EDP UNIVERSITY OF PUERTO RICO, INC.

RECINTO DE HATO REY

PROGRAMA DE MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Especialidad en Seguridad de Información e Investigación de Fraude Digital

LAVADO DE DINERO Y ATAQUE DE RANSOMWARE
ANÁLISIS DE CASO: UNITED STATES v. RAYMOND ODIGIE UADIALE

Caso Número: 18-CR-60073-WPD

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Especialidad en Seguridad de Información e Investigación de Fraude Digital

DICIEMBRE, 2018

PREPARADO POR:

LUIS A. GANDÍA VÁZQUEZ

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

LAVADO DE DINERO Y ATAQUE DE RANSOMWARE
ANÁLISIS DE CASO: UNITED STATES v. RAYMOND ODIGIE UADIALE

Caso Número: 18-CR-60073-WPD

Preparado por

Luis A. Gandía Vázquez

Ha sido aceptado como requisito parcial para el grado de

Maestría en Sistemas de Información

Especialidad en Seguridad de Información e Investigación de Fraude Digital

Diciembre, 2018

Aprobado por:

Dr. Miguel A. Drouyn, Director

TABLA DE CONTENIDO

SECCIÓN 1: INTRODUCCIÓN Y TRASFONDO

Introducción

Las tecnologías de información y telecomunicaciones se han convertido en parte esencial de nuestra vida cotidiana. Cada vez dependemos más de la conveniencia que nos ofrece una aplicación para manejar nuestras cuentas bancarias, un portal web para realizar gestiones con el gobierno, o una plataforma social para comunicarnos con nuestros seres allegados, entre muchos otros ejemplos. Sin embargo, esa conveniencia puede tener un costo. Las tecnologías de información y telecomunicaciones nos acercan más al mundo, pero también nos acercan más a los peligros que en el habitan.

Según la ACFE (2018a), las entidades gubernamentales y empresas privadas dependen completamente de sus sistemas de información para llevar a cabo sus operaciones diarias. De igual manera, los criminales han encontrado en la tecnología un nuevo instrumento para cometer actos delictivos que en tiempos de antaño se ejecutaban por medios más ortodoxos.

Existe un sinnúmero de categorías de crímenes cibernéticos, cuya diversidad solo se limita a la creatividad del delincuente. Ante dicho panorama, es de nuestro particular interés todo aquel tipo de delito cibernético que involucre alguna modalidad de fraude.

A continuación, se presenta y analiza el caso de un ex-ingeniero de Microsoft que se vio involucrado en un esquema internacional de extorsión y lavado de dinero, haciendo uso de un *ransomware*.

Descripción del caso

Número de caso: 18-CR-60073-WPD

Partes en el caso:

Acusados (autores)

- Raymond Odigie Uadiale, a/k/a, “Mike Roland”, de 41 años y residente de Maple Valley, Washington.
- Co-conspirador 1, a/k/a, “K!NG”, residente de Reino Unido.

Entidades involucradas

- Liberty Reserve - servicio de moneda digital.
- Individuos y otras entidades no identificadas - víctimas residentes en los Estados Unidos.

Investigadores

- Matthew J. DeSarno, Agente Especial a Cargo, División Criminal de la Oficina del FBI en Washington.
- Agencia Criminal Nacional de Reino Unido.

Abogado

- David J. Joffe, Abogado de Defensa.

Fiscales

- William Joss Nichols, Fiscal de la División de Delitos Informáticos y Propiedad Intelectual, Corte de Estados Unidos, Distrito de Columbia.
- Jared M. Strauss, Fiscal Asistente, Corte de Estados Unidos, Distrito Sur de Florida.
- Benjamin C. Greenberg, Fiscal, Corte de Estados Unidos, Distrito Sur de Florida.

- Brian A. Benczkowski, Fiscal Asistente de la División Criminal del Departamento de Justicia de Estados Unidos.

Jueces

- William P. Dimitrouleas, Juez, Corte de Estados Unidos, Distrito Sur de Florida.
- Barry S. Seltzer, Juez Magistrado, Corte de Estados Unidos, Distrito Sur de Florida.
- Lurana S. Snow, Juez Magistrado, Corte de Estados Unidos, Distrito Sur de Florida.

Trasfondo

El acusado y ahora convicto Raymond Odigie Uadiale, es un ciudadano estadounidense, nacido en Nigeria, tiene 41 años de edad, y se desempeñaba como ingeniero de redes en Microsoft (Uadiale Nigerian Microsoft Engineer, 2018). Según el *Department of Justice* (2018, August 13) Raymond Odigie Uadiale es residente de Mapple Valley, Washington, y realizó estudios graduados en FIU (Florida International University). Por otra parte, McMahon (2018), agrega que Raymond Odigie Uadiale también fue residente de Miramar, Florida, e impartió cursos de Matemáticas en Miami-Dade College.

Figura 1. Raymond Odigie Uadiale. Recuperado de www.nan.ng.

Las circunstancias bajo las cuales se da el caso se remontan al año 2012, cuando el Centro de Denuncia de Delitos de Internet (IC3) recibe quejas de múltiples víctimas que fueron infectadas con un *malware* que, luego de bloquear sus computadoras, solicitaba el pago de una multa para restaurar el acceso a las mismas (*Federal Bureau of Investigation*, 2012). Es entonces cuando el FBI comienza a publicar una serie de comunicados alertando a la ciudadanía sobre esta nueva amenaza cibernética conocida como Reveton.

Según el comunicado del *Federal Bureau of Investigation* (2012), Reveton es un programa maligno categorizado como *ransomware*. El comunicado indica que este tipo de *malware* es descargado de manera inadvertida por el usuario desde un sitio *web* infectado. Una vez descargado, el programa se instala de manera automática en la computadora y la bloquea inmediatamente. Luego de instalado, el programa muestra una pantalla de presentación con un mensaje, en el cual representa falsamente al FBI o algún otro organismo de ley y orden público (Figura 2). El mensaje presentado indica que la computadora fue asociada a algún tipo de actividad ilegal en Internet y provee instrucciones sobre cómo pagar una multa para proceder a desbloquearla y evitar cargos criminales.

Figura 2. Ransomware Reveton. Recuperado de www.fbi.gov.

Raymond Odigie Uadiale fue acusado de participar en un esquema de lavado de dinero junto a un co-conspirador conocido bajo el seudónimo “K!NG” (Nigerian Network Engineer, 2018). Según descrito en el artículo, “K!NG” distribuyó el ransomware Reveton e infectó múltiples computadoras, mientras que Raymond Odigie Uadiale cobraba los pagos emitidos por las víctimas y se los enviaba a “K!NG”, quien se localizaba en Reino Unido.

Según Neal (2018), este esquema ocurrió entre octubre de 2012 y marzo de 2013, mientras Raymond Odigie Uadiale era estudiante de FIU (Florida International University). Luego de haber finalizado el esquema, Uadiale inició una carrera como ingeniero de redes en Microsoft. Su empleo en Microsoft finalizó cuando fue acusado por lavado de dinero en marzo de 2018 (Neal, 2018).

Las autoridades no han divulgado como se generó la sospecha y, por ende, la captura de Raymond Odigie Uadiale (Nigerian Network Engineer, 2018). Sin embargo, Wei (2013) indica en su artículo que el líder de la ganga detrás de los ataques del *ransomware* Reveton, quien es de

nacionalidad rusa y tiene 27 años, fue arrestado por la Policía Española en Dubai en diciembre de 2012. De igual manera, Wei (2013) agrega que otras 10 personas fueron capturadas como parte dicho operativo.

Aparte de los arrestos, en mayo de 2013, el servicio de moneda virtual Liberty Reserve fue cerrado por las autoridades de Estados Unidos, ante acusaciones de lavado de dinero y otras actividades ilegales (Cloherty, 2013). Según Iannelli (2018), Raymond Odigie Uadiale utilizaba el servicio provisto por Liberty Reserve para perpetrar su esquema de lavado de dinero en complicidad con el sujeto conocido como "K!NG". Según el autor, "K!NG" aún se encuentra en libertad y se desconoce su identidad.

Descripción de hechos

Los hechos se dieron lugar en los Condados de Broward y Miami-Dade, en el Distrito Sur de Florida; y ocurrieron entre octubre de 2012 y el 27 de marzo de 2013 (United States v. Uadiale, 2018a).

A continuación, se esbozan los hechos según descritos en el pliego acusatorio (United States v. Uadiale, 2018a):

1. El co-conspirador 1 distribuyó el *ransomware* Reveton, y recaudó los pagos emitidos en forma de GreenDot MoneyPaks por parte de las víctimas.

2. Raymond Odigie Uadiale obtuvo múltiples tarjetas de débito prepagadas, cuyos números de cuenta envió al co-conspirador 1 mediante mensajería instantánea y utlizando el seudónimo "Mike Roland".

3. El co-conspirador 1 transfirió los fondos de GreenDot MoneyPaks a los números de cuenta de tarjetas de débito prepagadas provistos por Uadiale.

4. El co-conspirador 1, utilizando el seudónimo “K!NG”, envió a Uadiale mediante mensajería instantánea los últimos cuatro dígitos de las tarjetas de débito que habían recibido los pagos, e información sobre la cantidad de dinero correspondiente a cada una. De igual manera, indicaba si alguna tarjeta había sido cancelada por una institución financiera, para que Uadiale le facilitara un número de cuenta adicional.

5. Raymond Odigie Uadiale retiró los fondos de las tarjetas de débito prepagadas desde diversos cajeros automáticos y puntos de venta.

6. Raymond Odigie Uadiale envió al co-conspirador 1 una porción del dinero, según mutuamente acordado, usando el servicio de Liberty Reserve desde una o varias computadoras. La cantidad de dinero enviada por Uadiale al co-conspirador 1 fue el equivalente al 70 % del total de los pagos recibidos por parte de las víctimas del *ransomware*, o aproximadamente $93,640 (*Department of Justice*, 2018, August 13).

7. El 27 de marzo de 2013, Raymond Odigie Uadiale, bajo el seudónimo “Mike Roland”, realizó un envío de $840 desde una cuenta cuyo número terminaba en -0836, a otra cuyo número terminaba en -2547. Dicha transacción se efectuó utilizando el servicio de Liberty Reserve.

Acusaciones, cargos y penalidades

El 22 de marzo de 2018, un Gran Jurado acusó a Raymond Odigie Uadiale de cometer los siguientes delitos:

1. Conspiración para Cometer Lavado de Dinero (18 U.S.C. § 1956(h))

a. Raymond Odigie Uadiale fue acusado de intentar ejecutar y exitosamente completar múltiples transacciones financieras que afectaron el comercio interestatal. Dichas transacciones fueron diseñadas y ejecutadas para encubrir el producto de actividades ilegales.

b. La penalidad máxima para este cargo son 20 años de prisión; una multa de $500,000, y tres años de libertad supervisada.

2. Lavado de dinero (18 U.S.C. § 1956(a)(1)(B)(i))

a. Raymond Odigie Uadiale fue acusado de completar una transacción de $840, la cual fue ejecutada para encubrir el producto de una actividad ilegal.

b. La penalidad máxima para este cargo son 20 años de prisión; una multa de $500,000, y tres años de libertad supervisada.

3. Fraude informático (18 U.S.C. §1030(a)(7))

a. Raymond Odigie Uadiale utilizó una computadora para conspirar y perpetrar su esquema de lavado de dinero. Sin embargo, no se sometieron cargos adicionales por dicha acusación.

El acusado y ahora convicto inicialmente se declaró no culpable de los cargos sometidos, y prestó una fianza de $100,000 el 12 de abril de 2018 (United States v. Uadiale, 2018b). No obstante, el 4 de junio de 2018, el entonces acusado acordó declararse culpable del cargo de

Conspiración para Cometer Lavado de Dinero (18 U.S.C. § 1956(h)), según indicado en el acuerdo de culpabilidad (United States v. Uadiale, 2018c). Como parte de dicho acuerdo, se le retiró el cargo de Lavado de Dinero (18 U.S.C. § 1956(a)(1)(B)(i)). El 13 de agosto de 2018, Raymond Odigie Uadiale fue sentenciado a 18 meses de prisión y tres años de libertad supervisada por el cargo de Conspiración para Cometer Lavado de Dinero (*Department of Justice*, 2018, August 13).

Definición de términos

Fraude: se define fraude como cualquier tipo de crimen perpetrado para obtener ganancias, en el cual se utiliza el engaño como principal modo de operar. El fraude ocurre cuando existe una falsa declaración; se conoce de antemano que la declaración es falsa; la víctima confía en la falsa declaración, y la confianza en dicha declaración produce pérdidas o daños (Wells, 2014).

Fraude Informático: se define fraude informático como cualquier actividad asistida por un dispositivo computadorizado que implica una falsa representación de los hechos mediante la alteración de datos para obtener lucro, y que a la vez causa una pérdida financiera a alguna persona u organización (ACFE, 2018b).

GreenDot Moneypaks: según indicado en el pliego acusatorio (United States v. Uadiale, 2018a), GreenDot MoneyPaks son instrumentos financieros que se pueden cargar en efectivo en diversas ubicaciones físicas en todo Estados Unidos.

Lavado de Dinero: se define como lavado de dinero al mecanismo utilizado para encubrir la existencia, naturaleza, fuente, control, beneficio, propiedad, ubicación y disposición de bienes derivados de actividades delictivas (ACFE, 2018c).

Liberty Reserve: según indicado en el pliego acusatorio (United States v. Uadiale, 2018a), Liberty Reserve era un procesador de pagos en línea que ofrecía un servicio de moneda digital, a

través del cual los usuarios podían convertir los fondos depositados para transferir dinero a otras personas.

Malware: el término *malware* se utiliza para referirse genéricamente a cualquier tipo de *software* maligno (ACFE, 2018d).

Ransomware: se define *ransomware* como un tipo de *software* maligno que bloquea el sistema operativo de un usuario y restringe el acceso a sus datos hasta que se paga un rescate. El *ransomware* a menudo emplea una interfaz profesional convincente, comúnmente adornada con insignias de la policía o un logotipo oficial del gobierno para persuadir mediante intimidación al usuario a pagar un rescate. Dicha intimidación consiste en amenazas de acusación de que el usuario ha sido sorprendido viendo videos ilegales, descargando medios pirateados o accediendo a contenidos prohibidos en Internet (ACFE, 2018e).

Reveton: según definido en el pliego acusatorio (United States v. Uadiale, 2018a), Reveton es un tipo de *ransomware* que infectó computadoras en todo Estados Unidos y otros países. Cuando Reveton infecta la computadora de una víctima, muestra una pantalla de presentación que incluye el logotipo de una agencia de ley y orden público con un mensaje que informa falsamente a la víctima de que en la computadora infectada se encuentra material ilegal. La pantalla de inicio del *ransomware* Reveton dirige a la víctima a pagar una multa para recuperar el acceso a la computadora y sus datos. Muchas veces las víctimas no pueden recuperar su acceso, aun pagando la multa.

SECCIÓN 2: REVISIÓN DE LITERATURA

Introducción

El *Federal Bureau of Investigation* (s.f.) define el Fraude de Internet como el uso de servicios de Internet, o *software* con acceso al mismo, para defraudar o tomar alguna ventaja sobre individuos y/o entidades. Según la ACFE (2018f), la mayoría de los esquemas de fraude perpetrados de manera convencional, ahora han encontrado en Internet su nuevo entorno. En el caso presentado se muestra como el acusado, y ahora convicto, participó de un Fraude de Internet para perpetrar un esquema de lavado de dinero. Dicho lo anterior, la ACFE (2018g) indica que el Fondo Monetario Internacional (FMI) ha estimado el nivel agregado de lavado de dinero entre el dos y el cinco por ciento del Producto Interno Bruto del mundo, lo que equivale a trillones de dólares.

Para propósitos de esta investigación, se utiliza como marco teórico el Árbol del Fraude de Internet, según presentado por Wells (2010). Dicho autor presenta seis tipos principales de Fraude de Internet y sus correspondientes sub-categorías (Figura 3).

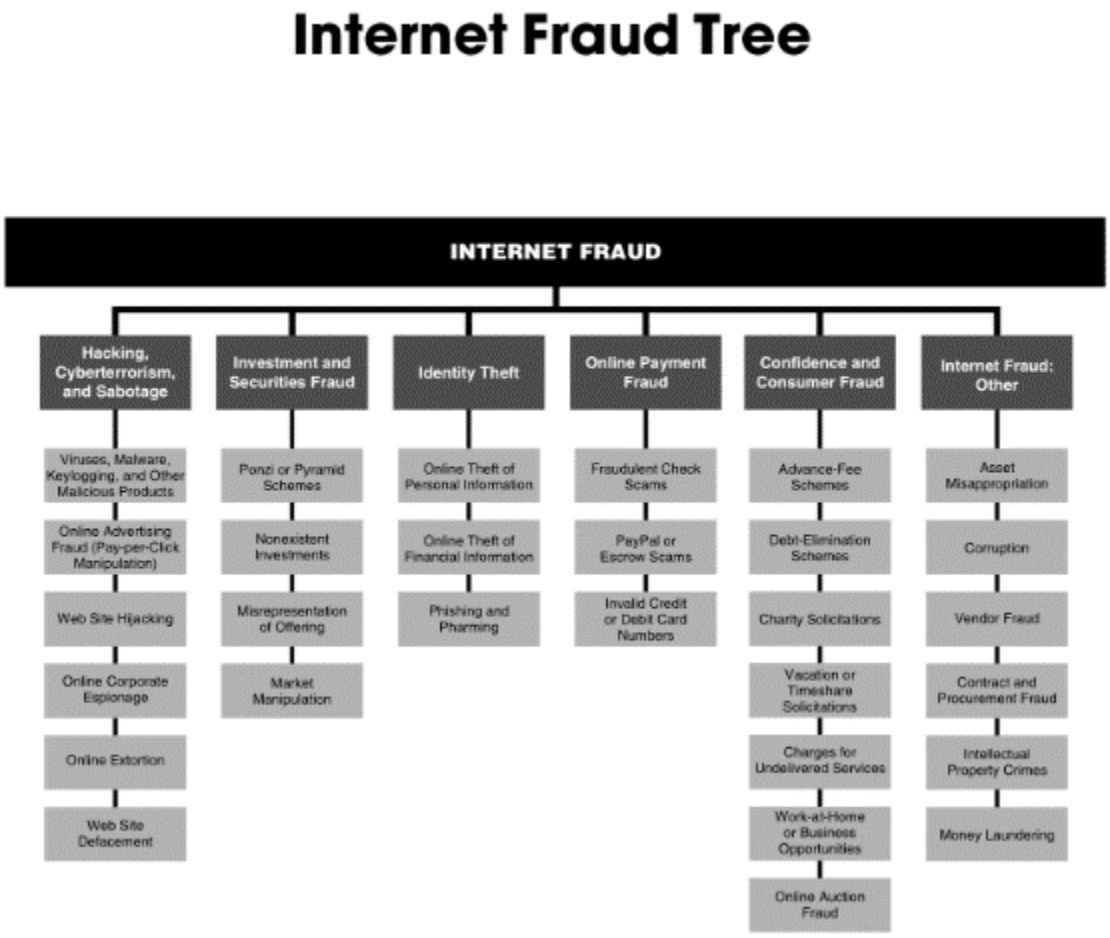


Figura 3. Árbol del Fraude de Internet (Wells, 2010).

El caso presentado contiene elementos de *malware*, extorsión y lavado de dinero. Según Wells (2010), el mismo pudiera clasificarse bajo las categorías de *Hacking, Cyberterrorism, and Sabotage*, e *Internet Fraud: Other*, entre los sub-esquemas cobijados bajo el Árbol del Fraude de Internet. Sin embargo, el contenido de esta sección girará en torno a los delitos por los cuales Raymond Odigie Uadiale fue acusado: lavado de dinero y conspirar para cometer lavado de dinero (United States v. Uadiale, 2018a).

Como se ha definido anteriormente, el lavado de dinero constituye un delito mediante el cual se busca encubrir el origen de activos que son producto de actividades ilegales (ACFE, 2018c). Según Renner (s.f.), un típico esquema de lavado de dinero se compone de las siguientes etapas (Figura 4):

1. **Placement:** es la etapa en la cual los ingresos en efectivo procedentes de actividades delictivas entran al sistema financiero.
2. **Layering:** es la etapa en la cual se transfieren los fondos entre diferentes instrumentos financieros, algunas veces mediante transacciones complejas.
3. **Integration:** es la etapa en la cual se reintroduce el dinero al sistema financiero de manera aparentemente legítima.

Figura 4. Etapas de lavado de dinero (Renner, s.f.)

Fraudes involucrados

El caso estudiado fue de carácter tecnológico con alcance internacional, ya que el lavado de dinero se perpetró mediante transacciones entre Estados Unidos y Reino Unido, haciendo uso de medios electrónicos e instrumentos financieros digitales (United States v. Uadiale, 2018a). Por tales motivos, resultan pertinentes las modalidades de lavado de dinero y delitos relacionados que se esbozan a continuación:

Financiamiento del terrorismo

El financiamiento del terrorismo implica la solicitud, recolección o provisión de fondos con la intención de que los mismos sean utilizados para apoyar actos u organizaciones terroristas. Los fondos pueden provenir de fuentes legales o ilegales. Por lo tanto, el objetivo principal de este tipo de esquema no es necesariamente ocultar las fuentes de dinero, sino ocultar tanto el financiamiento como la naturaleza de la actividad financiada (*International Monetary Fund,* s.f.).

Lavado de dinero basado en comercio internacional (trade-based)

El lavado de dinero basado en comercio internacional se basa en el intercambio de dinero procedente de actividades ilegales por dinero limpio de otros países, mediante la compra y envío de bienes internacionales. Esta es una modalidad emergente que representa un gran reto para las autoridades en cuanto a prevención y detección. (Tie, 2012).

Lavado de dinero virtual

El lavado de dinero virtual es la contraparte digital de su versión tradicional. Según el estudio presentado por CipherTrace (2018), existe una nueva modalidad de hurtar criptomonedas para eventualmente reintegrarlas a la economía formal. Dicho estudio expone que esta tendencia se ha triplicado durante los primeros seis meses del 2018, en comparación con todo el año 2017

(Figura 5). CipherTrace (2018) destaca en su estudio al Bitcoin como la criptomoneda predilecta de los criminales.

Figura 5. Valor en criptomonedas virtuales hurtadas (CipherTrace, 2018).

Según CipherTrace (2018), el lavado de criptomonedas es realizado por entidades que se dedican a proveer dicho servicio, a quienes se les conoce como *mixers*, *tumblers*, *foggers* y *laundries.* CipherTrace (2018) explica en su estudio que el trabajo de estos proveedores de servicios consiste en mezclar todos los fondos hurtados con el objetivo de obscurecer sus orígenes, para luego reintegrarlos al ecosistema virtual como dinero limpio (Figura 6). CipherTrace (2018) agrega que los proveedores de dicho servicio generalmente cobran entre un uno y tres por ciento del total de la transacción efectuada.

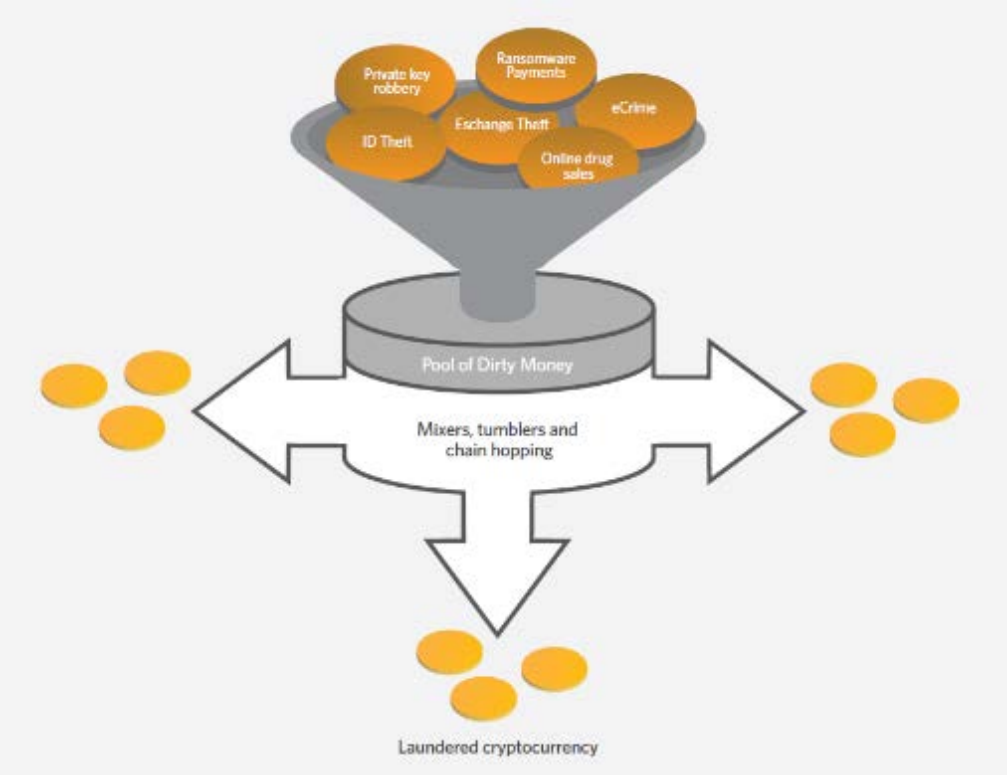


Figura 6. Lavado de dinero virtual (CipherTrace, 2018).

Money Muling

Según Gray (2018), esta modalidad consiste en reclutar individuos para recibir y transferir dinero robado; de manera que se pueda evitar la detección del esquema y ocultar la identidad de los malversadores. En ocasiones, se utilizan técnicas de ingeniería social para reclutar a desempleados, estudiantes y otras personas con dificultades económicas, haciéndoles creer que se les está ofreciendo una oportunidad legítima de empleo. Gray (2018) agrega que solo en el Reino Unido, se perdieron más de £ 100 millones ($132.3 millones) en esquemas de lavado de dinero mediante *money muling* durante los primeros seis meses de 2017; representando una pérdida promedio de £ 21,477 ($28,409) para víctimas comerciales.

Tráfico humano

Según Mundie (2012), el tráfico humano se ha convertido en una actividad muy lucrativa y prevalente que ocupa el tercer lugar como fuente de ingresos para el crimen organizado, luego del tráfico de drogas y armas. En su investigación, Mundie (2012) expone que los traficantes de personas en las Américas hacen uso de diversos recursos para lavar dinero proveniente de dicha actividad. Entre los recursos más utilizados por los traficantes de personas para lavar dinero se destacan los casinos, empresas de importación y exportación, negocios que ofrecen servicios financieros, transferencias electrónicas y pagos en línea (Mundie, 2012).

Leyes aplicables

A continuación, se esbozan los estatutos aplicables al caso estudiado (United States v. Uadiale, 2018a):

- Según el estatuto Fraud and Related Activity in Connection With Computers (18 U.S.C. §1030), cualquier persona que con intención de extorsionar a otra a cambio de dinero u otra cosa de valor, transmita una comunicación mediante el comercio interestatal o internacional haciendo uso excesivo o no autorizado de una computadora, y la misma contenga amenaza de causar daño a una computadora o a sus datos, será castigado con una multa o prisión por no más de cinco años, o ambos, en caso de una primera convicción; o una multa o prisión por no más de 10 años, o ambos, en caso de reincidencia.
- Según el estatuto Laundering of Monetary Instruments (18 U.S.C. § 1956), cualquier persona que realiza una transacción financiera, sabiendo que la propiedad involucrada en la misma representa el producto una actividad ilegal, y que dicha transacción tiene como propósito ocultar la procedencia de dicha propiedad, será castigado con una

> multa de $500,000 o el doble del valor de la propiedad involucrada en la transacción, la que sea mayor, o prisión por no más de 20 años o ambos. Adicional a ello, cualquier persona que conspire para cometer dicha ofensa estará sujeta a las mismas penalidades que las prescritas para la ofensa cuya comisión fue objeto de la conspiración.

Casos relacionados

United States v. Liberty Reserve (13-CR-368), Southern District of New York

Según publicado por el *Department of Justice* (2016, May 6), en el 2001 Arthur Budovsky fundó la compañía Liberty Reserve, la cual estuvo operacional desde el 2005 hasta el 2013. Según el comunicado de prensa, Liberty Reserve se fundó como un servicio de moneda digital exclusivamente diseñado para facilitar operaciones de lavado de dinero en escala masiva a nivel internacional.

Según el pliego acusatorio (United States v. Liberty Reserve, 2013), Budovsky, junto a otros seis co-conspiradores, fueron acusados por los cargos de conspiración para cometer lavado de dinero; conspiración para operar negocios de transmisión de dinero sin licencia, y operación de un negocio de transmisión de dinero sin licencia. Según el *Department of Justice* (2016, May 6), Budovsky fue arrestado en mayo de 2013 y extraditado a los Estados Unidos en octubre de 2014. El 6 de mayo de 2016 Budovsky fue sentenciado a 20 años de prisión por conspirar para cometer lavado de dinero, luego de haberse declarado culpable por dicho cargo el 29 de enero de 2016 (*Department of Justice*, 2016, May 6).

Los servicios de Liberty Reserve fueron utilizados por Raymond Uadiale junto a su co-conspirador para perpetrar el mencionado esquema de lavado de dinero (United States v. Uadiale, 2018a). Por lo tanto, el caso de Liberty Reserve guarda una estrecha relación con el de Raymond Uadiale.

United States v. Stanislav Nazarov (1:17-CR-00018-CKK), District of Columbia

Según publicado por el *Department of Justice* (2018, March 6), un ciudadano ruso e israelí de 46 años llamado Stanislav Nazarov, participó de un esquema de lavado de dinero internacional perpetrado desde el 2013 al 2015. Según el pliego acusatorio (United States v. Nazarov, 2017), la participación de Nazarov, cuyo rol en dicho esquema sería de facilitador y coordinador, consistió en proveer a otros cuatro co-conspiradores diversas cuentas bancarias las cuales serían utilizadas para depositar dinero procedente de actividades ilegales. Como parte del esquema perpetrado, los co-conspiradores enviaron un correo electrónico al director de una compañía, bajo el cual se representaba falsamente al dueño de la misma, y se le exhortaba al director a comprar acciones de una empresa basada en Estados Unidos. Luego de haber recibido dicho correo electrónico, el director de la compañía víctima transfirió la cantidad de $1.4 millones a una cuenta de banco en Estados Unidos. Como resultado de dicha transacción, Nazarov recibió $50,000 los cuales fueron transferidos a una cuenta bancaria en Rusia y luego a Israel, donde Nazarov residía.

Según el informe del *Department of Justice* (2018, March 6), en marzo de 2017 Nazarov fue arrestado en Israel, y en el 12 de diciembre de 2017 se declaró culpable por el cargo de Conspiración para Cometer Lavado de Dinero. El 5 de marzo de 2018 Nazarov fue sentenciado a 18 meses en prisión por conspirar para cometer lavado de dinero. Adicional a ello, se le ordenó restituir la cantidad de $50,000.

Este caso se asemeja al estudiado (United States v. Uadiale, 2018a) en que ambos implicados asumieron un rol de facilitador en el esquema correspondiente. De igual manera, ambos utilizaron la tecnología como herramienta de engaño. En el caso de Uadiale se utilizó un *ransomware* para extorsionar a las víctimas a pagar una supuesta multa; mientras que en el caso de Nazarov, se utilizó una técnica de *phishing* mediante correo electrónico para persuadir a la víctima a transferir dinero como parte de una supuesta compra de acciones.

United States v. Kerby Rigaud (1:17-CR-00323), Northern District of Georgia

Según publicado por el *Department of Justice* (2018, July 26), Kerby Rigaud, de 27 años y residente de Georgia, participó de un esquema de fraude de correos electrónicos dirigido a negocios, conocido como *Business Email Compromise (BEC).* Este esquema ocurrió entre abril del 2015 y abril del 2016, e impactó a víctimas en el Distrito Norte de Georgia y otras partes de Estados Unidos.

Según el comunicado de prensa del *Department of Justice* (2018, July 26), Kerby Rigaud y sus co-conspiradores enviaron correos electrónicos impersonando a representantes bancarios y otras fuentes de confianza a diversos negocios, persuadiendo a las víctimas a transferir cuantiosas cantidades de dinero a cuentas de banco específicas. Los perpetradores lograron acceso no autorizado a las cuentas de correo electrónico de dichas entidades y/o falsificaron las mismas según necesario para perpetrar este esquema. De igual manera, Rigaud reclutó varios individuos con el propósito de que prestaran sus cuentas bancarias para recibir dichas cantidades de dinero, las cuales serían luego depositadas a otras instituciones financieras localizadas en Asia. Mediante este esquema, Rigaud junto a sus co-conspiradores, hurtaron sobre un millón de dólares.

Según el *Department of Justice* (2018, July 26), Rigaud fue acusado por los delitos de conspiración para cometer fraude electrónico, conspiración para cometer fraude bancario y conspiración para cometer lavado de dinero. Por estos cargos, Rigaud fue sentenciado a dos años y tres meses de prisión, seguido de tres años de libertad supervisada y la restitución de $176,059.03.

Este caso se asemeja al estudiado (United States v. Uadiale, 2018a) en el uso de la tecnología como herramienta para defraudar. De igual manera, en ambos se utilizaron recursos internacionales como personas e instrumentos financieros para perpetrar el lavado de dinero. Sin embargo, este caso se distingue de todos los antes mencionados en este trabajo por el uso de *e-mail hacking* por parte de los perpetradores.

Herramientas de investigación

En el caso de Raymond Uadiale, al igual que en los relacionados, se perpetraron diversidad de ataques cibernéticos con el único fin de adquirir dinero fraudulentamente de parte de sus víctimas. El común denominador de todos los casos estudiados en este trabajo fue la sentencia por el cargo de conspiración para cometer lavado de dinero. Basado en ello, necesitamos la disponibilidad de herramientas de examinación forense que nos ayuden a demostrar la intención o participación del acusado en la conspiración para perpetrar el delito de lavado de dinero.

A continuación, se esbozan las herramientas de examinación forense utilizadas para el análisis de este caso. De igual forma, se incluye otro *software* de apoyo para dicha tarea.

- **ProDiscover Basic:** es una herramienta de obtención de imágenes diseñada para operar bajo los requerimientos de NIST, y que incorpora generación de reportes para presentar hallazgos como evidencia de procedimientos legales (ARC Group, 2018).

- **OSFMount:** es una herramienta que permite montar archivos de imagen como *read-only* para ser analizados con el programa OSForensics (PassMark Software, 2018a).
- **OSForensics:** es una herramienta que permite extraer evidencia forense de las computadoras rápidamente con búsquedas de archivos de alto rendimiento e indexación. De igual manera, con esta herramienta se pueden identificar correos electrónicos, datos binarios, archivos y actividades sospechosas con comparaciones de hash (PassMark Software, 2018b).
- **ClamWin AV:** es un programa antivirus de código abierto para Microsoft Windows. Esta herramienta ofrece altas tasas de detección de *malware* y realiza descargas automáticas de actualizaciones (ClamWin, 2018).
- **Beyond Compare:** es un programa que permite comparar directorios y archivos para identificar cambios y diferencias en los datos (Scooter Software, 2018).

SECCIÓN 3: SIMULACIÓN

Introducción

En esta sección se busca reconstruir la secuencia de los hechos que involucraron al acusado y ahora convicto Raymond Odigie Uadiale en el esquema de lavado de dinero perpetrado, según descrito en el caso estudiado. Tal como se ha discutido en esta investigación, Uadiale, fungiendo como agente facilitador, conspiró junto a un sujeto conocido como "K!NG" para extorsionar las víctimas de un *ransomware*, con el fin de adquirir dinero de las mismas y luego encubrir la procedencia del mismo. A base de la información expuesta en el caso (United States v. Uadiale, 2018a), se presenta la teoría sobre los hechos del esquema y el rol de los perpetradores dentro del mismo.

Teoría del esquema

El esquema de lavado de dinero perpetrado por Raymond Uadiale y su co-conspirador, conocido bajo el seudónimo "K!NG", fue un proceso cíclico que se estuvo ejecutando entre octubre de 2012 y el 27 de marzo de 2013. Dicho proceso inicia cuando Raymond Uadiale abre varias cuentas de tarjetas de débito prepagadas en diversas instituciones financieras en los Estados Unidos. Luego, adoptando el seudónimo "Mike Roland", Uadiale procede a enviar los números de cuenta a "K!NG" por mensajería instantánea. Una vez "K!NG" adquiere los números de cuenta, comienza a depositar en las mismas los pagos de las víctimas del *ransomware* Reveton. Luego "K!NG" envía a Uadiale mediante mensajería instantánea los números de cuenta de las tarjetas utilizadas y la cantidad depositada en cada una. En este punto, "K!NG" comunica a Uadiale si alguna tarjeta había sido cancelada, y le instruye que adquiera una cuenta adicional, la cual sería enviada junto a otras más en la próxima ronda. Uadiale recibe la información provista por "K!NG" y procede a retirar el dinero de diversos cajeros

automáticos. Luego entra al portal de Liberty Reserve, y utilizando dicho servicio, envía la cantidad correspondiente al 70 % del dinero retirado a “K!NG”.

En la Figura 7 se presenta un flujograma que expone la secuencia de los hechos del esquema y el rol de los perpetradores.

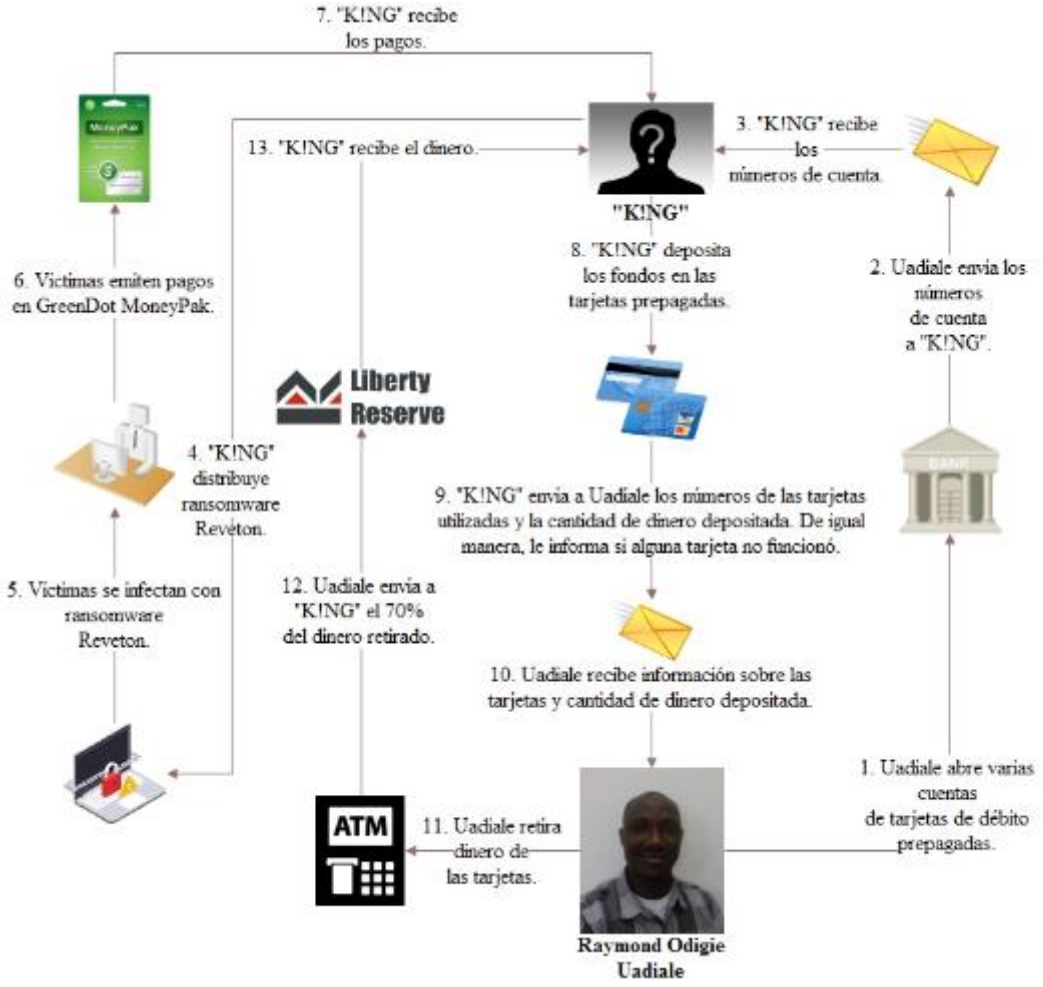


Figura 7. Esquema de lavado de dinero.

SECCIÓN 4: INFORME DEL CASO

Resumen ejecutivo

William Joss Nichols, Fiscal de la División de Delitos Informáticos y Propiedad Intelectual del Distrito de Columbia, delegó en LAG CyberForensics el análisis del disco duro de una computadora incautada durante un allanamiento realizado por el FBI en Maple Valley, Washington. Según indicado, esta pieza de evidencia corresponde a una investigación relacionada a un esquema de lavado de dinero perpetrado en el comercio interestatal e internacional mediante el uso de dispositivos digitales.

Como resultado de la examinación realizada al disco duro, se identificaron diversos documentos personales, entre los que se incluyen archivos de texto, hojas de cálculo, bitácoras de conversaciones y correos electrónicos. Dichos hallazgos relacionan al acusado con el esquema de lavado de dinero investigado.

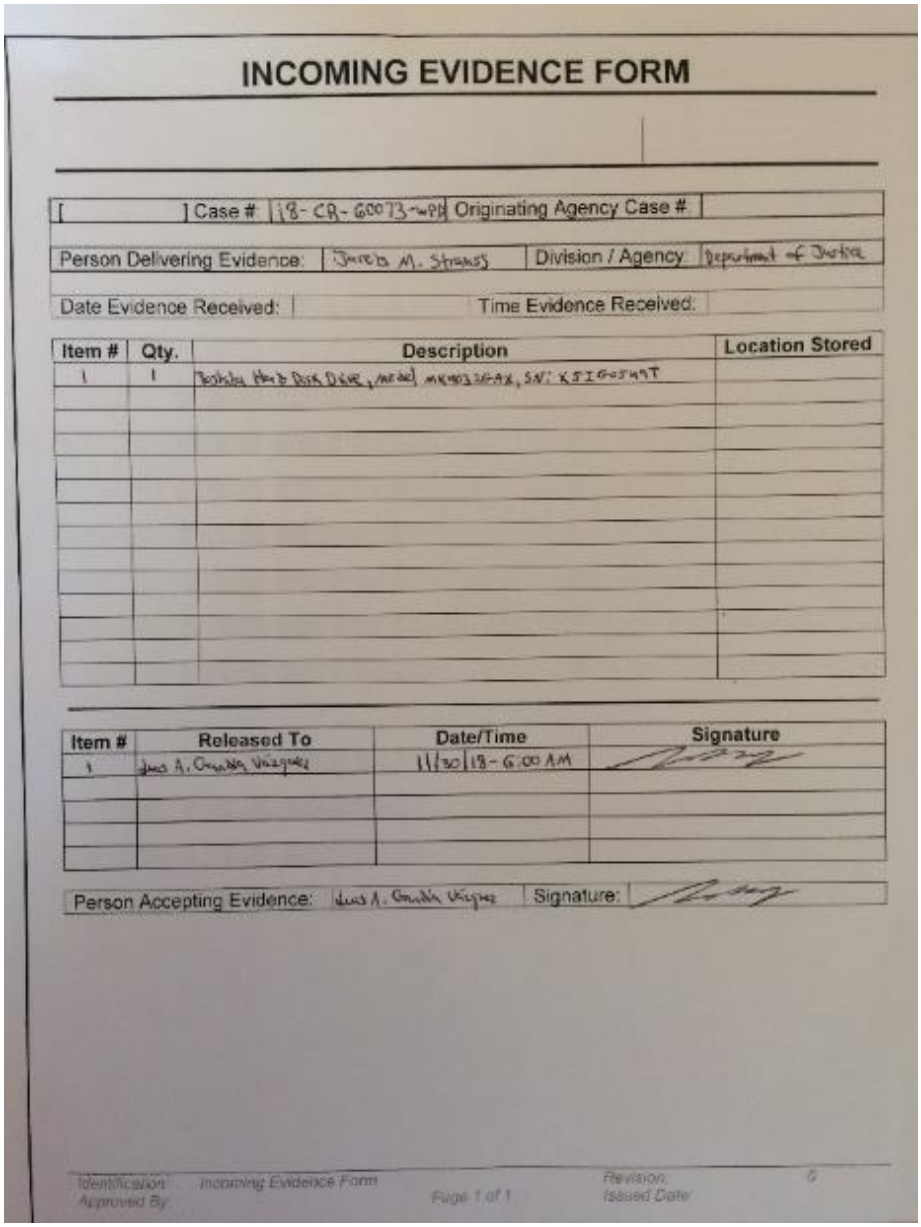
Luego de completarse la examinación, el disco duro fue devuelto al Fiscal Asistente de la Corte de Distrito Sur de Florida, Jared M. Strauss. Junto a la pieza de evidencia, se entregó copia digital de los documentos identificados y el informe de los análisis.

Objetivo

Los servicios de LAG CyberForensics fueron contratados por la fiscalía de la Corte de Distrito Sur de Florida para ejecutar una examinación forense al contenido del disco duro de una computadora incautada por el FBI como parte de una investigación. Esto con el propósito de identificar evidencia inculpatoria que muestre la participación del acusado, Raymond Odigie Uadiale, en un esquema de lavado de dinero perpetrado por medio de dispositivos electrónicos.

Alcance del trabajo

El 30 de noviembre de 2018, el Fiscal Asistente Jared M. Strauss, hizo entrega al examinador forense Luis A. Gandía Vázquez, de un disco duro marca Toshiba, identificado como *Item No. 2018-EV-01* (Figura 8 y Figura 9). Dicho dispositivo fue removido de una computadora incautada por el Agente Especial Matthew J. DeSarno, en Maple Valley, Washington.



INCOMING EVIDENCE FORM

Case # 18-CR-00073-wPH Originating Agency Case #

Person Delivering Evidence: Jared M. Strauss Division / Agency: Department of Justice

Date Evidence Received: Time Evidence Received:

Item #	Qty.	Description	Location Stored
1	1	Toshiba Hard Disk Drive, model MK3033GAX, SN: K5I6G5T9T	

Item #	Released To	Date/Time	Signature
1	Luis A. Gandía Vázquez	11/30/18 - 6:00 AM	

Person Accepting Evidence: Luis A. Gandía Vázquez Signature:

Identification Approved By: Incoming Evidence Form Page 1 of 1 Revision: Issued Date: 6

Figura 8. Recibo de evidencia.

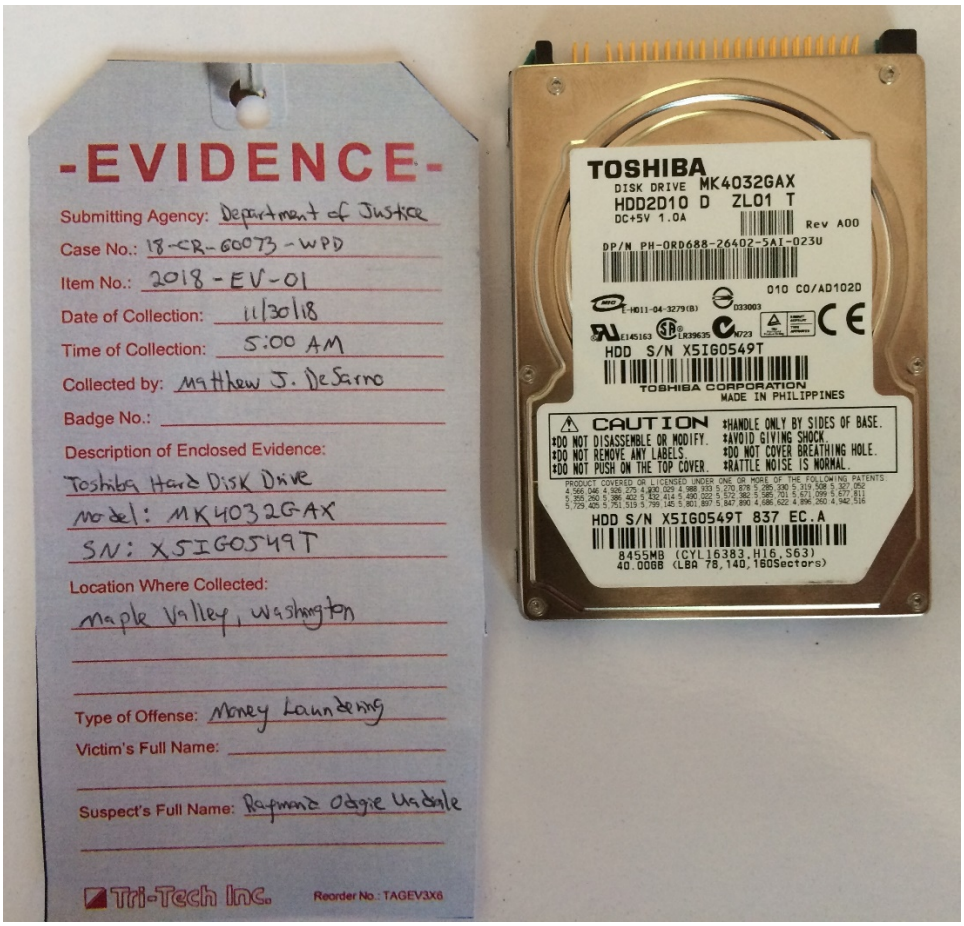


Figura 9. Disco duro marca Toshiba junto identificación de evidencia.

Esta entrega se hizo bajo la encomienda de que se genere una imagen íntegra del disco duro para obtener y analizar todos los datos (existentes y borrados) que albergan en el mismo, de manera que se puedan identificar piezas de evidencia relacionada al caso de lavado de dinero bajo investigación. Conforme los estándares de la investigación forense digital, esta tarea se ejecutó utilizando las herramientas ProDiscover Basic, OSForensics y OSFMount. De igual manera, se utilizó el programa ClamWin AV para identificar cualquier archivo de *malware* presente en el disco duro analizado; y el *software* Beyond Compare, para comparar los datos albergados en diferentes archivos de texto. Adicional a ello, se utilizó un USB Write Blocker y una bolsa anti-estática durante el proceso de análisis para asegurar la integridad física y lógica de

la pieza de evidencia.

Datos del caso

1. Número de caso: 18-CR-60073-WPD
2. Investigador: Luis A. Gandía Vázquez
3. Cliente: Departamento de Justicia de Estados Unidos
4. Representante del cliente: William Joss Nichols, Fiscal.

Descripción de los dispositivos utilizados

A continuación, se detallan los dispositivos que fueron utilizados en el proceso de examinación forense:

1. Computadora HP Notebook, modelo HP 15-ba018wm, con procesador AMD Quad-Core de 1.8 GHz, 4GB de RAM y sistema operativo Windows 7 Professional SP1 32bit (Figura 10). Esta computadora alberga todas las herramientas que fueron utilizadas para el proceso de examinación forense.

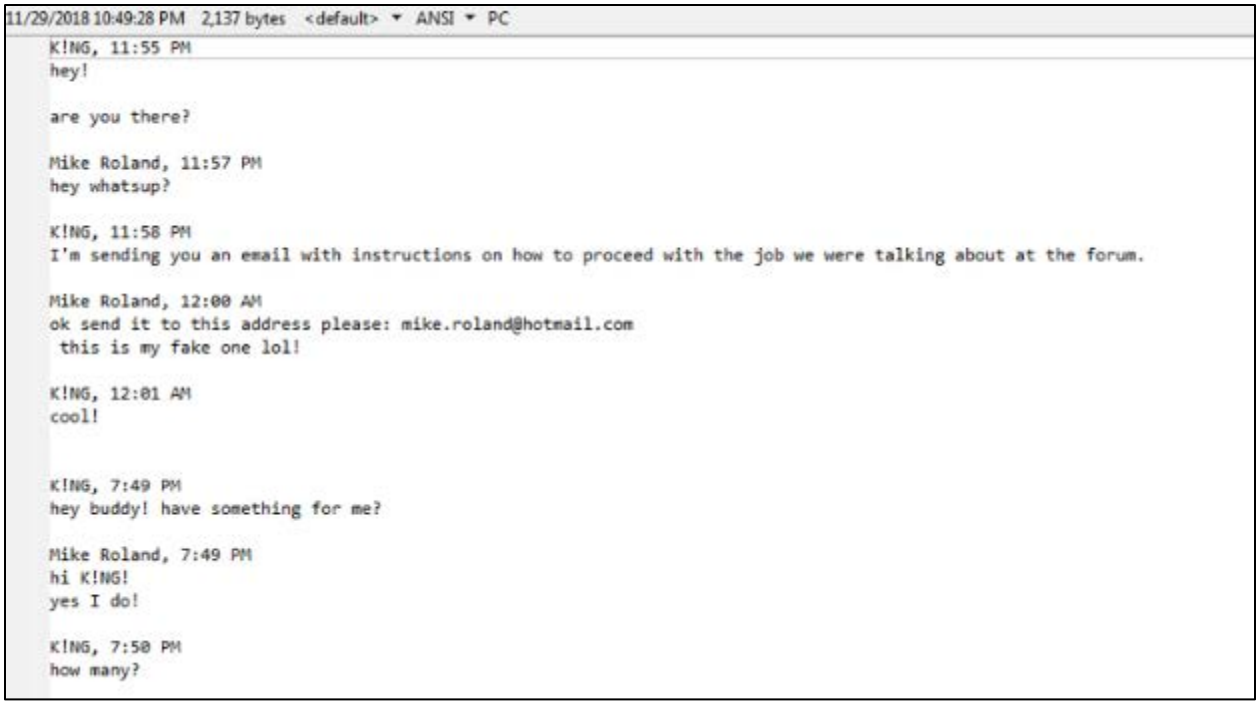
Figura 10. Ambiente de examinación forense.

2. Disco duro marca Toshiba, modelo MK4032GAX, con 37 GB de capacidad, número de serie X5IG0549T, e identificado como *Item No. 2018-EV-01* (Figura 9).
3. Cable convertidor de USB 2.0 a SATA/IDE, marca C2G.
4. USB Write Blocker, marca WiebeTech.
5. Bolsa anti-estática, marca genérica.

Resumen de hallazgos

A continuación, se presentan los hallazgos identificados durante la examinación forense del disco duro *(Item No. 2018-EV-01)* entregado por el Fiscal Asistente Jared M. Strauss:

1. Conversación inicial por la plataforma Skype (Figura 11). "K!NG" comunica a Raymond Uadiale, aka "Mike Roland", que le enviará instrucciones por correo electrónico en relación a un "trabajo". "Mike" procede a compartir su correo y le indica que es su dirección falsa.



11/29/2018 10:49:28 PM 2,137 bytes <default> ANSI PC

K!NG, 11:55 PM
hey!

are you there?

Mike Roland, 11:57 PM
hey whatsup?

K!NG, 11:58 PM
I'm sending you an email with instructions on how to proceed with the job we were talking about at the forum.

Mike Roland, 12:00 AM
ok send it to this address please: mike.roland@hotmail.com
this is my fake one lol!

K!NG, 12:01 AM
cool!

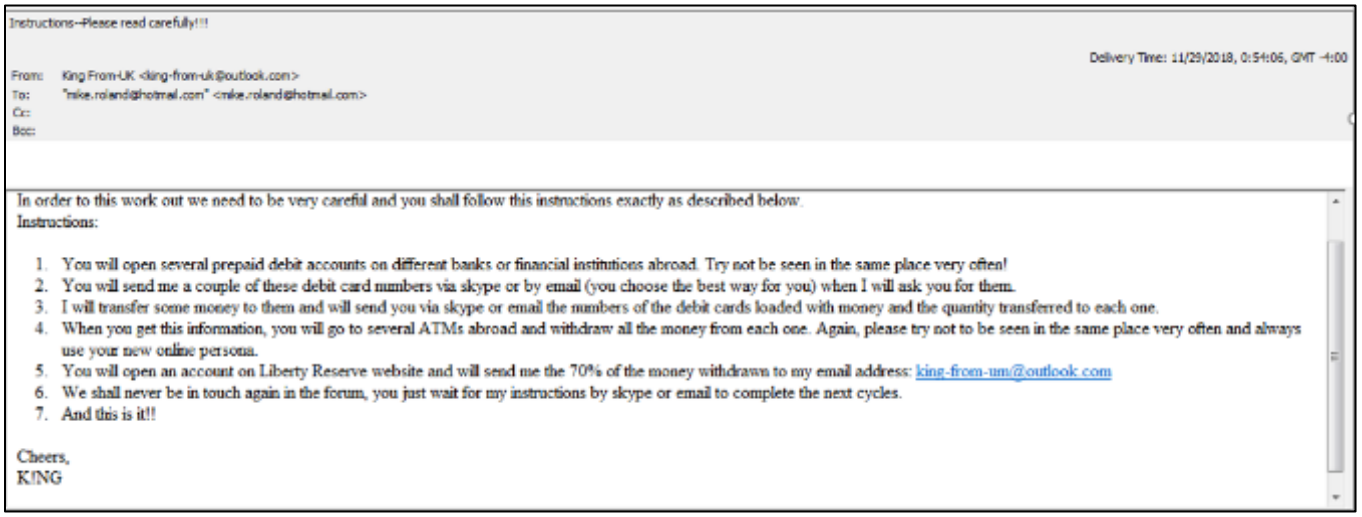
K!NG, 7:49 PM
hey buddy! have something for me?

Mike Roland, 7:49 PM
hi K!NG!
yes I do!

K!NG, 7:50 PM
how many?

Figura 11. Conversación inicial por Skype.

2. Primer correo electrónico (Figura 12). Raymond Uadiale, aka "Mike Roland", recibe instrucciones detalladas por parte de "K!NG" sobre como operar el esquema.



Instructions--Please read carefully!!!

Delivery Time: 11/29/2018, 0:54:06, GMT -4:00

From: King From-UK <king-from-uk@outlook.com>
To: "mike.roland@hotmail.com" <mike.roland@hotmail.com>
Cc:
Bcc:

In order to this work out we need to be very careful and you shall follow this instructions exactly as described below.
Instructions:

1. You will open several prepaid debit accounts on different banks or financial institutions abroad. Try not be seen in the same place very often!
2. You will send me a couple of these debit card numbers via skype or by email (you choose the best way for you) when I will ask you for them.
3. I will transfer some money to them and will send you via skype or email the numbers of the debit cards loaded with money and the quantity transferred to each one.
4. When you get this information, you will go to several ATMs abroad and withdraw all the money from each one. Again, please try not to be seen in the same place very often and always use your new online persona.
5. You will open an account on Liberty Reserve website and will send me the 70% of the money withdrawn to my email address: king-from-um@outlook.com
6. We shall never be in touch again in the forum, you just wait for my instructions by skype or email to complete the next cycles.
7. And this is it!!

Cheers,
K!NG

Figura 12. Primer correo electrónico.

3. Segundo correo electrónico (Figura 13). "K!NG" envía su dirección de correo electrónico corregida a Uadiale. De igual manera, en dicho mensaje se puede apreciar una respuesta anterior de Uadiale hacia "K!NG" concerniente a la obtención de unas tarjetas de débito.

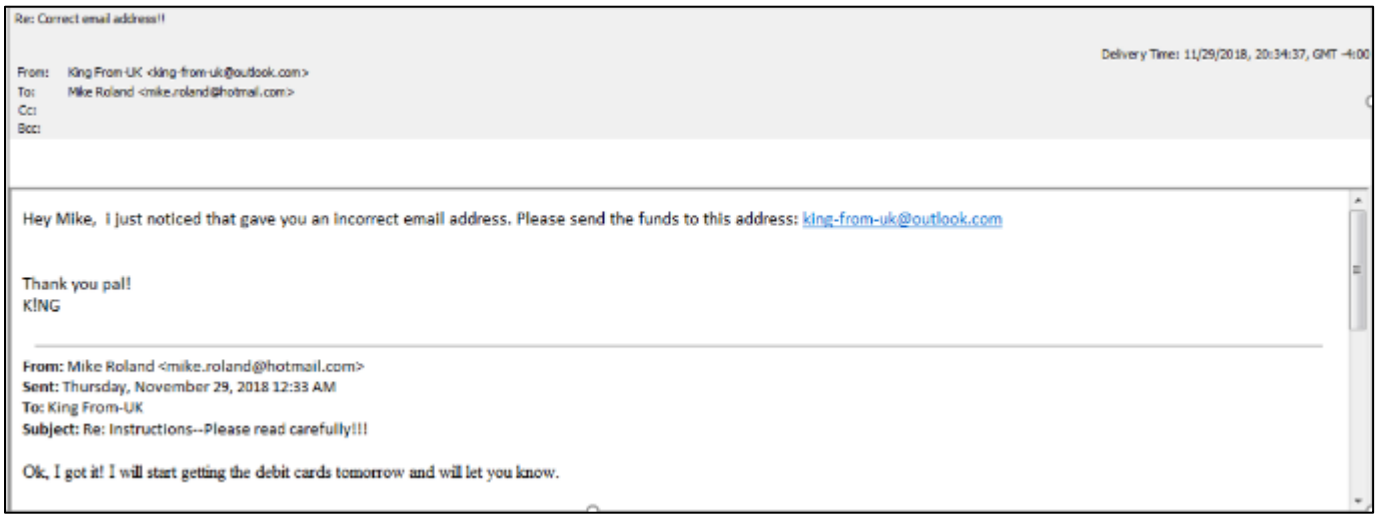
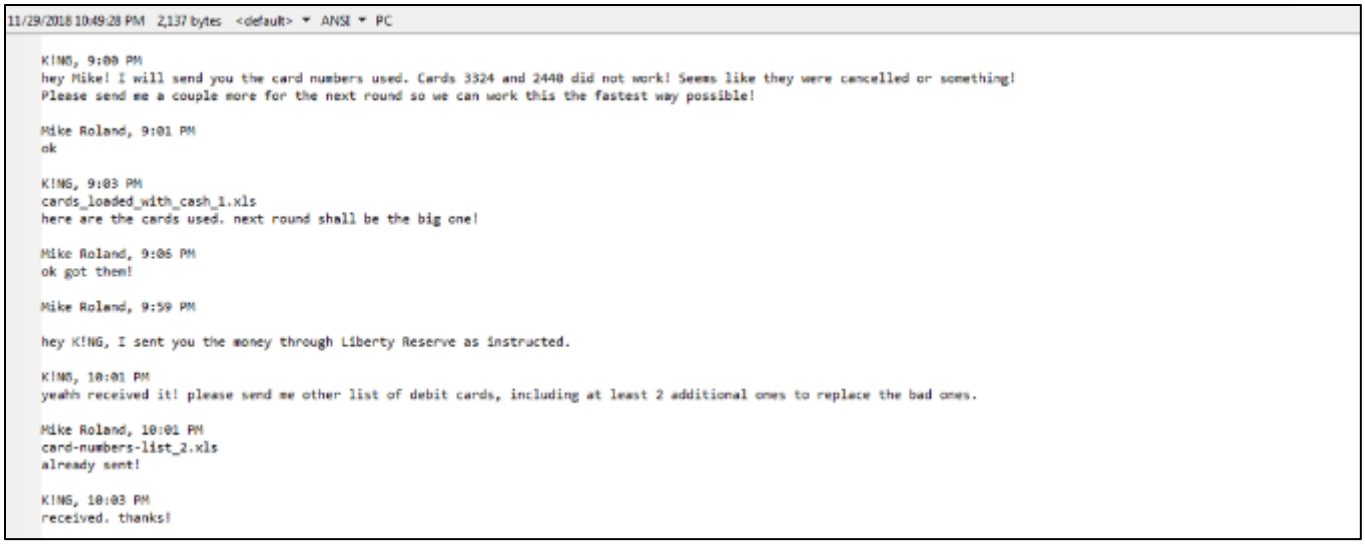


Figura 13. Segundo correo electrónico.

4. Penúltima conversación por la plataforma Skype (Figura 14). Uadiale y "K!NG" intercambian archivos de Microsoft Excel con información sobre tarjetas de débito cargadas con efectivo y números de cuenta disponibles para continuar con el esquema.



11/29/2018 10:49:28 PM 2,137 bytes <default> ANSI PC

K!NG, 9:00 PM
hey Mike! I will send you the card numbers used. Cards 3324 and 2440 did not work! Seems like they were cancelled or something!
Please send me a couple more for the next round so we can work this the fastest way possible!

Mike Roland, 9:01 PM
ok

K!NG, 9:03 PM
cards_loaded_with_cash_1.xls
here are the cards used. next round shall be the big one!

Mike Roland, 9:06 PM
ok got them!

Mike Roland, 9:59 PM

hey K!NG, I sent you the money through Liberty Reserve as instructed.

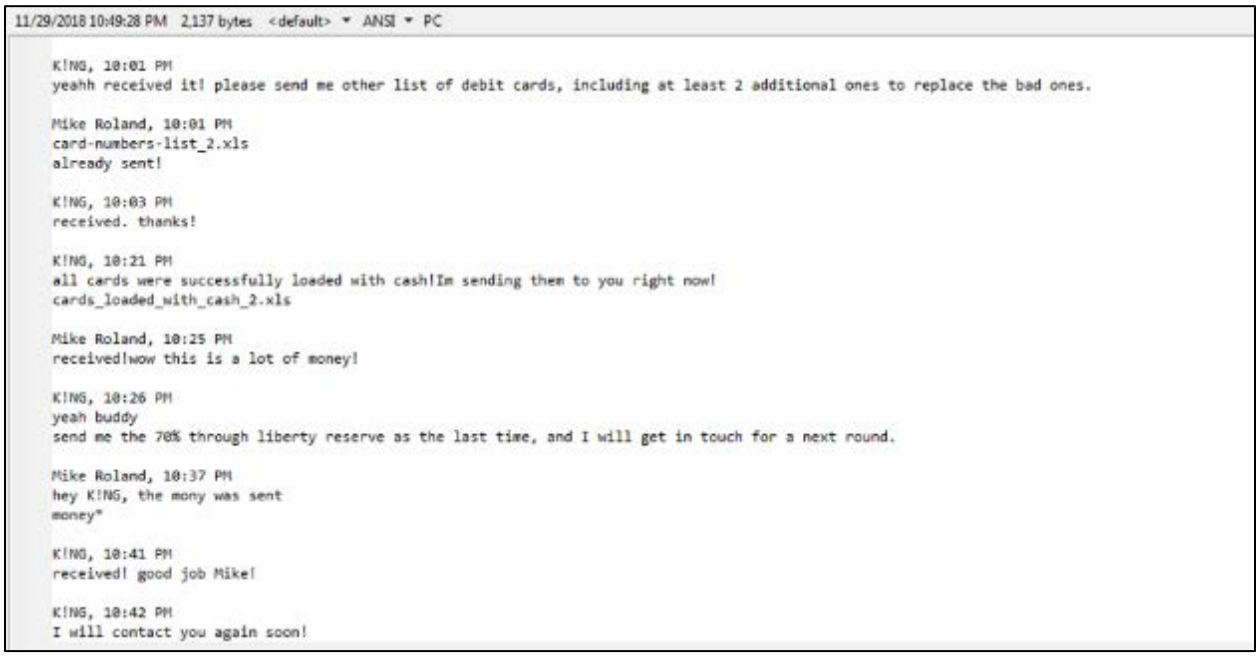
K!NG, 10:01 PM
yeahh received it! please send me other list of debit cards, including at least 2 additional ones to replace the bad ones.

Mike Roland, 10:01 PM
card-numbers-list_2.xls
already sent!

K!NG, 10:03 PM
received. thanks!

Figura 14. Penúltima conversación por Skype.

5. Última conversación por la plataforma Skype (Figura 15). Uadiale recibe otro archivo de Microsoft Excel con información sobre más tarjetas de débito cargadas con efectivo. En este mensaje, “K!NG” imparte instrucciones finales a Uadiale y este le confirma el envío de dinero a su cuenta por medio de Liberty Reserve.



11/29/2018 10:49:28 PM 2,137 bytes <default> ANSI PC

K!NG, 10:01 PM
yeahh received it! please send me other list of debit cards, including at least 2 additional ones to replace the bad ones.

Mike Roland, 10:01 PM
card-numbers-list_2.xls
already sent!

K!NG, 10:03 PM
received. thanks!

K!NG, 10:21 PM
all cards were successfully loaded with cash!Im sending them to you right now!
cards_loaded_with_cash_2.xls

Mike Roland, 10:25 PM
received!wow this is a lot of money!

K!NG, 10:26 PM
yeah buddy
send me the 70% through liberty reserve as the last time, and I will get in touch for a next round.

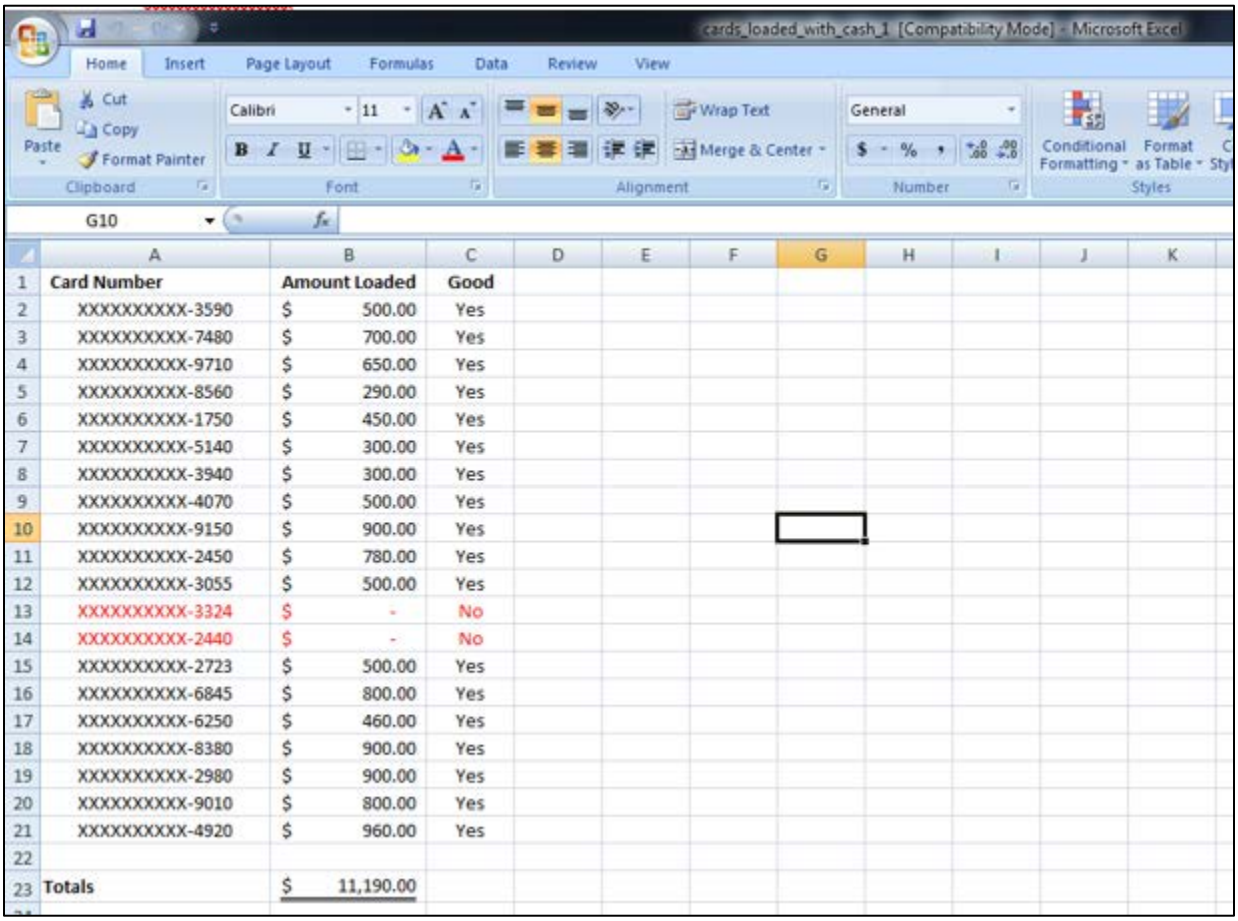
Mike Roland, 10:37 PM
hey K!NG, the mony was sent
money"

K!NG, 10:41 PM
received! good job Mike!

K!NG, 10:42 PM
I will contact you again soon!

Figura 15. Última conversación por Skype.

6. Archivo de Microsoft Excel identificado como *cards_loaded_with_cash_1.xls.* (Figura 16). Este archivo fue hallado en el directorio *Downloads*, del perfil de usuario de Uadiale. Este archivo detalla las tarjetas de débito cargadas con fondos, los cuales serían transferidos a "K!NG" mediante Liberty Reserve.

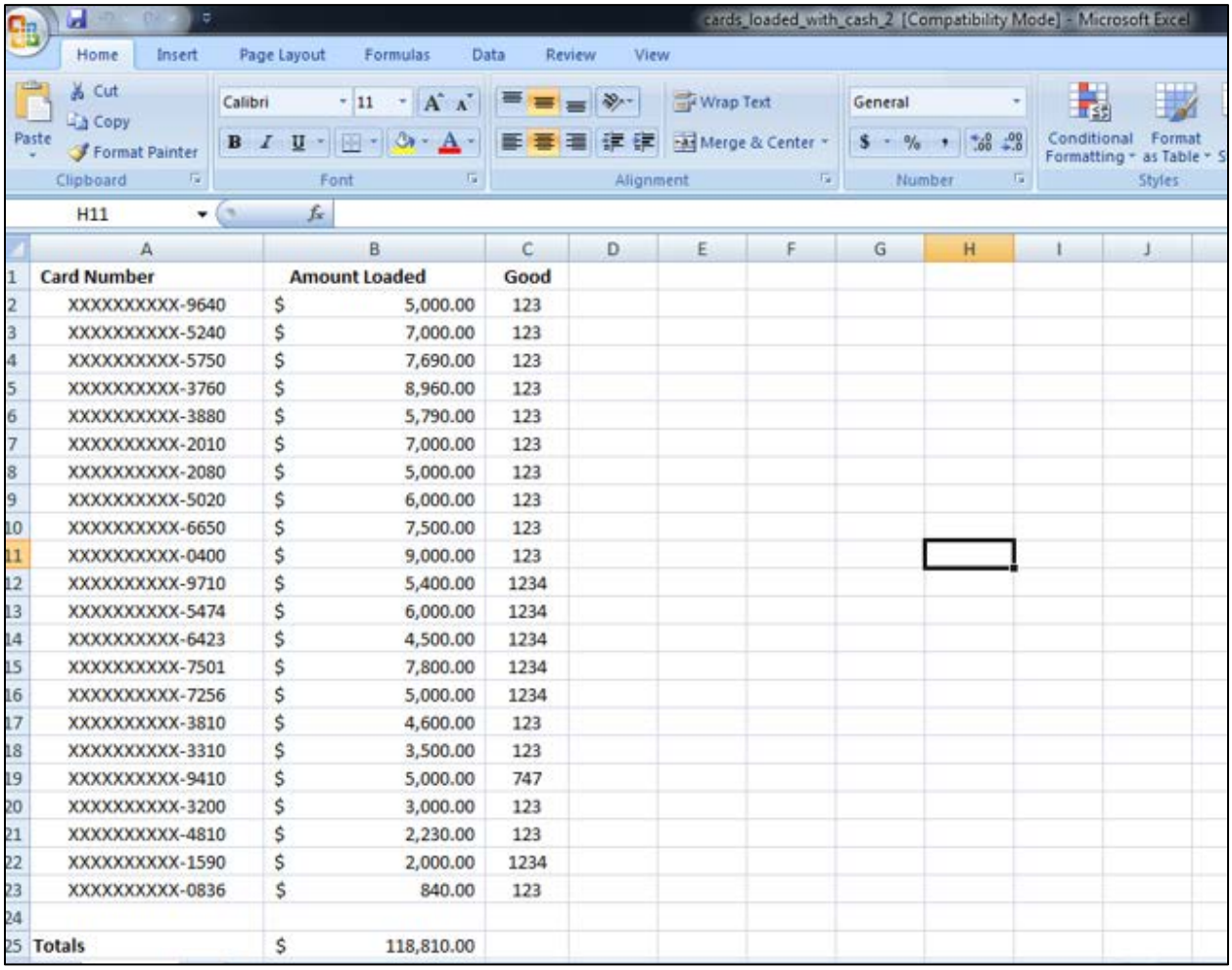


	A	B	C
1	**Card Number**	**Amount Loaded**	**Good**
2	XXXXXXXXXX-3590	$ 500.00	Yes
3	XXXXXXXXXX-7480	$ 700.00	Yes
4	XXXXXXXXXX-9710	$ 650.00	Yes
5	XXXXXXXXXX-8560	$ 290.00	Yes
6	XXXXXXXXXX-1750	$ 450.00	Yes
7	XXXXXXXXXX-5140	$ 300.00	Yes
8	XXXXXXXXXX-3940	$ 300.00	Yes
9	XXXXXXXXXX-4070	$ 500.00	Yes
10	XXXXXXXXXX-9150	$ 900.00	Yes
11	XXXXXXXXXX-2450	$ 780.00	Yes
12	XXXXXXXXXX-3055	$ 500.00	Yes
13	XXXXXXXXXX-3324	$ -	No
14	XXXXXXXXXX-2440	$ -	No
15	XXXXXXXXXX-2723	$ 500.00	Yes
16	XXXXXXXXXX-6845	$ 800.00	Yes
17	XXXXXXXXXX-6250	$ 460.00	Yes
18	XXXXXXXXXX-8380	$ 900.00	Yes
19	XXXXXXXXXX-2980	$ 900.00	Yes
20	XXXXXXXXXX-9010	$ 800.00	Yes
21	XXXXXXXXXX-4920	$ 960.00	Yes
22			
23	**Totals**	$ 11,190.00	

Figura 16. Archivo de Microsoft Excel identificado como *cards_loaded_with_cash_1.xls.*

7. Archivo de Microsoft Excel identificado como *cards_loaded_with_cash_2.xls.* (Figura 17). Este archivo fue hallado en el directorio *Downloads*, del perfil de usuario de Uadiale. Este archivo detalla las tarjetas de débito cargadas con fondos, los cuales serían transferidos a "K!NG" mediante Liberty Reserve. Cabe destacar la presencia de una tarjeta de débito cuyos últimos cuatro (4) dígitos son 0836, y con

cantidad de efectivo de $840. Dichos datos coinciden con una transacción registrada de $840, la cual se efectuó en el portal de Liberty Reserve desde una cuenta identificada con el número 0836.



	A	B	C
1	**Card Number**	**Amount Loaded**	**Good**
2	XXXXXXXXXX-9640	$ 5,000.00	123
3	XXXXXXXXXX-5240	$ 7,000.00	123
4	XXXXXXXXXX-5750	$ 7,690.00	123
5	XXXXXXXXXX-3760	$ 8,960.00	123
6	XXXXXXXXXX-3880	$ 5,790.00	123
7	XXXXXXXXXX-2010	$ 7,000.00	123
8	XXXXXXXXXX-2080	$ 5,000.00	123
9	XXXXXXXXXX-5020	$ 6,000.00	123
10	XXXXXXXXXX-6650	$ 7,500.00	123
11	XXXXXXXXXX-0400	$ 9,000.00	123
12	XXXXXXXXXX-9710	$ 5,400.00	1234
13	XXXXXXXXXX-5474	$ 6,000.00	1234
14	XXXXXXXXXX-6423	$ 4,500.00	1234
15	XXXXXXXXXX-7501	$ 7,800.00	1234
16	XXXXXXXXXX-7256	$ 5,000.00	1234
17	XXXXXXXXXX-3810	$ 4,600.00	123
18	XXXXXXXXXX-3310	$ 3,500.00	123
19	XXXXXXXXXX-9410	$ 5,000.00	747
20	XXXXXXXXXX-3200	$ 3,000.00	123
21	XXXXXXXXXX-4810	$ 2,230.00	123
22	XXXXXXXXXX-1590	$ 2,000.00	1234
23	XXXXXXXXXX-0836	$ 840.00	123
24			
25	**Totals**	$ 118,810.00	

Figura 17. Archivo de Microsoft Excel identificado como *cards_loaded_with_cash_2.xls.*

Cadena de custodia

Los procedimientos estándares de operación de LAG CyberForensics indican la documentación de las etapas de adquisición, procesamiento y control de la evidencia analizada. Dichas etapas se documentan en una cadena de custodia para asegurar la integridad del proceso.

Primer evento

- Descripción: Evidencia entregada por el Fiscal Asistente, Jared M. Strauss al examinador forense Luis A. Gandía Vázquez. La evidencia consiste en un disco duro identificado como *Item No. 2018-EV-01*.
- Verificado por: Luis A. Gandía Vázquez y Jared M. Strauss.
- Fecha de comienzo: 30 de noviembre de 2018 - 6:00 AM.
- Fecha de terminación: 30 de noviembre de 2018 - 6:15 AM.
- Lugar de origen: Oficina del FBI, Maple Valley, Washington, USA.
- Destino: Laboratorio forense - LAG CyberForensics, Puerto Rico.

Segundo evento

- Descripción: Creación de número de caso a evidencia recibida.
- Realizado por: Luis A. Gandía Vázquez
- Número de caso: 18-CR-60073-WPD
- Fecha de comienzo: 1 de diciembre de 2018 - 7:29 AM.
- Fecha de terminación: 1 de diciembre de 2018 - 7:30 AM.
- Lugar de origen: Laboratorio forense - LAG CyberForensics, Puerto Rico.
- Destino: Laboratorio forense - LAG CyberForensics, Puerto Rico.

Tercer evento

- Descripción: Proceso de imagen y análisis de evidencia recibida.
- Realizado por: Luis A. Gandía Vázquez
- Número de caso: 18-CR-60073-WPD
- Fecha de comienzo: 1 de diciembre de 2018 - 7:35 AM.

- Fecha de terminación: 2 de diciembre de 2018 - 2:30 PM.
- Lugar de origen: Laboratorio forense - LAG CyberForensics, Puerto Rico.
- Destino: Laboratorio forense - LAG CyberForensics, Puerto Rico.

Cuarto evento

- Descripción: Entrega de evidencia e informe de análisis forense al Fiscal Asistente Jared M. Strauss.
- Verificado por: Luis A. Gandía Vázquez y Jared M. Strauss.
- Número de caso: 18-CR-60073-WPD
- Fecha de comienzo: 2 de diciembre de 2018 - 5:00 PM.
- Fecha de terminación: 2 de diciembre de 2018 - 5:30 PM.
- Lugar de origen: Laboratorio forense - LAG CyberForensics, Puerto Rico.
- Destino: Oficina del FBI, Maple Valley, Washington, USA.

Procedimiento

A continuación, se describen los pasos ejecutados como parte del proceso de análisis forense realizado a la pieza de evidencia identificada como *Item No. 2018-EV-0*.

1. Procedimiento: Creación del caso
    a. Herramienta: ProDiscover Basic
    b. Fecha de comienzo: 1 de diciembre de 2018 - 7:29 AM
    c. Fecha de terminación: 1 de diciembre de 2018 - 7:30 AM
    d. Descripción: Asignar número de caso a la evidencia adquirida con la herramienta ProDiscover Basic (Figura 18).

Figura 18. Caso creado con la herramienta ProDiscover Basic.

2. Procedimiento: Creación de imagen original.
    a. Herramienta: ProDiscover Basic
    b. Fecha de comienzo: 1 de diciembre de 2018 - 7:35 AM
    c. Fecha de terminación: 1 de diciembre de 2018 - 2:50 PM
    d. Descripción: Proceso de captura de imagen original con la herramienta ProDiscover Basic (Figuras 19 y 20). La misma será preservada y no se someterá a los análisis programados.

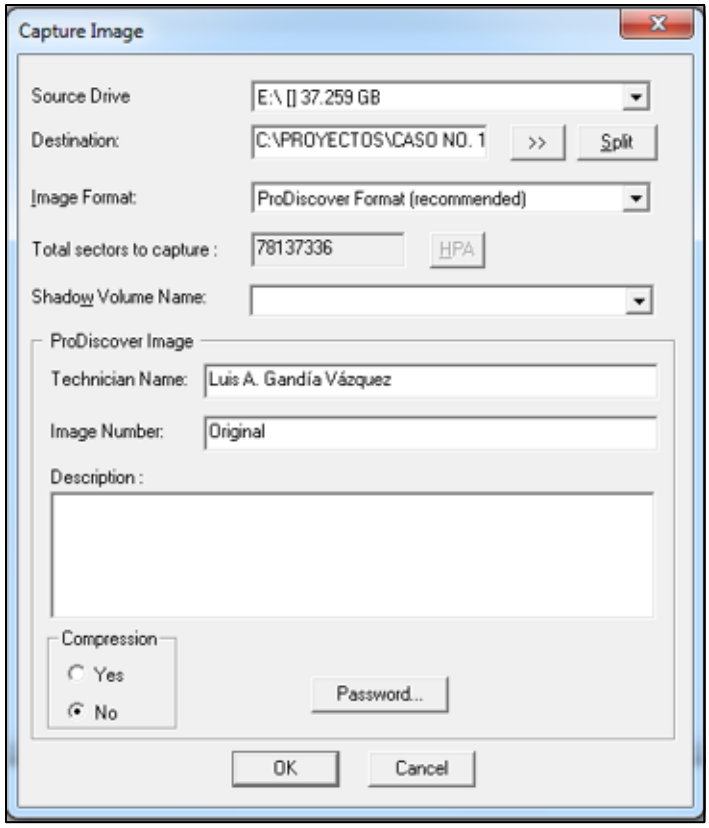


Figura 19. Proceso de captura de imagen original.

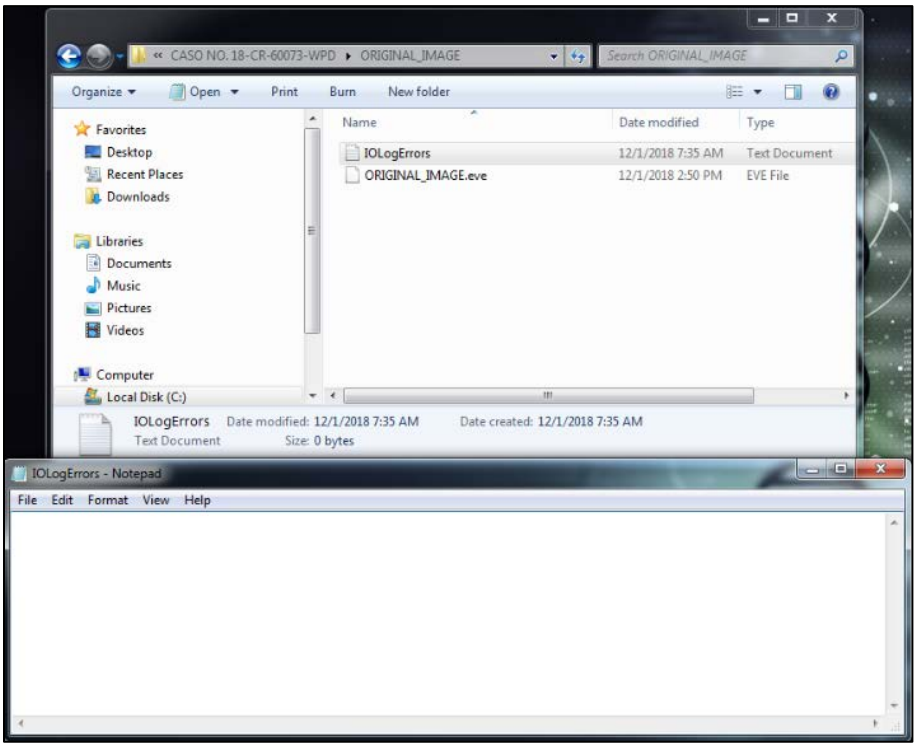


Figura 20. Imagen capturada exitosamente y almacenada en directorio del caso.

3. Procedimiento: Conversión de imagen

    a. Herramienta: ProDiscover Basic

    b. Fecha de comienzo: 1 de diciembre de 2018 - 6:02 PM

    c. Fecha de terminación: 1 de diciembre de 2018 - 6:46 PM

    d. Descripción: Proceso de conversión de imagen a formato .DD para lograr compatibilidad con otras herramientas forenses (Figura 21 y Figura 22). Esta copia será sometida a los análisis programados.

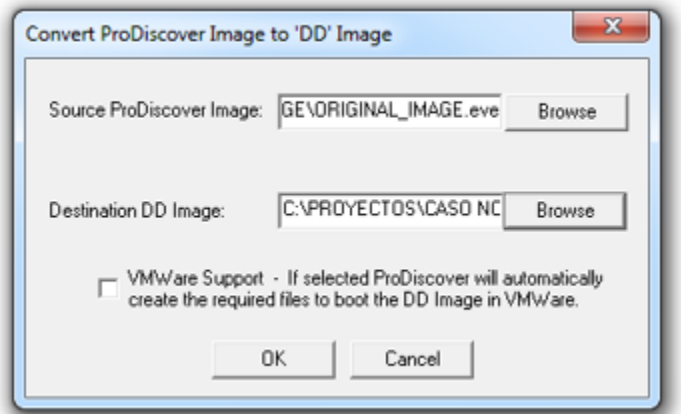


Figura 21. Inicio de proceso de conversión de imagen.

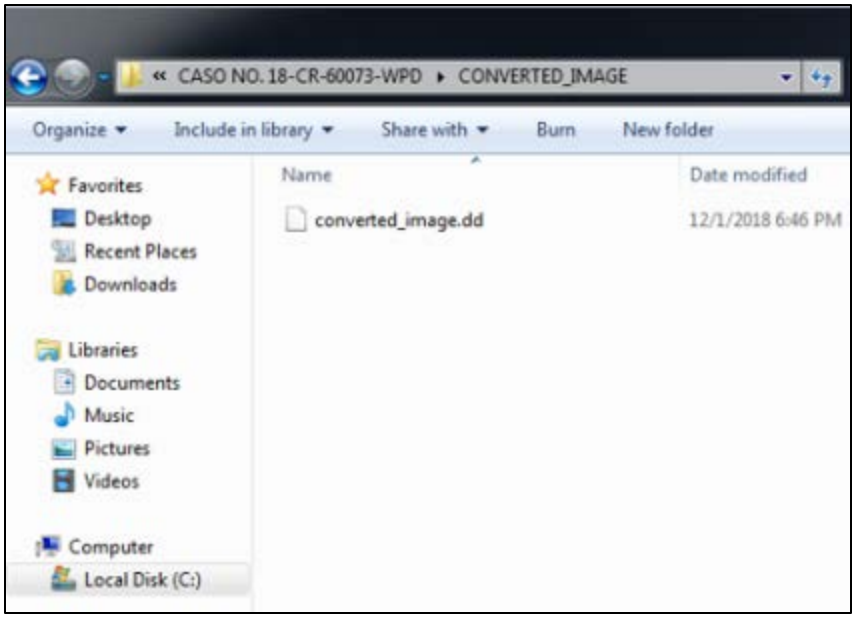


Figura 22. Imagen convertida exitosamente y almacenada en directorio del caso.

4. Procedimiento: Análisis de integridad a la imagen original

    a. Herramienta: ProDiscover Basic

    b. Fecha de comienzo: 1 de diciembre de 2018 - 7:35 PM

    c. Fecha de terminación: 1 de diciembre de 2018 - 7:50 PM

    d. Descripción: Generación de hash usando el algoritmo MD5 para comprobar que la imagen no ha sufrido cambios (Figura 23 y Figura 24).

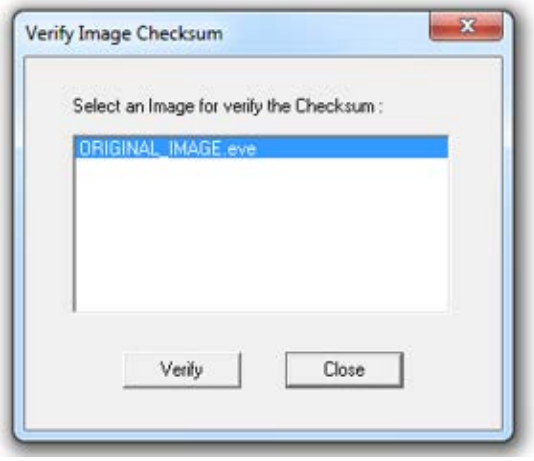


Figura 23. Inicio de generación de hash a imagen original.

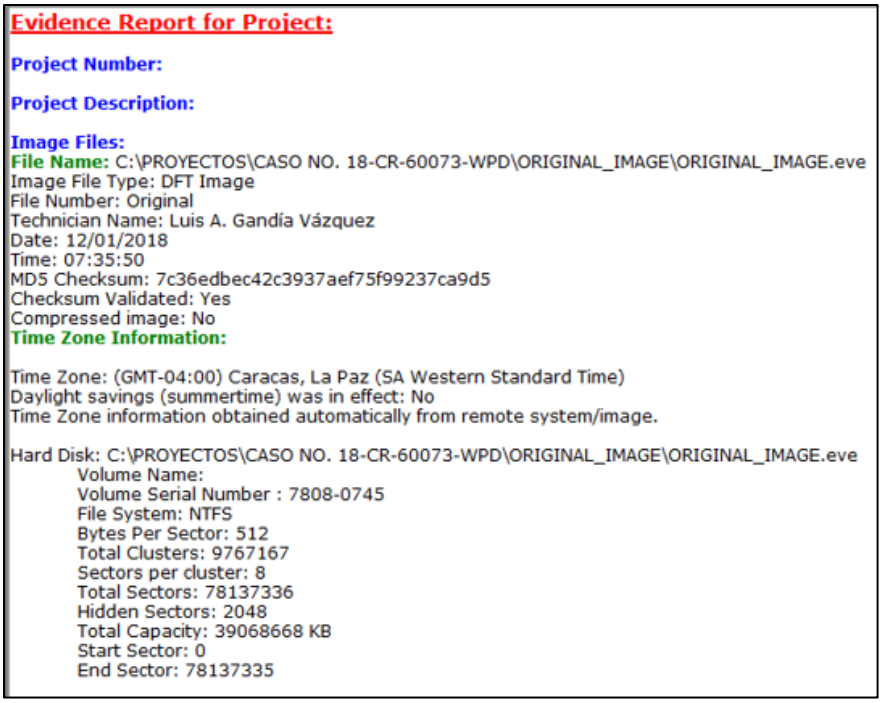


Figura 24. Reporte confirmando generación y validación de *hash*.

5. Procedimiento: Preparativos para análisis de imagen convertida

    a. Herramientas: OSForensics y OSFMount

    b. Fecha de comienzo: 1 de diciembre de 2018 - 11:07 PM

    c. Fecha de terminación: 1 de diciembre de 2018 - 11:32 PM

    d. Descripción: Creación de caso en OSForensics (Figura 25), generación de hash a imagen convertida (Figura 26) y montar la misma como partición E: en modo *read-only* (Figura 27).

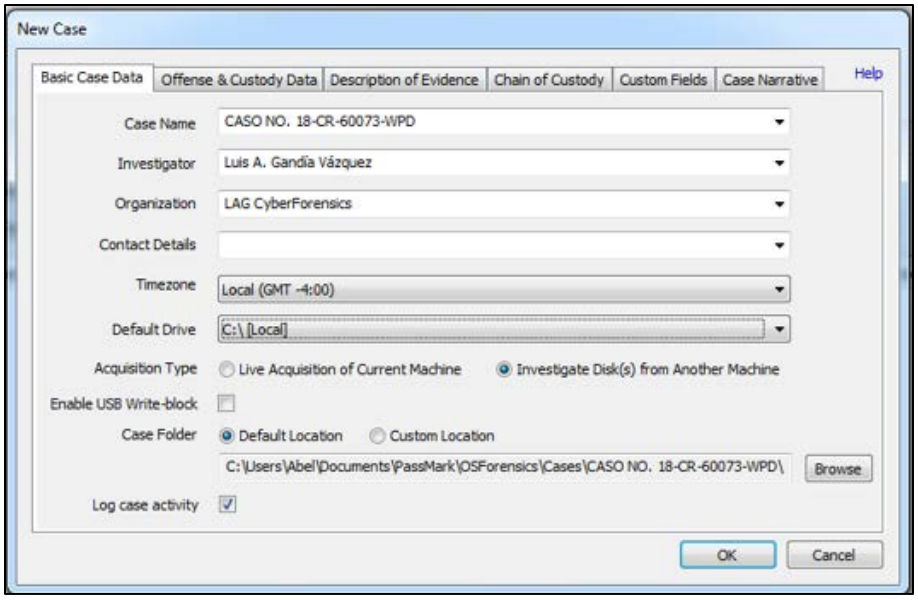


Figura 25. Creación de caso en OSForensics.

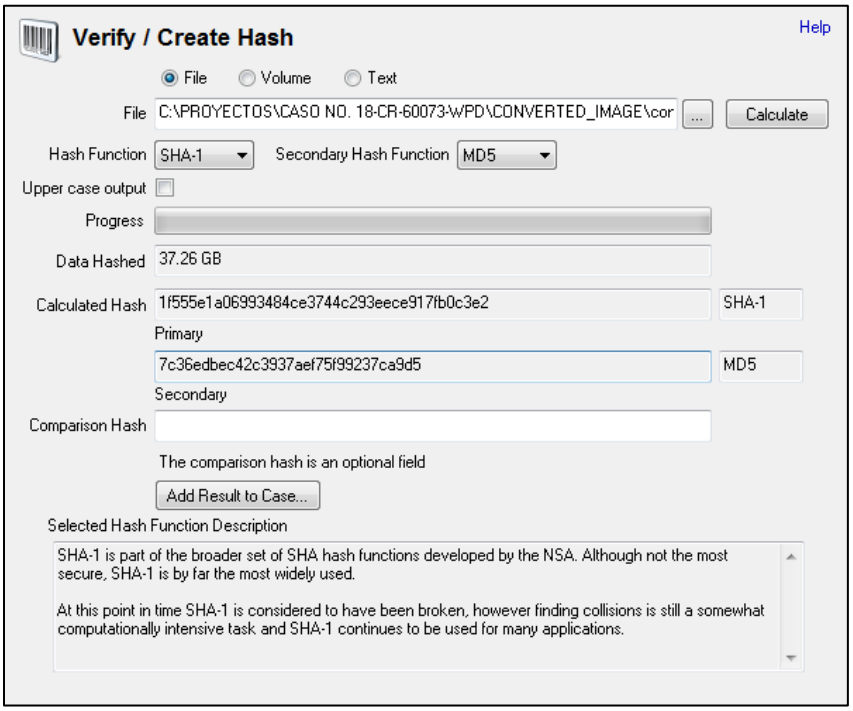


Figura 26. Generación de *hash* a imagen convertida con OSForensics.

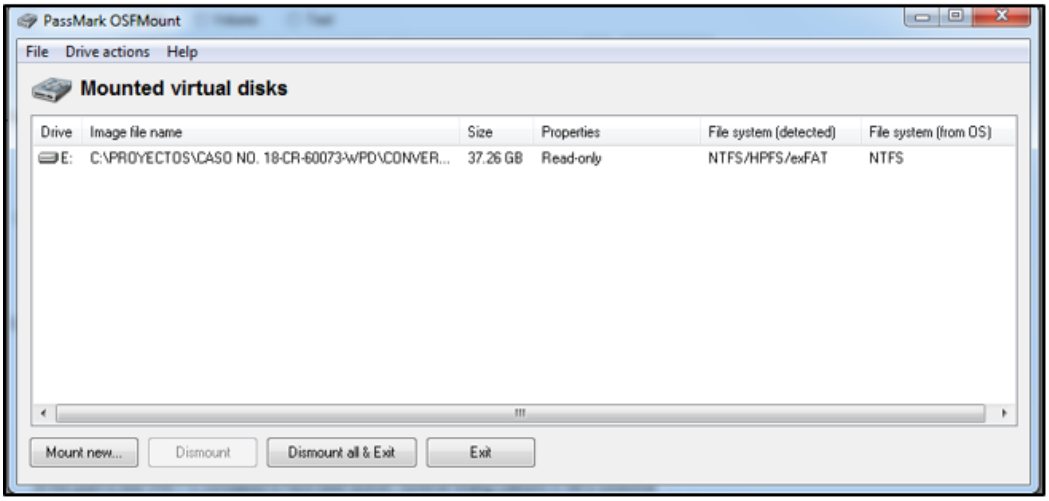


Figura 27. Imagen convertida, montada como partición E: en modo *read-only*.

6. Procedimiento: Identificar información general del sistema operativo
    a. Herramienta: OSForensics
    b. Fecha de comienzo: 1 de diciembre de 2018 - 11:33 PM
    c. Fecha de terminación: 1 de diciembre de 2018 - 11:35 PM
    d. Descripción: Se ejecutó el módulo *System Information* de OSForensics sobre la imagen montada para recuperar información general del sistema. Se captura el nombre de la computadora (RAYMOND-UADIALE), perfil del usuario (Uadiale) y versión del sistema operativo (Windows 7 Professional Build 7601). Dicha información se puede apreciar en las figuras 28, 29 y 30. Estos datos conectan a Raymond Uadiale con la computadora incautada.

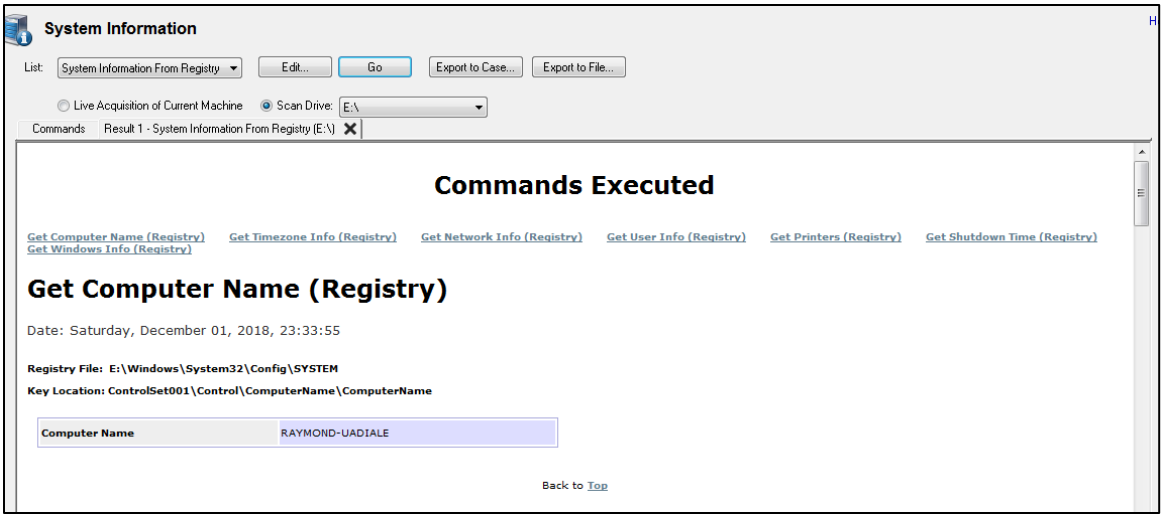


Figura 28. Nombre de la computadora.

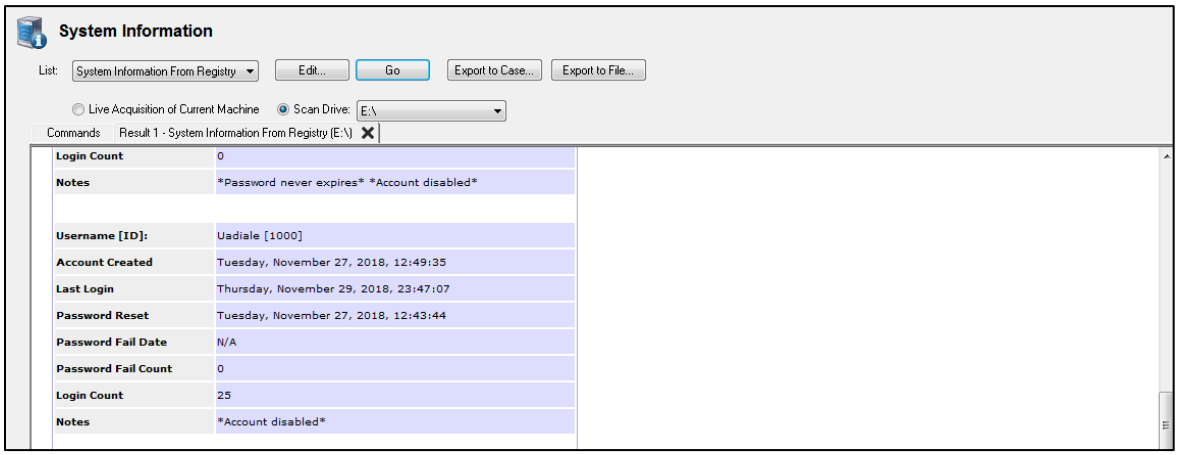


Figura 29. Perfil del usuario Uadiale.

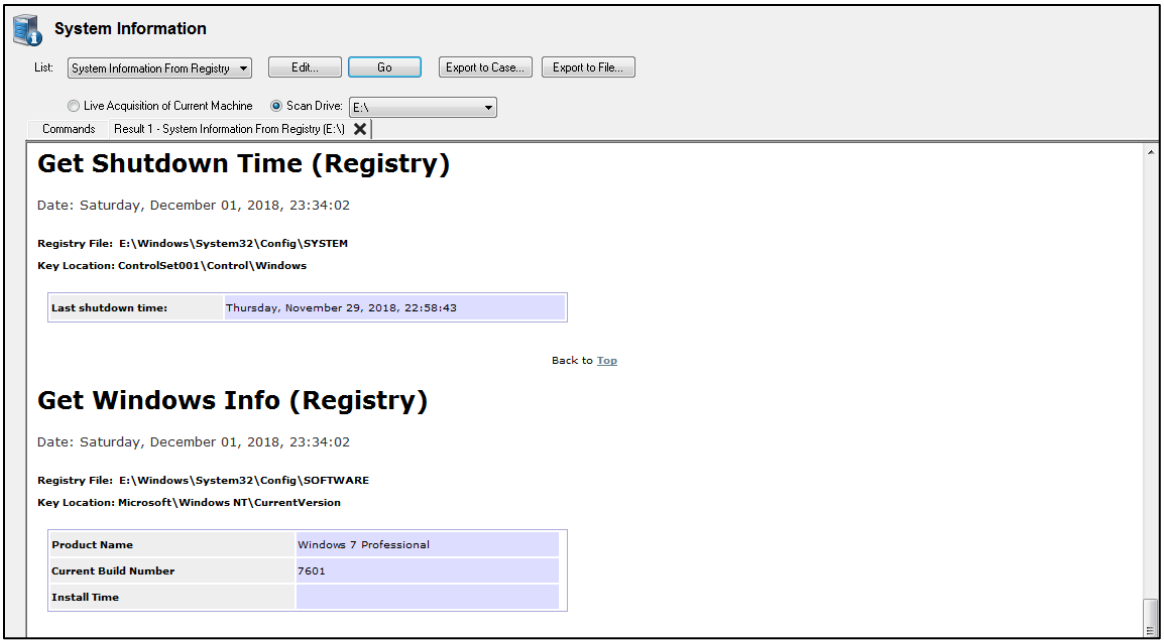


Figura 30. Versión del sistema operativo albergado en la imagen.

7. Procedimiento: Identificar programas instalados

    a. Herramienta: OSForensics

    b. Fecha de comienzo: 1 de diciembre de 2018 - 11:40 PM

    c. Fecha de terminación: 1 de diciembre de 2018 - 11:41 PM

    d. Descripción: Se ejecutó el explorador de archivos de OSForensics para identificar los programas instalados en la imagen montada (Figura 31). Entre los programas instalados se pueden identificar el buscador web Mozilla Firefox y el cliente de correos electrónicos Mozilla Thunderbird. La búsqueda de evidencia se enfocará en los archivos generados por dichas aplicaciones.

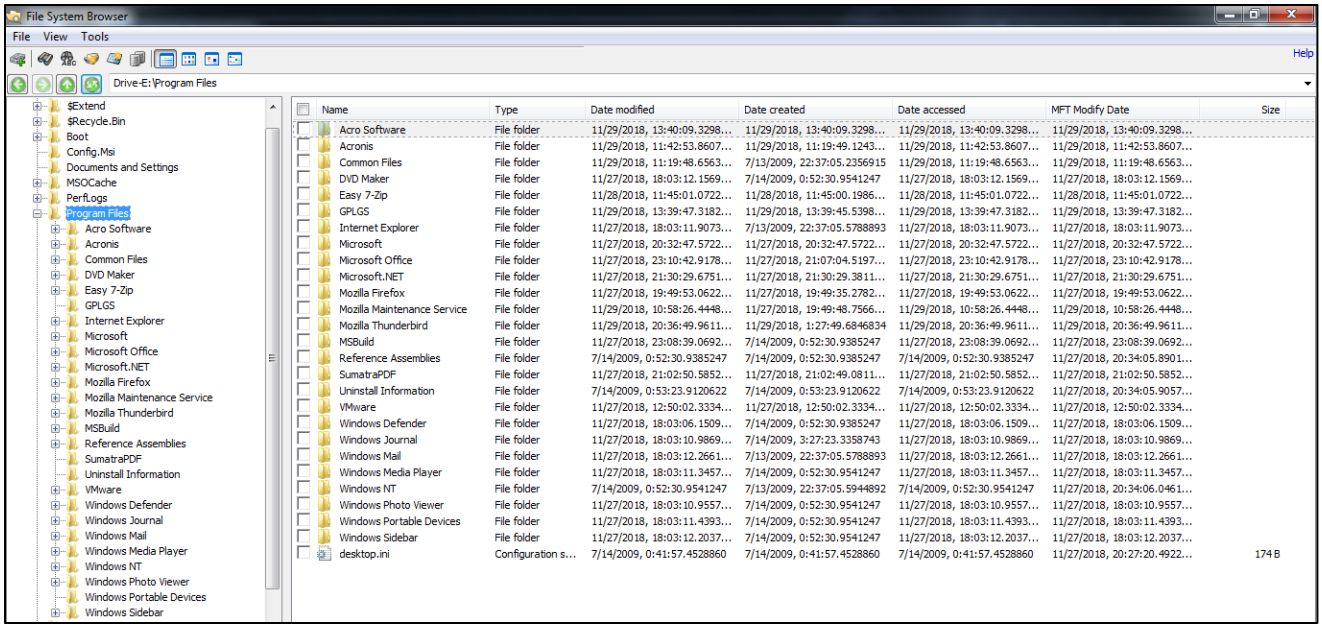


Figura 31. Directorio de programas instalados.

8. Procedimiento: Búsqueda de archivos encriptados

    a. Herramienta: OSForensics

    b. Fecha de comienzo: 1 de diciembre de 2018 - 11:45 PM

    c. Fecha de terminación: 1 de diciembre de 2018 - 11:50 PM

    d. Descripción: Se ejecutó el buscador de archivos de OSForensics para identificar la presencia de archivos encriptados en la imagen montada. La búsqueda arrojó resultados negativos (Figura 32).

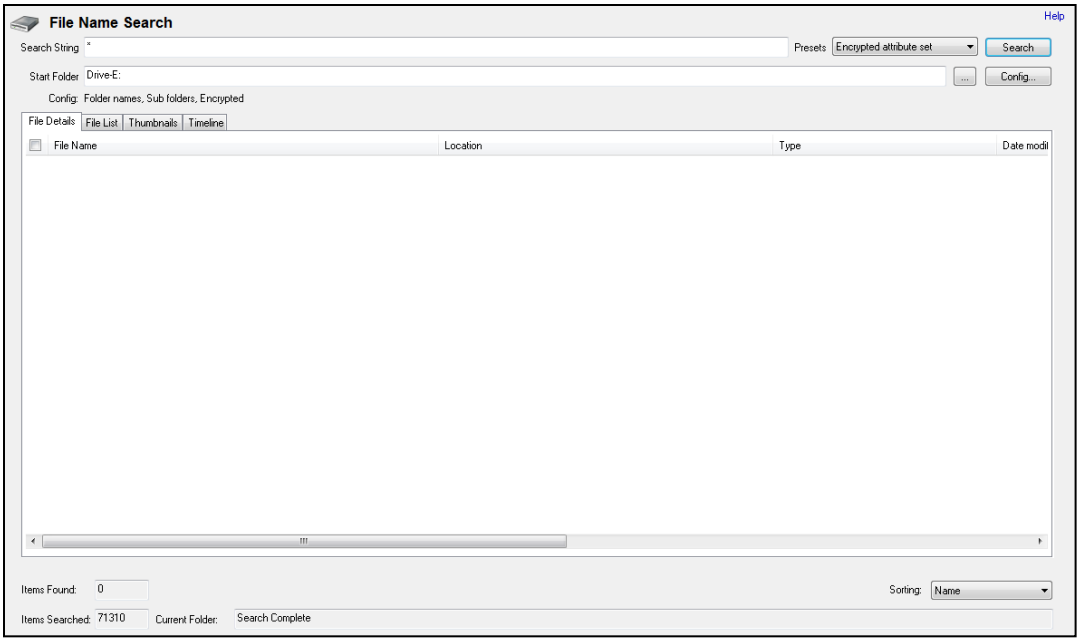


Figura 32. Resultados de búsqueda de archivos encriptados.

9. Procedimiento: Búsqueda de archivos borrados

    a. Herramienta: OSForensics

    b. Fecha de comienzo: 1 de diciembre de 2018 - 11:52 PM

    c. Fecha de terminación: 1 de diciembre de 2018 - 11:55 PM

    d. Descripción: Se ejecutó el buscador de archivos de OSForensics para identificar la presencia de archivos borrados en la imagen montada. Los resultados mostraron 9,235 archivos (Figura 33). Por tal razón, se aplicó un filtro para identificar archivos de interés. El filtro aplicado mostró resultados negativos (Figura 34).

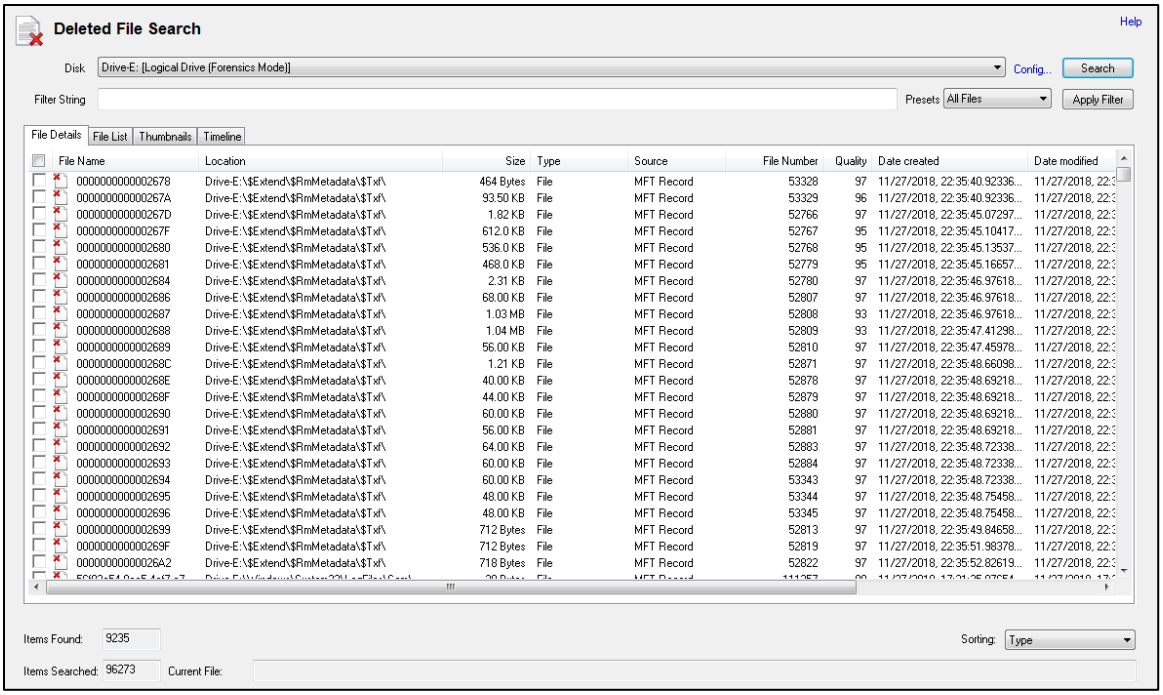


Figura 33. Resultados de búsqueda de archivos borrados.

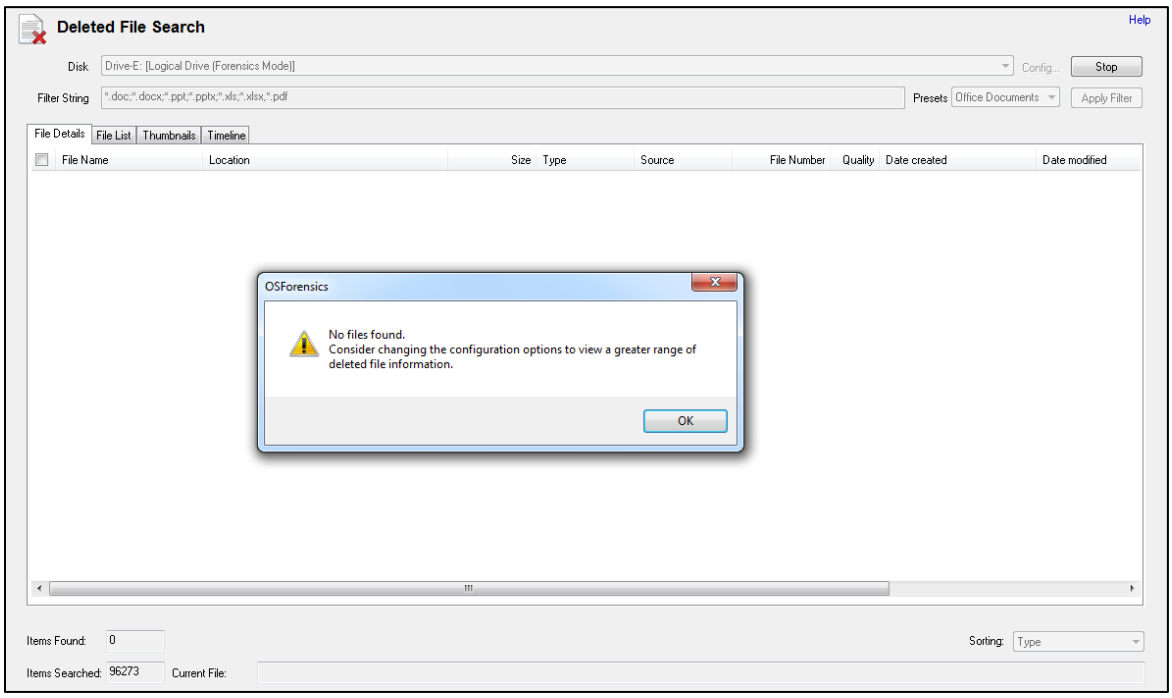


Figura 34. Filtro aplicado a búsqueda de archivos borrados.

10. Procedimiento: Identificar historial de Internet

    a. Herramienta: OSForensics

    b. Fecha de comienzo: 1 de diciembre de 2018 - 11:56 PM

    c. Fecha de terminación: 1 de diciembre de 2018 - 11:58 PM

    d. Descripción: Se consultó el módulo de actividades recientes de OSForensics contra la imagen montada. En la figura 35 se puede apreciar que Uadiale visitó el portal de Liberty Reserve y realizó búsquedas relacionadas al ransomware Reveton. En la figura 36 se puede apreciar que Uadiale gestionó la creación de una cuenta en Liberty Reserve. De igual manera, el buscador registró su acceso un archivo de Microsoft Excel identificado como *card-numbers-list.xls*. En la figura 37 se registró la creación y eventual acceso a una cuenta de correo electrónico bajo el nombre “Mike Roland” en el portal *outlook.live.com*.

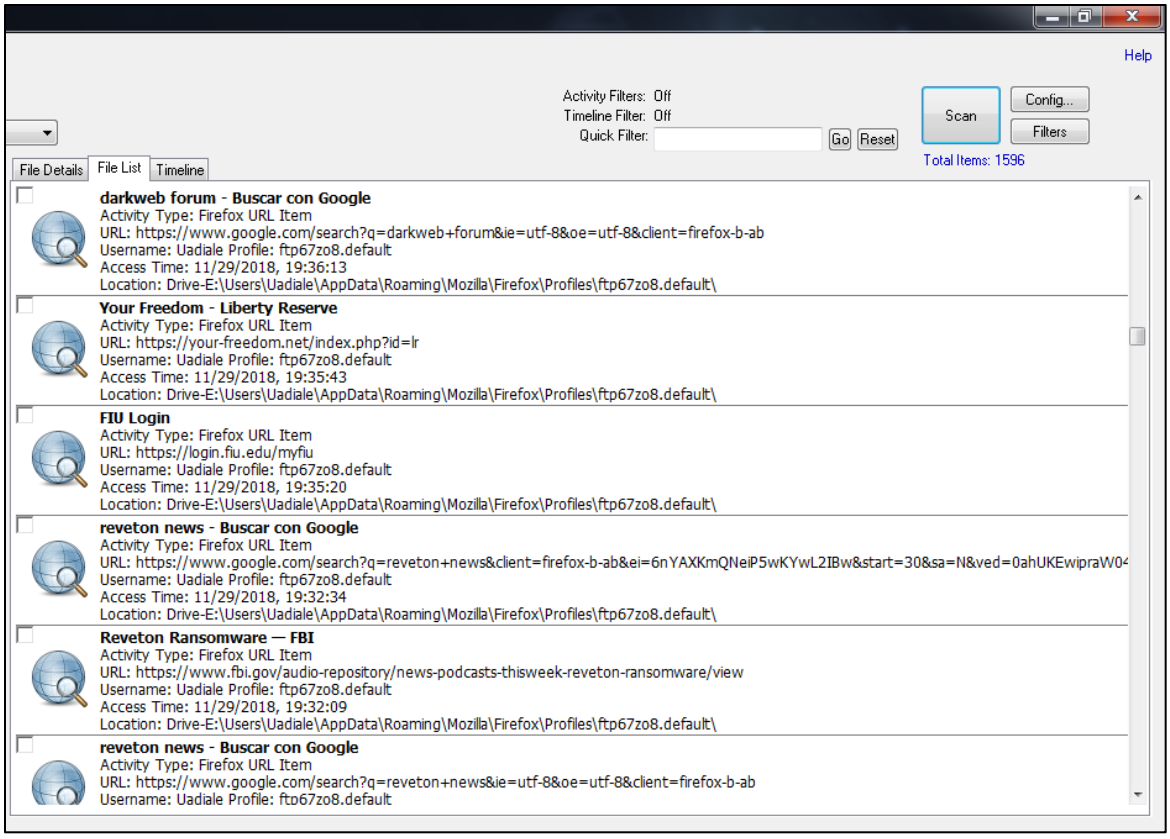


Figura 35. Historial de Internet que muestra acceso al portal de Liberty Reserve.

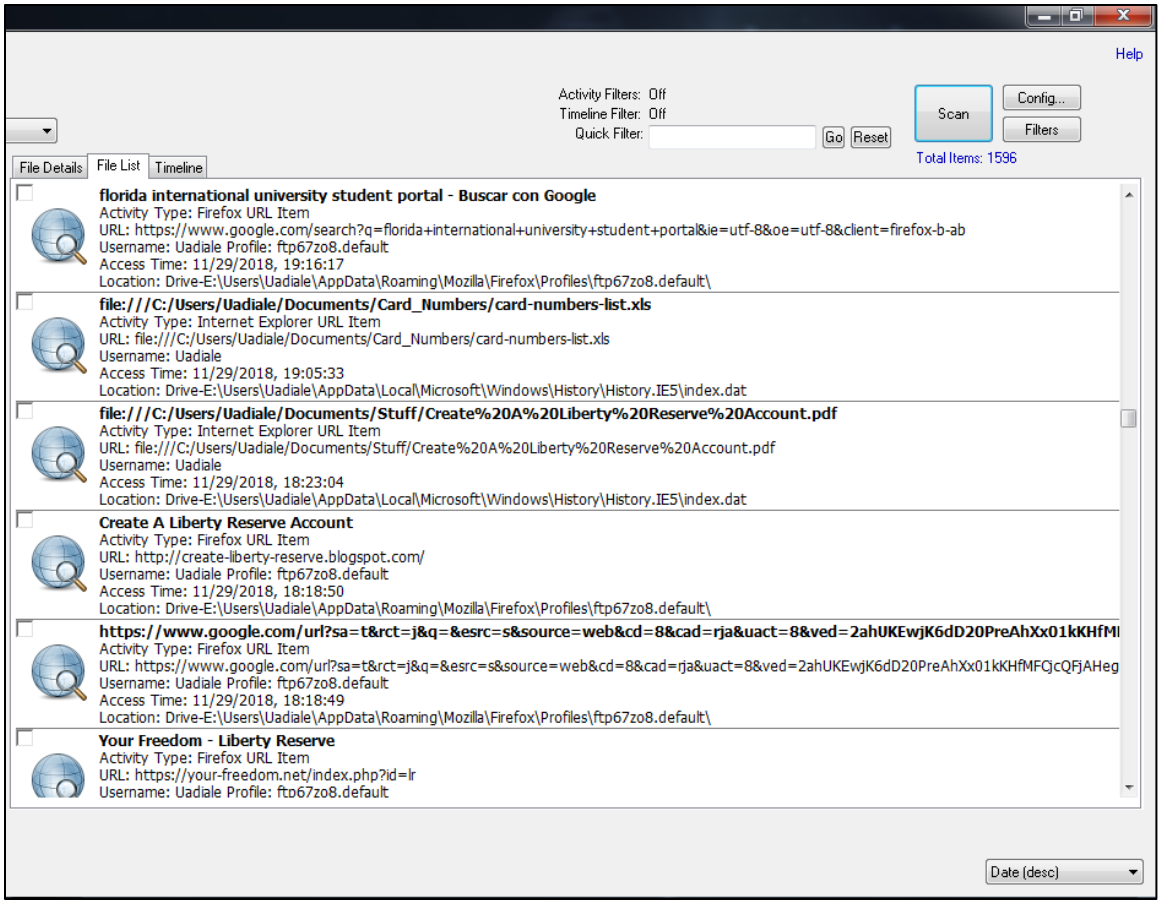


Figura 36. Historial de Internet que evidencia la creación de una cuenta en Liberty Reserve.

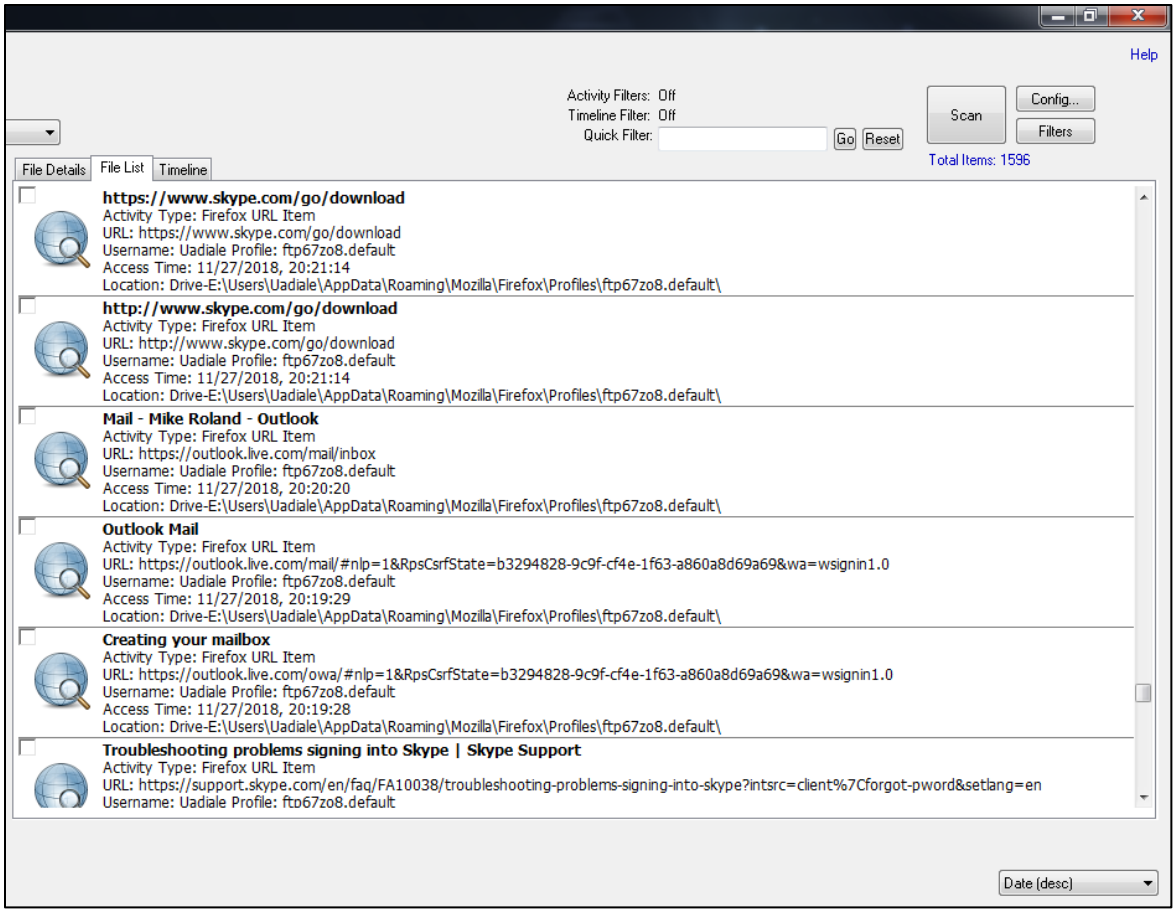


Figura 37. Creación y acceso a cuenta de correo electrónico a nombre de “Mike Roland”.

11. Procedimiento: Identificar *bookmarks* de páginas web

    a. Herramienta: OSForensics

    b. Fecha de comienzo: 2 de diciembre de 2018 - 12:00 AM

    c. Fecha de terminación: 2 de diciembre de 2018 - 12:01 AM

    d. Descripción: Se consultó el módulo de actividades recientes de OSForensics para identificar páginas web marcadas como favoritas. En la figura 38 se pueden apreciar los portales de Liberty Reserve, Florida International University, Miami Dade College y Microsoft. Los *bookmarks* de páginas web conectan a Raymond Uadiale con el personaje “Mike Roland”.

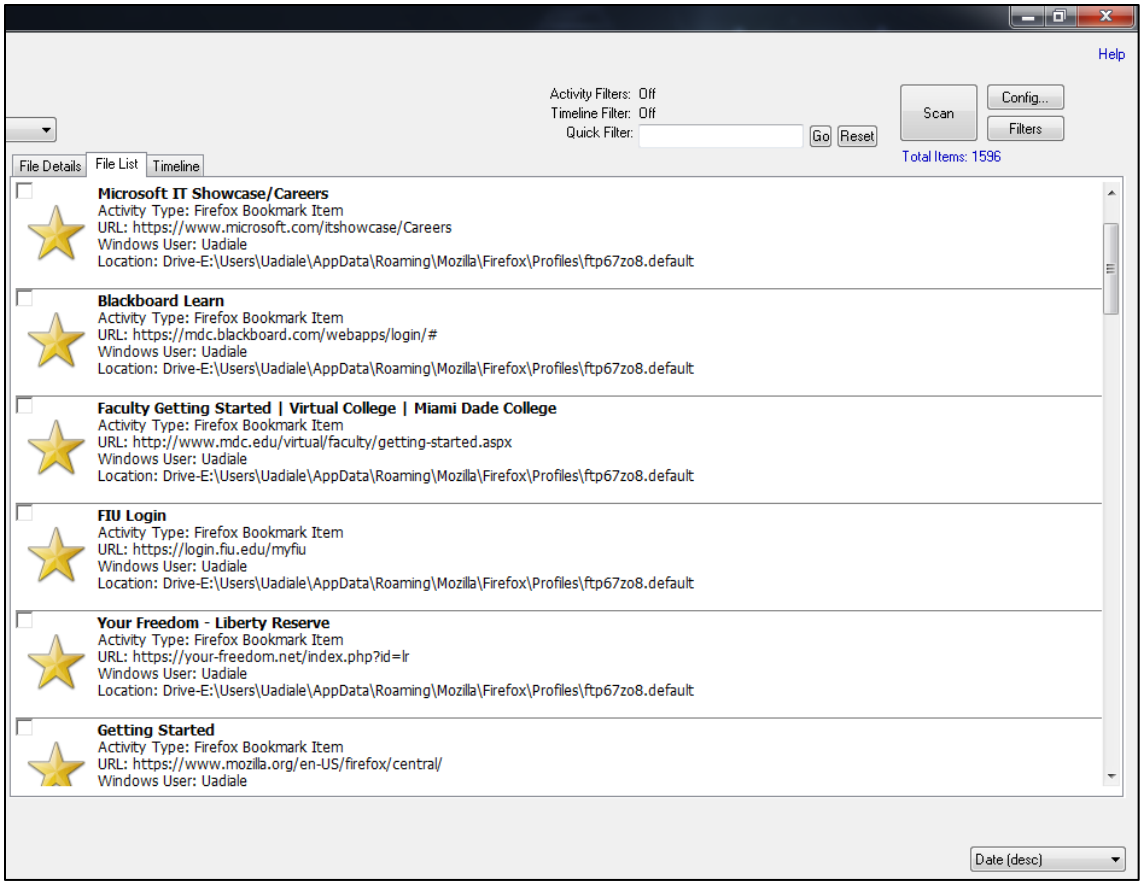


Figura 38. Bookmarks de páginas web.

12. Procedimiento: Búsqueda de correos electrónicos

    a. Herramienta: OSForensics

    b. Fecha de comienzo: 2 de diciembre de 2018 - 12:02 AM

    c. Fecha de terminación: 2 de diciembre de 2018 - 12:08 AM

    d. Descripción: Se consultó el buscador de archivos de OSForensics para identificar archivos de correos electrónicos. En el resultado de la búsqueda se identificaron 2 correos electrónicos (Figura 39). Se utilizó el módulo *E-mail Viewer* de OSForensics para abrir ambos archivos. En la figura 40 se puede apreciar el primer correo electrónico recibido por Raymond Uadiale, aka “Mike Roland” por parte de “K!NG”. En dicho mensaje, “K!NG” le imparte instrucciones detalladas a Raymond Uadiale

sobre como operar el esquema. En la figura 41 se muestra el segundo correo electrónico recibido por Raymond Uadiale, aka “Mike Roland” por parte de “K!NG”. En el mismo “K!NG” indica a Uadiale su dirección de correo electrónico corregida. De igual manera, se puede apreciar una respuesta anterior de Uadiale hacia “K!NG” relacionada a la obtención de unas tarjetas de débito.

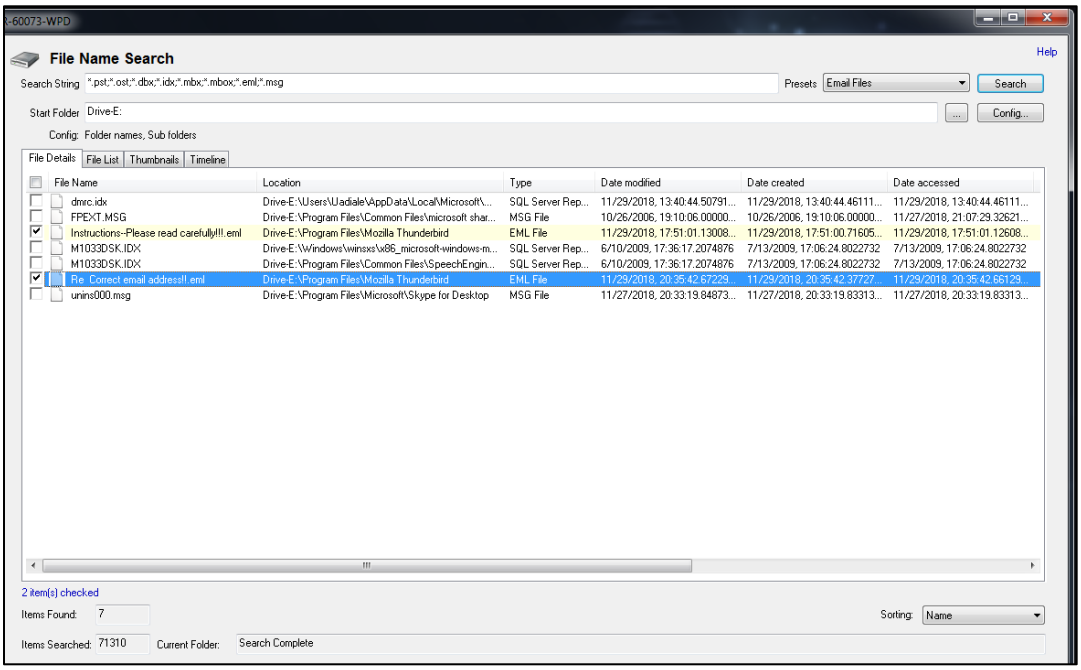


Figura 39. Correos electrónicos identificados.

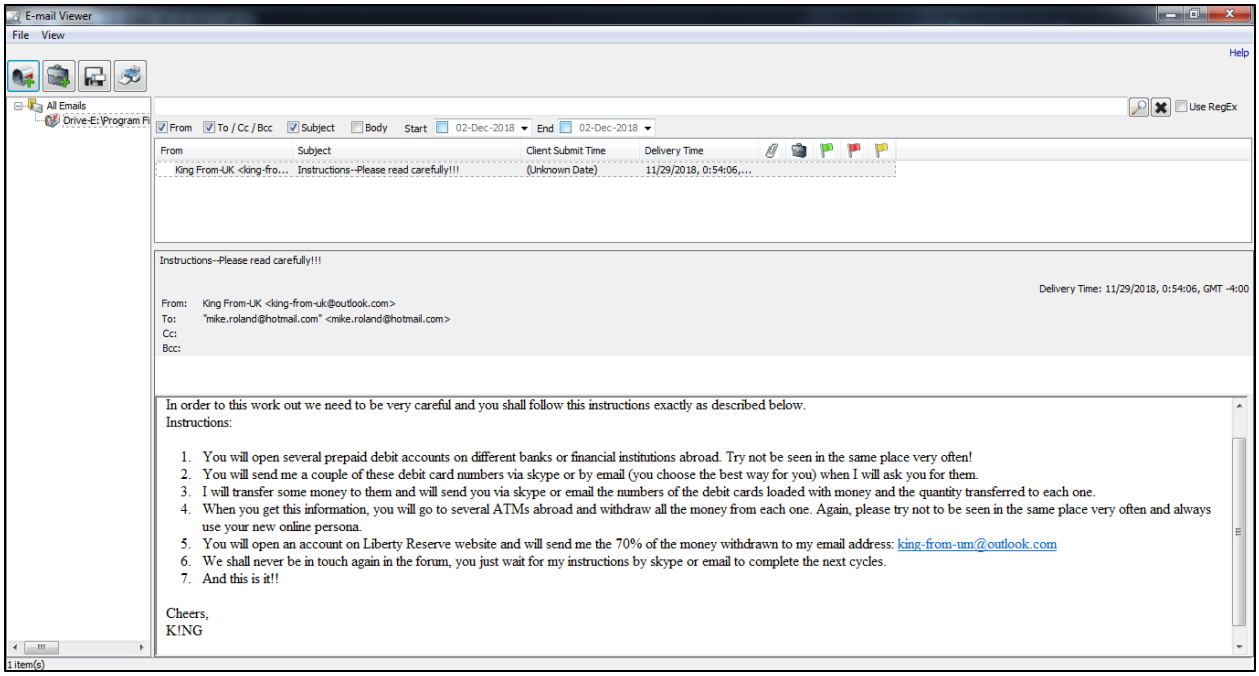


Figura 40. Correo electrónico con instrucciones detalladas.

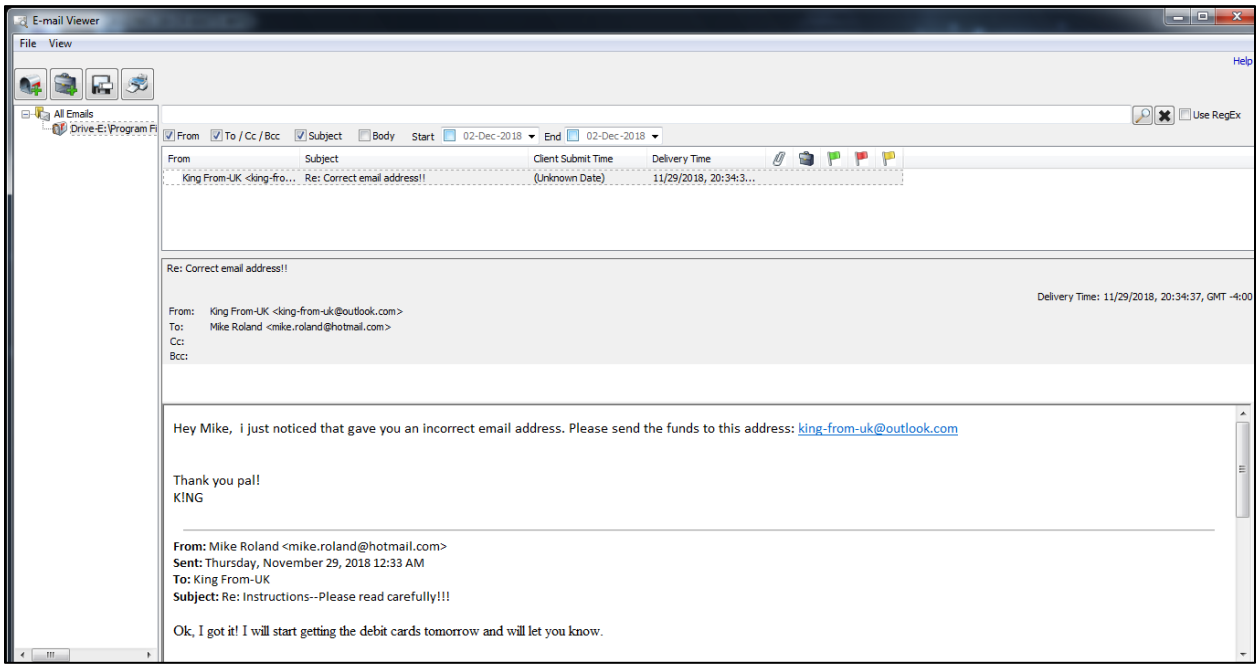


Figura 41. Correo electrónico con dirección corregida.

13. Procedimiento: Búsqueda y extracción de documentos existentes

a. Herramienta: OSForensics

b. Fecha de comienzo: 2 de diciembre de 2018 - 12:10 AM

c. Fecha de terminación: 2 de diciembre de 2018 - 12:30 AM

d. Descripción: Se utilizó el buscador de archivos de OSForensics para identificar documentos existentes en la imagen montada. El resultado de la búsqueda inicial fueron 62 documentos, entre los cuales se encuentran unos archivos de Microsoft Excel que son de interés (Figura 42). Luego se aplicó un filtro para capturar solamente documentos de Microsoft Excel y se encuentran 9 documentos relacionados a tarjetas de débito (Figura 43). Se procede a extraer la evidencia al directorio del caso creado (Figura 44). Se aplica un nuevo filtro a la búsqueda inicial para identificar archivos de texto simple y se identifican 5 archivos relacionados a bitácoras de conversaciones (Figura 45). Se procede a extraer los archivos al directorio del caso creado (Figura 46).

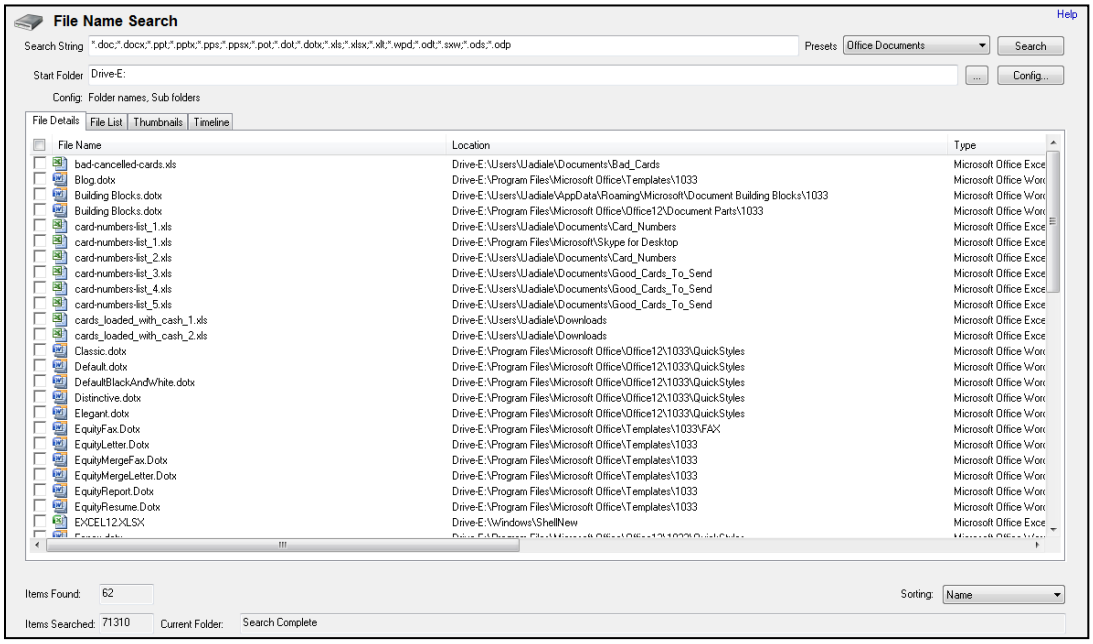


Figura 42. Resultado de búsqueda inicial.

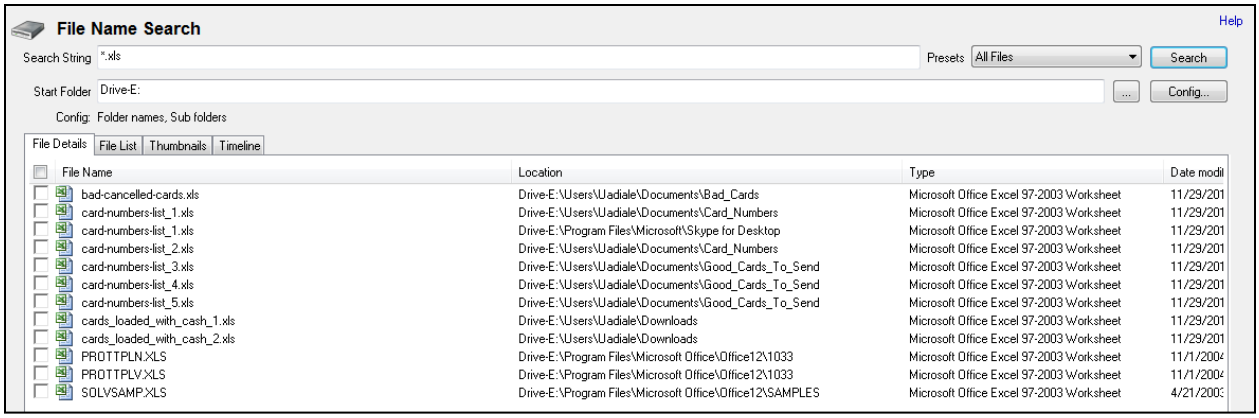


Figura 43. Filtro aplicado para identificar archivos de Microsoft Excel.

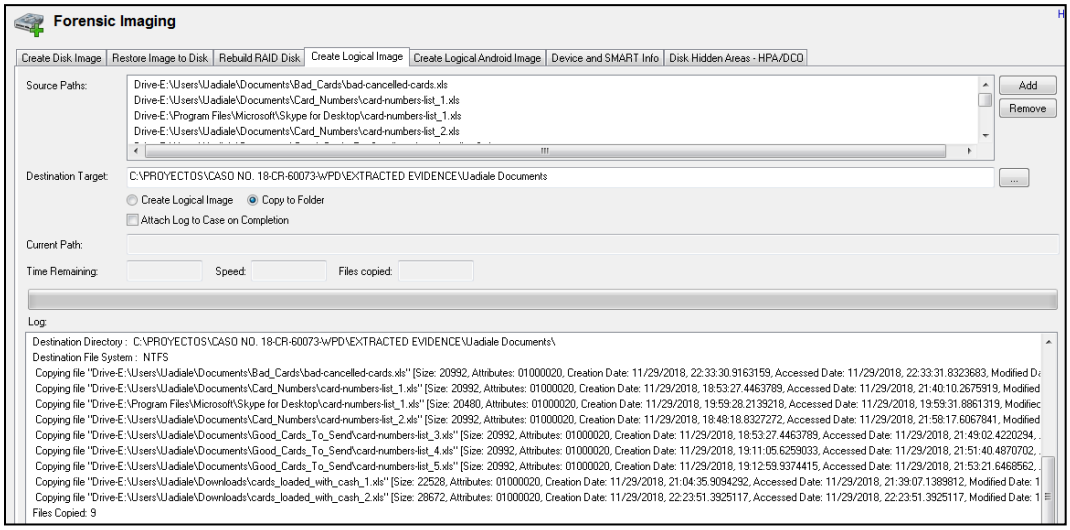


Figura 44. Extracción de archivos de Microsoft Excel.

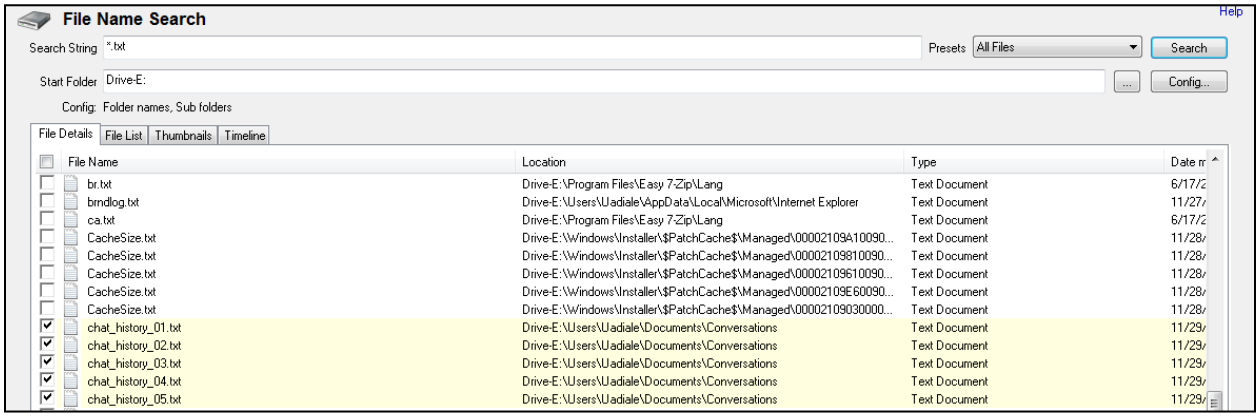


Figura 45. Filtro aplicado para identificar archivos de texto simple.

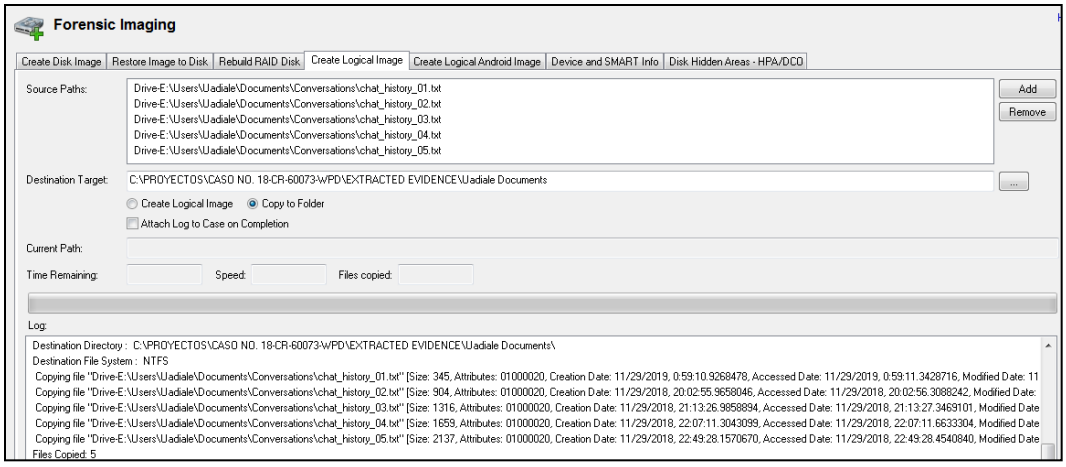


Figura 46. Extracción de archivos de texto simple.

14. Procedimiento: Identificar presencia de *malware*

    a. Herramienta: ClamWin AV

    b. Fecha de comienzo: 2 de diciembre de 2018 - 1:29 AM

    c. Fecha de terminación: 2 de diciembre de 2018 - 1:47 AM

    d. Descripción: Se realizó un *malware scan* a la imagen. El resultado mostró un archivo infectado localizado en el directorio de descargas del perfil de Uadiale (Figura 47).

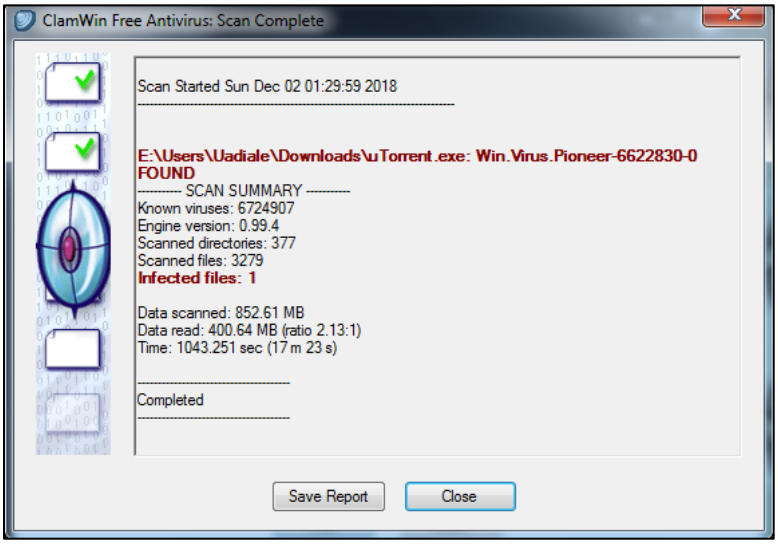


Figura 47. Malware identificado.

15. Procedimiento: Desmontar imagen

    a. Herramienta: OSFMount

    b. Fecha de comienzo: 2 de diciembre de 2018 - 1:50 AM

    c. Fecha de terminación: 2 de diciembre de 2018 - 1:51 AM

    d. Descripción: Se procedió a desmontar la imagen luego de haber finalizado el proceso de análisis y extracción de evidencia (Figura 48).

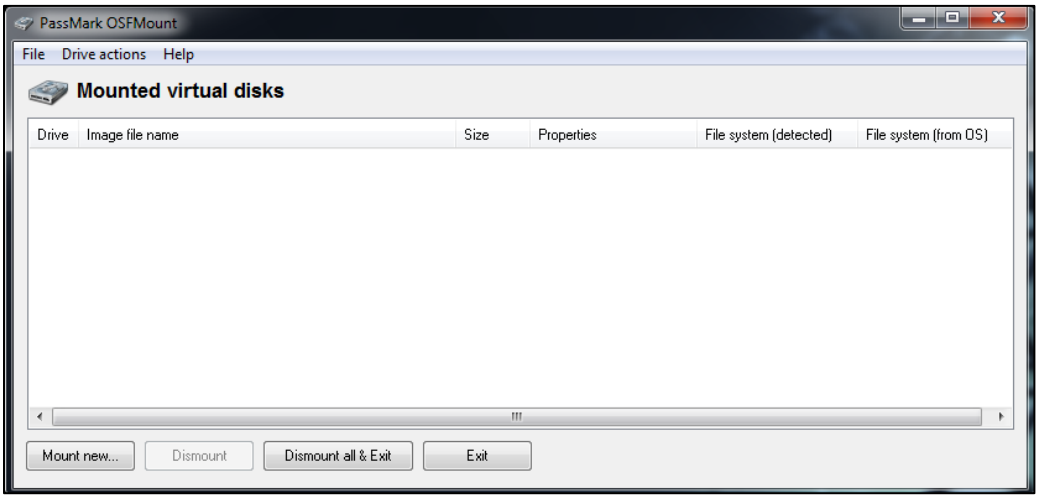


Figura 48. Imagen desmontada.

16. Procedimiento: Analizar bitácoras de conversaciones

    a. Herramienta: Beyond Compare

    b. Fecha de comienzo: 2 de diciembre de 2018 - 12:48 PM

    c. Fecha de terminación: 2 de diciembre de 2018 - 1:30 PM

    d. Descripción: Se hizo una comparación entre las bitácoras de conversaciones *chat_history_01.txt* y *chat_history_05.txt*, utilizando la herramienta BeyondCompare. Se identificó que existe una diferencia incremental en el contenido, lo cual confirma que el archivo *chat_history_05.txt* es un resguardo de todas las conversaciones entre

Raymond Uadiale y “K!NG”. En las Figuras 50, 51, 52 y 53 se pueden apreciar todas las conversaciones entre Raymond Uadiale y “K!NG”.

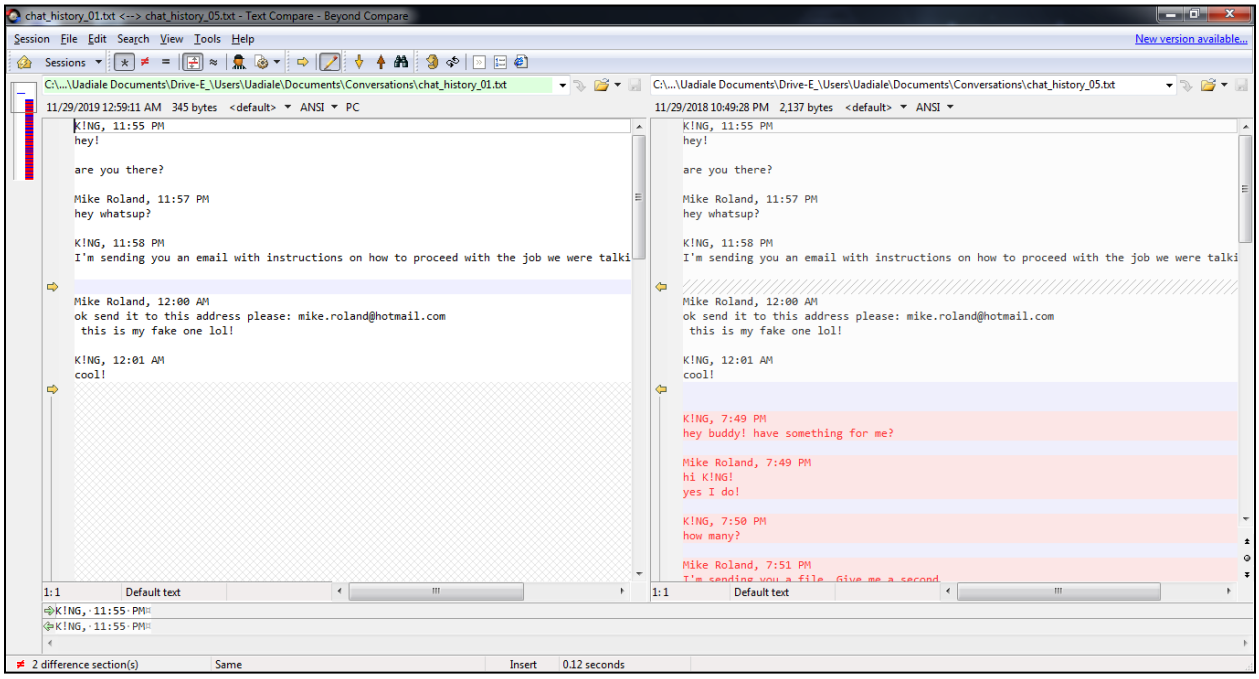


Figura 49. Comparación entre *chat_history_01.txt* y *chat_history_05.txt*.

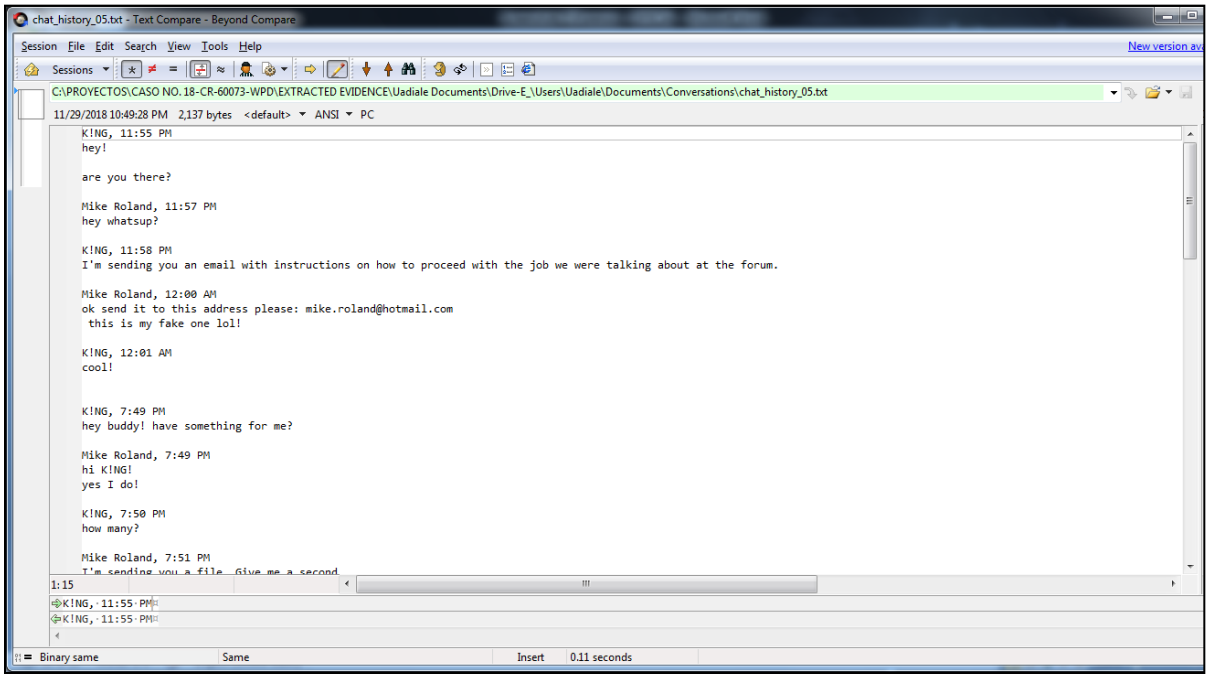


Figura 50. Conversación inicial entre Raymond Uadiale y “K!NG”.

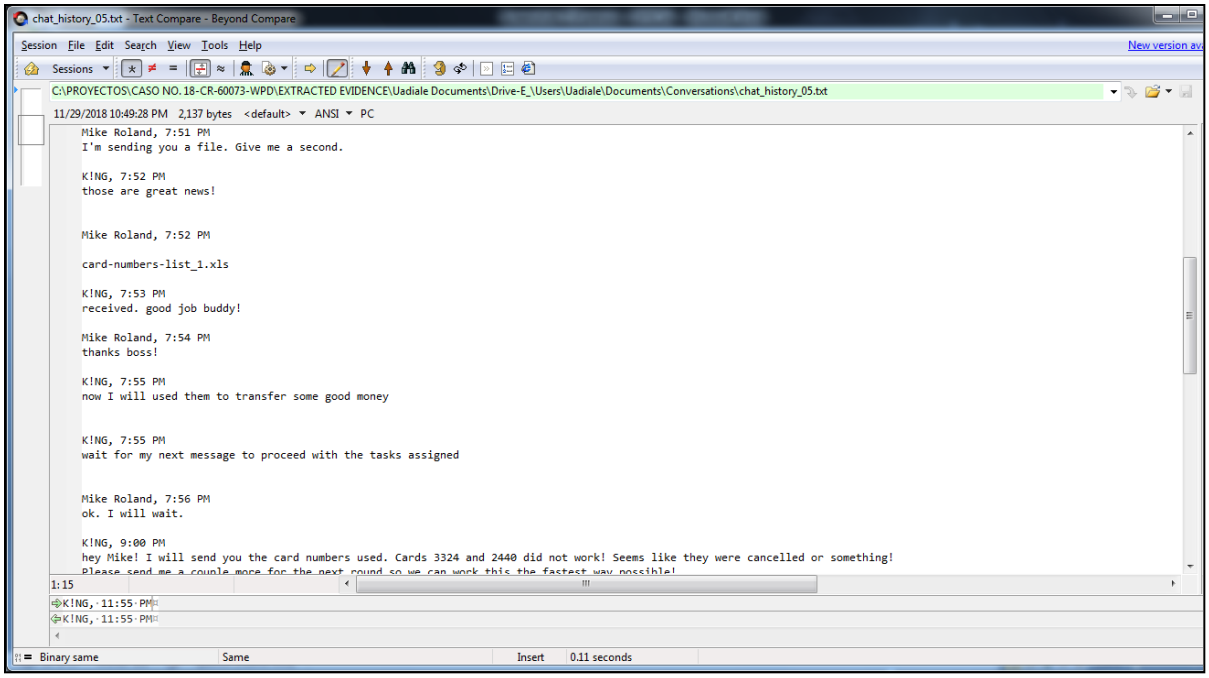


Figura 51. Segunda conversación entre Raymond Uadiale y "K!NG".

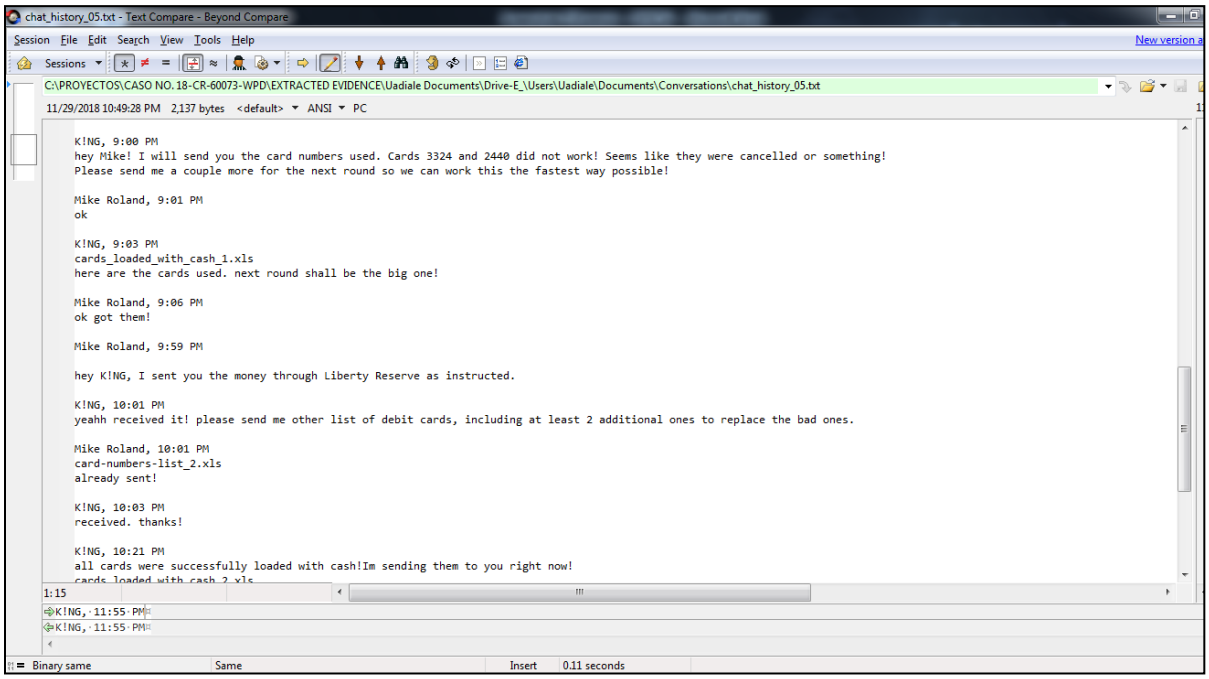


Figura 52. Tercera conversación entre Raymond Uadiale y "K!NG".

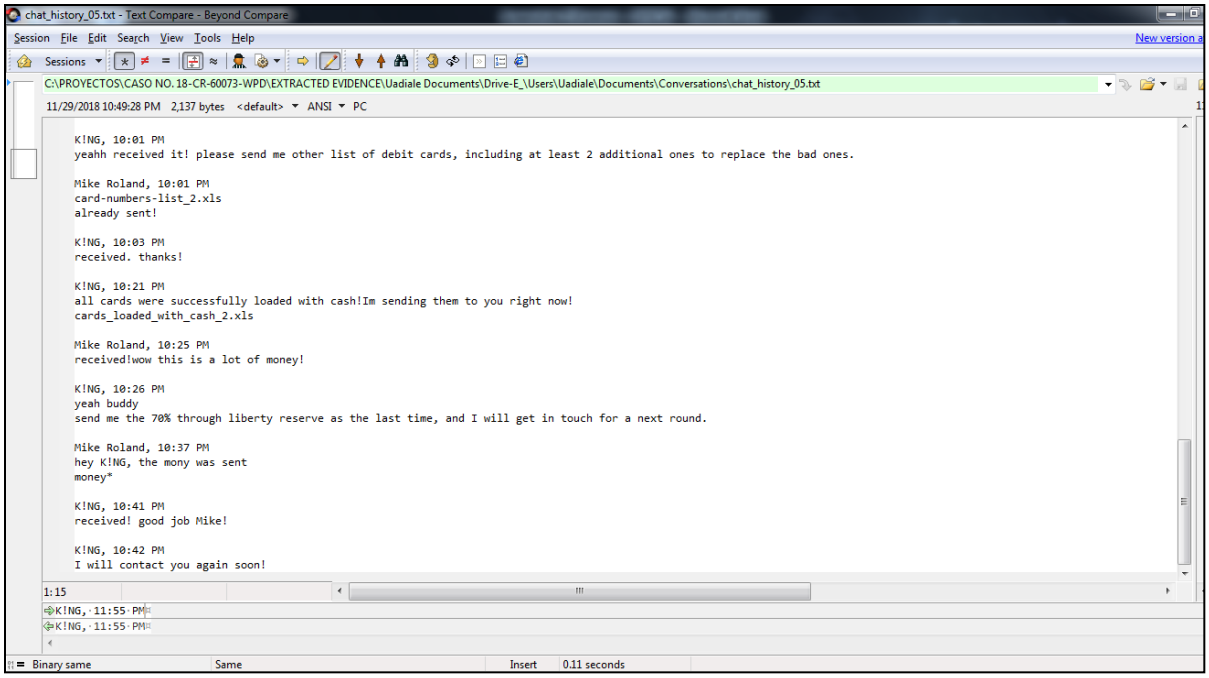


Figura 53. Cuarta conversación entre Raymond Uadiale y “K!NG”.

17. Procedimiento: Analizar hojas de cálculo

    a. Herramienta: Microsoft Excel

    b. Fecha de comienzo: 2 de diciembre de 2018 - 1:40 PM

    c. Fecha de terminación: 2 de diciembre de 2018 - 2:30 PM

    d. Descripción: El directorio de descargas extraído de la imagen, se identifican los archivos *cards_loaded_with_cash_1.xls* y *cards_loaded_with_cash_2.xls* (Figura 54). Se abre el archivo *cards_loaded_with_cash_1.xls*, y se identifica una lista de tarjetas con los fondos depositados (Figura 55). Se abre el archivo *cards_loaded_with_cash_2.xls*, y se identifica una segunda lista de tarjetas con sus fondos depositados (Figura 56).

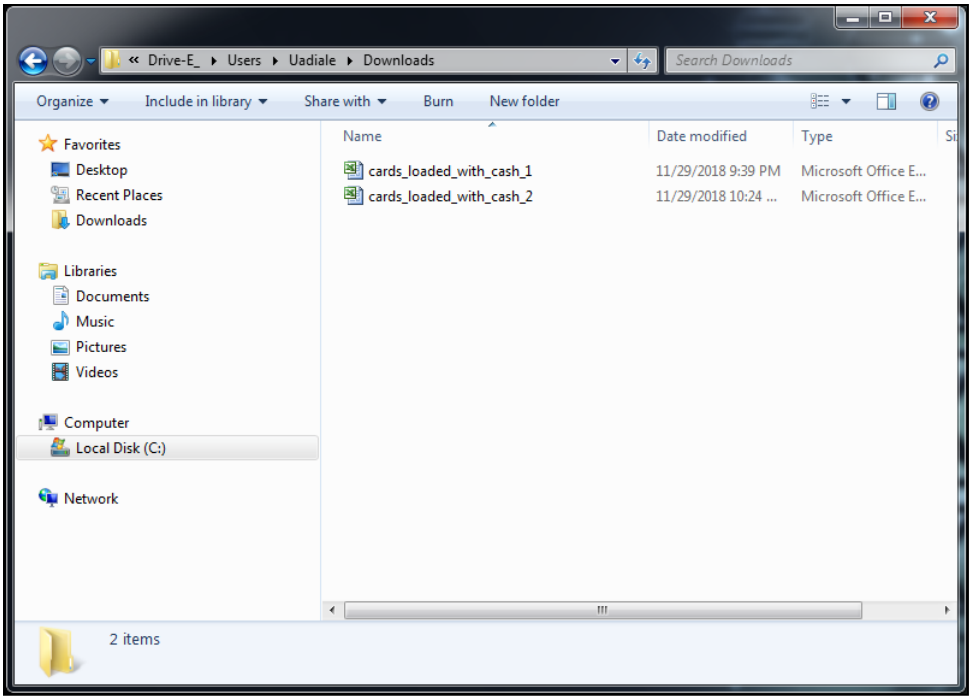
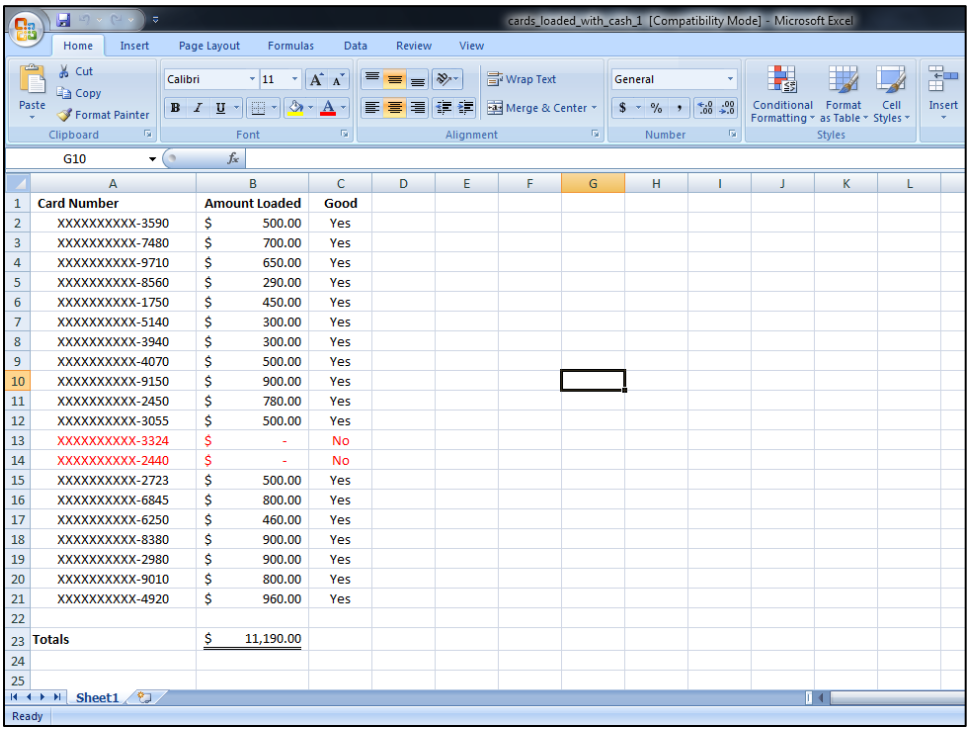
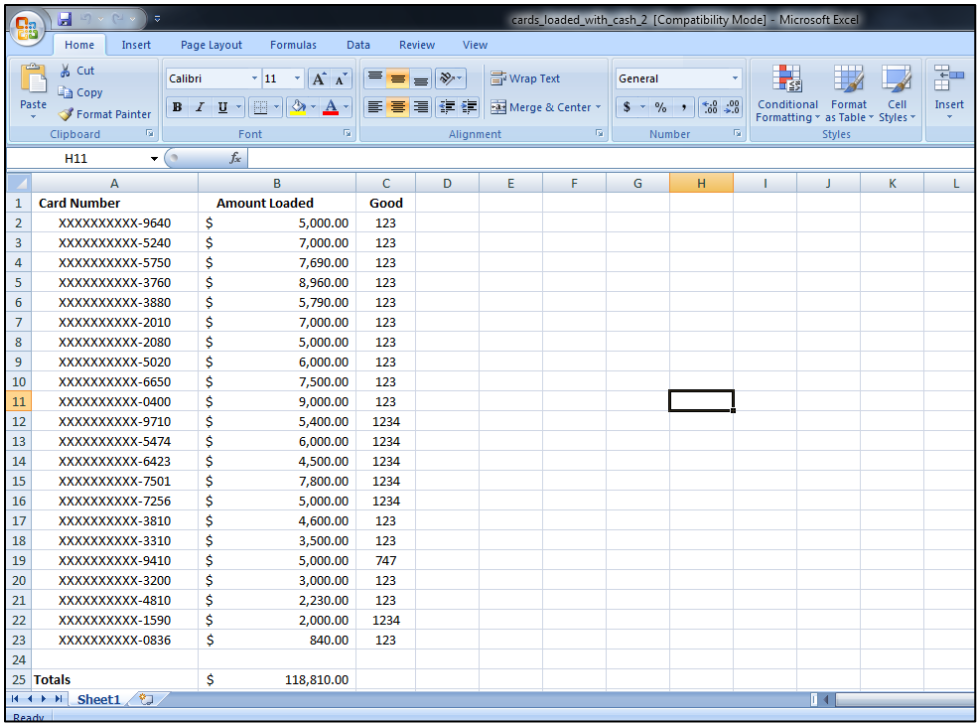


Figura 54. Archivos *cards_loaded_with_cash_1.xls* y *cards_loaded_with_cash_2.xls*.



	A	B	C
1	**Card Number**	**Amount Loaded**	**Good**
2	XXXXXXXXXX-3590	$ 500.00	Yes
3	XXXXXXXXXX-7480	$ 700.00	Yes
4	XXXXXXXXXX-9710	$ 650.00	Yes
5	XXXXXXXXXX-8560	$ 290.00	Yes
6	XXXXXXXXXX-1750	$ 450.00	Yes
7	XXXXXXXXXX-5140	$ 300.00	Yes
8	XXXXXXXXXX-3940	$ 300.00	Yes
9	XXXXXXXXXX-4070	$ 500.00	Yes
10	XXXXXXXXXX-9150	$ 900.00	Yes
11	XXXXXXXXXX-2450	$ 780.00	Yes
12	XXXXXXXXXX-3055	$ 500.00	Yes
13	XXXXXXXXXX-3324	$ -	No
14	XXXXXXXXXX-2440	$ -	No
15	XXXXXXXXXX-2723	$ 500.00	Yes
16	XXXXXXXXXX-6845	$ 800.00	Yes
17	XXXXXXXXXX-6250	$ 460.00	Yes
18	XXXXXXXXXX-8380	$ 900.00	Yes
19	XXXXXXXXXX-2980	$ 900.00	Yes
20	XXXXXXXXXX-9010	$ 800.00	Yes
21	XXXXXXXXXX-4920	$ 960.00	Yes
22			
23	**Totals**	$ 11,190.00	
24			
25			

Figura 55. Primera lista de tarjetas y fondos depositados.



	A	B	C
1	**Card Number**	**Amount Loaded**	**Good**
2	XXXXXXXXX-9640	$ 5,000.00	123
3	XXXXXXXXX-5240	$ 7,000.00	123
4	XXXXXXXXX-5750	$ 7,690.00	123
5	XXXXXXXXX-3760	$ 8,960.00	123
6	XXXXXXXXX-3880	$ 5,790.00	123
7	XXXXXXXXX-2010	$ 7,000.00	123
8	XXXXXXXXX-2080	$ 5,000.00	123
9	XXXXXXXXX-5020	$ 6,000.00	123
10	XXXXXXXXX-6650	$ 7,500.00	123
11	XXXXXXXXX-0400	$ 9,000.00	123
12	XXXXXXXXX-9710	$ 5,400.00	1234
13	XXXXXXXXX-5474	$ 6,000.00	1234
14	XXXXXXXXX-6423	$ 4,500.00	1234
15	XXXXXXXXX-7501	$ 7,800.00	1234
16	XXXXXXXXX-7256	$ 5,000.00	1234
17	XXXXXXXXX-3810	$ 4,600.00	123
18	XXXXXXXXX-3310	$ 3,500.00	123
19	XXXXXXXXX-9410	$ 5,000.00	747
20	XXXXXXXXX-3200	$ 3,000.00	123
21	XXXXXXXXX-4810	$ 2,230.00	123
22	XXXXXXXXX-1590	$ 2,000.00	1234
23	XXXXXXXXX-0836	$ 840.00	123
24			
25	**Totals**	$ 118,810.00	

Figura 56. Segunda lista de tarjetas y fondos depositados.

Conclusión

Los resultados del análisis realizado al dispositivo entregado por el fiscal asistente Jared M. Strauss evidencian que la computadora incautada pertenece a Raymond Uadiale, y que todas las actividades fueron realizadas desde la misma con su cuenta de usuario. De igual manera, los hallazgos de correos electrónicos, páginas web visitadas, *bookmarks* y bitácoras de conversaciones, dejan evidenciado que Raymond Uadiale y Mike Roland son la misma persona. También se confirma que Raymond Uadiale recibió y acató las instrucciones de “K!NG” sobre como operar el esquema de lavado de dinero del que se le acusa como conspirador. Dicha teoría se respalda con el hallazgo de dos (2) documentos en su directorio de descargas con información sobre tarjetas de débito y cantidad de fondos depositados.

SECCIÓN 5: DISCUSIÓN DEL CASO

Según la información obtenida del caso investigado, Raymond Uadiale fue acusado de participar como conspirador en un esquema de lavado de dinero mediante el comercio interestatal e internacional. Al acusado y ahora convicto se le atribuye específicamente el haber utilizado una computadora para comunicarse con su co-conspirador y realizar transferencias de fondos entre diversos instrumentos financieros con el propósito de ocultar su procedencia ilegal.

Los hallazgos identificados en el disco duro de la computadora incautada por el FBI demostraron que: Raymond Uadiale era el dueño de la computadora; las comunicaciones y transacciones fueron efectuadas desde dicho dispositivo con su cuenta de usuario bajo el alias "Mike Roland"; y los documentos encontrados en su carpeta de descargas contenían información sobre tarjetas de débito y cantidad de fondos correspondientes. Dicha evidencia conectó a Raymond Uadiale con los cargos sometidos de lavado de dinero (18 U.S.C. § 1956(a)(1)(B)(i)) y conspiración para cometer lavado de dinero (18 U.S.C. § 1956(h)). Como resultado del análisis del informe pericial, la defensa de Uadiale acordó una declaración de culpabilidad por ambos cargos. Finalmente, Raymond Uadiale fue sentenciado a 18 meses de prisión y tres (3) años de libertad supervisada por el cargo de conspiración para cometer lavado de dinero.

Retomando las diferentes modalidades de lavado de dinero y delitos relacionados según mencionado anteriormente en esta investigación, cabe destacar el *Money Muling* y su posible implicación en el caso de Raymond Uadiale. Como se ha mencionado antes en este trabajo, Raymond Uadiale fue reclutado por un individuo conocido como "K!NG" para ayudarlo a lavar dinero procedente de pagos emitidos por las víctimas del *ransomware* distribuido por este. Durante ese tiempo, Uadiale era estudiante graduado de la Florida International University. Con estos datos se puede crear el perfil de un *money mule*, similar al descrito por Gray (2018), que

incluye a estudiantes y personas con dificultades económicas reclutados para recibir y transferir dinero de procedencia ilegal.

Las motivaciones de Uadiale para participar del esquema analizado en esta investigación se pueden identificar en lo que Boyle, DeZoort, Hermanson y Wolfe (2018) llaman el Diamante del Fraude. Según los autores, el Diamante del Fraude consiste en: incentivo, oportunidad, capacidad y racionalización. Boyle, DeZoort, Hermanson y Wolfe (2018) contrastan este modelo del Triángulo del Fraude de Cressey, haciendo mayor énfasis en las características del individuo y como estas determinan las causas de fraude. Raymond Uadiale tuvo un incentivo para participar en el esquema, tuvo la oportunidad para ejecutar las actividades correspondientes, racionalizó sus acciones, pero sobre todo, tuvo la capacidad a nivel de recursos y conocimiento técnico para ejercer exitosamente su rol.

SECCIÓN 6: AUDITORÍA Y PREVENCIÓN

En esta sección se expondrán las debilidades de controles que propiciaron las circunstancias para que el ataque con el *ransomware* Reveton fuera exitoso, y por consiguiente, se configurara el esquema de lavado de dinero. A continuación, se presenta el informe de auditoría realizado por LAG Audit Services a la Organización XYZ, donde varios equipos fueron impactados por el mencionado *ransomware* y cuyos empleados emitieron los pagos correspondientes para el "rescate" de sus computadoras e información albergada en las mismas.

Trasfondo, alcance y objetivos

El 2 de marzo de 2013, la Organización XYZ fue víctima de un ataque de *ransomware*, lo cual resultó en que sus empleados pagaran una falsa multa a los perpetradores a cambio de devolver el acceso a las computadoras y la información albergada en las mismas. El pago de dicha multa no restauró el acceso a las computadoras y toda la información almacenada en estas fue catalogada como irrecuperable.

A base de dichos acontecimientos, el alcance de esta auditoría giró en torno a examinar la presencia de controles administrativos y seguridad lógica de la Organización XYZ. Para este ejercicio se utilizó como marco de referencia el estándar ISO/IEC 27002:2013. De igual manera, se utilizó el modelo de auditoría propuesto por Davis, Schiller y Wheeler (2011). El mismo hace énfasis en examinar los componentes físicos, *software*, configuraciones, procesos, políticas y documentación de un sistema de información, según ilustrado en la Figura 57.

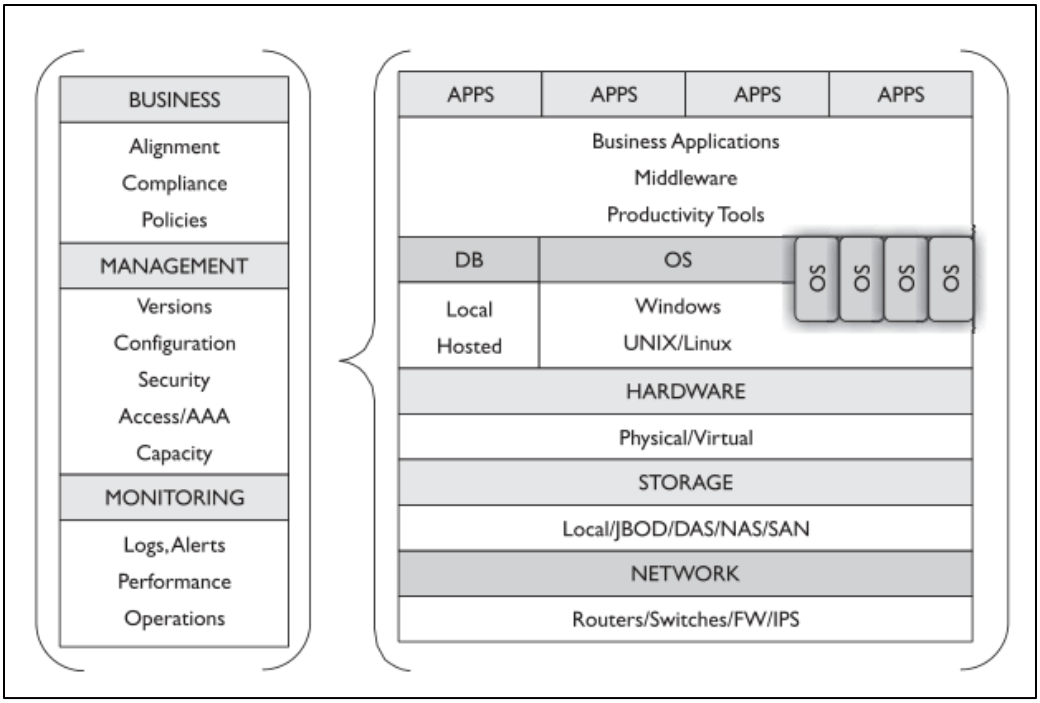


Figura 57. Modelo de auditoría (Davis, Schiller & Wheeler, 2011).

Hallazgos y recomendaciones

A continuación, se esbozan los hallazgos identificados durante la auditoría realizada a la Organización XYZ y las recomendaciones correspondientes para atender los mismos:

Hallazgo 1

Condición - Los empleados no están orientados sobre las políticas de uso aceptable de los recursos tecnológicos de la organización.

Criterio - La *International Organization for Standardization* (2013) indica que las organizaciones deben documentar e implementar políticas de buen uso de la información y activos relacionados al procesamiento de la misma.

Causa - La organización XYZ no posee una política explícita sobre el uso aceptable de sus recursos tecnológicos.

Efecto - Los empleados hicieron mal uso de los recursos tecnológicos provistos por la organización, lo cual resultó que las computadoras se infectaran con el *ransomware* Reveton.

Recomendación - Implementar el control *8.1.3 Acceptable use of assets*, según especificado por la *International Organization for Standardization* (2013).

Hallazgo 2

Condición - Los empleados de la Organización XYZ no poseen conocimientos básicos de los conceptos de seguridad informática.

Criterio - La *International Organization for Standardization* (2013) indica que empleados y contratistas deben recibir adiestramientos sobre seguridad informática basados en sus funciones dentro de la organización.

Causa - La Organización XYZ no ofrece adiestramientos de seguridad informática a su personal.

Efecto - Los empleados emitieron pagos al atacante del *ransomware* Reveton bajo engaño, para saldar una “multa” y recuperar el acceso a las computadoras.

Recomendación - Implementar el control *7.2.2 Information security awareness, education and training*, según especificado por la *International Organization for Standardization* (2013).

Hallazgo 3

Condición - Las computadoras de la Organización XYZ no tienen *software* de antivirus instalado.

Criterio - La *International Organization for Standardization* (2013) indica que las organizaciones deben tener procedimientos y mecanismos de prevención, detección y corrección contra código malicioso.

Causa - La Organización XYZ no gestionó la compra e instalación de *software* antivirus corporativo.

Efecto - Las computadoras de la Organización XYZ fueron infectadas con el *ransomware* Reveton.

Recomendación - Implementar el control *12.2.1 Controls against malware*, según especificado por la *International Organization for Standardization* (2013).

Hallazgo 4

Condición - Todos empleados de la Organización XYZ tienen nivel de acceso de administrador en sus cuentas de usuario.

Criterio - La *International Organization for Standardization* (2013) indica que las organizaciones deben tener un procedimiento para crear y desactivar cuentas de acceso a los sistemas de información. Del mismo modo, deben tener un procedimiento para revisar periódicamente los niveles de acceso de los usuarios.

Causa - La Organización XYZ no posee un procedimiento formal para la creación, el registro y revisión de cuentas de usuario en sus sistemas.

Efecto - El *ransomware* Reveton se descargó e instaló exitosamente en las computadoras usando los privilegios de administrador de sus usuarios.

Recomendación - Implementar los controles *9.2.1 User registration and de-registration*, *9.2.3 Management of privileged access rights*, *9.2.5 Review of user access rights* y *9.2.6 Removal or adjustment of access rights*, según especificados por la *International Organization for Standardization* (2013).

Hallazgo 5

Condición - La Organización XYZ no posee *backups* recientes de sus sistemas y datos.

Criterio - La *International Organization for Standardization* (2013) indica que, como mecanismo de prevención contra la pérdida de datos, las organizaciones deben tener un procedimiento para ejecutar y probar *backups* regularmente.

Causa - El departamento de IT de la Organización XYZ no tiene un procedimiento formal para ejecutar *backups* regulares de sus sistemas y datos.

Efecto - No se pudo recuperar la información albergada en las computadoras infectadas por el *ransomware* Reveton.

Recomendación - Implementar el control *12.3.1 Information backup*, según especificado por la *International Organization for Standardization* (2013).

SECCIÓN 7: CONCLUSIÓN

Durante la investigación de este caso, se pudo apreciar la manera como un incidente de *malware* resultó ser parte de un esquema internacional de lavado de dinero. Utilizando como marco teórico el Árbol del Fraude de Internet propuesto por Wells (2010), se pudo clasificar el delito perpetrado como *Hacking, Cyberterrorism, and Sabotage*, e *Internet Fraud: Other*. Asímismo, analizando el perfil de Raymond Uadiale, se pudo categorizar al mismo como un *money mule*, según descrito por Gray (2018). De igual manera, tomando en consideración las características y capacidades individuales del perpetrador, se utilizó como marco de referencia el Diamante del Fraude según propuesto por Boyle, DeZoort, Hermanson y Wolfe (2018), para explicar las circunstancias y motivaciones que llevaron al acusado a participar del mencionado esquema. Adicional a ello, se identificaron deficiencias en controles administrativos y de seguridad lógica en una organización, lo cual resultó en que sus computadoras se infectaran con el *ransomware* y que a la vez sirvió de vehículo para perpetrar el esquema de lavado de dinero.

Haciendo hincapié en la deficiencia de controles, es imperativo entender la condición humana y el riesgo que representa al entorno operacional de una organización. Considerando la naturaleza y magnitud del caso analizado, se puede concluir que el control más importante es la educación. Como parte de esta, resulta de vital importancia instruir a los usuarios y a la población general sobre los peligros inmediatos y las consecuencias nefastas a nivel macro del uso negligente de la tecnología.

SECCIÓN 8: REFERENCIAS

ACFE. (2018a). *Fraud examiners manual*. (US ed.). Section 1 – Computer and Internet Fraud (p. 1.1401). Austin, TX: Association of Certified Fraud Examiners.

ACFE. (2018b). *Fraud examiners manual*. (US ed.). Section 1 – Computer and Internet Fraud (p. 1.1402). Austin, TX: Association of Certified Fraud Examiners.

ACFE. (2018c). *Fraud examiners manual*. (US ed.). Section 2 – Money Laundering (p. 2.601). Austin, TX: Association of Certified Fraud Examiners.

ACFE. (2018d). *Fraud examiners manual*. (US ed.). Section 1 – Computer and Internet Fraud (p. 1.1417). Austin, TX: Association of Certified Fraud Examiners.

ACFE. (2018e). *Fraud examiners manual*. (US ed.). Section 1 – Computer and Internet Fraud (pp. 1.1426 - 1.1427). Austin, TX: Association of Certified Fraud Examiners.

ACFE. (2018f). *Fraud examiners manual*. (US ed.). Section 1 – Computer and Internet Fraud (p. 1.1436). Austin, TX: Association of Certified Fraud Examiners.

ACFE. (2018g). *Fraud examiners manual*. (US ed.). Section 2 – Money Laundering (p. 2.601). Austin, TX: Association of Certified Fraud Examiners.

ARC Group. (2018). ProDiscover Basic. Recuperado el 30 de noviembre de 2018 de http://www.arcgroupny.com/products/prodiscover-basic/

Boyle, D., DeZoort, F., Hermanson, D. & Wolfe, D. (2018, March/April). Improving fraud risk management with an enhanced Fraud Triangle. *Fraud Magazine*, *33*(2). Recuperado de https://www.fraud-magazine.com/article.aspx?id=4295000903

CipherTrace. (2018, July 3). Cryptocurrency anti-money laundering report. Recuperado de https://cdn2.hubspot.net/hubfs/4345106/crypto_aml_report_2018q2.pdf?submissionGuid=eedf473e-eb36-456b-90c9-1c3a58443f6b

ClamWin. (2018). ClamWin Free Antivirus. Recuperado el 30 de noviembre de 2018 de http://www.clamwin.com/content/view/71/1/

Cloherty, J. (2013, May 28). “Black market bank” accused of laundering $6B in criminal proceeds. *ABC News.* Recuperado de https://abcnews.go.com/US/black-market-bank-accused-laundering-6b-criminal-proceeds/story?id=19275887

Davis, C., Schiller, M. & Wheeler, K. (2011). *IT auditing: Using controls to protect information assets* (2nd ed.). New York, NY: McGraw-Hill.

Department of Justice. (2018, March 6). Dual Israeli/Russian citizen sentenced to 18-month prison term on money laundering charge in international scheme. Recuperado de https://www.justice.gov/usao-dc/pr/dual-israelirussian-sentenced-18-month-prison-term-money-laundering-charge-international

Department of Justice. (2016, May 6). Liberty reserve founder Arthur Budovsky sentenced in Manhattan Federal Court to 20 years for laundering hundreds of millions of dollars through his global digital currency business. Recuperado de https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years

Department of Justice. (2018, July 26). Defendant sentenced in international business email compromise scam. Recuperado de https://www.justice.gov/usao-ndga/pr/defendant-sentenced-international-business-email-compromise-scam

Department of Justice. (2018, August 13). Washington state man sentenced to prison for role in connection with Reveton ransomware. Recuperado de https://www.justice.gov/opa/pr/washington-state-man-sentenced-prison-role-connection-reveton-ransomware

Federal Bureau of Investigation. (s.f). Internet fraud. Recuperado el 17 de noviembre de 2018, de https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud

Federal Bureau of Investigation. (2012, August 9). *New internet scam.* Recuperado de https://www.fbi.gov/news/stories/new-internet-scam

Fraud and related activity in connection with computers, 18 U.S.C. §1030 (1986). Recuperado de https://www.gpo.gov/fdsys/pkg/USCODE-2017-title18/pdf/USCODE-2017-title18-partI-chap47-sec1030.pdf

Gray, I. (2018, July 30). Money mules remain instrumental in money-laundering schemes. Recuperado de https://www.flashpoint-intel.com/blog/money-mules-remain-instrumental/

Iannelli, J. (2018, August 14). Microsoft worker from FIU gets jail time for fake FBI ransomware attacks. *Miami New Times.* Recuperado de https://www.miaminewtimes.com/news/microsoft-fiu-hacker-gets-jail-for-reveton-ransomware-virus-10625753

International Monetary Fund. (s.f.). *Anti-money laundering/combating the financing of terrorism.* Recuperado del 19 de noviembre de 2018, de https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm

International Organization for Standardization. (2013). *ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls.* Geneva, Switzerland: ISO/IEC.

Laundering of monetary instruments, 18 U.S.C. § 1956 (1986). Recuperado de https://www.gpo.gov/fdsys/pkg/USCODE-2017-title18/pdf/USCODE-2017-title18-partI-chap95-sec1956.pdf

McMahon, P. (2018, April 12). Microsoft network engineer charged with money laundering linked to Reveton computer ransomware. *Sun Sentinel.* Recuperado de https://www.sun-sentinel.com/local/broward/fl-reg-computer-malware-reveton-ransomware-20180412-story.html

Mundie, A. (2012, May/June). International money laundering, part 1 of 2: The human toll. *Fraud Magazine, 27*(3). Recuperado de https://www.fraud-magazine.com/article.aspx?id=4294972748

Neal, D. (2018, August 16). They froze computers, then demanded ransom. A former FIU student is going to prison. *Miami Herald.* Recuperado de https://www.miamiherald.com/news/local/crime/article216654040.html

Nigerian network engineer who works for Microsoft accused of Reveton ransomware (2018, April 16). *USA Crime Today.* Recuperado de https://usacrimetoday.com/nigerian-network-engineer-works-microsoft-accused-reveton-ransomware/

PassMark Software. (2018a). *OSF Mount.* Recuperado el 30 de noviembre de 2018 de https://www.osforensics.com/tools/mount-disk-images.html

PassMark Software. (2018b). *Products & tools.* Recuperado el 24 de noviembre de 2018 de https://www.osforensics.com/products.html

Renner, P. (s.f.). *What is money laundering? The three stages in money laundering.* Recuperado el 19 de noviembre de 2018, de http://kycmap.com/what-is-money-laundering/

Scooter Software. (2018). Intelligent comparison. Recuperado el 30 de noviembre de 2018 de http://www.scootersoftware.com/features.php?zz=features_focused

Tie, R. (2012, May/June). Money laundering, 21st century-style, part 1 of 2: Far from washed up. *Fraud Magazine, 27*(3). Recuperado de https://www.fraud-magazine.com/article.aspx?id=4294972746

Uadiale Nigerian Microsoft engineer faces cyber theft charge in Florida. (2018, April 17). *News Agency of Nigeria (NAN)*. Recuperado de https://www.nan.ng/news/uadiale-nigerian-microsoft-engineer-faces-cyber-theft-charge-in-florida/

United States v. Liberty Reserve, 13-CR-368 (S.D.N.Y., 2013). Recuperado de https://www.justice.gov/usao/nys/pressreleases/May13/LibertyReserveetalDocuments/Liberty%20Reserve%2C%20et%20al.%20Indictment%20-%20Redacted.pdf

United States v. Nazarov, 1:17-CR-00018-CKK (D.D.C., 2017). Recuperado de https://www.courtlistener.com/recap/gov.uscourts.dcd.184184/gov.uscourts.dcd.184184.1.0.pdf

United States v. Uadiale, 18-CR-60073-WPD (S.D. Fla., 2018a). Recuperado de https://www.courtlistener.com/recap/gov.uscourts.flsd.523847/gov.uscourts.flsd.523847.1.0_5.pdf

United States v. Uadiale, 18-CR-60073-WPD (S.D. Fla., 2018b). Recuperado de https://www.courtlistener.com/recap/gov.uscourts.flsd.523847/gov.uscourts.flsd.523847.8.0.pdf

United States v. Uadiale, 18-CR-60073-WPD (S.D. Fla., 2018c). Recuperado de https://www.courtlistener.com/recap/gov.uscourts.flsd.523847/gov.uscourts.flsd.523847.27.0_1.pdf

Wei, W. (2013, February 14). Group behind largest ransomware campaign arrested by Spanish police. *The Hacker News*. Recuperado de https://thehackernews.com/2013/02/group-behind-largest-ransomware.html

Wells, J. (2010). *Internet fraud casebook: The world wide web of deceit.* Hoboken, NJ: John Wiley & Sons.

Wells, J. (2014). *Principles of fraud examination.* (4th ed.). Hoboken, NJ: John Wiley & Sons.