

EDP UNIVERSITY OF PUERTO RICO, INC.
RECINTO DE HATO REY
PROGRAMA DE MAESTRÍA EN SISTEMAS DE INFORMACIÓN CON
ESPECIALIDAD EN SEGURIDAD DE INFORMACIÓN E INVESTIGACIÓN DE
FRAUDE DIGITAL

**ESQUEMA FRAUDULENTO DE VOUCHERS FALSOS
ANÁLISIS DE CASO: UNITED STATES OF AMERICA VS. PATRICIA
URBANOVSKY**

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÓN CON
ESPECIALIDAD EN SEGURIDAD DE INFORMACIÓN E INVESTIGACIÓN DE
FRAUDE DIGITAL

MARZO, 2019

PREPARADO POR
CATHY PIÑERO CAMACHO

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

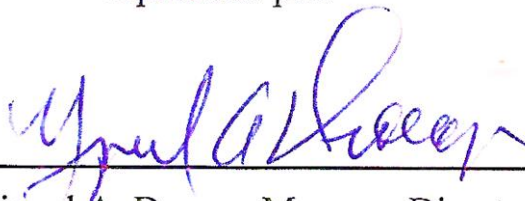
**ESQUEMA FRAUDULENTO DE VOUCHERS FALSOS
ANÁLISIS DE CASO: UNITED STATES OF AMERICA VS. PATRICIA
URBANOVSKY**

Preparado por
Cathy Piñero Camacho

Ha sido aceptado como requisito parcial para el grado de
Programa de Maestría en Sistemas de información con especialidad en seguridad de
información e investigación de fraude digital

MARZO, 2019

Aprobado por:



Dr. Miguel A. Drouyn Marrero, Director

TABLA DE CONTENIDO

INTRODUCCIÓN Y TRASFONDO	1
Introducción	1
Descripción del caso	2
Trasfondo	3
Descripción de Hechos	5
Acusaciones y cargos	7
Penalidad.....	9
Definición de términos.....	9
REVISIÓN DE LITERATURA	11
Introducción	11
Fraudes involucrados	11
Leyes aplicables	17
Casos Relacionados	18
Herramientas de investigación.....	21
SIMULACIÓN	24
INFORME DEL CASO	26
Resumen Ejecutivo	26
Objetivo.....	26
Alcance del trabajo	27
Datos del caso	27
Descripción de los dispositivos utilizados	27
Resumen de hallazgos.....	29
Cadena de custodia	37
Procedimiento	40
Conclusión	50
DISCUSIÓN DEL CASO	51
AUDITORÍA Y PREVENCIÓN.....	53
CONCLUSIÓN	55
REFERENCIAS	56

TABLA DE FIGURAS

Figura 1: Estadística general de quejas del IC3 (FBI, s.f.d).	13
Figura 2: Estadística de reclamaciones por Estado del IC3 (FBI, s.f.d).....	15
Figura 3: Estadística de pérdidas económicas del IC3 (FBI, s.f.d)	16
Figura 4: Esquema de fraude de la señora Urbanovsky	25
Figura 5: Sistema Microsoft Windows XP Professional 2002	28
Figura 6: USB Drive de 4GB marca <i>PNY Attaché</i>	28
Figura 7: Herramienta AccessData FTK Imager 3.1.4.6.....	29
Figura 8: Documento encontrado con el nombre Invoice 000123.	30
Figura 9: Documento encontrado con el nombre Invoice 000124.	31
Figura 10: Documento encontrado con el nombre Invoice 000125.	32
Figura 11: Documento encontrado con el nombre Publication2.	33
Figura 12: Correo electrónico enviado el 11/03/2014.....	34
Figura 13: Correo electrónico enviado el 12/01/2014.....	35
Figura 14: Correo electrónico enviado el 12/18/2014.....	35
Figura 15: Correo electrónico enviado el 1/2/2015.....	36
Figura 16: Correo electrónico enviado el 1/29/2015	36
Figura 17: Pantalla principal del dispositivo utilizado para el análisis.	41
Figura 18: Pantalla inicial de AccessData FTK Imager 3.1.4.6.	41
Figura 19: Información del caso y evidencia.....	42
Figura 20: Inicio de creación de imagen.	43
Figura 21: Proceso de creación de imagen.	43
Figura 22: Confirmación completada de creación de imagen	44
Figura 23: Validación de Hash MD5 y Hash SHA1	44
Figura 24: Documentos encontradas en el archivo Invoice.....	45
Figura 25: Primer documento - Invoice 000123.....	46
Figura 26: Segundo documento- Invoice 000124.....	46
Figura 27: Tercer documento - Invoice 000125	47
Figura 28: Cuarto documento – Publication2.....	47
Figura 29: Quinto document- 1-2-2015.....	48
Figura 30: Sexto documento - Bookings will be completed 1-29-2015.....	48
Figura 31: Séptimo documento - Last sales of the year 12-18-2014.....	49
Figura 32: Octavo documento - Station- declined 12-01-2014	49
Figura 33: Noveno documento - 11-03-2014	50

SECCIÓN 1: INTRODUCCIÓN Y TRASFONDO

Introducción

Se dice que la mejor forma de sentir es viajar. Todos sabemos que quien se prepara a salir de su casa rumbo al aeropuerto experimenta una adrenalina distinta a cualquier otra. Cuando el viajero deja atrás todo lo que le resulta familiar y cómodo (para así agarrar su maleta, abordar un avión y atravesar un océano hacia lo desconocido) siente de forma intensa que está viviendo un sueño. Luego, al salir de su hospedaje en el país nuevo con el fin de adentrarse en una ciudad encantadora y acercarse a una cultura diferente a la suya, dicha emoción se transforma en euforia. En muchas instancias ese sentimiento que produce viajar es tan positivo y terapéutico que lo solemos describir con frases como: “recargar baterías”, “desconectarse” o simplemente “irse de vacaciones”. También es un gran sacrificio que no muchas personas pueden realizar, ya que viajar requiere tener dinero adicional al que precisamos para cubrir las necesidades de nuestro diario vivir. Por esta razón, una de las experiencias más decepcionantes que puede tener una persona trabajadora es perder, mediante fraude o estafa, el dinero que con tanto esfuerzo ahorró para darse la oportunidad de viajar.

Entre los tipos de fraudes relacionados a viajes más comunes se encuentran: el recibo de anuncios falsos de que se ganó un premio por sorteo y que se debe redimir proveyendo información sensible, las páginas de Internet simuladas donde estafadores venden paquetes de vacaciones inexistentes, agencias de viaje autorizadas que prometen ofertas que una vez compradas e iniciado el viaje misteriosamente se cancelan, entre muchos otros (BBB, 2017). Por lo general, las víctimas de estos esquemas de fraude son personas descuidadas, o con poca experiencia planificando sus viajes, que confían

ciegamente en un tercero sin cotejar la autenticidad del negocio, la veracidad de sus representaciones o el historial de mercado a la hora de rendir dichos servicios.

En este informe presentaremos la comisión de un fraude en el estado de Nebraska en los Estados Unidos de América, el cual fue dirigido a personas que confiaron en una compañía de coordinación de eventos, que a su vez vendía *vouchers* de viajes, sólo para luego ser víctimas de un esquema similar al llamado Ponzi. La dueña de *Creative Creations*, que luego se declaró culpable en el caso que analizaremos a continuación, es la Sra. Patricia Urbanovsky y mediante sus actos delictivos defraudó a sus clientes por la suma de casi \$5,000,000.00 (United States of America vs. Patricia M. Urbanovsky, 2016). Para todas sus víctimas de fraude que sólo querían sentir la felicidad de “recargar baterías”, “desconectar” o simplemente “irse de vacaciones”, el viaje de ensueño se convirtió en una pesadilla.

Descripción del caso

Caso: United States of America vs. Patricia M. Urbanovsky

Número del Caso: 8:16CR52

Partes en el caso:

Acusada: Patricia M. Urbanovsky

Víctimas: Square, Inc.

Clientes de *Creative Creations*

Investigadores: Departamento de Policía de Omaha, Nebraska

Oficina Federal de Investigaciones (FBI, por sus siglas en inglés)

Servicios de Impuestos Internos (IRS, por sus siglas en inglés)

Abogado de defensa: Lcdo. Steven J. Lefler

Bufete de abogados Lefler y Kuehl

Fiscal: Lcdo. Donald J. Kleine

Fiscal Auxiliar de los Estados Unidos de América del Distrito de Nebraska

Juez: Joseph F. Bataillon, Juez de Distrito de los Estados Unidos para el

Distrito de Nebraska

Trasfondo

Según el documento del caso *United States of America vs. Patricia M. Urbanovsky (2016)*, Patricia M. Urbanovsky, de 32 años, presidenta, única accionista y quien operaba un negocio de planificación de eventos y bodas llamado *Creative Creations* ubicado en Omaha, Nebraska, fue acusada de cometer fraude electrónico, lavado de dinero y realizar transacciones monetarias sobre propiedad proveniente de actividades ilícitas. Desde mayo de 2014 hasta aproximadamente el mes de marzo de 2015, la señora Urbanovsky, personalmente y a través de su compañía *Creative Creations*, ideó y diseñó un esquema para obtener dinero por medio de representaciones y promesas falsas comercializando y promoviendo la venta de paquetes de vacaciones y *vouchers* supuestamente asociados con *Southwest Airlines* y *Southwest Vacations*.

Los costos reales del boleto de avión y de los paquetes de vacaciones asociados con los *vouchers* que ella vendía eran significativamente más altos que la cantidad de dinero que un cliente pagaba para comprar dichos productos. A medida que avanzaba el esquema fraudulento, la señora Urbanovsky, intentó que el dinero utilizado para comprar los boletos de avión o paquetes de vacaciones de clientes con *vouchers* ya comprados proviniera del dinero pagado por los clientes nuevos. Esta práctica permitió la prolongación de dicho esquema, pero fue poco rentable, ya que el costo a precio del mercado de los boletos de avión comprados por la señora Urbanovsky excedía constantemente el efectivo recaudado de las nuevas ventas. A pesar de los contratiempos, la acusada continuó procurando clientes

nuevos a través de la promoción de los *vouchers* por debajo del precio del mercado, debido a que su objetivo era mantener una constante entrada de dinero, manteniendo una práctica similar a un esquema Ponzi.

Como parte del esquema fraudulento, la señora Urbanovsky representó falsamente a sus empleados y clientes que mantenía una relación profesional con un supuesto vicepresidente de *Southwest Vacations* y que a través de éste recibía un descuento en los boletos de la línea aérea *Southwest Airlines*. Sin embargo, esta compañía de vuelos nunca tuvo relación o afiliación alguna con la acusada ni con su compañía, *Creative Creations*.

A finales de marzo de 2015 el esquema colapsó. Esto se debió a que el dinero y las líneas de crédito se habían agotado y la acusada no pudo generar fondos suficientes de las nuevas ventas para mantener la ficción a flote. Para esta fecha, un cliente que no pudo reclamar su *voucher* presentó una querrela a la compañía de su tarjeta de crédito. Dicha compañía, a su vez, le informó a *Square, Inc.*, un procesador de tarjetas de crédito con sede en California, sobre la disputa con el cliente. *Square, Inc.*, le envió un correo electrónico a la señora Urbanovsky notificándole de la disputa. En dicha comunicación se le solicitó que confirmara si dicha transacción era legítima.

La acusada utilizaba a *Square, Inc.*, para tramitar las transacciones provenientes de la venta de *vouchers* y paquetes de vacaciones. Entre el mes de mayo de 2014 y el mes de marzo de 2015, *Square, Inc.*, depositó aproximadamente \$ 6,719,724.00 en cuentas financieras utilizadas por la acusada. Hay que señalar que *Square, Inc.*, envió alrededor de 7,280 correos electrónicos solicitándole que confirmara si las transacciones reclamadas por los clientes eran legítimas, de las cuales la Sra. Urbanovsky sólo respondió a menos de 15 correos electrónicos y después del mes de marzo 2015 no respondió a ningún otro correo electrónico enviado por *Square, Inc.*

Square, Inc., fue la víctima principal de los actos fraudulentos de la señora Urbanovsky, ya que sufrió una pérdida económicamente de más de \$ 4,600,000.00 como resultado de los cargos de las tarjetas de crédito de las cuentas *Creative Creations*.

Descripción de Hechos

La siguiente lista es una relación descriptiva de los hechos ocurridos asociados al caso United States of America vs. Patricia M. Urbanovsky (2016):

- Desde el mes de mayo de 2014 hasta aproximadamente el mes de marzo de 2015, la señora Urbanovsky personalmente y a través de su negocio *Creative Creations*, comenzó a mercadear y a promocionar la venta de paquetes vacacionales y *vouchers* asociados con *Southwest Airlines* y *Southwest Vacations*.
- Los *vouchers* para vuelos domésticos fluctuaban entre \$ 78 a \$ 139 dólares por vuelo, mientras que los *vouchers* para vuelos internacionales variaban entre \$ 189 a \$ 250 dólares. El costo de estos *vouchers* incluía el pasaje aéreo, impuestos y cargos.
- La señora Urbanovsky les garantizaba a los clientes la fecha y el destino para viajar, pero no garantizaba la hora del vuelo.
- Como incentivo para promocionar y vender dichos *vouchers* la señora Urbanovsky pagaba a sus empleados una comisión por cada cupón vendido.
- Los clientes que compraban *vouchers* suministrarían a la señora Urbanovsky o a los empleados de *Creative Creations*, su nombre, correo electrónico, dirección, número de teléfono e información de la tarjeta de crédito. Dicha información era ingresada a una aplicación móvil llamada *Square, Inc.* la cual se usó para procesar los pagos.

- Después de finalizar la venta, la señora Urbanovsky o sus empleados creaban una factura que luego se les entregaban a los clientes como confirmación de la compra, esta factura servía como el *voucher* para los clientes.
- Para cambiar el *voucher* por un boleto de avión, los clientes deberían de notificar a *Creative Creations* entre treinta (30) a noventa (90) días antes del vuelo deseado.
- Los empleados de *Creative Creations* facilitarían a la señora Urbanovsky los tres precios de vuelo más bajos del sitio web de *Southwest Airlines* y ella haría la compra del boleto de avión para el cliente.
- Los clientes de *Creative Creations* eran mayormente de Estados Unidos: individuos, organizaciones de caridad, iglesias, empresas e instituciones educativas.
- La señora Urbanovsky se comunicaba regularmente con los clientes a través de correo electrónico.
- En diciembre de 2014, la señora Urbanovsky convenció a sus empleados para que usaran sus tarjetas de crédito personales para comprar boletos de avión para los clientes de *Creative Creations*. La señora Urbanovsky les dijo a sus empleados que dicho dinero sería reembolsado, algunos empleados aceptaron.
- Inicialmente pudo reembolsar el dinero de las tarjetas de crédito a sus empleados, pero en marzo de 2015 no cumplió con el reembolso el cual sobrepasaba los \$ 100,000.
- La señora Urbanovsky hizo falsas declaraciones y representaciones a sus empleados y clientes, diciendo que tenía una relación profesional con Christopher Frederick, un supuesto vicepresidente de *Southwest Vacations*.
- La señora Urbanovsky sabía que *Southwest Airlines* y *Southwest Vacations* no tenía un empleado con el nombre de Christopher Frederick o algún programa de *vouchers*.

- En el 2014 *Southwest Airlines* le envía una carta a la señora Urbanovsky exigiendo que *Creative Creations* dejara de usar el nombre de *Southwest Airlines* en la venta de los *vouchers*. Después de recibir la comunicación de *Southwest Airlines*, la señora Urbanovsky le indicó a sus empleados que en cualquier escrito o anuncio utilicen "SW" en vez de *Southwest*.
- En 30 de octubre de 2014 se hizo pasar por Frederick, creando una dirección de correo electrónico, identificada como christopherfrederickXXX@xxxxx.com. Usando esta dirección envió correos electrónicos a los empleados de *Creative Creations*.
- A partir de mayo de 2014 y aproximadamente hasta marzo de 2015, *Creative Creations* había vendido más de 36,000 *vouchers*.
- Para mayo de 2014 y aproximadamente hasta marzo de 2015, *Creative Creations* compró aproximadamente 7,000 boletos de avión de ida y vuelta de *Southwest Airline*.
- En marzo de 2015, la Sra. Urbanovsky realizó un viaje a México con clientes que compraron un paquete de vacaciones el cual le costó al menos \$169,000 y le cobró un total aproximado de \$80,000.
- Luego de ese viaje a México a finales del mes de marzo de 2015 el esquema colapsó.

Acusaciones y cargos

A la señora Urbanovsky se le presentaron los siguientes cargos:

1. Dieciséis (16) cargos por cometer fraude por cable, radio o televisión bajo la disposición legal del título 18 U.S.C. § 1343. Para ejecutar el esquema descrito anteriormente, la Sra. Urbanovsky utilizó medios de comunicaciones electrónicos o por cable en el comercio interestatal, envió correos electrónicos y publicó anuncios y promociones en redes sociales que contenían informaciones falsas, además de

realizar transferencias bancarias electrónicas a *Square, Inc.* (U.S.A vs. Patricia M. Urbanovsky, 2016, p.14)

2. Cinco (5) cargos por participación en transacciones monetarias en propiedades derivadas de actividades ilícitas bajo la disposición legal del título 18 de U.S.C. § 1957. La señora Urbanovsky realizó transacciones, sobrepasando los \$10,000.00, que afectaron el comercio interestatal y extranjero mediante el retiro de fondos, la ejecución y la entrega de cheques de las cuentas bancarias 8285 del *U.S. Bank* y 0806 y 7813 del *Wells Fargo Bank*, ambos bancos ubicadas en Omaha, Nebraska (U.S.A vs. Patricia M. Urbanovsky, 2016, p.15).
3. Cuatro (4) cargos por lavado de dinero bajo la disposición legal del título 18 de U.S.C. § 1956(a)(1)(A)(i). La señora Urbanovsky realizó transacciones bancarias tales como el retiro de fondos y la entrega de cheques de las cuentas bancarias 8285 del *U.S. Bank* y 7813 del *Wells Fargo Bank*, ambos bancos ubicadas en Omaha, Nebraska (U.S.A vs. Patricia M. Urbanovsky, 2016, p.16). Dichos bienes eran producto de una actividad ilegal violatoria del título 18 U.S.C. § 1343 (fraude por cable, radio o televisión).
4. Todos estos cargos se le imputaron a la acusada como autora de los delitos bajo la disposición legal del título 18 de U.S.C. § 2, ya que ésta fue quien ideó y ejecutó el esquema de fraude, personalmente y a través de sus empleados, anunciando, comercializando y vendiendo productos, promociones y servicios de *vouchers* los cuales eran falso.

Penalidad

La señora Urbanovsky aceptó el acuerdo con fiscalía federal (*plea bargain*) y se declaró culpable de los dieciséis (16) cargos de fraude electrónico. El Honorable Joseph F. Bataillon, Juez de la Corte de los Estados Unidos para el Distrito de Nebraska, condenó a la acusada a un período de sesenta y tres (63) meses de prisión sin libertad condicionada. Después de su liberación, la señora Urbanovsky comenzará un período de libertad supervisada por tres (3) años. Además, se le ordenó restituir la suma de \$ 4,700,000.00, el equivalente a la cantidad defraudada.

Definición de términos

Correo electrónico: Sistema de transmisión de mensajes por computadora a través de redes informáticas (Real Academia Española, 2018a).

Esquema Ponzi: esquema fraudulento que promete un alto rendimiento financiero o dividendos no disponibles a través de las inversiones tradicionales. Sin embargo, en lugar de invertir los fondos de las víctimas, el estafador paga "dividendos" a los inversores iniciales utilizando los fondos de los inversores posteriores. El esquema generalmente se derrumba cuando el operador huye con todas las ganancias o cuando no se puede encontrar un número suficiente de nuevos inversores para permitir el pago continuo de "dividendos" (Federal Bureau Investigation, s.f.a).

Fraude: El fraude puede abarcar cualquier delito para obtener una ganancia valiéndose del engaño como su principal modus operandi. Según el *Black's Law Dictionary (2004)*, el fraude se define como: una declaración falsa a sabiendas de la verdad o la ocultación de un hecho material para inducir a otro a actuar a en su detrimento. El fraude incluye cualquier

acto intencional o deliberado de privar a otro de una propiedad o dinero por la astucia, el engaño, la treta u otros actos desleales.

Fraude en Internet: es el uso de servicios de Internet o software con acceso al Internet con el fin de defraudar o aprovecharse de una víctima (Federal Bureau Investigation, s.f.b).

Restitución: Volver algo a quien lo tenía antes. Restablecer o poner algo en el estado que antes tenía (Real Academia Española, 2018b).

Square, Inc.: Compañía fundada en 2009 con sede en San Francisco, California, la cual proporciona soluciones de pago que permite realizar transacciones comerciales con tarjetas de banda magnética (*Square, Inc.*, 2018).

Tarjeta de crédito: tarjeta de plástico compuesta por una banda magnética o un microchip, la cual le permite a su titular pagar por productos o servicios sin necesidad de disponer de dinero en efectivo o cheques (Economía Simple, 2016).

Vouchers: es un término en inglés, el cual puede ser traducido como cupón, vale o comprobante. Según la Real Academia Española (2018c) es parte de un anuncio que se corta y que da derecho a participar en concursos o sorteos o a obtener una rebaja de precio en las compras. En el presente caso, dicho término aplica a la rebaja de precio en una compra.

SECCIÓN 2: REVISIÓN DE LITERATURA

Introducción

El fraude electrónico es un problema mundial que va en aumento y que nos afecta negativamente como sociedad. En los últimos años se han hecho grandes avances para combatir el mismo. Los ciudadanos, en general, se están educando cada vez más en torno a este tema gracias a páginas web como la de *Better Business Bureau (BBB)*, la cual sirve como guía para: crear una asociación de negocios confiables, establecer estándares para la confianza del mercado, celebrar los buenos modelos del mercado; además de permitir a los usuarios denunciar conductas inapropiadas en el mercado (BBB, 2018). Al igual que BBB, se encuentra la página de *Internet Crime Complaint Center (IC3)*, la cual le provee al público un mecanismo de información confiable y conveniente para enviar información a la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés) sobre presuntas actividades delictivas realizadas a través del Internet. La misma analiza e investiga la información suministrada, cuyo resultado luego se divulga para el conocimiento público. Desde el año 2000, IC3 ha recibido quejas relacionadas a fraudes electrónicos, lavado de dinero, robo de identidad, entre otros asuntos, con el fin de minimizar el fraude por Internet y de que el ciudadano promedio pueda distinguirlo de otros delitos o fraudes (FBI, s.f.c).

Fraudes involucrados

En el caso de la señora Urbanovsky, se observa que ésta se declaró culpable de realizar dieciséis (16) cargos de fraude electrónico y que la forma de operar el esquema es bastante similar al esquema Ponzi, para el cual creó y utilizó un correo electrónico falso. Según el FBI (s.f.b), el fraude en Internet se constituye mediante el uso de servicios de Internet, o *software* con acceso al Internet, para defraudar a las víctimas o para de alguna

forma aprovecharse de ellas. Estos esquemas permiten que los delincuentes roben millones de dólares cada año.

El Departamento de Asuntos del Consumidor (2018), define anuncios engañosos como cualquier anuncio que constituya o tienda a constituir fraude, engaño o comunique o tienda a comunicar una idea falsa o incorrecta sobre el bien o servicio anunciado. Al igual que cualquier anuncio que omite datos relevantes del producto, bien o servicio, limitando al consumidor de tomar decisiones informadas e inteligentes.

Según el FBI (s.f.b), otros casos más frecuentes de fraude electrónico incluyen: fraude comercial, fraude con tarjetas de crédito, fraude en subastas por Internet, esquemas de inversión y fraude de cartas en Nigeria. Para obtener información sobre las quejas y las estafas más comunes, se recomienda que los usuarios consulten el *Internet Crime Complaint Center* (IC3) y el *National White Collar Crime Center* (NW3C).

El *National White Collar Crime Center* (NW3C, 2014) es un centro que ofrece un sistema de apoyo a nivel nacional para las agencias policíacas y agencias del orden público encargadas de la prevención, investigación y procesamiento de delitos económicos y de alta tecnología. La NW3C recomienda que no se confíe en instrucciones enviadas por correo electrónico, ya que los delincuentes piratean las cuentas y envían mensajes con instrucciones falsas que resultan ser convincentes y sofisticados. Según la NW3C (2014), se recomienda que uno siempre confirme de forma independiente las instrucciones en persona o mediante una llamada telefónica a un número de teléfono confiable.

En el caso de *U.S.A. vs. Patricia Urbanovsky* (2016), se puede observar que la forma de operar el fraude de los *vouchers* y paquetes de vacaciones era bastante similar al esquema Ponzi, ya que la acusada compraba los boletos de avión con el dinero que obtenía de los clientes nuevos. Según el FBI (FBI, s.f.a), el esquema Ponzi es un tipo de fraude en

donde las víctimas invierten dinero a cambio de supuestas ganancias mayores. El estafador paga las ganancias a los inversionistas más antiguos con el dinero de los inversionistas más recientes y cuando ya no puede conseguir clientes nuevos para pagar los dividendos adeudados el esquema simplemente colapsa. Este tipo de fraude lleva el nombre de su creador, Charles Ponzi, de Boston, Massachusetts; quien, a principios de la década de 1900, lanzó un esquema que garantizaba a los inversores un retorno del cincuenta (50%) por ciento de su inversión en cupones postales.

Según el Reporte Anual del *Internet Crime Complaints Center* (FBI, s.f.d), y como se demuestra en la Figura 1, el total de quejas reportadas desde el año 2000 suman un total de 4,063,933. A su vez, las víctimas de fraude electrónico en el año 2017 perdieron un total de \$1.42 mil millones de dólares. Como norma general, el IC3 recibe más de 800 quejas por día y la siguiente gráfica refleja cómo las reclamaciones en los últimos cinco (5) años han aumentado, aproximadamente, en 284,000 por año.

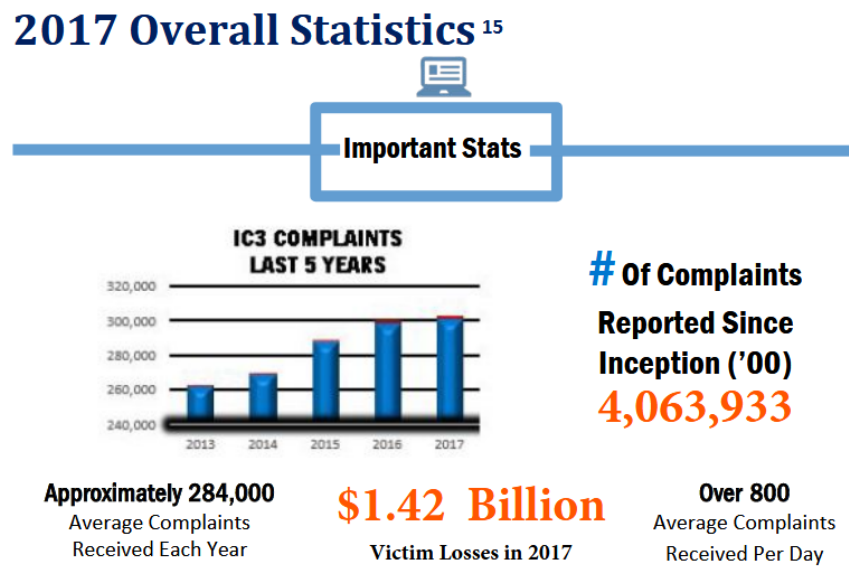


Figura 1: Estadística general de quejas del IC3 (FBI, s.f.d).

Además, según dicho Reporte Anual, se recibió un total de 301,580 reclamaciones de los cuales los fraudes con mayor incidencia fueron:

- *Business Email Compromise* (BEC), donde se reportaron 15,690 quejas con pérdidas ascendiendo a más de \$ 675 millones de dólares.
- *Ransomware*, donde se reportaron 1,783 quejas con pérdidas de más de \$ 2.3 millones de dólares.
- Fraude de soporte técnico, donde se reportaron 10,949 quejas con pérdidas reclamadas de casi \$15 millones de dólares, lo que representó un aumento del noventa (90%) por ciento comparado con el año 2016. Cabe resaltar que bajo este tipo de fraude el IC3 recibió 85 reclamaciones de diferentes países.
- Extorsión, donde se reportaron 14,938 quejas con pérdidas de más de \$ 15 millones de dólares.

Dentro de las reclamaciones recibidas por el IC3 en el año 2017, un total de 49,523 quejas fueron realizadas por víctimas mayores de sesenta (60) años de edad con pérdidas de más de \$ 342 millones de dólares. El estado con mayor número de reclamaciones y pérdidas económicas lo fue California con 14,786 reclamaciones y \$214, 217,307 de dólares en pérdida económica. Ahora bien, el fraude perpetrado por la señora Urbanovsky fue ideado y desarrollado en Omaha, Nebraska, estado que ocupa el puesto número cuarenta y uno (41) con 1,140 reclamaciones y el puesto número treinta y siete (37) con \$4,286,773 de dólares en pérdidas económicas. En las Figuras 2 y 3 se pueden observar las tablas con las estadísticas generales del Reporte Anual de IC3 de 2017, donde se muestran las reclamaciones y pérdidas económicas por cada estado que compone los Estados Unidos de América (FBI, s.f.d).

2017 Overall State Statistics

Count by Victim per State*					
Rank	State	Victims	Rank	State	Victims
1	California	41,974	30	Connecticut	2,662
2	Florida	21,887	31	Utah	2,260
3	Texas	21,852	32	Hawaii	1,923
4	New York	17,622	33	Mississippi	1,799
5	Pennsylvania	11,348	34	Kansas	1,767
6	Virginia	9,436	35	Arkansas	1,753
7	Illinois	9,381	36	Iowa	1,533
8	Ohio	8,157	37	Alaska	1,418
9	Colorado	7,909	38	New Mexico	1,415
10	New Jersey	7,657	39	Idaho	1,186
11	Washington	7,505	40	District of Columbia	1,143
12	North Carolina	7,316	41	Nebraska	1,140
13	Georgia	7,007	42	New Hampshire	1,106
14	Maryland	6,789	43	West Virginia	1,085
15	Arizona	6,417	44	Delaware	759
16	Michigan	6,400	45	Maine	740
17	Wisconsin	5,245	46	Montana	737
18	Massachusetts	5,221	47	Rhode Island	704
19	Tennessee	4,779	48	Puerto Rico	605
20	Nevada	4,675	49	Vermont	451
21	Missouri	4,187	50	Wyoming	434
22	Indiana	4,067	51	South Dakota	404
23	Alabama	3,865	52	North Dakota	355
24	South Carolina	3,687	53	Guam	66
25	Minnesota	3,619	54	U.S. Minor Outlying Islands	51
26	Oregon	3,455	55	U.S. Virgin Islands	48
27	Louisiana	3,319	56	American Samoa	17
28	Oklahoma	2,809	57	Northern Mariana Islands	13
29	Kentucky	2,740			

Figura 2: Estadística de reclamaciones por Estado del IC3 (FBI, s.f.d).

2017 Overall State Statistics *Continued*

Loss by Victim per State*					
Rank	State	Loss	Rank	State	Loss
1	California	\$214,217,307	30	Alabama	\$9,949,873
2	Texas	\$115,680,902	31	Idaho	\$7,657,726
3	Florida	\$110,620,330	32	Kentucky	\$7,220,342
4	New York	\$88,633,788	33	Mississippi	\$6,786,910
5	Arizona	\$59,366,635	34	Kansas	\$5,045,755
6	Washington	\$42,991,213	35	Arkansas	\$4,823,489
7	Illinois	\$42,894,106	36	New Mexico	\$4,716,033
8	New Jersey	\$40,441,739	37	Nebraska	\$4,286,773
9	Colorado	\$39,935,041	38	Iowa	\$4,013,395
10	Massachusetts	\$38,962,867	39	New Hampshire	\$3,725,739
11	Georgia	\$38,353,746	40	Rhode Island	\$3,390,078
12	Pennsylvania	\$36,319,408	41	Hawaii	\$3,368,323
13	Virginia	\$35,438,537	42	District of Columbia	\$2,707,684
14	Ohio	\$30,672,149	43	Montana	\$2,553,804
15	Maryland	\$30,045,488	44	South Dakota	\$2,472,062
16	Michigan	\$25,362,646	45	West Virginia	\$2,435,608
17	North Carolina	\$22,203,108	46	Delaware	\$2,376,718
18	Nevada	\$19,578,132	47	Wyoming	\$2,331,692
19	Missouri	\$19,475,647	48	North Dakota	\$2,006,821
20	Minnesota	\$19,126,165	49	Alaska	\$1,709,126
21	Wisconsin	\$15,787,242	50	Puerto Rico	\$1,590,979
22	Tennessee	\$13,561,295	51	Maine	\$1,310,506
23	Indiana	\$13,228,744	52	Vermont	\$1,291,941
24	South Carolina	\$13,048,133	53	Guam	\$819,163
25	Connecticut	\$12,465,243	54	U.S. Virgin Islands	\$625,169
26	Oklahoma	\$11,671,198	55	U.S. Minor Outlying Islands	\$61,445
27	Oregon	\$11,165,342	56	Northern Mariana Islands	\$21,320
28	Louisiana	\$10,696,284	57	American Samoa	\$2,200
29	Utah	\$10,302,892			

Figura 3: Estadística de pérdidas económicas del IC3 (FBI, s.f.d).

Leyes aplicables

Las leyes aplicables al caso 8:16CR52, *United States of America vs. Patricia Urbanovsky* (2016), son las siguientes:

Código 18 de los Estados Unidos sección 1343- Fraude por cable, radio o televisión. Cualquier persona que haya ideado o intente idear un plan o artificio para defraudar o para obtener dinero o propiedad mediante pretensiones, representaciones o promesas falsas o fraudulentas, transmita o haga que se transmitan por medio de comunicaciones por cable, radio o televisión en el comercio interestatal o extranjero, cualquier escritura, rótulo, señal, imagen o sonido con el fin de ejecutar dicho esquema o artificio será multado bajo esta disposición o será encarcelada no más de 20 años, o ambos (*18 U.S.C. § 1343: Fraud by wire, radio or television*).

Código 18 de los Estados Unidos sección 1957 - Participación en transacciones monetarias en propiedades derivadas de actividades específicas ilegales. Cualquier persona que en cualquiera de las circunstancias establecidas en la subsección (d), a sabiendas se comprometa o intente realizar una transacción monetaria en una propiedad derivada criminalmente de un valor superior a \$ 10,000 dólares y que provenga de una actividad ilegal, será castigado como indicado en la subsección (b) (*18 U.S.C. § 1957: Engaging in monetary transactions in property derived from specified unlawful activity*).

Código 18 de los Estados Unidos sección 1956 - Lavado de instrumentos monetarios. Cualquier persona que, a sabiendas que la propiedad involucrada en una transacción financiera constituye el producto de alguna forma de actividad ilícita, realiza o intenta realizar tal transacción financiera que efectivamente involucra el producto de actividades ilícitas especificadas, con intención de promover la realización de actividades

ilegales específicas, será multada en no más de \$ 500,000 dólares, o el doble del valor de la propiedad involucrada en la transacción, el que sea mayor, o será encarcelada por un término no mayor de 20 años, o ambos (*18 U.S.C. §1956(a)(1)(A)(i): Laundering of monetary instruments*).

Código 18 de los Estados Unidos sección 2- Autor del delito. Cualquier persona que cometa un daño contra el Gobierno de los Estados Unidos o ayude, incite, aconseje, ordene, induzca u obtenga su comisión, es punible como autor del delito. Cualquier persona que deliberadamente cometa un acto que, si es ejecutado directamente por él o por otro, sería una ofensa contra el Gobierno de los Estados Unidos será castigado como autor del delito (*18 U.S.C. § 2: Principals*).

Casos relacionados

United States of America vs. Eugene Robert LeClear

Según la página del *Department of Justice Northern District of West Virginia* (2018), el Sr. Eugene Robert LeClear, de 47 años de edad y de Wheeling, West Virginia, fue sentenciado el 8 de noviembre de 2018 a treinta (30) meses de cárcel por fraude electrónico. El señor LeClear se declaró culpable de un cargo de fraude electrónico en el mes de julio de 2018, al admitir haber estafado a otras personas por más de \$ 100,000 dólares durante agosto de 2016 hasta el mes de diciembre de 2017 en el condado de Ohio. Al señor LeClear se le ordenó pagar \$130,405 dólares como suma que debería restituir a las víctimas. El juez a cargo fue el Honorable John Preston Bailey.

La similitud con el caso escogido, y a discutirse, se reduce a que en ambas situaciones las partes acusadas aceptaron el acuerdo con fiscalía federal (*plea bargain*) para

declararse culpables de los cargos radicados por fraude electrónico y que a ambas se les ordenó que pagaran la correspondiente suma de restitución a sus víctimas.

United States of America vs. Victoria Scardigno

Según el documento del caso *United States of America vs. Victoria Scardigno (2010)*, la Sra. Victoria Scardigno, de 32 años y agente de ventas de la línea aérea *Continental Airlines*, es acusada de apropiarse cerca de \$1,000,000.00 imprimiendo *vouchers* falsos y vendiéndolos entre \$500.00 y hasta \$600.00 dólares por pasajero. La venta se la ofrecía a los clientes de mayor confianza, dichas ventas las realizaba desde su estación de ventas en el Aeropuerto Internacional Newark Liberty en New Jersey. La señora Scardigno vendió sobre 1,750 *vouchers* falsos y el esquema duró desde el mes de mayo de 2009 hasta el mes de diciembre de 2009.

Con el fin de ocultar su fraude, la señora Scardigno se servía de su estatus como empleada de *Continental Airlines* para comprar los boletos de algunas de sus víctimas que reclamaron dichos *vouchers* en vuelos de ida y vuelta. El dinero adquirido de este fraude fue utilizado para compras en productos Louis Vuitton y Coach, además de otros gastos personales. La señora Scardigno fue declarada culpable de los cargos presentados en su contra y fue sentenciada a cumplir 2 años y 5 meses prisión y restituir la suma de \$100,000.00.

La similitud con el caso escogido es que en ambos está involucrado el tema de las ventas de *vouchers* falsos.

United States of America vs. William Andrew Hightower

Según la página del *Department of Justice Southern District of Texas* (2018), el Sr. William Andrew Hightower, de 60 años, fue acusado de cometer trece (13) cargos de fraude electrónico, fraude postal y lavado de dinero. El señor Hightower fue presidente de Hightower Capital Group donde, fungiendo como asesor de inversiones, llevó a cabo un extenso esquema Ponzi. En dicho esquema, que duró desde el año 2013 hasta el año 2018, hizo falsas promesas al asegurarle a sus clientes que el dinero invertido estaba siendo destinado a varios proyectos, tales como: restaurantes, películas, contratos de seguros, entre otros asuntos.

Según el pliego acusatorio, el señor Hightower recibió más de \$10,000,000.00 de los inversionistas, muchos de los cuales creían que éste estaba colocando su dinero en proyectos legítimos, cuando en efecto éste utilizó los fondos para pagar a los inversionistas anteriores y pagarse a sí mismo con el fin de financiar su extravagante estilo de vida. Además, se acusó al señor Hightower de ocultar a sus clientes que, desde el mes de octubre de 2015, la Autoridad Reguladora de la Industria Financiera (FINRA, por sus siglas en inglés) le había prohibido actuar como intermediario o asociarse de alguna otra manera con una firma de corredores. Si es declarado culpable, éste puede enfrentarse a una pena de hasta veinte (20) años en prisión federal por cada cargo, así como miles de dólares en posibles multas.

La similitud con el caso escogido es que ambos versan sobre el delito de lavado de dinero mediante un esquema Ponzi.

Herramientas de investigación

En un análisis investigativo, aplicando las técnicas, metodologías y herramientas adecuadas, se puede descubrir información sobre un fraude o delito. Existen múltiples herramientas, las cuales sirven para realizar un análisis forense digital que permite encontrar rastros y descubrir datos que sirvan como prueba de la comisión del delito. Algunas de las herramientas de investigación recomendadas para el análisis del caso de la señora Urbanovsky son:

- *Bulk Extractor*, se trata de una herramienta de investigación forense que escanea una imagen del disco, archivo o un directorio de archivos, y extrae información útil sin analizar el sistema de archivos o las estructuras del sistema de archivos. Los resultados pueden ser fácilmente inspeccionados, analizados o procesados con herramientas automatizadas. Esta herramienta se distingue de otras por su velocidad y exactitud, debido a que ignora la estructura del sistema de archivos y puede procesar diferentes partes del disco en paralelo. Algunos ejemplos de la información que se puede obtener mediante el *Bulk Extractor* son: los números de tarjeta de crédito, los dominios de Internet que se encuentran en la unidad, las direcciones de correo electrónico, el histograma de los términos utilizados en búsquedas en Internet de servicios como Google, Bing, Yahoo y otros, lista de todas las "palabras" extraídas del disco, lo cual es útil para el desciframiento de contraseñas, entre muchas más (Kali Tools, 2014).
- *Forensic Tool Kit Imager* de Access Data, es una herramienta que permite una evaluación rápida de evidencia electrónica. La misma realiza réplicas y

visualizaciones previas de datos y crea copias exactas de datos sin realizar cambios en la evidencia original (Access Data, 2018).

- *Magnet AXIOM*, es una herramienta que permite que los examinadores pueden acceder y buscar los datos del sistema de archivos, ejecutar el descifrado del disco completo, aprovechar *Magnet.AI (artificial intelligence)* para el análisis de chat contextual y muchas más funciones adicionales. Se trata de una plataforma de investigación digital completa que permite a los examinadores adquirir y analizar datos forenses de forma transparente, así como compartir sus hallazgos. Además, prepara automáticamente los datos para la examinación, lo que le ahorrará tiempo al investigador. *AXIOM Examine* accede a los datos del sistema de archivos, del registro y de los artefactos para obtener un análisis integrado y en profundidad mediante enlaces activos, varias vistas, filtros, búsquedas, entre otras funciones (Magnet Forensics, 2018).
- *UFED Cloud Analyzer*, es una herramienta que permite extraer, preservar y analizar datos de mensajes instantáneos, redes sociales, almacenamiento de archivos y otros contenidos basados en la nube de fuentes públicas y privadas con aprobación legal previa. Además, se puede acceder inmediatamente a información sin tener que rastrear manualmente los datos o analizar abundante información, lo cual permite buscar, filtrar, clasificar y compartir datos con facilidad para identificar las actividades sospechosas, la ubicación, las víctimas, entre otros asuntos (Cellebrite, s.f.).
- *Belkasoft Live RAM Capturer*, es una herramienta forense que permite extraer de manera confiable todo el contenido de la memoria volátil de una computadora,

incluso si la misma está protegida por un sistema activo de *anti-debugging* y *antidumping*. Es compatible con todas las versiones y ediciones de Windows, XP, Vista, Windows 7, 8 y 10 (Belkasoft, 2018).

SECCIÓN 3: SIMULACIÓN

A continuación, el caso de la señora Urbanovsky será representado en la Figura 4. Dicho diagrama identifica paso por paso las acciones realizadas por ésta para llevar a cabo el esquema de fraude.

La señora Urbanovsky hizo falsas declaraciones y representaciones a sus empleados y clientes, asegurándole a estos que ella mantenía una relación profesional con el Sr. Christopher Frederick, un supuesto vicepresidente de la compañía *Southwest Vacations*. Para el mes de octubre de 2014, comenzaron a circular rumores de que la venta de los *vouchers* era falsa, lo cual alarmó a sus empleados y clientes. Fue entonces el 30 de octubre de 2014 que ésta se hizo pasar por el señor Frederick, creando una dirección de correo electrónico falsa identificada como christopherfrederickXXX@xxxxx.com, la cual utilizó para enviar correos electrónicos a los empleados de *Creative Creations* (CC) con el fin de motivarlos a continuar con las ventas.

Luego de efectuar una venta de *vouchers*, o paquetes de vacaciones, los clientes realizaban sus pagos por medio de *Square, Inc.*, un procesador de tarjetas de crédito con sede en California, que acto seguido realizaba el correspondiente depósito en la cuenta de banco a la cual la señora Urbanovsky era la única que tenía acceso. De dicha cuenta la señora Urbanovsky retiraba dinero para cubrir sus gastos personales. Por último, cuando los clientes viejos le hacían su reclamación de *voucher*, ésta compraba el boleto de avión con el dinero depositado de los clientes nuevos. Este ciclo continuó hasta finales del mes de marzo de 2015 cuando el esquema colapsó, ya que el dinero entrado había disminuido y no se pudo generar fondos suficientes de las nuevas ventas para mantener la ficción a flote.

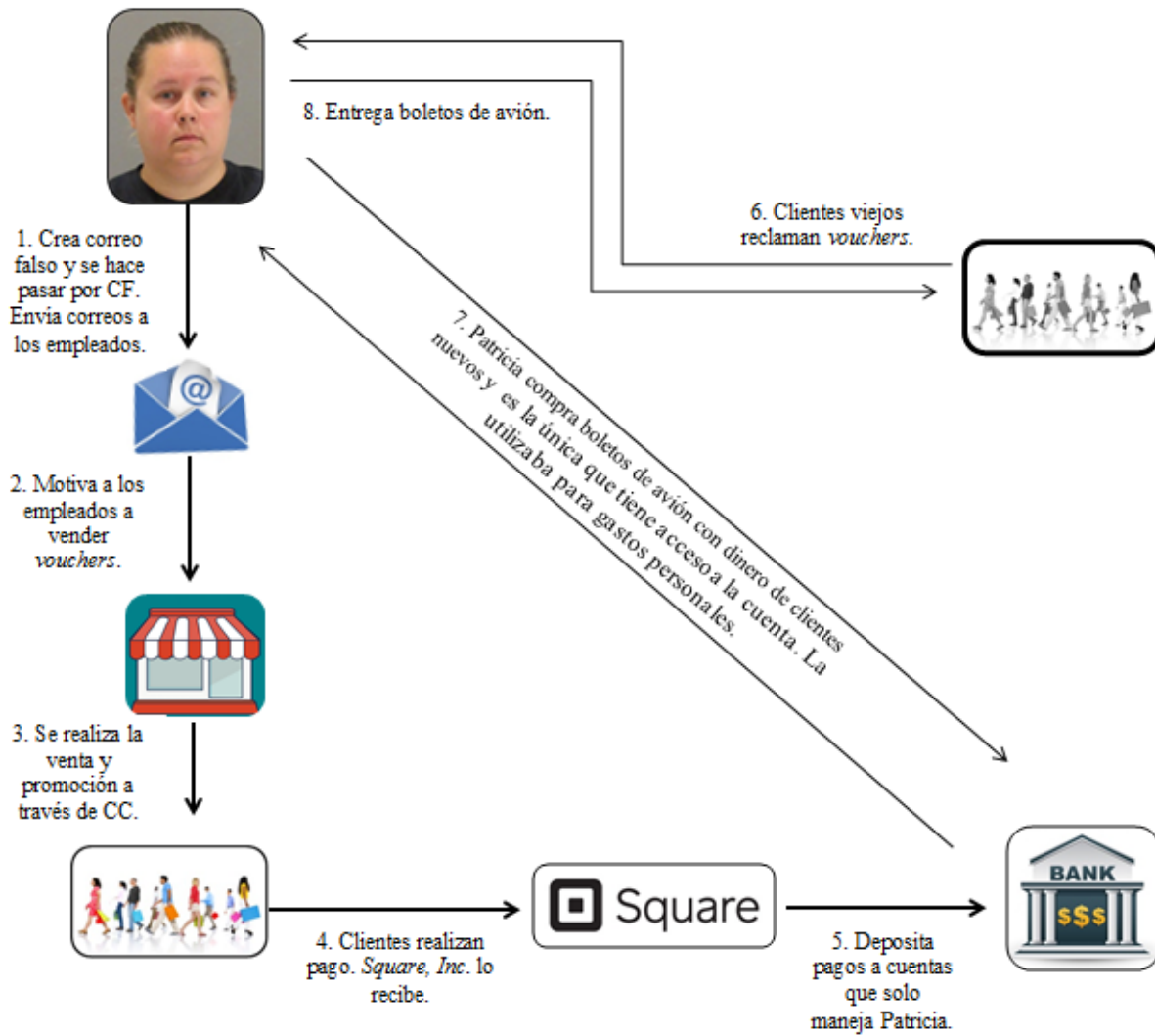


Figura 4: Esquema de fraude de la señora Urbanovsky.

SECCIÓN 4: INFORME DEL CASO

Resumen Ejecutivo

El 11 de diciembre de 2015, la Oficina de Fiscalía de los Estados Unidos de América para el Distrito de Nebraska, a través del Fiscal Donald J. Kleine, contactó a *CCDR Digital Forensics, Inc.* Dicha comunicación fue realizada con el fin de efectuar un análisis de imagen a un USB Drive de 4GB, el cual contenía una copia fiel y exacta del disco duro de la computadora personal de la señora Urbanovsky. La Investigadora asignada para el caso de fraude electrónico, lavado de dinero y realizar transacciones monetarias sobre propiedad proveniente de actividades ilícitas, fue la señorita Cathy Piñero Camacho.

Durante el análisis del USB Drive se pudo identificar facturas de clientes, documentos de promociones y varios correos electrónicos enviados por el señor Christopher Frederick. La evidencia encontrada formará parte de la prueba a presentarse en el caso *United States of America vs. Patricia M. Urbanovsky*, el cual inició el 18 febrero de 2016. Al finalizar el análisis se le entregó el dispositivo USB Drive al Fiscal, junto con copias digitalizadas de los documentos encontrados.

Objetivo

El Fiscal Kleine, en representación de la Fiscalía de los Estados Unidos de América, contrató los servicios de *CCDR Digital Forensics, Inc.*, para descubrir, recuperar y analizar la información que se encontraba en el USB Drive 0516PU, el cual contenía una copia del disco duro de la computadora incautada de la acusada. El propósito de dicha encomienda es obtener evidencia suficiente para determinar si la señora Urbanovsky tuvo relación alguna con el esquema de fraude de ventas de *vouchers*.

Alcance del trabajo

El trabajo de *CCDR Digital Forensics, Inc.*, consiste en descubrir y analizar la información almacenada en el USB Drive 0516PU, correspondiente al caso *United States of America vs. Patricia M. Urbanovsky*. La evidencia que se estudia debe cubrir el periodo del mes de mayo de 2014 hasta el mes de marzo de 2015. Se recomienda el uso de una copia del disco duro, ya que no es recomendable trabajar directamente en la computadora incautada para así mantener la integridad de la misma. Acorde a los estándares de la industria forense, se realizó el análisis encomendado utilizando la herramienta *AccessData FTK Imager 3.1.4.6*. Esto garantiza que el proceso realizado por la Investigadora Piñero Camacho sea uno que cumpla con los requisitos establecidos por el Gobierno Federal de los Estados Unidos de América.

Datos del caso

Número de caso: 2018-12-NE

Investigadora forense: Cathy Piñero Camacho

Cliente: Oficina de Fiscalía de los Estados Unidos de América para el Distrito de Nebraska

Representante de Cliente: Fiscal Donald J. Kleine

Descripción de los dispositivos utilizados

A continuación, se presenta una lista de los dispositivos utilizados durante el proceso investigativo:

- 1) Laptop marca Lenovo, modelo Lenovo Win 7PC con procesador Intel (R) Core(TM) i3-2350 CPU @ 2.30GHz y sistema Microsoft Windows XP Professional Version 2002 Service Pack 3. (Figura 5)

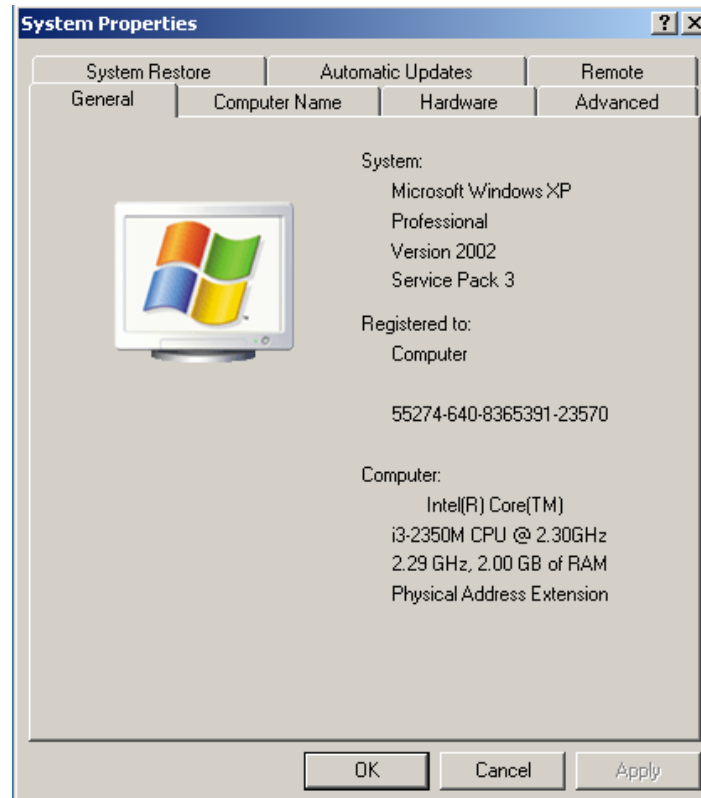


Figura 5: Sistema Microsoft Windows XP Professional 2002.

2) USB Drive de 4GB marca *PNY Attaché*, identificado como 0516PU. (Figura 6)



Figura 6: USB Drive de 4GB marca PNY Attaché.

3) La herramienta de investigación AccessData® FTK® Imager 3.1.4.6. (Figura 7)

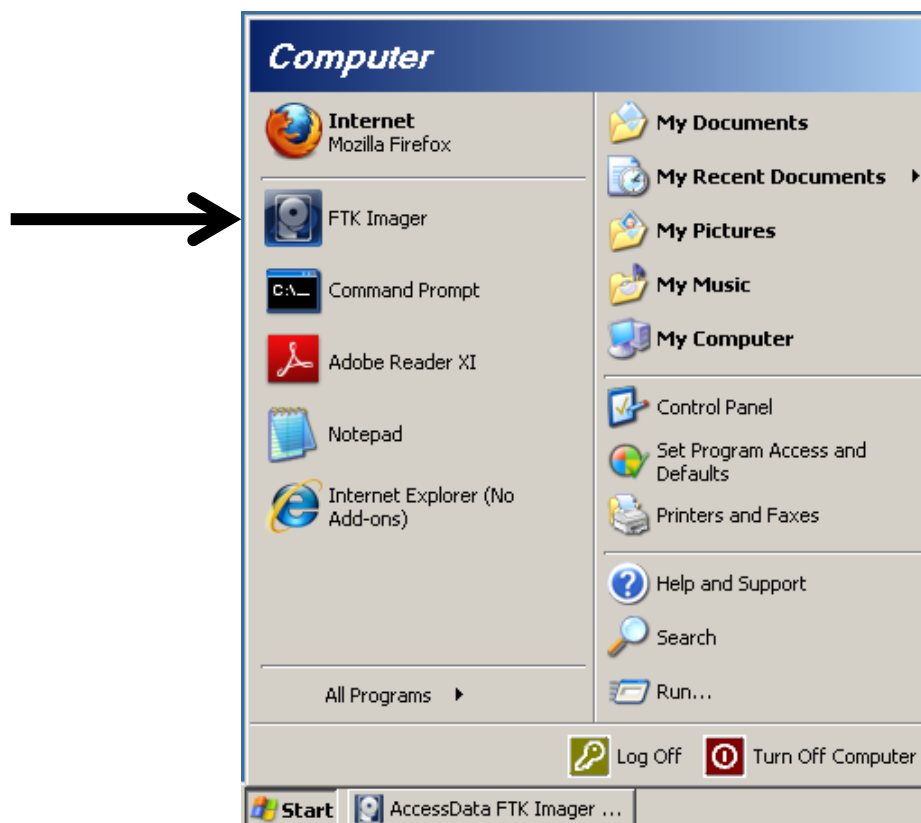


Figura 7: Herramienta AccessData FTK Imager 3.1.4.6.

Resumen de hallazgos

A continuación, se presentan los hallazgos encontrados con la herramienta *AccessData FTK Imager* durante la examinación realizada al USB Drive 0516PU, las mismas fueron:

- 1) Tres documentos con el nombre *Invoice* 000123, 000124 y 000125. Aparentemente son facturas de pagos recibidos por clientes de *Creative Creations* (Figuras 8 a la 10).

Creative Creations Omaha, Nebraska			
			INVOICE
			<u>05/15/2014</u>
			<u>000123 NO.</u>
Customer			
Name: Alfredo Smith			
Credit Card: 4549-1230-4569-7894			
Address: 2808 S 80th Ave #210, Omaha, NE 68124, USA			
Phone: 402-785-1254			
Email: Alfredosmith40@gmail.com			
DESCRIPTION	QTY	UNIT PRICE	TOTAL
4 International vouchers	4	250.00	1000.00
			0.00
			0.00
			0.00
			0.00
			0.00
			0.00
Instructions:			
To redeem the voucher for an actual airline ticket, customers must notify thirty (30) to ninety (90) days prior to the requested travel date.			
			1000.00
			TOTAL
			<hr/>
			<hr/>

Figura 8: Documento encontrado con el nombre Invoice 000123.


Creative Creations			
	Creative Creations Omaha, Nebraska	INVOICE	
		<u>05/16/2014</u>	
		<u>000124 NO.</u>	
Customer			
Name: Jorge Blanch			
Credit Card: 4549-1230-7788-1258			
Address: 8200 Dodge St, Omaha, NE 68114, USA			
Phone: 402-698-8595			
Email: jorgeblanch@gmail.com			
DESCRIPTION	QTY	UNIT PRICE	TOTAL
2 Domestic vouchers	2	139.00	278.00
			0.00
			0.00
			0.00
			0.00
			0.00
			0.00
Instructions:			
To redeem the voucher for an actual airline ticket, customers must notify thirty (30) to ninety (90) days prior to the requested travel date.			
			278.00
			TOTAL
			<hr/>
			<div style="background-color: #f4a460; width: 100px; height: 15px;"></div>

Figura 9: Documento encontrado con el nombre Invoice 000124.


 Creative Creations Omaha, Nebraska				INVOICE <u>06/23/2014</u> <u>000125 NO.</u>
Customer				
Name: Kiara Lopez				
Credit Card: 4549-2576-0102-9397				
Address: 4242 Farnam St #650, Omaha, NE 68131, USA				
Phone: 402-599-8900				
Email: kiara.lopez@gmail.com				
DESCRIPTION	QTY	UNIT PRICE	TOTAL	
5 International vouchers	5	205.00	1025.00	
			0.00	
			0.00	
			0.00	
			0.00	
			0.00	
			0.00	
Instructions: To redeem the voucher for an actual airline ticket, customers must notify thirty (30) to ninety (90) days prior to the requested travel date.			TOTAL 1025.00	

Figura 10: Documento encontrado con el nombre Invoice 000125.

- 2) Un documento con el nombre *Publication2*, el cual aparenta ser una hoja de promoción de *Creative Creations* de ventas de *vouchers* para vuelos domésticos e internacionales (Figura 11).



Creative Creations

Domestic and International
vouchers

From approximately \$78- \$250
Call now at 402-785-52681

Southwest 
Vacations

Southwest 

Creative Creations

Phone: 402-785-52681
E-mail: creativecreation@gmail.com
Facebook: Creative Creations
Instagram: Creative_creations

Figura 11: Documento encontrado con el nombre Publication2.

- 3) Cinco copias de correos electrónicos enviados desde una cuenta identificada como christopherfrederick383@XXXX.com a la siguiente cuenta rsanchezcreativecreations@XXXX.com, con fechas de: 11/03/2014; 12/01/2014; 12/18/2014; 1/2/2015 y 1/29/2015.

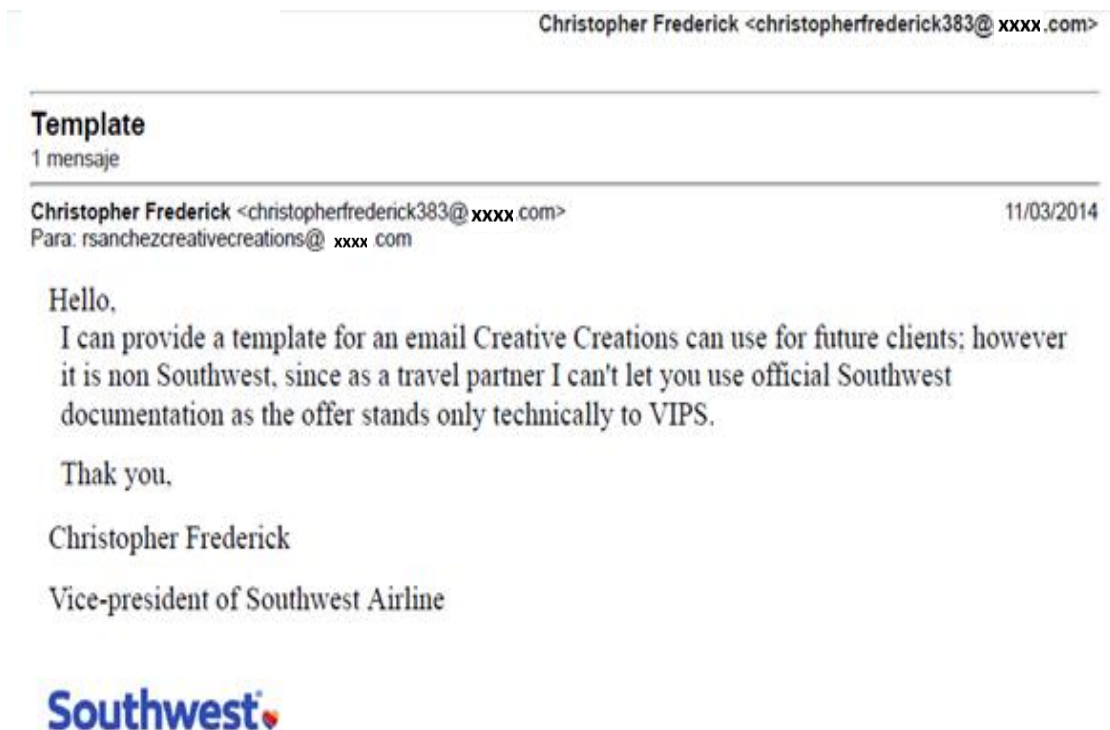


Figura 12: Correo electrónico enviado el 11/03/2014.

Christopher Frederick <christopherfrederick383@XXXX.com>

Station- declined

1 mensaje

Christopher Frederick <christopherfrederick383@XXXX.com>
 Para: rsanchezcreativecreations@XXXX.com

12/01/2014

Board has declined the approval for another station at your office, it appears that you're not quite at the volume of sales that we need to get you rolling. Thanks' for all you guys do to support Southwest Travel. You all ROCK!

Thak you,

Christopher Frederick

Vice-president of Southwest Airline

Southwest 

Figura 13: Correo electrónico enviado el 12/01/2014.

Christopher Frederick <christopherfrederick383@XXXX.com>

last sales of the year

1 mensaje

Christopher Frederick <christopherfrederick383@XXXX.com>
 Para: rsanchezcreativecreations@XXXX.com

12/18/2014

The last sales of the year are crucial to Southwest for making our end of the year quota's.

Thak you,

Christopher Frederick

Vice-president of Southwest Airline

Southwest 

Figura 14: Correo electrónico enviado el 12/18/2014.

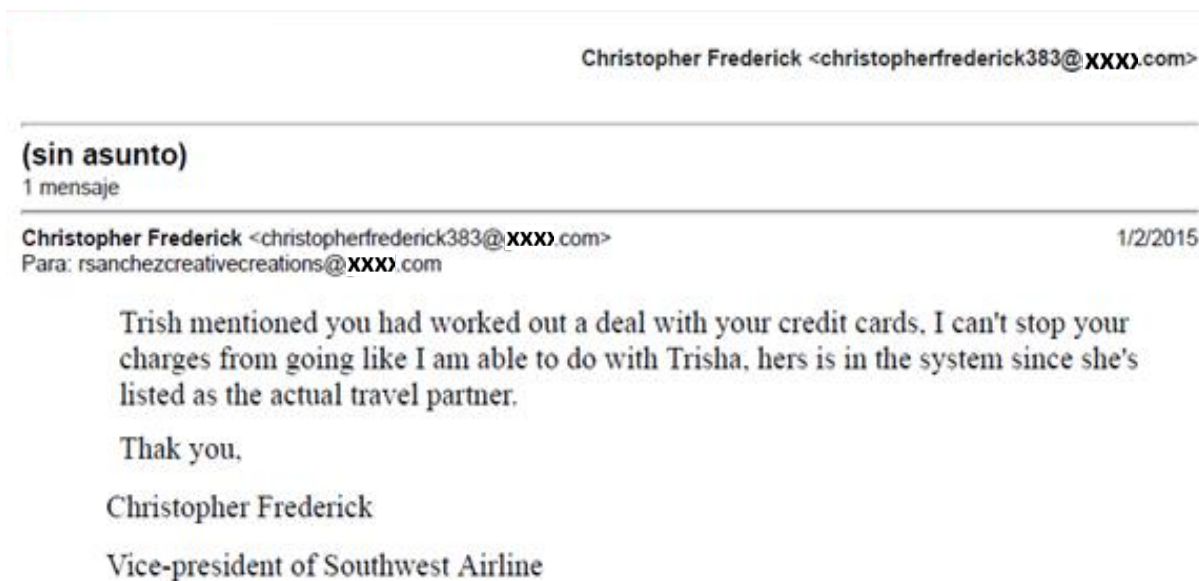


Figura 15: Correo electrónico enviado el 1/2/2015.

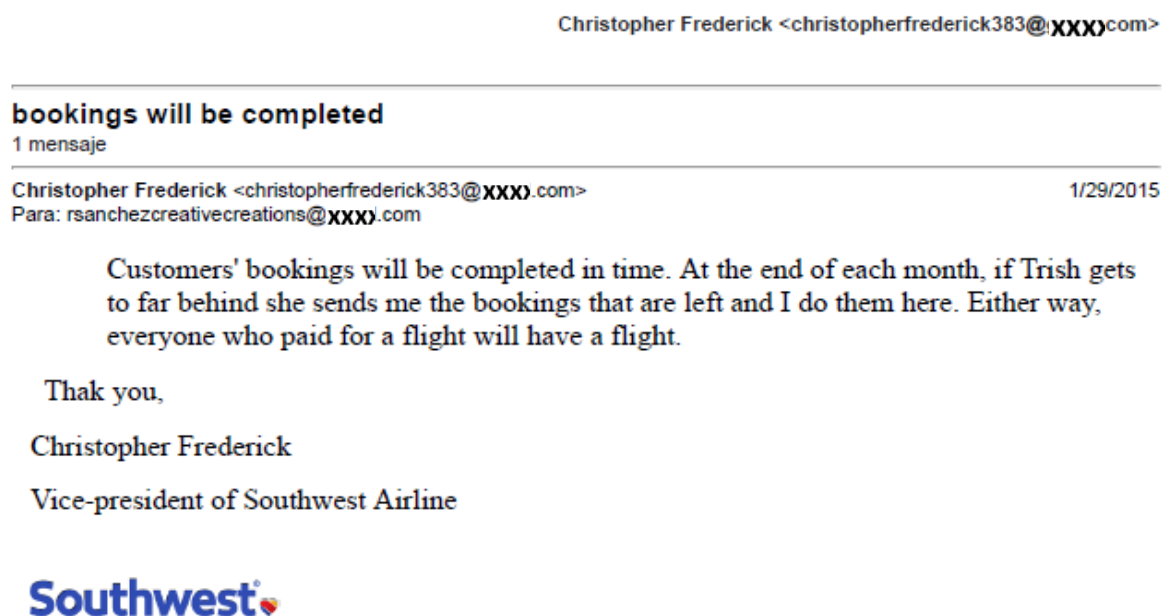


Figura 16: Correo electrónico enviado el 1/29/2015.

Cadena de custodia

Se presenta a continuación el control, procedimiento y registro que *CCDR Digital Forensics, Inc.*, utilizó para asegurar que la evidencia del hecho delictivo no sufriera ningún cambio, alteración o contaminación desde su recolección, custodia y examen. Este procedimiento debe controlar cómo, cuándo y dónde se encuentra la evidencia a examinar; por lo tanto, se deben tener en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, conservación, traslado, lugares y fechas de permanencia y los cambios que se haya realizado. Igualmente, se registrará el nombre de todas las personas que haya estado en contacto con la evidencia.

Primer evento:

1. Descripción del evento: Evidencia entregada por el Fiscal Donald J. Kleine en representación de la Oficina de Fiscalía de los Estados Unidos De América para el Distrito de Nebraska y recibida por la Investigadora Cathy Piñero Camacho en representación de *CCDR Digital Forensics, Inc.*. La evidencia consiste en un USB Drive de 4 GB marca PNY Attaché, identificado como evidencia NO. 0516PU.
2. Evento verificado por: Fiscal Donald J. Kleine e Investigadora Cathy Piñero Camacho.
3. Número de evidencia: 0516PU.
4. Fecha de comienzo: viernes, 11 de diciembre de 2015- 10:20 a.m.
5. Fecha de terminación: viernes, 11 de diciembre de 2015- 11:20 a.m.
6. Lugar de origen: Oficina de Fiscalía de los Estados Unidos De América, Distrito de Nebraska.
7. Destino: Laboratorio de *CCDR Digital Forensics, Inc.*, San Juan.

Segundo evento:

1. Descripción del evento: Creación de número de caso y designación del mismo.
2. Evento tramitado por: Investigadora Cathy Piñero Camacho.
3. Número de caso: 2018-12-NE asignado a la evidencia: 0516PU.
4. Fecha de comienzo: viernes, 11 de diciembre de 2015- 11:35 a.m.
5. Fecha de terminación: viernes, 11 de diciembre de 2015- 11:50 a.m.
6. Lugar de origen: Laboratorio de *CCDR Digital Forensics, Inc.*, San Juan.
7. Destino: Laboratorio de *CCDR Digital Forensics, Inc.*, San Juan.

Tercer evento:

1. Descripción del evento: Generación de dos imágenes del USB Drive de 4GB identificadas como Patricia Urbanovsky.001 y Patricia Urbanovsky.002, las cuales contienen una copia fiel y exacta del disco duro de la computadora personal de la acusada. Una imagen será preservada y otra para trabajar la abstracción de datos.
2. Realizado por: Investigadora Cathy Piñero Camacho.
3. Número de caso: 2018-12-NE asignado a la evidencia: 0516PU.
4. Fecha de comienzo: viernes, 11 de diciembre de 2015- 1:00 p.m.
5. Fecha de terminación: viernes, 11 de diciembre de 2015- 4:16 p.m.
6. Lugar de origen: Laboratorio de *CCDR Digital Forensics, Inc.*, San Juan.
7. Destino: Laboratorio de *CCDR Digital Forensics, Inc.*, San Juan.

Cuarto evento:

1. Descripción del evento: Guardar en la bóveda de evidencia las dos imágenes generadas identificadas como Patricia Urbanovsky.001 y Patricia Urbanovsky.002 y el USB Drive de 4GB identificado con el número de evidencia 0516PU.
2. Realizado por: Investigadora Cathy Piñero Camacho.

3. Número de caso: 2018-12-NE asignado a la evidencia: 0516PU.
4. Fecha de comienzo: viernes, 11 de diciembre de 2015- 4:25 p.m.
5. Fecha de terminación: viernes, 11 de diciembre de 2015- 4:40 p.m.
6. Lugar de origen: Laboratorio de *CCDR Digital Forensics, Inc.*, San Juan.
7. Destino: Bóveda de evidencia de *CCDR Digital Forensics, Inc.*, San Juan.

Quinto evento:

1. Descripción del evento: Buscar en la bóveda de evidencia la imagen identificada como Patricia Urbanovsky.001 generada del USB Drive de 4GB identificado con el número de evidencia 0516PU.
2. Realizado por: Investigadora Cathy Piñero Camacho.
3. Número de caso: 2018-12-NE asignado a la evidencia: 0516PU.
4. Fecha de comienzo: lunes, 14 de diciembre de 2015- 8:15 a.m.
5. Fecha de terminación: lunes, 14 de diciembre de 2015- 8:30 a.m.
6. Lugar de origen: Bóveda de evidencia de *CCDR Digital Forensics, Inc.*, San Juan.
7. Destino: Laboratorio de *CCDR Digital Forensics, Inc.*, San Juan.

Sexto evento:

1. Descripción del evento: Análisis de la imagen identificada como Patricia Urbanovsky.001. Para esto se utilizó la herramienta Access Data FTK Imager.
2. Realizado por: Investigadora Cathy Piñero Camacho.
3. Número de caso: 2018-12-NE asignado a la evidencia: 0516PU.
4. Fecha de comienzo: lunes, 14 de diciembre de 2015- 8:45 a.m.
5. Fecha de terminación: lunes, 14 de diciembre de 2015- 3:30 p.m.
6. Lugar de origen: Laboratorio de *CCDR Digital Forensics, Inc.*, San Juan.
7. Destino: Laboratorio de *CCDR Digital Forensics, Inc.*, San Juan.

Séptimo evento:

1. Descripción del evento: Devolución de la evidencia al Fiscal Donald J. Kleine. La evidencia consiste en un USB Drive de 4 GB marca PNY Attaché, identificado como evidencia NO. 0516PU.
2. Evento verificado por: Investigadora Cathy Piñero Camacho y Fiscal Donald J. Kleine.
3. Número de caso: 2018-12-NE asignado a la evidencia: 0516PU.
4. Fecha de comienzo: lunes, 14 de diciembre de 2015- 4:30 p.m.
5. Fecha de terminación: lunes, 14 de diciembre de 2015- 5:30 p.m.
6. Lugar de origen: Laboratorio de *CCDR Digital Forensics, Inc.*, San Juan.
7. Destino: Oficina de Fiscalía de los Estados Unidos De América, Distrito de Nebraska.

Procedimiento

A continuación, se detallan las operaciones realizadas durante la adquisición, recuperación, análisis y conservación de la evidencia 0516PU del caso 2018-12-NE.

Procedimiento 1: Creación de número de caso e información del dispositivo de evidencia.

- a) Herramienta: AccessData FTK Imager 3.1.4.6.
- b) Fecha de comienzo: viernes, 11 de diciembre de 2015- 11:35 a.m.
- c) Fecha de terminación: viernes, 11 de diciembre de 2015- 11:50 a.m.
- d) Descripción: Antes de crear la imagen se introduce la información del caso y evidencia, para poder identificarla. Número de Caso: 2018-12NE, Número de evidencia: 0516UP, Descripción: Urbanovsky y Examinador: Investigadora Cathy Piñero Camacho.



Figura 17: Pantalla principal del dispositivo utilizado para el análisis.

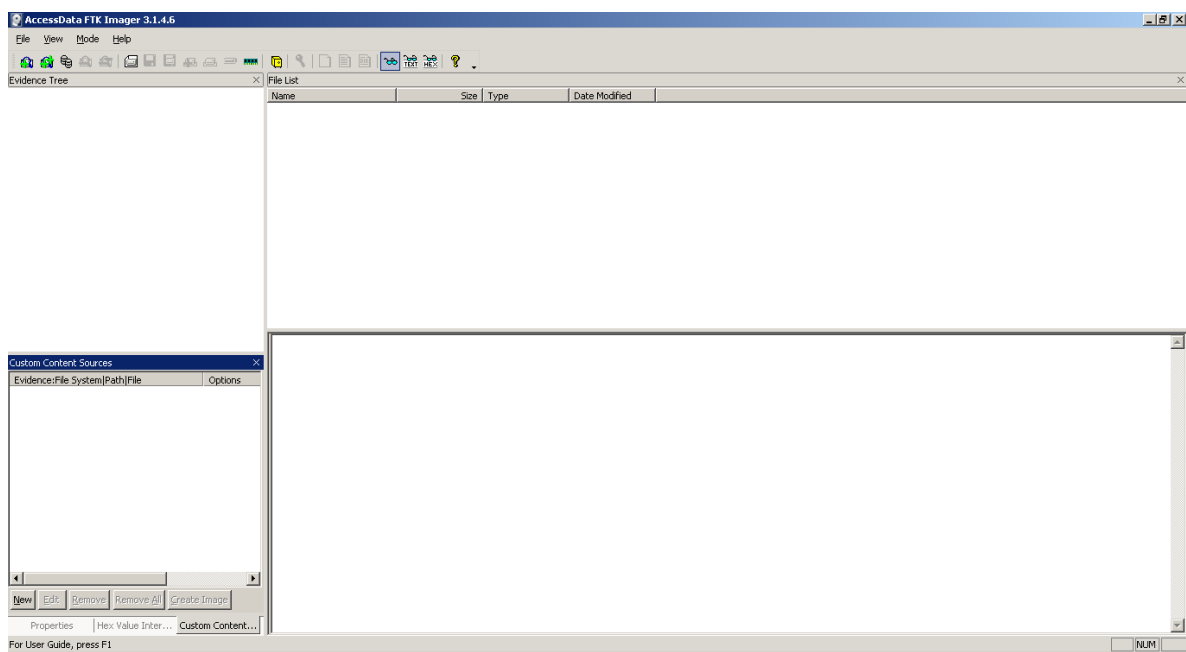


Figura 18: Pantalla inicial de AccessData FTK Imager 3.1.4.6.

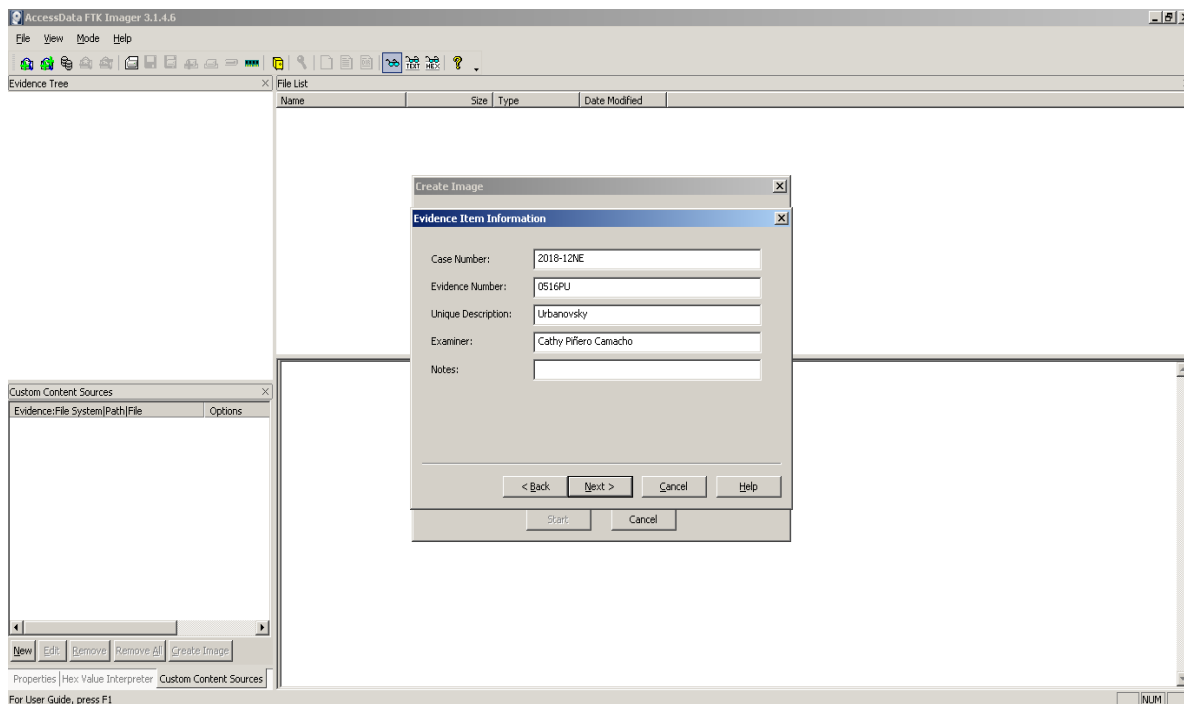


Figura 19: Información del caso y evidencia.

Procedimiento 2: Generación de imágenes.

- a) Herramienta: AccessData FTK Imager 3.1.4.6.
- b) Fecha de comienzo: viernes, 11 de diciembre de 2015- 1:00 p.m.
- c) Fecha de terminación: viernes, 11 de diciembre de 2015- 4:16 p.m.
- d) Descripción: Proceso de captura de imagen. Además, se muestra la validación de los *Hash MD5* y *Hash SHA1*, en donde existe coincidencia y no se encontraron sectores incorrectos. Esto nos permite comprobar que cada imagen es íntegra y que no fueron manipuladas.

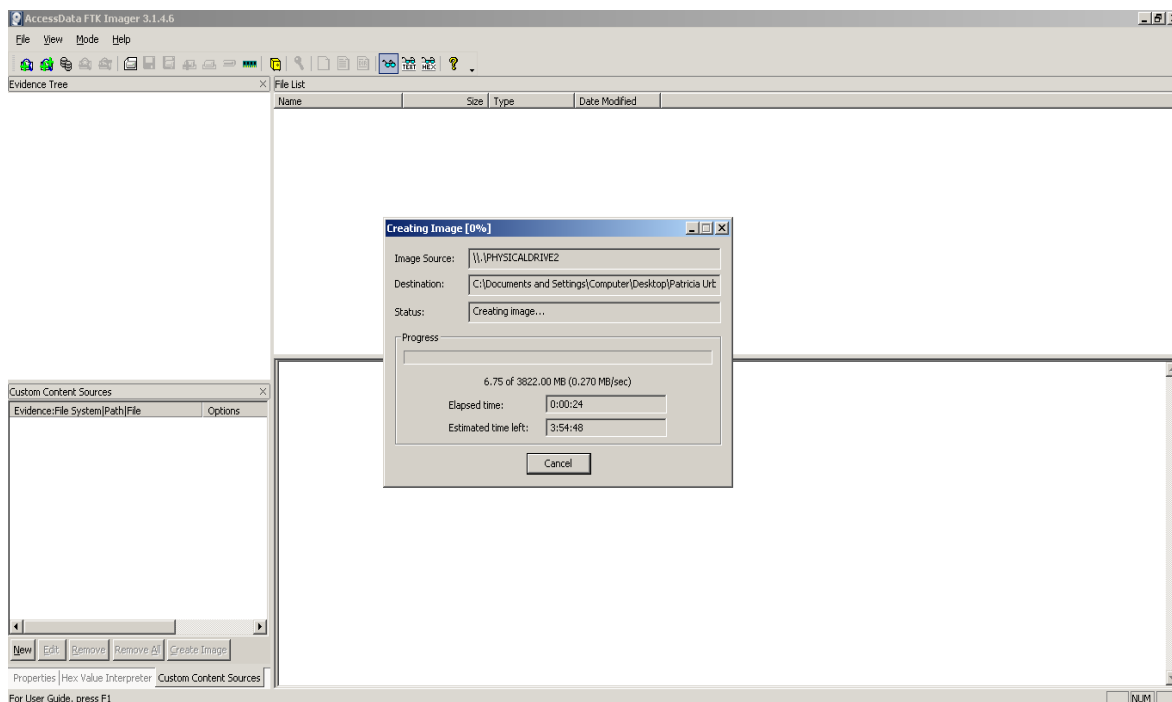


Figura 20: Inicio de creación de imagen.

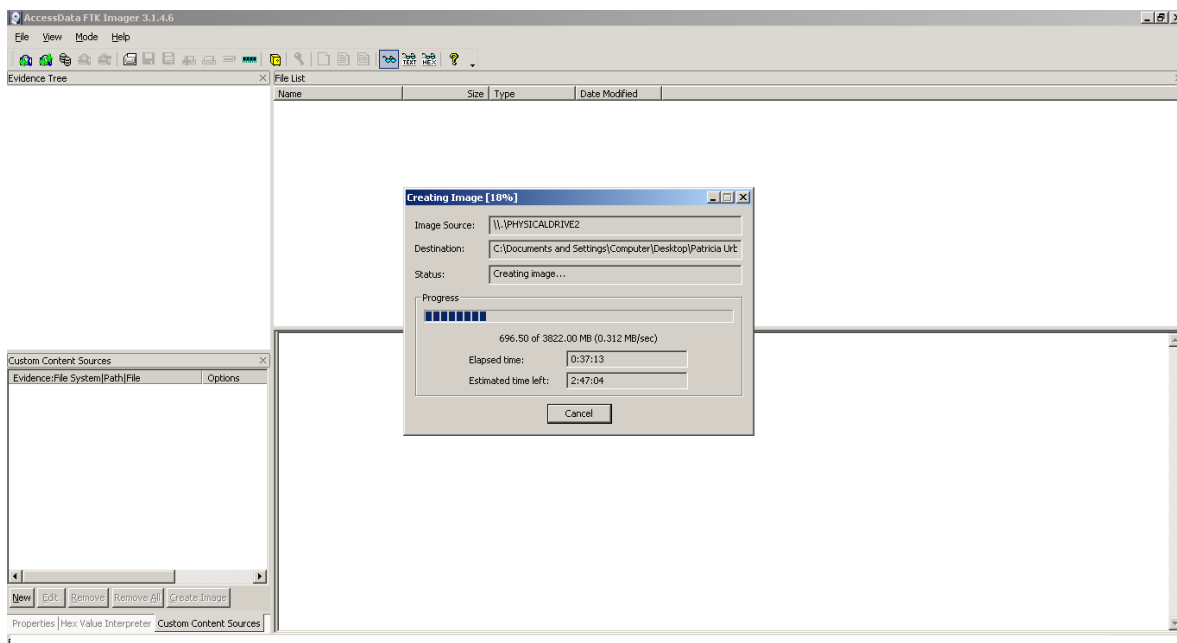


Figura 21: Proceso de creación de imagen.

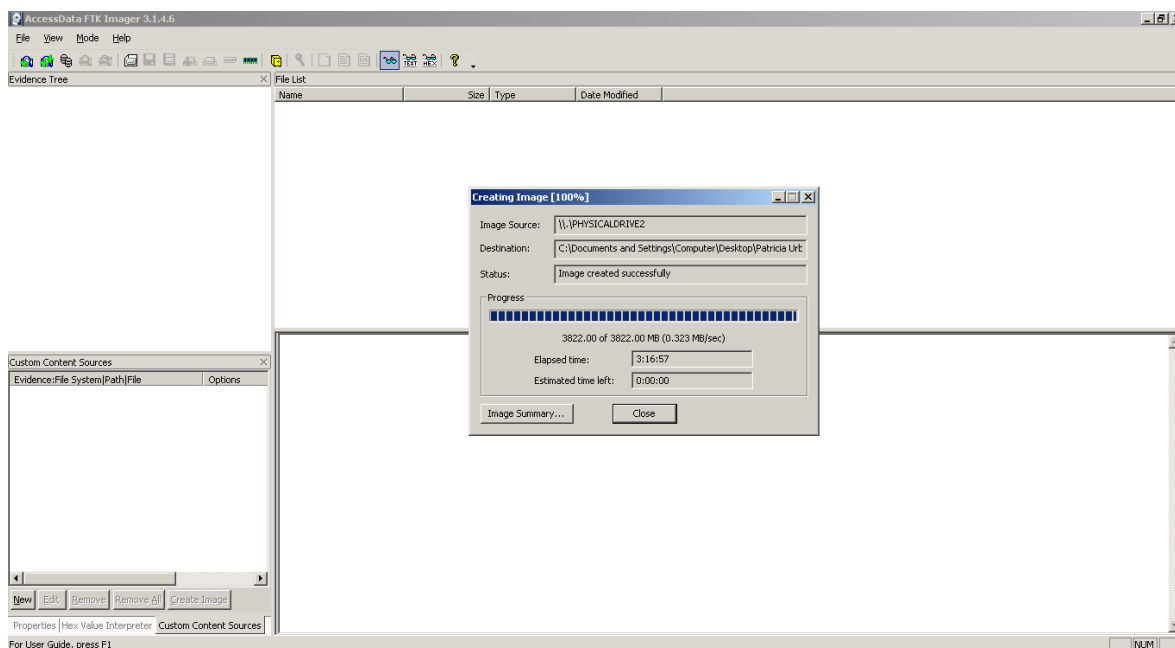


Figura 22: Confirmación completada de creación de imagen.

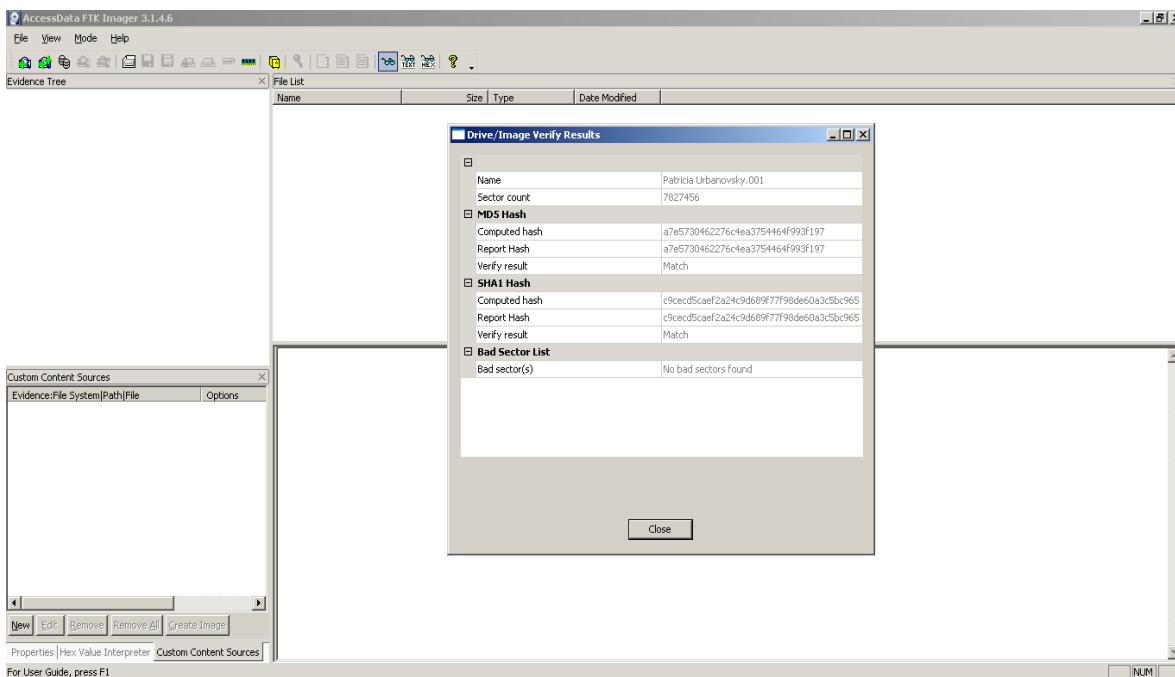


Figura 23: Validación de Hash MD5 y Hash SHA1.

Procedimiento 3: Análisis de imagen.

- a) Herramienta: AccessData FTK Imager 3.1.4.6.
- b) Fecha de comienzo: lunes, 14 de diciembre de 2015- 8:45 a.m.
- c) Fecha de terminación: lunes, 14 de diciembre de 2015- 3:30 p.m.
- d) Descripción: Análisis de la imagen identificada como Patricia Urbanovsky.001, con el fin de buscar archivos existentes o borrados del dispositivo USB Drive de 4 GB marca PNY Attaché, identificado como evidencia NO. 0516PU. A continuación de la *Figura 24* a la *Figura 33* se muestran los documentos encontrados.

Finalmente, se exponen las facturas encontradas en la carpeta *Invoice*, la cual se encontraba dentro de *Documents*. (Figuras 24 a la 27)

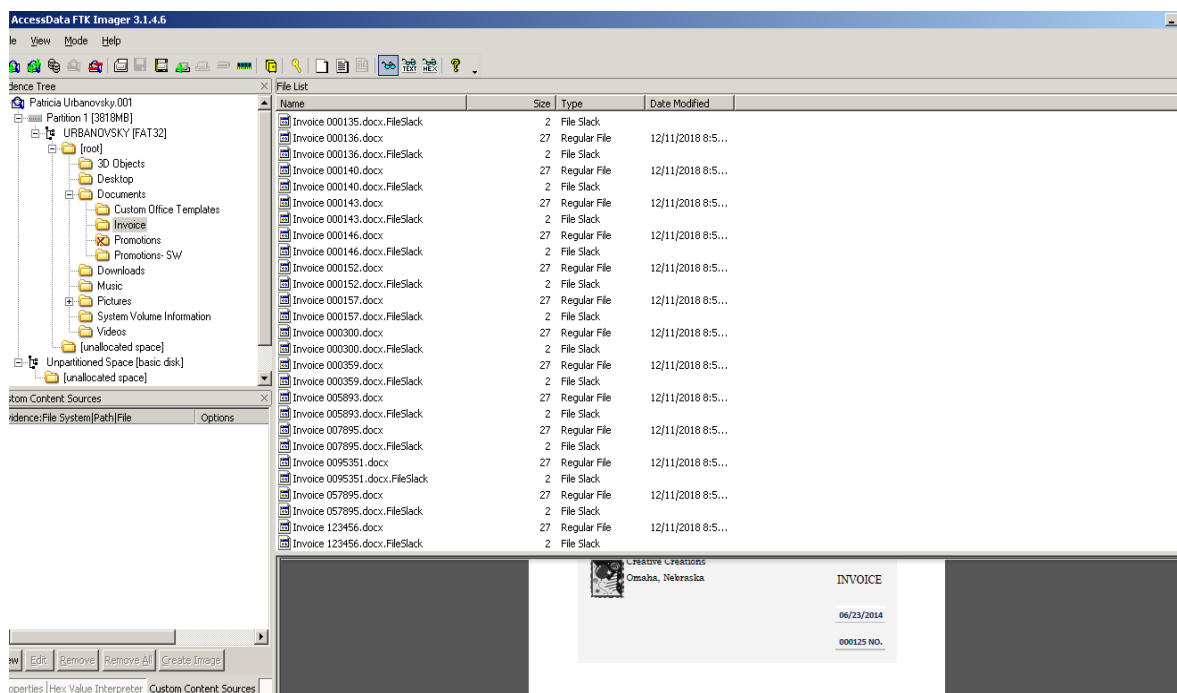


Figura 24: Documentos encontradas en el archivo *Invoice*

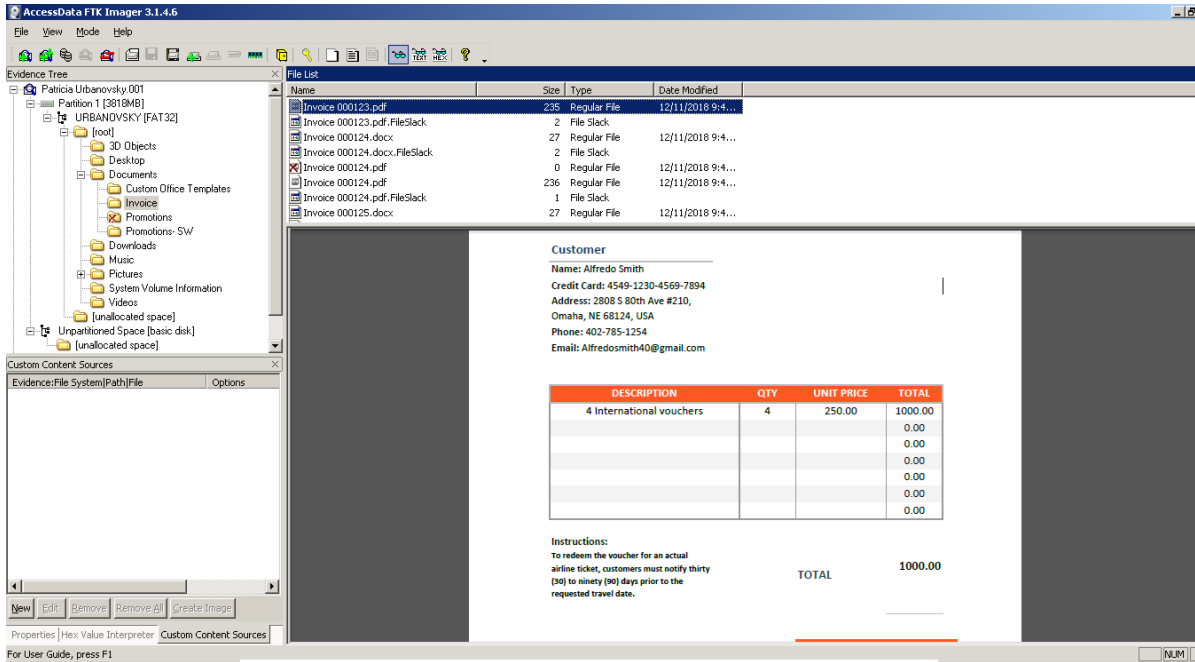


Figura 25: Primer documento - Invoice 000123

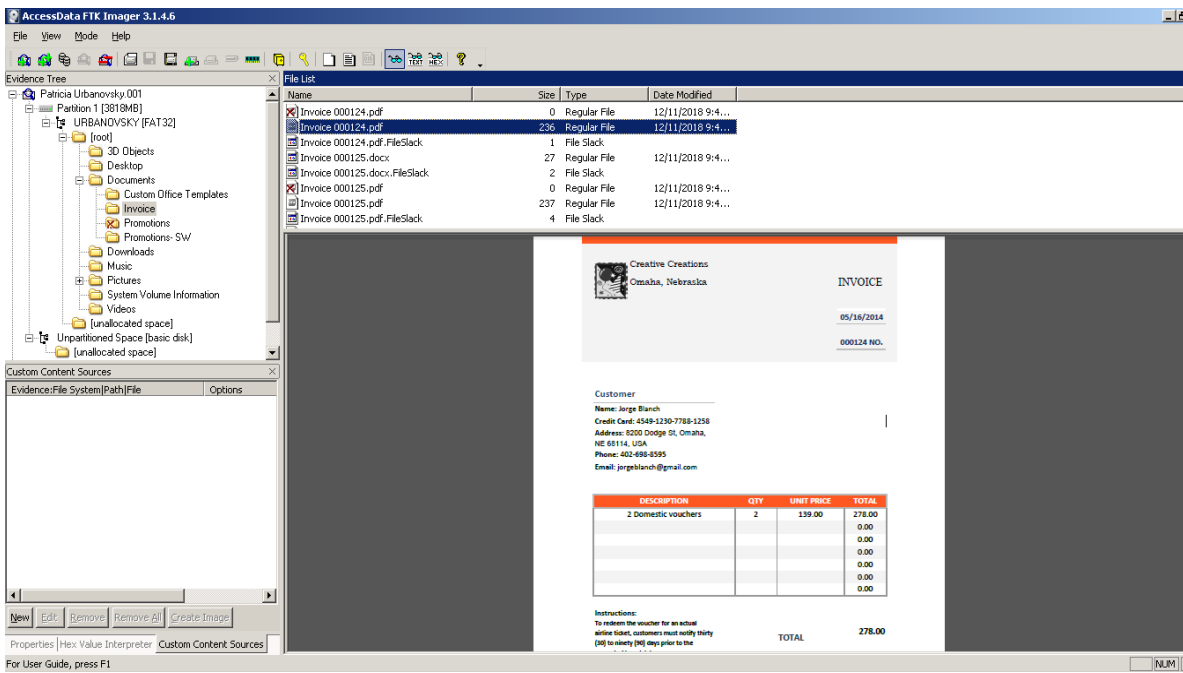


Figura 26: Segundo documento- Invoice 000124

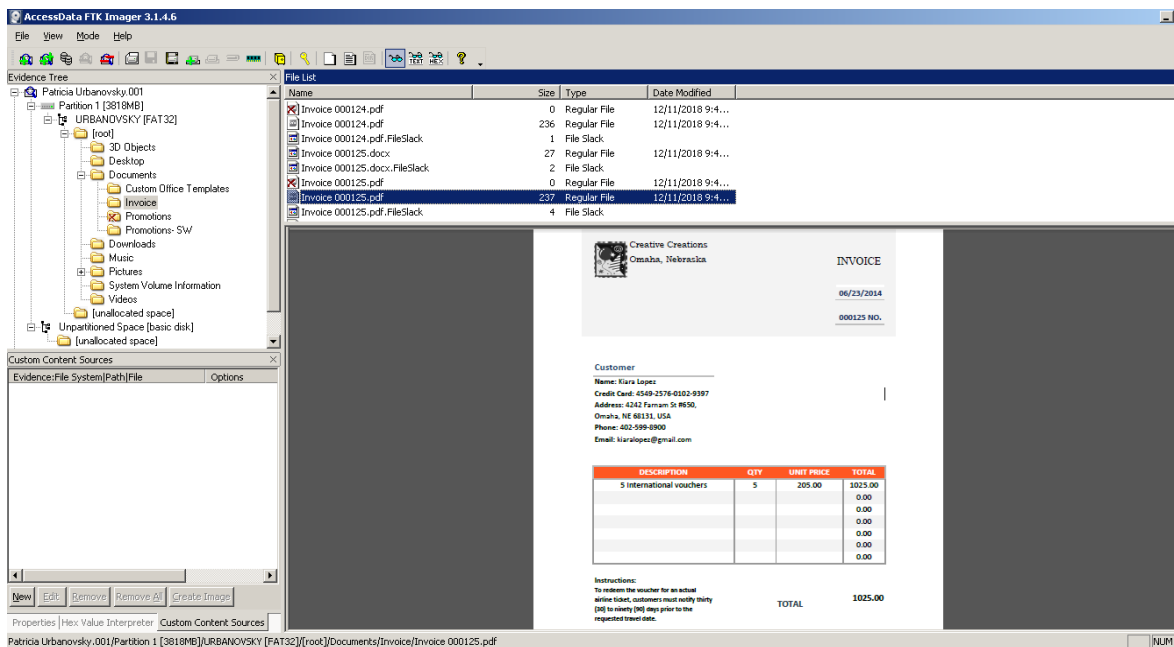


Figura 27: Tercer documento - Invoice 000125

A continuación, se muestra el documento encontrado en la carpeta de *Promotions-SW*:

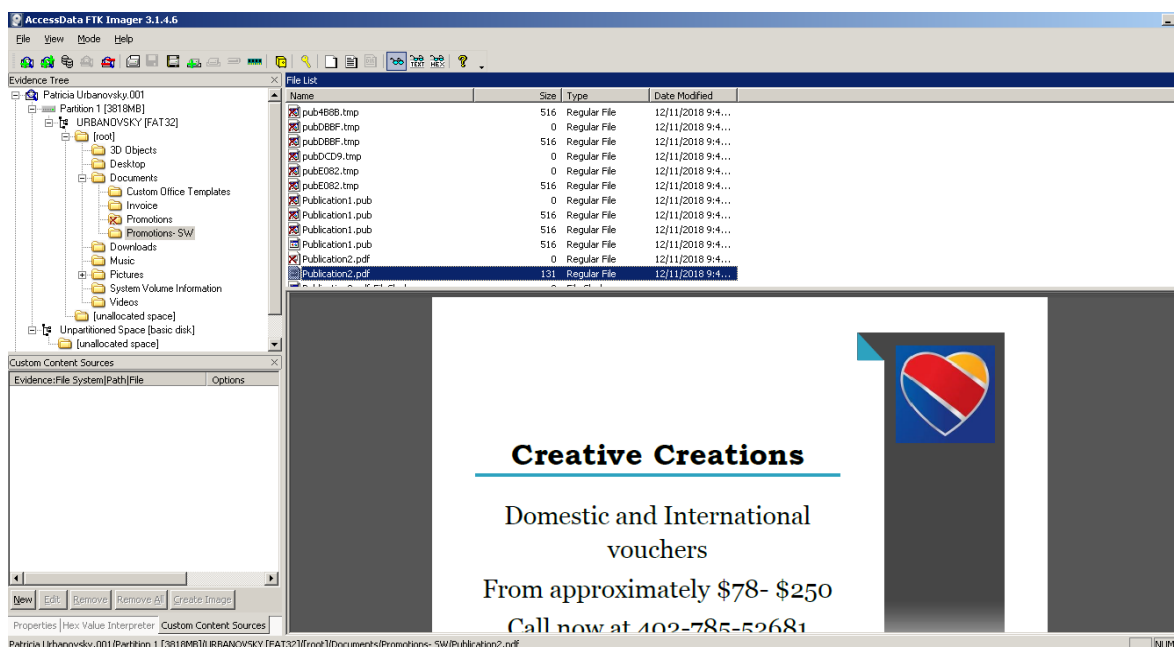


Figura 28: Cuarto documento – Publication2

De la Figura 29 a la 33 se muestran los correos electrónicos encontrados en la carpeta *Documents*:

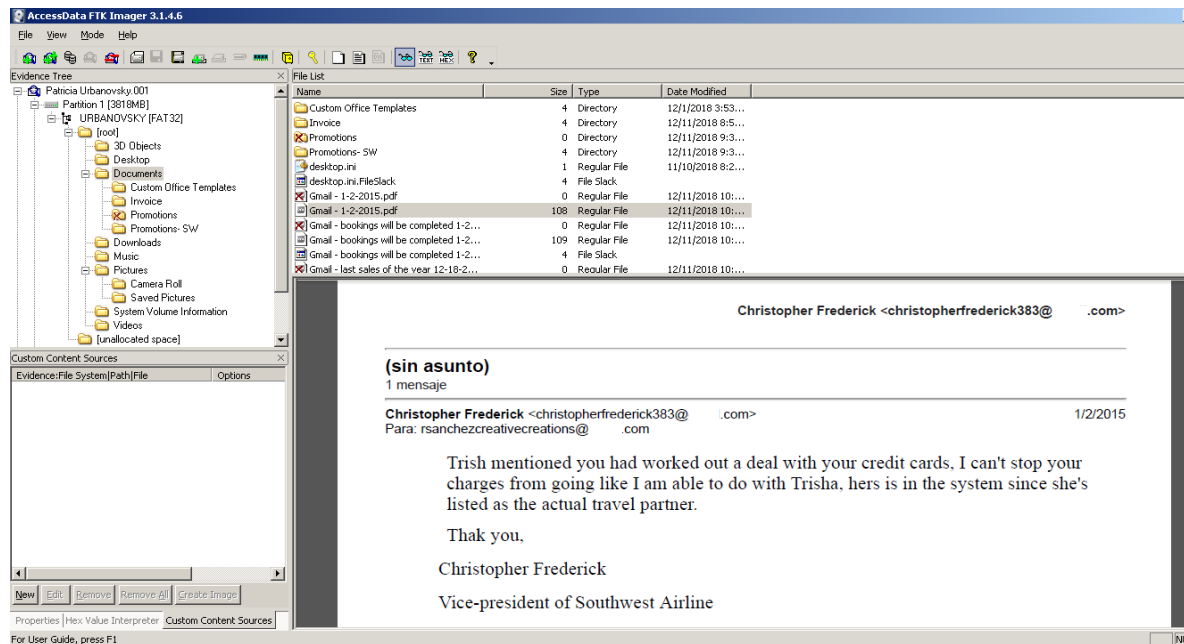


Figura 29: Quinto documento - 1-2-2015

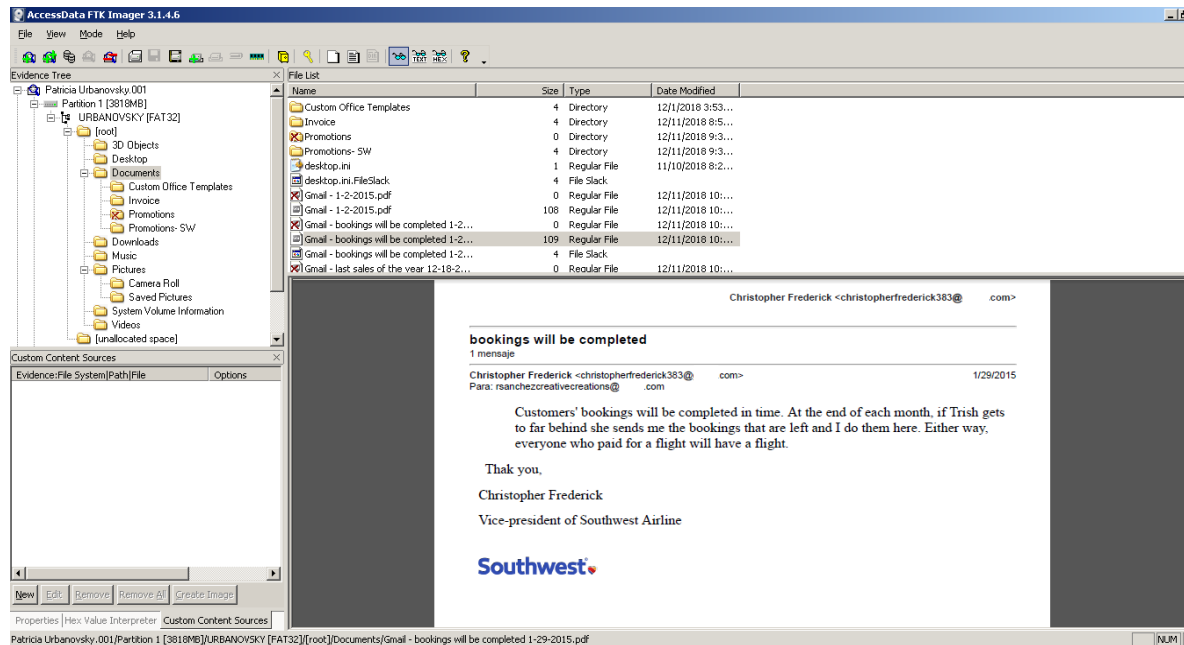


Figura 30: Sexto documento - Bookings will be completed 1-29-2015

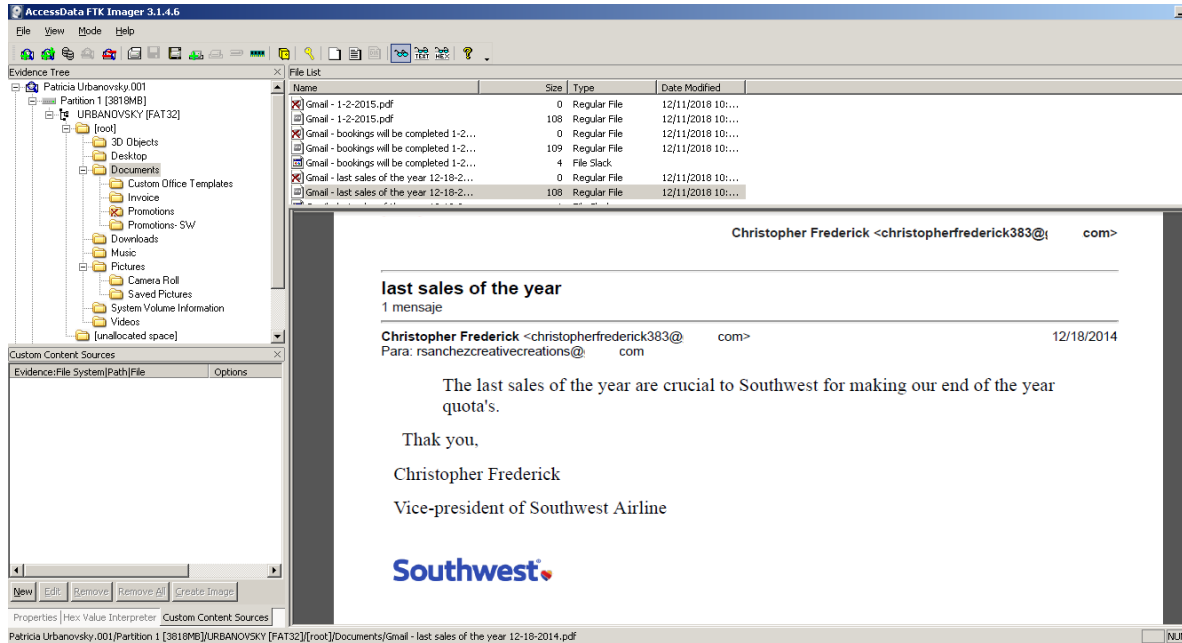


Figura 31: Séptimo documento - Last sales of the year 12-18-2014

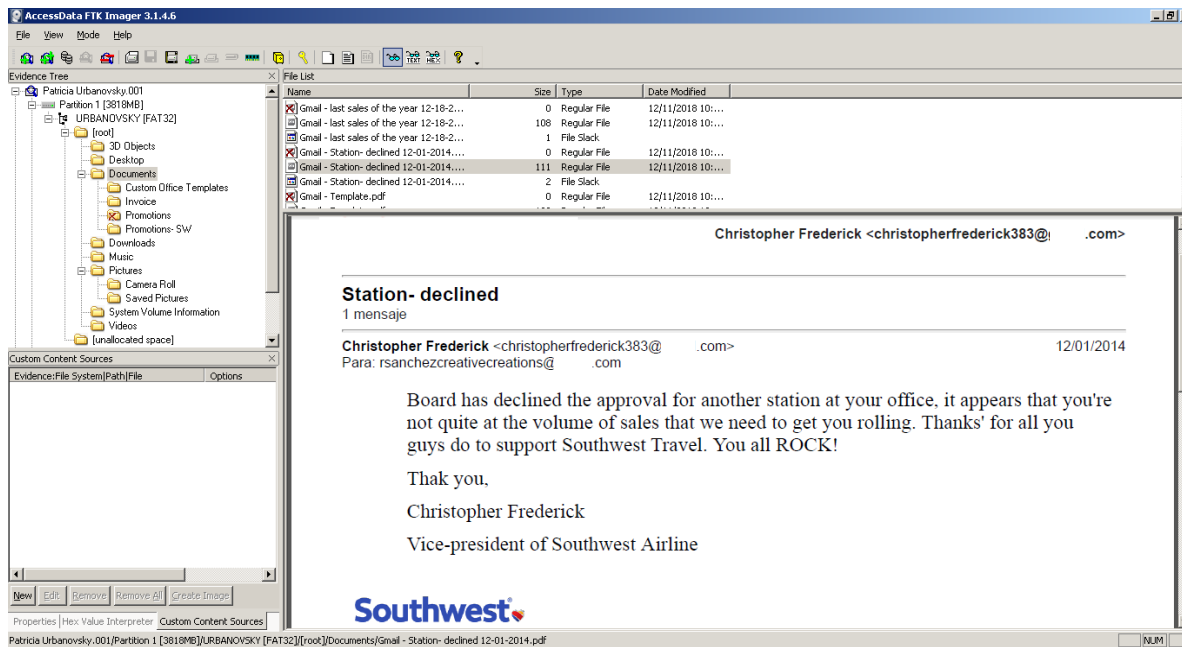


Figura 32: Octavo documento - Station- declined 12-01-2014

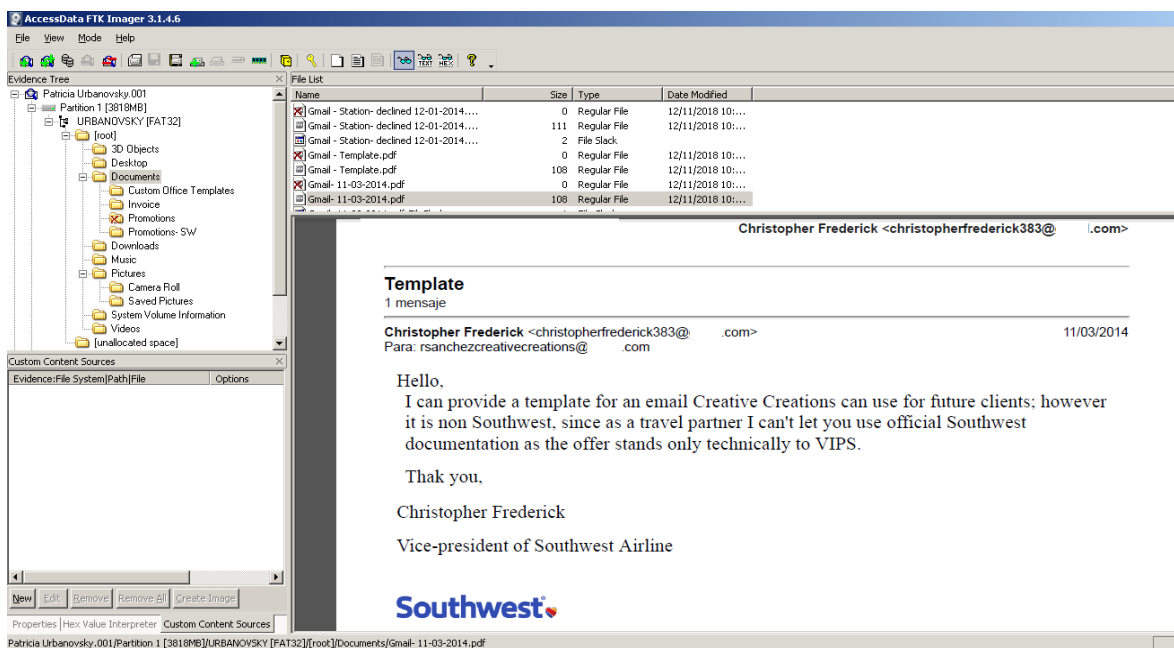


Figura 33: Noveno documento - 11-03-2014

Conclusión

Los resultados, luego de analizar e identificar los documentos encontrados en el dispositivo USB Drive de 4GB identificado como 0516PU, pueden indicar que la señora Urbanovsky realizó facturas a diferentes clientes de unas supuestas ventas de *vouchers* y promociones asociadas con la línea aérea *Southwest*. De igual forma, se observan correos electrónicos enviados de una cuenta creada a nombre del señor Christopher Frederick, supuesto vice-presidente de *Southwest*. La evidencia presentada en este informe corrobora la creación de documentos con información relacionada al esquema de fraude del cual está siendo acusada la señora Patricia Urbanovsky. No obstante, existen detalles que deben ser corroborados por las autoridades investigadoras que trabajan en este caso.

SECCIÓN 5: DISCUSIÓN DEL CASO

Según la información obtenida del documento del caso *United States of America vs. Patricia M. Urbanovsky* (2016), con el número de caso 8:16CR52 entregado por el Fiscal Auxiliar de los Estados Unidos de América del Distrito de Nebraska, Lcdo. Donald J. Kleine, a la acusada se le imputan un total de veintiséis (26) cargos, dieciséis (16) cargos por *wire fraud*, cinco (5) por participar en transacciones monetarias en propiedades derivadas de actividades ilegales, cuatro (4) por lavado de dinero y uno (1) por autora de los delitos.

Se acusa a la señora Urbanovsky de cometer estos delitos en su capacidad de presidenta y única accionista de *Creative Creations*, un negocio dedicado a la planificación de eventos y bodas ubicado en Omaha, Nebraska, desde donde elaboró un esquema de fraude contra sus clientes y empleados, el cual consistía en la representación y promesas falsas, comercializando y promoviendo la venta de paquetes vacacionales y *vouchers* supuestamente asociados con *Southwest Airlines* y *Southwest Vacations*.

Patricia Urbanovsky representaba falsamente a sus empleados y clientes que mantenía una relación profesional con un supuesto vicepresidente de *Southwest Vacations* y que a través de éste recibía un descuento en los boletos de la línea aérea. Como parte del esquema creó promociones, las cuales publicaba en internet. Además, enviaba correos electrónicos a sus empleados desde una cuenta falsa haciéndose pasar por Christopher Frederick y realizaba facturas con el nombre, correo electrónico, dirección, número de teléfono e información de tarjeta de crédito de los clientes. Con esta información se procesaban los pagos por medios de la aplicación móvil llamada *Square, Inc.* El tiempo de duración de este esquema de fraude fue aproximadamente diez (10) meses y resultó en una pérdida económica de más de \$4,600,000.00 para *Square, Inc.*

Luego de llevar a cabo el análisis y examinación del dispositivo USB Drive de 4GB identificado como evidencia número 0516PU, se encontraron en las carpetas de *Invoice*, *Promotion*, *Promotion- SW* y *Documents* documentos como facturas, detalles de clientes que compraron *vouchers* o paquetes de vacaciones, documentos de promociones de *vouchers* y correos electrónicos enviados a sus empleados desde una cuenta a nombre de Christopher Frederick. Con esta información se puede evidenciar que la señora Patricia Urbanovsky tenía en su poder el control y manejo de las ventas de *vouchers* supuestamente asociadas con la línea aérea *Southwest*. Estas muestras de evidencias presentadas detalladamente en este informe ayudaran a las autoridades a probar su caso en contra de la señora Urbanovsky.

SECCIÓN 6: AUDITORÍA Y PREVENCIÓN

Toda empresa es vulnerable al fraude electrónico. Por tal motivo se debe invertir en buenos controles que sean preventivos, detectores y correctivos, ya que permiten disminuir o mitigar dichos riesgos y amenazas. Para cumplir con estos controles se utiliza la auditoría la cual examina, analiza, previene, facilita, provee y asegura un mejor rendimiento a la organización. Luego de analizar y examinar el caso *United States of America vs. Patricia M. Urbanovsky*, se detectaron algunas fallas.

A continuación, presentaremos las fallas encontradas en la organización de *Creative Creations* y algunas sugerencias de prevención para los clientes y *Square, Inc.*, con el fin de disminuir este tipo de fraude.

Hallazgo #1: Administración de *Creative Creations*- segregación de funciones, abuso de poder y ninguna supervisión.

Situación: La señora Urbanovsky era la presidenta, única accionista y quien operaba todas las cuentas y realizaba la toma de decisiones de *Creative Creations*.

Efecto: Al no existir una segregación de funciones, ni supervisión a las acciones tomadas, la señora Urbanovsky pudo realizar los fraudes sin ningún impedimento y sin que hubiese a quien reportar dichos actos delictivos.

Causa: Falta de controles internos, segregación de funciones y ninguna supervisión.

Recomendación: Se sugiere que no se le asigne a un solo empleado tareas que confligen entre sí; además, las tareas de todos los empleados, independientemente de su puesto, deberían ser revisadas. Esto ayudaría a detectar irregularidades, errores y fraude.

Hallazgo #2: Clientes al momento de realizar una compra.

Situación: Los clientes de *Creative Creations* fueron engañados con las ventas fraudulentas de *vouchers* y paquetes de vacaciones.

Efecto: Más de 36,000 *vouchers* fueron comprados en un periodo de diez (10) meses y pérdida económica.

Causa: Falta de indagación y consulta con la línea aérea.

Recomendación: Verificar la autenticidad de las ofertas, consultar directamente con la línea aérea para cotejar que dicha oferta o afiliación fuera verdadera. Consultar y comparar precios antes de realizar una compra. Indagar a qué se dedica originalmente el negocio, buscar reseñas, opiniones y referencias del lugar donde desea comprar. Si es demasiado bueno para ser cierto, probablemente no lo sea.

Hallazgo #3: Procesador de pago *Square, Inc.*

Situación: *Square, Inc.* fue el procesador de tarjeta de crédito utilizado por la señora Urbanovsky.

Efecto: Pérdida económica que sobrepasa los \$4,600,000.00.

Causa: Control interno, falta de monitoreo de transacciones recibidas.

Recomendación: Se sugiere un sistema que monitoree las transacciones recibidas y que dé un aviso de alerta cuando se reciban transacciones no habituales o un exceso de transacciones. De esta forma se pueden comunicar con el negocio con el fin de consultar y verificar si tienen alguna oferta o indagar sobre por qué se están recibiendo tantos pagos. Esto, además, puede ayudar a comparar el historial de transacciones del negocio.

SECCIÓN 7: CONCLUSIÓN

El fraude en la industria de viajes y paquetes de vacaciones es más común de lo que de inicio se podría pensar. Según el Sumario Anual de Querellas reportadas por los Consumidores para el año 2017, que fue publicado por el *Federal Trade Commission* (FTC, por sus siglas en inglés), los llamados fraudes de *Travel, Vacation and Timeshare Plans* se encuentran clasificados en el número quince (15) entre sus treinta (30) categorías de fraude reportadas con un total 22,264 querellas presentadas, lo que constituye el 0.83% del total de los reclamos presentados (Federal Trade Commission, 2017a). Sin embargo, este tipo de fraude se encuentra clasificado en el séptimo (7mo) lugar de los diez (10) fraudes más dañinos a nivel económicos, ya que la pérdida total de los querellantes llega hasta los \$38,000,000.00, o \$1,710.00 promediado por cada uno de los 22,264 casos presentados (Federal Trade Commission, 2017b). Aunque dicho Sumario del FTC refleja que este tipo de fraude no está entre los más comunes o practicados en Puerto Rico, los consumidores boricuas deben proceder siempre con cautela a la hora de planificar sus viajes y verificar la autenticidad de las ofertas, consultar directamente con la línea aérea para cotejar que dicha oferta es verdadera. Consultar y comparar precios antes de realizar una compra. Buscar reseñas, opiniones y referencias del lugar donde desea comprar. De esta forma se pueden lograr minimizar el riesgo a caer o ser víctimas de un fraude.

SECCIÓN 8: REFERENCIAS

- Access Data. (2018). Forensic Toolkit (FTK). Recuperado de
<https://accessdata.com/products-services/forensic-toolkit-ftk>
- Belkasoft. (2018). Belkasoft RAM Capturer: Volatile Memory Acquisition Tool.
Recuperado de <https://belkasoft.com/ram-capturer>
- Better Business Bureau. (BBB). (2017, mayo, 07). Steer Clear of These Vacation Scams.
Recuperado de <https://www.bbb.org/northern-alabama/news-events/news-releases/2017/steer-clear-of-these-vacation-scams>
- Better Business Bureau. (BBB). (2018). Serving Southeast Florida & the Caribbean.
Recuperado de <https://www.bbb.org/local-bbb/bbb-serving-southeast-florida-and-the-caribbean>
- Cellebrite. (s.f.). UFED Cloud Analyzer. Recuperado de
<https://www.cellebrite.com/en/products/ufed-cloud-analyzer/>
- Department of Justice Northern District of West Virginia. (2018a). Wheeling man admits to wire fraud. Recuperado de
<https://www.justice.gov/usao-ndwv/pr/wheeling-man-admits-wire-fraud>
- Department of Justice Southern District of Texas. (2018b). Bellaire Man Charged in Ponzi Scheme. Recuperado de
<https://www.justice.gov/usao-sdtx/pr/bellaire-man-charged-ponzi-scheme>
- Departamento de Asuntos del Consumidor. (2018). Anuncios engañosos. Recuperado de
<https://www.daco.pr.gov/consumidores/conoce-tus-derechos/reglamento-anuncios-enganosos/>
- Economía Simple. (2016). Tarjetas de débito. Recuperado de
<https://www.economiasimple.net/tarjetas-de-debito.html>

Fraude. (2004). Black's Law Dictionary. (8va ed.). St. Paul, Minnesota: West a Thomson.

Federal Bureau of Investigation. (FBI). (s.f.a). Ponzi Schemes. Recuperado de

<https://www.fbi.gov/scams-and-safety/common-fraud-schemes/ponzi-schemes>

Federal Bureau of Investigation. (FBI). (s.f.b). Internet Fraud. Recuperado de

<https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud>

Federal Bureau of Investigation. (FBI). (s.f.c) Internet Crime Complaint Center (IC3)

About Us. Recuperado de <https://www.ic3.gov/about/default.aspx>

Federal Bureau of Investigation. (FBI). (s.f.d) Internet Crime Complaint Center (IC3) 2017

Internet Crime Report. Recuperado de https://pdf.ic3.gov/2017_IC3Report.pdf

Federal Trade Commission. (2017a). Consumer Sentinel Network Data Book 2017.

Recuperado de [https://www.ftc.gov/policy/reports/policy-reports/commission-staff-](https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/consumer-sentinel-network-data-book-2017/report-categories)

[reports/consumer-sentinel-network-data-book-2017/report-categories](https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/consumer-sentinel-network-data-book-2017/report-categories)

Federal Trade Commission. (2017b). Consumer Sentinel Network Data Book 2017.

Recuperado de [https://www.ftc.gov/policy/reports/policy-reports/commission-staff-](https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/consumer-sentinel-network-data-book-2017/top-ten-fraud-categories-id-)

[reports/consumer-sentinel-network-data-book-2017/top-ten-fraud-categories-id-](https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/consumer-sentinel-network-data-book-2017/top-ten-fraud-categories-id-)

[other](https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/consumer-sentinel-network-data-book-2017/top-ten-fraud-categories-id-)

KaliTools. (2014, febrero, 16). Bulk-extractor. Recuperado de

<https://tools.kali.org/forensics/bulk-extractor>

Magnet Forensics. (2018). Magnet AXIOM. Recuperado de

<https://www.magnetforensics.com/magnet-axiom/>

National White Collar Crime Center. (NW3C). (2014). Internet Fraud. Recuperado de

<https://www.nw3c.org/docs/research/internet-fraud.pdf?sfvrsn=10>

Real Academia Española. (2018a). Correo electrónico. Recuperado de

<https://dle.rae.es/?id=AyfHjz9>

Real Academia Española. (2018b). Restitución. Recuperado de

<https://dle.rae.es/?id=WEMpqPl>

Real Academia Española. (2018c). Cupón. Recuperado de <https://dle.rae.es/?id=Bhej8JH>

Square, Inc. (2018). About Us. Recuperado de <https://squareup.com/about>

United States of America vs. Patricia M. Urbanovsky, No.8:16CR52, (D. Neb., 2016).

Recuperado de <https://www.justice.gov/usao-ne/file/836971/downloadopular>

United States of America vs. Victoria Scardigno, No. 10CR384, (D. NY., 2010).

Recuperado de

<http://files.courthousenews.com/2010/04/02/ScardignoComplaint.pdf>