EDP UNIVERSITY OF PUERTO RICO, INC.
RECINTO DE HATO REY
PROGRAMA DE MAESTRÍA EN SISTEMAS DE INFORMACIÓN
Especialidad en Seguridad de Información e Investigación de Fraude

ESQUEMA DE FRAUDE ELECTRÓNICO EN DECLARACIONES DE IMPUESTOS

U.S. V. YOANDY PEREZ LLANES

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

mayo, 2017

PREPARADO POR:

YASHIRA M. GÓMEZ NARVÁEZ

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

ESQUEMA DE FRAUDE EN REEMBOLSO DE IMPUESTO FEDERAL
ANALISIS DE CASO: U.S. V. YOANDY PEREZ LLANES

Preparado por:
Yashira M. Gómez Narváez

Ha sido aceptado como requisito parcial para el grado de
Maestría en Sistemas de Información con Especialidad en Seguridad de Información e Investigación de Fraude.

mayo, 2017

Dr. Miguel A. Drouyn Marrero
Director de Programa Graduado

TABLA DE CONTENIDO

TABLA DE FIGURAS

SECCIÓN 1: INTRODUCCIÓN Y TRASFONDO

Introducción

Según el Internal Revenue Service (IRS) (2017a), en la actualidad el robo de identidad y el fraude de reembolso se han convertido en una dura realidad y un gran problema en crecimiento, con el que lleva varios años, luchando agresivamente. Desde el año 2015 hasta noviembre de 2016, el IRS rechazó el procesamiento de 4.8 millones de declaraciones sospechosas y detuvieron 1.4 millones de declaraciones confirmadas como robo de identidad, para un total de $8 mil millones de dólares.

El robo de identidad se puede definir de varias maneras. El IRS (2017b) lo define como robo de identidad relacionado con los impuestos cuando alguien roba un número de identificación personal y presenta una declaración de impuestos falsa con el fin de reclamar un reembolso fraudulento. De la misma manera define el término *phishing* como la práctica fraudulenta realizada a través de un correo electrónico no solicitado y/o sitios web que se presentan como sitios legítimos y logran atrapar a las personas para que revelen su información personal y financiera.

Por su parte, Norton (2016) define el robo de identidad *online* como el proceso en el que ladrones utilizan correos electrónicos y sitios *web* falsos para simular organizaciones legítimas. Se aprovechan de su confianza engañándole para que divulgue información personal, como contraseñas y números de cuentas. Del mismo modo, *hackers* y virus pueden infiltrarse en su ordenador e instalar registradores de pulsaciones para robar datos o capturar nombres y contraseñas de cuentas cuando usted las introduce.

Según la Comisión Federal de Comercio (s.f.), el robo de identidad y la reclamación de impuestos falsos se ha convertido en un juego para los estafadores y una pesadilla para las víctimas que deben estar alerta y proteger cuidadosamente su información personal.

Se analizará el caso U.S. v. Yoandy Pérez Llanes (2015b). Según el expediente, Yoandy Pérez Llanes ha sido acusado de montar una red de estafa entre Venezuela y Miami, para enviar 935 declaraciones de impuestos falsas, que solicitaban reembolsos por un total de 2.2 millones de dólares, usando datos robados del personal del Centro Médico de la Universidad de Pittsburgh.

Descripción del Caso

Caso:

- United States of América v. Yoandy Pérez Llanes

Número del caso:

- Penal No. 15-141 Pittsburgh
- Docket number: 2:15-cr-00141

Materia:

- Esquema de fraude electrónico en declaraciones de impuestos.

Acusados:

- Yoandy Pérez Llanes
- Tres (3) cómplices de los que no hay información.

Víctimas:

- Empleados de la Universidad de Pittsburgh Medical Center (UPMC)
- La oficina de Servicios de Impuestos Internos (IRS, por sus siglas en inglés)

Abogado de la Defensa:

- Thomas Livingston de la oficina del defensor público federal.

Representantes del Estado:

- Gregory C. Melucci, Fiscal Federal
- David Hickton, Fiscal Federal del Distrito Oeste de Pensilvania, Estado Unidos de América.

Investigadores del Caso:

- Timothy Burke, agente del Servicio Secreto de los Estados Unidos
- Robert Kickbush, agente del IRS y coordinador de robo de identidad de la oficina de Pittsburgh.

Juez de Distrito:

- Honorable Mark Raymond Hornak, Corte de Distrito de Oeste de Pensilvania

Trasfondo

Según los documentos del caso U.S. v. Yoandy Pérez Llanes (2015), un gran jurado federal de Pittsburgh, EE.UU., emitió una acusación formal de varios cargos contra Yoandy Pérez Llanes, ciudadano venezolano de 32 años de edad, nació en Cuba el 7 de septiembre de 1983 y contaba con domicilio en Maracaibo, Venezuela.

Pérez fue acusado de 14 cargos en un esquema para defraudar al Servicio de Rentas Internas (IRS) y al Tesoro de Estados Unidos, con el uso de identidades robadas a empleados de la Universidad de Pittsburgh Medical Center (UPMC) que cuenta con 62,000 empleados. El presentó declaraciones de impuestos federales falsas con el fin de obtener los reembolsos ilegales de estos impuestos. Pérez Llanes y sus conspiradores no identificados tramitaron las declaraciones de impuestos a través de un *software* llamado Turbo Tax.

Según Turbo Tax (2013). Turbo Tax es un *software* de preparación de impuestos que permitía en el año 2013 a los individuos calcular, presentar y cambiar, por *gift cards* (tarjetas de regalos) sus impuestos sobre las rentas federales y estatales. En el año 2015 debido al incremento en fraudes reportados en el IRS. Turbo Tax eliminó la opción del cambio de rembolsos de impuestos a *gift cards*.

A través de Turbo Tax, Yoandy Pérez Llanes y sus conspiradores adquirieron ilegalmente los reembolsos de impuestos, los cuales cambiaron por *gift cards* de la tienda online Amazon. Las *gift cards* fueron utilizadas para comprar miles de dólares en mercancía electrónica que era enviada a Miami, EE. UU, donde miembros del grupo de

conspiradores los re- empacaban y posteriormente los re-enviaban a Maracay, Venezuela. Yoandy estuvo prófugo de la justicia norteamericana desde que se emitió la acusación formal en mayo de 2015 hasta el 26 de junio 2015 fecha en que lo capturaron en Venezuela y fue extraditado por la Interpol a los Estados Unidos.

Descripción de Hechos

Según los documentos del caso U.S. v. Yoandy Pérez Llanes (2015a), el agente del IRS Robert Kickbush, coordinador de robo de identidad de la oficina de Pittsburgh, y Timothy Burke, investigador de la Oficina del Servicio Secreto alegan que, para enero de 2014, cientos de empleados de la Universidad de Pittsburgh Medical Center (UPMC) presentaron sus declaraciones de impuestos de Rentas Internas Federal de 2013, pero se llevaron tremenda sorpresa. El Internal Revenue Service (IRS) les envió avisos a todos notificándoles que ya habían emitido las devoluciones de los impuestos reclamados. Los empleados, al no recibir los reembolsos notifican lo ocurrido, al IRS y al Departamento de Seguridad de la Universidad de Pittsburgh Medical Center.

Entre el 31 de enero de 2014 y el 6 de marzo de 2014, el Servicio de Impuestos Internos identificó aproximadamente 935 declaraciones de impuestos electrónicas federales de forma 1040, l-040A y L040EZ no autorizadas y fraudulentas con los nombres de empleados vigentes y antiguos de UPMC. Estas declaraciones contenían información personal de los empleados, tales como nombre, dirección, número de seguro social, información de retención de ocupación y salario.

Los investigadores identificaron los reembolsos fraudulentos, en un total aproximado de $2,205,925.00 dólares de los cuales $1,475,593.00 ya había sido pagado, por el Tesoro de los Estados Unidos en forma de reembolsos ilegales.

Para abril de 2014 los investigadores encontraron bastante evidencia que involucraba directamente con el esquema de fraude a Yoandy Pérez Llanes:

1. Para principios del mes de febrero de 2014, el sr. Yoandy Pérez Llanes y tres (3) conspiradores comenzaron el fraude *hackeando* la base de datos de la UPMC extrajeron información sensible de empleados y ex empleados desde dispositivos electrónicos fuera de los Estados Unidos para esto utilizaron correos electrónicos anónimos y cifrados para ocultar sus identidades, también utilizaron dispositivos informáticos que aparentaban estar localizados en el Distrito Oeste de Pensilvania con direcciones IP de un *Proxy server*, lo que creó la apariencia engañosa.
2. A finales de febrero de 2014, Pérez y sus conspiradores solicitaron 932 devoluciones de impuestos, con los datos robados de los empleados de la Universidad de Pittsburgh Medical Center (UPMC), a través de una compañía de devolución de impuestos, por internet llamada *Turbo Tax* en forma de códigos de redención *gift cards* de la tienda Amazon.com en lugar de ser depósitos electrónicos o cheques del Tesoro de los Estados Unidos.
3. Entre 1 al 4 de marzo de 2014, aproximadamente $885,578.00 dólares de las devoluciones de impuestos fraudulentas, ya habían sido reembolsados y utilizados en la compra de mercancía electrónica tales como: Celulares, computadoras, tabletas y juegos electrónicos en la tienda de internet *Amazon.com*.

4. Toda la mercancía adquirida en Amazon.com era enviada, por la tienda a una dirección postal en Miami, Florida desde donde los conspiradores la reenviaban a Maracaibo, Venezuela donde parte de esta mercancía la vendían en páginas *web* de subastas.
5. De acuerdo con el Tribunal Supremo de Justicia de Venezuela (2015). El 16 de abril de 2015, la corte de distrito de Pensilvania, expide una orden de detención y extradición, al Tribunal de Justicia de Venezuela para la captura de Yoandy Pérez Llanes. en el mencionado país.
6. El 28 de mayo de 2015, Yoandy Pérez Llanes. fue capturado y extraditado desde Venezuela a Estados Unidos.
7. El 26 de junio de 2015, Yoandy Pérez Llanes fue encausado con otros individuos de cargos de fraude, lavado de dinero, robo de identidad y conspiración. Fue instruido de cargos en el Tribunal Federal de Pittsburgh.

Acusaciones, cargos y penalidades

Yoandy Pérez Llanes fue acusado de 14 cargos en un esquema para defraudar al Servicio de Rentas Internas (IRS, por sus siglas en inglés) y al Tesoro de Estados Unidos, con el uso de identidades robadas a empleados de la Universidad de Pittsburgh Medical Center (UPMC) para presentar falsas declaraciones de impuestos federales con el fin de obtener el reembolso ilegal de impuestos. Buscaban obtener 2.2 millones en reembolsos, según los fiscales. Tuvieron éxito en conseguir 1.5 millones de dólares.

Las acusaciones en contra del señor Pérez consisten en violaciones a los siguientes códigos:

1) Asociación ilícita para cometer los delitos federales de fraude por medios electrónicos, presentación de solicitudes de devolución de impuestos falsas, usurpación de identidad y sustracción de caudales públicos. Act,18 U.S.C § 371(2015)

2) Asociación ilícita con miras a defraudar a los Estados Unidos Act,18 U.S.C §371 (2015)

3) Robo de caudales públicos Act,18 U.S.C § 641(2015)

4) Asociación ilícita con miras a defraudar al fisco por medio de solicitudes de devolución de impuestos Act,18 U.S.C § 286(2015)

5) Presentación de solicitudes de devolución de impuestos falsas, ficticias o fraudulentas Act,18 U.S.C § 287(2015)

6) Fraude en relación con dispositivos de acceso Act,18 U.S.C § 1029(2015)

7) Usurpación de identidad con agravantes Act,18 U.S.C § 1028A (a)1(2015)

8) Usurpación de identidad Act,18 U.S.C § 1028(A)7(2015)

9) Fraude y actividades conexas relacionadas con dispositivos de acceso Act,18 U.S.C §1029(2015)

10) Fraude por medios postales Act,18 U.S.C § 1341(2015)

11) Fraude por medios electrónicos Act,18 U.S.C § 1343(2015)

12) Asociación ilícita para cometer fraude por medios postales o electrónicos Act,18 U.S.C § 1349(2015)

13) Asociación ilícita para blanquear instrumentos monetarios Act,18 U.S.C § 1956(2015)

14) Blanqueo de instrumentos monetarios Act,18 U.S.C § 1957(2015)

De ser hallado culpable Yoandy Pérez LLanes se enfrenta a una pena máxima de más de 20 años de privación a la libertad. U.S v. Yoandy Pérez Llanes (2015a)

1. El fraude y el lavado de dinero conllevan cada uno un máximo de 20 años de cárcel
2. El cargo de conspiración podría acarrear un máximo de cinco años.
3. El robo de identidad podría implicar dos años de cárcel.

Definición de Términos

Reembolso de impuestos- es un reembolso sobre los impuestos cuando la obligación tributaria es menor que el de los impuestos pagados. Los contribuyentes a menudo pueden obtener un reembolso de impuestos en su impuesto sobre la renta si el impuesto que deben es menor que la suma del monto total de la retención fiscal y los impuestos estimados que pagan, además de los créditos tributarios reembolsables que ellos reclaman. Los reembolsos de impuestos se devuelven en dinero al final del año fiscal. (IRS, 2017c)

Fraude informático- el fraude cibernético e informático o fraude de computadora se refiere al fraude realizado a través del uso de una computadora o del Internet. Es Cualquier desfalco o malversación mediante la manipulación de programas informáticos. La piratería informática *hacking* es una forma común de fraude: el delincuente usa herramientas tecnológicas sofisticadas para acceder a distancia a una computadora con información confidencial. Otra forma de fraude involucra la intercepción de una transmisión electrónica. Esto puede ocasionar el robo de la contraseña, el número de cuenta de una tarjeta de crédito u otra información confidencial sobre la identidad de una persona. (Lynch, s.f.)

El robo de identidad relacionado a los impuestos- sucede cuando alguien utiliza su número de Seguro Social robado y presenta una declaración de impuestos reclamando un reembolso fraudulento. Si usted llega a ser una víctima de este crimen, estamos comprometidos a ayudarle a resolver su caso lo más pronto posible. (IRS, 2017b)

Robo de identidad *online* - como el proceso en el que ladrones utilizan correos electrónicos y sitios "web" falsos para simular organizaciones legítimas. Se aprovechan de su confianza engañándole para que divulgue información personal, como contraseñas y números de cuentas. Del mismo modo, "hackers" y virus pueden infiltrarse en su ordenador e instalar registradores de pulsaciones para robar datos o capturar nombres y contraseñas de cuentas cuando usted las introduce. (Norton,2016)

Base de datos- De una manera simple, es un contenedor que permite almacenar la información de forma ordenada con diferentes propósitos y usos. En este sentido; una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. Actualmente, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital, siendo este un componente electrónico, por tanto se ha desarrollado y se ofrece un amplio rango de soluciones al problema del almacenamiento de datos. (IBM, 2015)

Gift Card- Es una tarjeta de regalo que puede describirse como una especie de tarjeta de débito o crédito precargada que le posibilita al titular de la misma poder adquirir una serie de bienes o servicios. (Collins, 2017)

IP address- Un *IP address* o dirección *IP* es un número que identifica, de manera lógica y jerárquica, a un Interfaz en red elemento de comunicación/conexión de un dispositivo computadora, tableta, portátil, o *smartphone* que utilice el protocolo *IP* (*Internet Protocol*), que corresponde al nivel de red del modelo TCP/*IP*. (Castro,2016)

Hacker- Es aquella persona experta en alguna rama de la tecnología, a menudo informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo. (Raymond, 2001)

Hacking- El término *hacking* es la acción de irrumpir o entrar de manera forzada a un sistema de cómputo o a una red. (Giménez, s.f).

SECCIÓN 2: REVISIÓN DE LITERATURA

Introducción

Según Homeland Security (2016), los delitos de fraudes electrónicos cometidos por *hackers* sin escrúpulos, que atacan a las empresas y a personas a través de Internet son cada vez más sofisticados. Los defraudadores se encuentran más preparados, disponen de mejores herramientas y tienen un mercado mucho más amplio sobre el cual actuar.

Cressey (1972), en su definición del Triángulo del Fraude, señala que las personas actúan de forma fraudulenta por una presión, oportunidad y una racionalización justificada. El caso U.S v. Yoandy Pérez Llanes (2015), asumimos que la presión o motivación que llevo a Yoandy Pérez Llanes a cometer el fraude fue para ganar dinero de una manera fácil apropiándose ilegalmente de unos reembolsos de impuestos que no le

pertenecían. La oportunidad que él tuvo fue el acceso a la información de los empleados de la Universidad de Pittsburgh Medical Center para cometer el delito y la racionalización es el daño ausente: él pensaría que nadie sufriría un daño real por el hecho de robar información de un archivo de un computador y luego reclamar unos impuestos en un país lejano al de él.

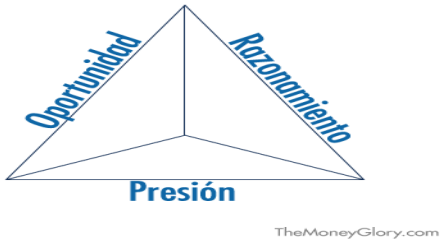


Figura 1: Triangulo de Fraude de Cressey

(tomado de TheMoneyGlory.com)

Fraudes Involucrados

El fraude es el delito más creativo que requiere de las mentes más agudas y maliciosas, podemos decir que es prácticamente imposible de evitar. En el momento en que se descubre el remedio, alguien inventa algo nuevo, pero su detección a tiempo puede ahorrarnos un mal rato e inclusive pérdidas muy generosas económicamente.

¿Qué constituye un fraude? ACFE (2017) conceptualiza el fraude como las actividades y/o acciones que tienen el propósito de enriquecimiento personal a través del uso inapropiado o la sustracción de recursos y/o activos de una organización por parte de una persona. Es decir, ACFE tiene en cuenta el mal uso o abuso de los bienes de una entidad en beneficio de un sujeto. Por lo tanto, el abuso es tenido en cuenta como Fraude.

Tomando en cuenta lo antes mencionado cabe señalar que existen muchos tipos de fraudes, pero en este caso U.S. v. Yoandy Perez Llanes (2015a) hubo unos fraudes en particular los cuales fueron parte del esquema cometido, por Yoandy Perez y sus cómplices como lo fue los fraudes por medios electrónicos, el *Phishing, pharming,* robo de identidad, los *botnets*, el *clean fraud*, *Account takeover.* Estos fraudes fueron los que se utilizaron en este caso para cometer delito. A continuación los resaltaré con una breve descripción:

Según Norton (2016**),** los fraudes por medios electrónicos o fraudes *online* se refiere al fraude realizado a través del uso de una computadora o del Internet. Es Cualquier desfalco o malversación mediante la manipulación de programas informáticos. La piratería informática *hacking* es una forma común de fraude: el delincuente usa herramientas tecnológicas sofisticadas para acceder a distancia a una computadora con información confidencial. Otra forma de fraude involucra la intercepción de una transmisión electrónica. Esto puede ocasionar el robo de la contraseña, el número de cuenta de una tarjeta de crédito u otra información confidencial sobre la identidad de una persona.

Norton (2016) señala que los sectores más afectados por el fraude electrónico son las entidades financieras con robos de datos bancarios, las organizaciones o empresas y cualquier otra persona como usted y como yo.

Por otra parte, Khan (2013) califica el fraude por medios electrónicos *online* de las siguientes maneras:

1. ***Phishing y Pharming-*** dos formas de suplantación de identidad. En el *phishing*, el delincuente cibernético consigue engañar al usuario mediante un correo, normalmente *spam*, invitándole por ejemplo a realizar una operación bancaria en una página que

aparentemente tiene la misma interfaz que la su banco. Por el contrario, en el *pharming* no es necesario que el usuario efectúe una operación bancaria accediendo a la página mediante un link que le proporciona el timador. El usuario intentará acceder directamente desde su navegador con la normalidad de siempre, excepto en que la página a la que acceda será una copia de la original.

El *phishing* se ha convertido en una de las modalidades de robo más utilizadas por los estafadores y defraudadores informáticos. Es común que las personas poco precavidas caigan en este peligroso método, cuyo fin es lograr acceder a fotografías personales, correos electrónicos o datos bancarios. Para el año 2014, Estados Unidos era el principal afectado por ataques *phishing* con un 62%, el Reino Unido ocupaba el segundo lugar con un 11%, España el tercero con un 7%, cuarto Japón con un 6% y quinto China con el 2%. Para el año 2015, Brasil encabezaba la lista en cuanto al número de usuarios afectados. Los brasileños siguen siendo las víctimas predilectas de los *phishers.*

Esta figura muestra el incremento en los reportes de *phishing* del año 2015 en diferentes países de América.

País	Porcentaje
Brasil	12,3%
Argentina	7,5%
Ecuador	5,7%
Venezuela	5,2%
Bolivia	5,2%
Colombia	5,1%
Chile	5,0%
México	4,4%
Perú	4,3%
Costa Rica	3,9%
Paraguay	3,9%
Uruguay	3,8%

Figura 2: Usuarios afectados por el *phishing*

(Tomado de Kaspersky Lab, 2017)

2. Robo de identidad- El robo de identidad es el fraude que se origina cuando alguien usa su información o datos personales sin su permiso tales como: nombres, dirección de domicilio, número de Seguro Social, contraseñas, nombres de usuario, información bancaria, el número de sus tarjetas de crédito o débito con el fin de estafar y/o defraudar.

3. *Botnets*-son robots informáticos que se instalan en los ordenadores, mediante spam o malware. Se ejecutan de manera autónoma y automática. El artífice de la *botnets* puede controlar todos los ordenadores/servidores infectados de forma remota.

A tenor con lo antes mencionado y más allá de cualquier definición, los fraudes constituyen grandes problemas en las organizaciones y/o agencias de diferentes rubros y dimensiones. ACFE (2017) señala que las compañías estadounidenses pierden alrededor del 6% de sus ingresos anuales debido a prácticas fraudulentas.

Leyes aplicables

Act, 18 U.S.C §371 (2015) Asociación ilícita con miras a defraudar a los Estados Unidos- Si dos o más personas conspiran para cometer cualquier ofensa contra los Estados Unidos, o para defraudar a los Estados Unidos, o cualquier agencia de la misma de cualquier manera o para cualquier propósito, y una o más de esas personas hacen cualquier acto para realizar el objetivo de la conspiración, cada uno será multado bajo este título o encarcelado no más de cinco años, o ambos. Sin embargo, si el delito cuya comisión es objeto de la conspiración es un delito menos grave, el castigo por tal conspiración no excederá el castigo máximo previsto para tal delito menor.

Act,18 U.S.C § 641(2015) Robo de caudales públicos- Quien desvíe, roba, o con conocimiento convierte a su uso o el uso de otro, o sin autoridad, vende, transmite o dispone de cualquier registro, vale, dinero o cosa de valor de los Estados Unidos o de cualquier departamento u organismo o cualquier propiedad hecha o bajo contrato para los Estados Unidos o cualquier departamento o agencia de la misma; o Quien recibe, oculta o retiene lo mismo con la intención de convertirlo a su uso o ganancia, sabiendo que ha sido malversado, robado, robado o convertido, Será multado bajo este título o encarcelado no más de diez años, o ambos; Pero si el valor de tales bienes en el agregado, combinando cantidades de todos los cargos por los cuales el acusado es condenado en un solo caso, no exceda la suma de $ 1,000, será multado bajo este título o encarcelado no más de un año o ambos.

Act,18 U.S.C § 286(2015) Asociación ilícita con miras a defraudar al fisco por medio de solicitudes de devolución de impuestos- Quien celebre cualquier acuerdo, combinación o conspiración para defraudar a los Estados Unidos o cualquier departamento o agencia de la misma, obteniendo o ayudando a obtener el pago o la concesión de cualquier reclamo falso, ficticio o fraudulento, será multado bajo este título o encarcelado No más de diez años, o ambos.

Act,18 U.S.C § 287(2015) Presentación de solicitudes de devolución de impuestos falsas, ficticias o fraudulentas- Quien haga o presente a cualquier persona o funcionario en el servicio civil, militar o naval de los Estados Unidos, cualquier departamento o agencia del mismo, cualquier reclamación sobre o contra los Estados Unidos, o cualquier departamento o agencia del mismo, conociendo dicha reclamación ser falsa, ficticia o

fraudulenta, será encarcelada no más de 5 años y estará sujeta a una multa en la cantidad prevista en este título.

Act,18 U.S.C § 1029(2015) Fraude en relación con dispositivos de acceso- Significa cualquier tarjeta de crédito, placa, código, número de cuenta, número de serie electrónico, número de identificación móvil, número de identificación personal u otro medio de acceso a la cuenta que pueda utilizarse, solo o conjuntamente con otro dispositivo de acceso, Para obtener dinero, bienes, servicios o cualquier otra cosa de valor, o que pueda ser usado para iniciar una transferencia de fondos que no sea una transferencia originada únicamente por un instrumento en papel. La esencia del Delito Federal de Fraude en relación con Tarjetas de Crédito Falsificadas u otros dispositivos de acceso es el uso deliberado de un dispositivo de acceso falsificado con la intención de defraudar, y no es necesario demostrar que alguien fue de hecho engañado o defraudado.

Act,18 U.S.C § 1028(A)7(2015) Usurpación de identidad- Cualquier persona que a sabiendas y sin autoridad legal produce un documento de identificación, rasgo de autenticación o un documento de identificación falso; transfiera conscientemente un documento de identificación, rasgo de autenticación o un documento de identificación falso sabiendo que dicho documento o característica fue robado o producido sin autoridad legal; posee a sabiendas, con la intención de usar ilícitamente o transferir ilegalmente cinco o más documentos de identificación (distintos de los expedidos legalmente para el uso del poseedor), características de autenticación o falsos documentos de identificación; A sabiendas transfiere, posee o utiliza, sin autoridad legal, un medio de identificación de otra persona con la intención de cometer, o para ayudar o incitar, o en relación con, cualquier actividad ilegal que constituya una violación de la ley Federal, o que constituya Un delito

grave bajo cualquier ley estatal o local aplicable; o trafica intencionadamente características de autenticación falsas o reales para su uso en documentos de identificación falsos, implementos de fabricación de documentos o medios de identificación; Será castigado según lo dispuesto de esta sección.

Act,18 U.S.C § 1028A (a)1(2015) Usurpación de identidad con agravantes- Cualquier persona que transfiera, posea o utilice conscientemente, sin autoridad legal, un medio de identificación de otra persona, además de la pena provista para tal delito mayor. Condenado a una pena de prisión de 2 años.

Fraude y actividades conexas relacionadas con dispositivos de acceso Act,18 U.S.C § 1029(2015)- Cualquier persona que a sabiendas y con la intención de defraudar produce, usa o trafica en uno o más dispositivos de acceso falsificados; a sabiendas y con la intención de defraudar tráficos en o usa uno o más dispositivos de acceso no autorizado durante cualquier período de un año, y por tal conducta obtiene cualquier cosa de valor que agregue $ 1,000 o más durante ese período; a sabiendas y con la intención de defraudar posee quince o más dispositivos que son dispositivos de acceso falsificados o no autorizados; a sabiendas y con la intención de defraudar, produce, trafica, tiene el control o la custodia de, o posee equipo de fabricación de dispositivos; a sabiendas y con intención de defraudar transacciones de efectos, con 1 o más dispositivos de acceso expedidos a otra persona o personas, para recibir pago o cualquier otra cosa de valor durante un período de 1 año cuyo valor agregado sea igual o mayor De $ 1,000; sin la autorización del emisor del dispositivo de acceso, a sabiendas y con la intención de defraudar solicita a una persona con el propósito de: que ofrece un dispositivo de acceso; o vender información relativa a una aplicación para obtener un dispositivo de acceso.

Act,18 U.S.C § 1341(2015) Fraude por medios postales- Quienquiera que haya ideado o pretenda idear algún esquema o artificio para defraudar, o para obtener dinero o propiedad mediante pretensiones, representaciones o promesas falsas o fraudulentas, o para vender, disponer, prestar, intercambiar, Distribuir, suministrar o adquirir para uso ilícito cualquier moneda falsa o falsa, obligación, seguridad u otro artículo, o cualquier cosa que se represente para ser dicho artículo falsificado o espurio, o artificio o intento de hacerlo, lugares en cualquier oficina de correos o depósito autorizado para el asunto del correo, cualquier cosa o cosa que sea enviada o entregada por el Servicio Postal, o depósitos o causas para ser depositados cualquier asunto o cosa que sea enviada o entregado por cualquier portador interestatal privado o comercial, o toma o recibe de él, cualquier cosa o cosa, o causa a sabiendas que sea entregado por correo o tal portador según la dirección en él, o en el lugar en el cual está dirigido a ser Entregado por la persona a quien se dirige, cualquier asunto o cosa, será multado bajo este título o encarcelado no más de 20 años, o ambos.

Act,18 U.S.C § 1343(2015) Fraude por medios electrónicos- Cualquier persona que haya ideado o pretenda idear algún esquema o artificio para defraudar, o para obtener dinero o propiedad mediante falsas o fraudulentas pretensiones, representaciones o promesas, transmita o hace que se transmitan por medio de comunicaciones por cable, radio o televisión En el comercio interestatal o extranjero, cualquier escritura, signo, señal, imagen o sonido con el fin de ejecutar tal esquema o artificio, será multado bajo este título o encarcelado no más de 20 años, o ambos. Si la infracción ocurre en relación con, o implica cualquier beneficio autorizado, transportado, transmitido, transferido, desembolsado o pagado en relación con, un desastre o emergencia principal declarado presidencialmente

como dichos términos se definen en la sección 102 del Robert T. Stafford (42 USC 5122), o afecta a una institución financiera, dicha persona será multada no más de $ 1,000,000 o encarcelada no más de 30 años, o ambos.

Act,18 U.S.C § 1349(2015) Asociación ilícita para cometer fraude por medios postales o electrónicos- Toda persona que intente o conspire para cometer un delito bajo este capítulo estará sujeta a las mismas penas que las prescritas para el delito cuya comisión fue objeto del intento o conspiración.

Act,18 U.S.C § 1956(2015) Asociación ilícita para blanquear instrumentos monetarios- Cualquier persona que sabiendo que la propiedad involucrada en una transacción financiera representa el producto de alguna actividad ilícita, conduce o intenta llevar a cabo dicha transacción financiera que de hecho involucra el producto de una actividad ilegal especificad con la intención de promover el ejercicio de una actividad ilícita determinada; o con la intención de entablar una conducta que constituya una violación de los artículos 7201 ó 7206 del Código de Rentas Internas de 1986; o sabiendo que la transacción está diseñada en su totalidad o en parte- ocultar o disimular la naturaleza, la ubicación, la fuente, la propiedad o el control del producto de una actividad ilícita determinada; o evitar un requisito de notificación de transacciones bajo la ley estatal o federal. Será condenado a una multa de no más de $ 500,000 o el doble del valor de los bienes involucrados en la transacción, cualquiera que sea mayor, o prisión por no más de veinte años, o ambos. A efectos del presente apartado, se considerará que una operación financiera implica el producto de una actividad ilícita determinada si forma parte de un conjunto de transacciones paralelas o dependientes, cualquiera de las cuales implica el producto de una actividad ilícita determinada y todas que son parte de un solo plan o arreglo.

Act,18 U.S.C § 1957(2015) Blanqueo de instrumentos monetarios- Cualquier persona que se involucre intencionalmente o intente realizar una transacción monetaria en una propiedad derivada de un delito de un valor mayor de $ 10,000 y que se derive de una actividad ilegal especificada, será condenado a una multa de no más de $ 500,000 o el doble del valor de los bienes involucrados en la transacción, cualquiera que sea mayor, o prisión por no más de veinte años, o ambos. A efectos del presente apartado, se considerará que una operación financiera implica el producto de una actividad ilícita determinada si forma parte de un conjunto de transacciones paralelas o dependientes, cualquiera de las cuales implica el producto de una actividad ilícita determinada y todas las que son parte de un solo plan o arreglo.

Casos relacionados

U.S. v. Mariely Malavet Rivera (2015):

Según los documentos del caso U.S. v. Mariely Malavet Rivera (2015), la señora Mariely Malavet Rivera se dedicaba a preparar planillas de contribución sobre ingresos y se apropió ilegalmente de $227,653.22. reclamando reintegros federales falsos por concepto de créditos sobre impuestos de niños, con el propósito de obtener reembolsos fraudulentos a través de cheques o depósitos directos.

Robo información de identificaciones personales, incluyendo nombres, fechas de nacimiento y números de Seguro Social estos fueron utilizados, sin el conocimiento de las personas afectadas. En algunas instancias, la acusada obtuvo la información cuando preparó planillas locales de Puerto Rico por una cantidad nominal. Los cargos que presentaron en

su contra incluyen fraude electrónico, robo de dinero público y robo de identidad agravado, por lo que las autoridades federales radicaron 46 cargos en su contra.

U. S. v. John Rusnak (2002):

Según los documentos del caso U.S. v. John Rusnak (2002), en el año 2002, el operador de divisas estadounidense John Rusnak y empleado del banco Allied Irish Bank (AIB), fue acusado de falsificar documentos para encubrir malas inversiones. El banco dijo que, como resultado, perdió US$750 millones. Después de una investigación de cuatro meses, fue acusado formalmente ante un jurado federal.

La fiscalía dijo que Rusnak no se benefició personalmente de las pérdidas, que fueron en su mayoría en transacciones entre el dólar estadounidense y el yen japonés. Según los documentos del caso, él le confesó al FBI que sus deudas se acumularon mientras trataba de concebir una táctica para recuperar el dinero perdido sin tener que admitir a sus jefes el problema inicial. En 2003, fue sentenciado a siete años y medio de prisión, luego de llegar a un acuerdo con la fiscalía.

U.S. v. Miosotis Ribot Figueroa (2015):

Según los documentos del caso U.S. v. Miosotis Ribot Figueroa (2015), la señora Miosotis Ribot Figueroa y el señor José González Guzmán fueron arrestados, por participar en un esquema de fraude bancario y fraude electrónico de aproximadamente $490,165.42.

El matrimonio fue acusado por un Gran Jurado de un total de 79 cargos. Treinta y cuatro cargos fraude electrónico, 34 cargos por fraude bancario y siete cargos por robo de identidad agravada y cuatro cargos adicionales por transacciones monetarias utilizando fondos robados. Asimismo, enfrentaron un cargo de confiscación de $490,165.42, la confiscación de un terreno en Gurabo y de un bote.

La acusación alega que entre mayo a octubre del 2014 Ribot Figueroa efectuó transferencias no autorizadas de las cuentas bancarias de su empleador una compañía de servicios y equipo médico no identificada a cuentas bancarias que la acusada controlaba. Estas transferencias totalizaron $490,165.42.

La acusada quien se desempeñaba como asistente de contralor de la compañía, logró acceso a la red de la empresa para la que trabajaba y accedió al sistema bancario para procesar pagos y transferencias a vendedores y clientes. Se alega que la acusada efectuó unas 34 transferencias para ella y para González Guzmán. Ribot Fernández, sometió facturas falsas y fraudulentas, así como información falsa a un sistema de vales para reflejar que las transferencias bancarias habían sido autorizadas por un supervisor. Para ello, utilizó los nombres y la firma de otras personas.

La pareja también enfrento cuatro cargos por transacciones monetarias derivadas de la actividad ilegal en sobre $10 mil. Estas transacciones ascienden los $75,406.82.

De ser encontrados culpables Ribot Fernández se expone a ser sentenciada a un máximo de 30 años por el fraude bancario, fraude electrónico y por las transacciones monetarias y dos años mandatorios consecutivos por robo de identidad agravado. Mientras,

que González Guzmán enfrenta penas de hasta diez años de prisión.

Herramientas de Investigación:

Según Porolli (2017), el análisis forense digital corresponde con un conjunto de técnicas destinadas a extraer información valiosa de discos, sin alterar el estado de los mismos. Esto permite buscar datos que son conocidos previamente, tratando de encontrar un patrón o comportamiento determinado, o descubrir información que se encuentra oculta.

En el campo de la Informática Forense existen diversas etapas que definen la metodología a seguir en una investigación: identificación, preservación o adquisición, análisis y presentación de los resultados. Siguiendo el flujo lógico de actividades, primero se debe identificar las fuentes de datos a analizar y aquello que se desea encontrar, luego se debe adquirir las imágenes forenses de los discos o fuentes de información, posteriormente se realiza el análisis de lo adquirido para extraer información valiosa y finalmente se ordenan los resultados del análisis y se presentan, de tal modo que resulten útiles.

A continuación, se detallan las herramientas tecnológicas utilizadas para resolver el caso en cuestión:

1. **Forensic Toolkit**, o FTK- es un "software" de análisis informático forense diseñado leer y rastrear un disco duro en busca de diversa información a través del cual se puede localizar correos electrónicos eliminados y analizar una cadena de texto para utilizarlos como diccionario y así poder descifrar contraseñas. (AccessData,2017)

2. FTK Imager -una herramienta en la cual se guarda la imagen de un disco duro en un archivo o en segmentos que posteriormente pueden ser reconstruida. Además, permite

calcular los valores de "*hash MD5"* y confirma la integridad de los datos antes de cerrar los archivos. (AccessData,2017)

3. AccessData Registry Viewer- es un programa que le permite ver el contenido de los registros del sistema operativo *Windows. Registry Viewer* le da acceso al almacenamiento protegido de un registro. El almacenamiento protegido puede contener contraseñas, los nombres de usuario, y otra información que no es accesible en el editor de Registro de *Windows*. (AccessData, 2014)

SECCIÓN 3: SIMULACIÓN

En esta sección se estará simulando el esquema de fraude mediante un diagrama explicativo de como el señor Yoandy Pérez Llanes y varios de sus conspiradores desde Venezuela, atacaron la base de datos de la University of Pittsburgh Medical Center (UPMC) robaron los datos personales de sus empleados y los usaron para presentar declaraciones de impuestos falsas.

Yoandy y sus conspiradores utilizaron servidores *proxy* para que pareciera que las solicitudes de reembolso de impuestos se presentaban en el oeste de Pennsylvania, también utilizaron servicios de correo electrónico anónimos para obtener los códigos de canjes de reembolsos del IRS, a través del *software* Turbo Tax.

Por petición de Yoandy, $885,578.00 dólares fueron rembolsados y depositados en *gift cards* de Amazon.com. Las *gift card*s fueron utilizadas en la compra de cientos de artículos electrónicos tales como: teléfonos celulares Galaxy IV, iPhones, ordenadores portátiles HP, tabletas, dispositivos de juego y otros productos electrónicos en Amazon.com.

Todos los artículos adquiridos en Amazon.com eran enviados a una dirección postal en Miami, donde miembros del grupo de Yoandy los recibían, re empacaban y los reenviaban a Maracay, Venezuela para luego venderlos en sitios *web* de subastas en línea, según los documentos del caso. (Ver figura 3)

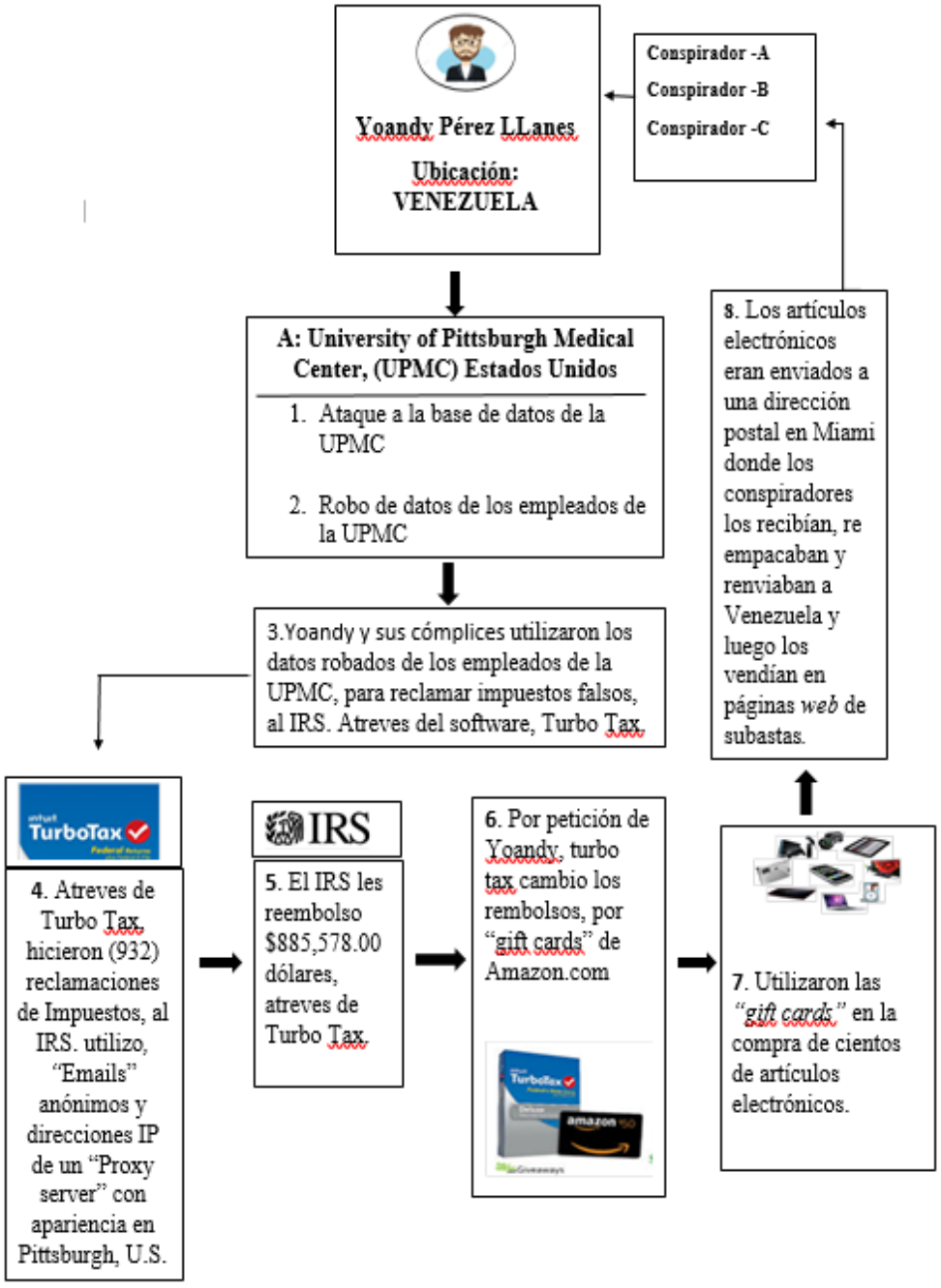


Figura 3: Esquema de fraude realizado por Yoandy Pérez LLanes

SECCIÓN 4: INFORME DEL CASO

Resumen Ejecutivo

El agente Robert Kickbush, del la agencia federal de Servicio de Rentas Internas (IRS, por sus siglas en inglés) del Gobierno de los Estados Unidos y el Fiscal Federal David Hickton, del FBI hacen entrega a la investigadora Yashira Gómez Narváez de YGN Investigation Forensic un *USB* marca SanDisk Cruzer Blade de 8gb se identifica como: A-1-2015-1. Este dispositivo fue encontrado en el pantalón del acusado Yoandy Pérez Llanes el día 26 de junio de 2015 cuando fue puesto bajo arresto, este mismo día el *USB* quedo bajo la custodia del FBI. Esto con el propósito de analizar la información contenida en el mismo y evidenciar un esquema de fraude al IRS y el robo de datos de los empleados de la UPMC.

El proceso del análisis forense que llevaré a cabo al *USB* implica la adquisición, conservación, análisis y presentación de evidencia digital. Este tipo de pruebas es frágil y el investigador puede, sin darse cuenta, alterar o destruir la información en cualquier dispositivo que se está analizando. La consecuencia de esto es que la evidencia se vuelve inadmisible en los tribunales. Para minimizar la posibilidad de que esto ocurra YGN Investigation Forensics, utiliza el Electronic Data Recovery para así obtener la evidencia propiamente preservada, y confiable.

Un grupo de empleados de la (Universidad de Pittsburgh Medical Center) UPMC del estado Pensilvania, U.S. alertaron al Servicio de Rentas internas Federal (IRS, por sus siglas en inglés) de que no habían sido ellos los que reclamaron unos impuestos del año 2013, luego de que el IRS les enviaran avisos, notificándoles que ya habían recibido las

devoluciones de sus impuestos y que por consiguiente se habían emitido los rembolsos del año 2013.

Después de la alerta que dieron los empleados, el IRS rápidamente sospecha que fueron víctimas de fraude, por lo que comienzan una investigación, junto a la oficina del (Federal Bureau Investigation) FBI.

Al concluir el análisis de la evidencia del dispositivo *USB* se encontraron documentos de Word, tablas de Excel, imágenes personales que vinculan al señor Yoandy Pérez LLanes, con los hechos de los cuales se le acusa.

Objetivo

El objetivo del análisis que se le realizara *al USB,* es para investigar, descubrir y recuperar información que vincule al sospechoso con la reclamación de unos impuestos y reembolsos de miles de dólares al Servicio de Rentas Internas de los Estados Unidos.

Alcance del trabajo

El proceso del análisis forense que llevare a cabo al *USB* implica la adquisición, conservación, análisis y presentación de evidencia digital. El proceso de esta investigación estará dirigido en analizar los archivos, documentos y toda la información que el *USB* almacene con este proceso se busca recuperar evidencia que vincule a Yoandy Pérez LLanes y sus cómplices con el esquema de fraude cometido contra el IRS y la UPMC.

Durante el proceso del análisis se utilizó las siguientes herramientas:

- FTK 3.2.0.0
- FTK Imager
- Acces Data Registry

Datos del caso

Esta investigación estará enfocada en el análisis del *USB* para lograr obtener evidencia que vinculen al sospechoso con el fraude cometido contra el Servicio de Rentas Internas (IRS, por sus siglas en inglés). Se empezará por analizar, el contenido almacenado en la base de datos del dispositivo, también los *folders* y documentos que haya en esta, si es que contiene.

Número del Caso: A-1-2015-1

Examinador: Yashira Gómez Narváez

Cliente: IRS, Departamento de Justicia del Estado de Pittsburgh, FBI.

Investigador de Caso: El agente Robert Kickbush, del IRS y el Fiscal Federal David Hickton del FBI.

Descripción de los dispositivos utilizados

Los dispositivos utilizados en esta investigación son:

1.*Laptop Lenovo Modelo Ideapad 100* Memoria *RAM* de 8.0 esta máquina se utiliza exclusivamente para realizar análisis e investigaciones y no se encuentra conectada a ninguna red.

Figura 4: Especificaciones del sistema operativo de la laptop “Lenovo Ideapad 100”.

2. El otro dispositivo utilizado es el *USB, SanDisk 2.0 GB,* color negro y rojo tomado como evidencia, el cual será analizado.

Figura 5: *USB, SanDisk* 2.0 GB evidencia: A-1-2015-1

Resumen de Hallazgos

- Tres Doc. de Word con declaraciones de impuestos
- Dos tablas de Excel con información de empleados de la UPMC
- Cuatro imágenes del proceso de Turbo Tax en los rembolsos de impuestos
- Una imagen de una factura electrónica de la compra de dispositivos electrónicos.
- Dos fotos de Yoandy Pérez LLanes

Cadena de Custodia

Desde el comienzo de la investigación, se estableció una cadena de custodia de la evidencia entregada para la investigación un *'USB"* identificado como: A-1-2105-1. La cadena de custodia ayuda a que se legalice el proceso de adquisición, análisis y control de toda la evidencia. Próximamente, se observará la cadena de custodia que siguió YGN Investigation Forensics.

Primer Evento

Descripción del Evento: El agente Robert Kickbush, del IRS y David Hickton del FBI, pusieron a mi disposición el *USB* para ser analizado.

Personas Presentes: Robert Kickbush, David Hickton y Yashira Gómez Narváez

- Numero de Evidencia: A-1-2015-1
- Fecha de Comienzo: 28 de junio de 2015 a las 8:00 a.m.
- Fecha de Terminación: 28 de junio de 2015 a las 10:30 a.m.
- Lugar de Origen: Oficina del Fiscal Federal, David Hickton
- Destino: Laboratorio Forense - YGN Investigation Forensics

Segundo Evento

Descripción del Evento: Creación del número de caso y asignación de la evidencia.

- Personas Presentes: Yashira Gómez Narváez
- Numero de Evidencia: A-1-2015-1 Asignado al caso No. 15-141 Pittsburgh
- Fecha de Comienzo: 28 de junio de 2015 a las 11:00 a.m.

- Fecha de Terminación: 28 de junio de 2015 a las 3:00 p.m.
- Lugar de Origen: YGN Investigation Forensics
- Destino: Laboratorio Forense – YGN Investigation Forensics

Tercer Evento

Descripción del Evento: Proceso de adquisición y análisis de evidencia.

- Personas Presentes: Yashira Gómez Narváez
- Numero de Evidencia: A-1-2015-1 – Asignado al caso No. 15-141 Pittsburgh
- Fecha de Comienzo: 29 de junio de 2015 a las 8:00 a.m.
- Fecha de Terminación: 29 de junio de 2015 a las 9:00 p.m.
- Lugar de Origen: Laboratorio Forense – YGN Investigation Forensics
- Destino: Laboratorio Forense – YGN Investigation Forensics

Cuarto Evento

Descripción del Evento: Entrega del reporte de análisis forense a El agente Robert Kickbush, del IRS y David Hickton del FBI. Personas Presentes: Yashira Gómez Narváez, el agente Robert Kickbush, del IRS, David Hickton del FBI y 4 agentes del FBI.

- Numero de Evidencia: A-1-2015-1 – Asignado al caso No. 15-141 Pittsburgh
- Fecha de Comienzo: 30 de junio de 2015 a las 8:00 a.m.
- Fecha de Terminación: 30 de junio de 2015 a las 5:15:20 p.m.
- Lugar de Origen: Laboratorio Forense – YGN Investigation Forensics
- Destino: Oficina del Fiscal Federal, David Hickton

Quinto Evento

Descripción del Evento: Entrega de la evidencia original sometida, por el agente Robert Kickbush, del IRS y David Hickton del FBI.

Personas Presentes: Yashira Gómez Narváez, el agente Robert Kickbush, del IRS, David Hickton del FBI y 4 agentes del FBI.

- Personas Presentes: Yashira Gómez Narváez
- Numero de Evidencia: A-1-2015-1– Asignado al caso No. 15-141 Pittsburgh
- Fecha de Comienzo: 31 de junio de 2015 a las 8:30 a.m.
- Fecha de Terminación: 31 de junio de 2015 a las 3:00 p.m.

- Lugar de Origen: Laboratorio Forense - YGN Investigation Forensics
- Destino: Oficina del Fiscal Federal, David Hickton

Procedimiento

Este proceso del analisis fue realizado, por Yashira Gomez Narvaez investigadora del caso teniendo en cuenta la cadena de evidencia, la preservación de cada hallazgo y que cada dato obtenido es confidencial. A continuación, veremos el proceso detallado.

El analisis de la evidencia se llevara a cabo con la herramienta *Forensic Toolkit*.

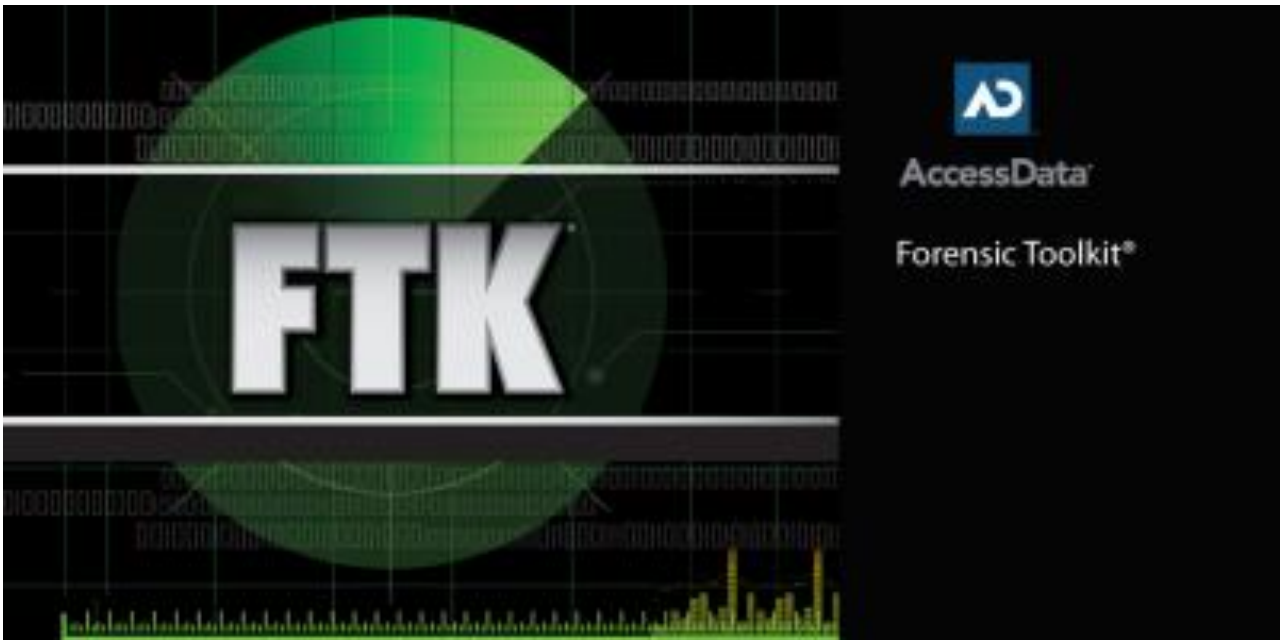


Figura 6: Herramienta *Forensic Toolkit*

En la siguiente figura comenzamos escribiendo la información para la creación del caso.

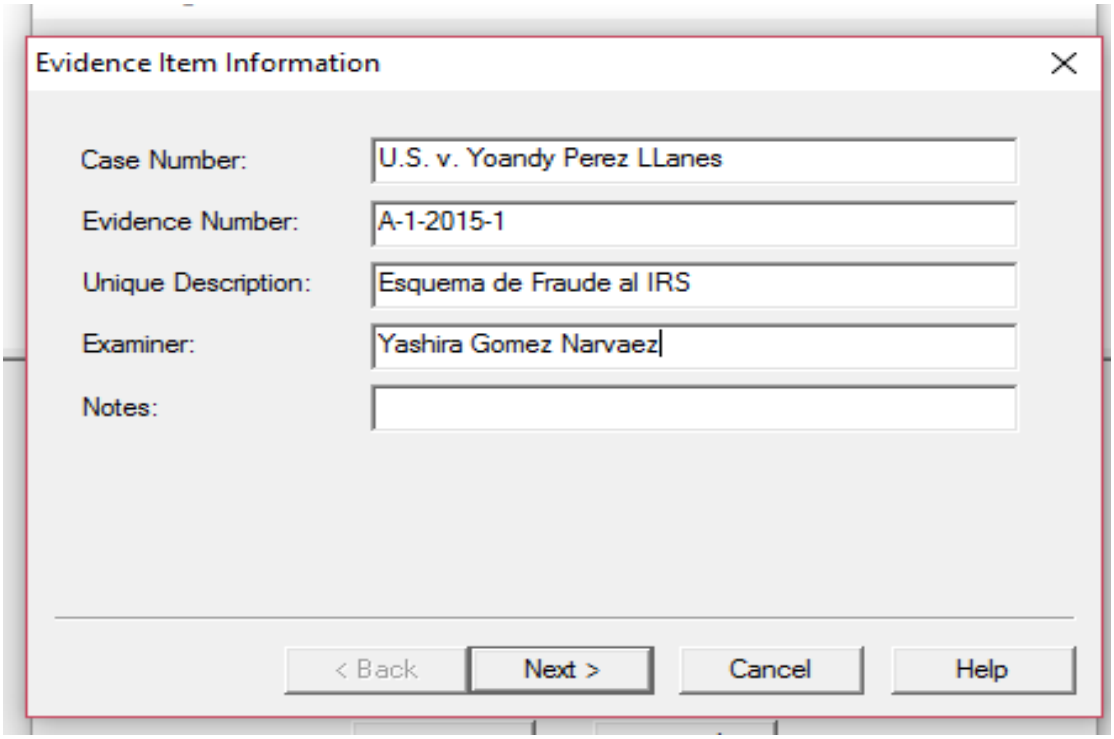


Figura 7: Creación del caso

En la figura 8 se seleccionó el dispositivo que se va a examinar.

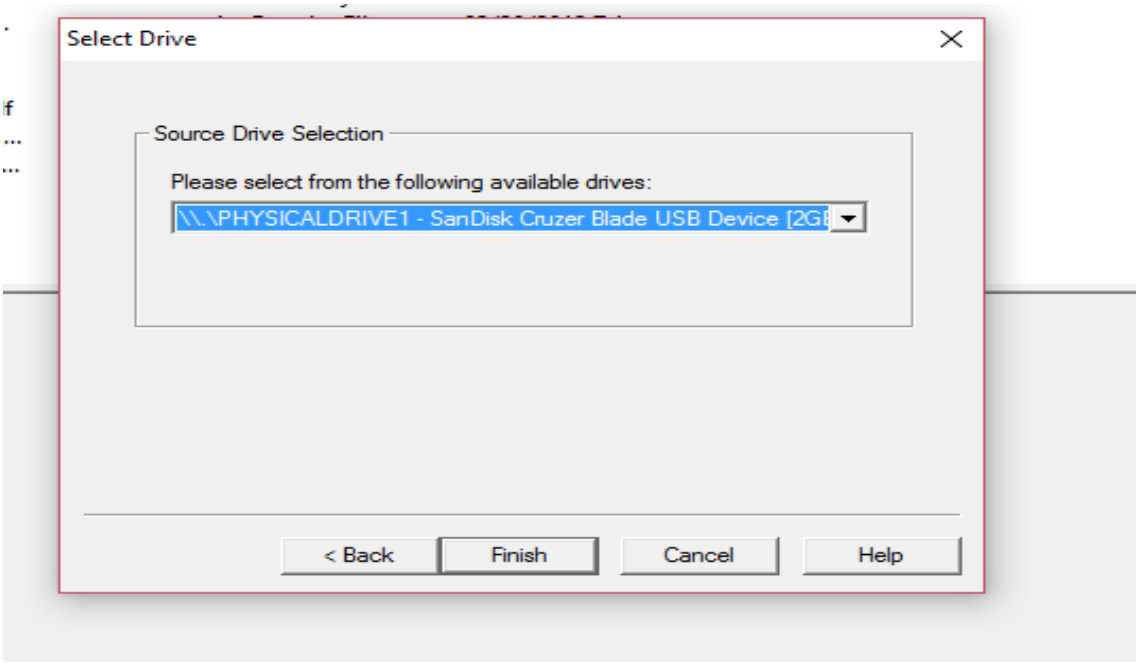


Figura 8: Selección del *USB* a examinar

En la figura 9 se comenzó el análisis y la creación de la imagen del *USB.*

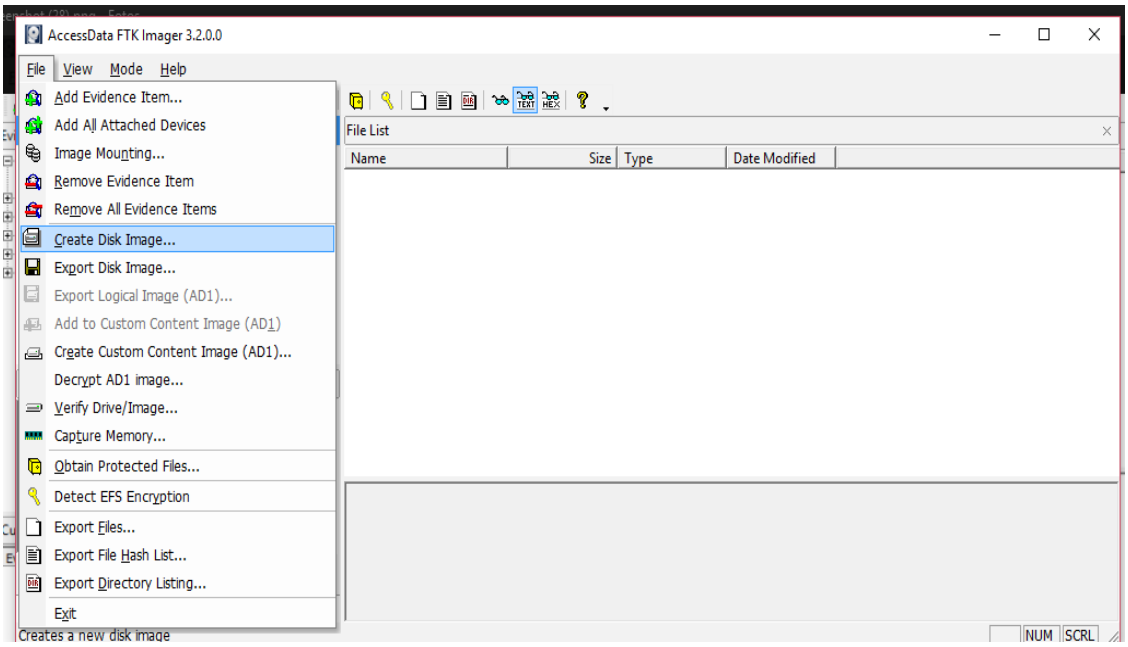


Figura 9: Proceso para crear imagen de la evidencia

En la figura 10 se verifican los archivos y se convierte la imagen de estos.

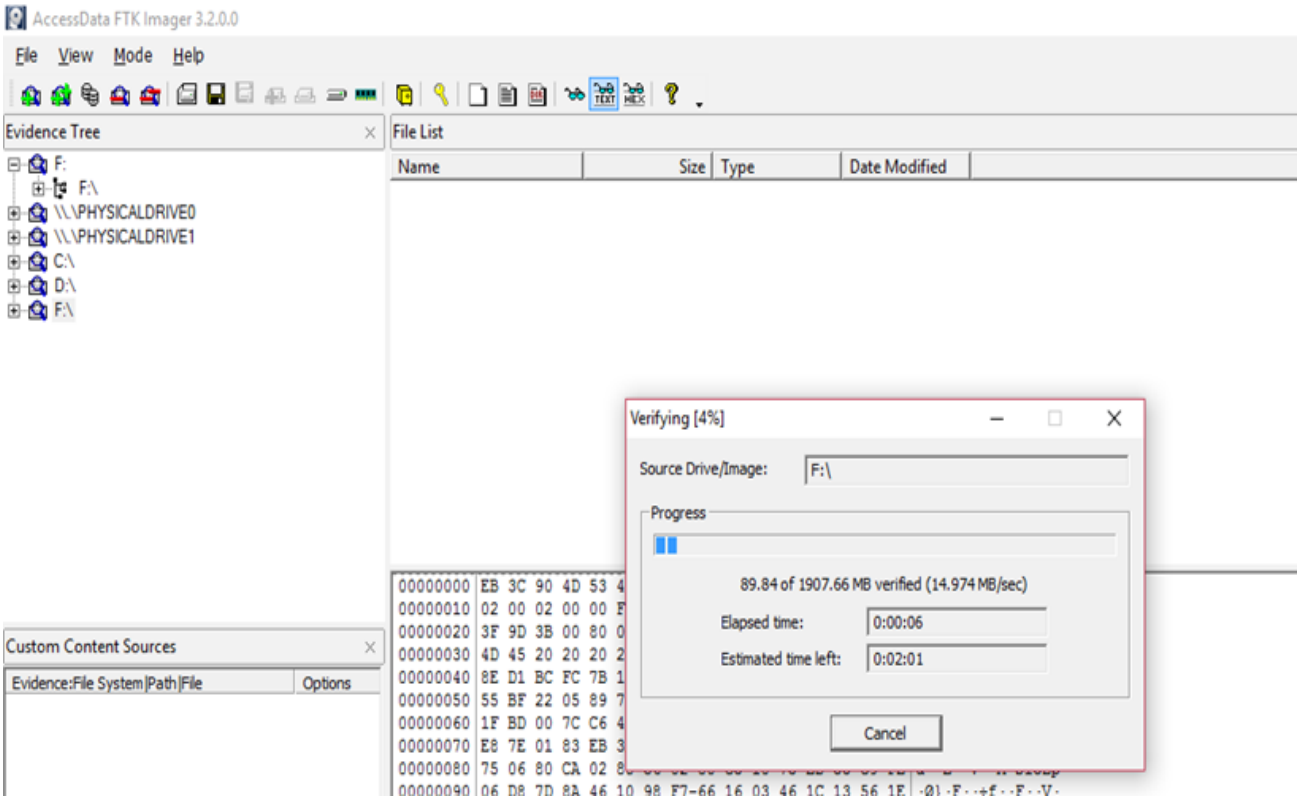


Figura 10: Verificación y conversión de los archivos.

La figura 11 presenta el proceso en el que la herramienta detectó (15) archivos guardados en el *USB* algunos con el nombre de Yoandy Pérez LLanes, otros con el nombre de Turbo Tax *y* otros archivos que trae el *USB.*

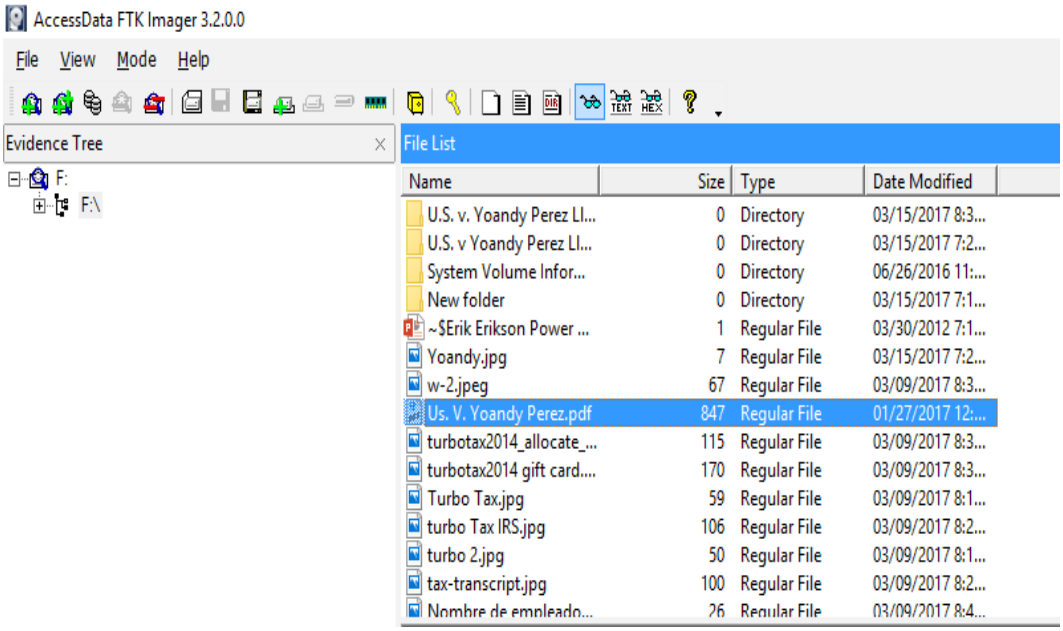


Figura 11: Imagen de documentos detectados en el *USB*

La imagen 12 presenta el proceso en el cual la herramienta buscó y no detectó ningun archivo cifrado.

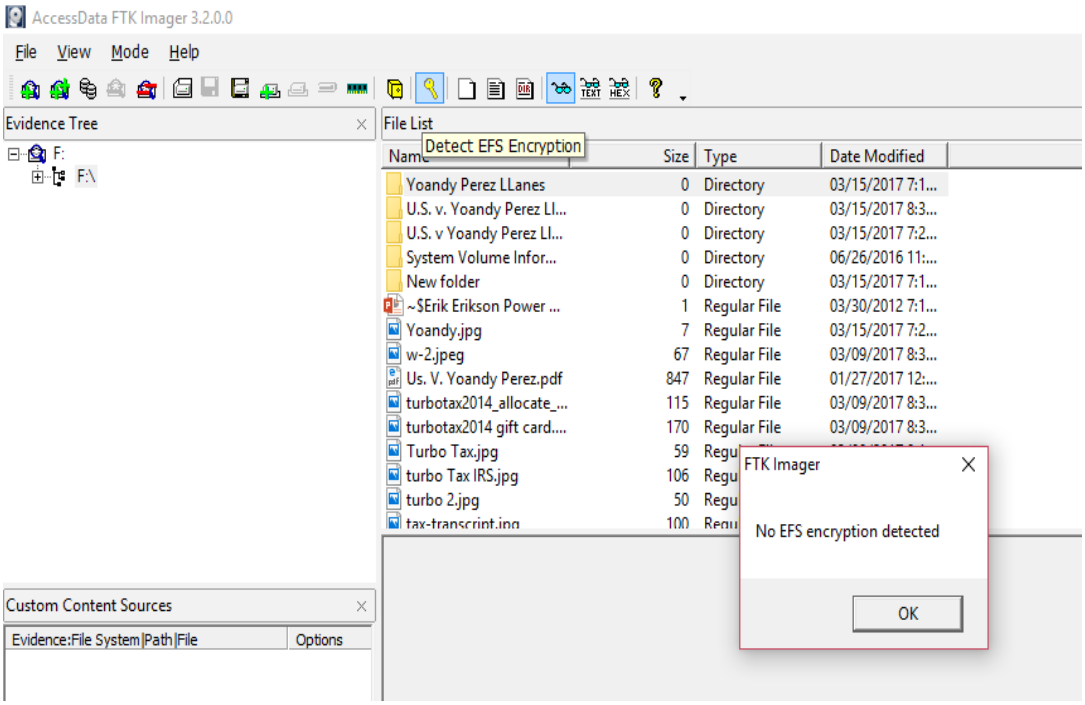


Figura 12: proceso en el que se buscaron archivos cifrados

En esta imagen la herramienta localizó un documento de Excel, el cual contenia informacion personal de varias personas. Todos empleados de la Universidad de Pittsburgh Medical Center (UPMC). (Ver figura 13)

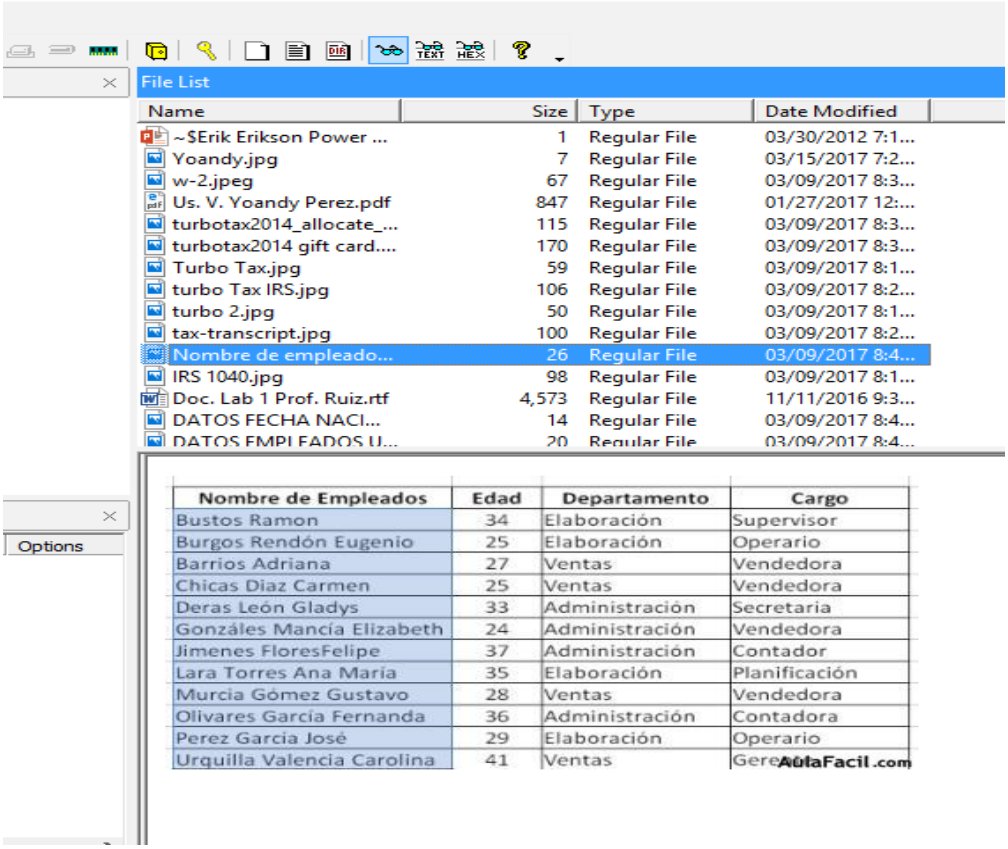
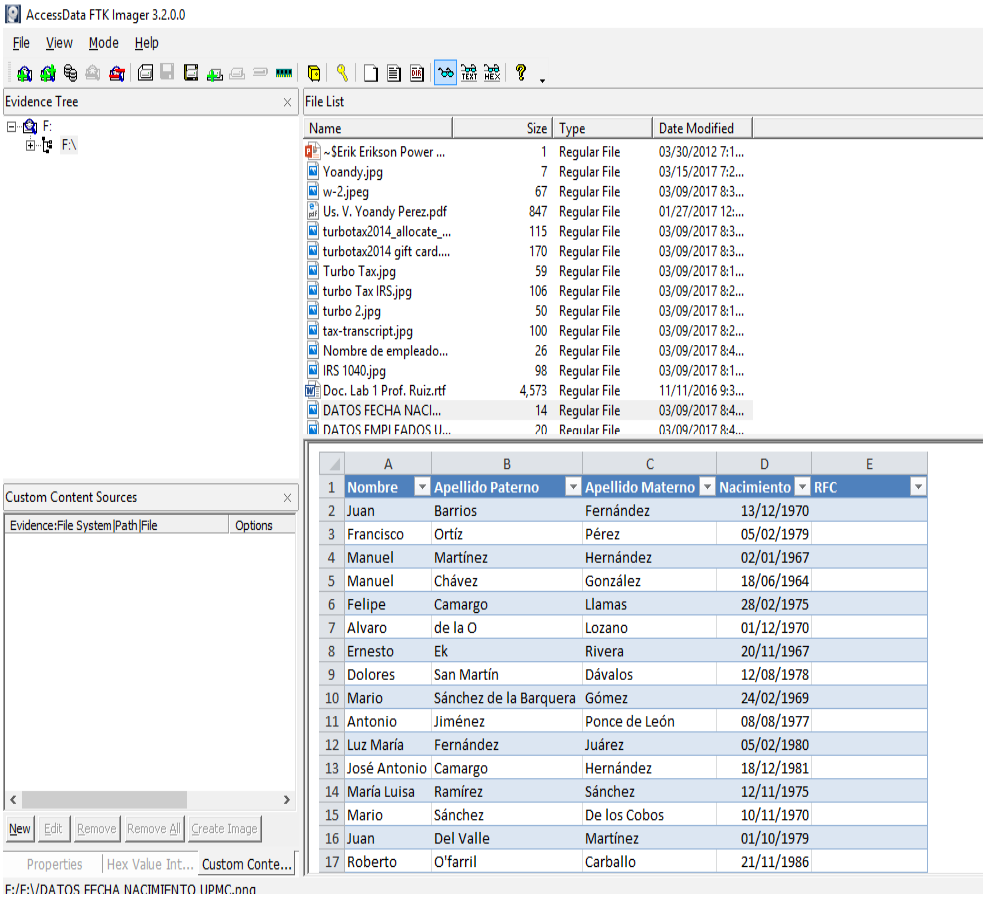


Figura 13: Tabla de Excel con información personal de empleados de la UPMC

Se encontró un segundo documento de Excel que contenía nombres, apellidos, y fechas de nacimientos de empleados de la UPMC. (ver figura 14)



	A	B	C	D	E
1	Nombre	Apellido Paterno	Apellido Materno	Nacimiento	RFC
2	Juan	Barrios	Fernández	13/12/1970	
3	Francisco	Ortíz	Pérez	05/02/1979	
4	Manuel	Martínez	Hernández	02/01/1967	
5	Manuel	Chávez	González	18/06/1964	
6	Felipe	Camargo	Llamas	28/02/1975	
7	Alvaro	de la O	Lozano	01/12/1970	
8	Ernesto	Ek	Rivera	20/11/1967	
9	Dolores	San Martín	Dávalos	12/08/1978	
10	Mario	Sánchez de la Barquera	Gómez	24/02/1969	
11	Antonio	Jiménez	Ponce de León	08/08/1977	
12	Luz María	Fernández	Juárez	05/02/1980	
13	José Antonio	Camargo	Hernández	18/12/1981	
14	María Luisa	Ramírez	Sánchez	12/11/1975	
15	Mario	Sánchez	De los Cobos	10/11/1970	
16	Juan	Del Valle	Martínez	01/10/1979	
17	Roberto	O'farril	Carballo	21/11/1986	

Figura 14: documento con información de empleados de la UPMC

En la figura 15 se encontró la Forma 1040 del Servicio de Rentas Internas, (IRS) este es uno de los tres formularios que puedes utilizar para presentar tu declaración de impuestos federales sobre la renta atreves del *software* Turbo Tax.

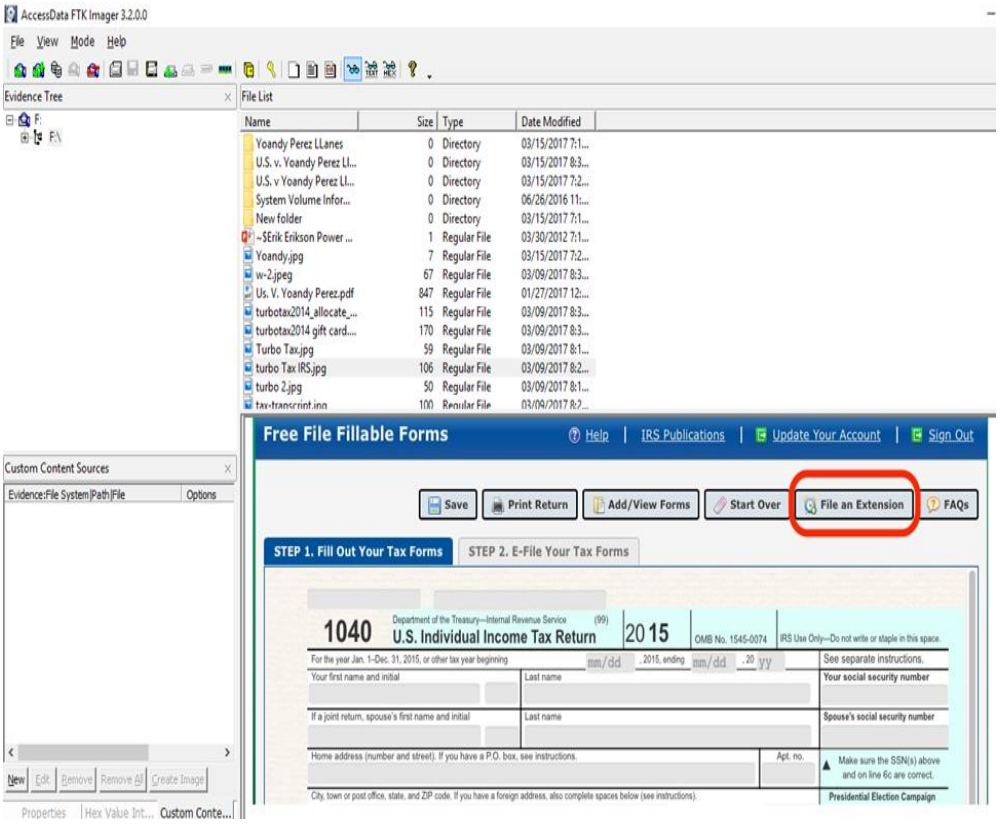


Figura 15: Plantilla 1040 del IRS

En la figura 16 se ve una segunda página de la forma 1040 del IRS, en el cual claramente se ve el reclamo de $23,737 dólares en rembolsos de impuestos.

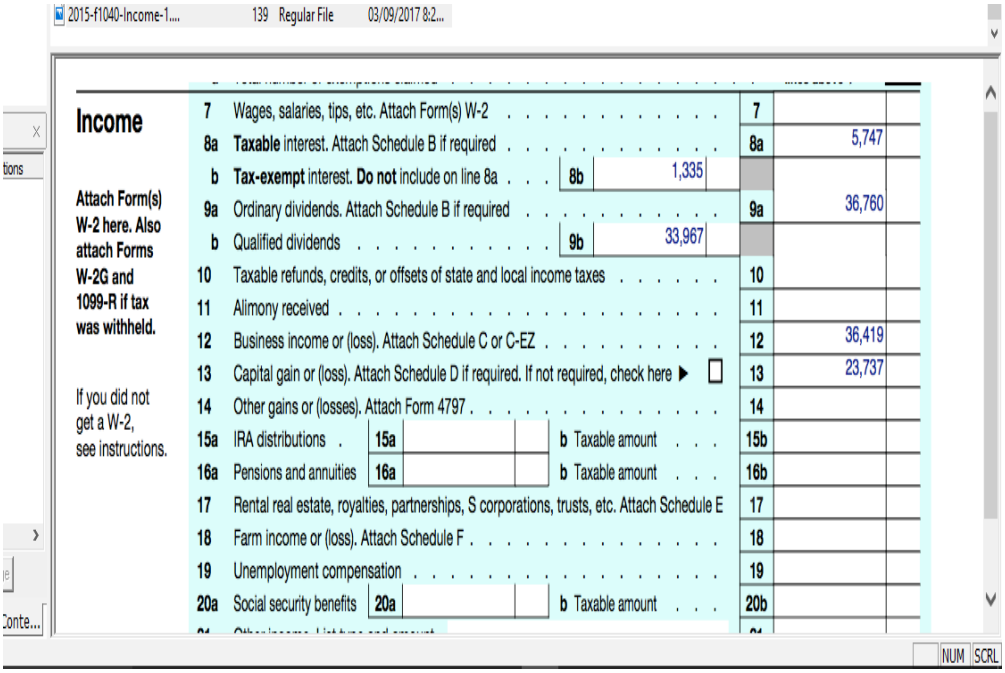


Figura 16: Segunda página de la forma 1040 del IRS.

En la figura 17 se ve un documento de una transcripción de *taxes* del IRS con información sobre rembolsos de impuestos a nombre de uno de los empleados del IRS.

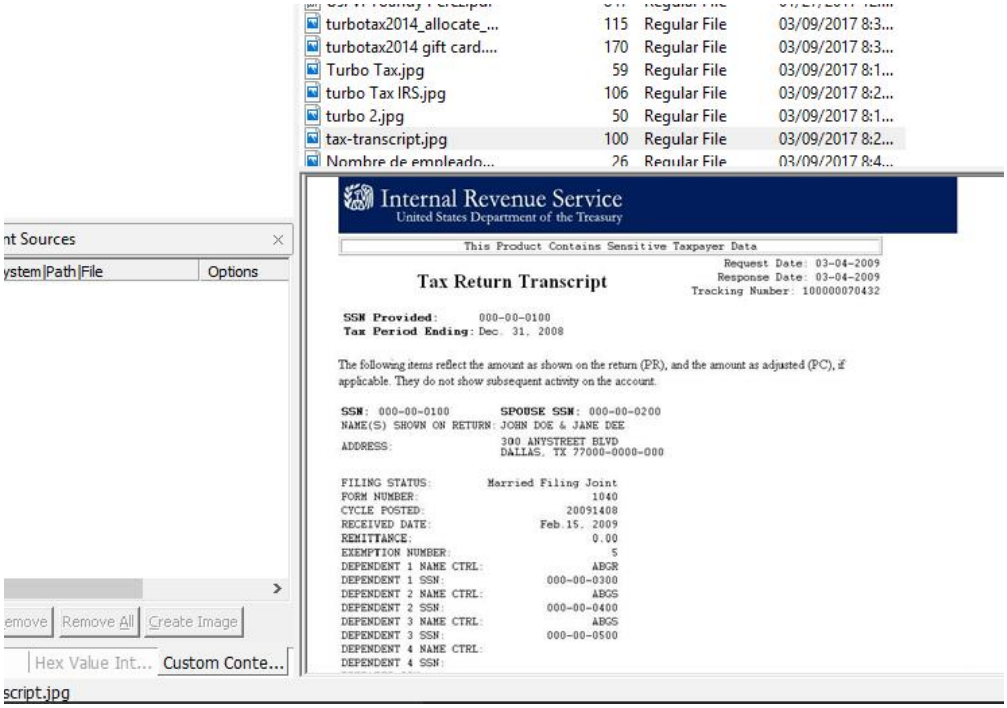


Figura 17: Documento sobre la transcripción de *taxes* del IRS

.

Se encontró un rembolso del *software* Turbo Tax con la cantidad de $2,345.01 dólares el cual decía “welcome home”. (Ver figura 18)

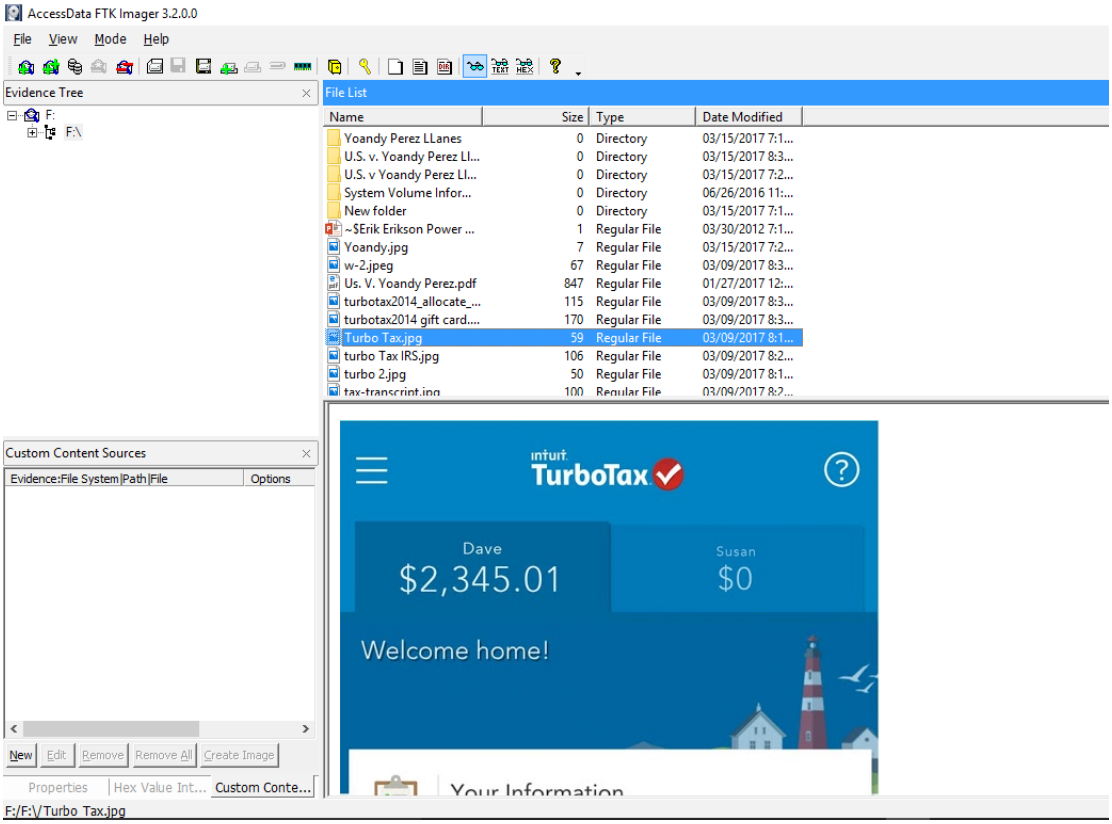


Figura 18: Imagen de reembolso en *Turbo Tax.*

.

La figura 19 muestra un rembolso de $2,889.00 dólares y el proceso del cambio del rembolso a una *gift cards* de amazon.com.

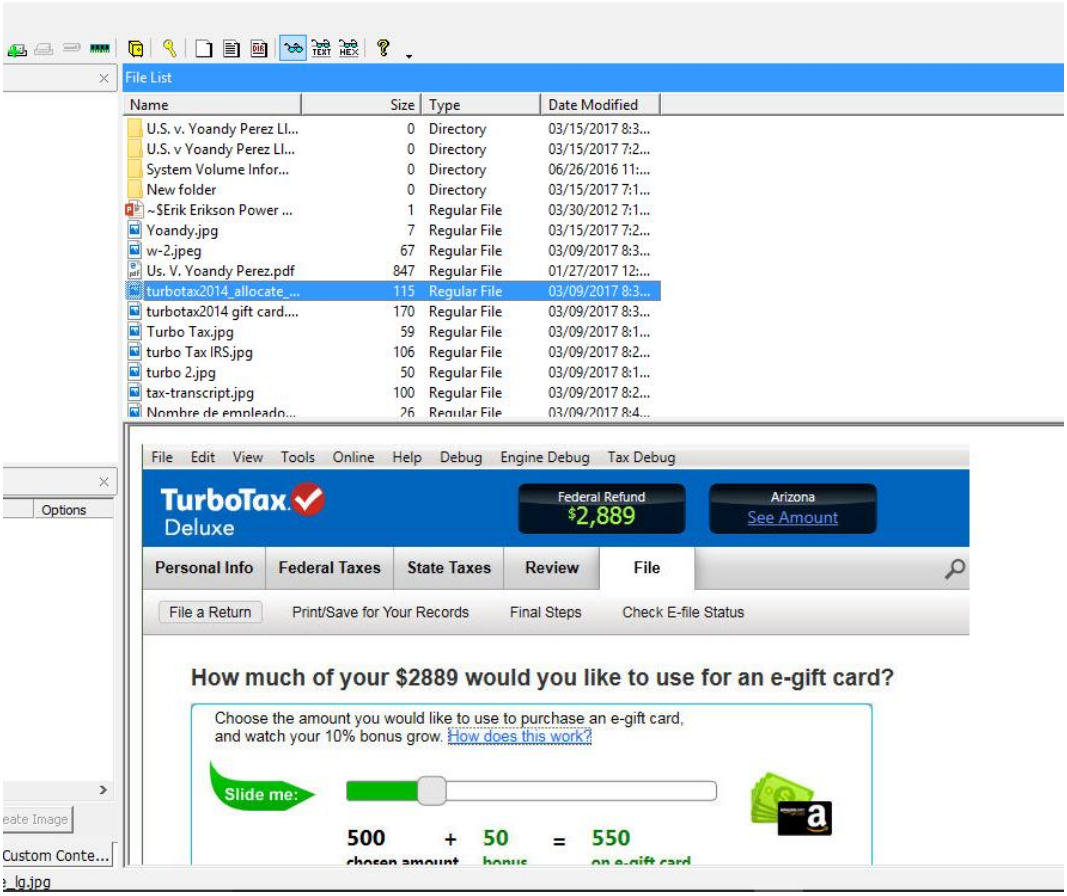


Figura19: Proceso de cambio del rembolso a una *gift cards* de Amazon.

La figura 20 muestra una factura por la cantidad de $877.90 dólares de la compra de unos dispositivos electrónicos realizados en amazon.com

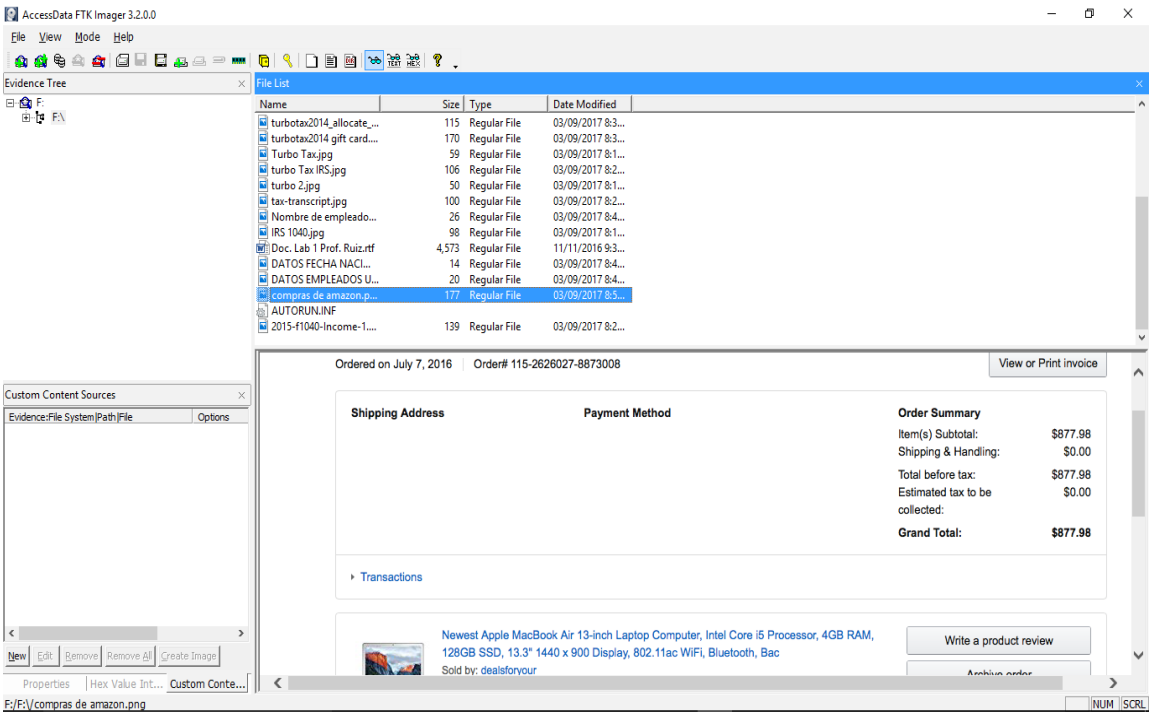


Figura 20: Imagen de la factura de unas compras en amazon.com

La figura 21 muestra varios de los dispositivos electrónicos comprados en Amazon.

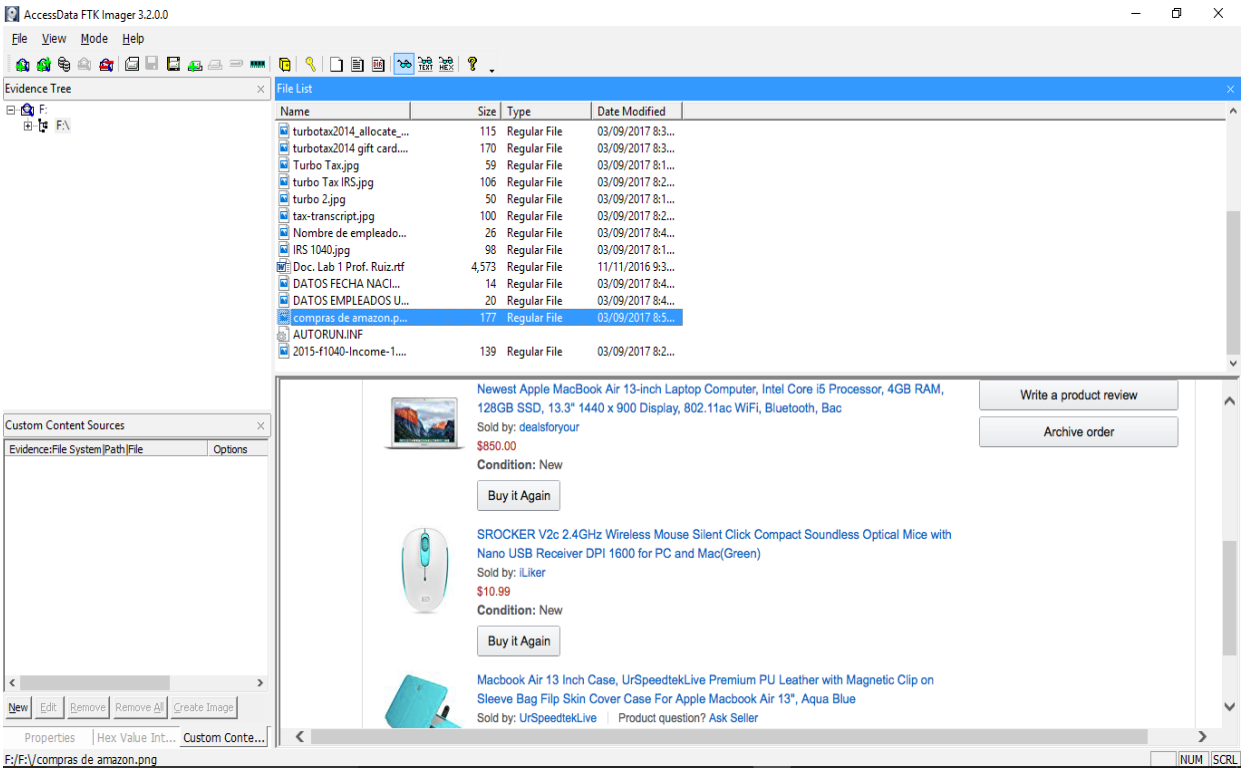


Figura 21: Dispositivos electrónicos comprados en Amazon

En este proceso se encontraron dos fotos de Yoandy Pérez LLanes guardadas en un documento del *USB* analizado. (ver figura 22)

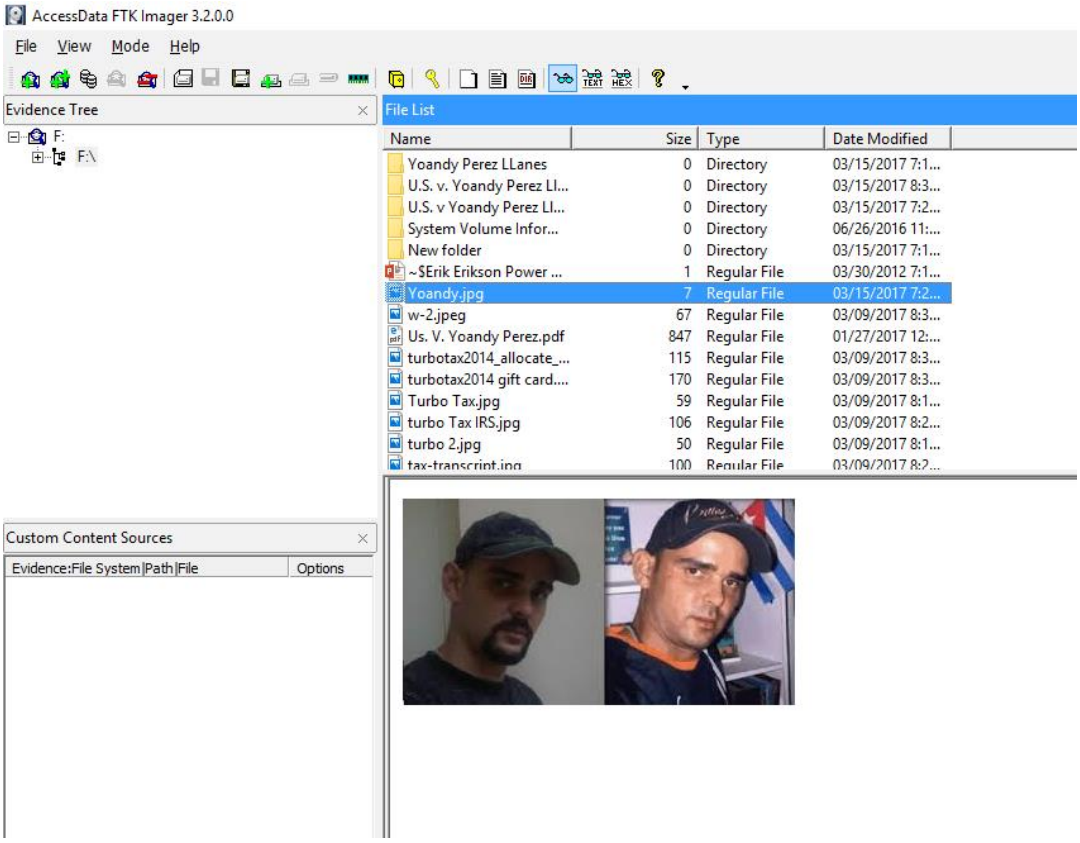


Figura 22: Dos fotos personales de Yoandy Pérez LLanes encontradas en el *USB*

Conclusión

De acuerdo con los resultados que se obtuvieron en la investigación realizada se puede establecer un vínculo entre el acusado en el esquema de fraude. Se identifican hallazgos pertinentes para establecer un caso ante la corte y esclarecer los delitos de los que se le acusa.

Cabe señalar que como parte de esta investigación se analizó el *USB* propiedad de Yoandy Pérez LLanes y se encontraron varios documentos del IRS, Turbo Tax, y dos

listas con información personal de los empleados de la UPMC, así como también se encontraron dos fotos de Yoandy.

Para concluir con esta investigación se establece que la evidencia obtenida no fue alterada en ningún momento y que se siguió todo el procedimiento de la cadena de custodia. Certificamos que el proceso de manejo de la evidencia cumple o excede los estándares establecidos por el gobierno federal de los Estados Unidos y las prácticas de los estándares de la industria forense digital.

SECCIÓN 5: DISCUSIÓN DEL CASO

En este caso el Fiscal Federal, David Hickton con 20 años de experiencia como Fiscal Federal en el Tribunal Federal del estado de Pensilvania, se valió de su experiencia, credibilidad y expertise para presentar toda la prueba posible contra el acusado y así demostrar en corte causa probable contra Yoandy Pérez Llanes.

Como parte de la investigación, se llevó a cabo un análisis forense de un *USB* que se le ocupó, al acusado en el bolsillo de su pantalón en el momento de su arresto en Maracaibo, Venezuela. Dicha prueba concluyó que el acusado era el autor del fraude contra el Servicio de Rentas Internas (IRS, por sus siglas en inglés) y de montar una red de estafa entre Venezuela y Miami, para enviar declaraciones de impuestos falsas, que solicitaban los reembolsos por un total de 2.2 millones de dólares, usando datos robados del personal del Centro Médico de la Universidad de Pittsburgh.

Un mes después de su arresto y recluido en una prisión federal en Pittsburgh, Estados Unidos, el FBI le levantó 14 cargos a Yoandy Pérez LLanes, por haber defraudado al Servicio de Rentas Internas (IRS, por sus siglas en inglés) y por haber robado los datos personales de los empleados de la Universidad de Pittsburgh Medical Center, (UPMC).

El acusado está en espera de ser sentenciado y se expone a una pena de más de 20 años de prisión.

SECCIÓN 6: AUDITORÍA Y PREVENCIÓN

Todos los días son publicados artículos en los periódicos y en Internet de fraudes en compañías y/o agencias, se informa que el fraude puede pasar en cualquiera de estas. Los fraudes provocan daños materiales que se evalúan en cientos de miles y, en algunos casos, hasta en millones de pesos, sin mencionar los efectos secundarios que esto provoca. Es por esto que las compañías y/o agencias deberían tener la instrumentación necesaria, un protocolo que la dirección pueda seguir y mantenerse a la vanguardia con las nuevas tecnologías para que pueden enfrentar el riesgo al fraude. Esto puede ser una práctica deseable para todas las compañías, especialmente en aquéllas que fomentan la conciencia del control interno, ya que estas prácticas ayudan a mitigar el riesgo de fraude.

Después de haberse descubierto el esquema de fraude cometido, por Yoandy Pérez LLanes y sus cómplices caso U.S. v. Yoandy Pérez LLanes (2015), el acusado encontró la oportunidad para cometer el fraude en un sistema vulnerable, violo la seguridad de la base de datos del sistema de la Universidad de Pittsburgh Medical Center (UPMC) y extrajo, la información personal de cientos de empleados de dicha organización. Luego de esto burlo los controles de los sistemas del Servicio de Rentas Internas (IRS, por sus siglas en inglés) he hiso cientos de reclamaciones falsas de impuestos del Servicio de Rentas Internas atreves de un *software* llamado Turbo Tax.

El IRS es una agencia federal que desde 1862, es la encargada de la recaudación fiscal y de los cumplimientos de las leyes tributarias. Constituye una agencia encuadrada en el Departamento de Tesorería de los Estados Unidos y también es responsable de la interpretación y aplicación de las leyes fiscales de carácter federal.

Según el IRS, (2017) Los esquemas de fraude contra esta agencia aumentaron considerablemente desde el 2013. Debido a estos aumentos y al esquema de fraude cometido, por Yoandy Perez LLanes en el caso U.S. v. Yoandy Pérez LLanes (2015), se le recomienda a esta agencia llevar a cabo auditorías internas en las operaciones de sus Centros de Sistemas de Información constantemente, también se le recomienda hacer auditorías a la UPMC en sus centros de cómputos constantemente.

I. Recomendaciones al IRS:

Pruebas internas y análisis de los documentos que se encuentran almacenados en la base de datos constantemente.

Hallazgos y Controles Recomendados:

1. Hallazgo: Según los hechos los individuos hicieron reclamaciones de impuestos a través de Turbo Tax este *software* con su sistema hace el trabajo, por sí mismo. Hace preguntas bien simples, arregla los errores y hasta hace los cálculos, sin ningún tipo de control en su sistema.

a. Control Recomendado: Establecer una ley que prohíba este tipo de *software* para que solo la agencia del IRS con su sistema sea quien haga las reclamaciones de impuesto de cada individuo.

2. Hallazgo: Al ver como Yoandy y sus cómplices accesaron e hicieron estas reclamaciones de impuestos tan fácilmente a través de un *software* vemos que el IRS permite el acceso no autorizado sin ningún tipo de control de estos softwares.

a. Control Recomendado: Establecer un control de seguridad de codificación para prevenir acceso no autorizado de softwares que acceden ilegalmente y que se actualice automáticamente para cuando surjan amenazas.

3. Hallazgo: Por lo que se puede ver de esta investigación el IRS no mantiene un registro de servicios de los programas y los equipos de la red que entran a sus sistemas para hacer las reclamaciones de impuestos que presentan problemas y amenazas. Tampoco cuentan con un plan de mantenimiento.

a. Control Recomendado 1: Establecer un registro de servicios de los programas y los equipos de la red que entran a sus sistemas que presentan problemas y amenazas.

b. Control Recomendado 2: Establecer un plan para el mantenimiento preventivo de los equipos computadorizados conectados a la red y que el mismo incluya un itinerario de limpieza rutinario.

4. Hallazgo: No cuentan con un control para los correos electrónicos no identificados**.**

a. Control Recomendado: Establecer un control en el sistema operativo que restrinja el acceso a los correos electrónicos no identificados.

5. Hallazgo: No cuentan con un control que restrinja el acceso de ordenadores con direcciones IP fuera de los Estados Unidos.

a. Control Recomendado 1: Establecer un control que detecte y restrinja automáticamente las direcciones IP que estén fuera de los Estados Unidos.

b. Control Recomendado 2: Restringir el acceso a toda dirección de IP de los ordenadores que parezcan sospechosas.

5. Hallazgo: Deficiencias en los parámetros de seguridad de los servidores del IRS para controlar las cuentas de acceso a los recursos de la red.

a. Control Recomendado1: Requerir un mínimo de cinco contraseñas diferentes antes de volver a utilizar la misma.

b. Control Recomendado 2: Requerir que las contraseñas fueran combinaciones de letras y números.

c. Control Recomendado 3: Restringir el horario de acceso a los recursos de la red y activar en los servidores la opción para desconectar automáticamente las cuentas de acceso cuando éstas son utilizadas para acceder los recursos de la red fuera de horas laborables.

II. Recomendaciones a la UPMC:

- Pruebas internas y análisis de los documentos que están almacenados en la base de datos constantemente.
- Pruebas y análisis de los procedimientos de controles internos y de otros procesos con frecuencia.
- Educar a sus empleados como un plan de prevención

1. Hallazgo: Según los hechos Yoandy y sus cómplices extrajeron de la base de datos de la UPMC información de sus empleados sin ningún tipo de restricción.

a. Control Recomendado 1: Conservar la información financiera sensitiva de la organización revisando y actualizando su plan de seguridad constantemente.

b. Control Recomendado 2: Establecer un tipo de control de seguridad que restrinja el acceso no autorizado.

c. Control Recomendado 3: Mejora en los sistemas de seguridad muchos sistemas de ficheros dejan que sea el usuario quien proporcione las medidas necesarias para proteger los datos ante fallos en el sistema o en las aplicaciones. Los usuarios tienen que hacer copias de seguridad cada día, y si se produce algún fallo, utilizar estas copias para restaurarlos.

2. Hallazgo: Los hechos se cometieron desde Venezuela con *IP* disfrazados.

a. Control Recomendado: Establecer un tipo de control de seguridad que detecte y restrinja *IP* disfrazados y que estén fuera de los Estados Unidos.

3. Hallazgo: Este sistema pudo haber carecido de algún antivirus o estar sin actualización y esto pudo haber provocado alguna vulnerabilidad o algún fallo en el sistema.

a. Control Recomendado 1: Establecer un *software* que le de actualización constante a los antivirus.

b. Control Recomendado 2: Si el sistema se puso vulnerable con los fallos se deben tener copias de seguridad *Backup*.

3. Hallazgo: Deficiencias en los parámetros de seguridad de los servidores de la UPMC para controlar las cuentas de acceso a los recursos de la red.

a. Control Recomendado 1: Requerir un mínimo de cinco contraseñas diferentes antes de volver a utilizar la misma.

b. Control Recomendado 2: Requerir que las contraseñas fueran combinaciones de letras y números.

c. Control Recomendado 3: Restringir el horario de acceso a los recursos de la red, y activar en los servidores la opción para desconectar automáticamente las cuentas de acceso cuando éstas son utilizadas para acceder los recursos de la red fuera de horas laborables.

4. Hallazgo: No se había establecido como medida de seguridad una zona desmilitarizada (DMZ, por sus siglas en inglés). Esto, para brindar a la red interna de la UPMC una protección que minimice los riesgos de que la información sea accedida de forma no autorizada.

a. Control Recomendado: Establecer una configuración que incluya una Zona Desmilitarizada (DMZ, por sus siglas en inglés) que limite el acceso desde Internet a los servidores de la red de la UPMC y viceversa. Esto es necesario para proteger la red de ataques cibernéticos, y para evitar que personas externas y no autorizadas puedan acceder a ésta y comprometer la seguridad de sus sistemas.

Una vez finalizado este informe de auditoría se le recomienda al Servicio de Rentas Internas (IRS, por sus siglas en inglés), y a la Universidad de Pittsburgh Medical Center (UPMC), invertir en nuevas medidas de prevención para minimizar los riesgos de fraudes, deben de contar con métodos eficaces como lo son los controles correctivos, detectivos y preventivos para que los ayude en la prevención, detección y el manejo del fraude. Y que se mantengan a la vanguardia de nuevos controles, a medida que vaya evolucionando la tecnología.

SECCIÓN 7: CONCLUSIÓN

Queda demostrado que el fraude es un acto que pone a las organizaciones y/o agencias en peligro. Este delito no solo lo comete el personal interno de alguna organización y/o agencia también lo puede cometer cualquier individuo externo, como sucedió en el caso U.S. v. Yoandy Pérez Llanes (2015). No se los motivos, ni las razones que llevaron a este individuo a cometer fraude, pero lo que, si se es que, su mala acción lo llevo tras las rejas. Por esto es que se debe fomentar los valores, el comportamiento ético y una cultura llena de honestidad no solo dentro de las organizaciones, sino afuera de estas, no obstante, las organizaciones tienen en sus manos el papel más importante, el de prevenir, ser víctimas de fraude.

Todas las organizaciones son susceptibles de padecer algún tipo de fraude, ya que cuando hay intención, es difícil detectarlo y frenarlo. A pesar de esto, se ha visto que este riesgo se mitiga sustancialmente cuando las empresas cuentan con un programa integral que permite combinar mecanismos de cambio cultural con controles internos en los procesos, pero los controles no son la única herramienta para prevenir que las organizaciones sean víctimas defraude también está la figura de los auditores y para mí la más importante, ya que estos son los que buscan, y los que todo lo observan en su organización, pero también estos son los que cargan con toda la responsabilidad de prevenir, detectar y corregir todo tipo de fraude que ocurra en su entorno de trabajo.

No obstante, y a pesar de la carga que conlleva una auditoria, los auditores deben realizar su trabajo con estricto apego a las normas que regulan su actuación profesional, pero sobre todo con ética. También es indispensable que las entidades logren concientizarse de la necesidad de invertir con los recursos necesarios para implementar mecanismos efectivos de prevención y detección de los riesgos de fraudes; de esta manera, los principales beneficiarios serán las propias organizaciones.

Y para concluir los dejo con este pensamiento,

“Se puede engañar algunos todo el tiempo, a todos algún tiempo, pero no se puede engañar a todos todo el tiempo”. Abraham Lincoln

SECCIÓN 8: REFERENCIAS

Act,18 U.S.C § 371(2015) Título 18 del Código Criminal de los Estados Unidos, Sección 371

Act,18 U.S.C § 1349(2015) Título 18 del Código Criminal de los Estados Unidos, Sección 1349

Act,18 U.S.C § 1956(2015) Título 18 del Código Criminal de los Estados Unidos, Sección 1956

Act,18 U.S.C § 286(2015) Título 18 del Código Criminal de los Estados Unidos, Sección 286

Act,18 U.S.C § 1957(2015) Título 18 del Código Criminal de los Estados Unidos, Sección 1957

Act,18 U.S.C § 1029(2015) Título 18 del Código Criminal de los Estados Unidos, Sección 1029

Act,18 U.S.C § 1341(2015) Título 18 del Código Criminal de los Estados Unidos, Sección 1341

Act,18 U.S.C § 1343(2015) Título 18 del Código Criminal de los Estados Unidos, Sección 1343

Act,18 U.S.C § 641(2015) Título 18 del Código Criminal de los Estados Unidos, Sección 641

Act,18 U.S.C § 287(2015) Título 18 del Código Criminal de los Estados Unidos, Sección 287

Act,18 U.S.C § 1028A (a)1(2015) Título 18 del Código Criminal de los Estados Unidos, Sección1028A(a)

Act,18 U.S.C § 1028(A)7(2015) Título 18 del Código Criminal de los Estados Unidos, Sección1028(A)7

Association of Certified Fraud Examiner (ACFE) (2017). Prevención del

Fraude Recuperado de: http://www.acfe.com/fraud-prevention-checkup.aspx

AccessData (2017). Forensic Toolkit. Recuperado de: http://accessdata.com/products-services/forensic-toolkit-ftk

AccessData (2014). Registry Viewer user guide. Recuperado de: https://ad-pdf.s3.amazonaws.com/RegistryViewer_UG.pdf

Collins, H. (2017). Gift Card. Recuperado. de: https://www.collinsdictionary.com /es/diccionario/ingles/gift-card

Castro, L. (2016). ¿Qué es un IP address o Dirección IP? Recuperado de: http://aprenderinternet.about.com/od/general/fl/Que-es-IP-address.htm

Cressey, D. R. (1972). Other People's Money: Study in the Social Psychology of Embezzlement. Wadsworth Publishing Company.

Comisión Federal de Comercio (s.f). Robo de identidad. Recuperado de: https://www.robodeidentidad.gov/

Giménez, V.M. (s.f.). Hacking y Ciberdelito. Recuperado. de: https://riunet.upv.es/ bitstream/handle/10251/11856/memoria.pdf?sequence=1

Griffin, M. (2015). CBS Pittsburgh Foreign Suspect Indicted in UPMC Identity Theft Tax Case. Recuperado de: http://pittsburgh.cbslocal.com

Homeland Security (2016). Combating Cyber Crime. Recuperado de: https://www.dhs.gov/topic/combating-cyber-crime

Internal Revenue Service (IRS) (2017a). IRS español. Recuperado de: https://www.irs.gov/español.com

Internal Revenue Service (IRS)(2017b). Protección de la Identidad: Prevención, Detección Ayuda para Víctimas. Recuperado de: https://www.irs.gov/spanish/el-irs-trabajara-con-victimas-del-robo-de-identidad

Internal Revenue Service (IRS) (2017c). Reembolso de impuestos. Recuperado de: https://www.irs.gov/spanish/presentacion-de-impuestos

IBM (2015). Características y Tipos de bases de datos. Recuperado de: https://www.ibm.com/developerworks/ssa/data/library/tipos_bases_de_datos/

Khan, A. (2013). Principales Tipos de Fraudes. Recuperado de: http://www.cybersource.com/esLAC/solutions/featured_solutions/optimizing_fraud_management/manage_fraud_risk/?&dcid=&gclid=Cj0KEQjwxbDIBRCL99Wls-nLicoBEiQAWroh6mQzaOCWks

Kasperskys Labs (2017). Comunicados de prensa. Recuperado de: https://latam.kaspersky.com/about/press-releases?page=1

Lynch, J. (s.f). Computer Crime and intellectual property sections. Recuperado de: https://www.justice.gov/criminal-ccips

Norton (2016). Fraude en línea. Recuperado de: https://es.norton.com/cybercrime-phishing

Porolli, M. (2013). En que consiste el análisis forense de información. Recuperado de: https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-

de-informacion/

Raymond, E. S. (2001). How To Become A Hacker. Recuperado de: http://www.catb.org /~esr/faqs/hacker-howto.html

Turbo Tax (2013). El poder de quedarte con lo que es tuyo. Recuperado de: http://blog.turbotax.intuit.com/media-lounge/turbotax-2012-el-poder-de-quedarte-con-lo-que-es-tuyo/

Tribunal Supremo de Justica, Republica de Venezuela Extradición (2015). Recuperado de: http://historico.tsj.gov.ve/decisiones/scp/julio/179157-447-3715-2015-E15-200.HTML

The Money Glory (2014). Los 3 factores que motivan un fraude empresarial. Recuperado de: http://www.themoneyglory.com

U.S. v. Yoandy Pérez Llanes (2015a). Recuperado de: https://media.scmagazine.com /documents/132/yoandy_perez_llanes_indictment_32909df

U.S. v. Yoandy Perez Llanes (2015b). Public Notifications. Recuperado de: https://www.justice.gov/usao-wdpa/vw/us-v-yoandy-perez-llanes

U.S. v. Mariely Malavet Rivera (2016). Recuperado de: https://www.justice.gov/usao pr/pr/woman-sentenced-prison-defrauding-irs

U.S. v. Miosotis Ribot Figueroa (2015). Recuperado de: https://www.justice.gov/usao-pr/pr/two-individuals-indicted-bank-and-wire-fraud

U. S. v. John Rusnak (2002). Recuperado de: https://www.justice.gov

/archive/dag/cftf/chargingdocs/allfirst.pdf

Wells, J. T. (2013). Principles of Fraud Examination (4ta ed.). Wiley.