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

FRAUDE EN DEVOLUCIONES A COMPRAS EN AMAZON.COM
ANÁLISIS DEL CASO: USA VS. ERIN FINAN, LEAH FINAN Y DANIJEL GLUMAC
NÚMERO DE CASO 1:17-CR-00087 / 1:17-CR-0091

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

FEBRERO DE 2019

PREPARADO POR
RAÚL A. CORDERO ORTIZ

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

FRAUDE EN DEVOLUCIONES A COMPRAS EN AMAZON.COM
ANÁLISIS DEL CASO: USA VS. ERIN FINAN, LEAH FINAN Y DANIJEL GLUMAC
NÚMERO DE CASO 1:17-CR-00087 / 1:17-CR-0091

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

PREPARADO POR
RAÚL A. CORDERO ORTIZ

Ha sido aceptado como requisito parcial para el grado de:
Maestría en Seguridad de Información e Investigación de Fraude Digital

FEBRERO DE 2019

APROBADO POR:

Dr. Miguel A. Drouyn Marrero
Director Escuela Graduada

TABLA DE CONTENIDO

SECCIÓN 4: INFORME DEL CASO

TABLA DE FIGURAS

SECCIÓN I- INTRODUCCIÓN Y TRASFONDO

Introducción

En el mundo cibernético, el internet es el epicentro que posibilita el flujo de datos e información a todos los niveles y de todas las procedencias. Las empresas, el gobierno, y las industrias, se mueven y operan a través de sistemas o plataformas en internet, las posibilidades de acceso al internet permiten que una persona pueda conectarse fácilmente para encontrar todo tipo de bienes, servicios e información deseada. En esta interacción con los medios cibernéticos existen no solo posibilidades, también riesgos y con estos, el fraude.

La Asociación de Examinadores de Fraude Certificados define el fraude como “el acto intencional y deliberado de privar a otra persona de propiedad, dinero y otros bienes, mediante engaño y otras formas injustas" (ACFE, 2018). Para que se constituya el fraude, deben darse las siguientes condiciones: una declaración falsa o una falsa representación de la verdad, el conocimiento del perpetrador de que la declaración o la representación pronunciada es falsa, la confianza de la víctima en dicha declaración y, por último, que haya daños como resultado de la confianza brindada por la víctima (Wells, 2013). Para efectos de este trabajo, el fraude es el acto premeditado e intencional de engañar a una persona o entidad con el fin de obtener un bien o servicio. Como se consecuencia de este acto, la persona o entidad engañada, sufre daño y pérdidas.

En cuanto a las compras en línea o compras *online*, es importante mencionar que se han convertido en una popular forma de adquirir todo tipo de objeto deseado o reconocido como necesario. Ante el auge y la popularidad del internet, Amazon.com, una compañía de ventas en línea se ha impuesto como la líder y principal imagen del mercado. Los números de Amazon.com son evidencia de su éxito, desde sus inicios han superado sus propios límites,

creciendo en ganancias de forma exponencial. En el año 2017, el magnate de las ventas reportó la cifra de 178 billones de dólares en ganancias. Actualmente es el más grande centro de ventas de artículos en línea, reportando cerca de 140 millones de ventas mensuales a través de plataforma, seguido por Walmart con 82 millones de ventas mensuales, y por el popular portal eBay que reporta cerca de 58 millones (Statista, 2018b).

Por otra parte, Amazon.com no solo se dedica a vender, sino que también ofrece servicios para vendedores externos los llamados *third party retail sellers,* quienes generan ingresos adicionales de suscripciones con servicios exclusivos como: *Amazon Prime, Web Service, Music, Instant Video y* por último son los fabricantes de sus propios artículos electrónicos como las tabletas: *Kindle e-Reader, Kindle Fire y* el sistema inteligente *Alexa* (Mohan, 2018). Datos adicionales afirman que los miembros de *Amazon Prime*, gastan un promedio anual de $1,400 dólares en la plataforma, comparados con los compradores no miembros de la membresía Prime, que gastan cerca de $600 dólares, accediendo desde dispositivos móviles o desde la comodidad de sus hogares (Statista, 2018a).

Habiendo compartido algunos detalles sobre el uso de internet y como el fraude es una constante posibilidad, se presentará el caso de una pareja que defraudó a Amazon.com con la ayuda de un cómplice, logrando engañar, abusar y vender artículos obtenidos ilegalmente.

Descripción del caso

Caso: Estados Unidos vs Erin and Leah Finan

Estados Unidos vs Danijel Glumac

Número de Caso 1:17-cr-00087-TWP-MJD (Erin y Leah Finans)

1:17-cr-00091 (Danijel Glumac)

Partes del Caso

1. Erin J. Finan
2. Leah J. Finan
3. Danijel Glumac

Investigadores

1. Gabriel Grchan (IRS-CI Special Agent, Agente Especial Rentas Internas)
2. Patricia Armstrong (Inspector in Charge US Postal Inspection Service, Inspector a Cargo del Servicio de Inspección del Correo Postal)

Abogados

1. Dominic David Martin representando a Erin Finan
2. Richard L. Ford representando a Leah Finan
3. Charles C. Hayes y Nicholas J. Linder representando a Danijel Glumac

Fiscal

1. Nicholas J. Linder (Fiscal Distrito Sur de Indiana)
2. Josh Minkler (Fiscal Asistente Distrito Sur de Indiana)

Jueza:

1. Hon. Tanya Walton Pratt (Corte del Distrito Sur de Indiana)

Trasfondo

En el caso a discutir, Erin Finan y su esposa reportaban ser residentes de varias propiedades localizadas en algunas ciudades y pueblos de las afueras del Distrito Sur de Indiana. Estos procrearon cuatro hijos como parte de su unión matrimonial. Los Finans operaron y controlaron varias cuentas de banco bajo el nombre de los siguientes negocios: "Tech Pro Services" y "Trade Plus". (United States of America vs Erin Finan, 2017)

Danijel Glumac, tercer cómplice era residente de Indianápolis, una ciudad en el Distrito Sur de Indiana. Era el dueño de la corporación SO TRADE LLC, la cual era usada para operar un supuesto negocio de ropa. Glumac también controlaba varias cuentas de banco a nombre de SO TRADE LLC. (United States v. Danijel Glumac, 2017)

Erin Finan y su esposa Leah Finan, junto a Danijel Glumac, fueron acusados por participar de un esquema para defraudar la política de devoluciones de Amazon, reclamando reemplazos nuevos por artículos que no estaban dañados. Los artículos devueltos por Amazon les eran vendidos a Danijel Glumac, quien a su vez los vendía a una tercera entidad, para culminar haciéndole pagos a los Finan a través de transferencias por cable o depósitos de cheques. (United States v. Danijel Glumac, 2017)

Descripción de hechos

Según descritos en los documentos legales de los casos: United States vs Erin Finan y United States v. Danijel Glumac, se encontró que entre el 2014 y el 2018, los Finans ejecutaron un esquema para defraudar a Amazon, reclamando falsamente que artículos ordenados estaban dañados, le faltaban partes y requerían reemplazos. Los Finan indicaban falsamente que los reemplazos que enviaba Amazon.com también estaban dañados o no trabajan correctamente. Los hechos se dieron de la siguiente forma:

1. Explotaron la política de servicio al cliente reclamando repetida y falsamente, que los electrónicos ordenados estaban dañados o no trabajaban y requiriendo y recibiendo reemplazos de Amazon, sin ningún costo.
2. Los Finans crearon identidades falses, recuperando sus artículos robados de tiendas de envío al por menor en Indiana y vendiéndolas, a su socio Danijel Glumac.
3. Glumac compraba los equipos y artículos a los Finans a sabiendas que estos eran hurtados y obtenidos fraudulentamente. La compra de los objetos se daba a un costo sustancialmente menor al costo del mercado. Estos artículos obtenidos por Glumac eran revendidos a una entidad en Nueva York que también los vendía, pero al público en general.
4. Los Finans recibían los artículos directamente de Amazon en el estado de Indiana. El envío de los artículos se llevaba a cabo a través de un transportista comercial como UPS o FedEx y también por el correo postal de los Estados Unidos.
5. Danijel Glumac lavaba el dinero obtenido usando una cuenta de banco a nombre de la comparación comercial SO TRADE LLC para recibir pagos desde la entidad en Nueva York que le compraba los artículos robados. Glumac usaba esos fondos recibidos para

pagarle a los Finans, ya fuera por cheque, en efectivo o a través de transferencias bancarias.

6. Los Finans reclamaban los artículos en establecimientos de entrega de Amazon y vendían el artículo a Danijel Glumac, que les pagaba por transferencia por cable, o cheque depositado en cuentas de compañías ficticias (*Shell Companies*) que Erin Finan creó para eso propósitos.
7. De octubre del 2014 a junio del 2016 recibieron un total de $580,000 a través de 200 transferencias por cable (*Wire Transference*) y aproximadamente 20 cheques de la cuenta de banco de Glumac.
8. Erin y Leah Finans enfocaron el esquema en artículos requeridos por Glumac: consolas *Xbox One* de Microsoft, Tabletas *Surface* de Microsoft, relojes inteligentes Samsung, y computadoras portátiles Apple *Macbook.*
9. Los Finans usaron el dinero para gastos de la vida diaria, comidas y artículos, y comprar tarjetas de regalo de Amazon.com que continuaron usando para el esquema.

Acusaciones, cargos y penalidades

Los Cargos Incurridos según la Información Provista en los "Documentos de Penalidades" o *Penalty Sheets* de los casos 1:17-cr-0091 y 1:17-cr-0087.

Danijel Glumac

1. 18 U.S.C. § 2314 *Interstate Transportation of Stolen Property* / Transporte de bienes robados, de valores, fondos, fraudulentas Sellos de Impuestos del Estado, o de los artículos usados en la falsificación. Danijel Glumac transportó artículos robados que obtuvo a través de los Finans, uso el correo postal de los Estados Unidos y otros

proveedores privados para transportar la mercancía obtenida ilegalmente a una entidad en Nueva York que le pagaba por lo artículos.

2. 18 U.S.C. §§ 1956(a)(1)(A)(i) and 1956 (a) (1) (B) (i) *Money Laundering.* Lavado de Dinero. El dinero que el Glumac obtenía de las ventas ilícitas, lo depositaba en cuentas bancarias asociadas a un negocio de ropa. Utilizaba cheques emitidos a nombre de su compañía para pagar por artículos ilegales que le vendían los Finans.

Erin y Leah Finan

1. 18 U.S.C. §§ 1341 *Frauds and swindles*. Fraude y Estafas. Erin y Leah Finan, defraudaron a Amazon.com, solicitando que le hicieran cambios y reembolsos por artículos que no se encontraban realmente dañados.
2. 18 U.S.C. §§ 1956 (a) (1) (A) (i) y 1956 (a) (1) (B) (i) *Money Laundering.* Lavado de Dinero. Los Finan depositaron dinero en cuentas bancarias y recibieron pagos a través de cheques por la mercancía robada a Amazon y vendida al Danijel Glumac.

Penalidades

Según Información descrita por el Departamento de Justicia de los Estados Unidos. Los tres acusados, accedieron a declararse culpables y recibieron:

1. Pena de Cárcel de 71 meses para Erin Finan
2. Pena de Cárcel de 68 meses para Leah Finan
3. Pena de Cárcel de 24 meses para Danijel Glumac
4. Restitución de la cantidad de $1,218.504.00 a Amazon.com.

Definición de Términos

1. *third party retail sellers* que son vendedores independientes que formalizan un acuerdo con Amazon.com para vender sus productos a través de la plataforma, a cambio de ceder un porcentaje de la venta. (Rankin, 2016)
2. Compras en línea, se refiere a la compra de productos y servicios a través del Internet (The Law Dictionary, 2018)
3. Transportista Comercial, se refiere a una entidad comercial que recibe un pago por transportar bienes. Algunos ejemplos son el Correo Postal (USPS), FedEx, UPS, entre otros.

SECCIÓN II-REVISIÓN DE LITERATURA

Introducción

La prevención del fraude a los comercios y a las tiendas ha sido objeto de múltiples investigaciones y acuerdos colaborativos. En la actualidad el gobierno de Estados Unidos entiende que el fraude a estos comercios constituye un gran problema a la economía. En una investigación ordenada por el Congreso de los Estados Unidos y realizada por la investigadora especialista en seguridad doméstica, Kristin M. Finklea (2012), documentó el grave problema que causa el llamado: "Crimen organizado a minoristas" u *Organized Retail Crime* (ORC). En la mencionada investigación se definió el ORC "como robo y fraude a minoristas a gran escala por parte de grupos organizados de ladrones de tiendas profesionales." (pág. 1) Finklea también menciona que: "los ladrones profesionales ganan dinero robando mercancía del comercio minorista y otros lugares y revendiéndolos a personas o comercios que a su vez venden los bienes, a través de medios económicos o ilegales, por una fracción del costo minorista." (pág. 3). La investigadora expuso la forma de operar de estas organizaciones delictivas y hasta vinculó este quehacer criminal con posibles afiliaciones económicas a grupos terroristas, el lavado de dinero y la exportación de estos artículos robados al exterior.

Fraudes Involucrados

La investigación del Congreso trajo como consecuencia gestiones oficiales del estado respecto a este problema, dando paso a la creación de una unidad especializada de las fuerzas de ley y orden para manejar el asunto. El Departamento de Seguridad Nacional de los Estados Unidos y el *US Immigration and Customs Enforcement* (ICE), crearon en el 2012 la iniciativa SEARCH (*Seizing Earning and Assets from Retain Crime Heists*) que busca encontrar estas organizaciones criminales que atacan comercios. Realizando acuerdos colaborativos con organizaciones como: la Federación Nacional de Minoristas o *National Retail Federation* (NRF) y la Asociación de Líderes de la Industria Minorista o la *Retail Industry Leaders Association* (RILA), y otras, se han unido en el esfuerzo de identificar y erradicar este problema. Estas entienden que el fraude no solo se da físicamente en las tiendas y establecimientos comerciales, sino a través del robo mediante apropiación, compras no autorizadas con tarjetas de débito o crédito, a través de compras en la tienda o en plataformas en línea a utilizando el internet (U.S. Immigration and Customs Enforcement, 2012).

El esfuerzo por detener esta práctica ha sido estudiado y replicado por las organizaciones que intervienen con comercios de ventas. La NRF, realizó un estudio para evaluar el impacto financiero del llamado ORC, y el fraude a los reembolsos y devoluciones. La NRF concluyó que el promedio del impacto económico es mayor a los $700,000 por cada billón de dólares en ventas. Ante esta alarmante cifra, las organizaciones y comercios descritos asumen el problema como uno crítico y una amenaza seria a una industria que tiene que luchar con decenas de modalidades de robo y fraude. De la misma forma, el estudio concluyó que en promedio, los vendedores esperan que el 11% de los artículos vendidos sean devueltos, y que de esos artículos devueltos, un 11% sean de forma fraudulenta. En la época

navideña las devoluciones aumentan, asimismo el fraude (Moraca, 2017). Ya desde el 2012 se estaban investigando los lugares de ventas en línea como eBay, donde se identificó que estas compañías estaban tomando medidas para combatir la venta de artículos obtenidos fraudulentamente, y entre estas medidas se encontraban: la educación a vendedores y consumidores, la supervisión de actividad sospechosa y las alianzas con las agencias de ley y orden (Finklea, 2012). Los investigadores del fraude han concluido que "las áreas de mejora para para la detección y prevención del fraude a los minoristas deben estar dirigidas a aumentar la colaboración y la información que se comparte dentro de la industria, usar técnicas de autenticación avanzadas y adoptar los estándares de las industrias de pagos." (Malphrus, 2009, p. 33).

En relación con el caso de fraude a Amazon, cometido por Erin y Leah Finan, hay otros casos donde se identificó esta actividad ilegal, pero contra las tiendas Target y Walmart, mediante el uso indebido de la política de devoluciones. Estas políticas son formas en las que los comercios aumentan la satisfacción de sus clientes, brindándoles confianza en el producto obtenido al momento de la compra. Las políticas de devolución le garantizan al cliente que, de haber alguna situación con el producto obtenido, tienen la oportunidad de cambiarlo por otro artículo o de solicitar un reembolso, esta forma de operar es esperada por los consumidores. Es importante comprender que así como son beneficios para los clientes, también son medios y formas en las que los comercios pueden protegerse y cumplir con regulaciones o leyes aplicables. Según Thomson Reuters (2018), los estados tienen sus propias leyes para regular los reembolsos y las devoluciones. En algunos estados la regulación se limita a que los establecimientos tengan estas políticas colocadas en lugares visibles donde los clientes puedan verlas.

La Comisión Federal de Intercambio o el *Federal Trade Commision* (FTC) en inglés, es la agencia que se encarga de proteger a los consumidores y regular la forma en la que los comercios trabajan los cambios y los reembolsos. En Puerto Rico está el Departamento de Asuntos al Consumidor (DACO), y en los Estados Unidos el FTC, que recibe querellas de los clientes y realiza investigaciones para identificar posibles abusos e incumplimientos de parte de los comercios. Este proteccionismo es importante, porque crea balances en una economía altamente consumista y capitalista, pero no necesariamente protegiendo al comerciante en caso de que sea el defraudado. Ante la realidad de los abusos cometidos en contra de los comercios, han cobrado gran importancia las alianzas dirigidas por organizaciones junto a agencias de ley y orden, dando paso a la discusión de elementos relacionados a la llamada industria minorista. La ya mencionada NRF y la llamada *Retail Industry Leaders Association* (RILA), son perfectos ejemplos de organizaciones que proveen toda clase de material, adaptado a la vanguardia de la industria, para que los participantes y comerciantes puedan protegerse del fraude (National Retail Federation, 2018).

En el caso donde Erin y Leah Finan, junto a Danijel Glumac defraudaron a Amazon, quedó en evidencia la vulnerabilidad del proceso de reclamos que la compañía tiene con sus clientes y al mismo tiempo, los conocimientos, la suspicacia y la brillantez de estos defraudadores. Es sabido que Amazon es un titán de las ventas en línea, levantándose como el indiscutible campeón en su generación. Como fue mencionado anteriormente, para el año 2017 se reportó la cifra de 178 billones de dólares en ganancias; también son el centro de ventas en línea más grande, reportando 140 millones de ventas mensuales (Statista, 2018b). Es lógico considerar que una empresa que tiene tantas ganancias pueda tomarse ciertas

libertades o ciertos riesgos con el fin de satisfacer a sus clientes y atraer muchos más compradores.

Una mirada a la política de devoluciones de Amazon nos permite comprender la gran capacidad que tiene la compañía para atraer a sus clientes. Desde su propio portal en el área de Servicio al Cliente, salta a los ojos el título “Acerca de las devoluciones gratuitas”. A continuación, se estarán mencionado algunos fragmentos importantes de la política de devoluciones, según indica el portal de Amazon (2018a):

> Solo los productos que se mencionan que son elegibles para devoluciones gratuitas en la página de detalles del producto son elegibles para una devolución gratuita. Las devoluciones gratuitas solo se aplican a los productos despachados por Amazon. No se aplican a los mismos productos despachados por otros vendedores. No se requiere ninguna compra mínima para recibir devoluciones gratuitas.
>
> Todo el empaque del producto y los certificados de autenticidad, calificación y valoración se deben devolver con el producto. Se rechazarán todos los productos que se devuelvan sin la documentación original. No se aceptará la devolución de ningún producto cuyo tamaño haya sido modificado o que haya sido dañado o alterado de alguna otra manera después de la entrega.

En cuanto a los reembolsos según el portal Amazon (2018b) “Acerca de los reembolsos”

> En algunos casos, es posible que se te ofrezca la opción de un "reembolso instantáneo" para que puedas usar tu reembolso sin tener que esperar a que procesemos tu devolución. Los reembolsos instantáneos se emitieron a tu tarjeta de crédito o como un saldo de la tarjeta de regalo de Amazon. Las entidades emisoras de tarjetas de crédito requieren entre 3 y 5 días hábiles adicionales para procesar los reembolsos emitidos a la tarjeta. Aun así, debes devolver tus productos en un plazo de 30 días. Amazon puede determinar que el reembolso puede emitirse sin la necesidad de una devolución. Si no es necesario que envíes el producto de vuelta para obtener un reembolso, te lo notificaremos en el Centro de devoluciones o por medio de nuestro agente del Servicio de Atención al Cliente.

Según indican las políticas, las devoluciones y los reembolsos tienen criterios aplicables claramente definidos, sin embargo, en la sección “Acerca de los Reembolsos” Amazon, indica lo siguiente: “En algunos casos, es posible que se te ofrezca la opción de un "reembolso instantáneo" para que puedas usar tu reembolso sin tener que esperar a que procesemos tu devolución.” (Amazon, 2018b). Esta sección de la política de reembolso plantea básicamente que habrá ocasiones en las que se realizará el reembolso, aun cuando no se haya procesado la devolución del artículo. Luego vuelve a indicar que “Amazon puede determinar que el reembolso puede emitirse sin la necesidad de una devolución.” (Amazon, 2018b). La Figura 1, ofrece unos detalles adicionales sobre los criterios para las devoluciones.

Reembolsos parciales y tarifas de reabastecimiento

Si devuelves	Recibirás
Productos en su condición original pasado el plazo de devolución*	80% del precio del producto
CD, DVD, videos, videojuegos, casetes o discos de vinilo que han sido abiertos (sacados del envoltorio plástico)	50% del precio del producto
Productos dañados, con partes faltantes, que no se encuentran en su condición original o tienen signos evidentes de uso, que se devuelven por causas ajenas a Amazon.com	Hasta 50% del precio del producto
Software abierto devuelto por causas ajenas a Amazon.com	0% del precio del producto

Figura 1 Reembolsos parciales y tarifas de reabastecimiento (Amazon, 2018a)

En las instancias anteriormente mencionadas es que Leah Finan, Erin Finan y Danijel Glumac defraudaron a Amazon y por motivo de los espacios no definidos en su política de devoluciones. En definitiva, desde el lado de la satisfacción del cliente, Amazon atiende muy generosamente los reclamos y las devoluciones según indica su propia política; pero en el mundo real existe el fraude y este coexiste con personas con el conocimiento suficiente para explotar cualquier vulnerabilidad que puedan identificar. Es necesario considerar que “el fraude comienza con simple y pequeño evento. Típicamente la avaricia aparece y después de unos pequeños incidentes la actividad delictiva se dispara, costando miles al comercio.” (Snocken, 2004, p. 52).

A continuación, se comentará sobre algunos casos donde se hizo mal uso de las políticas de evoluciones y/o reembolsos de unos importantes comercios, y se presentará un caso donde se realizaron solicitudes fraudulentas de reembolsos al IRS.

Casos Relacionados

Se puede hacer mención de varios casos de renombre donde se explotaron fraudulentamente las políticas de devoluciones y reembolsos en unos comercios muy importantes en los Estados Unidos.

Caso United States v Claude Allen, 06-BG-958 (Corte de Apelaciones Distrito de Columbia, 2011). Las declaraciones iniciales del caso fueron las siguientes: Claude Allen, funcionario del Gobierno de los Estados Unidos bajo el gobierno del expresidente George W. Bush, fue arrestado en el estado de Maryland por cargos de robo de propiedad. Allen robó un equipo de sonido Bose, valorado en $525 de una tienda Target en Montgomery Country en Maryland. En enero del 2006 robó también un *stereo* marca RCA, valorado en $88.00 de otra tienda Target en Maryland. La gestión fue realizada mediante un esquema de compras y regresos fraudulentos, donde el convicto compraba los artículos con una tarjeta de crédito y procedía a salir de la tienda, luego regresaba a la misma tienda o a otra tienda cercana con el recibo de compra, pero sin el artículo; se dirigía entonces a tomar un artículo idéntico de las góndolas y lo devolvía usando el recibo del articulo original. A través de este esquema de devoluciones, el defraudador salía con el dinero de la devolución y se quedaba con el artículo comprado inicialmente. Cuando se identificó el fraude, fue arrestado y acusado de robo de propiedad por debajo de $500.00. Es importante mencionar que el Claude Allen fue asesor del presidente Bush en la política doméstica y lideró parte de la respuesta de casa blanca con el Huracán Katrina.

El convicto no solo fue encausado por Target, también atacó la tienda Hecht's, según reseñó el importante medio CNN (2006). Se indica que visitó en más de 25 ocasiones los establecimientos comerciales para comprar y devolver artículos con el mismo modo de

operar. Los artículos fueron en su mayoría: equipos de sonido *Bose*, impresoras de foto, ropa y otros artículos de mucho menos valor. Este caso tomó gran notoriedad por la relación con el presidente Bush, ya que Allen era un asesor importante del ala derecha conservadora, incluso fue nominado por el expresidente para ser juez federal en el 2003. El crimen salió a la luz cuando un gerente de la Tienda *Target* en Gaithersburg, observó a Allen entrando a la tienda con un carro de compra vacío, luego llenó el carro de unos artículos y pasó por el área de servicios, donde solicitó un reembolso por los artículos que acaba de colocar en el carro sin haberlos pagado. El convicto también colocó artículos adicionales que no pagó al salir de la tienda. Es importante mencionar que este tipo de crímenes no siempre está asociado a criminales de bajos ingresos, porque Allen ganó más de $161,000 en su trabajo como asesor del presidente. (CNN, 2006).

Caso US v. Thomas Frudaker (2018). Un segundo caso de gran notoriedad fue reseñado por diversos medios en los Estados Unidos; un hombre de Yuma, Arizona, fue acusado por realizar devoluciones fraudulentas a más de 1,000 tiendas Walmart a través de los Estados Unidos. Thomas Frudaker de tan solo 23 años, fue arrestado luego de que las autoridades recibieran reportes de una transacción fraudulenta a un Walmart de la zona de Yuma (Sheets, 2018). El fraude era realizado cuando Frudaker compraba computadoras, les sacaba piezas y procedía a devolverlas; en síntesis: exigía reembolsos y devoluciones por artículos que había alterado (Popovich, 2018). Walmart estima que el fraude le pudo haber costado cerca de 1.3 millones. El joven fue arrestado, enfrentando seis cargos incluyendo dos cargos por robo, dos cargos por esquemas fraudulentos y dos cargos por daños criminales (Perano, 2018). Este caso puso en evidencia las viles formas en las que los defraudadores abusan de las políticas de devolución de las compañías. Este crimen no solo ocurre con los

comercios, tiendas y detallistas, también ocurre en el gobierno, quien tiene una situación parecida con las reclamaciones al IRS para devoluciones por impuestos.

US v. Tomasino, 17-1331P (Corte de Apelaciones del Primer Circuito, 2018). Hace unos años tomó gran notoriedad un caso que vinculaba el robo de identidad a ciudadanos de Puerto Rico, para ser utilizadas por un grupo de criminales, con un esquema de fraude al Servicio de Impuestos Internos de los Estados Unidos o IRS, por sus siglas en inglés. El caso trajo convicciones criminales por lavado de dinero y el robo de identidad. Se identificó que cuatro individuos, tres mujeres y un hombre propietario de un supermercado, participaron en el esquema. Estos hicieron uso de declaraciones falsas, recibiendo reintegros de los impuestos federales y generando ganancias millonarias que fueron colocadas en diversas cuentas bancarias. El esquema fraudulento de reembolsos y reclamaciones se extendió del 2010 al 2014, y se evidenció que los acusados usaron tarjetas de seguro social, tarjetas de identificación personal, junto a otros documentos de personas nacidas exclusivamente en Puerto Rico. El IRS se percata del fraude y logra detener a los acusados con la ayuda de las agencias federales, que determinaron que el fraude ascendió a los $2.8 millones de dólares en reclamaciones falsas. (Departamento de Justicia de los Estados Unidos, 2016)

En el caso US v. Tomasino, no se aprecia el fraude en reembolsos y devoluciones a una tienda, comercio o detallista, sino al gobierno de los Estados Unidos. Para llevarse a cabo el fraude, se requirió el engaño, una falsa representación de la verdad, asumir una identidad fraudulenta y tramitar el lavado del dinero obtenido. Este quehacer fraudulento e ilegal para obtener un beneficio, fue el proceder de Claude Allen, Tomas Frundaker, Tomasino sus cómplices y finalmente Erin y Leah Finan, junto al Danijel Glumac.

Leyes Aplicables:

Según el Código Penal de los Estados Unidos: Los casos reseñados anteriormente fueron enjuiciados en los Estados Unidos de América, por tal motivo es fundamental poder mirar de cerca algunas de las disposiciones expresadas el código penal de la nación americana. Se entiende que en la mayoría de las instancias donde se llevan a cabo esquemas de fraude, se logran convicciones por cargos de fraude al Correo Postal y lavado de dinero. Es totalmente lógico que se usen medios disponibles para la transportación de artículos y bienes obtenidos fraudulentamente, y que luego de obtenidas las ganancias, se busque insertarlas en alguna cuenta de banco o algún otro medio legitimo para manejar el dinero.

En el caso US v. Erin y Leah Finan alcanzaron convicción por los siguientes delitos:

1) 18 U.S. Code § 1341 – Fraudes y estafas/ *Frauds and swindles.* El código penal de los Estados Unidos indica que;

   Cualquier persona que haya ideado o tenga la intención de idear cualquier plan o artificio para defraudar o para obtener dinero o propiedad mediante pretensiones, representaciones o promesas falsas o fraudulentas, o para vender, disponer, prestar, intercambiar, alterar, regalar, distribuir, suministrar o proporcionar o procurar para uso ilegal cualquier moneda, obligación, garantía u otro artículo falsificado o cualquier cosa que se represente o se considere como tal. (Legal Information Institute, 2018a)

2) 18 U.S. Code § 1956 (a)(1)(B)(i) – Lavado de dinero/ *Money Laundering.* El código penal de los Estados Unidos cita*:*

   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 sabiendo que la transacción está diseñada en su totalidad o en parte: para ocultar o disfrazar la naturaleza, la ubicación, la fuente, la propiedad o el control de los productos de actividades ilícitas especificadas. (Legal Information Institute, 2018b)

El tercer implicado Danijel Glumac, se declaró culpable de los siguientes cargos:

1) 18 U.S. Code § 1956 (a)(1)(B)(i) – Lavado de dinero/ *Money Laundering*. El código penal de los Estados Unidos cita:

   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 sabiendo que la transacción está diseñada en su totalidad o en parte: para ocultar o disfrazar la naturaleza, la ubicación, la fuente, la propiedad o el control de los productos de actividades ilícitas especificadas. (Legal Information Institute, 2018b)

2) 18 U.S. Code § 2314 - Transporte de bienes robados, valores, dineros, estampillas de impuestos estatales fraudulentas o artículos usados en la falsificación. / *Transportation of stolen goods, securities, moneys, fraudulent State tax stamps, or articles used in counterfeiting.* El código penal de los Estados Unidos cita:

   Quien transporta, transmite o transfiere, en el comercio interestatal o en el extranjero, bienes, mercancías, mercaderías, valores o dinero, de un valor de $ 5,000 o más, sabiendo que fueron robados, convertidos o tomados por fraude. Quienquiera que transporte, transmita o transfiera, en el comercio interestatal o en el extranjero,

> cualquier objeto conmemorativo de veteranos, sabiendo que fue robado, convertido o tomado por fraude, (Legal Information Institute, 2018c)

Herramientas de Investigación

Las agencias de ley y orden utilizan la investigación forense para esclarecer casos y encontrar la verdad de lo ocurrido. La investigación forense digital se ha convertido en ese medio para encontrar la verdad en casos donde se integran los sistemas de información. Forense digital puede definirse como: “la preservación, identificación, extracción y documentación de evidencia computadorizada guardada en alguna forma magnética, óptica o electrónica.” (Craiger, 2016, p. 3). Este proceso envuelve la investigación metódica y empírica de recursos digitales en lo que se entiende como una ciencia en crecimiento. Al igual que se obtiene evidencia en una escena de crimen, en el aspecto digital la evidencia debe ser comprendida como “cualquier dato almacenado o transmitido usando una computadora que respalde o rechace una teoría de cómo ocurrió una ofensa o que aborda elementos críticos de la ofensa, como la intención o la coartada" (Casey, 2011, p. 8) El que se utilice esta evidencia recopilada para asuntos legales, ha permitido el establecimiento de estándares y criterios de autenticidad, al igual que una serie de herramientas y metodologías de investigación.

En su artículo “Computer Forensics Procedures and Methods” el Dr. Philip Craiger (2016), añade que se pueden identificar dos tipos de análisis forense digital: el análisis en línea y el análisis fuera de la red. El análisis fuera de la red ocurre cuando el investigador apaga la computadora y lo remueve de la red. Esto permite al investigador crear una copia exacta del disco duro de la computadora para asegurar que los archivos de la computadora permanezcan sin ser cambiados. El análisis en línea requiere el uso de programas de auditoria y plataformas que permiten el análisis de tráfico y datos.

Las reglas federales de evidencia deben ser asumidas a la hora de realizar metodología y procesos forenses en una computadora o equipo electrónico. El no realizarlo, puede significar que la evidencia no recopilada acorde a las reglas federales de evidencia puede ser desestimada por un juez. Esta recopilación exitosa ayuda a las empresas a y organizaciones a protegerse a sí mismas contra situaciones de invasión de privacidad, y reclamaciones fraudulentas (Casey, 2011).

La Investigación forense digital y sus herramientas, buscan mayormente el analizar la imagen forense capturada por el investigador, quien, a través de los programas, captura, guarda y replica los procesos que el sistema computadorizado realizaba. Usando las herramientas forenses es posible: recuperar archivos borrados, identificar artefactos, ver todos los archivos aun si estos han sido ocultos, y realizar análisis con diagnósticos que brinden información de lo que pudo haberles sucedido a los sistemas. (Cowen, 2013, págs. 11-12). Hay dos herramientas muy importantes en la auditoria y en la investigación forense digital, CaseWare IDEA y el Forensics Tool Kit o como es conocido mayormente por sus siglas FTK Imager.

La herramienta de auditoria CaseWare IDEA es muy popular, junto a ACL forma parte de las principales herramientas de monitoreo en muchas industrias. IDEA es famoso por su capacidad de convertir bases de datos de distintos formatos, además de tener una excelente facilidad de navegación entre reportes (CaseWare IDEA, 2019).

Las herramientas ofrecidas por FTK son muy útiles para la labor forense digital. En el campo investigativo digital, el FTK Imager goza de popularidad y prestigio. El uso principal del programa es el analizar evidencia de discos o imágenes de memoria, para obtener datos, analizar documentos y crear reportes, entre muchos otros asuntos (Nelson, Phillips, & Steuart,

2015, p. 111). Al momento en que se ejecuta la investigación forense, el software permite localizar evidencia y recolectar información, ya sea de múltiples dispositivos o aplicaciones. Los datos obtenidos se pueden guardar en carpetas, para crear informes y análisis que son bien aceptados por agencias de ley y orden (Forensics Toolkit, 2017). Estas herramientas forenses de investigación tienen el potencial de elevar grandemente la precisión y confiabilidad del proyecto a presentar.

SECCIÓN III- SIMULACIÓN DEL CASO

Introducción

El fraude cometido por Erin Finan y Leah Finan junto a Danijel Glumac en contra Amazon fue perpetrado muy inteligentemente. Los convictos tomaban ventaja de las vulnerabilidades en el proceso de compra, solicitud de reembolsos y devoluciones, de la famosa empresa de compras en línea. Una empresa de la importancia de Amazon.com, atiende cientos de miles de compras diariamente, y no solo compras, sino llamadas, correos electrónicos y reclamaciones de sus clientes. Esta gran cantidad de gestiones a realizar convierte a Amazon en un blanco vulnerable a ataques. Los defraudadores hicieron uso de múltiples cuentas y correos electrónicos, lo que les permitía pasar desapercibidos, imposibilitando que Amazon pudiera establecer patrones e indicadores que los vincularan con las reclamaciones. Para fines de esta investigación se detallará el esquema fraudulento de los Finans y su asociado Danijel Glumac.

El esquema comenzaba cuando Erin y Leah Finan creaban múltiples cuentas de correos electrónicos y procedían a registrarse en Amazon.com. Visitaban tiendas y locales comerciales donde venden tarjetas de regalo de Amazon, compraban las tarjetas por la cantidad necesaria para poder adquirir el artículo que deseaban y seguido de esto, realizaban las compras. Los artículos obtenidos eran en su mayoría consolas *Xbox One*, tabletas *Surface*, relojes inteligentes *Samsung* y computadoras portátiles *Apple Macbooks*. Los Finans solicitaban el envío de estos artículos a unos locales comerciales dedicados a recibir mercancía de Amazon para el recogido de sus clientes, mayormente conocidos como *Amazon Retail Pick Up Stores*. Una vez que los Finans recibían el artículo, se comunicaban con el Centro de Servicio al Cliente de Amazon para indicarles que el artículo no servía, le faltaban

piezas y requería reemplazo. Luego de recibir los reemplazos de Amazon, estos indicaban que tampoco servían, solicitando que les fuera enviado otro reemplazo sin haber tenido que devolver los primeros dos artículos recibidos.

Luego de que Erin y Leah Finan recibían los artículos robados a Amazon, contactaban a Danijel Glumac, que les compraba los artículos a sabiendas de su procedencia. Glumac pagaba por los artículos a través de cheques, efectivo o transferencias bancarias; los Finans por su parte, seguían comprando más tarjetas de regalo de Amazon, perpetuando el esquema. El dinero que obtenían también lo utilizaban para los gastos diarios de su familia. Danijel Glumac continuaba haciendo negocios, ya que enviaba los artículos a una entidad en Nueva York que le pagaba por los mismos. El transporte de los artículos se daba a través del correo postal de los Estados Unidos (USPS) y de transportistas comerciales como UPS o FedEx. El dinero obtenido de estas ventas era "lavado" a través de la cuenta de banco abierta por el Sr. Danijel Glumac a nombre de SO TRADE LLC, una cuenta asociada a una supuesta compañía de ropa. En la Figura 2 se describe el esquema de fraude contra Amazon.com.

Diagrama Simulación del Fraude

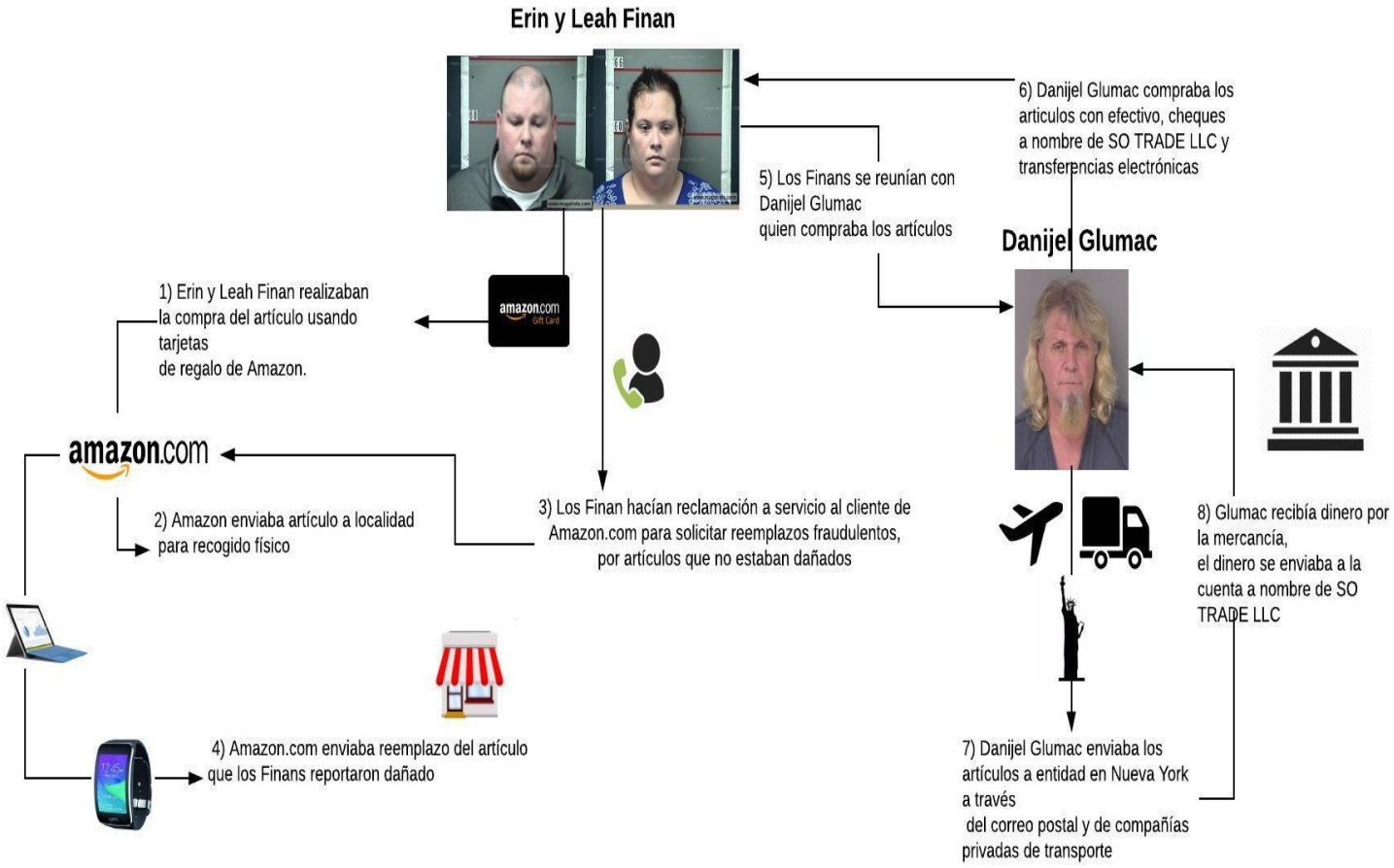


Figura 2- Detalle del esquema de fraude a Amazon

SECCIÓN IV- INFORME DEL CASO

Resumen Ejecutivo

La fiscalía federal del estado de Indiana, el agente especial del IRS Gabriel Grchan y Patricia Armstrong, Inspectora del Servicio Postal de los Estados Unidos, encargados de la investigación en curso en contra de los acusados Erin Finan, Leah Finan y Danijel Glumac, requieren de los servicios de un Investigador Forense Digital. Como parte de la investigación y el curso legal de los casos US vs Erin y Leah Finan y el caso US vs Danijel Glumac, se ha realizado una imagen del disco duro de la computadora personal de los Finans; con el fin de obtener evidencia sobre las imputaciones de fraude, estafas y lavado de dinero que pesan en contra de los acusados.

Con el objetivo de investigar la imagen del disco duro se contrataron los servicios del Raúl Cordero, investigador de fraude y especialista en forense digital. El investigador pudo examinar el disco duro con la imagen de la computadora personal de los Finans, recuperando conversaciones via correos electrónicos, y un documento con información de órdenes y artículos de mucha importancia que vincula a los acusados con artículos comprados en Amazon.com y sus cuentas de correo electrónico. La información encontrada vincula a Erin y Leah Finan a los cargos imputados, encontrándose conversaciones con el otro acusado Danijel Glumac, y un documento Excel con información que vincula los reemplazos solicitados por los Finan, con órdenes que Amazon identificó que no se devolvieron los artículos reclamados como dañados. Luego de obtenida la información le fue devuelto el disco duro a las autoridades con las evidencias encontradas.

Objetivo

El equipo de investigadores encargados para el caso US vs Finans y US vs Glumac, contrataron los servicios de Raúl Cordero, para realizar una examinación forense digital de la imagen del disco duro de la computadora personal de los Finans. La evidencia a recuperar tiene el objetivo de añadir peso a las evidencias ya obtenidas y lograr el éxito en la convicción de los acusados, quienes se alega que, reclamaron remplazos por artículos que no estaban realmente dañados y luego los vendían a Danijel Glumac, quien a su vez, los revendía a una entidad no identificada por las Autoridades en el estado de Nueva York. Los investigadores entienden que los Finans usaron múltiples números de teléfono, cuentas de correo electrónico y otras gestiones adicionales para ocultar su identidad y no ser identificados por Amazon.

Alcance del Trabajo

El 26 de febrero de 2019, los investigadores Gabriel Grchan y Patricia Armstrong, junto al fiscal del Distrito Sur de Indiana el Sr. Nicholas J. Linder, hicieron entrega del disco duro de 1Tb de memoria, marca *WD My Passport* con número de serie WX31A87C9HJI al investigador forense Raúl Cordero. El disco contenía una imagen de la memoria de la computadora personal de los Finans, una PC portátil marca *Windows Surface Book*. El fiscal y los investigadores aseguraron haber provisto una copia fiel y exacta de la memoria, cumpliendo con los estándares legales para el manejo forense de evidencia digital.

Para manejar los datos de la evidencia obtenida, se utilizó una computadora que contiene los programas FTK Imager y CaseWare IDEA para el análisis especifico de los datos contenidos en un documento formato Excel. IDEA es una herramienta de auditoría de mucho prestigio, utilizada por muchas industrias para mantener monitoreo de sus datos e información

financiera, proveedores y clientes, permitiendo la generación de reportes, gráficos e incidencias sobre los datos revisados. El programa de análisis de datos es una herramienta de facilidad que garantiza la integridad de los datos y acelera el análisis para auditorias eficientes. (IDEA Caseware, 2019)

La otra herramienta utilizada FTK Imager provee acceso a imágenes y archivos borrados de la computadora. Según el portal accessdata.com (2017), esta herramienta es frecuentemente citada en corte y en investigaciones, por motivo de su velocidad, estabilidad y facilidad de uso. También porque localiza evidencia, recolecta y analiza cualquier dispositivo digital que almacene datos.

Datos del Caso

Número de Caso: 2018-13-USSDI

Examinador Forense: Raúl Cordero Ortiz

Cliente: Oficina del Fiscal de los Estados Unidos del Distrito Sur de Indiana

Representante del Cliente: Ayudante Especial del Fiscal de distrito Sr. Josh Minkler

Descripción de los dispositivos utilizados

Los dispositivos utilizados durante el proceso de investigación forense digital fueron los siguientes:

1) Computadora portátil marca Hewlett Packard (HP), modelo Pavilion g6 Notebook, con procesador AMD A6-4400M APU con Readeon, un disco duro de 500 gb y 4 gb de RAM. Esta computadora cuenta con las herramientas FTK Imager, CaseWare IDEA y una serie de programas adicionales de investigación forense.

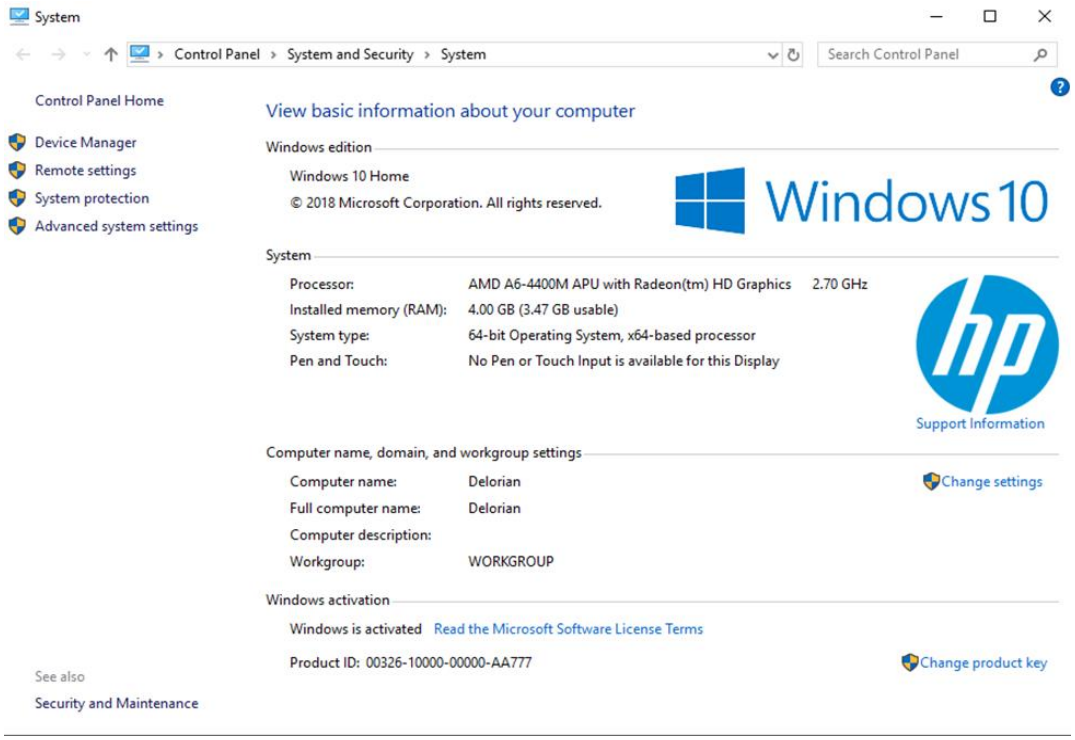


Figura 3 **-Especificaciones computadora portátil HP Pavilion g6**

2) Disco duro de 1Tb, marca *WD My Passport* con número de serie WX31A87C9HJI. Identificado como E1- 2018-13-USSDI. El disco fue entregado al investigador Raúl Cordero por el ayudante del Fiscal Especial, el Sr. Josh Minkler el 26 de febrero del 2019. El disco duro contiene una imagen de la memoria de la computadora portátil personal de Erin y Leah Finan.

3) USB Flash Drive, marca PNY de 8gb con tag de evidencia E2- 2018-13-USSDI. El USB contiene un documento Excel facilitado por Amazon, con información de solicitudes de reemplazos para clientes del Estado de Indiana. El documento contiene correos electrónicos de clientes, el articulo reclamado y si el primer articulo comprado fue o no fue devuelto. (ver Figura 5)

En la Figura 4 se muestra el disco duro entregado por las autoridades para el análisis forense.

Figura 4*- Imagen del disco duro marca *WD My Passport

La Figura 5 muestra USB PNY de 8gb con documento Excel provisto por Amazon.

***Figura 5*- USB con documento provisto por Amazon**

Resumen de Hallazgos

A continuación, se presentan los hallazgos identificados como producto de la examinación del disco duro entregado por la fiscalía federal. Se utilizaron las herramientas FTK Imager y CaseWare IDEA para analizar los datos. Los hallazgos identificados son:

1) Se encontraron dos archivos pdf y un documento formato Excel. Se entiende que estos archivos habían sido borrados de la computadora de los Finans. Los archivos formato pdf presentaban correos electrónicos de conversaciones entre Leah y Erin Finan con Danijel Glumac, donde se mencionaban reembolsos y devoluciones a artículos electrónicos ordenados.

En la Figura 6 se muestran los archivos recuperados en el disco duro a través de la herramienta FTK Imager, los archivos se encontraban bajo las carpetas “Confidential Files” y “Outlook Files”.

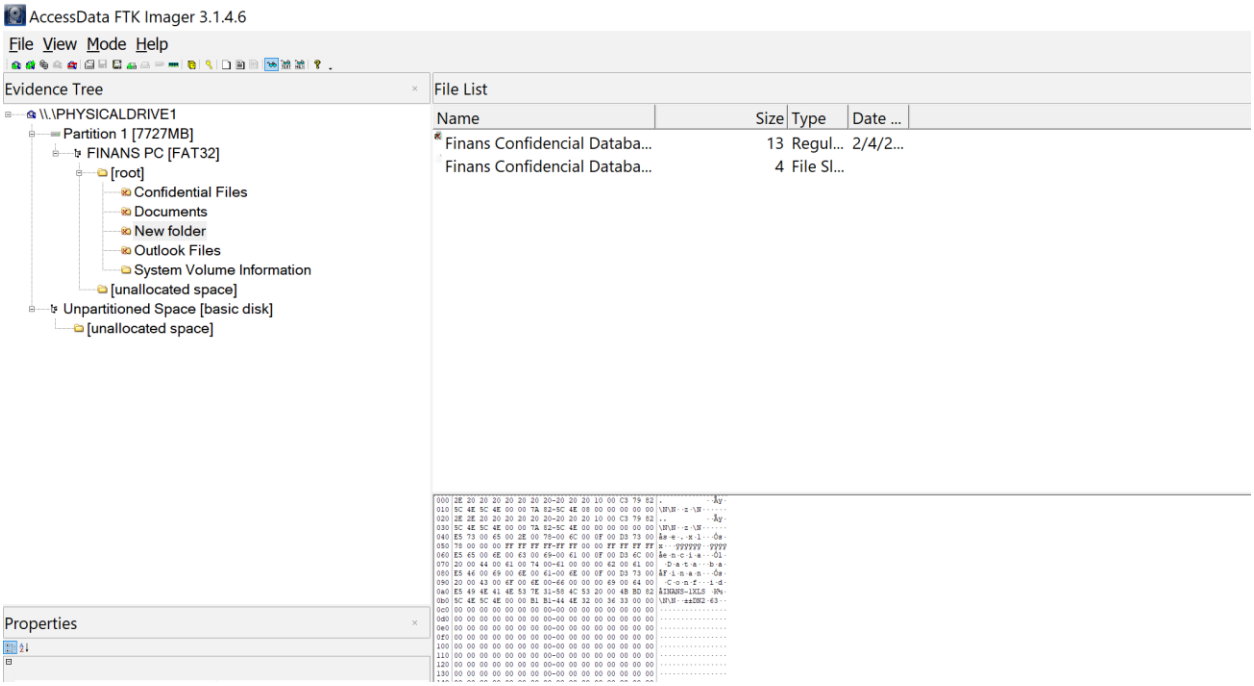


***Figura 6*- Documentos recuperados en la memoria del disco**

La Figura 7 muestra un documento pdf encontrado a través de FTK que enseña una conversación donde aparece el nombre de Leah Finan como emisaria y Danijel Glumac como destinatario. El correo indica que necesitan reunirse porque recibieron unos objetos de los "movimientos" usuales con Amazon. El mensaje añade que obtuvieron computadoras marca *Apple*, consolas *Xbox One* y relojes inteligentes Samsung. El emisor del correo indica que la ha sido difícil engañar a Amazon y que espera al menos 10,000 dólares por los objetos, finalizando con que Danijel Glumac se comunicara con Leah y Erin Finan.

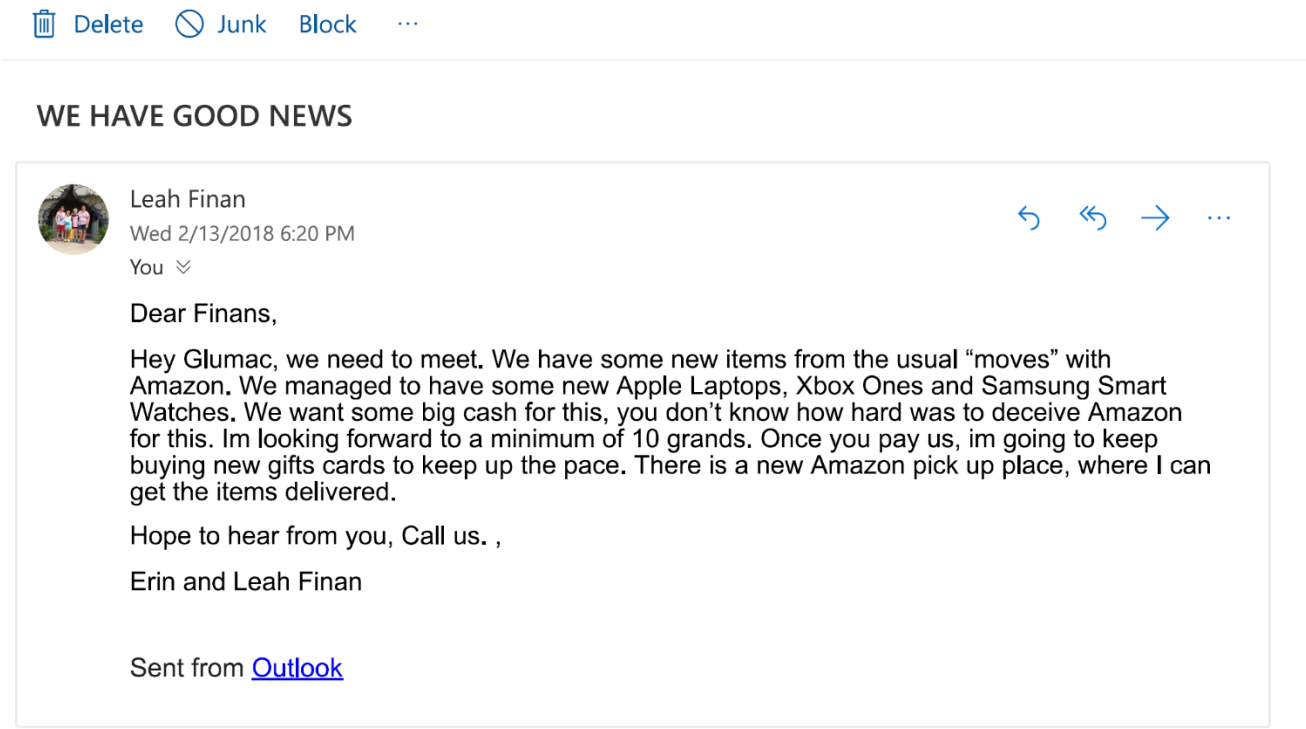


***Figura 7*- Correo electrónico de Leah Finan**

La Figura 8 muestra otra conversación encontrada a través de FTK donde Danijel Glumac menciona que logró vender los artículos que los Finans obtuvieron de Amazon, y que el negocio seguiría prosperando si continuaba recibiendo artículos de los Finans, para pagarles por medio de una compañía falsa con el fin de evadir las autoridades.

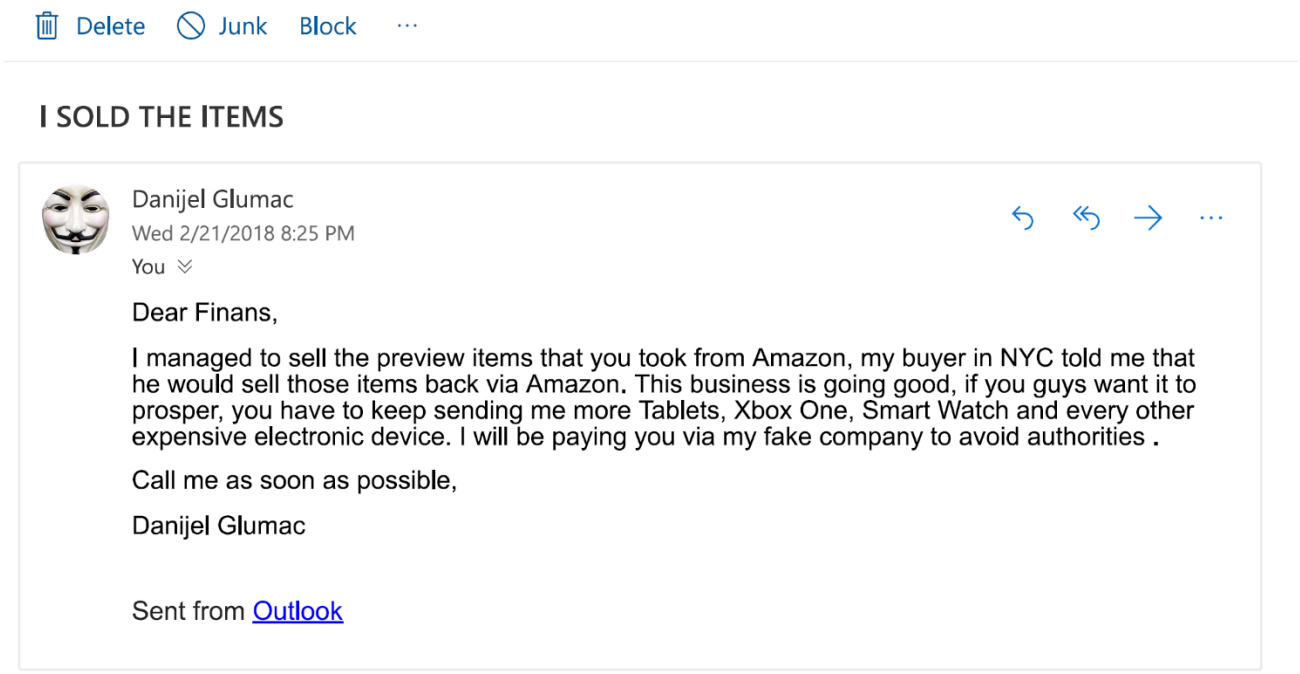
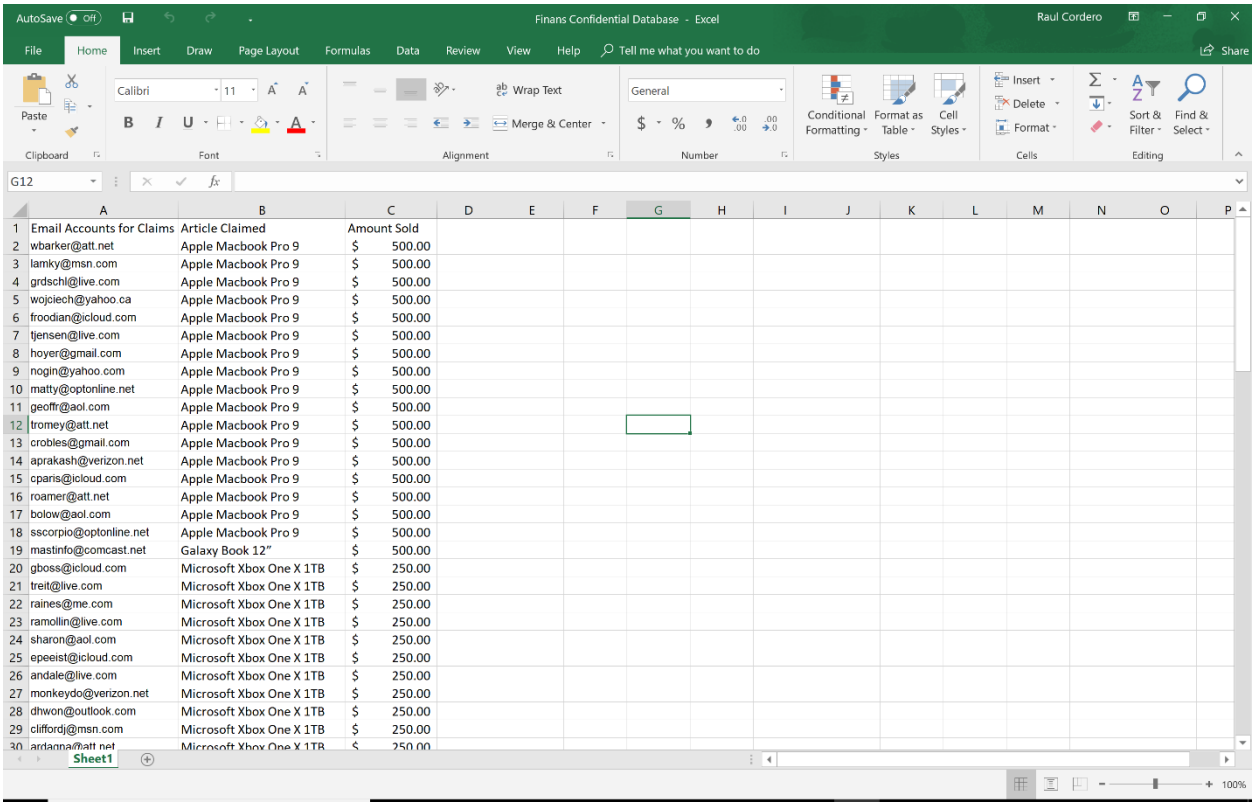


***Figura 8*- Correo electrónico de Danijel Glumac**

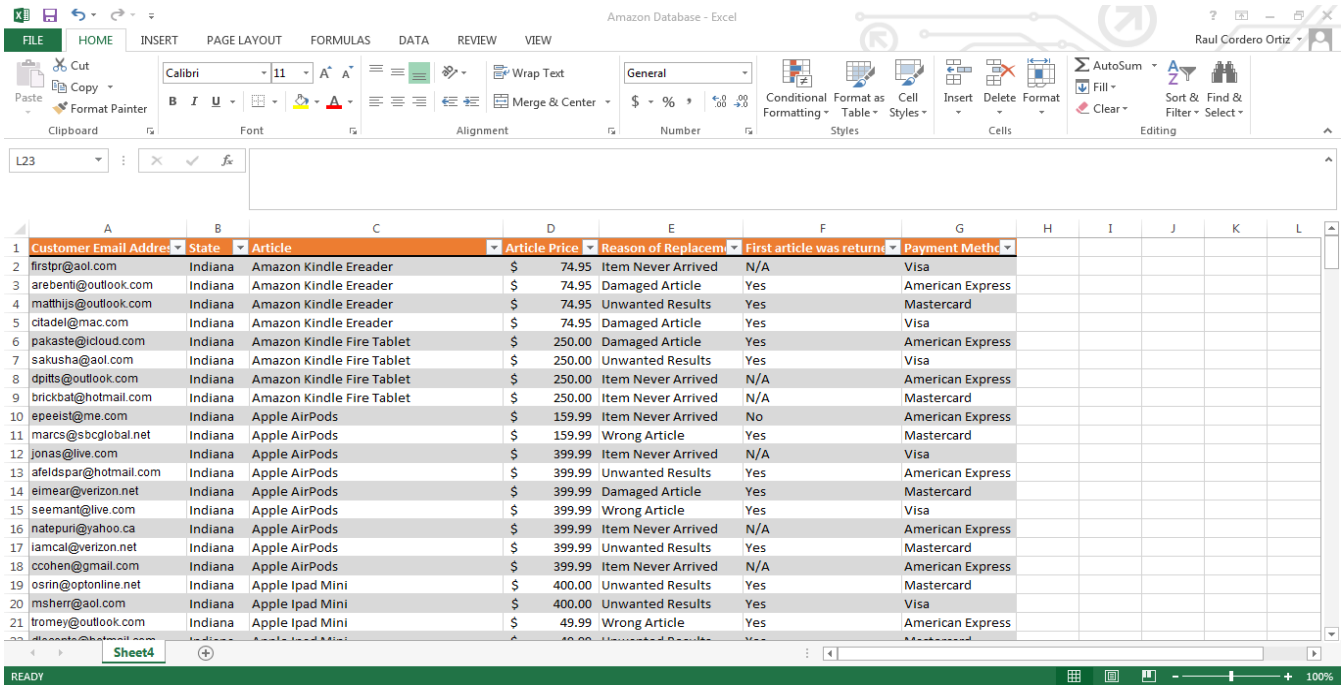
La Figura 9 muestra los detalles contenidos en el documento Excel titulado “Finans Confidential Database” donde se muestran tres columnas, una con múltiples cuentas de correo electrónico, artículos reclamados y la cantidad a la que fueron vendidos. Se entiende que esta información era mantenida por los Finans a manera de registro por los artículos reclamados fraudulentamente a Amazon.



	A	B	C
1	Email Accounts for Claims	Article Claimed	Amount Sold
2	wbarker@att.net	Apple Macbook Pro 9	$ 500.00
3	lamky@msn.com	Apple Macbook Pro 9	$ 500.00
4	grdschl@live.com	Apple Macbook Pro 9	$ 500.00
5	wojciech@yahoo.ca	Apple Macbook Pro 9	$ 500.00
6	froodian@icloud.com	Apple Macbook Pro 9	$ 500.00
7	tjensen@live.com	Apple Macbook Pro 9	$ 500.00
8	hoyer@gmail.com	Apple Macbook Pro 9	$ 500.00
9	nogin@yahoo.com	Apple Macbook Pro 9	$ 500.00
10	matty@optonline.net	Apple Macbook Pro 9	$ 500.00
11	geoffr@aol.com	Apple Macbook Pro 9	$ 500.00
12	tromey@att.net	Apple Macbook Pro 9	$ 500.00
13	crobles@gmail.com	Apple Macbook Pro 9	$ 500.00
14	aprakash@verizon.net	Apple Macbook Pro 9	$ 500.00
15	cparis@icloud.com	Apple Macbook Pro 9	$ 500.00
16	roamer@att.net	Apple Macbook Pro 9	$ 500.00
17	bolow@aol.com	Apple Macbook Pro 9	$ 500.00
18	sscorpio@optonline.net	Apple Macbook Pro 9	$ 500.00
19	mastinfo@comcast.net	Galaxy Book 12”	$ 500.00
20	gboss@icloud.com	Microsoft Xbox One X 1TB	$ 250.00
21	treit@live.com	Microsoft Xbox One X 1TB	$ 250.00
22	raines@me.com	Microsoft Xbox One X 1TB	$ 250.00
23	ramollin@live.com	Microsoft Xbox One X 1TB	$ 250.00
24	sharon@aol.com	Microsoft Xbox One X 1TB	$ 250.00
25	epeeist@icloud.com	Microsoft Xbox One X 1TB	$ 250.00
26	andale@live.com	Microsoft Xbox One X 1TB	$ 250.00
27	monkeydo@verizon.net	Microsoft Xbox One X 1TB	$ 250.00
28	dhwon@outlook.com	Microsoft Xbox One X 1TB	$ 250.00
29	cliffordj@msn.com	Microsoft Xbox One X 1TB	$ 250.00
30	ardagna@att.net	Microsoft Xbox One X 1TB	$ 250.00

***Figura 9*- Detalle de correos electrónicos y artículos reclamados**

2) A partir del análisis realizado con la herramienta CaseWare IDEA se comparó el archivo formato Excel con título “Finans Confidential Database” con el archivo provisto por los investigadores del gobierno de los Estados Unidos, donde Amazon desglosó las devoluciones y reemplazos brindados para artículos electrónicos de clientes del estado de Indiana durante el año 2018 (**ver Figura 10**). El análisis de las dos bases de datos arrojó resultados concluyentes donde se identificó que los artículos que Amazon.com reemplazó a clientes que pagaron con *gift cards* y que no devolvieron el primer artículo, el cual identificaron dañado, coincidieron en tu totalidad con los correos electrónicos encontrados en el documento “Finans Confidential Database” y los artículos reclamados asociados a estos. La Figura 11 y 12 muestran el resultado de la función “join” de IDEA donde se buscaron los datos que ambas bases tuvieran en común en las columnas “Customer Email Address” y “Article” en la base de datos provista por Amazon, junto a las columnas con título “Email Account for Claims” y la columna “Article Claimed” de la base incautada a los Finans.



	A	B	C	D	E	F	G
1	Customer Email Addres	State	Article	Article Price	Reason of Replacem	First article was returne	Payment Metho
2	firstpr@aol.com	Indiana	Amazon Kindle Ereader	$ 74.95	Item Never Arrived	N/A	Visa
3	arebenti@outlook.com	Indiana	Amazon Kindle Ereader	$ 74.95	Damaged Article	Yes	American Express
4	matthijs@outlook.com	Indiana	Amazon Kindle Ereader	$ 74.95	Unwanted Results	Yes	Mastercard
5	citadel@mac.com	Indiana	Amazon Kindle Ereader	$ 74.95	Damaged Article	Yes	Visa
6	pakaste@icloud.com	Indiana	Amazon Kindle Fire Tablet	$ 250.00	Damaged Article	Yes	American Express
7	sakusha@aol.com	Indiana	Amazon Kindle Fire Tablet	$ 250.00	Unwanted Results	Yes	Visa
8	dpitts@outlook.com	Indiana	Amazon Kindle Fire Tablet	$ 250.00	Item Never Arrived	N/A	American Express
9	brickbat@hotmail.com	Indiana	Amazon Kindle Fire Tablet	$ 250.00	Item Never Arrived	N/A	Mastercard
10	epeeist@me.com	Indiana	Apple AirPods	$ 159.99	Item Never Arrived	No	American Express
11	marcs@sbcglobal.net	Indiana	Apple AirPods	$ 159.99	Wrong Article	Yes	Mastercard
12	jonas@live.com	Indiana	Apple AirPods	$ 399.99	Item Never Arrived	N/A	Visa
13	afeldspar@hotmail.com	Indiana	Apple AirPods	$ 399.99	Unwanted Results	Yes	American Express
14	eimear@verizon.net	Indiana	Apple AirPods	$ 399.99	Damaged Article	Yes	Mastercard
15	seemant@live.com	Indiana	Apple AirPods	$ 399.99	Wrong Article	Yes	Visa
16	natepuri@yahoo.ca	Indiana	Apple AirPods	$ 399.99	Item Never Arrived	N/A	American Express
17	iamcal@verizon.net	Indiana	Apple AirPods	$ 399.99	Unwanted Results	Yes	Mastercard
18	ccohen@gmail.com	Indiana	Apple AirPods	$ 399.99	Item Never Arrived	N/A	American Express
19	osrin@optonline.net	Indiana	Apple Ipad Mini	$ 400.00	Unwanted Results	Yes	Mastercard
20	msherr@aol.com	Indiana	Apple Ipad Mini	$ 400.00	Unwanted Results	Yes	Visa
21	tromey@outlook.com	Indiana	Apple Ipad Mini	$ 49.99	Wrong Article	Yes	American Express

***Figura 10*- Base de datos provista por Amazon**

Rec #	CUSTOMER_EMAIL_ADDRES	ARTICLE	EMAIL_ACCOUNTS_FOR_CLAIMS	ARTICLE_CLAIMED
1	aprakash@verizon.net	Apple Macbook Pro 9	aprakash@verizon.net	Apple Macbook Pro 9
2	bolow@aol.com	Apple Macbook Pro 9	bolow@aol.com	Apple Macbook Pro 9
3	cparis@icloud.com	Apple Macbook Pro 9	cparis@icloud.com	Apple Macbook Pro 9
4	crobles@gmail.com	Apple Macbook Pro 9	crobles@gmail.com	Apple Macbook Pro 9
5	froodian@icloud.com	Apple Macbook Pro 9	froodian@icloud.com	Apple Macbook Pro 9
6	geoffr@aol.com	Apple Macbook Pro 9	geoffr@aol.com	Apple Macbook Pro 9
7	grdschl@live.com	Apple Macbook Pro 9	grdschl@live.com	Apple Macbook Pro 9
8	hoyer@gmail.com	Apple Macbook Pro 9	hoyer@gmail.com	Apple Macbook Pro 9
9	lamky@msn.com	Apple Macbook Pro 9	lamky@msn.com	Apple Macbook Pro 9
10	matty@optonline.net	Apple Macbook Pro 9	matty@optonline.net	Apple Macbook Pro 9
11	nogin@yahoo.com	Apple Macbook Pro 9	nogin@yahoo.com	Apple Macbook Pro 9
12	roamer@att.net	Apple Macbook Pro 9	roamer@att.net	Apple Macbook Pro 9
13	sscorpio@optonline.net	Apple Macbook Pro 9	sscorpio@optonline.net	Apple Macbook Pro 9
14	tjensen@live.com	Apple Macbook Pro 9	tjensen@live.com	Apple Macbook Pro 9
15	tromey@att.net	Apple Macbook Pro 9	tromey@att.net	Apple Macbook Pro 9
16	wbarker@att.net	Apple Macbook Pro 9	wbarker@att.net	Apple Macbook Pro 9
17	wojciech@yahoo.ca	Apple Macbook Pro 9	wojciech@yahoo.ca	Apple Macbook Pro 9
18	mastinfo@comcast.net	Galaxy Book 12"	mastinfo@comcast.net	Galaxy Book 12"
19	alfred@yahoo.com	Microsoft Xbox One X 1TB	alfred@yahoo.com	Microsoft Xbox One X 1TB
20	andale@att.net	Microsoft Xbox One X 1TB	andale@att.net	Microsoft Xbox One X 1TB
21	andale@live.com	Microsoft Xbox One X 1TB	andale@live.com	Microsoft Xbox One X 1TB
22	ardagna@att.net	Microsoft Xbox One X 1TB	ardagna@att.net	Microsoft Xbox One X 1TB
23	barjam@msn.com	Microsoft Xbox One X 1TB	barjam@msn.com	Microsoft Xbox One X 1TB
24	cliffordj@msn.com	Microsoft Xbox One X 1TB	cliffordj@msn.com	Microsoft Xbox One X 1TB
25	dhwon@me.com	Microsoft Xbox One X 1TB	dhwon@me.com	Microsoft Xbox One X 1TB
26	dhwon@outlook.com	Microsoft Xbox One X 1TB	dhwon@outlook.com	Microsoft Xbox One X 1TB
27	epeeist@icloud.com	Microsoft Xbox One X 1TB	epeeist@icloud.com	Microsoft Xbox One X 1TB
28	gboss@icloud.com	Microsoft Xbox One X 1TB	gboss@icloud.com	Microsoft Xbox One X 1TB
29	grossman@aol.com	Microsoft Xbox One X 1TB	grossman@aol.com	Microsoft Xbox One X 1TB
30	jelmer@verizon.net	Microsoft Xbox One X 1TB	jelmer@verizon.net	Microsoft Xbox One X 1TB
31	kwilliams@yahoo.com	Microsoft Xbox One X 1TB	kwilliams@yahoo.com	Microsoft Xbox One X 1TB
32	monkeydo@verizon.net	Microsoft Xbox One X 1TB	monkeydo@verizon.net	Microsoft Xbox One X 1TB
33	mschwartz@yahoo.com	Microsoft Xbox One X 1TB	mschwartz@yahoo.com	Microsoft Xbox One X 1TB
34	raines@me.com	Microsoft Xbox One X 1TB	raines@me.com	Microsoft Xbox One X 1TB
35	ramollin@live.com	Microsoft Xbox One X 1TB	ramollin@live.com	Microsoft Xbox One X 1TB
36	sharon@aol.com	Microsoft Xbox One X 1TB	sharon@aol.com	Microsoft Xbox One X 1TB
37	treit@live.com	Microsoft Xbox One X 1TB	treit@live.com	Microsoft Xbox One X 1TB
38	aaribaud@yahoo.ca	Samsung Galaxy Smartwatch	aaribaud@yahoo.ca	Samsung Galaxy Smartwatch
39	alfred@hotmail.com	Samsung Galaxy Smartwatch	alfred@hotmail.com	Samsung Galaxy Smartwatch
40	arebenti@aol.com	Samsung Galaxy Smartwatch	arebenti@aol.com	Samsung Galaxy Smartwatch
41	bmidd@yahoo.ca	Samsung Galaxy Smartwatch	bmidd@yahoo.ca	Samsung Galaxy Smartwatch
42	boftx@msn.com	Samsung Galaxy Smartwatch	boftx@msn.com	Samsung Galaxy Smartwatch
43	duchamp@hotmail.com	Samsung Galaxy Smartwatch	duchamp@hotmail.com	Samsung Galaxy Smartwatch
44	dunstan@live.com	Samsung Galaxy Smartwatch	dunstan@live.com	Samsung Galaxy Smartwatch
45	hyper@verizon.net	Samsung Galaxy Smartwatch	hyper@verizon.net	Samsung Galaxy Smartwatch
46	jmgomez@att.net	Samsung Galaxy Smartwatch	jmgomez@att.net	Samsung Galaxy Smartwatch
47	kimvette@sbcglobal.net	Samsung Galaxy Smartwatch	kimvette@sbcglobal.net	Samsung Galaxy Smartwatch
48	mstrout@optonline.net	Samsung Galaxy Smartwatch	mstrout@optonline.net	Samsung Galaxy Smartwatch
49	naoya@hotmail.com	Samsung Galaxy Smartwatch	naoya@hotmail.com	Samsung Galaxy Smartwatch
50	seanq@sbcglobal.net	Samsung Galaxy Smartwatch	seanq@sbcglobal.net	Samsung Galaxy Smartwatch
51	amaranth@sbcglobal.net	Windows Surface Book	amaranth@sbcglobal.net	Windows Surface Book
52	bebing@sbcglobal.net	Windows Surface Book	bebing@sbcglobal.net	Windows Surface Book
53	citizenl@optonline.net	Windows Surface Book	citizenl@optonline.net	Windows Surface Book
54	gavollink@me.com	Windows Surface Book	gavollink@me.com	Windows Surface Book
55	haddawy@live.com	Windows Surface Book	haddawy@live.com	Windows Surface Book
56	hstiles@aol.com	Windows Surface Book	hstiles@aol.com	Windows Surface Book
57	imightb@att.net	Windows Surface Book	imightb@att.net	Windows Surface Book

***Figura 11*- Resultado de la unión de las dos bases de datos**

58	isaacson@yahoo.ca	Windows Surface Book	isaacson@yahoo.ca	Windows Surface Book
59	kidehen@aol.com	Windows Surface Book	kidehen@aol.com	Windows Surface Book
60	kwilliams@msn.com	Windows Surface Book	kwilliams@msn.com	Windows Surface Book
61	melnik@yahoo.com	Windows Surface Book	melnik@yahoo.com	Windows Surface Book
62	mlewan@hotmail.com	Windows Surface Book	mlewan@hotmail.com	Windows Surface Book
63	neuffer@icloud.com	Windows Surface Book	neuffer@icloud.com	Windows Surface Book
64	ngedmond@me.com	Windows Surface Book	ngedmond@me.com	Windows Surface Book
65	nichoj@yahoo.ca	Windows Surface Book	nichoj@yahoo.ca	Windows Surface Book
66	pajas@gmail.com	Windows Surface Book	pajas@gmail.com	Windows Surface Book
67	ralamosm@live.com	Windows Surface Book	ralamosm@live.com	Windows Surface Book
68	rjones@outlook.com	Windows Surface Book	rjones@outlook.com	Windows Surface Book
69	seano@comcast.net	Windows Surface Book	seano@comcast.net	Windows Surface Book
70	telbij@optonline.net	Windows Surface Book	telbij@optonline.net	Windows Surface Book
71	tlinden@hotmail.com	Windows Surface Book	tlinden@hotmail.com	Windows Surface Book
72	ullman@optonline.net	Windows Surface Book	ullman@optonline.net	Windows Surface Book
73	willg@att.net	Windows Surface Book	willg@att.net	Windows Surface Book
74	amimojo@yahoo.com	Windows Surface Pro 4	amimojo@yahoo.com	Windows Surface Pro 4
75	bmorrow@live.com	Windows Surface Pro 4	bmorrow@live.com	Windows Surface Pro 4
76	dglumac@yahoo.com	Windows Surface Pro 4	dglumac@yahoo.com	Windows Surface Pro 4
77	efinan@hotmail.com	Windows Surface Pro 4	efinan@hotmail.com	Windows Surface Pro 4
78	finanskids13@msn.com	Windows Surface Pro 4	finanskids13@msn.com	Windows Surface Pro 4
79	happyfamilyfinans@yahoo.com	Windows Surface Pro 4	happyfamilyfinans@yahoo.com	Windows Surface Pro 4
80	hauma@hotmail.com	Windows Surface Pro 4	hauma@hotmail.com	Windows Surface Pro 4
81	iamcal@gmail.com	Windows Surface Pro 4	iamcal@gmail.com	Windows Surface Pro 4
82	johnbob@msn.com	Windows Surface Pro 4	johnbob@msn.com	Windows Surface Pro 4
83	lfinan@aol.com	Windows Surface Pro 4	lfinan@aol.com	Windows Surface Pro 4
84	magusnet@yahoo.com	Windows Surface Pro 4	magusnet@yahoo.com	Windows Surface Pro 4
85	mcast@msn.com	Windows Surface Pro 4	mcast@msn.com	Windows Surface Pro 4
86	mdielmann@yahoo.com	Windows Surface Pro 4	mdielmann@yahoo.com	Windows Surface Pro 4
87	moxfulder@icloud.com	Windows Surface Pro 4	moxfulder@icloud.com	Windows Surface Pro 4
88	nevermind@yahoo.com	Windows Surface Pro 4	nevermind@yahoo.com	Windows Surface Pro 4
89	podmaster@sbcglobal.net	Windows Surface Pro 4	podmaster@sbcglobal.net	Windows Surface Pro 4
90	squirrel@optonline.net	Windows Surface Pro 4	squirrel@optonline.net	Windows Surface Pro 4
91	suresh@yahoo.com	Windows Surface Pro 4	suresh@yahoo.com	Windows Surface Pro 4
92	tarreau@yahoo.ca	Windows Surface Pro 4	tarreau@yahoo.ca	Windows Surface Pro 4
93	thefinan@live.com	Windows Surface Pro 4	thefinan@live.com	Windows Surface Pro 4
94	thefraudster@gmail.com	Windows Surface Pro 4	thefraudster@gmail.com	Windows Surface Pro 4
95	ubergeeb@comcast.net	Windows Surface Pro 4	ubergeeb@comcast.net	Windows Surface Pro 4
96	william@verizon.net	Windows Surface Pro 4	william@verizon.net	Windows Surface Pro 4

***Figura 12*-Continuación de los resultados obtenidos**

Cadena de Custodia

La fiscalía federal, los investigadores del caso, y el examinador forense digital, Raúl Cordero, llevaron a cabo los protocolos y las practicas esperadas para el manejo de evidencia. A continuación, se describe la cadena de custodia, que relata el manejo de la información obtenida del caso y la interacción entre los investigadores del caso y examinador forense.

1. **Primer Evento:**
    a. Descripción del Evento: Evidencia entregada por ayudante especial del fiscal John Minkler, y recibida por Raúl Cordero, investigador forense digital. La evidencia recibida fue un disco duro de 1Tb de memoria, marca *WD My Passport* con número de serie WX31A87C9HJI. El disco está identificado con el número de evidencia E1- 2018-13-USSDI. Tambien se recibió el USB Flash Drive, marca PNY de 8gb con tag de evidencia E2- 2018-13-USSDI.
    b. Evento verificado por: Raúl Cordero, investigador y ayudante especial del fiscal
    c. Fecha de comienzo: 26 de febrero de 2019 9:00 am
    d. Fecha de terminación: 26 de febrero de 2019 9:30 am
    e. Lugar de origen: Laboratorio Forense Digital, Departamento de Justicia Federal
    f. Destino: Oficina de investigaciones cibernéticas de Raúl Cordero, investigador forense digital
2. **Segundo evento:**
    a. Descripción del evento: Creación de numero de caso y asignación
    b. Evento tramitado por: Raúl Cordero, investigador forense digital.

c. Se asignó el número de caso: IFD-2018-13-USSDI

d. Fecha de comienzo: 26 de febrero de 2019 1:00 pm

e. Fecha de terminación: 26 de febrero de 2019 1:10 pm

f. Lugar de origen: Oficina de investigaciones cibernéticas de Raúl Cordero, investigador forense digital

g. Destino: Oficina de investigaciones cibernéticas de Raúl Cordero, investigador forense digital

3. **Tercer evento:**

a. Descripción del evento: realización de análisis a la imagen identificada como Disco Incautado Finans PC extraída del disco identificado con el número de evidencia E1- 2018-13-USSDI. Se utilizó FTK Imager y CaseWare IDEA para el análisis

b. Evento tramitado por: Raúl Cordero, investigador forense digital

c. Trabajo realizado bajo número de caso: IFD-2018-13-USSDI

d. Fecha de comienzo: 26 de febrero de 2019 1:15 pm

e. Fecha de terminación: 26 de febrero de 2019 9:30 pm

f. Lugar de origen: Oficina de investigaciones cibernéticas de Raúl Cordero, investigador forense digital

g. Destino: Oficina de investigaciones cibernéticas de Raúl Cordero, investigador forense digital

4. **Cuarto evento:**

a. Descripción del evento: entrega del disco duro de 1Tb identificado como E1-2018-13-USSDI, a John Minkler fiscal asistente del distrito sur de Indiana.

También se entregó el informe pericial del caso identificado bajo el número IFD-2018-13-USSDI.

b. Evento tramitado por: Raúl Cordero, investigador forense digital y John Minkler fiscal asistente del distrito sur de Indiana.

c. Número de caso: IFD-2018-13-USSDI

d. Fecha de comienzo: 27 de febrero de 2019 3:00 pm

e. Fecha de terminación: 27 de febrero de 2019 3:15 pm

f. Lugar de origen: Laboratorio Forense Digital, Departamento de Justicia Federal

g. Destino: Laboratorio Forense Digital, Departamento de Justicia Federal

Procedimiento

El quehacer investigativo de los investigadores forense digital, requiere el uso de metodologías y estrategias de investigación que permitan comprender los datos analizados y su procedencia. “Las funciones principales de la investigación forense digital son: recuperar datas escondidos y borrados, recuperar información de acceso, determinar cuáles herramientas fueron utilizadas por el atacante, recopilar evidencia para construir un caso” (Cowen, 2013, págs. 11-12).

A continuación se describe el proceso llevado a cabo para examinar los datos del disco provisto por fiscalia, y la metodología utilizada. Es importante comprender que en el tipo de investigaciones solicitadas para los tribunales requieren confidencialidad y que se sigan las solicitudes de fiscalía para extraer los datos necesarios (Bradley & Garfinkel, 2015).

1. Procedimiento: Preparación para análisis de imagen de disco nombrado como Finans FTK, del disco duro etiquetado como E1- 2018-13-USSDI.
    a. Herramienta: Access Data FTK Imager
    b. Fecha de comienzo: 26 de febrero de 2019 3:15 pm
    c. Fecha de terminación: 26 de febrero de 2019 3:25 pm

La Figura 13 menú principal de FTK Image y pestaña color verde para añadir nueva evidencia.

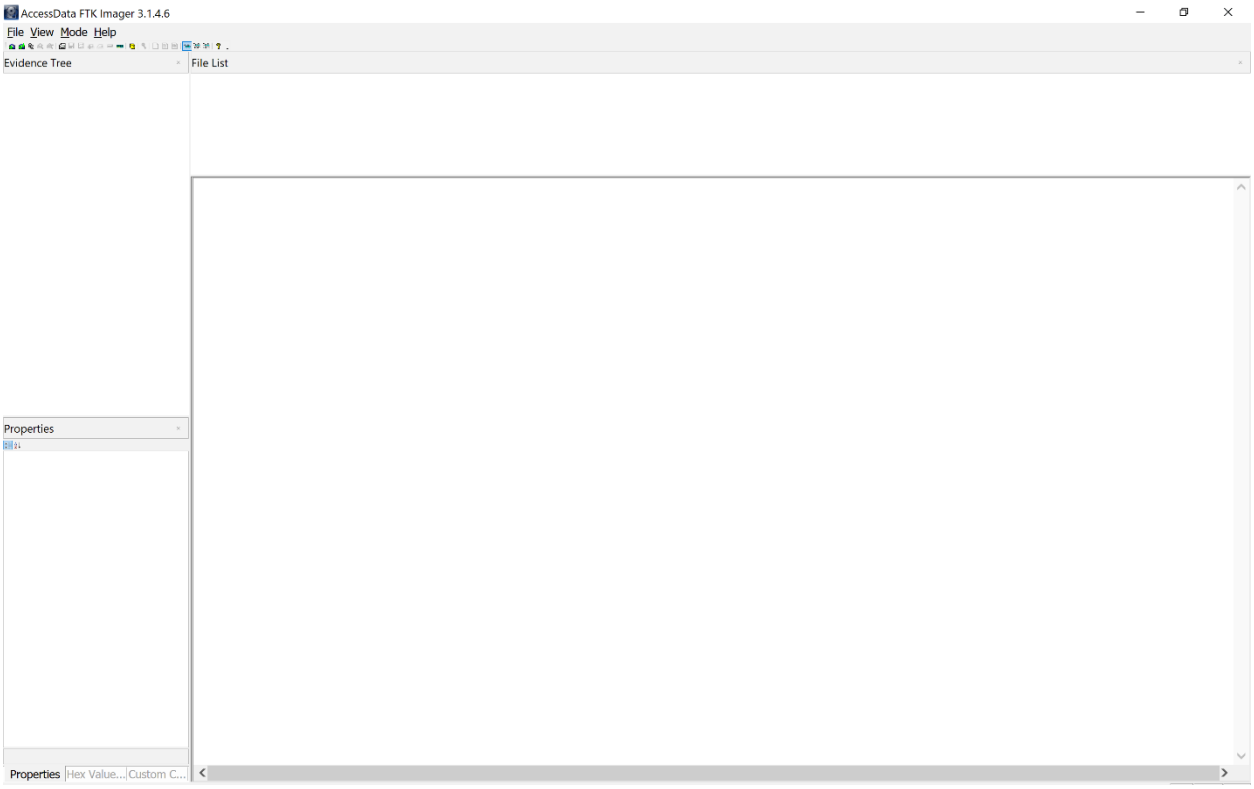


Figura 13*- Menú principal de *FTK Imager

La figura 14 muestra el momento en que se escoge el tipo de evidencia a investigar, se escogió evidencia en un dispositivo físico por tratarse de un disco duro.

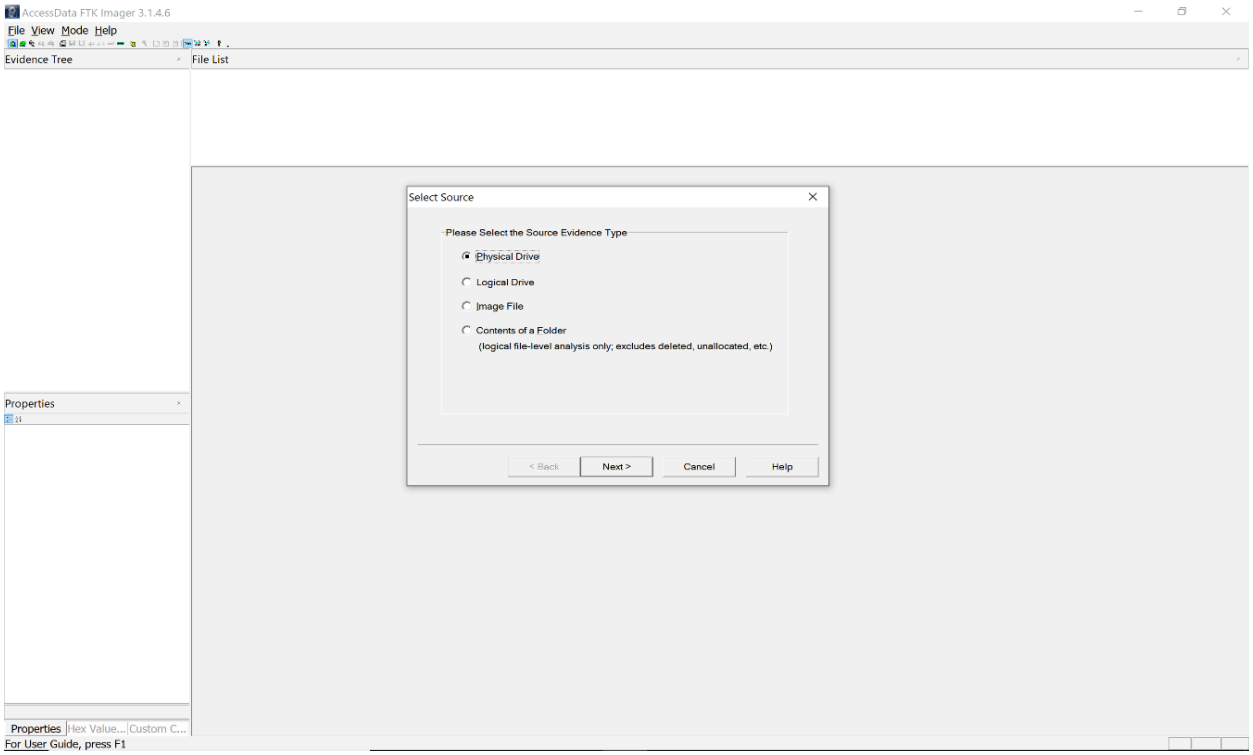


***Figura 14*-Se añade evidencia física**

d. Descripción del Resultado: Se accedió a la herramienta FTK Imager para el análisis de la Imagen Disco E1-2018-12-USSDI, creada para la inspección de los datos. Luego se procedió a añadir la evidencia y se selecciona la fuente de los datos que en este caso es un dispositivo físico de memoria, véase **Figura 14**. Se muestra en la **Figura 15** muestra cuando se logró el acceso al disco.

La Figura 15 muestra el momento en que se logra acceso a los datos contenidos en el disco duro usado la herramienta FTK Imager.

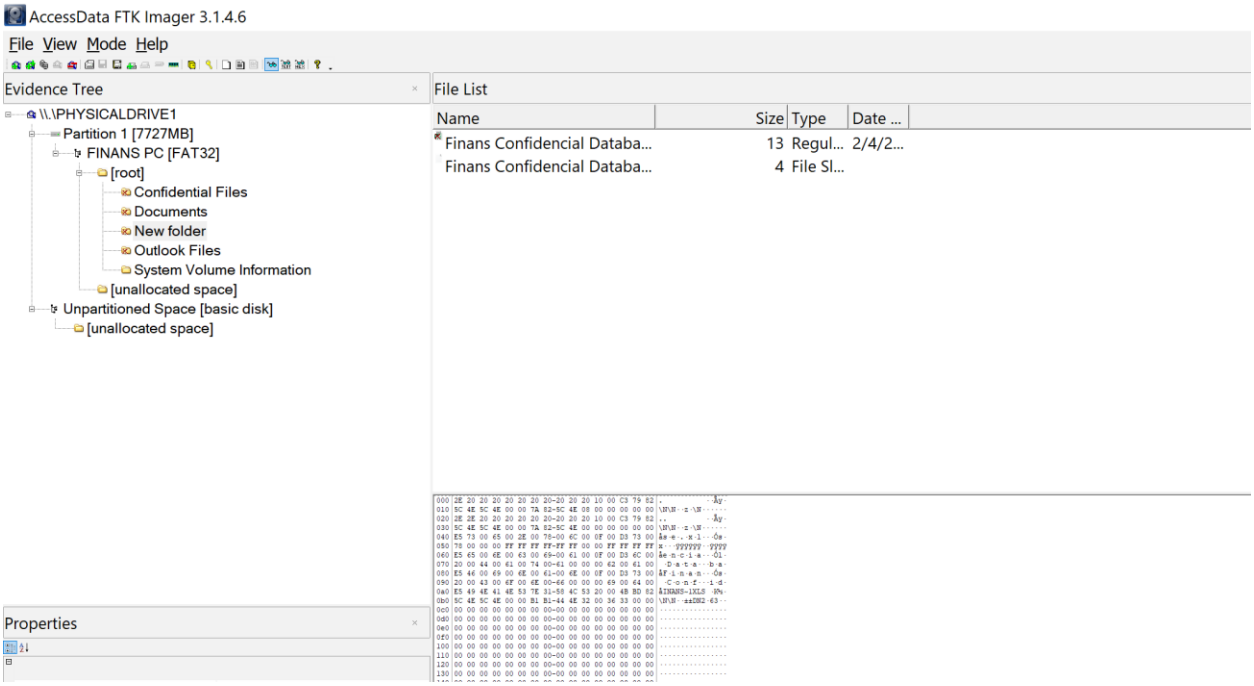


***Figura 15*-Acceso al disco y a sus datos**

2. Procedimiento: Análisis de imagen de disco nombrado como E1-2018-13-USSDI.
    a. Herramienta: Access Data FTK Imager
    b. Fecha de comienzo: 26 de febrero de 2019 3:25 pm
    c. Fecha de terminación: 26 de febrero de 2019 4:00 pm

d. Descripción del resultado: Se encontraron carpetas de datos contenidos en la imagen del disco, (**véase Figura 15**) descubriendo varios archivos en las carpetas “Confidential Files” y “Outlook Files”.

3. Procedimiento: Examen de archivos en la carpeta “Outlook Files”.

   a. Herramienta: Access Data FTK Imager

   b. Fecha de comienzo: 26 de febrero de 2019 2:02 pm

   c. Fecha de terminación: 26 de febrero de 2019 3:40 pm

   d. Descripción: Se observaron los archivos, identificándose 3 documentos, dos formatos pdf y uno formato Excel. Los archivos pdf muestran conversaciones via correo electrónico donde se mencionan elementos relacionados a las acusaciones realizadas por las autoridades (**véase Figura 16 y 17**). El archivo Excel muestra un inventario de correos electrónicos, artículos reclamados y precio de venta de los mismos.

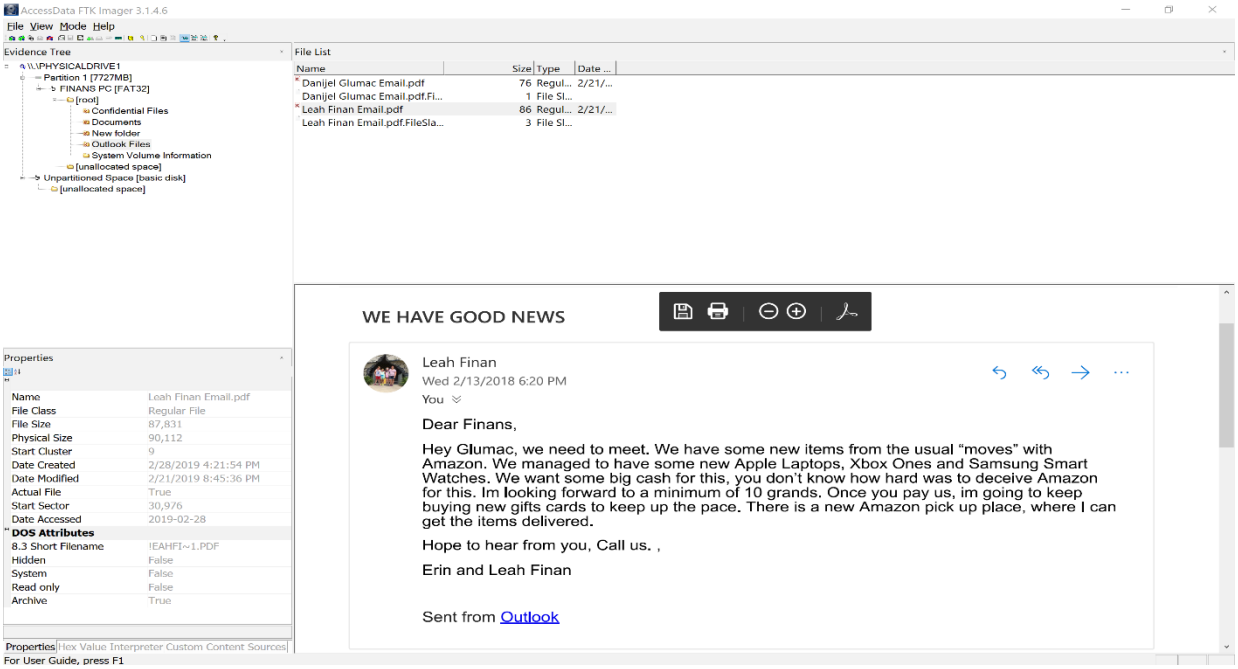


***Figura 16*- Correo electrónico encontrado de los Finans**

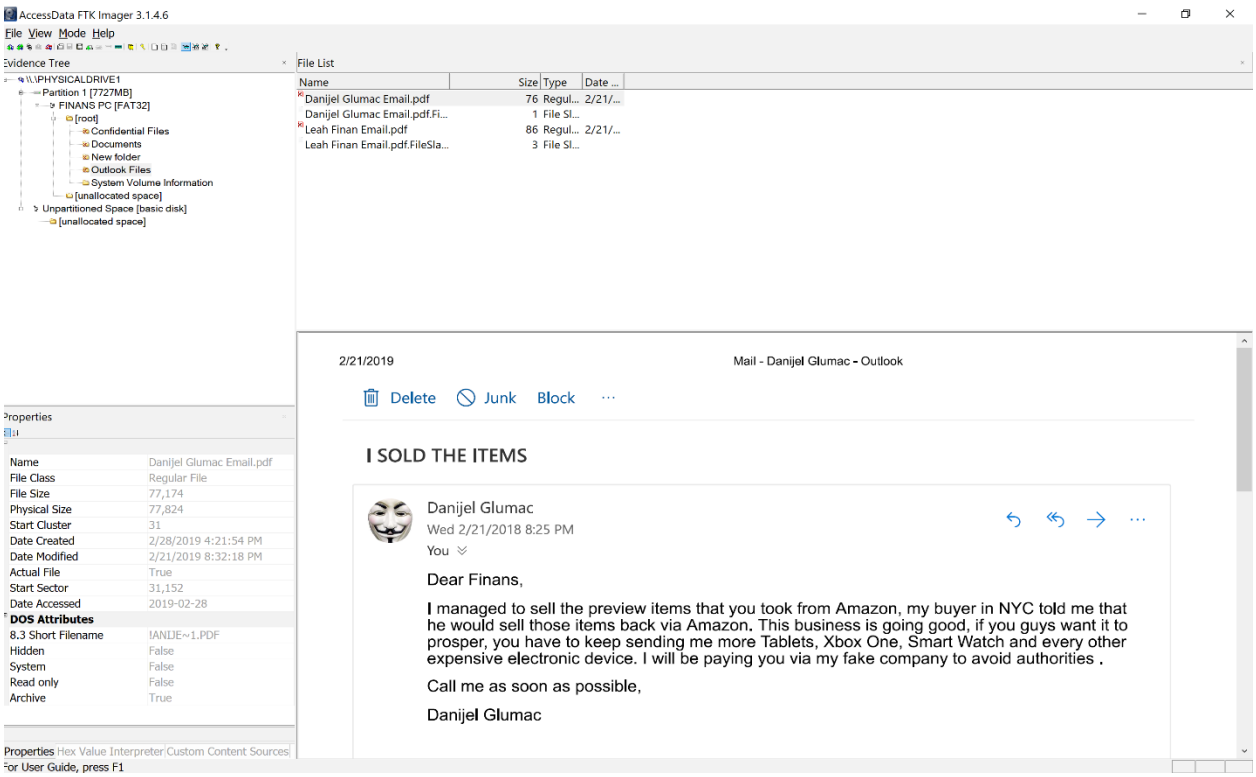
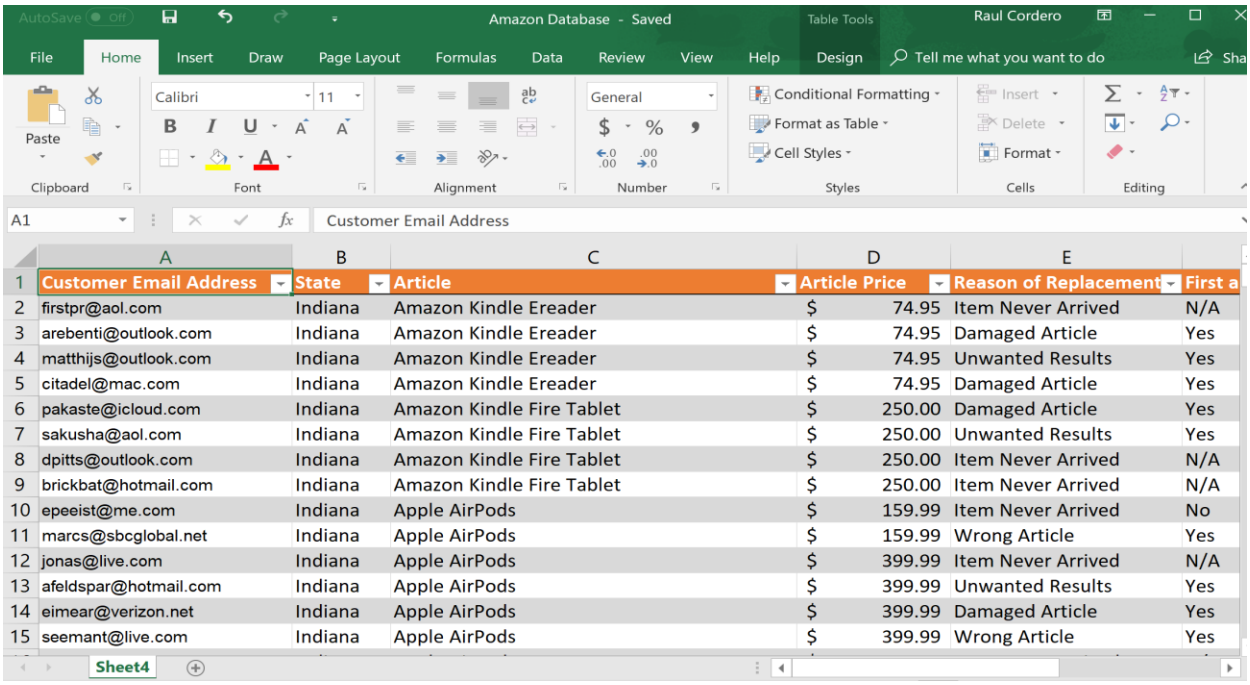


***Figura 17*- Correo electrónico encontrado de Danijel Glumac**



	A	B	C	D	E	
1	Customer Email Address	State	Article	Article Price	Reason of Replacement	First a
2	firstpr@aol.com	Indiana	Amazon Kindle Ereader	$ 74.95	Item Never Arrived	N/A
3	arebenti@outlook.com	Indiana	Amazon Kindle Ereader	$ 74.95	Damaged Article	Yes
4	matthijs@outlook.com	Indiana	Amazon Kindle Ereader	$ 74.95	Unwanted Results	Yes
5	citadel@mac.com	Indiana	Amazon Kindle Ereader	$ 74.95	Damaged Article	Yes
6	pakaste@icloud.com	Indiana	Amazon Kindle Fire Tablet	$ 250.00	Damaged Article	Yes
7	sakusha@aol.com	Indiana	Amazon Kindle Fire Tablet	$ 250.00	Unwanted Results	Yes
8	dpitts@outlook.com	Indiana	Amazon Kindle Fire Tablet	$ 250.00	Item Never Arrived	N/A
9	brickbat@hotmail.com	Indiana	Amazon Kindle Fire Tablet	$ 250.00	Item Never Arrived	N/A
10	epeeist@me.com	Indiana	Apple AirPods	$ 159.99	Item Never Arrived	No
11	marcs@sbcglobal.net	Indiana	Apple AirPods	$ 159.99	Wrong Article	Yes
12	jonas@live.com	Indiana	Apple AirPods	$ 399.99	Item Never Arrived	N/A
13	afeldspar@hotmail.com	Indiana	Apple AirPods	$ 399.99	Unwanted Results	Yes
14	eimear@verizon.net	Indiana	Apple AirPods	$ 399.99	Damaged Article	Yes
15	seemant@live.com	Indiana	Apple AirPods	$ 399.99	Wrong Article	Yes

***Figura 18*- Base de datos formato Excel obtenida**

4. Procedimiento: Preparación para análisis de las dos bases de datos formato Excel recuperadas a través de FTK Imager.
    a. Herramienta: CaseWare IDEA
    b. Fecha de comienzo: 26 de febrero de 2019 4:00 pm
    c. Fecha de terminación: 26 de febrero de 2019 4:20 pm
    d. Descripción: Se accedió a la herramienta CaseWare IDEA para analizar las dos bases de datos obtenidas y ver si estas se relacionan.

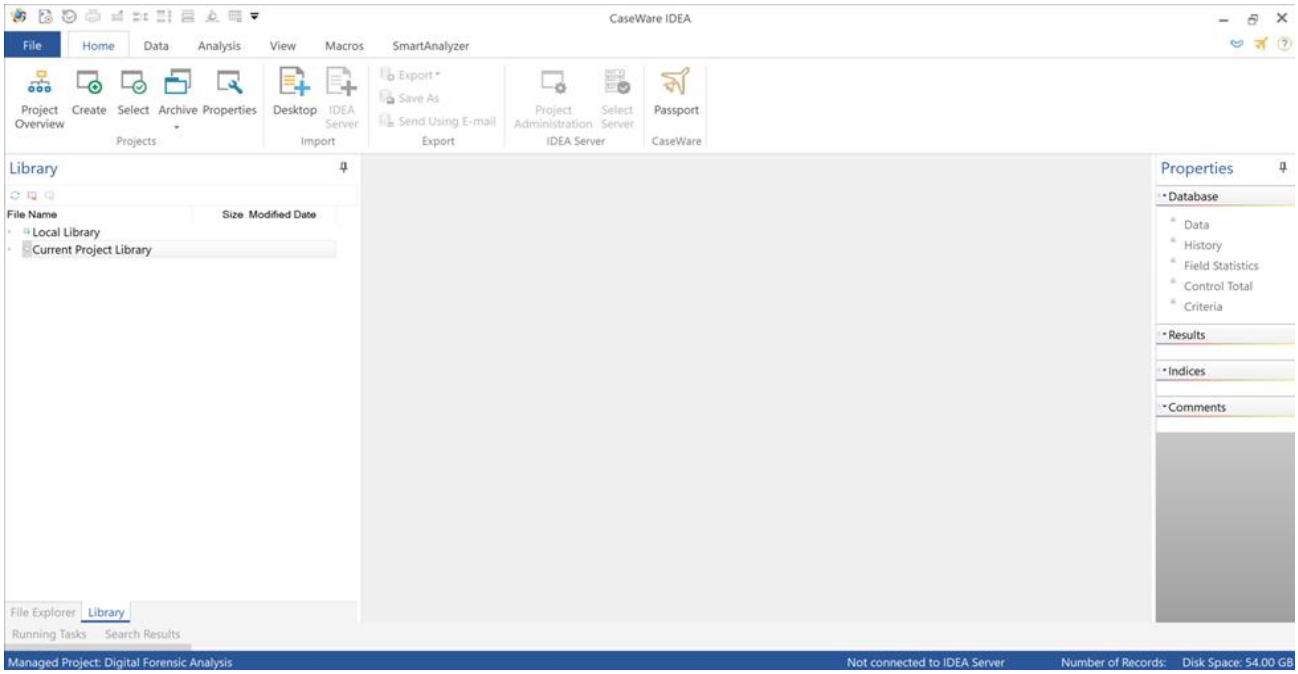


Figura 19- Menú principal de CaseWare IDEA

5. Procedimiento: Crear Proyecto para realizar la auditoria forense digital. Se creó el proyecto “Digital Forensic US vs Finans-Glumac”.
    a. Herramienta: CaseWare IDEA
    b. Fecha de comienzo: 26 de febrero de 2019 4:20 pm
    c. Fecha de terminación: 26 de febrero de 2019 4:25 pm

d. Descripción: Se escogió la opción “Create” y se colocó el nombre “Digital Forensics US vs Finans- Glumac” (**ver Figura 20**). Una vez creado el proyecto se importó la base de datos provista por Amazon en formato Excel, a través de la función “Desktop” (**ver Figura 21 y 22**).

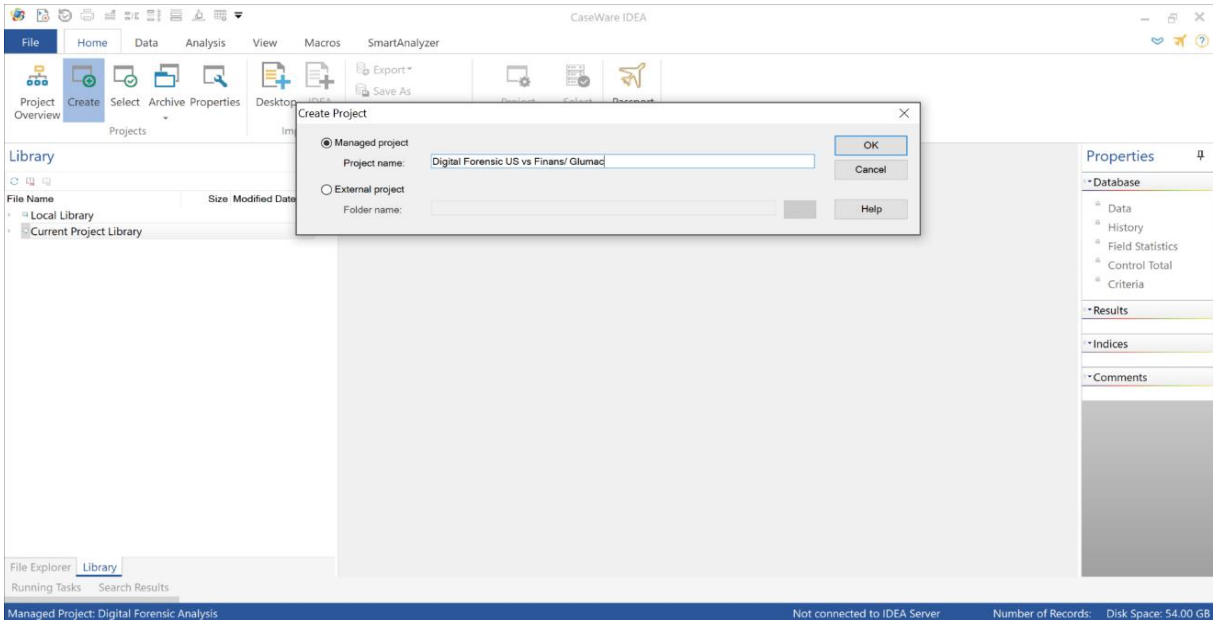


***Figura 20*- Creación de Proyecto en IDEA**

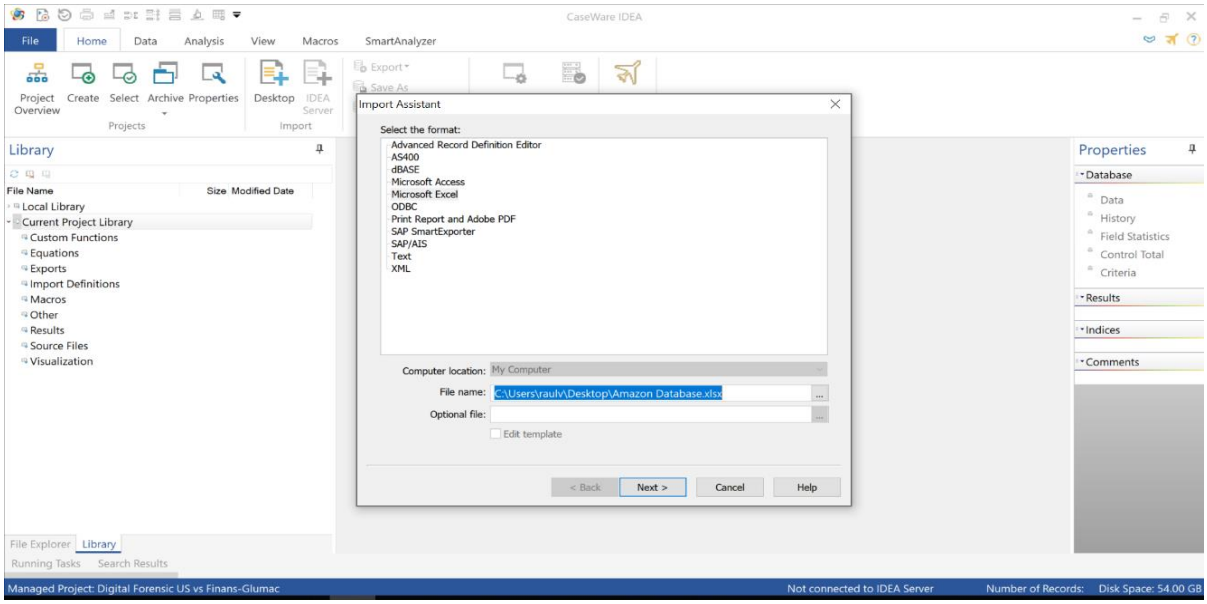
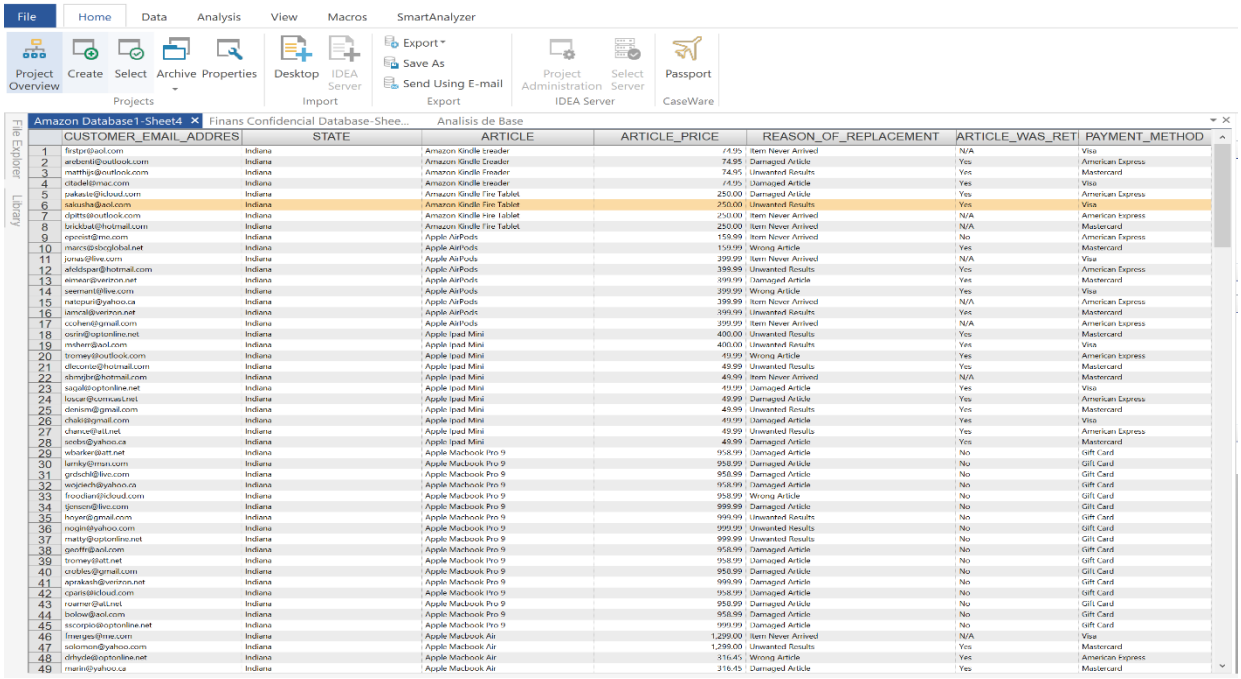


***Figura 21*- Importe de Base de Datos**



	CUSTOMER_EMAIL_ADDRES	STATE	ARTICLE	ARTICLE_PRICE	REASON_OF_REPLACEMENT	ARTICLE_WAS_RET	PAYMENT_METHOD
1	firstyr@aol.com	Indiana	Amazon Kindle Ereader	74.95	Item Never Arrived	N/A	Visa
2	arebenti@outlook.com	Indiana	Amazon Kindle Ereader	74.95	Damaged Article	Yes	American Express
3	matthjs@outlook.com	Indiana	Amazon Kindle Ereader	74.95	Unwanted Results	Yes	Mastercard
4	citadel@mac.com	Indiana	Amazon Kindle Ereader	74.95	Damaged Article	Yes	Visa
5	oakasle@icloud.com	Indiana	Amazon Kindle Fire Tablet	250.00	Damaged Article	Yes	American Express
6	saiusha@aol.com	Indiana	Amazon Kindle Fire Tablet	250.00	Unwanted Results	Yes	Visa
7	dpitts@outlook.com	Indiana	Amazon Kindle Fire Tablet	250.00	Item Never Arrived	N/A	American Express
8	brickbat@hotmail.com	Indiana	Amazon Kindle Fire Tablet	250.00	Item Never Arrived	N/A	Mastercard
9	eperint@me.com	Indiana	Apple AirPods	159.99	Item Never Arrived	No	American Express
10	marcs@sbcglobal.net	Indiana	Apple AirPods	159.99	Wrong Article	Yes	Mastercard
11	jonas@live.com	Indiana	Apple AirPods	399.99	Item Never Arrived	N/A	Visa
12	afeldspar@hotmail.com	Indiana	Apple AirPods	399.99	Unwanted Results	Yes	American Express
13	eimear@verizon.net	Indiana	Apple AirPods	399.99	Damaged Article	Yes	Mastercard
14	seemant@live.com	Indiana	Apple AirPods	399.99	Wrong Article	Yes	Visa
15	natepuri@yahoo.ca	Indiana	Apple AirPods	399.99	Item Never Arrived	N/A	American Express
16	jamcal@verizon.net	Indiana	Apple AirPods	399.99	Unwanted Results	Yes	Mastercard
17	ccohen@gmail.com	Indiana	Apple AirPods	399.99	Item Never Arrived	N/A	American Express
18	osiris@optonline.net	Indiana	Apple Ipad Mini	400.00	Unwanted Results	Yes	Mastercard
19	msherr@aol.com	Indiana	Apple Ipad Mini	400.00	Unwanted Results	Yes	Visa
20	tromey@outlook.com	Indiana	Apple Ipad Mini	49.99	Wrong Article	Yes	American Express
21	dlcorrie@hotmail.com	Indiana	Apple Ipad Mini	49.99	Unwanted Results	Yes	Mastercard
22	sbmejhr@hotmail.com	Indiana	Apple Ipad Mini	49.99	Item Never Arrived	N/A	Mastercard
23	saqalt@optonline.net	Indiana	Apple Ipad Mini	49.99	Damaged Article	Yes	Visa
24	loscar@comcast.net	Indiana	Apple Ipad Mini	49.99	Damaged Article	Yes	American Express
25	denism@gmail.com	Indiana	Apple Ipad Mini	49.99	Unwanted Results	Yes	Mastercard
26	chaki@gmail.com	Indiana	Apple Ipad Mini	49.99	Damaged Article	Yes	Visa
27	chance@att.net	Indiana	Apple Ipad Mini	49.99	Unwanted Results	Yes	American Express
28	seebs@yahoo.ca	Indiana	Apple Ipad Mini	49.99	Damaged Article	Yes	Mastercard
29	wbarker@att.net	Indiana	Apple Macbook Pro 9	958.99	Damaged Article	No	Gift Card
30	lamky@msn.com	Indiana	Apple Macbook Pro 9	958.99	Damaged Article	No	Gift Card
31	grdschl@live.com	Indiana	Apple Macbook Pro 9	958.99	Damaged Article	No	Gift Card
32	wojciech@yahoo.ca	Indiana	Apple Macbook Pro 9	958.99	Damaged Article	No	Gift Card
33	froodian@icloud.com	Indiana	Apple Macbook Pro 9	958.99	Wrong Article	No	Gift Card
34	tjensen@live.com	Indiana	Apple Macbook Pro 9	999.99	Damaged Article	No	Gift Card
35	hoyer@gmail.com	Indiana	Apple Macbook Pro 9	999.99	Unwanted Results	No	Gift Card
36	nojim@yahoo.com	Indiana	Apple Macbook Pro 9	999.99	Unwanted Results	No	Gift Card
37	matty@optonline.net	Indiana	Apple Macbook Pro 9	999.99	Unwanted Results	No	Gift Card
38	geoffr@aol.com	Indiana	Apple Macbook Pro 9	958.99	Damaged Article	No	Gift Card
39	tromey@att.net	Indiana	Apple Macbook Pro 9	958.99	Damaged Article	No	Gift Card
40	crubles@gmail.com	Indiana	Apple Macbook Pro 9	958.99	Damaged Article	No	Gift Card
41	aprakash@verizon.net	Indiana	Apple Macbook Pro 9	999.99	Damaged Article	No	Gift Card
42	cparis@icloud.com	Indiana	Apple Macbook Pro 9	958.99	Damaged Article	No	Gift Card
43	roumer@att.net	Indiana	Apple Macbook Pro 9	958.99	Damaged Article	No	Gift Card
44	bolow@aol.com	Indiana	Apple Macbook Pro 9	958.99	Damaged Article	No	Gift Card
45	escorpio@optonline.net	Indiana	Apple Macbook Pro 9	999.99	Damaged Article	No	Gift Card
46	fmerges@me.com	Indiana	Apple Macbook Air	1,299.00	Item Never Arrived	N/A	Visa
47	solomon@yahoo.com	Indiana	Apple Macbook Air	1,299.00	Unwanted Results	Yes	Mastercard
48	drhyde@optonline.net	Indiana	Apple Macbook Air	316.45	Wrong Article	Yes	American Express
49	marin@yahoo.ca	Indiana	Apple Macbook Air	316.45	Damaged Article	Yes	Mastercard

***Figura 22*- Base de datos de Amazon importada**

6. Procedimiento: Realizar importación de base de datos incautada a través del análisis con FTK. Comparar base importada con la información obtenida de los Finans para identificar los campos que tengan la misma información en ambos reportes.
    a. Herramienta: CaseWare IDEA
    b. Fecha de comienzo: 26 de febrero de 2019 4:25 pm
    c. Fecha de terminación: 26 de febrero de 2019 4:45 pm
    d. Descripción: Luego de importada la primera base, se procedió a importar la segunda para entonces realizar la función “Join” con el fin de comparar los campos que tienen los mismos datos. (Ver Figura 23, 24 y 25)

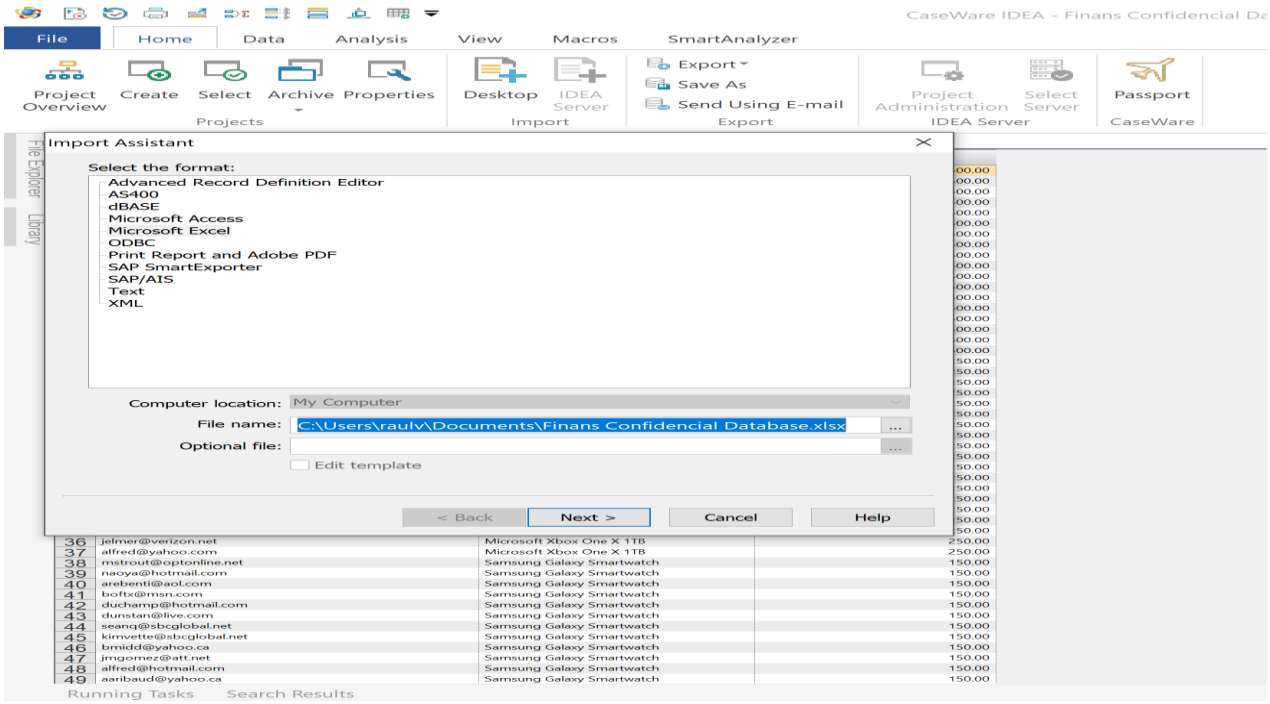


***Figura 23*- Importación del documento Excel**

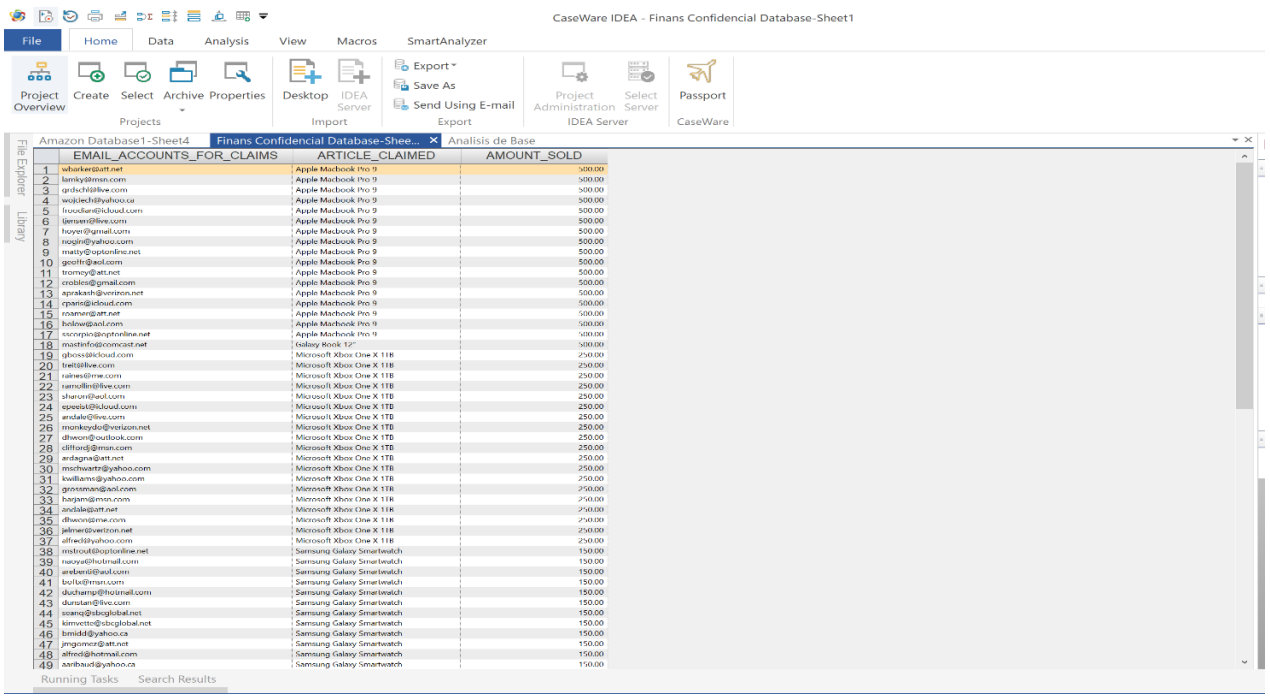


***Figura 24*- Base de datos recuperada de los Finans**

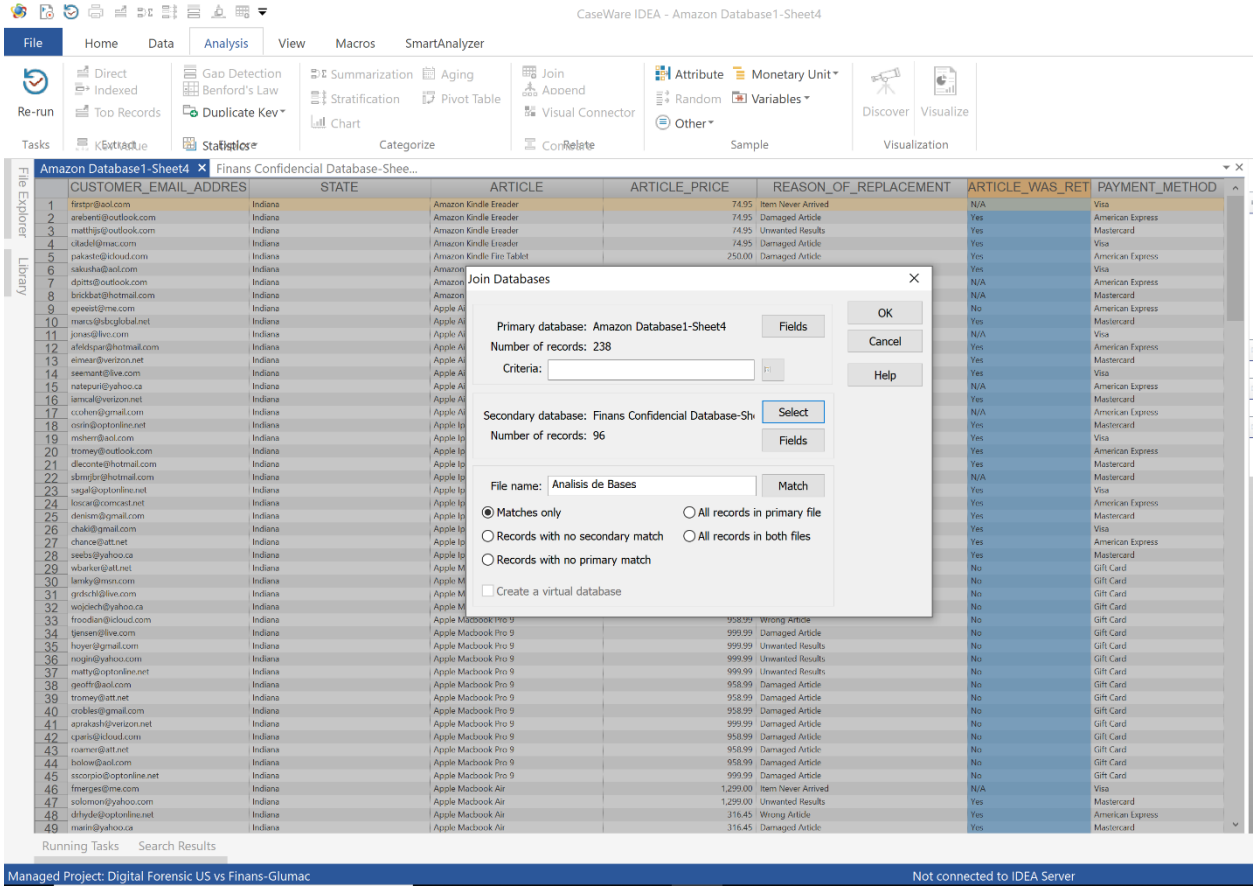


***Figura 25*- Aplicación de los criterios para "Join"**

7. Procedimiento: Completar la unión de las dos bases de datos a través de la función "Join" para el análisis de la información encontrada. Se establecieron los criterios de para unir las dos bases y destacar los campos que tienen la misma información en ambos documentos.

    e. Herramienta: CaseWare IDEA

    f. Fecha de comienzo: 26 de febrero de 2019 4:45 pm

    g. Fecha de terminación: 26 de febrero de 2019 5:10 pm

    h. Descripción: Se procedió a seleccionar la función "Join". Estableciendo que se muestren los resultados que coinciden. Se seleccionaron en la base de

datos provista por Amazon, las columnas “Customer Email Address” y “Article” para compararla con las columnas “Email Accounts for Claims” y “Article Claimed” con el fin de ver si esos artículos que Amazon, identificó como reclamados pero que no devolvieron el articulo original, tenían que ver con los Finans, como se entiende. En la Figura 27 se contemplan los resultados que arrojó el unir las dos bases, donde se encontraron 96 resultados. (Ver Figura 26 y 27).

La Figura 26 muestra los criterios utilizados para unir las dos bases, donde se interrogó la base para que brindará resultados equivalentes en las columnas “Customer Email Address” de Amazon y “Email Accounts for Claims” de los Finans. Se unieron también la columna de “Article” y “Article Claimed”, de las bases de Amazon y de los Finans, respectivamente.

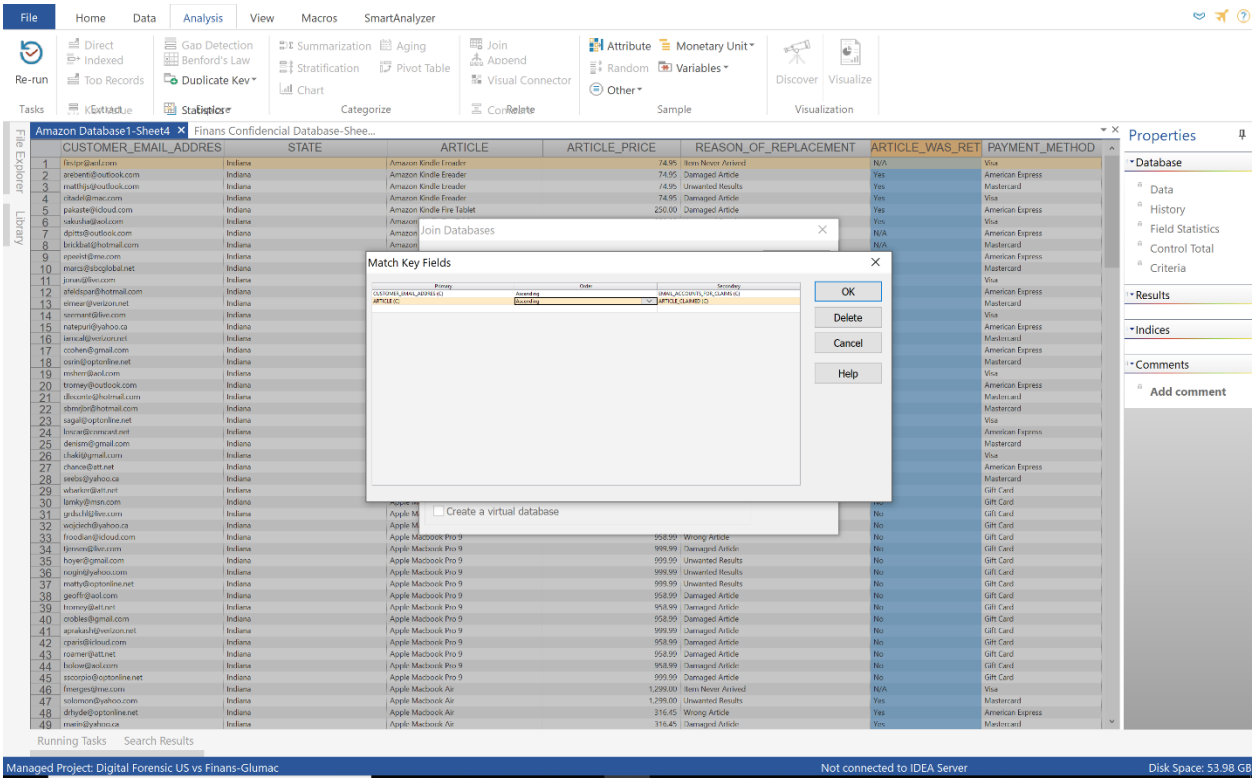


***Figura 26*- Se establecen criterios adicionales para el “Join”**

La Figura 27 muestra los resultados obtenidos, donde se unen los dos documentos Excel con los campos comunes donde comparten datos. Las primeras dos columnas son de Amazon y las dos últimas de los Finans. Ambas muestran los mismos correos electrónicos y los mismos artículos reclamados.

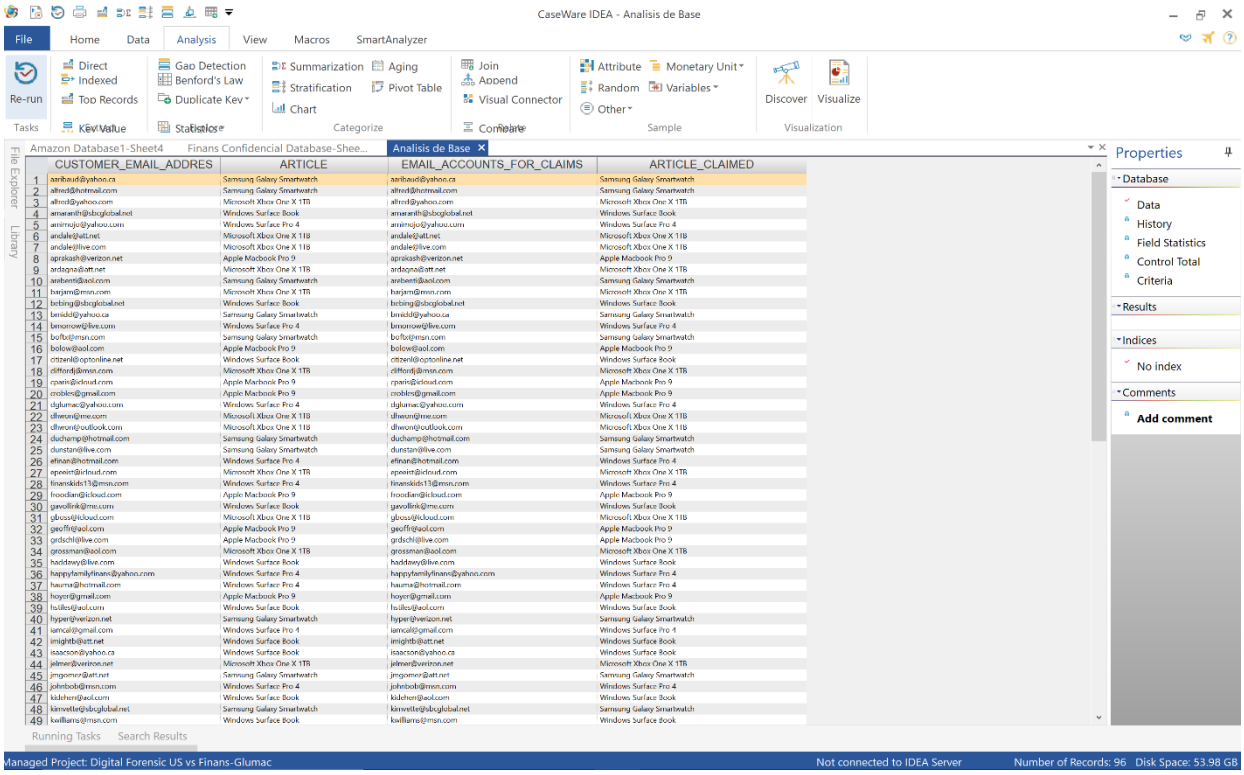


***Figura 27*- Resultados obtenidos**

Conclusión

La gestión forense realizada en las evidencias obtenidas del caso, arrojó resultados concluyentes sobre la participación de los tres acusados en el fraude. Las herramientas utilizadas fueron muy útiles para manejar la evidencia obtenida en un ambiente seguro y sin alterar la integridad de los datos. La información será suministrada a las autoridades pertinentes al caso para el fortalecimiento de la prueba.

SECCIÓN V- DISCUSIÓN DEL CASO

El análisis forense digital realizado con las herramientas FTK Imager y CaseWare IDEA, evidenció de forma contundente el vínculo de los Finans y su socio Danijel Glumac con el fraude realizado a Amazon. A través de los correos electrónicos se prueba la intención, la motivación y la planificación utilizada para llevar a cabo el fraude a Amazon. De parte de Danijel Glumac, pudimos corroborar el conocimiento de la procedencia de los artículos, así como la intención de lavar el dinero obtenido de forma ilegal, utilizando su Shell Company o compañía de fachada. Utilizando IDEA se pudo vincular directamente a los Finans con las múltiples cuentas de correos electrónicos que realizaron reclamaciones, en los 96 correos electrónicos que contenía el documento Excel encontrado de los Finans, se indicaba que el total en dinero de sus ventas fue de $67,500.00. Esos mismos correos electrónicos fueron encontrados en la base de datos de Amazon con el mismo artículo que indicaba el documentó de los Finans. Las pérdidas de Amazon en estas 97 órdenes fueron de $141,272.05. Las autoridades tienen conocimiento de que este fraude estuvo presente por mucho más tiempo y con mucho más dinero perdido, se recomienda continuar solicitando información a Amazon para vincular otras falsas reclamaciones con los acusados de este caso.

SECCIÓN VI- AUDITORÍA Y CONTROLES

En esta sección se discutirán las fallas encontradas en los procesos y controles en las devoluciones realizadas por Amazon. Estas fallas permitieron que los Finans defraudaran en repetidas ocasiones, causando pérdidas monetarias al minorista, y afectando el nombre y prestigio de la empresa de compras. Se entiende que de Amazon haber implementado algunos controles adicionales, hubiesen podido identificar de forma más efectiva el fraude que estaban sufriendo.

Es un hecho que Amazon es una compañía grande y realiza miles de transacciones al día, donde su tamaño constituye una vulnerabilidad para los defraudadores que se aprovechan grietas y puntos grises en los procesos. A través de la discusión de estas fallas, se ofrecerán recomendaciones que podrán evitar situaciones similares y que prepararán a Amazon para los constantes riesgos asociados a la industria de minoristas.

Hallazgo 1: Falta de sistemas de identificación de cliente

Criterio: En un entorno donde no hay contacto persona con persona y el medio para llevar a cabo la venta o la transacción sea el internet, el comercio debe tener la oportunidad de identificar el dispositivo del cliente, y asociarlo al mismo, permitiéndole levantar indicadores de clientes peligrosos. (Hudson, 2018)

Causa: La identificación de los clientes y usuarios de Amazon se realiza a través de los datos entrados en la cuenta por usuario, contraseña, dirección física, y tarjeta de crédito o de regalo. Cualquier persona puede crear múltiples cuentas de Amazon y realizar pagos a través de tarjetas de regalo sin ofrecer sus datos reales.

Efecto: Amazon tendrá que lidiar con personas que creen cuentas con información falsa, que realicen reclamaciones y soliciten reembolsos fraudulentos sin ser debidamente identificados y detenidos.

Recomendación: Implementar de inmediato sistemas de identificación de dispositivos y clientes, que utilicen geolocalización y vinculen a los usuarios con la dirección de Protocolo de Internet (IP) (Hudson, 2018). De esta forma pueden identificar las direcciones IP de los defraudadores, asociándolos a cualquier cuenta que estos puedan crear y refiriéndolos debidamente a las agencias de ley y orden.

Hallazgo 2: No se requiere información personal de los clientes a la hora de realizar una devolución o un reembolso.

Criterio: Se debe requerir identificación para aceptar cualquier mercancía devuelta, o para realizar algún reembolso. Los datos del cliente serán entrados en una base de datos que identificará a clientes que solicitan reembolsos fraudulentos y excesivos cambios de mercancía. (Cimiotti & Merschen, 2013)

Causa: Amazon utiliza los datos contenidos en la cuenta del cliente para ejecutar el reembolso o el cambio de mercancía. Esta reclamación puede hacerse a través de la aplicación móvil, del buscador en internet, por teléfono, y no requiere necesariamente el validar datos de identidad.

Efecto: Pueden tener clientes que soliciten reembolsos y cambios de mercancía de forma repetida y fraudulenta, y sin que Amazon los pueda identificar.

Recomendación: Implementar de inmediato procesos de validación de identidad y de requisitos de información personal. Uso de sistemas computadorizados que ayuden a Amazon

a mantener registro de devoluciones. El acercamiento de un minorista debe manejar los cambios de mercancía identificando a los clientes que solicitan cambios, y actuar en torno a sus historiales de compras, cambios y reembolsos. (Retail Merchandiser, 2008)

Hallazgo 3: Amazon no siguió sus propias políticas de devolución de artículos.

Criterio: "Las computadoras de escritorio, portátiles o tabletas nuevas (a excepción de los lectores electrónicos Kindle y Kindle Fire) comprados en Amazon.com que no arrancaron cuando llegaron, llegaron defectuosas o todavía están en el empaque original sin abrir pueden devolverse a Amazon dentro de los 30 días de la compra para un reembolso total (Amazon, 2018d)"

Causa: Los clientes podían realizar reclamaciones sin tener que devolver los artículos supuestamente dañados. En el caso de Leah y Erin Finan, estos realizaban reclamaciones desde múltiples cuentas de correos electrónicos, y Amazon enviaba artículos nuevos buscando satisfacer y retener al cliente. No se les exigió a los Finans el tener que devolver los artículos "supuestamente" dañados.

Efecto: Erin y Leah Finan realizaron reclamaciones falsas donde solicitaron reemplazos de artículos que no estaban dañados, sin tener que entregar el primer artículo recibido. Las perdidas de Amazon se estimaron en más de 1 millón de dólares.

Recomendación: Orientar al personal de servicio al cliente de la empresa sobre la necesidad del cumplimiento fiel de las políticas, reglamentos y procedimientos para las devoluciones, trayendo datos sobre el impacto negativo en las ganancias de la empresa (Cimiotti & Merschen, 2013). Se recomienda auditar y mantener monitoreo sobre las devoluciones y autorizadas y el personal que las realiza.

SECCIÓN VII- CONCLUSIÓN

El análisis de los casos US vs Erin y Leah Finan, y el caso US vs Danijel Glumac, puso en evidencia las vulnerabilidades que las compras en línea manifiestan. El énfasis de los minoristas por décadas ha sido el prevenir los robos, el fraude ocupacional y las devoluciones fraudulentas. Es suficiente con visitar una megatienda para ver el aparato de seguridad que tienen las tiendas y comercios montado, para prever y disuadir a los criminales de cometer algún delito de robo de mercancía. En caso de una devolución se debe proveer información personal y en ocasiones hasta una identificación con el recibo de compra del artículo. Estas realidades y controles preventivos no funcionan necesariamente igual en una compra en línea, donde no se atiende cara a cara a un cliente, donde los datos que este provee no son necesariamente los correctos.

El magnate de ventas en línea, Amazon.com, demostró que hasta los más grandes pueden ser defraudados y que el riesgo siempre estará presente, con la posibilidad de pérdidas latente. En esta investigación se logró demostrar que los acusados explotaron de forma fraudulenta la política de devoluciones de Amazon, logrando a través del engaño que la compañía les reemplazara artículos que supuestamente estaban dañados, enviándole reemplazos sin exigirle la devolución del primer artículo comprado. La vulnerabilidad en el proceso de identificación de Amazon les permitió crear múltiples cuentas de correos electrónicos, pagar con tarjetas de regalo y recoger los artículos en centros de recogido, sin tener que colocar datos de identificación reales. En este proceso, no solo se cometió el fraude con el engaño, sino que se utilizó el Servicio Postal de los EU para transitar mercancía obtenida ilegalmente, además de que se lavó el dinero a través de instituciones financieras y una compañía de fachada de uno de los acusados tenía.

El análisis forense digital que se realizó se enfocó en recuperar datos borrados de la computadora de los Finans, donde las autoridades federales garantizaron la obtención de la evidencia de forma íntegra y en conformidad con los estándares de la industria. La herramienta FTK Imager localizó varios archivos, entre ellos correos electrónicos muy comprometedores que demuestran de forma clara el fraude realizado, además de un documento en Excel que se entiende era una forma de inventario que los Finans utilizaban para registrar la mercancía reclamada ilegalmente. Se reconoce la gestión de colaboración de Amazon al brindar una base de datos en formato Excel, con evidencia de ordenes de reemplazo sometidas a clientes del Estado de Indiana. Para este análisis CaseWare IDEA fue una herramienta vital que permitió vincular los registros de Amazon, con el registro personal de los Finans.

De este análisis se generaron unos señalamientos y recomendaciones que se espera, sean atendidas por Amazon.com para el mejoramiento de los bienes y servicios que ofrece, al igual que los datos brindados a las Autoridades Federales para la convicción de los acusados. Definitivamente todos estamos expuestos al fraude, y por consiguiente debemos actuar para prevenirlo, detectarlo y erradicarlo.

SECCIÓN VIII-REFERENCIAS

Amazon (2018a). *About Refunds.* Recuperado de:

https://www.amazon.com/gp/help/customer/display.html?nodeId=201819300

Amazon (2018b). *Acerca de las devoluciones gratuitas.* Recuperado de:

https://www.amazon.com/gp/help/customer/display.html?language=es_US&nodeId=20207510

Amazon (2018c). *Prime Insider.* Recuperado de Amazon Prime:

https://www.amazon.com/primeinsider

Association of Certified Fraud Examiners ACFE (2018). Recuperado de

https://www.acfe.com/fraud-101.aspx

Bradley, J. R., & Garfinkel, S. L. (2015). *Bulk Extractor User Manual.*

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* Maryland: Elsevier.

CaseWare IDEA (2019). *The Trusted Tool for Data Analysis.* Recuperado de: https://idea.caseware.com/products/idea/

Cimiotti, G., & Merschen, T. (2013). *Trends in consumer payment fraud: A call for consistent strong authentication across all consumer payments*. Journal of Payments Stratery & Sistems, 8(1), 54.

CNN (2016). *Ex-White House aide arrested in alleged refund scam.* Recuperado de: http://edition.cnn.com/2006/US/03/11/claude.allen.arrest/index.html

Cowen, D. (2013). *Computer Forensics.* Nueva York: Mc Graw Hill.

Craiger, P. (2016). *Computer Forensics Procedures and Methods. Handbook of Information Security, 3.*

Finklea, K. M. (2012). *Organized Retail Crime* . Washington: CRS Report for Congress.

Forensics Toolkit (FTK) (2017). *What is FTK?* Recuperado de: https://accessdata.com/assets/images/misc-content/FTK-6.3-WEB_.pdf

Garfinkel, S. L. (2012). *Using bulk_extractor for digital forensics triage and cross-drive analysis.* California: NPS.

Garfinkel, S. (2014). *Bulk_extractor*. Recuperado de: https://tools.kali.org/forensics/bulk-extractor

Huddleston, T. (2018). *How this young Indiana couple stole $1.2 million from Amazon.* Recuperado de CNBC: https://www.cnbc.com/2018/06/07/how-the-finans-stole-1-point-2-million-in-consumer-electronics-from-amazon.html

Hudson, M. (2018). *Recognizing Return Fraud*. Recuperado de: https://www.thebalancesmb.com/recognizing-return-fraud-2890255

Kenton, W. (2017). *Common Carrier*. Recuperado de Investopedia: https://www.investopedia.com/terms/c/common-carrier.asp

Legal Information Institute (a). Ley número 18 Código de los EU § 1341. *Frauds and swindles.* (2018, diciembre 12). Recuperado de: https://www.law.cornell.edu/uscode/text/18/1341

Legal Information Institute (b) Ley número 18 Código de los § 1956. *Laundering of monetary instruments*. (2018, diciembre 12). Recuperado de: https://www.law.cornell.edu/uscode/text/18/1956

Legal Information Institute (c) Ley número 18 Código de los § 2314. *Transportation of stolen goods, securities, moneys, fraudulent State tax stamps, or articles used in counterfeiting*. (2018, diciembre 12). Recuperado de: https://www.law.cornell.edu/uscode/text/18/2314

Malphrus, Steve.(2009)*Perspectives on Retail Payments Fraud*. Economic Perspectives, Vol. 33(*1*).

Mohan, M. (2018). *Over 71 Amazon Products & Services You Probably Don't Know.* Recuperado de: https://www.minterest.com/list-of-all-amazon-products-and-services/

Moraca, B. (2017). *2017 Organized Retail Crime Survey.* National Retail Federation. NRF.

National Retail Federation (2018). State Retail Associations. Recuperado de: https://nrf.com/hill/action-center/state-retail-associations

Nelson, B., Phillips, A., & Steuart, C. (2015). *Guide to Computer Forensics and Investigations.* Boston: Cengage Learning.

Perano, U. (2018). *Walmart shopper accused of making more than 1,000 fake returns.* Recuperado de: https://edition.cnn.com/2018/06/17/us/walmart-shopper-accused-fake-returns/index.html

Popovich, J. (2018). *Yuma Police: Man arrested for $1.3 million in fraudulent returns to Walmart.* Recuperado de:

https://www.abc15.com/news/region-central-southern-az/yuma/yuma-police-man-arrested-for-13-million-in-fraudulent-returns-to-walmart

Rankin, J. (2016). *Third-party sellers and Amazon - a double-edged sword in e-commerce.* Recuperado de: https://www.theguardian.com/technology/2015/jun/23/amazon-marketplace-third-party-seller-faustian-pact

Retail Merchandiser (2008). *Stopping Return Fraud*. *48*(4), 36.

Sheets, M. (2018). *Man, 23, 'defrauded 1,000 Walmart stores out of $1.3million by buying laptops and taking out parts before returning them'.* Recuperado de MailOnline: https://www.dailymail.co.uk/news/article-5852433/Man-suspected-defrauding-1-000-Walmart-stores.html

Snocken, D. (2004). Retail Fraud: How to out think shrink. Europeaon Retail Digest(42), 52-54.

Statista (2018a). Annual Amazon Prime member expenditure 2018. Recuperado de: https://www.statista.com/statistics/304938/amazon-prime-and-non-prime-members-average-sales-spend/

Statista (2018b). *Net sales revenue of Amazon from 2004 to 2017.* Recuperado de: https://www.statista.com/statistics/266282/annual-net-revenue-of-amazoncom/

The Law Dictionary (2018). *¿Qué son las compras en línea?* Recuperado de: https://espanol.thelawdictionary.org/compras-en-linea/

Thomson Reuters (2018). *Return Policies and Refunds.* Recuperado de: https://consumer.findlaw.com/consumer-transactions/return-policies-and-refunds.html

U.S. Department of Justice (2018). *Amazon fraudsters sentenced to years in federal prison.* Recuperado de https://www.justice.gov/usao-sdin/pr/amazon-fraudsters-sentenced-years-federal-prison

U.S. Department of Justice (2018). *Supermarket Owner, Accomplice Sentenced in Identity Theft, Tax Fraud Scheme.* Recuperado de https://www.justice.gov/usao-ri/pr/supermarket-owner-accomplice-sentenced-identity-theft-tax-fraud-scheme

U.S. Immigration and Customs Enforcement (2012). *Organized Retail Crime (The SEARCH Initiative).* Recuperado de: https://www.ice.gov/factsheets/retail-crime

US v. Claude Allen (Cort of Appeal District of Columbia, 2011).

US v. Danijel Glumac (Southern District of Indiana, 2017).

US v. Erin Finan (Southern District of Indiana, 2017).

US v. Thomas Frudaker (Distrito de Arizona, 2018).

US v. Tomasino (Corte de Apelaciones del Primer Circuito, 2018).

Wells, J. T. (2013). *Principles of Fraud Examination.* Austin: Wiley