relativas a la elusión de las medidas tecnológicas.

(A) Ninguna persona debe eludir una medida tecnológica que controle efectivamente el acceso a una obra protegida bajo este título. La prohibición contenida en la oración anterior entrará en vigor al final del período de 2 años que comienza en la fecha de la promulgación de este capítulo.

- (B) La prohibición contenida en el subpárrafo (A) no se aplicará a las personas que son usuarios de un trabajo protegido por derechos de autor que se encuentra en una clase particular de trabajos, si dichas personas son, o es probable que estén en el período de 3 años subsiguiente, afectados adversamente en virtud de dicha prohibición en su capacidad para hacer usos no infractores de esa clase particular de obras bajo este título, según lo determinado en el subpárrafo (C).

  (C) Durante el período de 2 años descrito en el subpárrafo (A), y durante cada período de 3 años subsiguiente, el Bibliotecario del Congreso, por recomendación del Registro de Derechos de Autor, quien consultará con el Subsecretario de Comunicaciones e Información. del Departamento de Comercio e informar y

comentar sobre sus puntos de vista al hacer tal recomendación, deberá tomar una decisión en un procedimiento de reglamentación a los fines del subpárrafo (B) de si las personas que son usuarios de una obra con derechos de autor son, o es probable que lo hagan. estar en el siguiente período de 3 años, afectado adversamente por la prohibición en virtud del subpárrafo (A) en su capacidad para hacer usos no infractores bajo este título de una clase particular de obras con derechos de autor. Al llevar a cabo dicha reglamentación, el bibliotecario examinará:

(i) la disponibilidad para el uso de obras con derechos de autor;

(ii) la disponibilidad para el uso de obras para fines de archivo, conservación y educación sin fines de lucro;

(iii) el impacto que la prohibición sobre la elusión de las medidas tecnológicas aplicadas a las obras protegidas por derechos de autor tiene sobre críticas, comentarios, noticias, docencia, becas o investigación;

(iv) el efecto de la elusión de medidas tecnológicas en el mercado o el valor de las obras con derechos de autor; y

(v) otros factores que el bibliotecario considere apropiados.

(D) El Bibliotecario publicará cualquier clase de trabajos con derechos de autor para los cuales el Bibliotecario haya determinado, de conformidad con la reglamentación realizada en virtud del subpárrafo (C), que los usos no infractores por parte de personas que son usuarios de un trabajo con derechos de autor son, o es probable que sean, afectado adversamente, y la prohibición contenida en el subpárrafo (A) no se aplicará a dichos usuarios con respecto a dicha clase de trabajos durante el período de 3 años subsiguiente.

(E) Ni la excepción bajo el subpárrafo (B) de la aplicabilidad de la prohibición contenida en el subpárrafo (A), ni ninguna determinación hecha en una reglamentación conducida bajo el subpárrafo (C), puede ser usada como una defensa en cualquier acción para hacer cumplir cualquier disposición de este título distinto de este párrafo.

(2) Ninguna persona fabricará, importará, ofrecerá al público, proporcionará ni traficará de ninguna otra forma ninguna tecnología, producto, servicio, dispositivo, componente o parte de este que:

(A) está diseñado o producido principalmente con el propósito de eludir una medida tecnológica que controla efectivamente el acceso a una obra protegida bajo este título;

(B) solo tiene un propósito o uso comercialmente significativo que no sea eludir una medida tecnológica que controle efectivamente el acceso a una obra protegida bajo este título; o

(C) es comercializado por esa persona u otra persona que actúa en concierto con esa persona con el conocimiento de esa persona para utilizarla en eludir una medida tecnológica que controle efectivamente el acceso a una obra protegida bajo este título.

(3) Según se utiliza en esta subsección:

(A) "burlar una medida tecnológica" significa descifrar un trabajo codificado, descifrar un trabajo encriptado, o de otra manera evitar, omitir, eliminar, desactivar o menoscabar una medida tecnológica, sin la autoridad del propietario de los derechos de autor; y

(B) una medida tecnológica "controla efectivamente el acceso a un trabajo" si la medida, en el curso ordinario de su operación, requiere la aplicación de información,

o un proceso o un tratamiento, con la autoridad del propietario del derecho de autor, para obtener acceso al trabajo.

(b) Violaciones adicionales.

(1) Ninguna persona fabricará, importará, ofrecerá al público, proporcionará ni traficará de ninguna otra forma ninguna tecnología, producto, servicio, dispositivo, componente o parte de este que:

(A) está diseñado o producido principalmente con el propósito de eludir la protección otorgada por una medida tecnológica que protege efectivamente el derecho de un titular de derechos de autor bajo este título en una obra o una parte de ella;

(B) solo tiene un propósito o uso comercialmente significativo que no sea para eludir la protección otorgada por una medida tecnológica que proteja efectivamente el derecho de un titular de derechos de autor bajo este título en una obra o una parte de este; o

(C) es comercializado por esa persona u otra persona que actúa en concierto con esa persona con el conocimiento de esa persona para utilizarla en eludir la protección otorgada por una medida tecnológica que protege efectivamente el derecho de un propietario de derechos de autor con respecto a un trabajo cuando una copia idéntica de ese trabajo no está razonablemente disponible en otra forma.

(3) Una biblioteca sin fines de lucro, archivos o instituciones educativas que, deliberadamente, con el propósito de obtener una ventaja comercial o ganancia financiera, infringe el párrafo (1):

(A) estará sujeto, por la primera ofensa, a los recursos civiles bajo la sección 1203; y

(B), por infracciones reiteradas o posteriores, además de los recursos civiles en virtud del artículo 1203, perderá la exención prevista en el párrafo (1).

(4) Esta subsección no se puede usar como defensa de una reclamación bajo la subsección (a) (2) o (b), ni esta subsección permite que una biblioteca, archivo o institución educativa sin fines de lucro fabrique, importe, ofrezca a la pública, proporciona, o de otro modo, el tráfico en cualquier tecnología, producto, servicio, componente o parte de este, que elude una medida tecnológica.

(5) Para que una biblioteca o archivos califiquen para la exención bajo esta subsección, las colecciones de esa biblioteca o archivos serán:

(A) abierto al público; o

(B) disponible no solo para los investigadores afiliados a la biblioteca o los archivos o para la institución de la que forma parte, sino también para otras personas que realizan investigaciones en un campo especializado.

(e) Aplicación de la ley, inteligencia y otras actividades gubernamentales.

Esta sección no prohíbe ninguna actividad de investigación, protección, seguridad de la información o inteligencia legalmente autorizada de un oficial, agente o empleado de los Estados Unidos, un Estado o una subdivisión política de un Estado o una persona que actúe de conformidad con un contrato con los Estados Unidos, un Estado o una subdivisión política de un Estado. Para los fines de esta subsección, el término "seguridad de la información" significa las actividades realizadas para identificar y abordar las vulnerabilidades de una computadora, sistema informático o red de computadoras del gobierno.

(f) Ingeniería inversa.

(1) A pesar de las disposiciones de la subsección (a) (1) (A), una persona que haya obtenido legalmente el derecho de usar una copia de un programa de computadora puede eludir una medida tecnológica que controle efectivamente el acceso a una parte particular de ese programa. con el único propósito de identificar y analizar aquellos elementos del programa que son necesarios para lograr la interoperabilidad de un programa de computadora creado de manera independiente con otros programas, y que no han sido previamente disponibles para la persona involucrada en la elusión, en la medida en que tales Los actos de identificación y análisis no constituyen una infracción bajo este título.

(2) No obstante las disposiciones de los incisos (a) (2) y (b), una persona puede desarrollar y emplear medios tecnológicos para eludir una medida tecnológica, o para eludir la protección otorgada por una medida tecnológica, a fin de permitir la identificación y análisis bajo el párrafo (1), o con el propósito de permitir la interoperabilidad de un programa de computadora creado independientemente con otros programas, si tales medios son necesarios para lograr dicha interoperabilidad, en la medida en que hacerlo no constituya una infracción bajo este título.

(3) La información adquirida a través de los actos permitidos en virtud del párrafo (1), y los medios permitidos en virtud del párrafo (2), pueden ponerse a disposición de otros si la persona mencionada en el párrafo (1) o (2), según sea el caso puede ser, proporciona dicha información o medios con el único fin de permitir la interoperabilidad de un programa informático creado de forma independiente con otros programas, y en la medida en que hacerlo no constituya una infracción bajo este título ni viole las leyes aplicables que no sean esta sección.

(4) Para los fines de esta subsección, el término "interoperabilidad" significa la capacidad de los programas informáticos para intercambiar información, y de dichos programas usar mutuamente la información que se ha intercambiado.

(g) Investigación de encriptación.

(1) Definiciones. — Para los propósitos de esta subsección—

(A) el término "investigación de encriptación" significa actividades necesarias para identificar y analizar fallas y vulnerabilidades de las tecnologías de encriptación aplicadas a trabajos con derechos de autor, si estas actividades se llevan a cabo para mejorar el estado del conocimiento en el campo de la tecnología de encriptación o para ayudar en el desarrollo. de productos encriptados; y

(B) el término "tecnología de encriptación" significa el cifrado y descifrado de información utilizando fórmulas matemáticas o algoritmos.

(2) Actos permisibles de investigación de encriptación. A pesar de las disposiciones de la subsección (a) (1) (A), no es una violación de esa subsección para una persona eludir una medida tecnológica aplicada a una copia, un fonograma, un rendimiento., o visualización de un trabajo publicado en el curso de un acto de investigación de cifrado de buena fe si:

(A) la persona obtuvo legalmente la copia encriptada, el registro telefónico, la ejecución o la visualización de la obra publicada;

(B) tal acto es necesario para llevar a cabo dicha investigación de cifrado;

(C) la persona hizo un esfuerzo de buena fe para obtener la autorización antes de la elusión; y

(D) tal acto no constituye una infracción bajo este título o una violación de la ley aplicable que no sea esta sección, incluida la sección 1030 del título 18 y las disposiciones del título 18 enmendadas por la Ley de abuso y fraude informático de 1986.

(3) Factores para determinar la exención. Al determinar si una persona califica para la exención en virtud del párrafo (2), los factores que deben considerarse deben incluir:

(A) si la información derivada de la investigación de cifrado se difundió y, de ser así, si se difundió de una manera razonablemente calculada para avanzar en el estado del conocimiento o desarrollo de la tecnología de cifrado, en comparación con si se difundió de una manera que facilite la infracción bajo este título o una violación de la ley aplicable que no sea esta sección, incluida una violación de la privacidad o el incumplimiento de la seguridad;

(B) si la persona está involucrada en un curso de estudio legítimo, está empleada o cuenta con la capacitación o experiencia adecuadas en el campo de la tecnología de encriptación; y

(C) si la persona proporciona el propietario del derecho de autor del trabajo al que se aplica la medida tecnológica con notificación de los hallazgos y la documentación de la investigación, y el momento en que se proporciona dicha notificación.

(4) Uso de medios tecnológicos para actividades de investigación. A pesar de las disposiciones de la subsección (a) (2), no es una violación de esa subsección para una persona:

(A) desarrollar y emplear medios tecnológicos para eludir una medida tecnológica con el único propósito de que esa persona realice los actos de investigación de cifrado de buena fe descritos en el párrafo (2); y

(B) proporcione los medios tecnológicos a otra persona con la que esté trabajando en colaboración con el fin de realizar las investigaciones de cifrado de buena fe descritas en el párrafo (2) o con el fin de que esa otra persona verifique sus actos investigación de encriptación de buena fe descrita en el párrafo (2).

(5) Informar a. — A más tardar un año después de la fecha de promulgación de este capítulo, el Registro de Derechos de Autor y el Subsecretario de Comunicaciones e Información del Departamento de Comercio informarán conjuntamente al Congreso sobre el efecto de esta subsección ha tenido en

(A) investigación de encriptación y desarrollo de tecnología de encriptación;

(B) la adecuación y eficacia de las medidas tecnológicas diseñadas para proteger las obras protegidas por derechos de autor; y

(C) la protección de los propietarios de derechos de autor contra el acceso no autorizado a sus obras encriptadas con derechos de autor.

El informe incluirá recomendaciones legislativas, si las hay.

(h) Excepciones relacionadas con menores de edad. Al aplicar la subsección (a) a un componente o parte, el tribunal puede considerar la necesidad de su incorporación prevista y real en una tecnología, producto, servicio o dispositivo, que:

(1) no viola las disposiciones de este título; y

(2) tiene el único propósito de impedir el acceso de menores a material en Internet.

(i) Protección de la información de identificación personal.

(1) Se permite la elusión. No obstante, las disposiciones de la subsección (a) (1) (A), no es una violación de esa subsección para una persona eludir una medida tecnológica que controle efectivamente el acceso a una obra protegida bajo este título. Si-

(A) la medida tecnológica, o el trabajo que protege, tiene la capacidad de recopilar o difundir información de identificación personal que refleje las actividades en línea de una persona física que busca obtener acceso al trabajo protegido;

(B) en el curso normal de su operación, la medida tecnológica o el trabajo que protege recopila o difunde información de identificación personal sobre la persona que busca obtener acceso al trabajo protegido, sin proporcionar un aviso visible de dicha recopilación o difusión a esa persona, y sin proporcionar a dicha persona la capacidad de prevenir o restringir dicha recopilación o difusión;

(C) el acto de elusión tiene el único efecto de identificar y deshabilitar la capacidad descrita en el subpárrafo (A), y no tiene ningún otro efecto sobre la capacidad de cualquier persona para acceder a cualquier trabajo; y

(D) el acto de elusión se lleva a cabo únicamente con el propósito de evitar la recopilación o diseminación de información de identificación personal sobre una persona física que busca obtener acceso al trabajo protegido y no viola ninguna otra ley.

(2) Inaplicabilidad a ciertas medidas tecnológicas.

Esta subsección no se aplica a una medida tecnológica, o un trabajo que protege, que no recopila ni difunde información de identificación personal y que se revela a un usuario como que no tiene o no utiliza dicha capacidad.

(j) Pruebas de seguridad.

(1) Definición.

Para los fines de esta subsección, el término "pruebas de seguridad" significa acceder a una computadora, sistema informático o red de computadoras, únicamente con el propósito de realizar pruebas, investigaciones o correcciones de buena fe, una falla o vulnerabilidad de seguridad, con la autorización del propietario. u operador de dicha computadora, sistema informático o red informática.

(2) Actos permisibles (2) Actos permisibles de pruebas de seguridad.

No obstante, las disposiciones de la subsección (a) (1) (A), no es una violación de esa subsección para que una persona participe en un acto de prueba de seguridad, si tal acto no constituye una infracción bajo este título o una violación de otra ley que no sea esta sección, incluida la sección 1030 del título 18 y las disposiciones del título 18 enmendadas por la Ley de abuso y fraude informático de 1986.

(3) Factores para determinar la exención. Al determinar si una persona califica para la exención en virtud del párrafo (2), los factores que deben considerarse deben incluir:

(A) si la información derivada de las pruebas de seguridad se utilizó únicamente para promover la seguridad del propietario u operador de dicha computadora, sistema o red informáticos, o se compartió directamente con el desarrollador de dicha computadora, sistema o red informáticos; y

(B) si la información derivada de las pruebas de seguridad se usó o mantuvo de una manera que no facilita la infracción bajo este título o una violación de la ley aplicable que no sea esta sección, incluida una violación de la privacidad o la violación de la seguridad.

(4) Uso de medios tecnológicos para pruebas de seguridad.

No obstante, las disposiciones de la subsección (a) (2), no es una violación de esa subsección para que una persona desarrolle, produzca, distribuya o emplee medios tecnológicos con el único propósito de realizar los actos de pruebas de seguridad descritos en la subsección (2), [1] siempre que dichos medios tecnológicos no violen la sección [2] (a) (2).

(k) Ciertas medidas analógicas y ciertas tecnológicas. —

(1) Cierto análogo. —

(A) A partir de los 18 meses posteriores a la fecha de promulgación de este capítulo, ninguna persona fabricará, importará, ofrecerá al público, proporcionará ni realizará ningún otro tráfico en ningún:

(i) grabadora de videocasetes analógica en formato VHS, a menos que dicha grabadora cumpla con la tecnología de control de copia con control automático de ganancia;

(ii) videocámara de videocasetes analógica en formato de 8 mm a menos que dicha videocámara se ajuste a la tecnología de control automático de ganancia;

(iii) Grabadora de videocasetes analógica de formato Beta, a menos que dicha grabadora sea compatible con la tecnología de control de copia de control de ganancia automática, excepto que este requisito no se aplicará hasta que haya 1,000 grabadoras de videocasetes analógicas de formato Beta vendidas en los Estados Unidos en un año calendario. después de la fecha de promulgación de este capítulo;

(iv) grabadora de videocasetes analógica de formato 8 mm que no es una videocámara de videocasetes analógica, a menos que dicha grabadora sea compatible con la tecnología de control de copia de control de ganancia automática, excepto que

este requisito no se aplicará hasta que haya 20,000 grabadoras vendidas en los Estados Unidos en cualquier año calendario posterior a la fecha de promulgación de este capítulo; o

(v) grabadora de videocasetes analógica que graba utilizando una entrada de video de formato NTSC y que no está cubierta de otro modo en las cláusulas (i) a (iv), a menos que dicho dispositivo cumpla con la tecnología de control automático de copia de control de ganancia.

(B) A partir de la fecha de promulgación de este capítulo, ninguna persona fabricará, importará, ofrecerá al público, proporcionará ni traficará de ningún otro modo:

(i) cualquier grabadora de videocasetes analógica en formato VHS o cualquier videograbadora analógica de formato 8 mm si el diseño del modelo de dicha grabadora se ha modificado después de dicha fecha de promulgación, de modo que un modelo de grabadora que anteriormente se ajustara a la copia de control de ganancia automática la tecnología de control ya no se ajusta a dicha tecnología; o

(ii) cualquier grabadora de videocasetes analógica en formato VHS, o cualquier grabadora de videocasetes analógica de formato 8 mm que no sea una videocámara de videocasetes analógica de 8 mm, si el diseño del modelo de dicha grabadora se ha modificado después de dicha fecha de promulgación para que un modelo del grabador que anteriormente se ajustaba a la tecnología de control de copia de la línea de color de cuatro líneas ya no se ajusta a dicha tecnología.

Los fabricantes que no hayan fabricado o vendido previamente una grabadora de videocasetes analógica de formato VHS, o una grabadora de videocasetes analógica de formato de 8 mm, deberán cumplir con la tecnología de control de copia de rayas

de color de cuatro líneas en el modelo inicial de cualquier grabadora fabricada después de la fecha de la promulgación de este capítulo y, posteriormente, continuar de conformidad con la tecnología de control de copia de rayas de color de cuatro líneas. Para los fines de este subpárrafo, una grabadora de videocasetes analógica "se ajusta a" la tecnología de control de copia de la franja de color de cuatro líneas si registra una señal que, cuando se reproduce por la función de reproducción de esa grabadora en el modo de visualización normal, se exhibe en un dispositivo de pantalla de referencia, una pantalla que contiene líneas visibles que distraen a través de partes de la imagen visible.

(2) Ciertas restricciones de codificación. Ninguna persona aplicará la tecnología de control de copia de control de ganancia automática o la tecnología de control de copia de banda de color para evitar o limitar la copia al consumidor, excepto dicha copia.

(A) de una transmisión única, o grupo específico de transmisiones, de eventos en vivo o de obras audiovisuales para las cuales un miembro de la

Casos relacionados

El primer caso Dish Network L.L.C. v. Singh No. 5:16-cv-00539-JSM-PRL sucedido el 24 de agosto de 2016. Según el dictamen (UNITED STATES DISTRICT COURT MIDDLE DISTRICT OF FLORIDA, 2016) los demandantes demandaron a Profulla Singh, por violaciones de 17 estados unidos. Sección 1201 (a) (1) (count i), 47 u.s.c. Sección 605 (a) (count ii), y 18 u.s.c. Las secciones 2511 (1) (a) y 2520 (count iii), todas relacionadas con la supuesta piratería del servicio de televisión satelital por parte del demandado. Los demandantes solicitaron daños y una orden judicial para prevenir la piratería continuada por parte de Profulla Singh. El 19 de octubre de 2016, el demandado presentó una moción para desestimar la demanda. El tribunal denegó la moción de desestimación y otorgó 14 días para que el demandado respondiera. Sin embargo, el acusado no respondió. Los demandantes se mudaron por incumplimiento de un secretario el 22 de noviembre de 2016, y el incumplimiento se ingresó al día siguiente. Luego, los demandantes presentaron la moción instantánea de fallo por defecto. Por los motivos que se detallan a continuación, los demandantes tienen derecho a un fallo de incumplimiento definitivo.

Los demandantes presentaron esta acción contra el demandado Profulla Singh (en adelante, "demandado") por eludir ilegalmente el sistema de seguridad de Dish Network y recibir programación de televisión satelital de Dish Network basada en derechos de autor, sin autorización y sin pago a Dish Network. El demandado logró esto en parte al suscribirse a un servicio de televisión pirata conocido como nfusion servidor pirata ("nfps"). El servicio de televisión pirata del nfps permitió al demandado descifrar ilegalmente la señal de satélite de Dish Network y ver la programación de televisión por satélite con derechos de autor sin la autorización de Dish Network.

En el segundo caso que se va a mostrar el caso de “Dish Network vs Donald Singh” NO. 1:14-cv-1581 no fue por distribución si no por el uso de servicio pirata. El demandado ha eludido el sistema de seguridad de “Dish Network” y recibió las transmisiones satelitales de “Dish Network” de programas de televisión con derechos de autor sin el pago de la tarifa de suscripción a “Dish Network” requerida. Según el dictamen (UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF OHIO EASTERN DIVISION, 2015) el demandado logró esto al suscribirse a “Internet Key Sharing” (IKS) “Rocket” por un año aproximadamente el 1 de enero de 2012 y al comprar una suscripción a “Fish TV” en abril de 2013. A través de IKS “Rocket y Fish TV”, el demandado obtuvo las contraseñada “Dish Network” que usó intencionalmente para interceptar el satélite de “Dish Network”. Señal y ver la programación de la red “DISH” sin autorización. El demandado violó la ECPA al obtener las contraseñas de “Dish Network” a través de los servicios IKS Rocket y Fish TV y usándolos para interceptar intencionalmente programación de la red DISH. IKS Rocket y Fish TV son servicios de intercambio de claves de Internet ("IKS") que proporcionar a los usuarios finales suscriptores las contraseñas necesarias para descifrar la programación de televisión de Dish Network sin autorización y sin pagar una tarifa de suscripción a “Dish Network”.

Por consiguiente, el acusado Donald Singh queda por el presente obligado a de: (1) eludir o ayudar a otros a burlar la seguridad de “DISH Network” sistema o de otro modo interceptar o ayudar a otros a interceptar la “Dish Network” señal de satélite y (2) pruebas, análisis, ingeniería inversa, manipulación o de lo contrario, extraer códigos, datos o información de los receptores de satélite de “DISH Network”, tarjetas inteligentes, flujo de datos satelitales o cualquier otra parte o componente de la “Dish Network” sistema de seguridad.

El Juez ha establecido la responsabilidad al demandado por las declaraciones presentadas por los demandantes en apoyo de la moción. También establecen que “DISH Network” ha gastado sumas significativas en medidas de seguridad para evitar la intercepción ilegal y que la piratería requiere actualizaciones constantes a un gran costo para evitar que los dispositivos no autorizados intercepten la programación de “DISH Network”. Además del costo de las nuevas medidas de seguridad para vencer las últimas técnicas de piratería y los ingresos de suscripción perdidos, la piratería y su impacto en la seguridad del sistema de “DISH Network” interfiriendo con la relación de este con sus proveedores de programación y clientes suscriptores. La conducta ilegal del acusado ha contribuido a estas lesiones, que son irreparables y no pueden ser calculadas o compensadas únicamente por daños monetarios. Además, el balance de las dificultades pesa claramente en favor de los demandantes: el acusado no puede quejarse de que se le haya prohibido violar una ley federal. Finalmente, el público no se ve perjudicado al proteger la propiedad intelectual y hacer cumplir la ley federal, y también puede beneficiarse si los costos para prevenir la piratería son reducidos.

Herramientas de investigación

FTK Imager

FTK Imager es herramientas usadas para hacer para recuperación de data en los dispositivos de almacenamiento o imágenes. Este programa otras de su utilidad es la capacidad de capturar una imagen de un dispositivo de almacenamiento en un archivo, para ser analizado. Dependiendo el caso que no son común un auditor para llevar una investigación más profunda utilizan esta herramienta para hacer una reconstrucción del dispositivo de almacenamiento del usuario en caso de que el mismo haya destruido la data. (Accessdata.com 2019).

IDEA Caseware

La herramienta de IDEA Caseware es una utilizada para analizar data y observar su contenido sin afectar su contenido. Al tener un poco de experiencia con anterioridad al utilizarlo se puede observar los datos específicos como fechas, número de serie, nombres o transacciones están duplicadas, ayudando obtener un análisis para detectar un posible fraude. Puedes organizar la data en forma descendente, ascendente o generando análisis grafico basado en estadísticas. (Caseware.com, 2019).

Sección 3: Simulación

Introducción

Los señores Vázquez y Jiménez eran los propietarios y operadores de una compañía que proporcionaba los servicios pirateados a los clientes que pagaron una tarifa mensual en efectivo u otros métodos que permitía obtener dinero para recibir contenido protegido por derechos de autor de los satélites Dish. Asimismo, identifica a Lamboy como su vendedor y reparador equipo que proporcionaba a sus clientes. También, describió un complejo esquema para robar el contenido con derechos de autor para obtener ganancias financieras mediante la intercepción de señales cifradas de Dish.

Esquema

La acusación formal alega que los acusados operaban utilizaron los foros de chat en línea y redes sociales en busca de cliente y promoviendo sobre su servicio satelital pirata. Además, ofrecían servicios técnicos para la instalación de nuevos receptores satelital o modificación de la caja descodificadora. Los acusados utilizaban diferentes métodos de pagos para facilitar sus acciones criminales y el mantenimiento necesarios equipos para la operación de la organización.

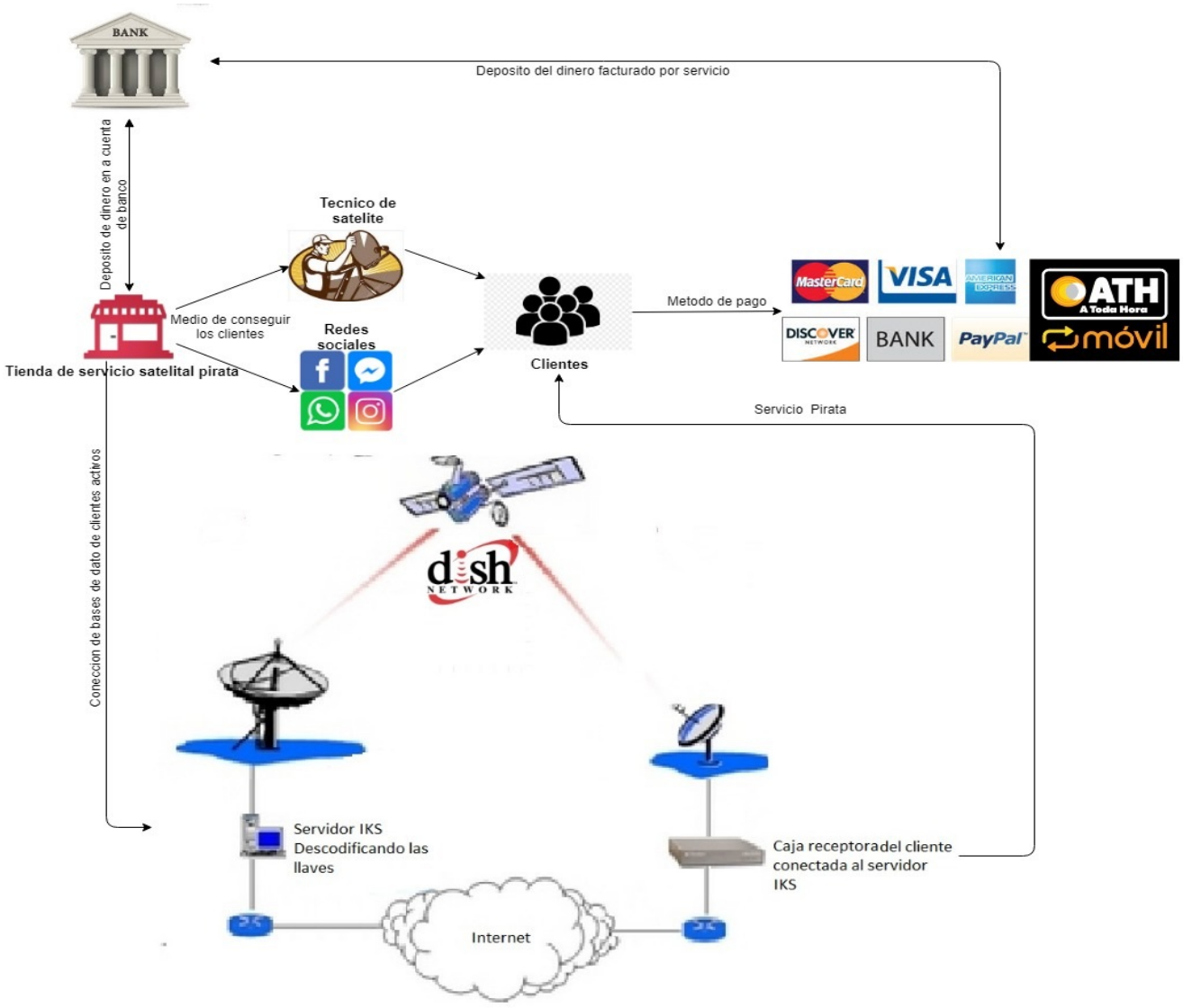


Figura 3: Diagrama de operación.

Sección 4: Informe del caso

Resumen Ejecutivo

La oficina de FBI división de crímenes cibernético se realizó el análisis de disco duro de una computadora que utilizaban de servidor IKS con información de las transacciones bancarias de los clientes de Alnardo Vázquez. Los datos fueron recuperados mediante una incautación de la computadora de Sr Vázquez. Además, se evaluó los clientes que aparecen en el libro de Excel que utilizaban para operar la organización.

En el análisis de los dispositivos se encontraron documentos en formato *Microsoft Excel* que contenían información bancaria de Awildo Jiménez y Higinio Lamboy con otros programas que se utilizó para la instalación de máquina virtual para instalar un servidor Linux para proveer servicio IKS. También se encontraron documentos en formato pdf que son facturas de servicio y compras de equipo para la operación de la organización del sr Vázquez. Durante en el proceso de analizar estas cuentas utilizando la herramienta de IDEA se descubrió la mayoría de las transacciones son ventas de servicios y donaciones.

En síntesis, del resultado de la examinación forense se a cargo de la investigación determinó que la data recolectada se utilizó para varios esquemas como: crimen organizado para cometer delito, preparación de equipo para eludir los derechos de autor y apropiación de bienes violando los derechos de autor.

Objetivo

FBI delegó la investigación de disco duro que contenían la información de las cuentas bancarias utilizadas por Alnardo Vázquez y la data recuperada de su computadora al investigador Wing Siang Ng Rosa. Esto con el fin de realizar un análisis forense a la cuenta de pertenecen al Sr Alnardo Vázquez con más los documentos encontrados en la imagen de la computadora de los

acusados. Una imagen de la computadora incautada a la acusada fue creada por los oficiales de FBI y entregada al examinador en un Disco Duro conteniendo estado cuentas de Banco Popular por la juez Aida M. Delgado Colon del distrito de Puerto Rico. En el proceso de la investigación se evaluó las cuentas de Alnardo Vázquez fueron utilizadas para desarrollar y mantener un esquema de crimen organizado.

Alcance del trabajo

El 28 de agosto de 2015, el fiscal José Capo Iriarte asistente fiscal de los Estados Unidos, división criminal le entregó al examinador forense Wing Siang Ng Rosa un disco duro de marca Toshiba de una capacidad de 500GB de memoria, identificado como *Evidence No. 2015-EVI-1* para crear una imagen de la computadora del acusado. El equipo fue tomado bajo custodia de agentes federales de FBI, luego de una orden de requisición firmada Aida M. Delgado Colon del distrito de Puerto Rico 26 de noviembre de 2015. El propósito de este trabajo es la captura integra y exacto de un disco duro real a un USB previamente mencionados para obtener cualquier información borrada para luego ser analizado críticamente.

Datos del caso

- Número del caso: 18-670(ADC)
- Examinador Forense: Wing Siang Ng Rosa
- Cliente: FBI de los Estados Unidos, ciberdelitos y explotación infantil
- Representante: José Capo Iriarte (Asistente del fiscal)

Descripción de los dispositivos utilizados

A continuación, se detallan los dispositivos utilizados durante el proceso investigativo:

- Una PC customizada, cuyos componentes principales son un procesador AMD FX ™-6100 Six-Core de 3.30GHz, RAM de 10GB, Disco Duro con capacidad de 3 TB,

sin suporte de Touch Screen y corrido un sistema operativo de Windows 10 de 64bits.

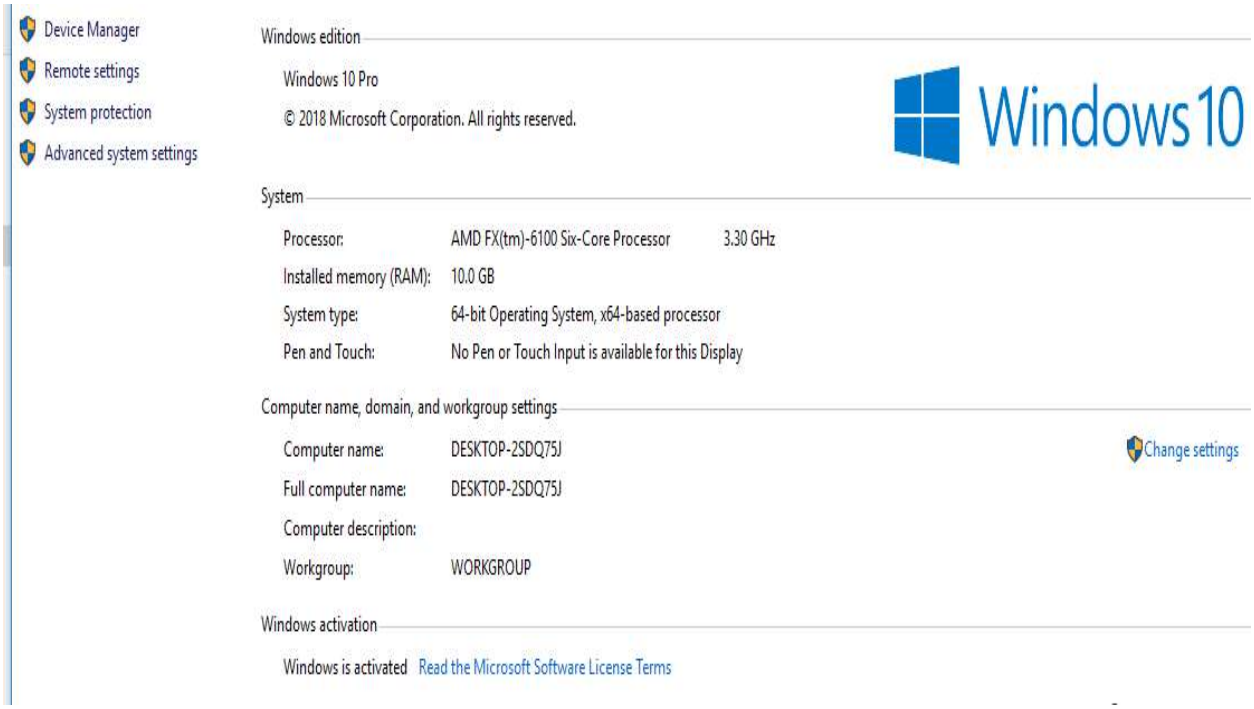


Figura 4: Especificaciones de la computadora de la investigación.

- Un Disco Duro marca Toshiba de capacidad de 500GB de memoria. Proveído al examinador Wing Siang Ng Rosa por el asistente del fiscal José Capo Iriarte. Dentro de este disco duro se contiene la información de los estados de cuenta del demandante y una máquina virtual.

Figura 5: Disco Duro entregado por el fiscal

- Este disco duro será utilizado para crear imágenes de la información proveída por el ayudante del fiscal José Capo Iriarte. Estas imágenes de la data luego serán examinadas mientras las versiones originales evitando la alteración de la evidencia.

Figura 6: UBS utilizado para hacer la imagen.

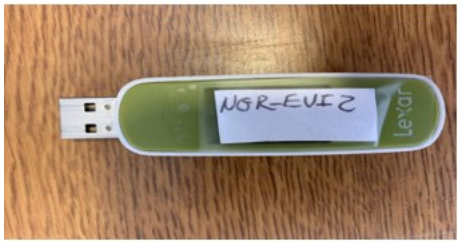
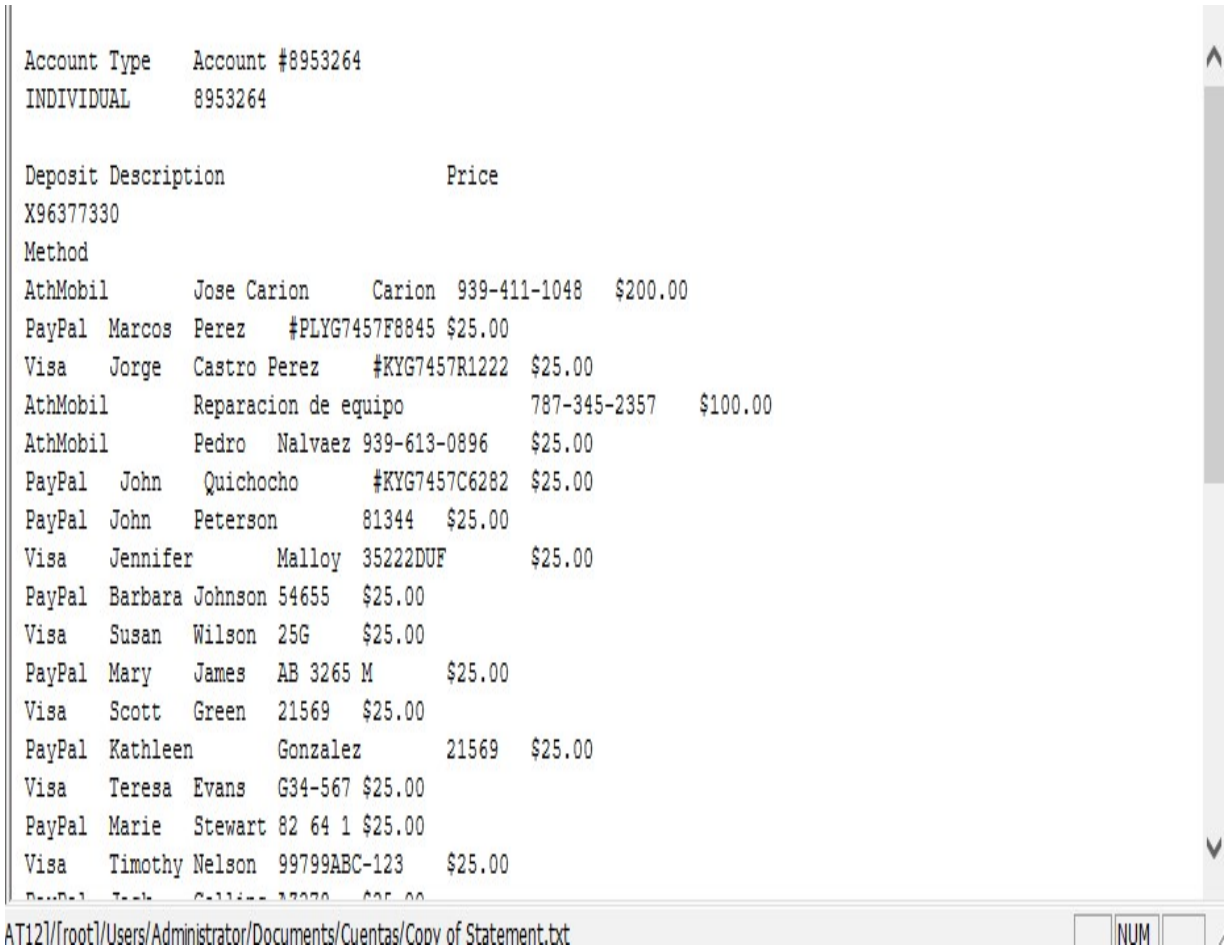


Figura 7: Segundo UBS utilizado para hacer la imagen.

Resumen de hallazgo

A continuación, se presentan los hallazgos identificados durante la investigación realizada al dispositivo entregado asistente fiscal del FBI de los Estados Unidos división criminal. En la examinación del disco duro identificado como *Evidence No. 2015-EVI-1* se encontraron 2 documentos guardados en formato Microsoft Excel y el otro en texto, representado en la figura 8. Estos documentos contienen la información bancaria de los depósitos de los clientes que han depositado para obtener el servicio pirata.



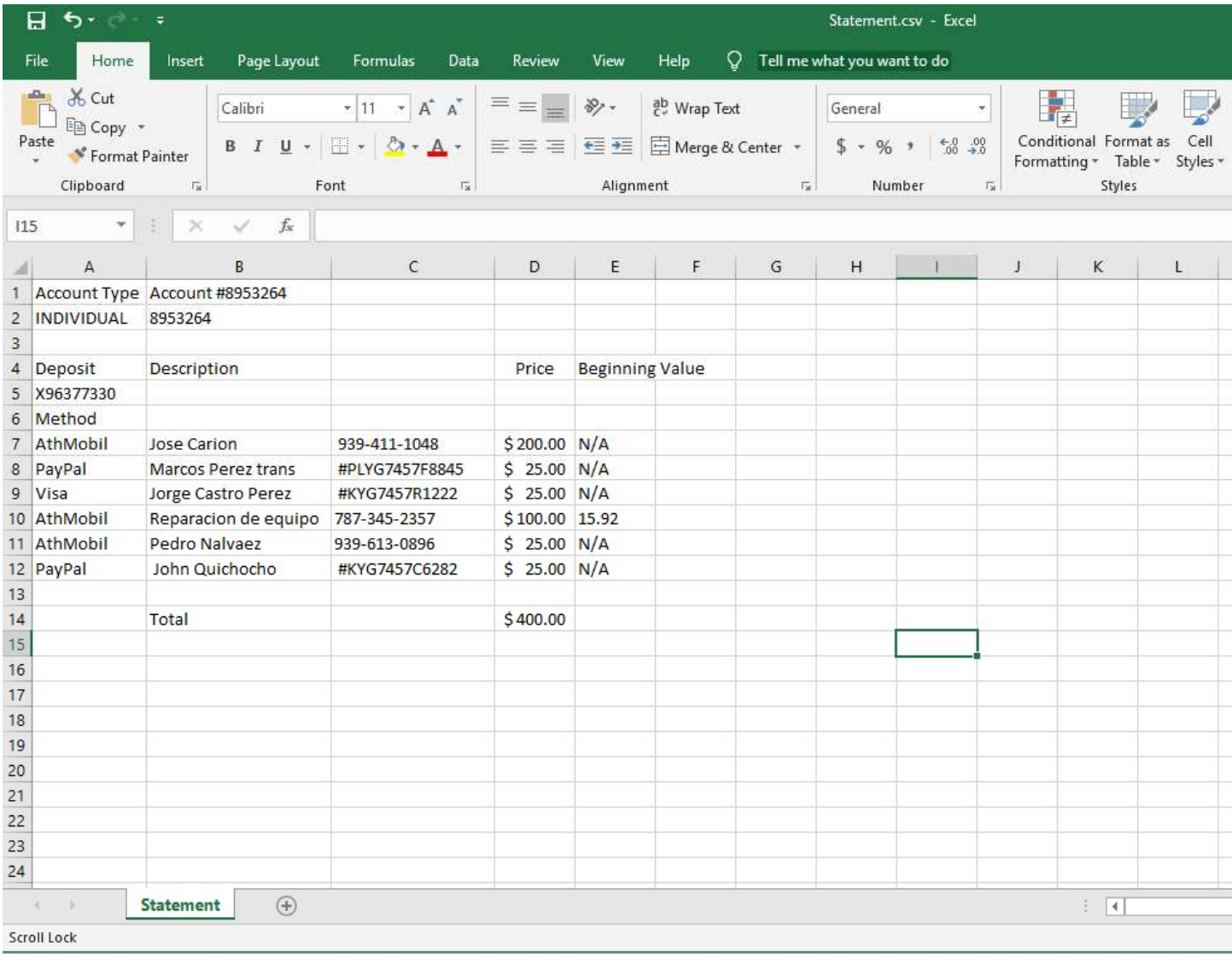
```
Account Type    Account #8953264
INDIVIDUAL      8953264

Deposit Description                     Price
X96377330
Method
AthMobil        Jose Carion      Carion  939-411-1048   $200.00
PayPal  Marcos  Perez    #PLYG7457F8845 $25.00
Visa    Jorge   Castro Perez     #KYG7457R1222  $25.00
AthMobil        Reparacion de equipo            787-345-2357    $100.00
AthMobil        Pedro   Nalvaez 939-613-0896    $25.00
PayPal   John    Quichocho       #KYG7457C6282  $25.00
PayPal  John    Peterson        81344   $25.00
Visa    Jennifer        Malloy  35222DUF        $25.00
PayPal  Barbara Johnson 54655   $25.00
Visa    Susan   Wilson  25G     $25.00
PayPal  Mary    James   AB 3265 M       $25.00
Visa    Scott   Green   21569   $25.00
PayPal  Kathleen        Gonzalez        21569   $25.00
Visa    Teresa  Evans   G34-567 $25.00
PayPal  Marie   Stewart 82 64 1 $25.00
Visa    Timothy Nelson  99799ABC-123    $25.00
```

AT12\/[root]/Users/Administrator/Documents/Cuentas/Copy of Statement.txt NUM

Figura 8: Contenido de documentos texto almacenado del disco duro.

El documento contiene los deposito efectuado la cuenta de banco del Sr Vázquez. Vemos que utiliza diferentes métodos de pago para que la operación de su organización. De esa forma lleva el control de los clientes para proveer el servicio pirata evitando que otros clientes reciba dicho servicio sin pagar.



	A	B	C	D	E
1	Account Type	Account #8953264			
2	INDIVIDUAL	8953264			
3					
4	Deposit	Description		Price	Beginning Value
5	X96377330				
6	Method				
7	AthMobil	Jose Carion	939-411-1048	$ 200.00	N/A
8	PayPal	Marcos Perez trans	#PLYG7457F8845	$ 25.00	N/A
9	Visa	Jorge Castro Perez	#KYG7457R1222	$ 25.00	N/A
10	AthMobil	Reparacion de equipo	787-345-2357	$ 100.00	15.92
11	AthMobil	Pedro Nalvaez	939-613-0896	$ 25.00	N/A
12	PayPal	John Quichocho	#KYG7457C6282	$ 25.00	N/A
13					
14		Total		$ 400.00	

Figura 9: Documento Excel depósitos de los clientes.

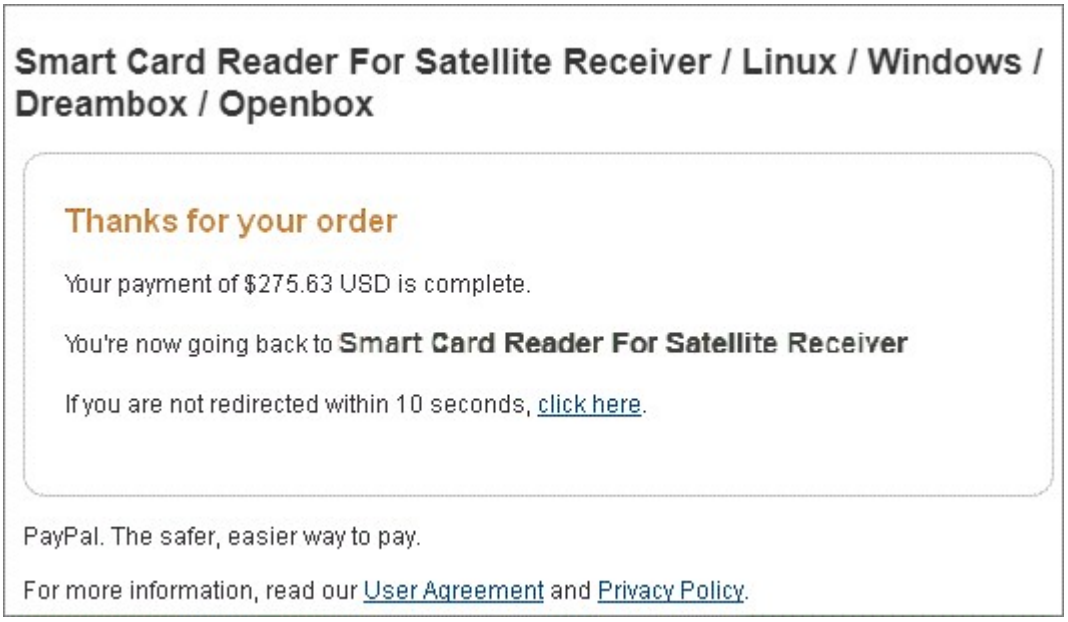


Figura 10: Recibo de compra de lector de tarjetas inteligente para receptores satelital

- Se realizó una compra de equipo para aumentar la cantidad de lectura en las tarjetas en el servidor en consecuencia aumentar la cantidad de clientes que puede recibir el servicio pirata.

Figura 11: Como lucen un lector de tarjetas inteligente.

Copy of Statement.IMD

	METODO_DE_PAGO	NOMBRE	APELLIDO	IDENTIFICACION	PAGOS
1	AthMobil	Jose Carion	Carion	939-411-1048	$200.00
2	PayPal	Marcos	Perez	#PLYG7457F8845	$25.00
3	Visa	Jorge	Castro Perez	#KYG7457R1222	$25.00
4	AthMobil	Reparacion de equipo		787-345-2357	$100.00
5	AthMobil	Pedro	Nalvaez	939-613-0896	$25.00
6	PayPal	John	Quichocho	#KYG7457C6282	$25.00
7	PayPal	John	Peterson	81344	$25.00
8	Visa	Jennifer	Malloy	35222DUF	$25.00
9	PayPal	Barbara	Johnson	54655	$25.00
10	Visa	Susan	Wilson	25G	$25.00
11	PayPal	Mary	James	AB 3265 M	$25.00
12	Visa	Scott	Green	21569	$25.00
13	PayPal	Kathleen	Gonzalez	21569	$25.00
14	Visa	Teresa	Evans	G34-567	$25.00
15	PayPal	Marie	Stewart	82 64 1	$25.00
16	Visa	Timothy	Nelson	99799ABC-123	$25.00
17	PayPal	Jack	Collins	AZ278	$25.00
18	Visa	Juan	Sanchez	81340	$25.00
19	Visa	Jonathon	Reed	971004A	$25.00
20	PayPal	Julie	Morris	10000 A	$25.00
21	Visa	Albert	Rogers	100139	$25.00
22	PayPal	Carolyn	Young	TJ9729	$25.00
23	Visa	Frank	Wright	000496CJW	$25.00
24	PayPal	Larry	Lopez	2828 BNA	$25.00
25	Visa	Joshua	Gonzalez	147865CTR	$25.00
26	PayPal	Melissa	King	54976/10	$25.00
27	Visa	Rebecca	Green	CS - 563 -97	$25.00
28	PayPal	Mitchell	Roberts	FR-963 32	$25.00

Figura 12: Importación data recuperado del documento llamado stament.

Cadena de custodia

NG DATA RECOVER está comprometido a cumplir con los protocolos al seguir al manejar la evidencia requerida para ser presentada y que sea requerida utilizar ante un tribunal. A continuación de describe en detalle la cadena de custodia de los dispositivos que se van a procesar. La cadena de custodia es utilizada para comprobar el proceso de adquisición, análisis y control de toda evidencia.

Primer Evento

- Descripción del evento: Recibo de evidencia entregado por el ayudante fiscal José Capo Iriarte y recibida por Wing Siang Ng Rosa, examinador de Ng Data Recover. La evidencia un disco duro marca Toshiba con una capacidad de 500GB de memoria. Están identificados como *Evidence No. 2015-EVI-1*.

- Evento verificado por: Ayudante fiscal José Capo Iriarte (Representante del cliente) y Wing Siang Ng Rosa (Examinador Forense)
- Fecha de comienzo: 28 de agosto de 2016, – 8:35am
- Fecha de terminación: 16 de septiembre de 2016, – 8:40am
- Lugar de origen: 150 Avenida Carlos E. Chardón, San Juan, 00918
- Destino: Laboratorio Forense de Ng Data Recover

Segundo Evento

- Descripción del evento: Creación de número del caso y asignación de evidencia.
- Evento verificado por: Wing Siang Ng Rosa (Examinador Forense)
- Asignar número al caso: 18-670(ADC)
- Fecha de comienzo: 16 de septiembre de 2016 – 8:43am
- Fecha de terminación: 16 de septiembre de 2016 – 8:46am
- Lugar de origen: Laboratorio Forense de NG DATA RECOVER
- Destino: Laboratorio Forense de NG DATA RECOVER

Tercer Evento

- Descripción del evento: Generación de las imágenes del disco duro para evitar la contaminación de la evidencia y su preservación durante la examinación de la memoria de está utilizando *FTK Imager*.
- Evento verificado por: Wing Siang Ng Rosa
- Número de caso: 18-670(ADC)
- Fecha de comienzo: 19 de septiembre de 2016 – 8:50am
- Fecha de terminación: 19 de septiembre de 2016 – 9:48am

- Lugar de origen: Laboratorio Forense de NG DATA RECOVER
- Destino: Laboratorio Forense de NG DATA RECOVER

Cuarto Evento

- Descripción del evento: Guardar en la bóveda de evidencia del disco duro 500GB identificados como *Evidence No. 2017-EVI-1y* una imagen en un USB de 128GB marca Lexar de color verde con blanco y una imagen en un USB de 64GB marca EMTEC de color gris.
- Evento verificado por: Wing Siang Ng Rosa (Examinador Forense) y José Carrión (Encargado de la Bóveda)
- Número de caso: 18-670(ADC)
- Fecha de comienzo: 20 de septiembre de 2016 – 9:50am
- Fecha de terminación: 20 de septiembre de 2016 – 11:52am
- Lugar de origen: Laboratorio Forense de NG DATA RECOVER
- Destino: Cuarto de evidencia de NG DATA RECOVER

Quinto Evento

- Descripción del evento: Buscar en la bóveda del cuarto de evidencia de NG DATA RECOVER una imagen identificada como *NGR-EVI-01* y una imagen identificada como *NGR-EVI-02* para analizar.
- Evento verificado por: Wing Siang Ng Rosa (Examinador Forense) y José Carrión (Encargado de la Bóveda)
- Número de caso: 18-670(ADC)
- Fecha de comienzo: 21 de septiembre de 2016– 8:05am
- Fecha de terminación: 21 de septiembre de 2016 – 8:15am

- Lugar de origen: Cuarto de evidencia de NG DATA RECOVER
- Destino: Laboratorio Forense de NG DATA RECOVER

Sexto Evento

- Descripción del evento: Análisis de las imágenes identificados como *NGR-EVI-1* y *NGR-EVI-2* utilizando los programas *FTK Imager* e *IDEA*.
- Evento verificado por: Wing Siang Ng Rosa (Examinador Forense)
- Número de caso: 18-670(ADC)
- Fecha de comienzo: 21 de septiembre de 2016 – 8:20am
- Fecha de terminación: 06 de febrero de 2017 – 6:00pm
- Lugar de origen: Laboratorio Forense de NG DATA RECOVER
- Destino: Laboratorio Forense de NG DATA RECOVER

Séptimo evento

- Descripción del evento: Devolución de las imágenes identificadas como *NGR-EVI-1*y *NGR-EVI-2*a la bóveda de evidencia del cuarto de evidencias de NG DATA RECOVER.
- Evento verificado por: Wing Siang Ng Rosa (Examinador Forense) y José Carrión (Encargado de la Bóveda)
- Número del caso: 18-670(ADC)
- Fecha de comienzo: 07 de febrero de 2017 – 5:40pm
- Fecha de terminación: 07 de febrero de 2017 -5:45pm
- Lugar de origen: Laboratorio Forense de NG DATA RECOVER
- Destino: Cuarto de evidencia de NG DATA RECOVER

Octavo evento

- Descripción del evento: Buscar en la bóveda del cuarto de evidencia de NG DATA RECOVER las imágenes identificadas como *NGR-EVI-1*y *NGR-EVI-2*para analizar.
- Evento verificado por: Wing Siang Ng Rosa (Examinador Forense) y José Carrión (Encargado de la Bóveda)
- Número del caso: 18-670(ADC)
- Fecha de comienzo: 8 de febrero de 2017 – 8:30am
- Fecha de terminación: 8 de febrero de 2017 – 8:38am
- Lugar de origen: Cuarto de evidencia de NG DATA RECOVER
- Destino: Laboratorio Forense de NG DATA RECOVER

Noveno evento

- Descripción del evento: Análisis de las imágenes identificadas como *NGR-EVI-1*y *NGR-EVI-2*con la herramienta llamada IDEA.
- Evento verificado por: Wing Siang Ng Rosa (Examinador Forense)
- Número del caso: 18-670(ADC)
- Fecha de comienzo: 9 de febrero de 2017 – 8:00am
- Fecha de terminación: 9 de febrero de 2017 – 4:50pm
- Lugar de origen: Laboratorio Forense de NG DATA RECOVER
- Destino: Laboratorio Forense de NG DATA RECOVER

Decimo evento

- Descripción del evento: Devolución de las imágenes identificadas como *NGR-EVI-1* y *NGR-EVI-2* a la bóveda de evidencia del cuarto de evidencias de NG DATA RECOVER.
- Evento verificado por: Wing Siang Ng Rosa (Examinador Forense) y José Carrión (Encargado de la Bóveda)

- Número del caso: 18-670(ADC)
- Fecha de comienzo: 10 de febrero de 2017 – 8:00am
- Fecha de terminación: 10 de febrero de 2017 – 8:10am
- Lugar de origen: Laboratorio Forense de NG DATA RECOVER
- Destino: Cuarto de evidencia de NG DATA RECOVER

Decimoprimero evento

- Descripción del evento: Devolución de la evidencia al cliente. Entrega realizada por el Sr. Wing Siang Ng Rosa, examinador forense de NG DATA RECOVER y recibida por el ayudante fiscal de FBI José Capo Iriarte. La evidencia consiste en un Disco duro Toshiba de 500GB identificado como *Evidence No. 2017-EVI-1*.
- Evento verificado por: Wing Siang Ng Rosa (Examinador Forense), José Capo Iriarte (Representante de FBI) y José Carrión (Encargado de la Bóveda)
- Número del caso: 18-670(ADC)
- Fecha de comienzo: 2 de marzo de 2017 – 8:00am
- Fecha de terminación: 2 de marzo de 2017 – 11:55am
- Lugar de origen: Cuarto de evidencia de NG DATA RECOVER

Destino: 300 Recinto Sur Street Old San Juan Puerto Rico 00901

Procedimiento

En la investigación de la información se utilizó el programa FTK Imager para crear una copia idéntica de la data contenida del disco duro entregados al examinador. Motivo de esto es evitar la alteración de la información de cualquier tipo de modificación causado por los procesos de análisis, lo cual puede anular su validez de misma. La razón de crear imágenes para poder

estudiar la información sin tener preocupación de dañar la data originalmente ya recuperada por los oficiales.

En la ilustración se muestra el programa FTK Imager al ser iniciado en la computadora. Utilizan esta herramienta que se crea una copia exacta en una del dispositivo de almacenamiento entregado al examinador para ser analizada.

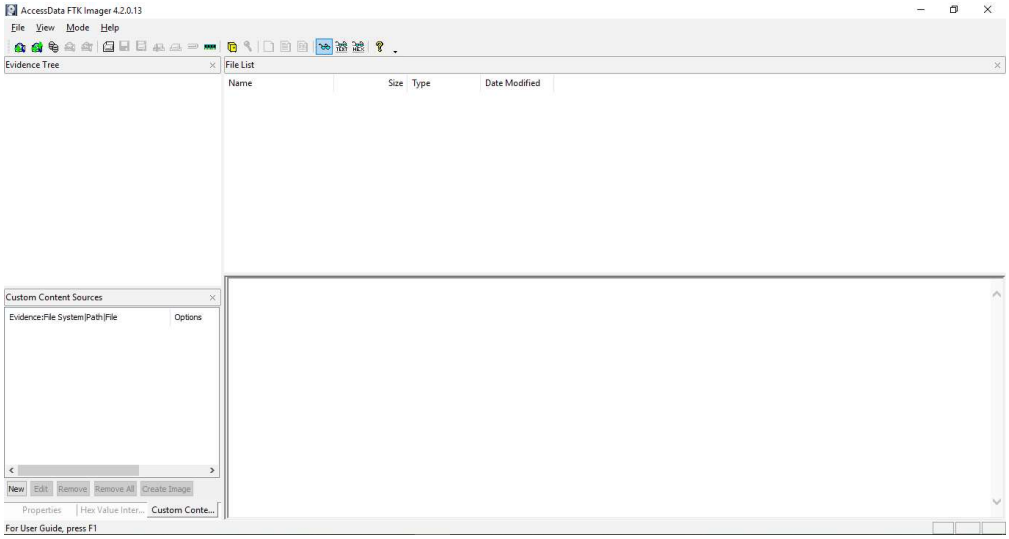


Figura 13: Página principal de FTK Imager

La siguiente imagen muestra al ir file, add evidence ítem puedes agregar el dispositivo de almacenamiento cuando se selecciona tipo de imagen se va a crear según el dispositivo que se va a copiar. En esta situación ya que en copiar la información en el USB se escoge "PhysicalDrive2" para que el programa reconocer que se estará duplicando un disco físico. También se escoge el drive número dos debido a que FTK Imager reconoce a disco duro local de la computadora como el drive número uno.

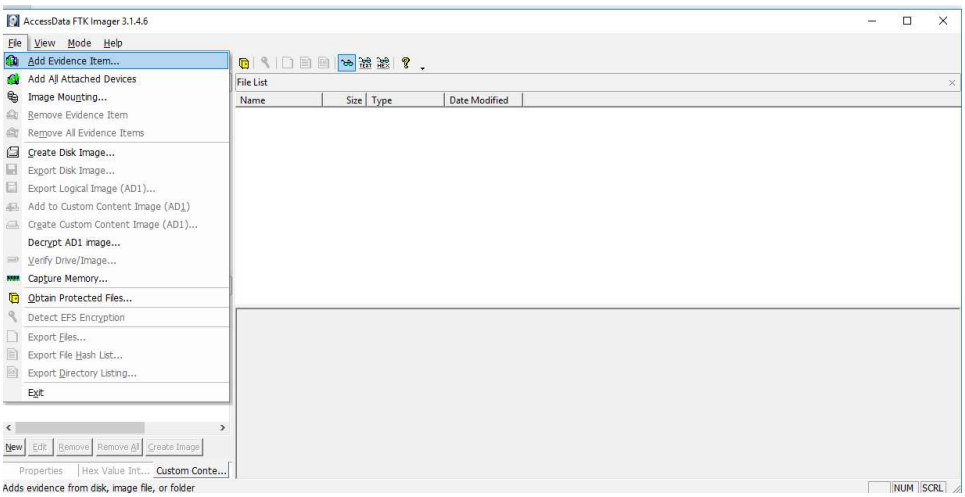


Figura 14: Agregando evidencia

El proceso de crear una imagen para analizarla te da opción para anotar número de caso, numero de evidencia, nombre de examinada nota y una descripción única.

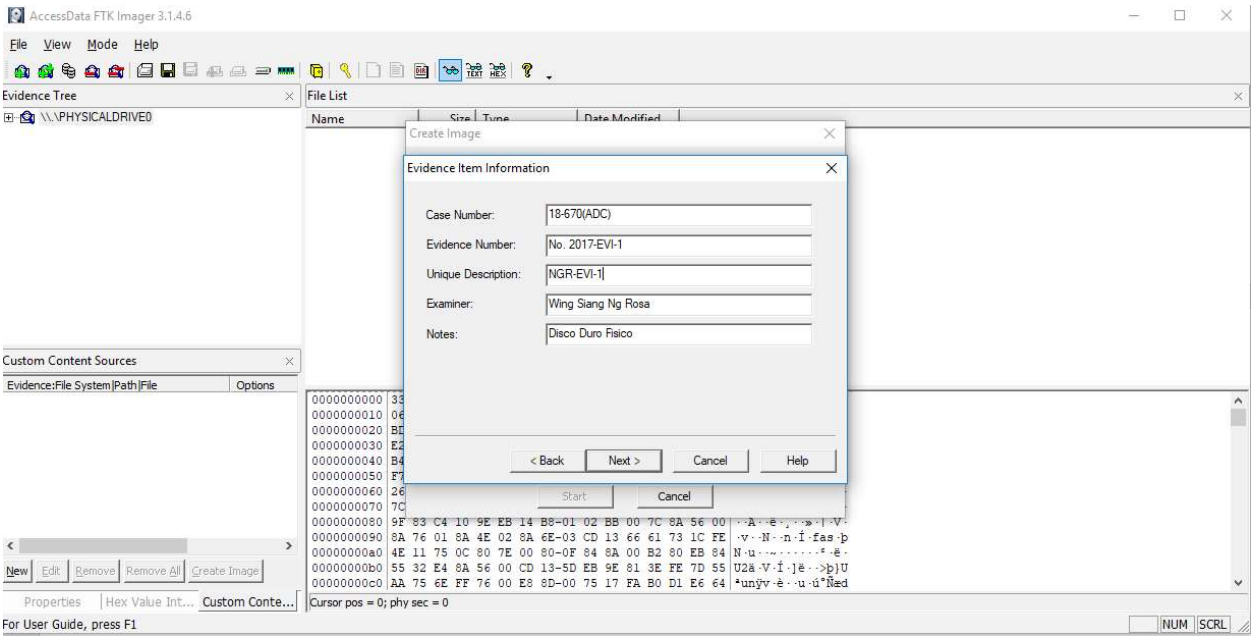


Figura 15: Creación de imagen disco duro físico

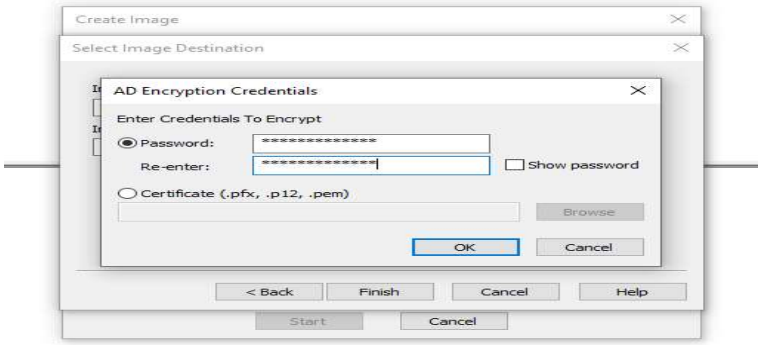


Figura 16: Contraseña de la imagen

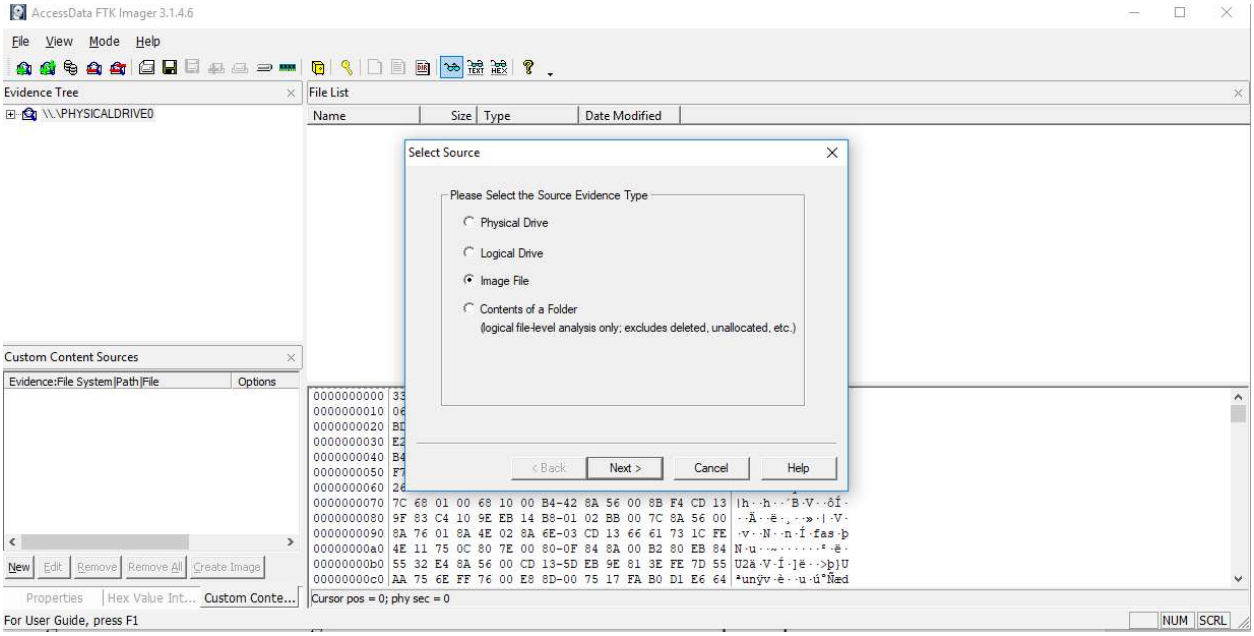


Figura 17: FTK – Montando la imagen creada

En el proceso de montar la imagen en FTK se selección en dispositivo donde esta guardad la imagen (Figura 6) requiriendo insertar la contraseña ya que se agregó esa opción en su creación para evitar el acceso no autorizado.

Cuando la imagen está agregada en el programa FTK en la computadora y está la reconoce como el objeto original se puede iniciar acceso a los datos. El programa de FTK existe una opción de crear un árbol en forma jerarquía el examinador puede estudiar la data dentro de la imagen creada. Este árbol jera hico es representado en forma de librería (Figura 22). La interfase

de FTK similar a como el explorador de Windows mostrando las carpetas y archivos. Al usar librería se puede observar cada sección de la imagen para descubrir la ubicación de la data. Similar al examinar fuera la situación en la cual se estuviera examinado un disco duro extraído de una computadora o un servido utilizando esta librería, se pudiera investigar las diferentes carpetas para revelar si existe información borrada. Además, te muestra nombre de los archivos que fueron borrado y donde estaban ubicado.

Al utilizar esta herramienta se pudo encontrar que la organización de Sr Vázquez detectar recibo y cuenta de sus clientes en Excel también operaba un servido Linux utilizando una máquina virtual para brindar el servicio pirata.

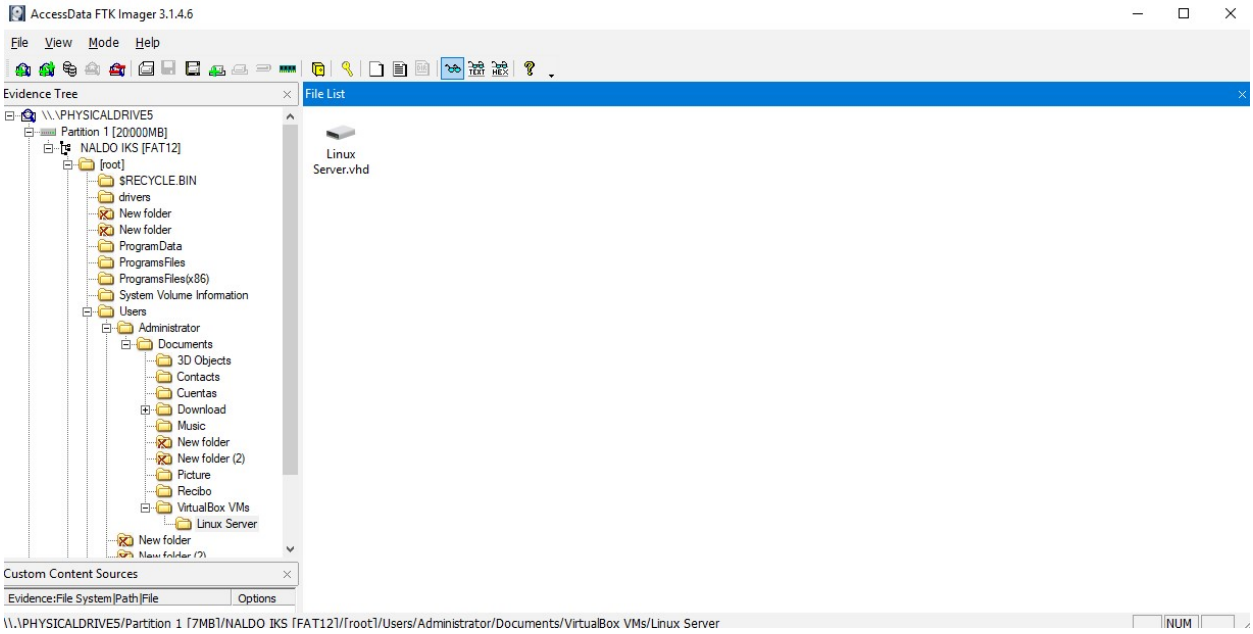


Figura 18: Data dentro de la imagen

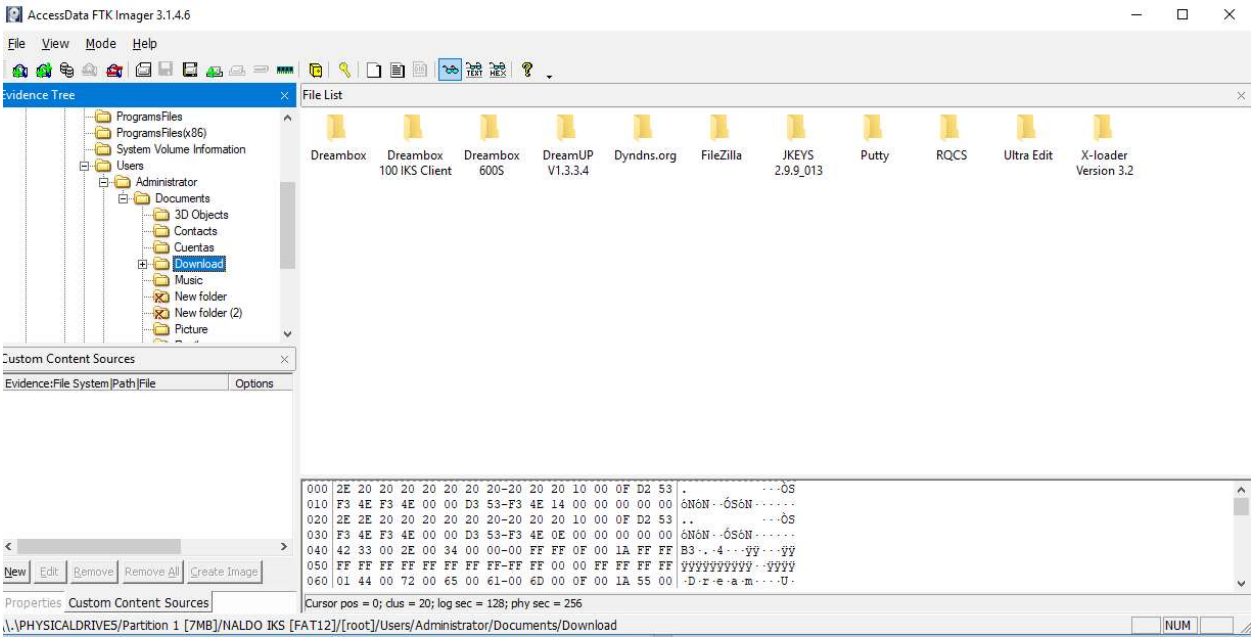


Figura 19: Programa descargado que se utiliza en un servidor internet key sharing.

Ademase, en la imagen de la computadora del acusado se encontraron documentos en los formatos de pdf y Excel. La imagen de la computadora contiene documentos de Excel con la información bancaria de los clientes de la Sr. Vázquez. Las siguientes figuras ilustran como FTK mostraron los documentos al examinador durante la investigación de la evidencia.

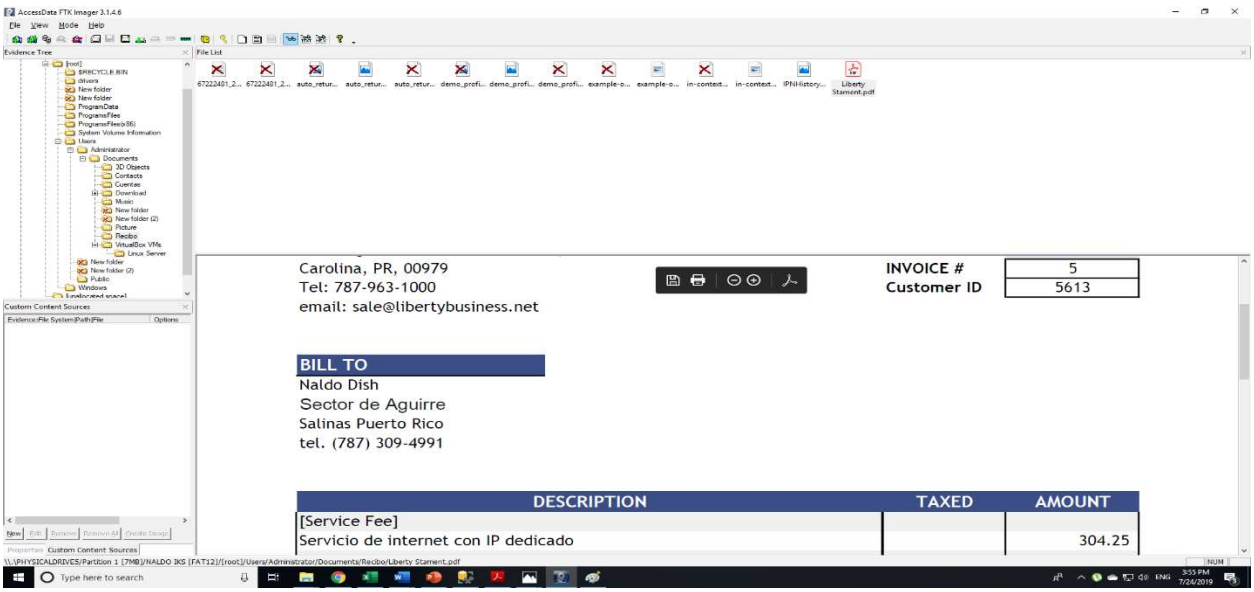


Figura 20: Factura de Liberty Business por servicio de internet.

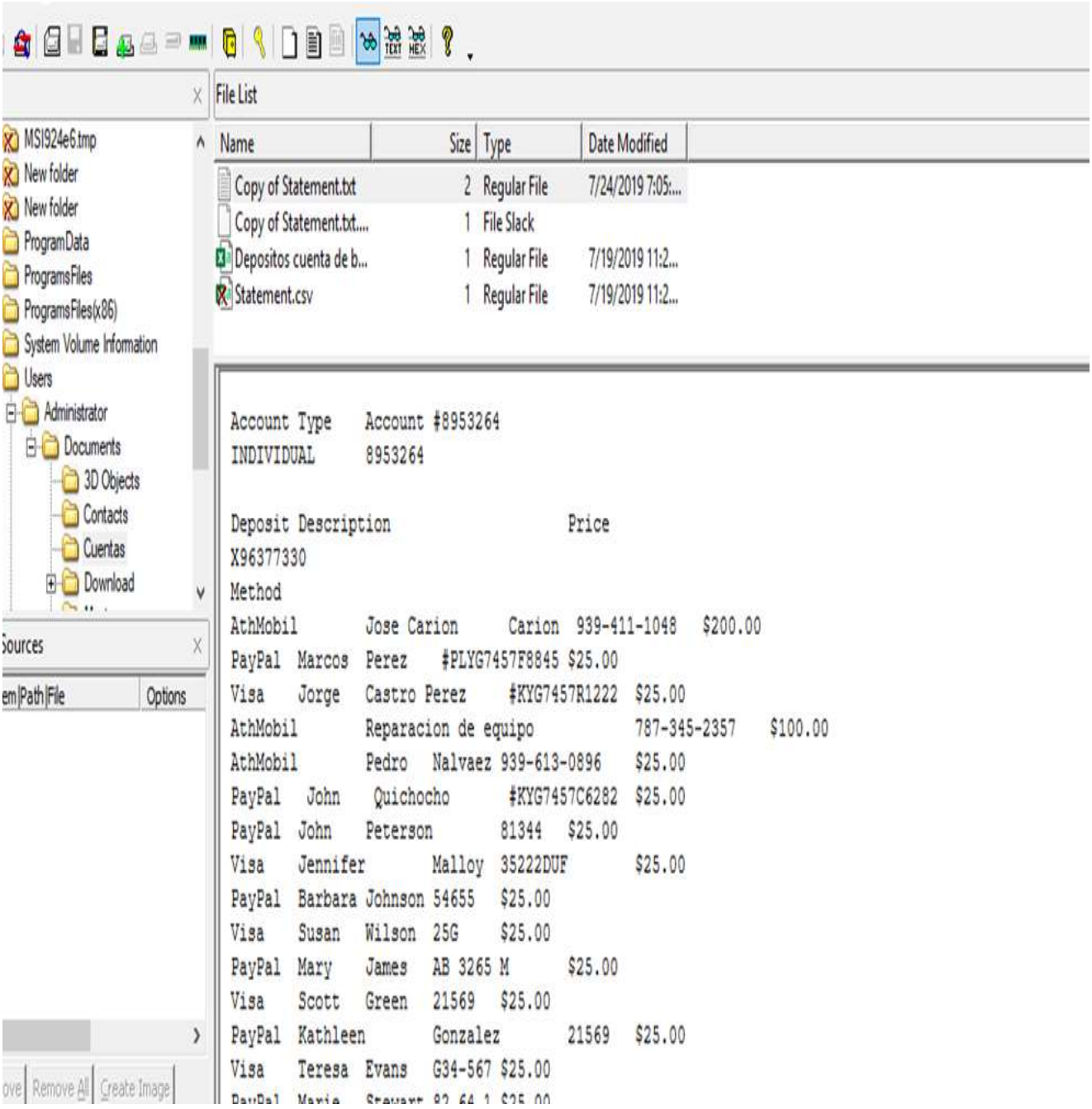


Figura 21: Ubicación del archivo en Excel.

Al obtener la data se inició el proceso a tener acceso a la data mediante la herramienta llamada IDEA que ayuda a organizar la data en bruto. La aplicación de IDEA ayuda visualizar de diferente forma disponibles en esta herramienta para obtener una investigación más robusta.

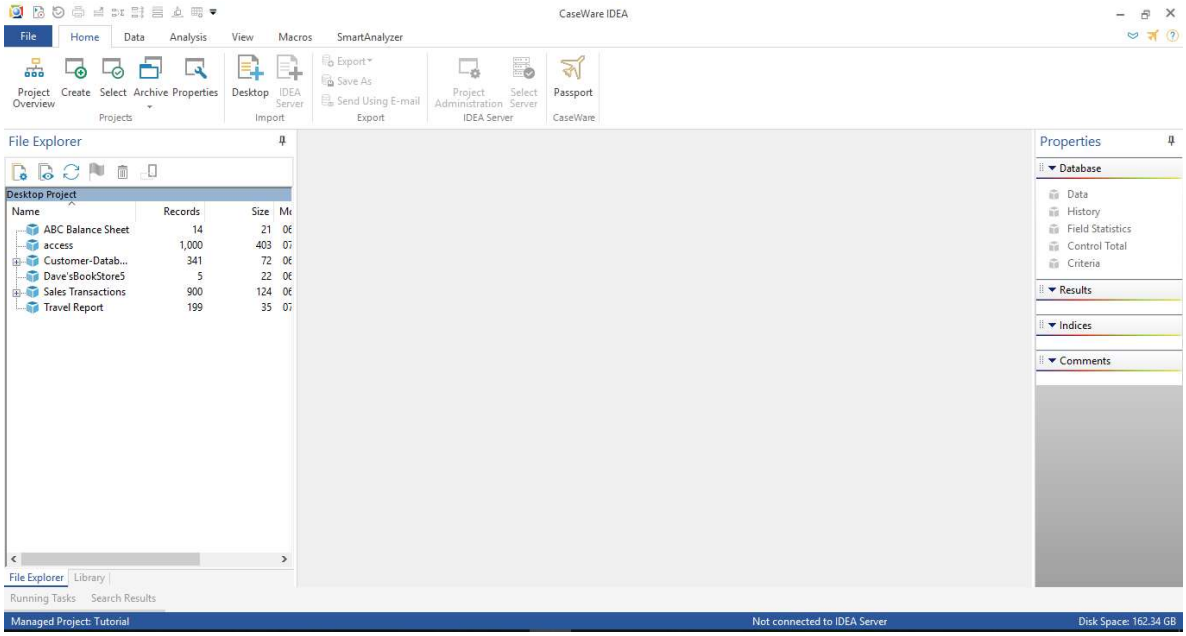


Figura 22: Foto de aplicación de IDEA cuando se abre por primera vez.

Al abrir la aplicación de IDEA fue oprimir el botón de Desktop para crear una nueva base de datos en el programa. De esta manera se podía tener acceso a la información de manera más rápida a través de la investigación sin tener que alterar la data. La siguiente imagen muestra esta creación.

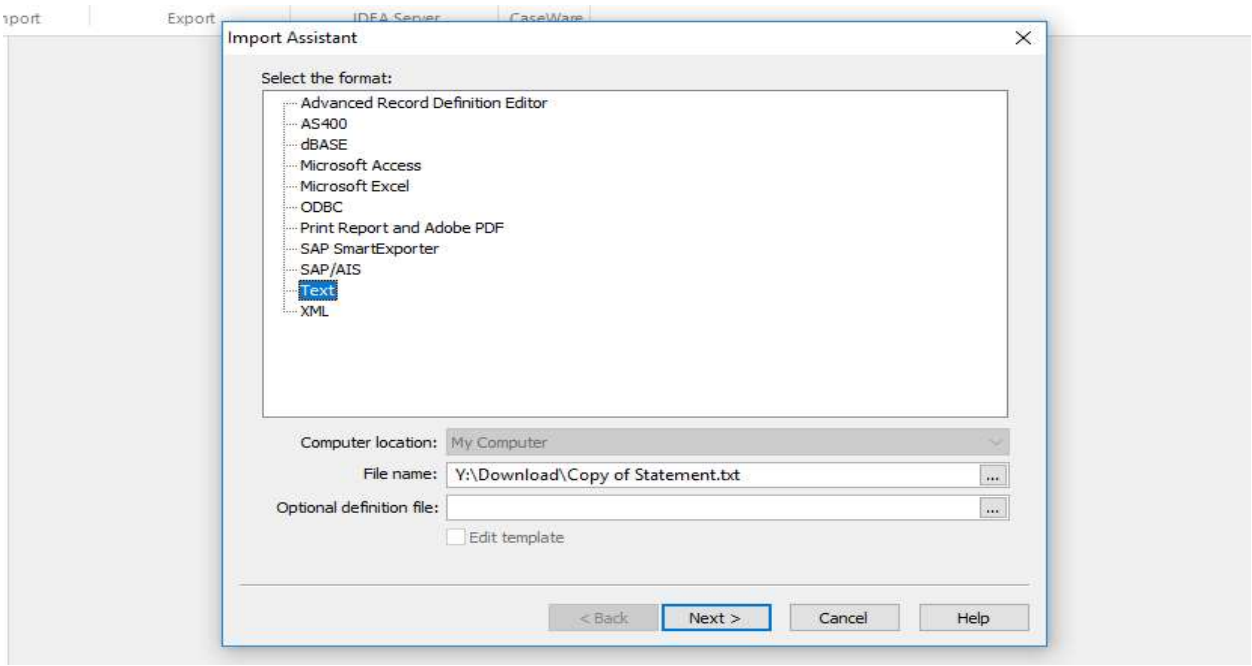


Figura 23: Creación de base de datos en IDEA

En la creación de la base de dato hay que clasificar la data para llevar un análisis efectivo. Se seleccionó que ignore las primeras 6 líneas de la hoja de texto para no tener data innecesaria.

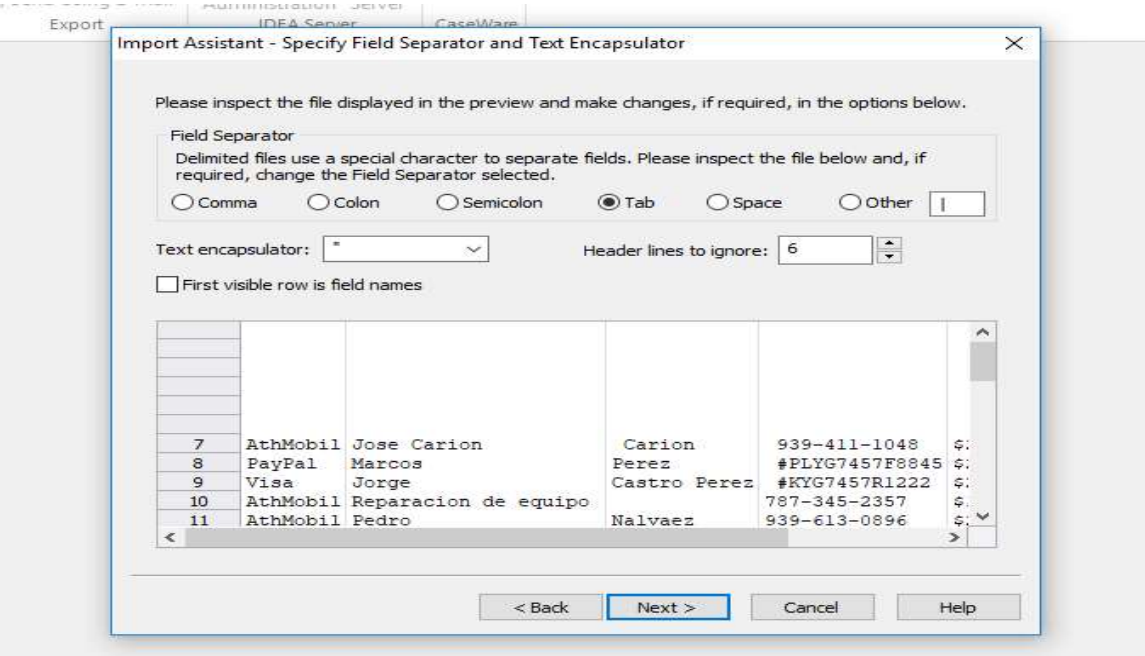


Figura 24: Selección de los separadores de campos.

En la siguiente venta iniciamos la clasificación de las columnas. Hay que ser cauteloso en el momento de nombrar las columnas. Porque hay que distinguir bien la data antes de nombrar. La primera a hacia la quinta columna se llamó método de pago, nombre, apellido, identificación y pagos.

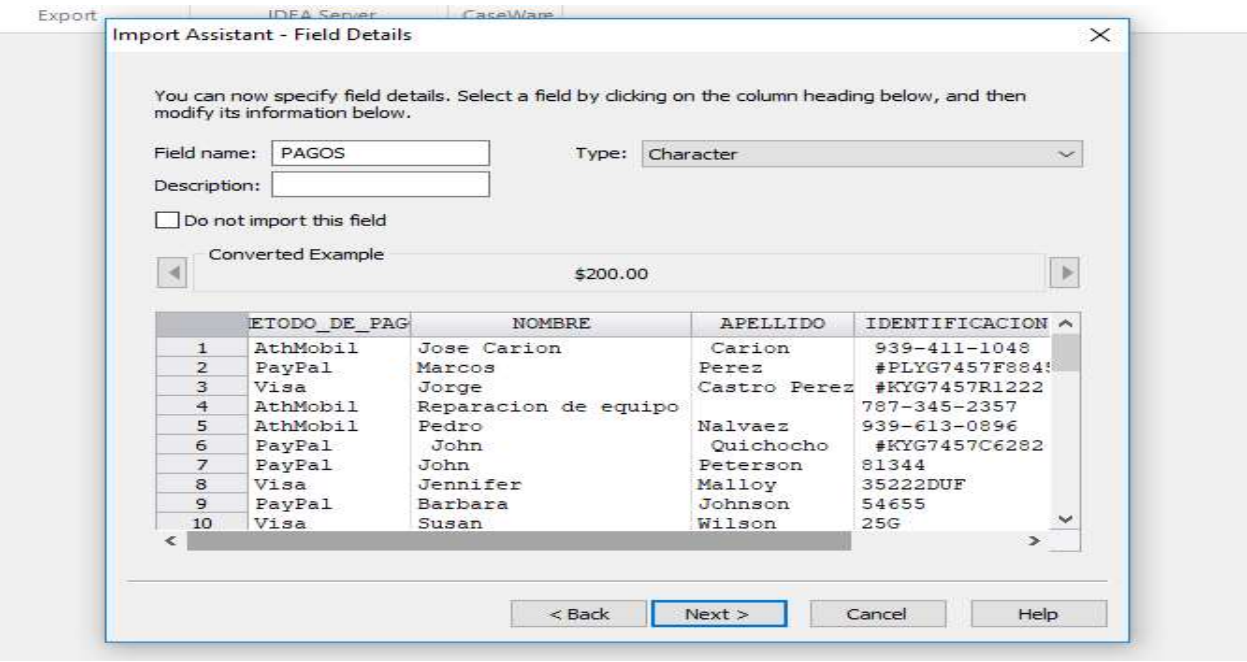


Figura 25: Nombrar la columna de la data.

Ya terminado el proceso de nombrar las columnas se puede apreciar la data más organizada. Podemos observar la cantidad de clientes que emitieron pagos para recibir el servicio pirata. Pero por medio del nombre, apellido e identificación el Sr. Alnardo Vázquez verifica que cliente puede recibir el servicio pirata.

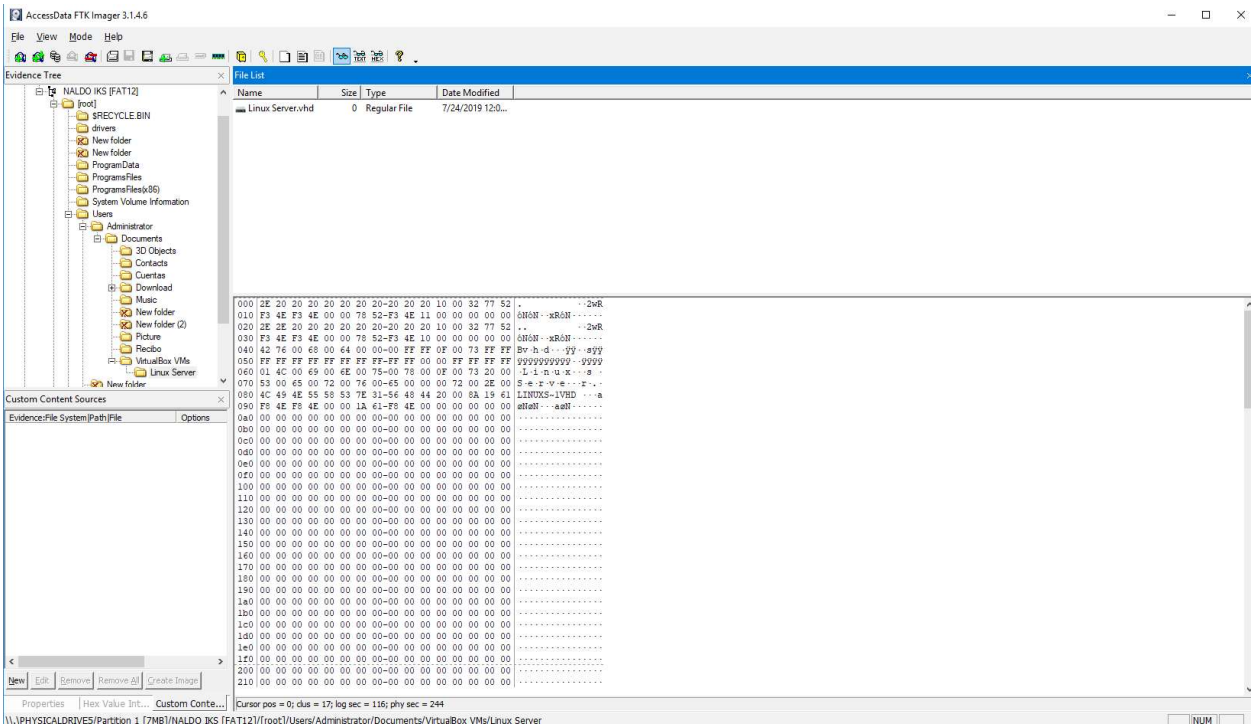


Figura 26: Ubicación del servidor que provee servicio internet key sharing.

Al encontrar una máquina virtual donde operaba un servidor y contiene su disco duro virtual. Se procedió investigar su disco duro virtual convirtiéndolo a una imagen para no alterar su contenido. En la (figura 28) veremos el hallazgo que se encontró tenía todos los programas para correr el servicio pirata.

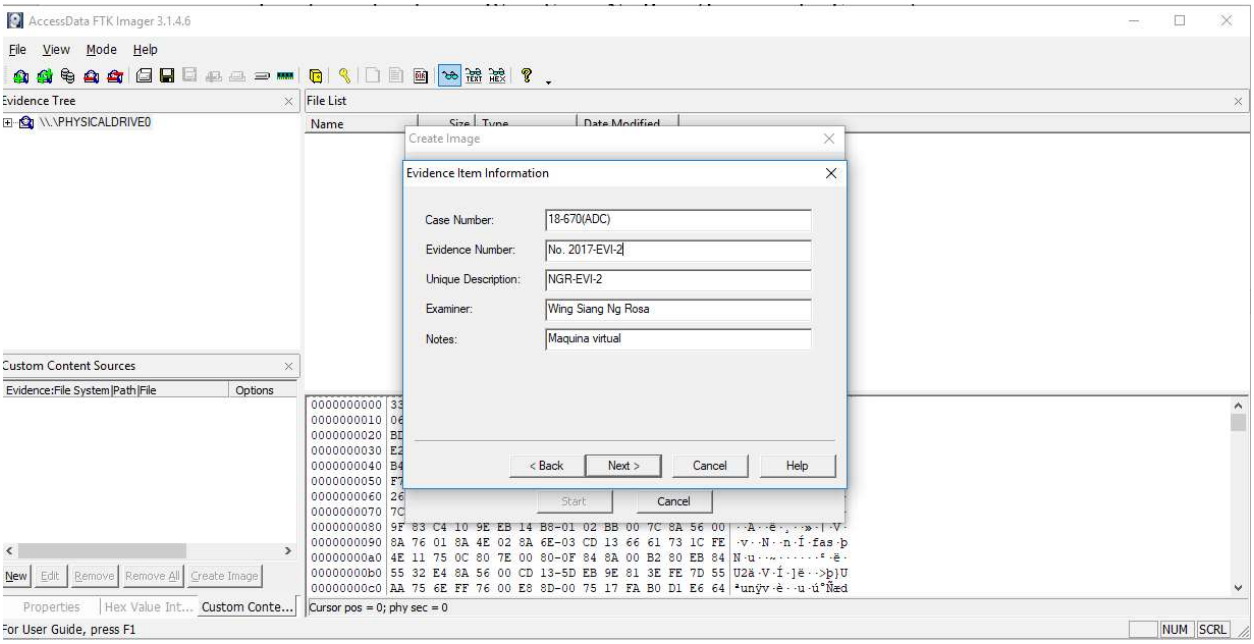


Figura 27: Creación de una imagen proveniente de un disco duro virtual.

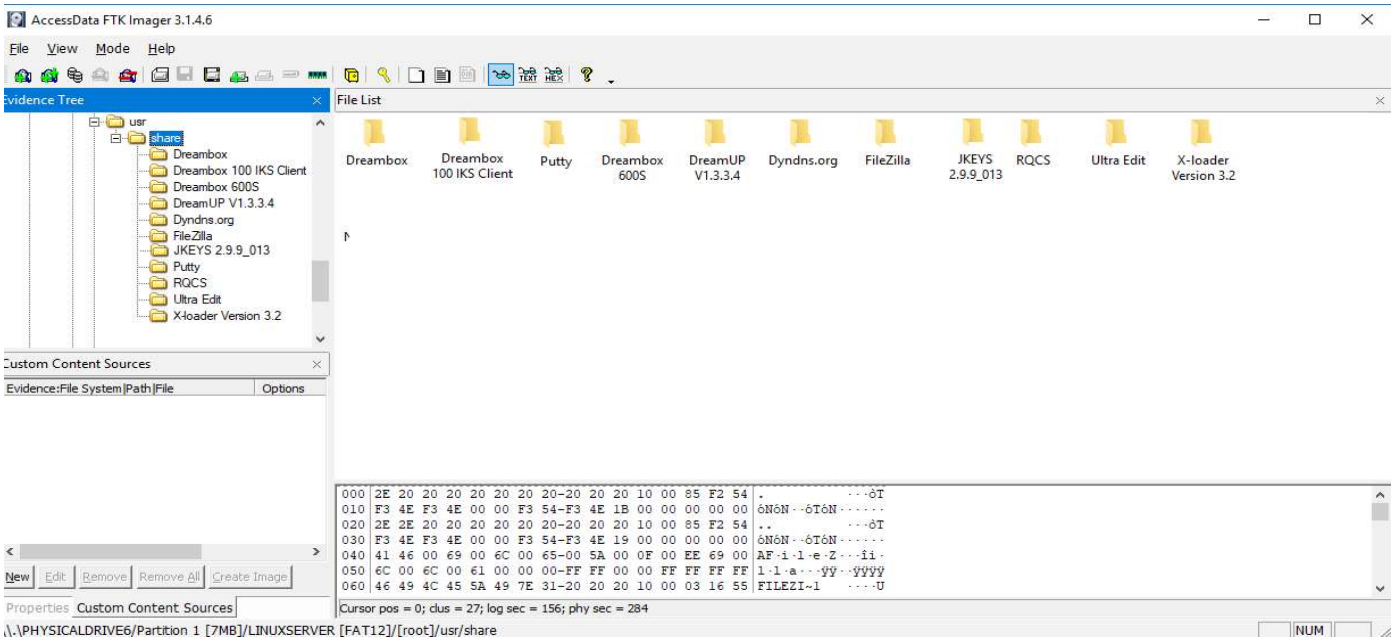


Figura 28: Directorio de los programas requerido para operar el servicio pirata instalado en Linux.

Sección 5: Discusión del caso

La evidencia recopilada por NG DATA RECOVER durante la examinación de las imágenes identificados como *Evidence NGR-EVI-1* y *Evidence NGR-EVI-2* más los documentos encontrados, factura y programas dentro de éste, sirven como claves importantes para los oficiales del FBI con el propósito de probar que los acusados Alnardo Vázquez, Awildo Jiménez, And Higinio Lamboy cometieron varios fraudes en crimen organizado, alteración de dispositivo para cometer fraude y eludir los derechos de autor. Se evidenció que durante la investigación de las transacciones que se hacían en la cuenta bancaria del Sr Vázquez con múltiples transacciones monetarias que las mayorías eran regalo o donaciones hacia esa cuenta. Con la intención de que no se detectara que se estaba haciendo venta de un servicio pirata.

Sección 6: Auditoria y prevención

En la investigación, análisis y evaluación de este caso, se notaron una falla en el monitoreó en que el tipo de fraude que se está cometiendo en Dish Network no lo han corregido. Ya que son varios casos en estados unido y fuera que promueven el uso de servicio pirata satelital.

A continuación, están los hallazgos encontrados con recomendaciones para detectar y mitigar a estos:

- **Hallazgo #1:** Dish network no ha podido resolver el gran problema que tiene al seguir utilizando tarjetas inteligentes.
  - Recomendación: Tratar de dejar de utilizar tarjetas inteligentes y la numeración de la tarjeta pasarlo a la tarjeta madre del receptor y que sea difícil de replicar o alterar la numeración.
- **Hallazgo #2:** La mayoría de los casos que Dish Network a procesado termina siempre en negociación.
  - Recomendación: Cada vez que se presenta un juicio que el demandado pague las multa y con cárcel. Ya que siempre el que comete el delito es más fácil pagarle a Dish Network a que ir a cárcel.

Sección 7: Conclusión

Al analizar del caso de United States of America vs Alnardo Vázquez, Awildo Jiménez, y Higinio Lamboy, se pudo determinar lo fácil que se puede crear un servidor internet key sharing (IKS), ya que hay tutoriales en “youtube” de esos servidores y la facilidad de hacerlo por sí mismo. Unos de los errores que ellos cometieron es que se promovieron por las redes sociales y utilizaron “WhatsApp” para enviar cotizaciones o hacer pago utilizando “ATH Mobile”. Además, no solo brindaba servicio en Puerto Rico, sino que también en los Estados Unidos hasta Guam.

La organización logro obtener ganancias monetarias para sí mismos como parte fraudulenta. Fácilmente ellos tenían una cantidad considerable de cliente aparte en la instalación de nuevas antenas, pero en ventas de receptores modificado y servicio satelital pirata eran muchos clientes. Una falla que pude notar en este caso era que los demandantes no fueron cautelosos en la implementación del servicio pirata. Ya que el servidor estaba en jurisdicción de los Estados Unidos fue fácil de procesar a los acusados.

En fin, todo tipo de fraude que sé que cometen siempre sale a la luz. Por tal razón es bien importante ser cauteloso al utilizar tutoriales en “youtube”, ya que pueden ser parte de un fraude que podemos cometer sin darnos cuenta. Porque siempre se va a saber cómo uno ejecuto el fraude.

Sección 8: Referencias

Accessdata. (2019).) FORENSIC TOOLKIT (FTK). 2019, de Accessdata.com Recuperado de: https://accessdata.com/products-services/forensic-toolkit-ftk

Cordero, G. (2013). Apoyo múltiple a ley estatal contra la piratería de señales de televisión. Retrieved 28 May 2019, from https://www.primerahora.com/noticias/gobierno-politica/nota/apoyomultiplealeyestatalcontralapirateriadesenalesdetelevision-949762/

DISH NETWORK L.L.C. V. SINGH CASE NO. 5:16-CV-00539-JSM-PRL (UNITED STATES DISTRICT COURT MIDDLE DISTRICT OF FLORIDA, 2016). Recuperado de: https://casetext.com/case/dish-network-llc-v-singh-1

DISH NETWORK VS DONALD SINGH NO. 1:14-CV-1581. 2019 (UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF OHIO EASTERN DIVISION, 2015). Recuperado de: https://casetext.com/case/dish-network-llc-v-singh

IDEA. (2019). IDEA Audit Software | IDEA Data Analysis Software | IDEA. (2019). IDEA. Recuperado el 18 Julio 2019 de: https://idea.caseware.com/products/idea/

UNITED STATES OF AMERICA VS ARNALDO VÁZQUEZ, AWILDO JIMENEZ, AND HIGINIO LAMBOY. 2019, (United State of America District Court of Puerto Rico, 2018). Recuperado de: https://www.justice.gov/usao-pr/pr/three-puerto-rican-men-arrested-federal-charges-dish-network-services-piracy-scheme

Zamorano, (2019). NAVEGANDO POR LA TELEVISIÓN SATELITAL LEGAL E ILEGAL. 2019, de Entretenimiento Fiyer Mayer Recuperado de: https://www.fayerwayer.com/2012/08/navegando-por-la-television-satelital-legal-e-ilegal/