

EDP UNIVERSITY OF PUERTO RICO, INC.

RECINTO DE HATO REY

PROGRAMA DE MAESTRÍA EN SISTEMAS DE INFORMACION

Especialidad en Seguridad de Información e Investigación de Fraude Digital

FRAUDE ELECTRÓNICO Y ROBO DE IDENTIDAD

ANÁLISIS DE CASO: USA V. EMIL RENSING

1:16-cr-00442-VM

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACION

Especialidad en Seguridad de Información e Investigación de Fraude Digital

MARZO, 2019

PREPARADO POR

JANICE A. FUENTES NALES

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

FRAUDE ELECTRÓNICO Y ROBO DE IDENTIDAD

ANÁLISIS DE CASO: USA V. EMIL RENSING

1:16-cr-00442-VM

Preparado por
Janice A. Fuentes Nales

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 Digital

Marzo, 2019

Aprobado por:


Dr. Miguel A. Drouyn Marrero, Director

Tabla de Contenido

1.Introducción y Tránsito	9
Introducción	9
Descripción del caso	11
Tránsito	13
Descripción de los hechos:	14
Definición de términos:	16
2.Revisión de literatura	17
Introducción	17
Leyes aplicables	21
Casos Relacionados	22
Herramientas de investigación	25
3.Simulación	27
4.Informe del caso	30
Resumen Ejecutivo	30

Objetivo	30
Alcance del trabajo	31
Datos del caso	31
Descripción de los dispositivos utilizados	31
Resumen de hallazgos	33
Cadena de custodia	44
Procedimiento	47
Conclusión	67
5.Discusión del caso	69
6.Auditoria y prevención	70
Introducción	70
Resumen y hallazgos	71
7.Conclusión	73
8.Referencias	74

Tabla de Figuras

Figura #1 Sistema de Clasificación del Fraude Ocupacional y Abuso.....	19
Figura #2 Esquema de fraude de Emil Rensing.....	29
Figura #3 Computadora en la cual se realizo el análisis.....	32
Figura #4 USB Drive identificado como Evidence #94802.....	33
Figura #5 Correo electrónico enviado por Emil Rensing a James Robins.....	34
Figura # 6 Correo electrónico enviado por a James Robins a Emil Rensing	35
Figura # 7 : Correo electrónico para coordinar sesiones de servicio	35
Figura # 8 Correo electrónico de confirmación de las sesiones de servicios.....	36
Figura # 9 Correo electrónico de James Robins con la primera factura de servicio.	36
Figura # 10 Correo electrónico de Emil Rensing confirmando transferencia de pago.....	37
Figura #11 Formulario del W-9 del IRS de Accounting Company.....	38
Figura #12 Formulario del W-9 del IRS a nombre de AG Project Management.....	30
Figura #13 Factura No.0000002 a nombre de Accounting Company.....	40
Figura #14 Factura No.0000547 a nombre de Accounting Company.....	41

Figura #15 Factura No.623 a nombre de AG Project Management.	42
Figura #16 Factura No.901 a nombre de AG Project Management	43
Figura #17 Imagen con especificaciones de la computadora.....	47
Figura #18 Imagen con las herramientas instaladas para realizar la investigación	44
Figura #19 Imagen de la aplicación AccessData FTK Imager 3.1.4.6	47
Figura #20 Creación de la imagen del disco	48
Figura #21 Selección de la fuente de evidencias.....	49
Figura #22 Selección del dispositivo que se analizará.....	49
Figura #23 Añadir el destino de la imagen a crearse.....	50
Figura #24 Selección del tipo de imagen que se creará	50
Figura #25 Información de la evidencia recopilada.....	51
Figura #26 Seleccionar donde se guardará la imagen creada	51
Figura #27 Creación de folder en donde se guardará la imagen.....	52
Figura #28 Selección y nombre de folder de la imagen	52
Figura #29 Comienzo de la creación de la imagen del disco	53

Figura #30 Proceso de inicio creación de la imagen del disco	53
Figura #31 Estatus de la creación de la imagen del disco	54
Figura #32 Creación de la imagen del disco completada	54
Figura #33 Verificación de la imagen creada.....	55
Figura #34 Resultados de la imagen MD5 Hash y SHA1 Hash	55
Figura #35 Resumen de la imagen creada.....	56
Figura #36 Continuación resumen de la imagen creada	56
Figura #37 Añadir imagen creada para análisis.....	57
Figura #38 Selección tipo de evidencia	57
Figura #39 Selección de fuente que se analizará	58
Figura #40 Imagen creada aparece en el árbol de evidencia	58
Figura #41 Expansión de archivos del árbol de evidencia	59
Figura #42 Folders que aparecieron de la imagen creada	60
Figura #43 Folder con evidencia de conversaciones	60
Figura #44 Correo electrónico enviado por Emil Rensing a James Robins.....	61
Figura #45 Correo electrónico enviado por a James Robins a Emil Rensing	61

Figura #46 : Correo electrónico para coordinar sesiones de servicio	62
Figura #47 Correo electrónico de confirmación de las sesiones de servicios	62
Figura #48 Correo electrónico de James Robins con la primera factura de servicio	63
Figura #49 Correo electrónico de Emil Rensing confirmando transferencia de pago.....	63
Figura #50 Folder encontrado con formularios.....	64
Figura #51 Formulario del W-9 del IRS de Accounting Company.....	64
Figura #52 Formulario del W-9 del IRS a nombre de AG Project Management.....	65
Figura #53 Folder encontrado con facturas	65
Figura #54 Factura No.0000002 a nombre de Accounting Company.....	66
Figura #55 : Factura No.0000547 a nombre de Accounting Company.....	66
Figura #56 Factura No.623 a nombre de AG Project Management	67
Figura #57 Factura No.901 a nombre de AG Project Management	67

1.Introducción y Trasfondo

Introducción

El fraude interno es un delito cometido por empleados de una empresa. Es una realidad que el fraude interno no puede obviarse en las organizaciones, especialmente en un momento de crisis económica e inestabilidad política. La crisis económica con la que vivimos actualmente ha provocado que varias empresas hayan tenido que reducir los controles internos, y debido a esto se han incrementado las oportunidades para cometer fraude. Esta situación, junto con otros factores ha hecho caer la lealtad de los empleados hacia sus empresas, éstos están actuando como presión ambiental favorable en los perpetradores de fraude interno. El 65% de los fraudes a las compañías son cometidos por empleados de las propias empresas, que en un 61% de los casos carecen de sistemas de control interno efectivos (Inter Economía, 2016).

Los empleados que realizan los fraudes se aprovechan de su puesto o de la información que administran y la utilizan o manipulan datos y equipos para su beneficio personal. El perfil mayoritario del defraudador es un empleado de entre 35 y 55 años (el 69% de los casos), que dispone de gran poder en la empresa (44%), que actúa en colaboración con terceros (62%) y cuya motivación es el lucro personal (60%) (Inter Economía, 2016). El fraude en colusión es uno muy común. Este se produce mediante acuerdo de personas de dentro y fuera de la organización, que aprovechan las relaciones que se establecen o la información que se comparte (Confirma sistemas, 2016).

Según Confirma Sistemas (2016), durante los últimos años las empresas han ido disminuyendo los recursos humanos y materiales dedicados al control interno para utilizarlos en otras actividades directamente relacionadas con su propia supervivencia, como son la financiación o el equilibrio presupuestario. Esta política restrictiva está afectando a las inversiones que han de hacerse para incrementar la seguridad en sus diferentes vertientes: control interno, seguridad informática, análisis de riesgos, o seguridad general contra el fraude interno y externo, lo que está costando miles de euros a las organizaciones.

J. Wells (2013) nos explica la teoría de Donald Cressey llamada El Triángulo Clásico de fraude, este presentaba los condicionantes para que se materialice el fraude, debiendo coexistir para ello estas tres situaciones:

1. Motivación (incentivo, presión). Cuando la Administración u otros empleados tienen un estímulo o presiones que les aportan razones justificativas para cometer fraudes.
2. Poder (Oportunidad). Serían las circunstancias que facilitan las posibilidades de perpetuar fraudes (por ejemplo, la ausencia de controles, controles ineficaces, o la capacidad de la administración para abrogar los controles).
3. Racionalización, actitud. Cuando las personas son capaces de racionalizar un acto fraudulento en total congruencia con su código de ética personal o que poseen una actitud, carácter o conjunto de valores que les permiten, consciente e intencionalmente, cometer un acto deshonesto.

La mejor manera de combatir los riesgos de fraude es incidir sobre estos tres factores, reduciéndolos, pero no de forma simultánea, pues basta con que uno de ellos no esté presente para que el riesgo no se materialice, o en el peor de los casos, que se minimice. En este sentido, combatir convenientemente el factor “oportunidad”, en donde radicaría el éxito de controlar la probabilidad de ocurrencia, de forma que, si pudiésemos suprimirlo, habríamos conseguido eliminar totalmente el riesgo de fraude, a pesar de lo importante y altos que fuesen las motivaciones y la racionalización (Confirma sistemas, 2016).

Como resultado de este planteamiento, deberíamos priorizar los controles con los que minimizar las “oportunidades” que puedan presentarse a los defraudadores, pues controlando estas, habremos incidido de forma eficaz en su combate. Contar con un sistema de evaluación frecuente del riesgo obliga a las empresas a buscar el fraude y les da la agilidad necesaria para encontrarlo. Implementar sistemas de prevención del fraude resulta esencial para identificar las amenazas potenciales y las debilidades en los controles. (Confirma sistemas, 2016).

En este trabajo investigativo se estará exponiendo un caso de fraude interno en una compañía, del cual es acusado un hombre de 44 años residente de Manhattan, y exdirector digital de la compañía Epix en la cual se realizó el fraude.

Descripción del caso

Número de caso: 1:16-cr-00442-VM -1:16-mj-02650-UA

USA v. Emil Rensing

Partes del caso:

Acusado (autor)

- Emil Rensing, exdirector digital de la compañía

Entidades relacionadas al caso (víctimas):

- Compañía EPIX (cadena de televisión)

Investigadores

- Diego Rodríguez, subdirector de la oficina Federal de Nueva York (FBI)
- Angela E. Tassone, Agente especial del Federal Bureau of Investigation (FBI)
asignada a crímenes de cuello blanco

Abogados

- Henry Mazurek, abogado de la defensa

Fiscales

- Preet Bharara, fiscal federal de los Estados Unidos para el Distrito del Sur de Nueva York
- Joon H. Kim, fiscal interino de los Estados Unidos para el Distrito del Sur de Nueva York
- Geoffrey S. Berman, fiscal de los Estados Unidos para el Distrito del Sur de Nueva York
- Elisha Kobre, asistente del fiscal de los Estados Unidos para el Distrito del Sur de Nueva York

Jueces

- Frank Maas, juez magistrado de la Corte Federal de Manhattan

- James L. Cott, juez de primera instancia en el Tribunal Federal de Manhattan
- Victor Marrero, juez de Distrito de la Corte Federal de Manhattan

Trasfondo

Esta investigación es basada en el fraude que alegadamente cometió Emil Rensing a Epix. Según los documentos judiciales obtenidos, Rensing fue acusado en el Tribunal del Distrito Sur de Nueva York por fraude electrónico y robo de identidad relacionado con un esquema que presuntamente cometió durante el tiempo que estuvo empleado en la red de cable premium Epix. Se le acusó de robar más de \$8 millones durante 5 años a la compañía Epix donde ejercía como director digital entre el 2010 y 2015. Rensing estableció una red de proveedores falsos para realizar servicios de medios digitales para la compañía. Aparentemente, la mayoría de estos servicios nunca se llevaron a cabo. (Otterson, 2016).

Emil Rensing, asistió a la Universidad George Washington. Este fue uno de los primeros empleados de America Online (AOL) en la década de 1990. El ayudó a desarrollar su servicio pionero de mensajería instantánea, entre otras innovaciones. Se desempeñó en MTV Networks y estuvo involucrado en numerosas empresas digitales, incluida la empresa Frederator Studios con el ex ejecutivo de MTV Networks y Hanna-Barbera Fred Seibert, y Next New Networks, con Seibert y el ex ejecutivo de Nickelodeon Herb Scannell (Littleton, 2018).

Aparentemente Rensing fue sacudido en el 2009 por el final de su matrimonio de 13 años con su novia de la escuela secundaria y el inicio de problemas de salud no revelados.

Por otro lado, la muerte inesperada de su hermana fue otra experiencia traumática, según los documentos judiciales (Littleton, 2018).

Los abogados de Rensing previo a la sentencia ante el juez, escribieron que Rensing “Sentía que su compensación no era lo suficientemente alta para el trabajo o el valor que entregaba; creía que tenía la aprobación tácita de la gerencia; que la cultura corporativa lo alentó mientras produjera resultados; y las reglas no eran tan importantes en ese negocio” (Littleton, 2018)

Descripción de los hechos:

A continuación, presento los hechos asociados al caso United States of America vs. Emil Rensing (2016):

En abril 2010 Rensing comenzó a trabajar en la compañía Epix, como director digital. En octubre de 2010, creó cuentas de correo electrónico falsas y firmó los nombres de ex compañeros de trabajo para facturar a una empresa que prestaba servicios técnicos. Rensing hizo que la Epix contratara dos compañías de proveedores de propiedad que el mismo controlaba, para realizar servicios de medios digitales. Estos servicios prometidos nunca fueron realizados. La política corporativa de Epix cambió para prohibir el uso de proveedores externos asociados con los empleados, Aun así, Rensing continuó su fraude al crear otro proveedor falso para facturarle a la compañía servicios que nunca fueron proporcionados o manejados por otros empleados de Epix.

Al FBI investigar, notaron que los socios comerciales de Rensing estaban enlistados como empleados de estos proveedores, pero cuando los contactaron, las personas no tenían la más mínima idea de porque sus nombres estaban asociados con dichas compañías.

Alegadamente Rensing, también uso identidades robadas para ocultar su participación. Al Epix enterarse del esquema fraudulento de Rensing, este fue entrevistado por los abogados de la compañía, y realizó múltiples declaraciones falsas para seguir ocultando su esquema. Rensing fue despedido de Epix en agosto de 2015 luego de que los ejecutivos sospecharan de las prácticas de facturación en su departamento. En abril 2016, Rensing fue acusado y arrestado por dos delitos, fraude electrónico y robo de identidad. En junio 2017 Rensing se declara culpable. En junio 2018, fue sentenciado.

Acusaciones:

Rensing fue acusado de robar más de \$8 millones a la compañía Epix donde era el Director Digital, esto mediante un esquema en el cual usaba compañías que él mismo poseía, para presentar facturas fraudulentas de millones de dólares, además de utilizar identidades falsas.

Cargos:

- 18 U.S.C. §§ 1028A -Robo de identidad agravado
- 18 U.S.C. §§ 1343 -Fraude por cable, radio o televisión.

Penalidades:

Rensing fue sentenciado y se le impuso las siguientes penalidades:

- Cincuenta y un (51) meses de cárcel
- Tres (3) años de libertad supervisada
- Pagar \$7,774,469.52 en restitución a la compañía Epix, más los gastos que incurrió durante su participación en la investigación

Definición de términos:

Correo electrónico - es un servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos (Pérez y Merino, 2014)

Fraude- es una acción que resulta contraria a la verdad y a la rectitud (Pérez y Merino, 2013).

Fraude por cable- es un delito en el que una persona elabora un plan para defraudar u obtener dinero basado en una representación o promesas falsas (Kenton, 2018).

Robo de identidad- se produce cuando un atacante obtiene información personal de una persona física o jurídica y la utiliza ilegalmente (OSI, 2011)

2.Revisión de literatura

Introducción

El delito más temido por las empresas en países desarrollados es el fraude, aún frente a otros crímenes como el terrorismo, el secuestro, el sabotaje y el hurto. Lejos de estar bajo control, este flagelo al parecer está adquiriendo fuerza, ayudado en gran parte por una mayor complejidad en los negocios, la creciente globalización de los movimientos de fondos, las dificultades implícitas en el trato con diferentes culturas y un mayor uso de tecnologías como el Internet. Todo ello ha llevado a una sensación de mayor riesgo entre los empresarios de los más diversos sectores y países (Cano, 2018).

Las compañías no se están protegiendo lo suficiente contra el fraude o los defraudadores se le están adelantando a los controles, especialmente en las áreas de sistemas y de compras. De hecho, los fraudes más temidos son los que se hacen a través de computadores y tarjetas de crédito. Después se anotan otras áreas, como el robo de efectivo, fraudes en tesorería, fraudes en impuestos, fraudes en seguros y fraudes por negociación directa. Sin embargo, en todos los casos puede prevenirse y puede volver a ocurrir bajo las circunstancias actuales de control. Un alto porcentaje de fraude cuenta con la participación de empleados de las empresas en donde ocurre el hecho (Cano, 2018).

Según Cano (2018), un empleado que está involucrado en un fraude, en la gran mayoría de los casos, siempre incurre en este tipo de actitudes:

- Concentración de funciones
- Imprescindibilidad
- Disponibilidad en la resolución de problemas

- Nunca toma vacaciones
- Inestabilidad financiera
- Cambios en los hábitos de consumo y nivel de vida

Según Castellnou (2018), el fraude va muy en consonancia con el nivel de control percibido por los trabajadores a sus gastos. Dado que los procesos de análisis y revisión de los gastos reportados son tradicionalmente lentos y costosos, los encargados de la supervisión a menudo trabajan tomando solamente una muestra del conjunto de notas de gasto recibidas o realizando análisis demasiado superficiales que no llegan a la raíz. Este nos dice que existen cinco tipos de fraude interno en las empresas, estos son:

- Tipo 1 fraude interno documental - este se da siempre que el documento aportado como justificante no cumple con las condiciones reglamentarias por parte del emisor para poder ser considerado una factura válida.
- Tipo 2 fraude interno de tipo cronológico - este ocurre cuando existe una falta de coincidencia de la fecha de la nota de pago con el día en que efectivamente tuvo lugar ese gasto.
- Tipo 3 fraude interno por exceso de gasto - esto sucede cuando los gastos presentados por el empleado a través de una nota de gastos no se ajustan a los límites marcados por las políticas de viaje de la empresa, ósea que exceden el máximo autorizado.
- Tipo 4 fraude interno por compra de artículos *no compliance* - se comete cuando el empleado adquiere un producto sin autorización previa de la empresa.

- Tipo 5 fraude interno por presentación de gastos fuera del plazo - las empresas deben tener estipulado y convenientemente reflejado en su política de viajes un plazo o tiempo límite para que el empleado presente sus correspondientes notas de gastos. Todas las notas presentadas con posterioridad a estos plazos límite no pueden ser aceptadas como gastos reembolsables y deberán ser asumidos por el trabajador.

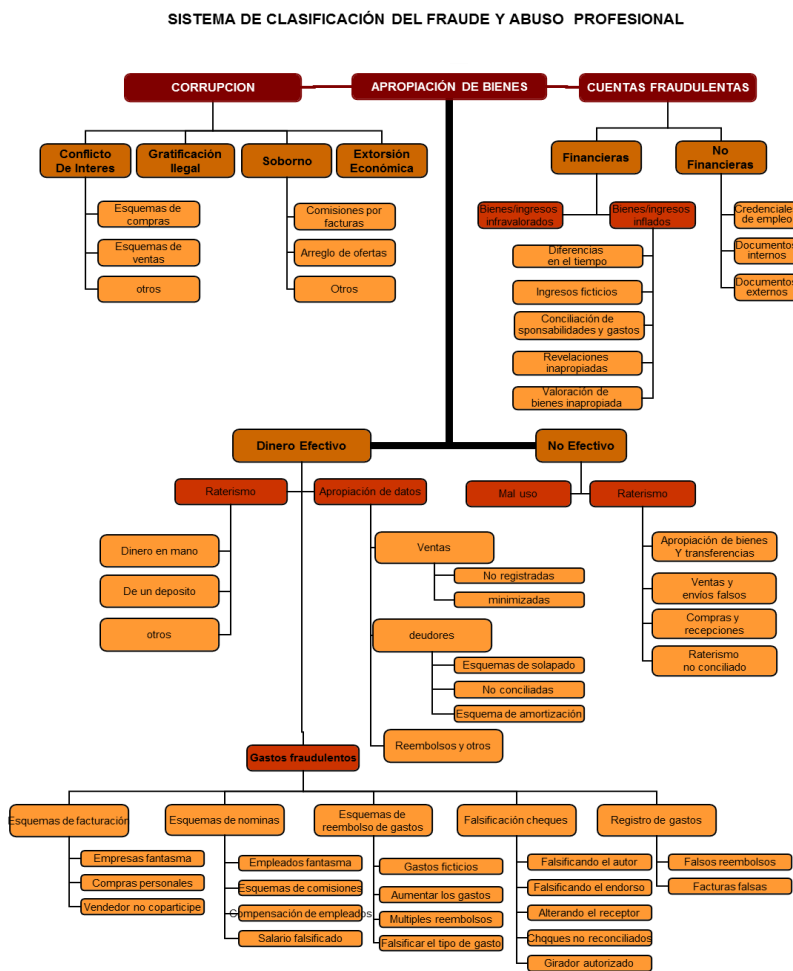


Figura # 1: Sistema de Clasificación del Fraude Ocupacional y Abuso, también conocido como el Árbol de fraude (ACFE, 2018)

Por otro lado, se encuentra el robo de identidad. Este ocurre cuando un delincuente obtiene tu información personal e intenta robar dinero de tus cuentas, abrir nuevas tarjetas de crédito, solicitar préstamos, alquilar apartamentos y cometer otros delitos, todo esto usando tu identidad. El robo de identidad puede dañar tu crédito, dejarte con facturas no deseadas y tomarte mucho tiempo y disgustos para resolver el problema (JP Morgan Chase, 2018).

Según el JPMorgan Chase (2018), el robo de identidad puede empezar cuando alguien obtiene y hace uso indebido de tu información personal, como tu nombre y número de seguro social, número de tarjeta de crédito u otra información financiera de tus cuentas.

Los ladrones pueden usar varios métodos para robar tu información, incluyendo:

- **Skimming:** Consiste en robar números de tarjetas de crédito/débito usando un dispositivo especial en un ATM o al procesar una compra
- **Phishing:** Consiste en simular ser una institución financiera u otra compañía y enviar mensajes de email o emergentes para que reveles tu información personal
- **Pretextar:** Consiste en simular que eres tú al llamar a instituciones financieras, compañías telefónicas y otras fuentes para obtener información adicional
- **Redireccionar tu correo:** Consiste en presentar un formulario de cambio de dirección para que tus estados de cuenta de facturación se envíen a otra dirección
- **Robo tradicional:** Consiste en robar carteras y bolsos, correspondencia (incluyendo los estados de cuenta bancarios y de tarjeta de crédito), ofertas de crédito pre-aprobado, nuevos cheques o información impositiva; incluso pueden

robar los archivos de personal de una compañía o asociarse con empleados que tienen acceso a tu información

- **Revisar la basura:** Consiste en revisar la basura para encontrar facturas y otros papeles con tu información personal

Leyes aplicables

Las leyes aplicables al esquema de fraude cometido por el Sr. Emil Rensing según el código penal de los Estados Unidos, son las siguientes:

18 U.S.C. §§ 1028A -Robo de identidad agravado. Según la ley de Robo de identidad agravado, Quienquiera, durante y en relación con cualquier violación de delito grave enumerada en la subsección (c), a sabiendas transfiere, posee o utiliza, sin la autoridad legal, un medio de identificación de otra persona será, además del castigo provisto para tal delito , será sentenciado a una pena de prisión de 2 años.

18 U.S.C. §§ 1343 -Fraude por cable, radio o televisión. Según la ley de Fraude por cable, radio o televisión, Quienquiera que haya ideado o tenga la intención de diseñar algún plan o artificio para defraudar, o para obtener dinero o bienes por medio de pretensiones, representaciones o promesas falsas o fraudulentas, transmita o haga que se transmita mediante comunicación por cable, radio o televisión. En el comercio interestatal o extranjero, cualquier escrito, rótulo, señal, imagen o sonido con el propósito de ejecutar dicho esquema o artificio, deberá ser multado bajo este título o encarcelado por no más de 20 años, o ambos. Si la violación ocurre en relación con, o involucra cualquier beneficio autorizado, transportado, transmitido, desembolsado o pagado en relación con, un desastre o emergencia mayor declarado por el presidente (según se definen dichos términos en la sección 102 de

Robert T. Stafford). La Ley de Asistencia de Emergencia y Ayuda por Desastres (42 USC 5122), o afecta a una institución financiera, dicha persona debe ser multada por no más de \$ 1,000,000 o encarcelada por no más de 30 años., o ambos.

Casos Relacionados

USA v. Zheng Geng (2017)

Zheng Geng es el Director Ejecutivo de Xigen LLC (Xigen). Este fue acusado de seis cargos de fraude electrónico y de robo de identidad agravado. Alegadamente Geng ideó un plan entre 2005 y 2016 para defraudar a los Estados Unidos mediante la presentación de solicitudes de subvenciones falsas y fraudulentas en el marco del Programa de Investigación de Innovación para Pequeñas Empresas (SBIR). El programa SBIR tiene como objetivo estimular la innovación tecnológica de los Estados Unidos. Otro objetivo es fomentar y alentar la participación en la innovación técnica de las pequeñas empresas en desventaja social y económica que en algunos casos son al menos el 51 por ciento de propiedad y control de las mujeres. Geng preparó propuestas materialmente fraudulentas para premios, informes subsiguientes y comunicaciones relacionadas con los programas.

Para tener respaldo este presentó sus solicitudes de subvención utilizando las identidades de las personas sin consentimiento, o representando erróneamente sus posiciones dentro de Xigen. Por otro lado, este presentó endosos que tergiversaron afiliaciones activas con varias universidades, entre ellas, la Escuela de Medicina de la Universidad de Harvard y la Escuela de Medicina de la Universidad Johns Hopkins, y fondos presupuestados para subcontratistas sin su conocimiento y sin proporcionarles fondos presupuestados. Con esta información falsa, el gobierno de los Estados Unidos aprobó los premios y subvenciones del

programa SBIR a través de los Institutos Nacionales de Salud del Departamento de Salud y Servicios Humanos y la Administración Nacional de Aeronáutica y del Espacio. Los premios totalizaron más de \$ 1.8 millones.

Según los documentos judiciales, Geng usó los fondos recompensados para su uso personal y el uso de los miembros de su familia y asociados. La acusación fue anunciada por el Fiscal Interino de los Estados Unidos para el Distrito de Maryland Stephen M. Schenning; El Inspector General Paul Martin de la Oficina del Inspector General de la Administración Nacional de Aeronáutica y del Espacio ; La Inspectora General Allison Lerner de la Oficina Nacional de la Fundación de Ciencia del Inspector General; El agente especial a cargo Nick DiGiulio de la Oficina del Inspector General de Salud y Servicios Humanos; El agente especial a cargo Gordon Thompson de la Oficina del Inspector General del Servicio Postal de los EE. UU. y el Agente Especial a Cargo Gordon B. Johnson de la Oficina Federal de Investigaciones, Oficina de Campo de Baltimore

USA v. Reynaldo “Sonny” Jesus Peralez (2019)

Reynaldo “Sonny” Jesus Peralez, de 53 años de edad, propietario y operador de Bohannon Oil Services, LLC, fue condenado por estafar a los inversionistas por más de \$ 3.5 millones de dólares al canalizar inversiones falsas y fraudulentas en camiones y transporte involucrado en el transporte de arenas de *fracking* y por robar la identidad de una de sus víctimas para promover sus planes fraudulentos, anunció el Fiscal de los Estados Unidos John F. Bash y el Agente Especial de la Oficina Federal de Investigaciones (FBI) a cargo Christopher Combs, División de San Antonio.

Según los documentos judiciales, Peralez hizo declaraciones falsas y fraudulentas a los posibles inversionistas que indicaban que su compañía necesitaba camiones adicionales

para transportar arena para cumplir con los contratos que tenía con los servicios en yacimientos petrolíferos. compañías. De hecho, Peralez no tenía tales contratos con las empresas. Peralez luego infla bruscamente el valor de los camiones, que compró con fondos de inversionistas, y conservó los fondos restantes para su uso personal. Peralez envió correos electrónicos a los inversionistas que incluían documentación falsa sobre sus negocios. Peralez también hizo declaraciones falsas a los inversionistas con respecto a los pagos que supuestamente estaba recibiendo su negocio. Peralez creó negocios ficticios que, según él, vendían camiones directamente a los inversionistas.

Peralez el 30 de abril de 2018, se declaró culpable de un cargo de fraude electrónico y un cargo de robo de identidad con agravantes. Al declararse culpable de los cargos, Peralez admitió haberse involucrado a sabiendas en un plan para estafar a los inversionistas y poseer y usar a sabiendas la identificación de otra persona.

USA v. Roberta Czap (2017)

Roberta Czap fue acusada de fraude electrónico y malversación de fondos. Alegadamente a partir de enero de 2011 y hasta agosto de 2016, mientras Czap trabajaba como Vicepresidente de Contabilidad en una compañía de servicios financieros en Newark, el demandado realizó 497 transacciones de ACH fraudulentas separadas desde las cuentas de la compañía a sus cuentas bancarias personales. La Demandada disfrazó estas transacciones, que oscilaron entre \$ 1,000 y \$ 38,527, como pagos a pagos de seguros de salud corporativos o pagos a vendedores corporativos y modificó el libro mayor de la compañía para ocultar sus acciones. En total, la Sra. Czap obtuvo más de \$ 6.1 millones a través de su fraude.

Tras la malversación de fondos de la corporación, la Sra. Czap convirtió estas transferencias electrónicas en efectivo, a través de retiros en cajeros automáticos o adelantos

en efectivo en varios casinos. Después de apostar, a menudo brevemente, el demandado retiraría el dinero del casino y recibiría la moneda de los Estados Unidos. La ley federal requiere que todos los ingresos, ya sean obtenidos legal o ilegalmente, se declaren en las declaraciones de impuestos. Sin embargo, la Sra. Czap no informó los beneficios de su fraude en su declaración de impuestos de los años 2013 a 2015.

Entre abril de 2014 y septiembre de 2016, el esposo del demandado realizó una serie de depósitos en efectivo estructurados por un total de \$ 1,212,910, en incrementos que se acercan, pero de menos de \$ 10,000. Anteriormente fue condenado a un año y un día de prisión por su conducta en una acción penal separada, Estados Unidos v. Matthew Czap , 17-4-LPS.

Herramientas de investigación

Según Pepenella (s.f.), el tema de conversación que más a menudo tiene con otros examinadores es sobre qué herramientas están utilizando para completar sus exámenes e investigaciones. Esta ha recibido una amplia gama de respuestas que van desde código abierto hasta productos comerciales.

A continuación, se presentarán algunas las herramientas y técnicas utilizadas para examinar casos de fraude digital:

- FTK Imager- Es una herramienta de visualización de imágenes y vista previa de datos que le permite examinar archivos y carpetas en discos duros locales, unidades de red, CD / DVD y revisar el contenido de imágenes forenses o volcados de memoria. Con FTK Imager también puede crear hashes SHA1 o MD5 de archivos, exportar archivos y carpetas desde imágenes forenses al disco, revisar y recuperar

archivos que se eliminaron de la Papelera de reciclaje (siempre que sus bloques de datos no se hayan sobrescrito) y montar Una imagen forense para ver su contenido en el Explorador de Windows (Hernando, 2009).

- Data Extraction Kit for Outlook- Es una poderosa herramienta todo en uno para la conversión de correo electrónico de Outlook / PST, la migración y el análisis de datos. El producto se puede utilizar para extraer correos electrónicos y otros objetos de dichas fuentes, así como para generar informes detallados sobre su contenido para investigaciones forenses. Los escenarios de uso detallados se describirán en artículos separados, mientras que esta página explicará las funciones de los controles del programa y el propósito de las múltiples opciones de extracción de datos (Gordon, 2014).
- Idea Software - proporciona a auditores, contables, contadores y profesionales de sistemas informáticos y financieros, la posibilidad de mostrar, leer, visualizar, analizar, manipular, obtener muestras y extraer datos de cualquier archivo de datos procedente de cualquier origen, desde grandes sistemas a equipos personales, incluyendo informes impresos en archivos (Caseware, 2018).

3.Simulación

Se puede definir la simulación como un modelo que imita ciertos aspectos de la realidad. Esto permite trabajar en condiciones similares a las reales, pero con variables controladas y en un entorno que se asemeja al real pero que está creado o acondicionado artificialmente. La idea es que la simulación permita comprobar el comportamiento de una persona, de un objeto o de un sistema en ciertos contextos que, si bien no son idénticos a los reales, ofrecen el mayor parecido posible. Así, es posible corregir fallos antes de que la experiencia, efectivamente, se concrete en el plano de lo real (Pérez y Merino, 2014).

A continuación, presento una simulación como ocurrieron los hechos en el caso de USA v. Emil Rensing. Según Otterson (2016), Emil Rensing, fue acusado de robar más de ocho millones a la compañía Epix, donde este de desempeñaba como director digital. Se le acusó de fraude electrónico y robo de identidad. Aparentemente entre 2010 y 2015, Rensing estableció proveedores falsos que contrató para realizar servicios de medios digitales a Epix, pero al parecer estos servicios nunca se llevaron a cabo.

El FBI notó que los socios comerciales de Rensing estaban enlistados como empleados de estos proveedores, pero cuando se les contactó, las persona no tenían idea de porque sus nombres aparecían asociados a estas compañías. Supuestamente, Rensing también utilizó identidades robadas para ocultar su participación en este esquema de fraude.

Rensing hizo que la compañía Epix contratara a varias empresas proveedoras de servicios, los cuales los agentes del FBI afirman que nunca se realizaron. Las personas que Rensing enumeró en el papeleo del proveedor, a menudo sus antiguos socios comerciales, supuestamente tampoco sabían que Rensing estaba usando sus nombres de esa manera. al

menos dos compañías de proveedores que estaban controladas por él para realizar servicios de medios digitales. En este esquema Rensing usaba compañías que él poseía y controlaba para obtener dinero de la compañía para la cual laboraba. Este lo hacía mediante identidades falsas y robadas, además de presentar facturas fraudulentas por servicios que no se realizaron.

En cuanto a uno de los proveedores utilizados para perpetrar el esquema al proveedor-1, Rensing le proporcionó a Epix un nombre falso y una dirección de correo electrónico como el “contacto” la cual utilizaría la compañía para comunicarse con el proveedor. Al proveedor-2 Rensing le proporciono a Epix el nombre de un conocido personal como el “gerente de proyecto” y “contacto”, cuando en realidad este conocido no tenía nada que ver con el proveedor-2. También este, creo un correo electrónico con el nombre del conocido personal, y haciéndose pasar por esa persona se comunicaba regularmente con Epix para la facturación y otros asuntos administrativos.

Rensing presentó facturas falsas por el trabajo técnico realizado para Epix por un proveedor externo que él mismo controlaba, sin que lo supiera Epix. El cargo por fraude electrónico se debió al hecho de que Epix transfirió los pagos a una cuenta bancaria controlada por Rensing.

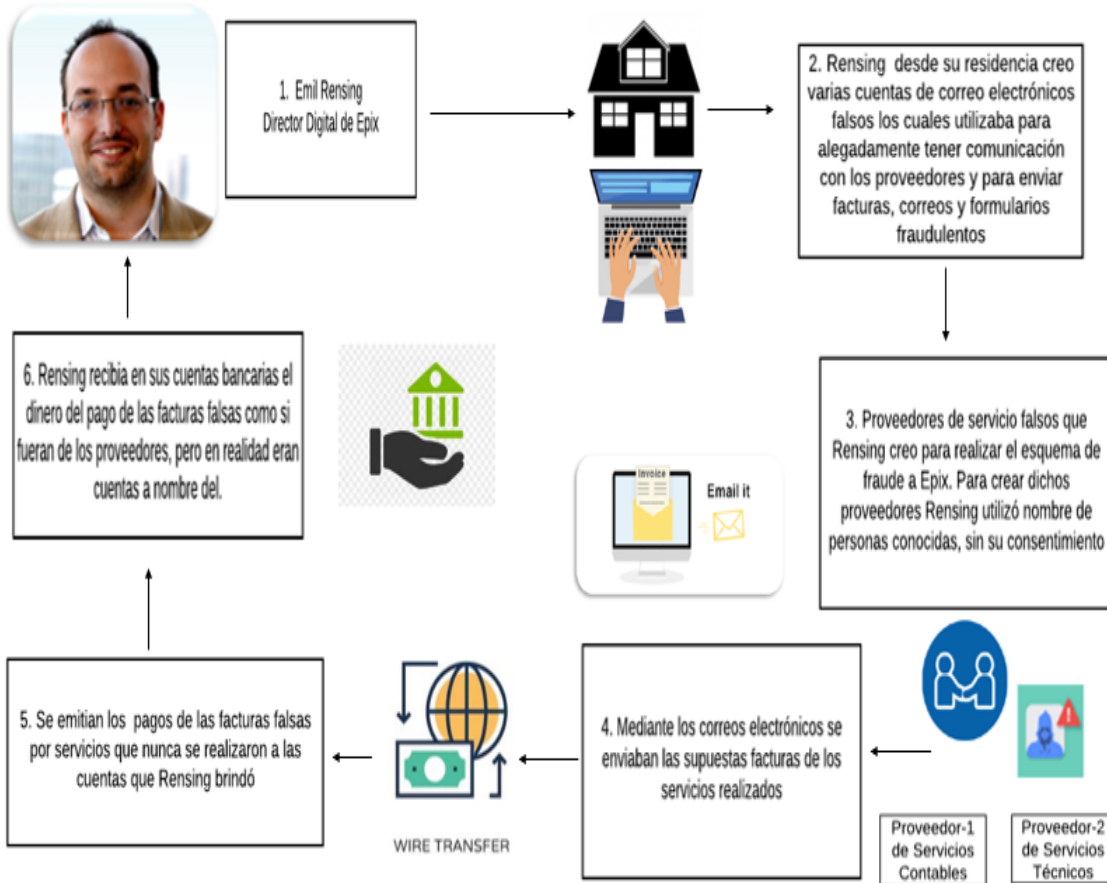


Figura # 2: Esquema de fraude de Emil Rensing

4.Informe del caso

Resumen Ejecutivo

Los fiscales de Estados Unidos para el Distrito del Sur de Nueva York Preet Bharara Joon H. Kim y Geoffrey S. Berman, solicitaron los servicios de una examinadora de fraude de JA Forensics, Janice A. Fuentes Nales para que analizara la evidencia incautada durante un allanamiento en la residencia del acusado Emil Rensing en Manhattan, New York. Esta forma parte de la evidencia recopilada con relación al caso USA v. Emil Rensing. Este caso está vinculado con al fraude de correo electrónico y robo de identidad.

Janice Fuentes, examinadora de fraude de JA Forensics procedió a analizar un usb con una copia de la imagen del disco duro de la computadora que le fue incautada a Rensing en su residencia. Durante el análisis realizado se encontraron correos electrónicos, facturas, evidencias de pago, transferencias bancarias, contratos de servicio, registros bancarios, formularios y listas de proveedores.

En los emails encontrados se puede apreciar la comunicación que mantenía Rensing con los supuestos proveedores. Por este medio llegaba a acuerdos con los proveedores, ya fuera para el tema de facturación o para temas administrativos. Las facturas, evidencias de pago y los registros bancarios demuestran que el dinero que se le pagaba a los proveedores iba a una cuenta personal de Rensing.

Objetivo

La fiscalía de Estados Unidos para el Distrito del Sur de Nueva York contrató a JA Forensics para examinar, analizar y recuperar la información electrónica almacenada en el

usb que fue entregado con una copia fiel y exacta del disco duro que fue incautado. Con el propósito de obtener la evidencia suficiente para poder ser utilizada en corte y a su vez vincular al acusado en este caso de fraude por correo electrónico y robo de identidad.

Alcance del trabajo

Este trabajo pretende analizar y presentar toda la evidencia recopilada del USB que fue entregado por los fiscales Preet Bharara, Joon H. Kim, Geoffrey S. Berman, con una copia exacta de la imagen del disco duro de la computadora que le fue incautada a Rensing

Datos del caso

1. Número de caso: 103882-NY
2. Investigador: Janice Fuentes
3. Cliente: Oficina del Fiscal de los Estados Unidos para el Distrito de Nueva York Sur
4. Representante del cliente: Preet Bharara, Joon H. Kim y Geoffrey S. Berman
fiscales de los Estados Unidos para el Distrito del Sur de Nueva York

Descripción de los dispositivos utilizados

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

1. Laptop Marca Lenovo, modelo ideapad donde habitan las herramientas y aplicaciones utilizadas durante el proceso de análisis.



Figura # 3: Computadora en la cual se realizó el análisis

2. USB Drive de 14GB, identificado como Evidence #94802.

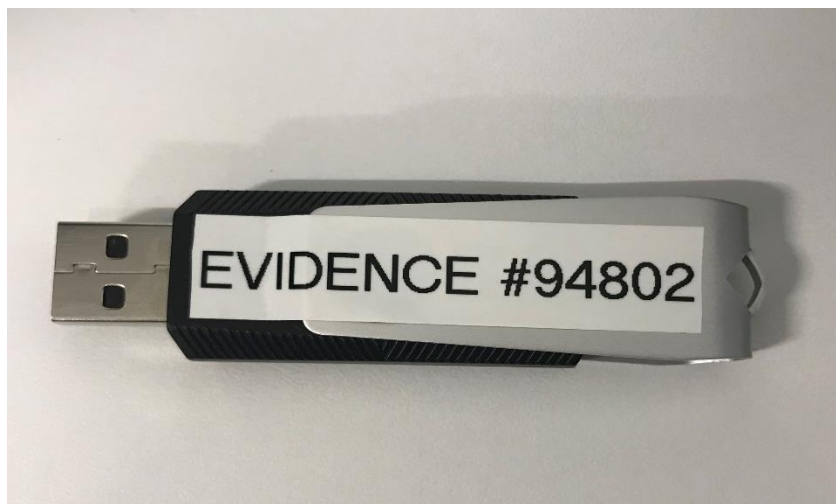


Figura # 4: USB Drive identificado como Evidence #94802

Resumen de hallazgos

A continuación, se presentan los hallazgos encontrados durante el análisis realizado al usb drive identificado como evidence #94802, con la herramienta AccessData FTK Imager 3.1.4.6.

- Tres (3) copias de conversaciones de correos electrónicos identificadas con la cuenta rensing@outlook.com perteneciente a Emil Rensing.
- Tres (3) copias de conversaciones de correos electrónicos identificadas con la cuenta proveedor-1@outlook.com, esta aparecía a nombre de James Robins
- Dos (2) formularios W-9 del IRS en formato pdf, uno a nombre de Accounting Company y otro a nombre de AG Project Management.

- Cuatro (4) copias de facturas de servicio en formato pdf, dos a nombre de Accounting Company y dos a nombre de AG Project Management.

En esta figura Emil Rensing está enviando a James Robins (proveedor-1), un formulario de W-9 del IRS para que este sea completado en su totalidad y se lo reenvíe.



Figura # 5: Correo electrónico enviado por Emil Rensing a James Robins.

En esta figura James Robins le está enviando a Emil Rensing el formulario W-9 del IRS que este le había indicado que completara.

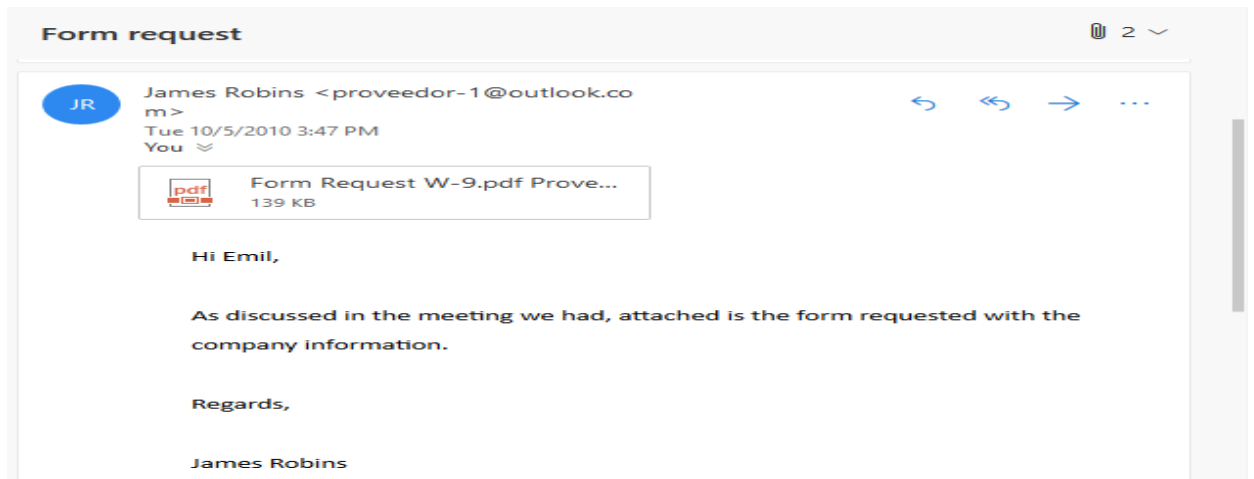


Figura # 6: Correo electrónico enviado por a James Robins a Emil Rensing.

En esta figura Emil Rensing le está indicando a James Robins que los servicios se realizaran tres veces a la semana comenzando el próximo lunes y preguntándole si está de acuerdo.

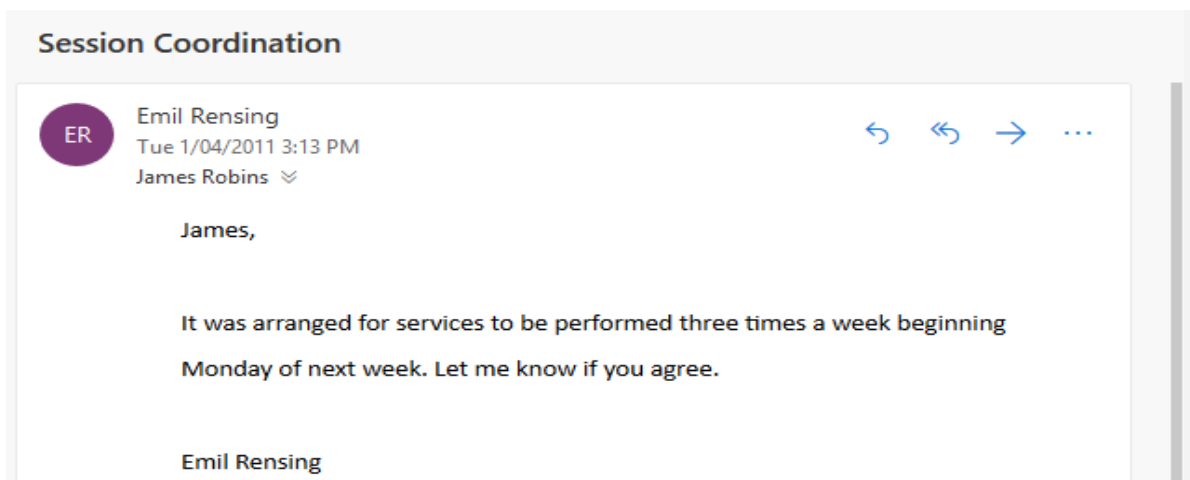


Figura # 7: Correo electrónico para coordinar sesiones de servicio.

En esta figura James Robins le está confirmando a Emil Rensing que está de acuerdo con la coordinación de los servicios pautados.

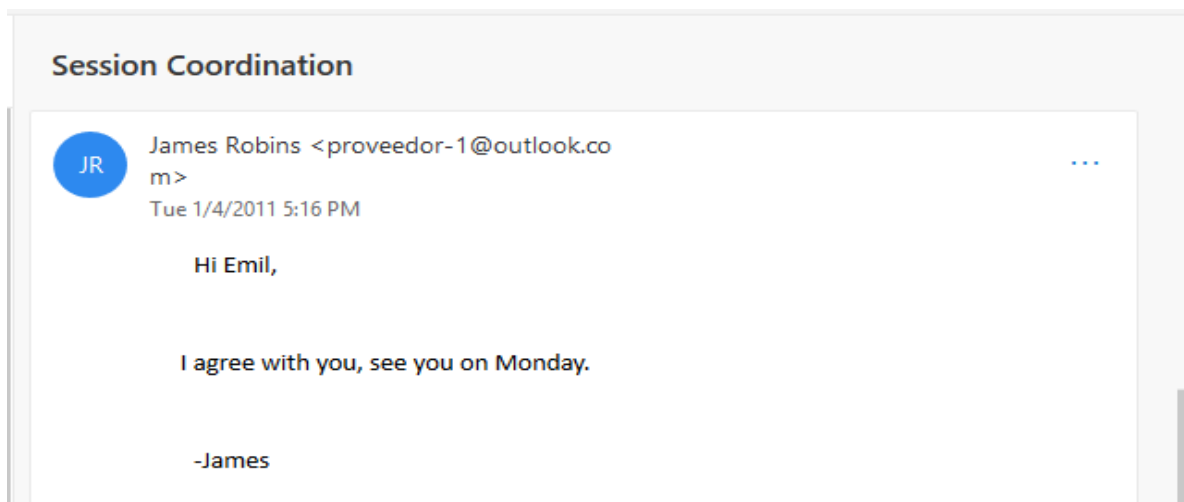


Figura # 8: Correo electrónico de confirmación de las sesiones de servicios.

En esta figura James Robins le esta enviado a Emil Rensing la primera factura de los servicios realizados durante el primer mes.

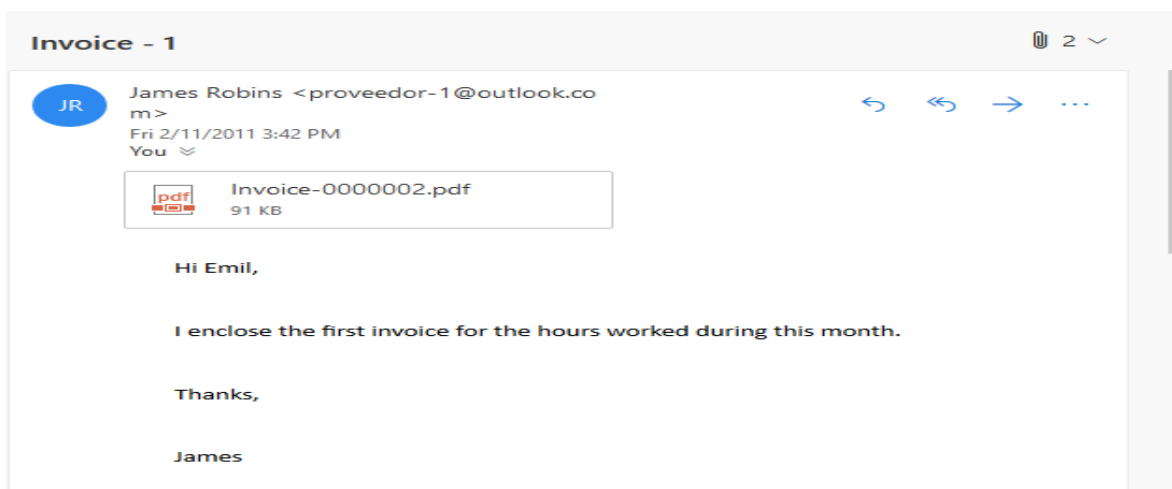


Figura # 9: Correo electrónico de James Robins con la primera factura de servicio.

En esta figura Emil Rensing esra enviando a James la evidencia de la transferencia bancaria de la primera factura de servicio.

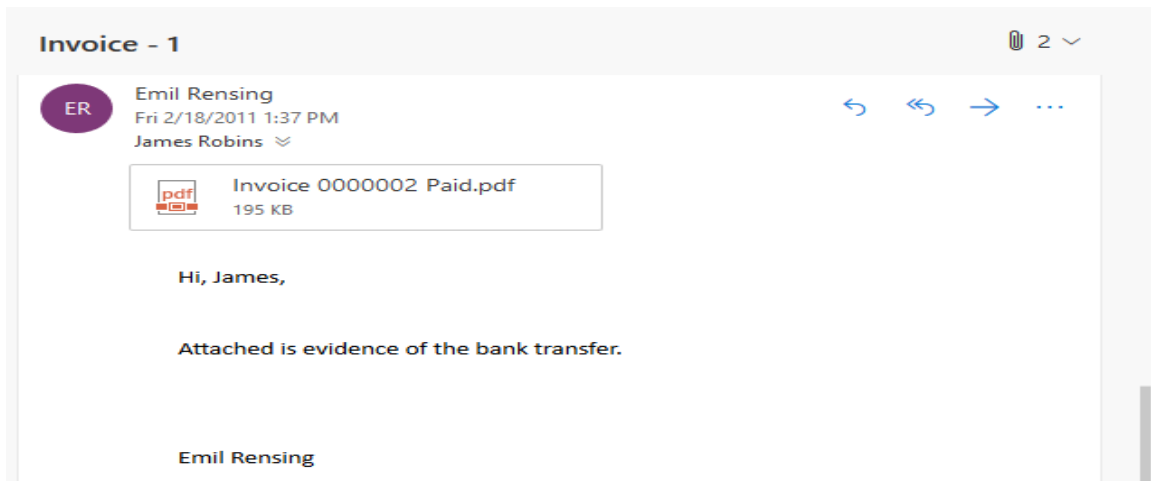


Figura # 10: Correo electrónico de Emil Rensing confirmando transferencia de pago.

En esta figura esta el formulario W-9 del IRS a nombre de Accounting Company con datos de la compania.

<p>Form W-9 (Rev. October 2010) Department of the Treasury Internal Revenue Service</p>	<p>Request for Taxpayer Identification Number and Certification</p> <p>Go to www.irs.gov/FormW9 for instructions and the latest information.</p>	<p>Give Form to the requester. Do not send to the IRS.</p>																						
<p>Print or type. See Specific Instructions on page 3.</p>	<p>1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.</p> <p>Provider</p>																							
	<p>2 Business name/disregarded entity name, if different from above</p> <p>Accounting Company</p>																							
	<p>3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only one of the following seven boxes.</p> <p><input type="checkbox"/> Individual sole proprietor or single-member LLC</p> <p><input checked="" type="checkbox"/> C Corporation</p> <p><input type="checkbox"/> S Corporation</p> <p><input type="checkbox"/> Partnership</p> <p><input type="checkbox"/> Trust/estate</p> <p><input type="checkbox"/> Limited liability company. Enter the tax classification (S-C corporation, 3-S corporation, P-Partnership) ▶ _____</p> <p>Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.</p> <p><input type="checkbox"/> Other (see instructions) ▶ _____</p>																							
	<p>4 Exemption codes apply only to certain entities, not individuals; see instructions on page 3:</p> <p>Exempt payee code (if any) _____</p> <p>Exemption from FATCA reporting code (if any) _____</p> <p>Applies to accounts maintained outside the U.S.</p>																							
	<p>5 Address (number, street, and apt, or suite no.) See instructions.</p> <p>740 Broadway #702</p>																							
	<p>6 City, state, and ZIP code</p> <p>Manhattan, NY 10003</p>																							
	<p>7 List account number(s) here (optional)</p>																							
<p>Part I Taxpayer Identification Number (TIN)</p>																								
<p>Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I later. For other entities, it is your employer identification number (EIN). If you do not have a number, see <i>How to get a TIN</i> later.</p> <p>Note: If the account is in more than one name, see the instructions for line 1. Also see <i>What Name and Number To Give the Requester</i> for guidelines on whose number to enter.</p>																								
		<p>Social security number</p> <table border="1" style="width: 100%; text-align: center;"> <tr> <td>0</td><td>6</td><td>7</td><td>-</td><td>5</td><td>8</td><td>-</td><td>5</td><td>7</td><td>7</td><td>8</td> </tr> </table> <p>or</p> <p>Employer identification number</p> <table border="1" style="width: 100%; text-align: center;"> <tr> <td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td> </tr> </table>	0	6	7	-	5	8	-	5	7	7	8											
0	6	7	-	5	8	-	5	7	7	8														
<p>Part II Certification</p>																								
<p>Under penalties of perjury, I certify that:</p> <ol style="list-style-type: none"> The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and I am a U.S. citizen or other U.S. person (defined below); and The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct. <p>Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.</p>																								
<p>Sign Here</p>	<p>Signature of U.S. person ▶ <u>James Robins</u></p>	<p>Date ▶ <u>10/12/2010</u></p>																						
<p>General Instructions</p> <p>Section references are to the Internal Revenue Code unless otherwise noted.</p> <p>Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to www.irs.gov/FormW9.</p> <p>Purpose of Form</p> <p>An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following:</p> <ul style="list-style-type: none"> Form 1099-INT (interest earned or paid) Form 1099-DIV (dividends, including those from stocks or mutual funds) Form 1099-MISC (various types of income, prizes, awards, or gross proceeds) Form 1099-B (stock or mutual fund sales and certain other transactions by brokers) Form 1099-S (proceeds from real estate transactions) Form 1099-K (merchant card and third party network transactions) Form 1098 (home mortgage interest), 1098-C (student loan interest), 1099-T (tuition) Form 1099-C (canceled debt) Form 1099-A (acquisition or abandonment of secured property) <p>Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.</p> <p>If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See <i>What is backup withholding</i>, later.</p>																								
<p>Get No. 10231X Form W-9 (Rev. 10-2010)</p>																								

Figura #11 : Formulario del W-9 del IRS de Accounting Company.

En esta figura esta el formulario W-9 del IRS a nombre de AG Project Management con datos de la compañía.

W-9 Request for Taxpayer Identification Number and Certification

Form (Rev. October 2014)
Department of the Treasury
Internal Revenue Service

Go to www.irs.gov/FormW9 for instructions and the latest information.

Give Form to the requester. Do not send to the IRS.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.
Provider-2

2 Business name/disregarded entity name, if different from above
AG Project Management

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only one of the following seven boxes.
 Individual sole proprietor or single-member LLC
 C Corporation
 S Corporation
 Partnership
 Trust/estate
 Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) **P**
 Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is not disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.
 Other (see instructions) **P**

4 Exemption codes apply only to certain entities; not individuals; see instructions on page 3:
Exempt payee code (if any) _____
Exemption from FATCA reporting code (if any) _____
(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.). See instructions.
45 Main St #526

6 City, state, and ZIP code
Brooklyn, NY 11201

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)
Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN), however, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see How to get a TIN, later.
Note: If the account is in more than one name, see the instructions for line 1. Also see What Name and Number To Give the Requester for guidelines on whose number to enter.

Social security number										
0	6	7	-	3	9	-	4	5	6	3
or										
Employer identification number										

Part II Certification
Under penalties of perjury, I certify that:
 1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
 2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
 3. I am a U.S. citizen or other U.S. person (defined below); and
 4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.
Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part I, later.

Sign Here Signature of U.S. person **Alan Goodman** Date **12/05/2014**

General Instructions
Section references are to the Internal Revenue Code unless otherwise noted.
Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to www.irs.gov/FormW9.

Purpose of Form
An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following:
 • Form 1099-INT (interest earned or paid)
 • Form 1099-DIV (dividends, including those from stocks or mutual funds)
 • Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
 • Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
 • Form 1099-S (proceeds from real estate transactions)
 • Form 1099-K (merchant card and third party network transactions)
 • Form 1098 (home mortgage interest), 1098-C (student loan interest), 1098-T (tuition)
 • Form 1099-C (canceled debt)
 • Form 1099-A (acquisition or abandonment of secured property)
 Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.
 If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, later.

OMB No. 1545-0047 Form **W-9** (Rev. 10-2014)

Figura # 12: Formulario del W-9 del IRS a nombre de AG Project Management.

Esta figura muestra la factura No.0000002 de la primera sesion de servicio a nombre de Accounting Company.



Accounting Company

740 Broadway, #702
Manhattan, NY 10003
United States

Amount due

\$500,000.00

USD

Due
Upon receipt

Issued
2/11/11

Invoice No. 0000002

Accounting Services

Description	Qty	Price	Amount
Accounting Services	1	\$500,000.00	\$500,000.00
		Total	\$500,000.00
		Amount due	\$500,000.00

Notes:

First session

EPIX CORPORATE
United States

Figura # 13: Factura No.0000002 a nombre de Accounting Company

Esta figura muestra la factura No.0000547 de la quinta sesion de servicio a nombre de Accounting Company.



Accounting Company
740 Broadway, #702
Manhattan, NY 10003
United States

Amount due
\$500,000.00

USD

Due
Upon receipt

Issued
5/27/11

Invoice No. 0000547

Accounting Services

Description	Qty	Price	Amount
Accounting Services	1	\$500,000.00	\$500,000.00
Total			\$500,000.00
Amount due			\$500,000.00

Notes:

Fifth session

EPHX CORPORATE
United States

Figura # 14: Factura No.0000547 a nombre de Accounting Company

Esta figura muestra la factura No.623 del primer proyecto de AG Project Management.



AG Project Management
45 Main, #526
Brooklyn, NY 11201
United States

Amount due
\$250,000.00

USD

Due
Upon receipt

Issued
1/23/15

Invoice No. 623

Digital Services

Description	Qty	Price	Amount
Digital Services	1	\$250,000.00	\$250,000.00
Total			\$250,000.00
Amount due			\$250,000.00

Notes:

First project

EPIX CORPORATE
United States

Figura # 15: Factura No.623 a nombre de AG Project Management.

Esta figura muestra la factura No.901 del primer proyecto de AG Project Management.



AG Project Management
45 Main, #526
Brooklyn, NY 11201
United States

Amount due
\$250,000.00

USD

Due Upon receipt Issued 4/24/15

Invoice No. 901

Digital Services

Description	Qty	Price	Amount
Digital Services	1	\$250,000.00	\$250,000.00
Total			\$250,000.00
Amount due			\$250,000.00

Notes:

Third project

EPIX CORPORATE
United States

Figura # 16: Factura No.901 a nombre de AG Project Management

Cadena de custodia

JA Forensics. está comprometida con cumplir los protocolos y las reglas de evidencia requeridas para que cualquier evidencia pueda ser utilizada ante un tribunal, por lo que a continuación se describe en detalle la cadena de custodia del dispositivo en cuestión. La cadena de custodia se ocupa de evidenciar el proceso de adquisición, análisis y control de evidencia.

Primer evento:

1. Descripción del evento: Evidencia entregada por los fiscales Preet Bharara, Joon H. Kim y Geoffrey S. Berman y recibida por la Sra. Janice Fuentes, examinadora de Forense Digital de JA Forensics. La evidencia consiste en un USB Drive de 15GB.
2. Evento verificado por: La Sra. Janice Fuentes examinadora de Forense Digital, Preet Bharara, Joon H. Kim y Geoffrey S. Berman fiscales
3. Fecha de comienzo: 10 de enero de 2019 8:25 am
4. Fecha de terminación: 10 de enero de 2019 8:30 am
5. Lugar de origen: Corte Federal de Manhattan
6. Destino: Laboratorio Forense de JA Forensics

Segundo evento:

1. Descripción del evento: Creación de número de caso y asignación de la evidencia
2. Evento tramitado por: Sra. Janice Fuentes
3. Asignar número de caso: 103882-NY
4. Fecha de comienzo: 10 de enero de 2019 8:31 am

5. Fecha de terminación: 10 de enero de 2019 8:34 am
6. Lugar de origen: Laboratorio forense de JA Forensics
7. Destino: Laboratorio forense de JA Forensics

Tercer evento:

1. Descripción del evento: Creación de dos imágenes, una para ser preservada y la otra para realizar el análisis
2. Realizado por: Sra. Janice Fuentes
3. Número de caso asignado: 103882-NY
4. Fecha de comienzo: 10 de enero de 2019 8:35 am
5. Fecha de terminación: 10 de enero de 2019 12:45 pm
6. Lugar de origen: Laboratorio forense de JA Forensics
7. Destino: Laboratorio forense de JA Forensics

Cuarto evento:

1. Descripción del evento: Realización de análisis al USB Drive identificado como Evidence #94802
2. Realizado por: Sra. Janice Fuentes
3. Número de caso asignado: 103882-NY
4. Fecha de comienzo: 10 de enero de 2019 12:46 pm
5. Fecha de terminación: 10 de enero 2019 4:30 pm
6. Lugar de origen: Laboratorio forense de JA Forensics

Destino: Laboratorio forense de JA Forensics

Cuarto evento:

1. Descripción del evento: Guardar evidencia a ser analizada en la bóveda

2. Realizado por: Sra. Janice Fuentes y Sr. Eldel Meléndez
3. Número de caso asignado: 103882-NY
4. Fecha de comienzo: 10 de enero de 2019 4:31 pm
5. Fecha de terminación: 10 de enero 2019 4:33 pm
6. Lugar de origen: Laboratorio forense de JA Forensics
7. Destino: Laboratorio forense de JA Forensics

Quinto evento:

1. Descripción del evento: Sacar evidencia analizada en la bóveda
2. Realizado por: Sra. Janice Fuentes y Sr. Eldel Meléndez
3. Número de caso asignado: 103882-NY
4. Fecha de comienzo: 11 de enero de 2019 8:45 am
5. Fecha de terminación: 11 de enero 2019 8:47 am
6. Lugar de origen: Laboratorio forense de JA Forensics
7. Destino: Laboratorio forense de JA Forensics

Sexto evento:

1. Descripción del evento: Devolución de la evidencia a los fiscales Preet Bharara, Joon H. Kim y Geoffrey S. Berman
2. Realizado por: Sra. Janice Fuentes
3. Número de caso asignado: 103882-NY
4. Fecha de comienzo: 11 de enero de 2019 8:50 am
5. Fecha de terminación: 11 de enero de 2019 9:00 am
6. Lugar de origen: JA Forensics
7. Destino: Corte Federal de Manhattan

Procedimiento

Esta figura muestra las especificaciones de la computadora en la cual se realizó las investigación.

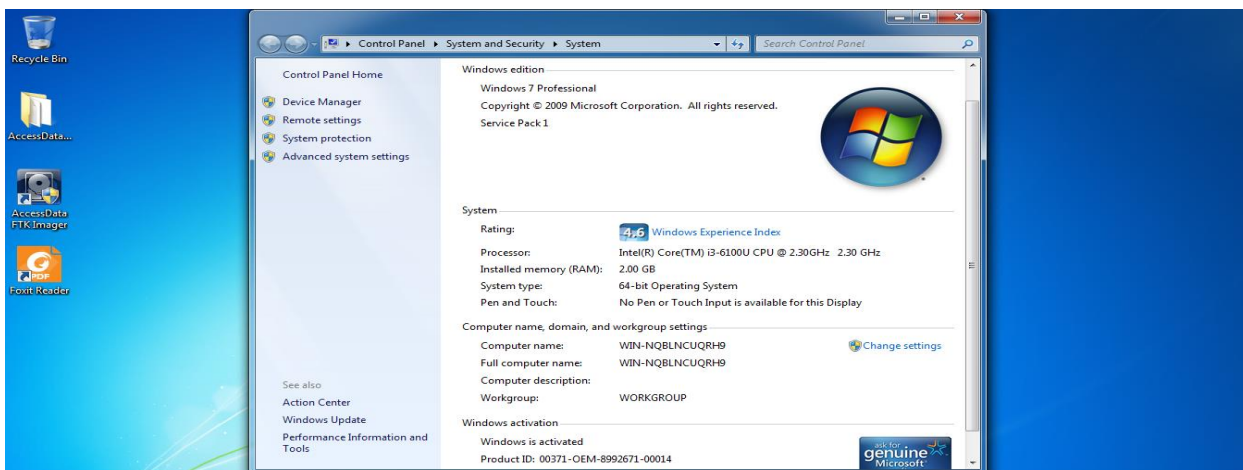


Figura # 17: Imagen con especificaciones de la computadora

Esta figura muestra las herramientas utilizadas para realizar la investigación

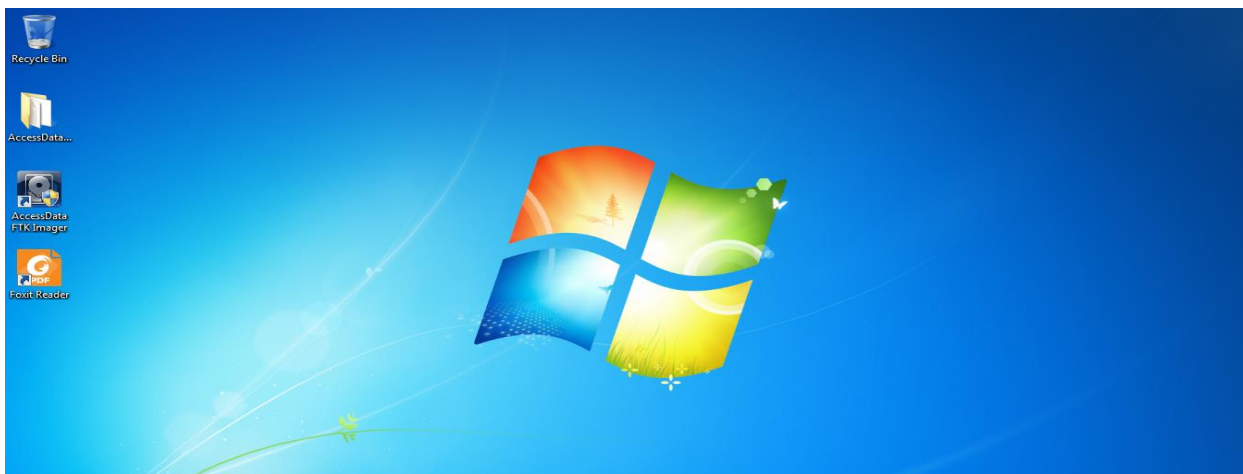


Figura # 18: Imagen con las herramientas instaladas para realizar la investigación

Esta figura muestra la pantalla principal de la herramienta AccessData FTK Imager

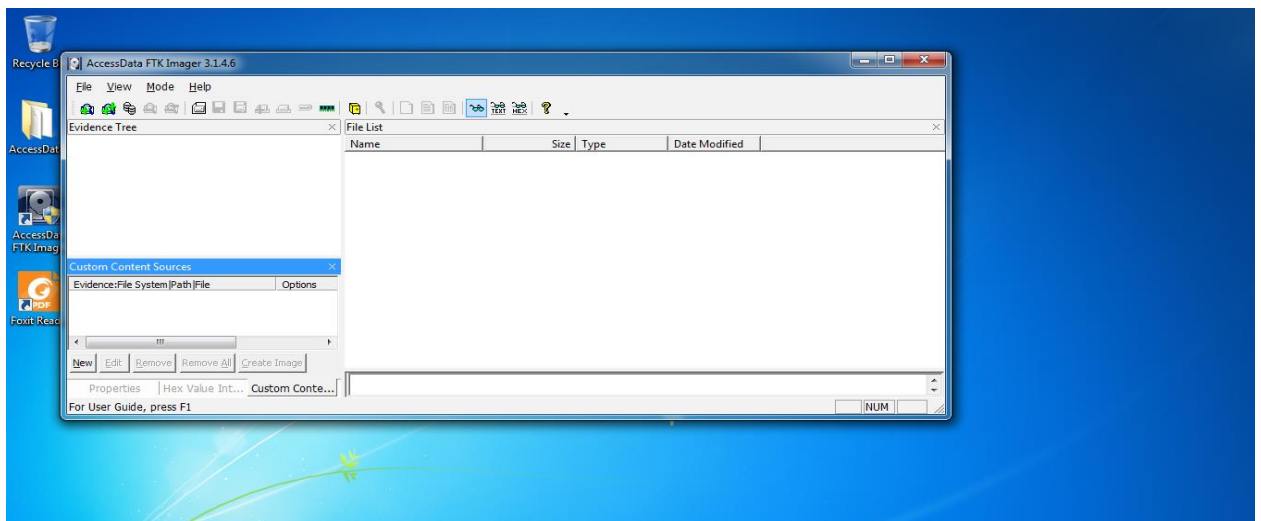


Figura # 19: Imagen de la aplicación AccessData FTK Imager 3.1.4.6

De la figura # 20 a la # 37 se puede observar el proceso realizado para crear la imagen del disco en la herramienta AccessData FTK Imager 3.1.4.6

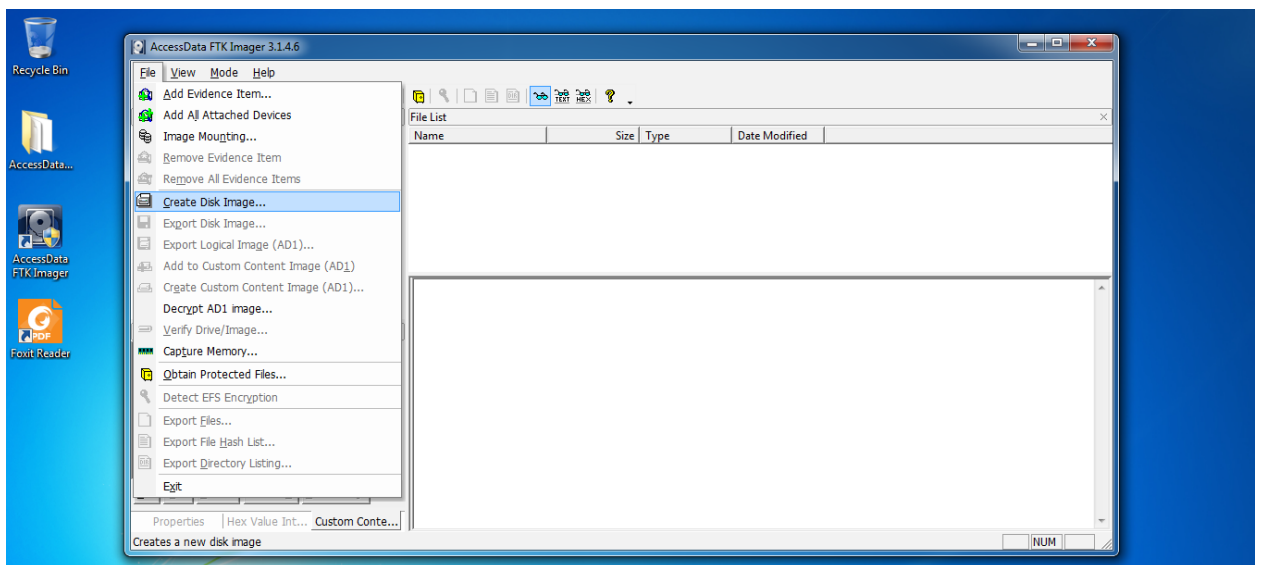


Figura # 20: Creación de la imagen del disco

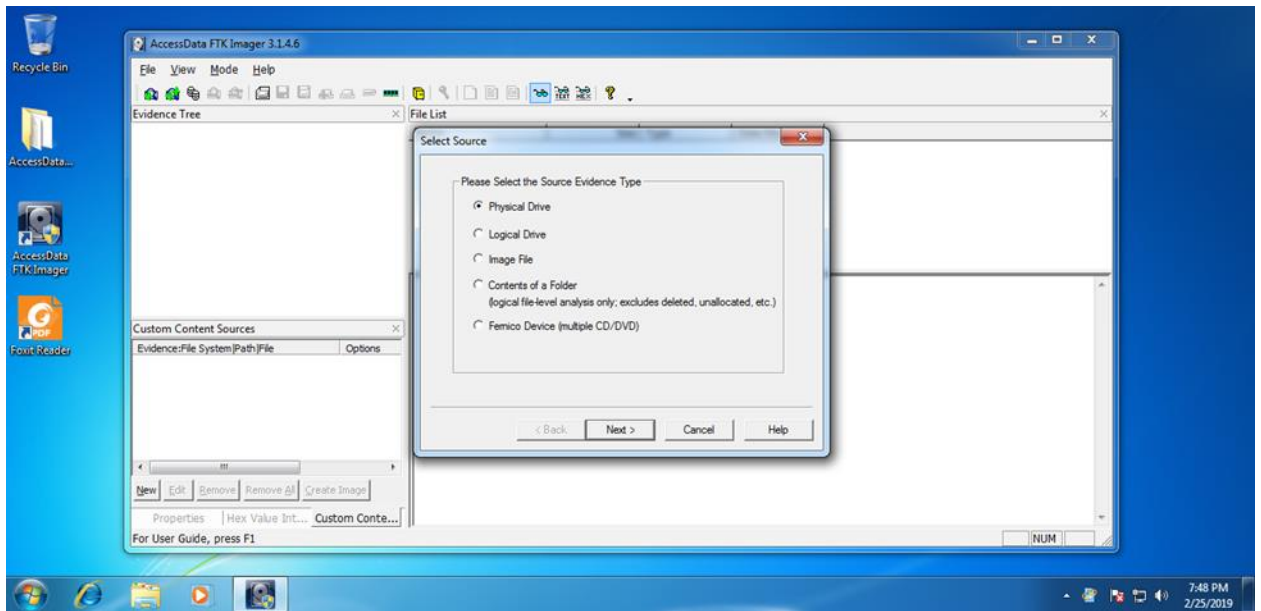


Figura # 21: Esta figura muestra la selección de la fuente de evidencias

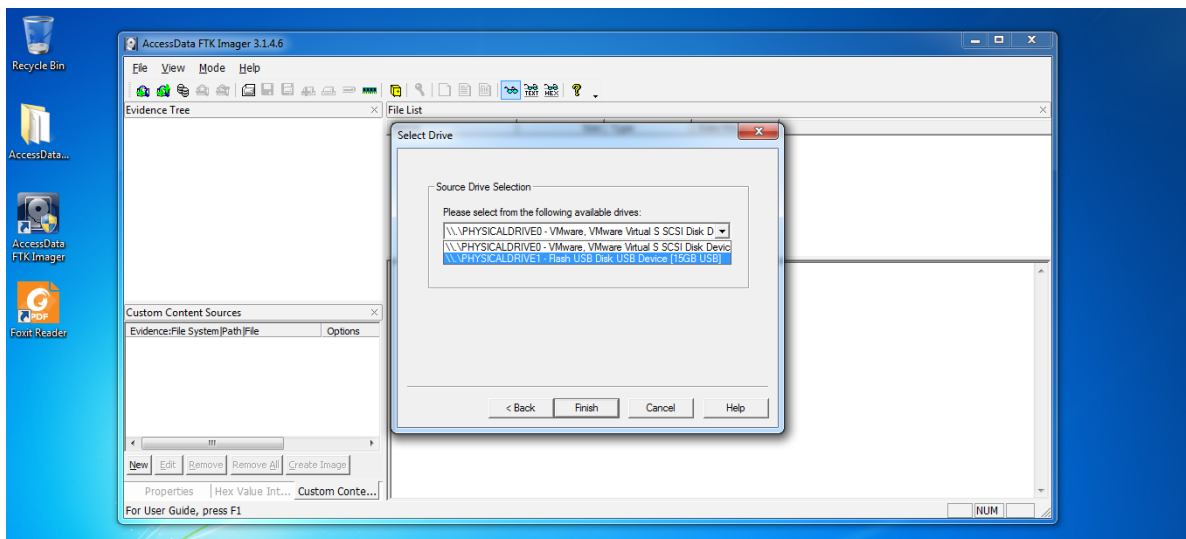


Figura # 22: Selección del dispositivo que se analizará

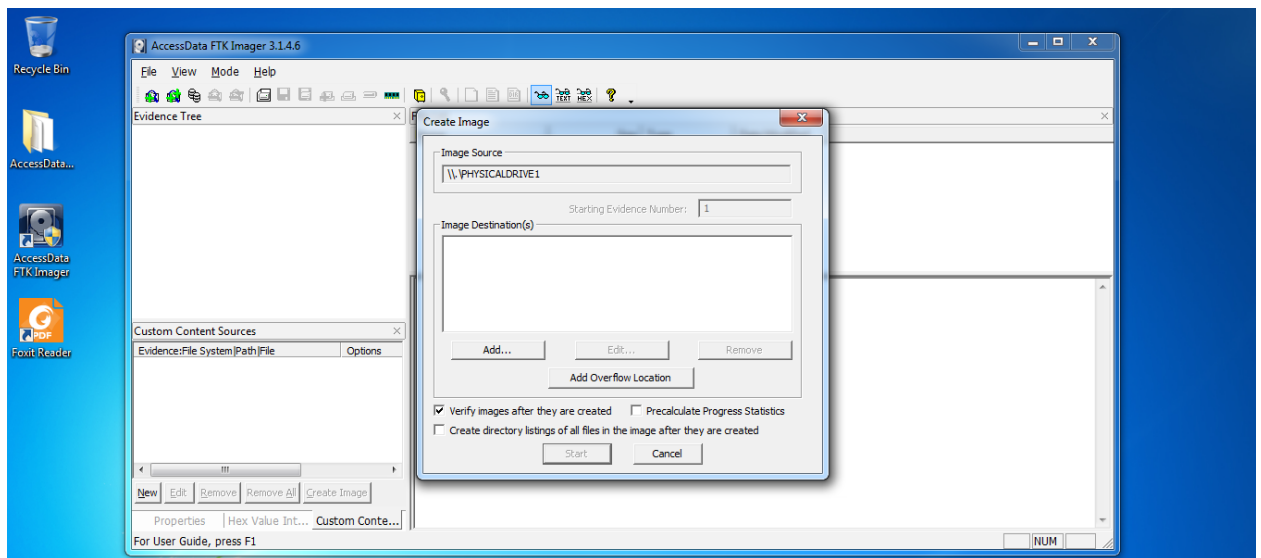


Figura # 23: Añadir el destino de la imagen a crearse

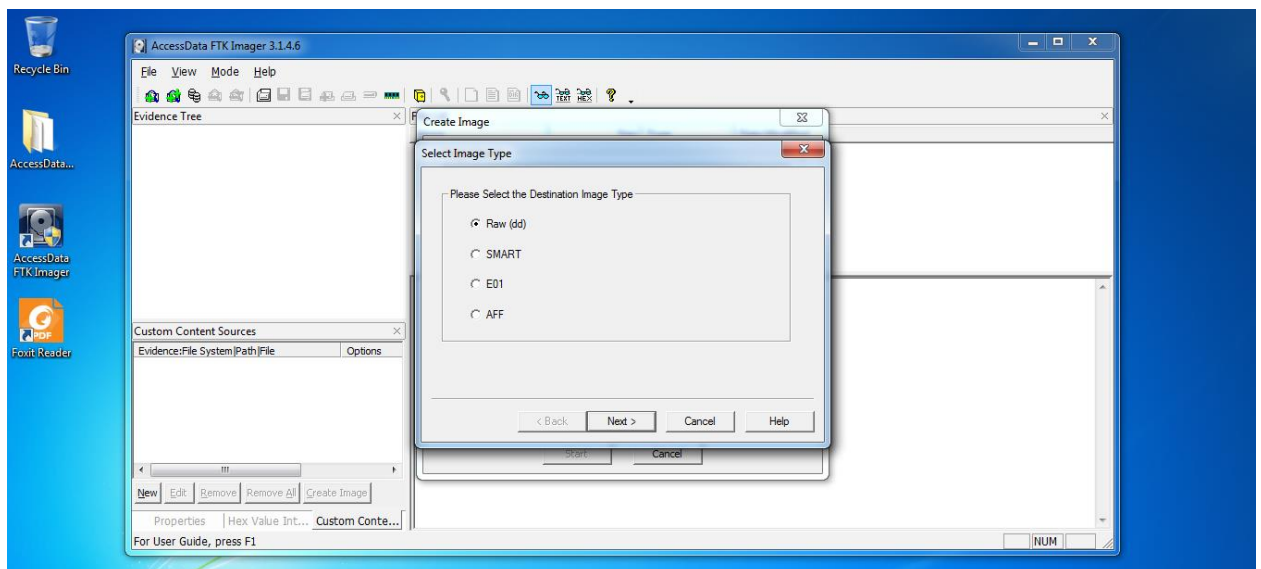


Figura # 24: Selección del tipo de imagen que se creará

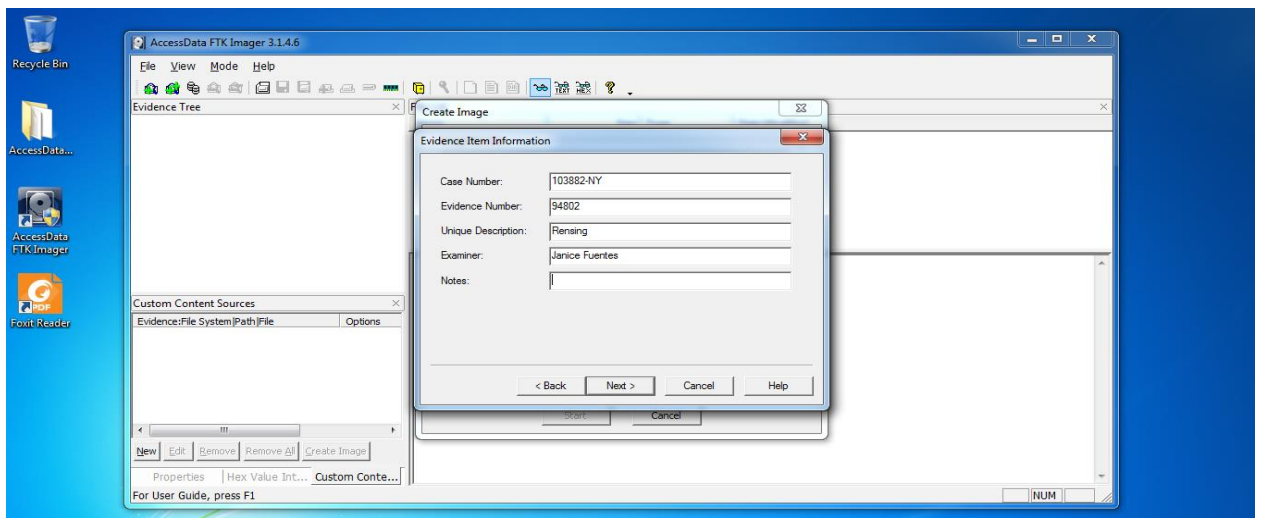


Figura # 25: Información de la evidencia recopilada

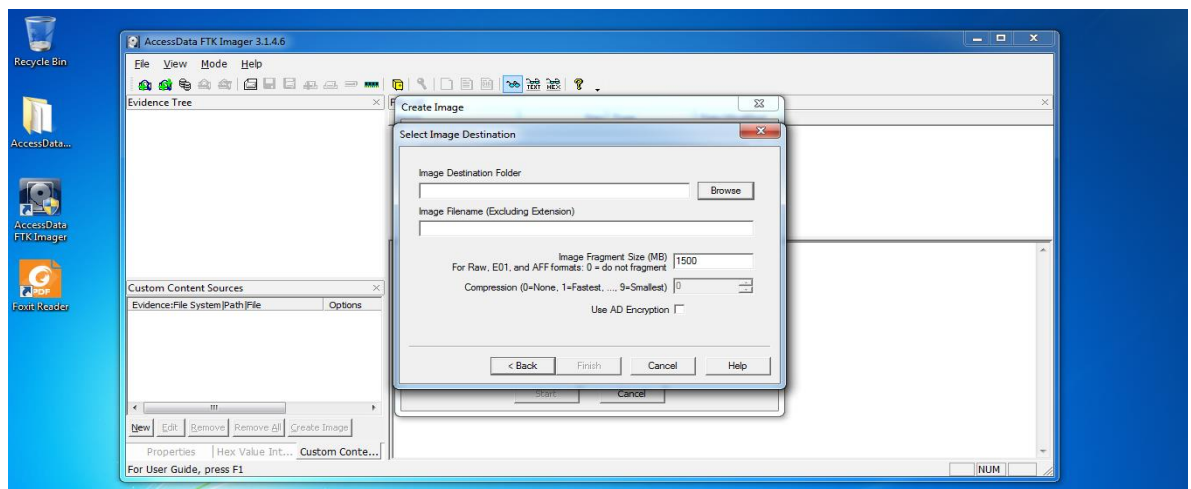


Figura # 26: Seleccionar donde se guardará la imagen creada

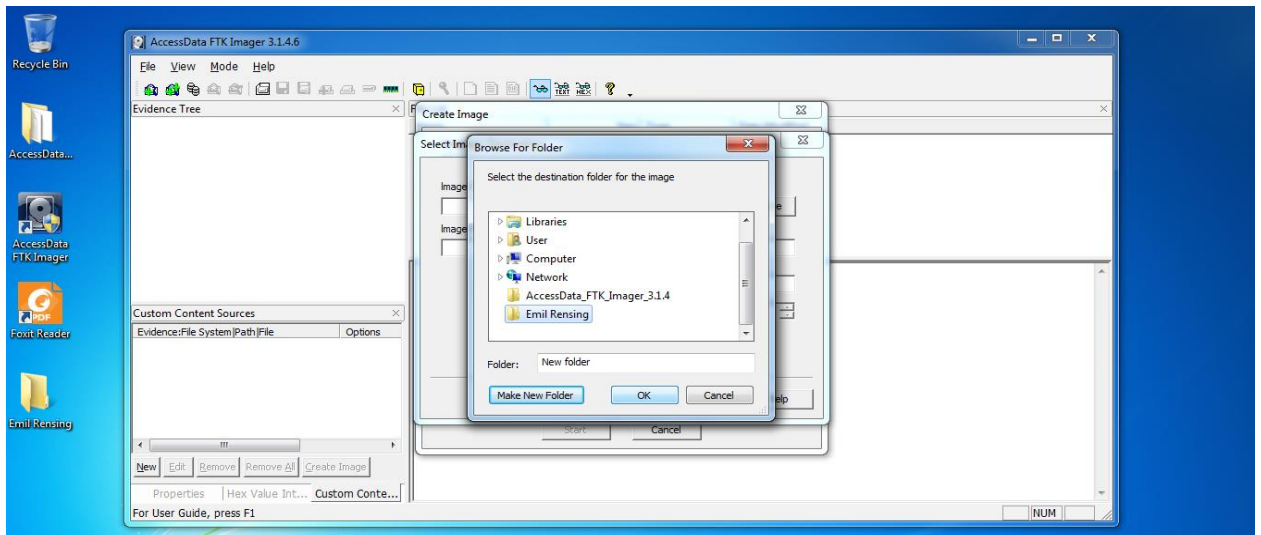


Figura # 27: Creación de folder en donde se guardará la imagen

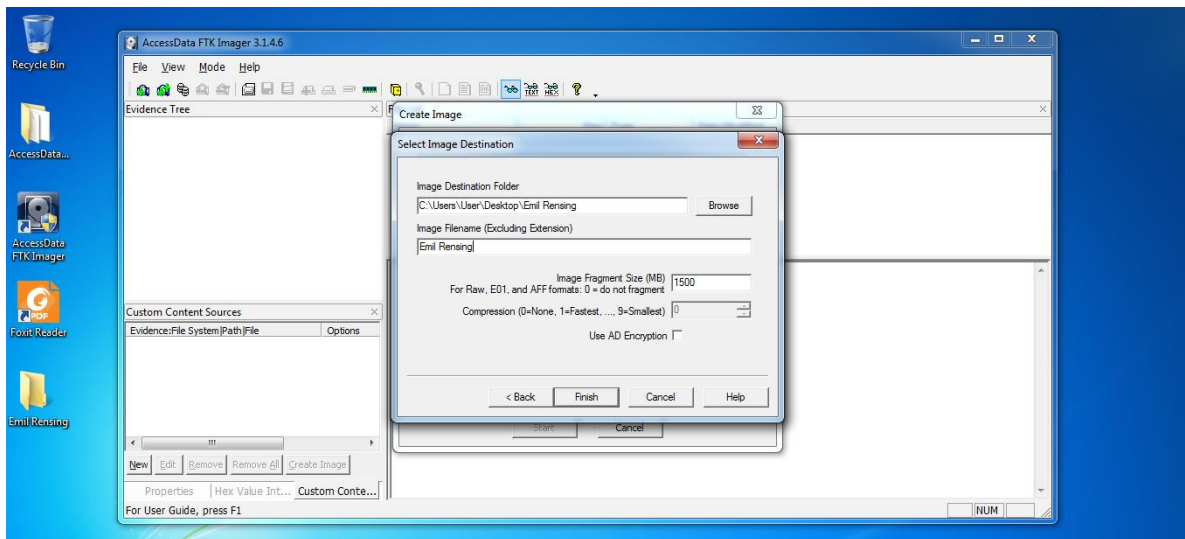


Figura # 28: Selección y nombre de folder de la imagen

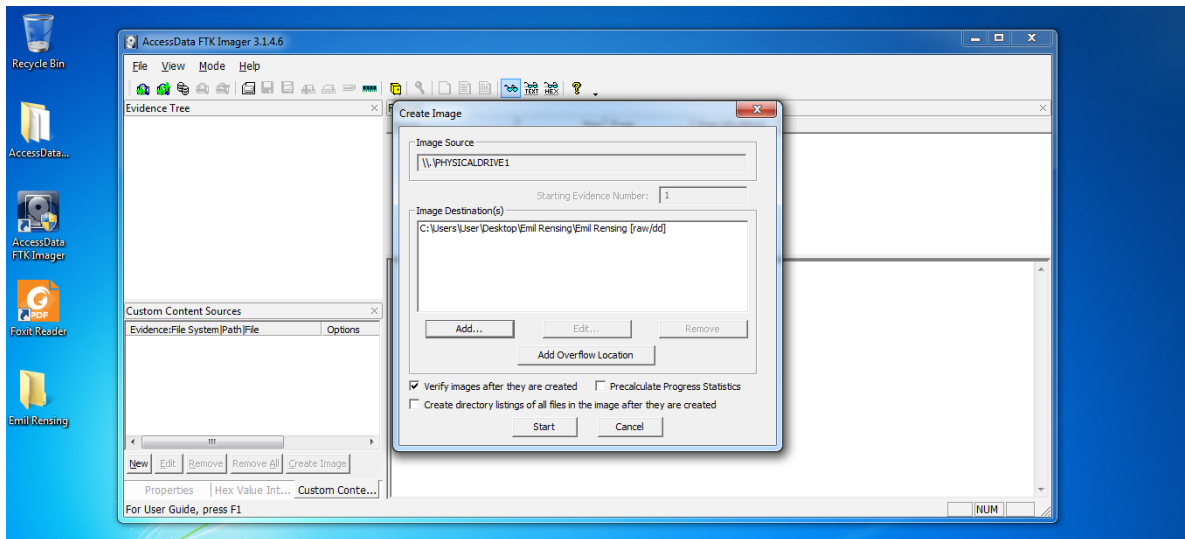


Figura #29: Comienzo de la creación de la imagen del disco

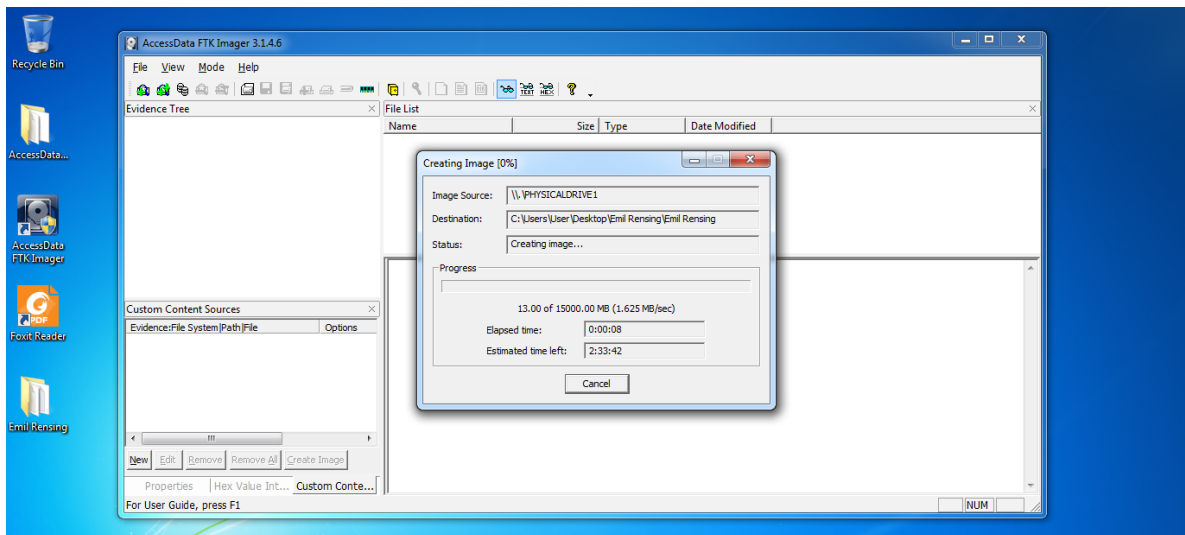


Figura # 30: Proceso de inicio creación de la imagen del disco

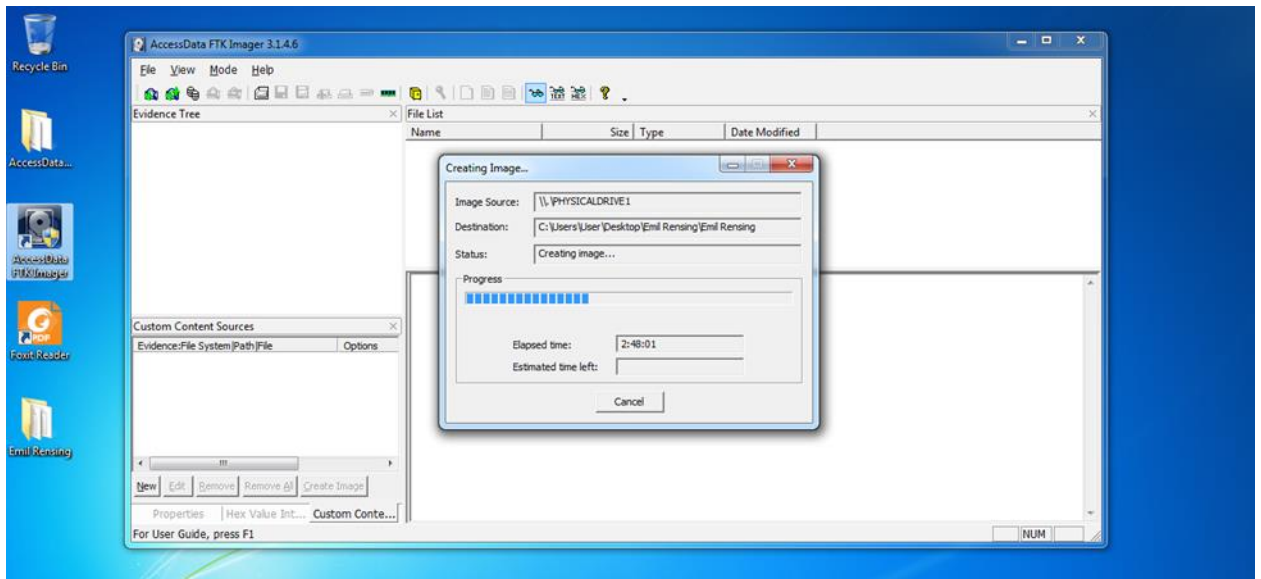


Figura # 31: Estatus de la creación de la imagen del disco

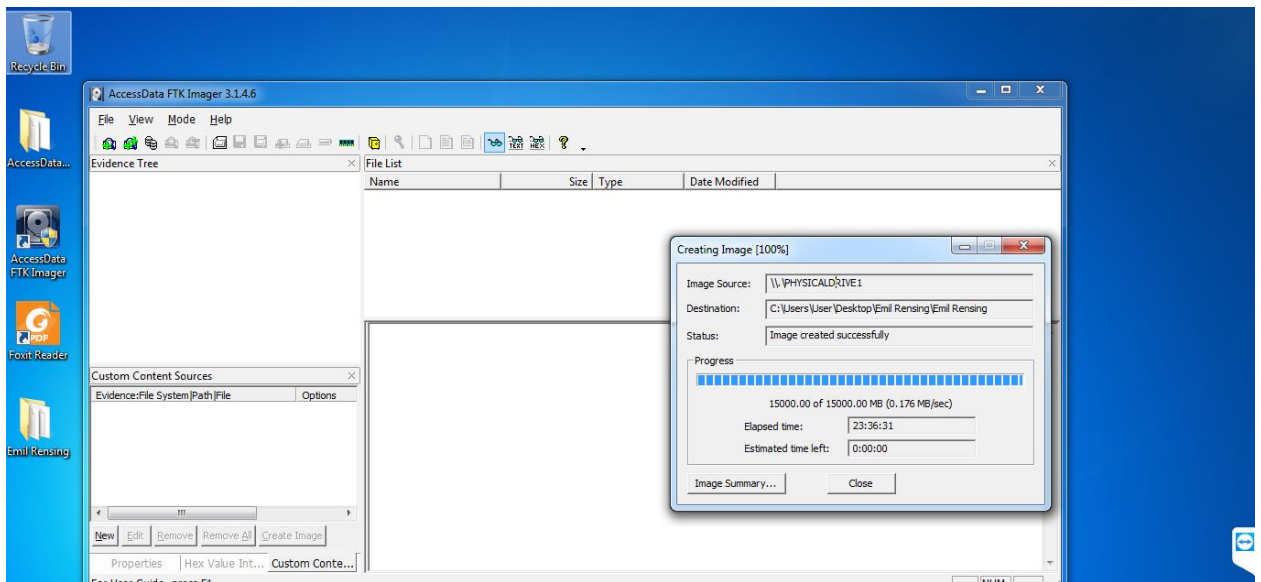


Figura # 32: Creación de la imagen del disco completada

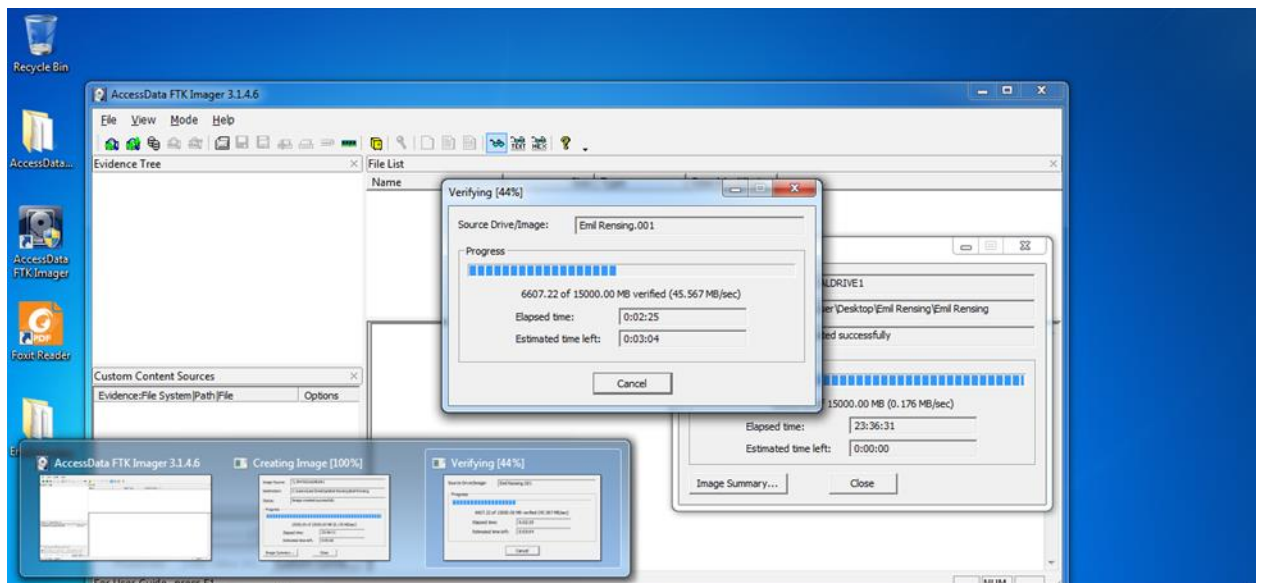


Figura # 33: Verificación de la imagen creada

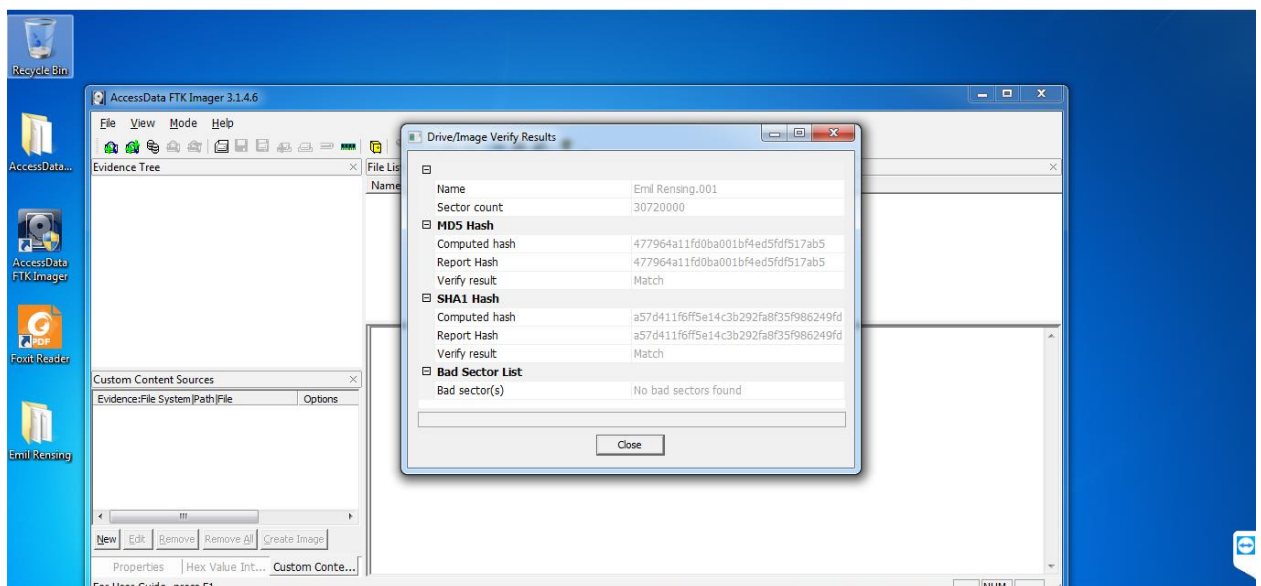


Figura # 34: Resultados de la imagen MD5 Hash y SHA1 Hash

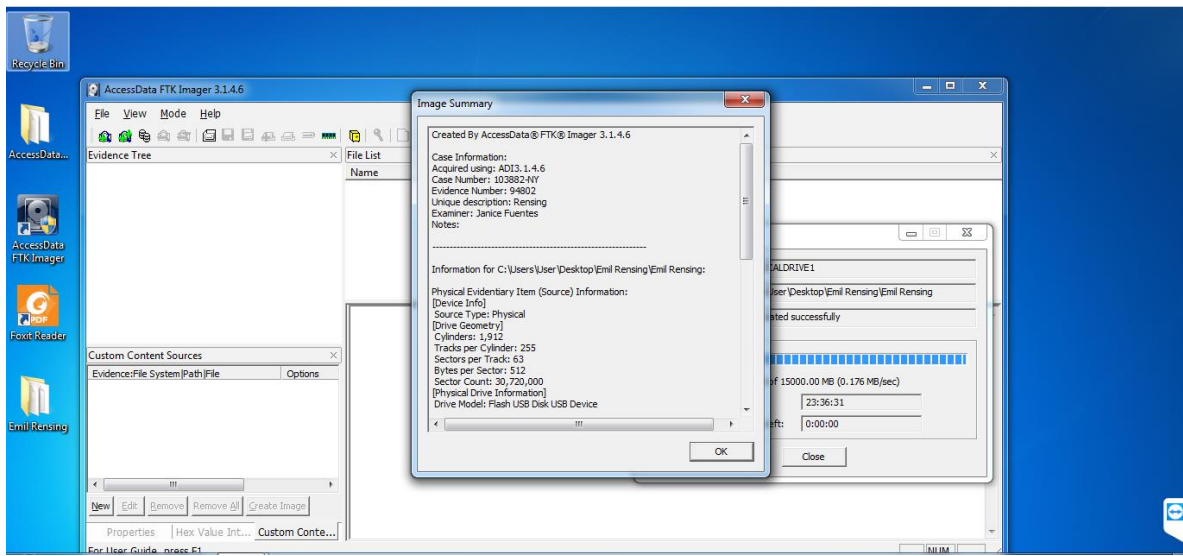


Figura # 35: Resumen de la imagen creada

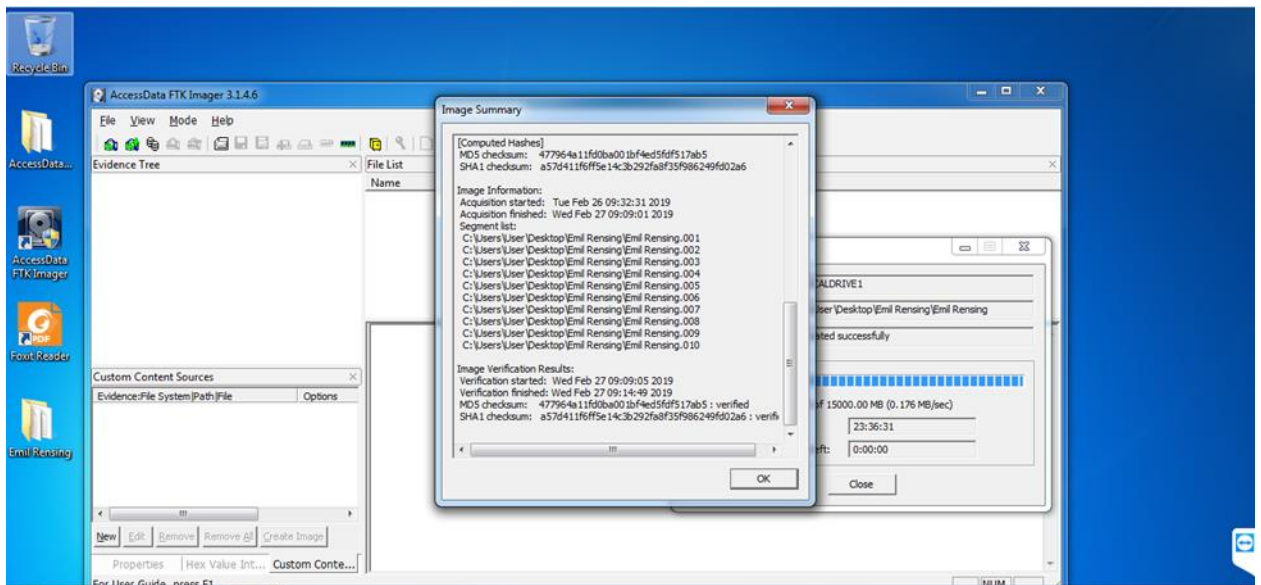


Figura # 36: Continuación resumen de la imagen creada

En las figuras de la #37 a la #41 se puede observar el proceso realizado luego de crear la imagen del disco, que es añadir la imagen para ser analizada.

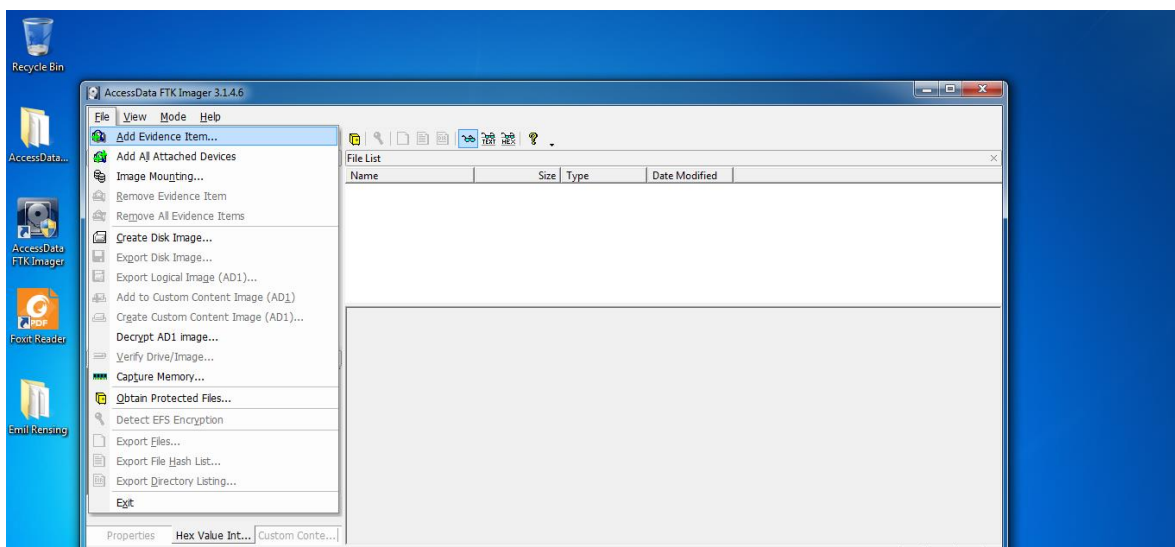


Figura # 37: Añadir imagen creada para análisis

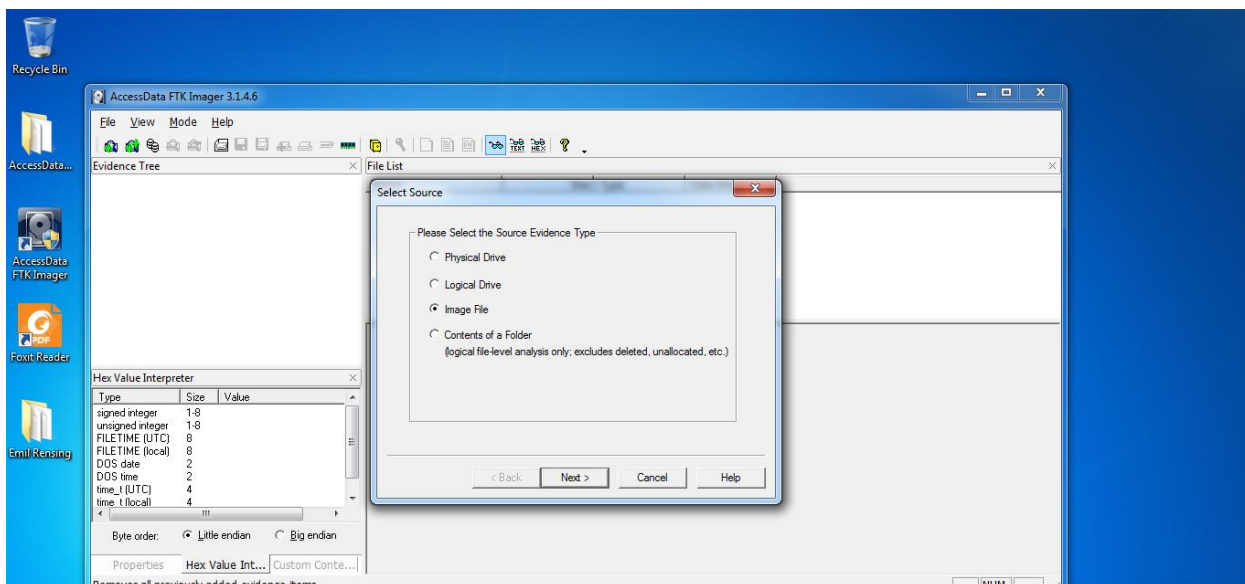


Figura # 38: Selección tipo de evidencia

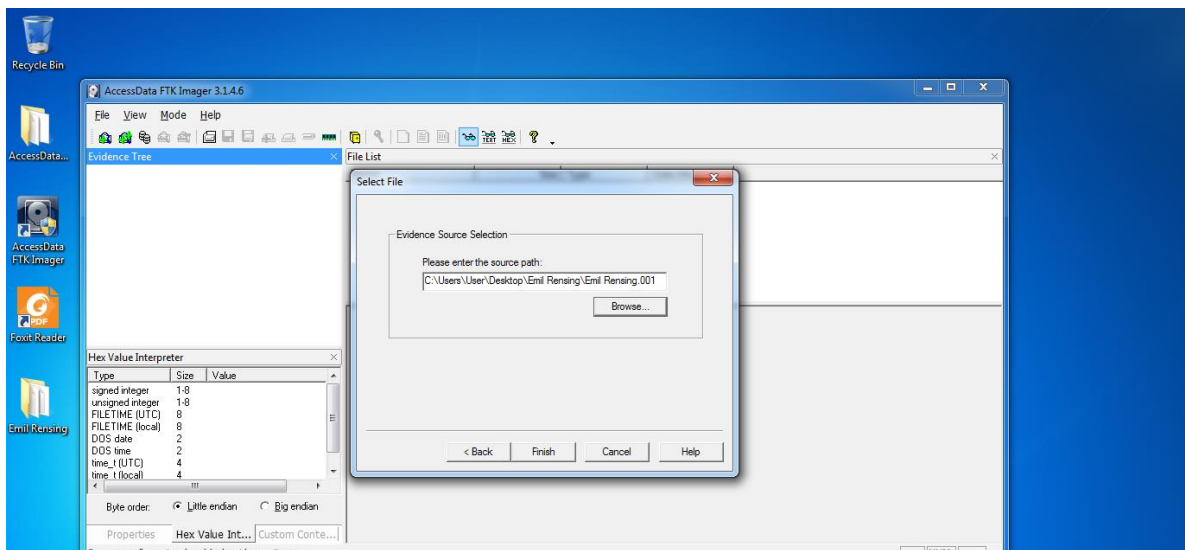


Figura # 39: Selección de fuente que se analizará

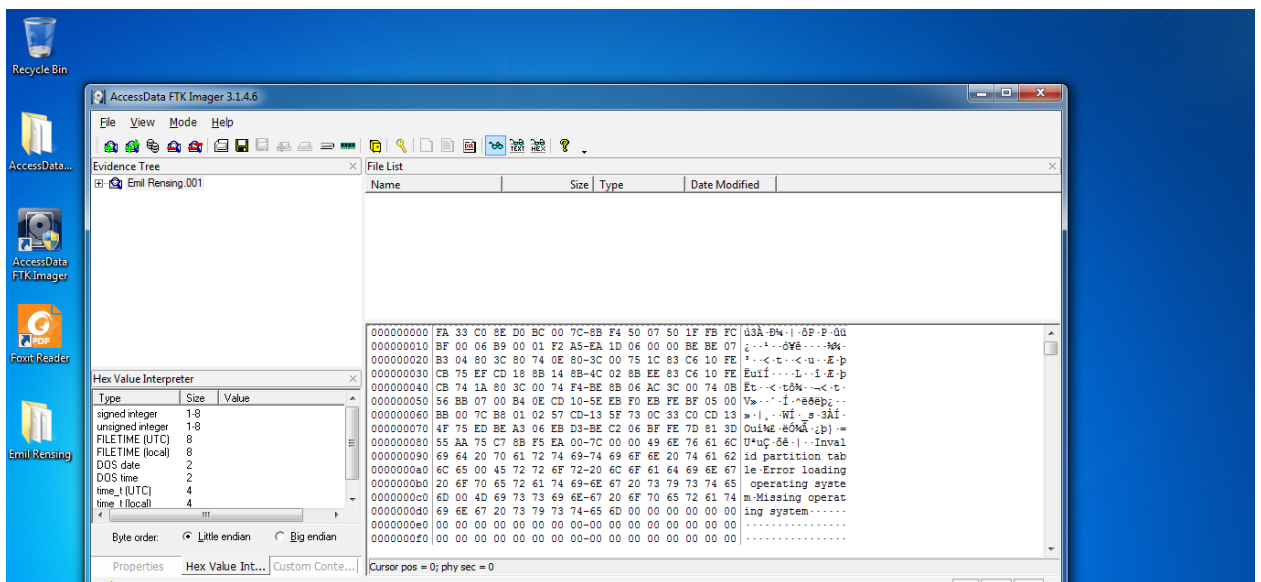


Figura # 40: Imagen creada aparece en el árbol de evidencia

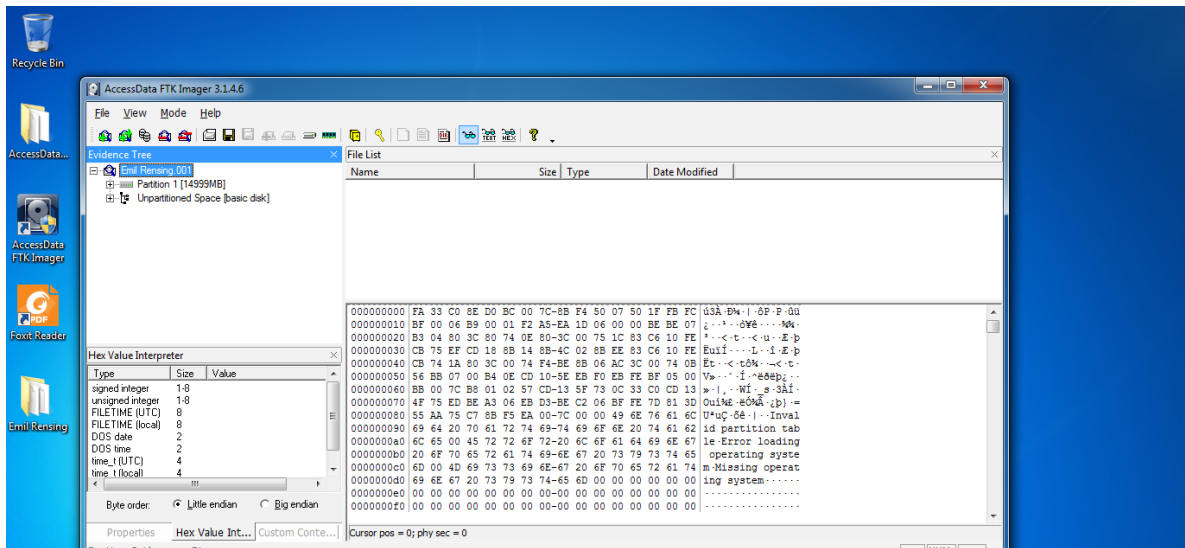


Figura # 41: Expansión de archivos del árbol de evidencia

En las figuras de la # 42 a la # 57 se puede observar toda la evidencia recopilada de la imagen de disco que fue analizada, el mismo es una copia fiel y exacta de la computadora incautada a Emil Rensing. Entre la evidencia recopilada se pueden apreciar correos electrónicos entre Rensing y los supuestos proveedores, facturas de los servicios que nunca se realizaron y formularios W-2 de los proveedores.

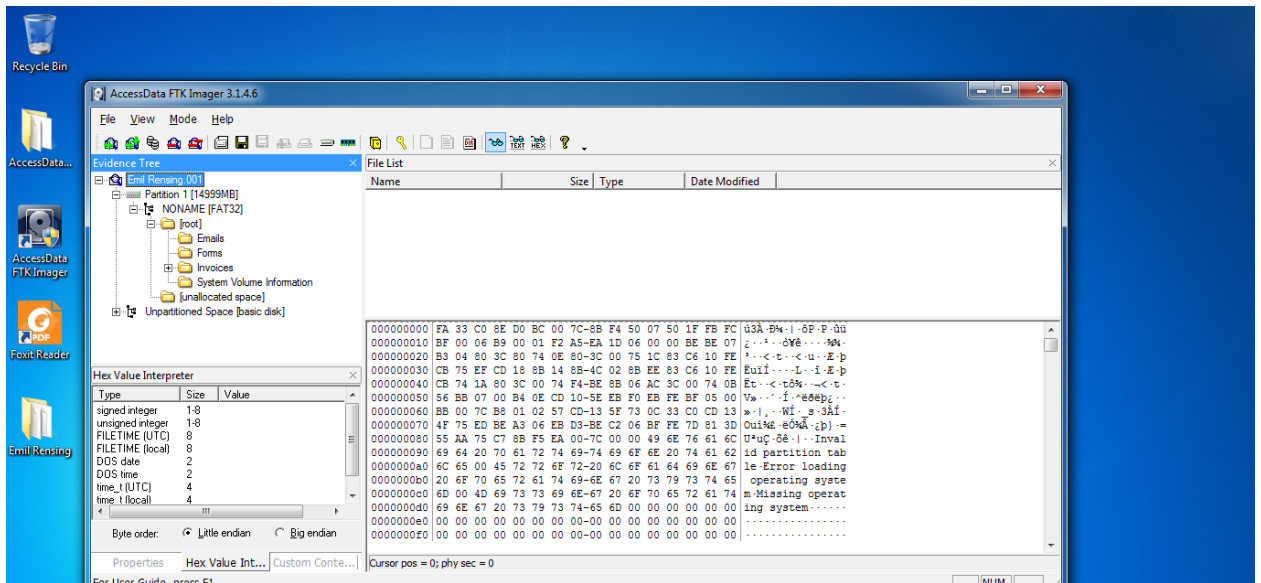


Figura # 42: Folders que aparecieron de la imagen creada

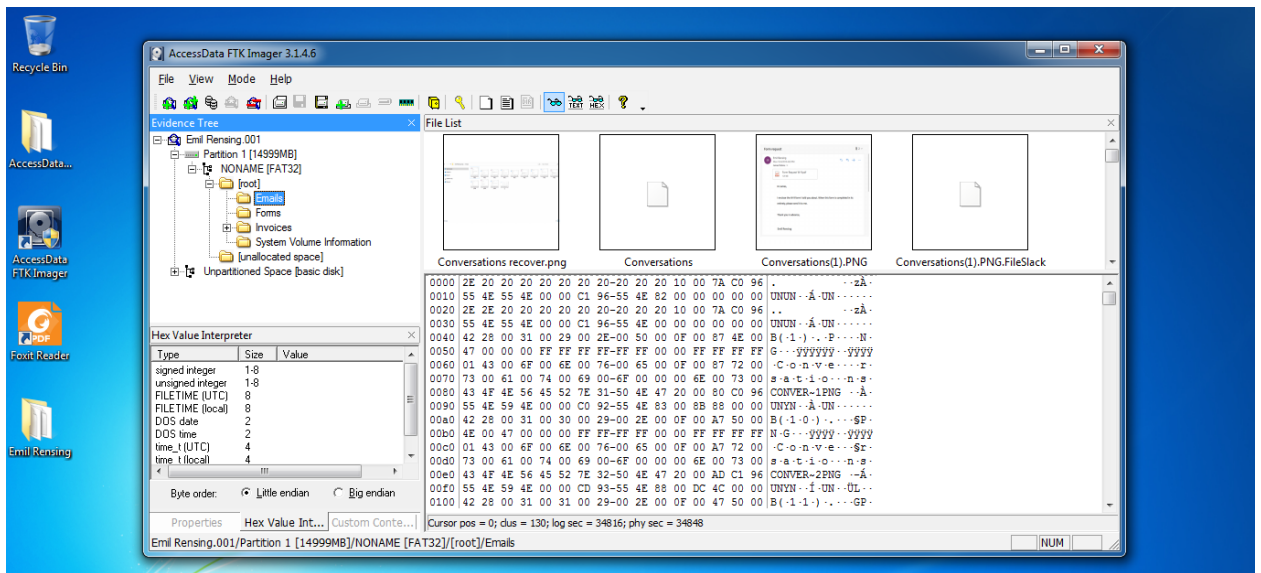


Figura # 43: Folder con evidencia de conversaciones

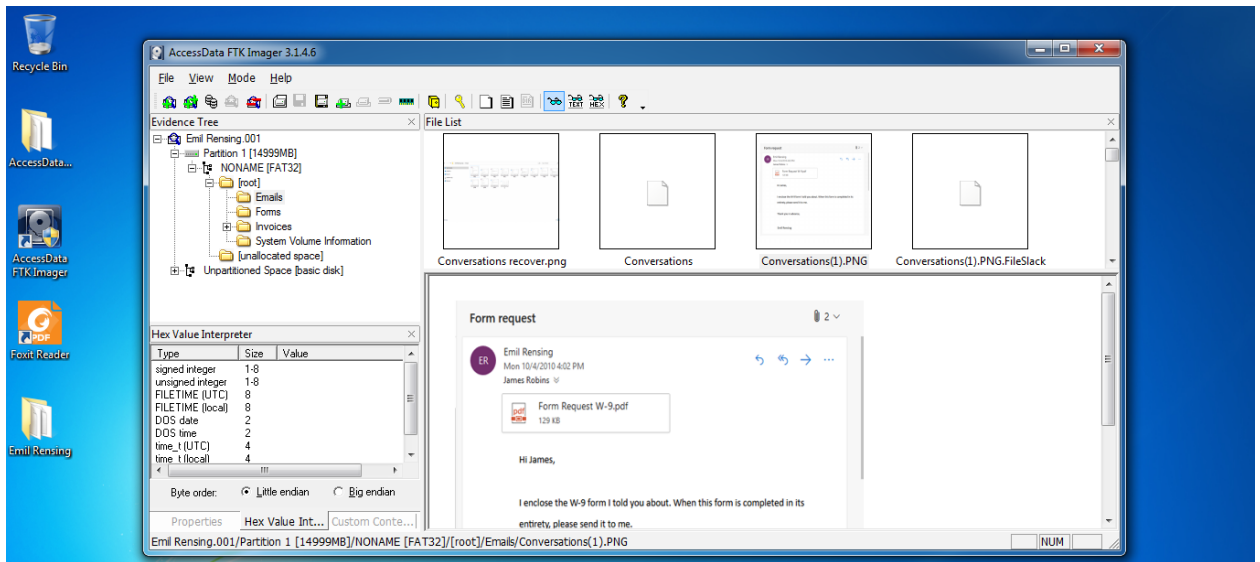


Figura # 44: Correo electrónico enviado por Emil Rensing a James Robins.

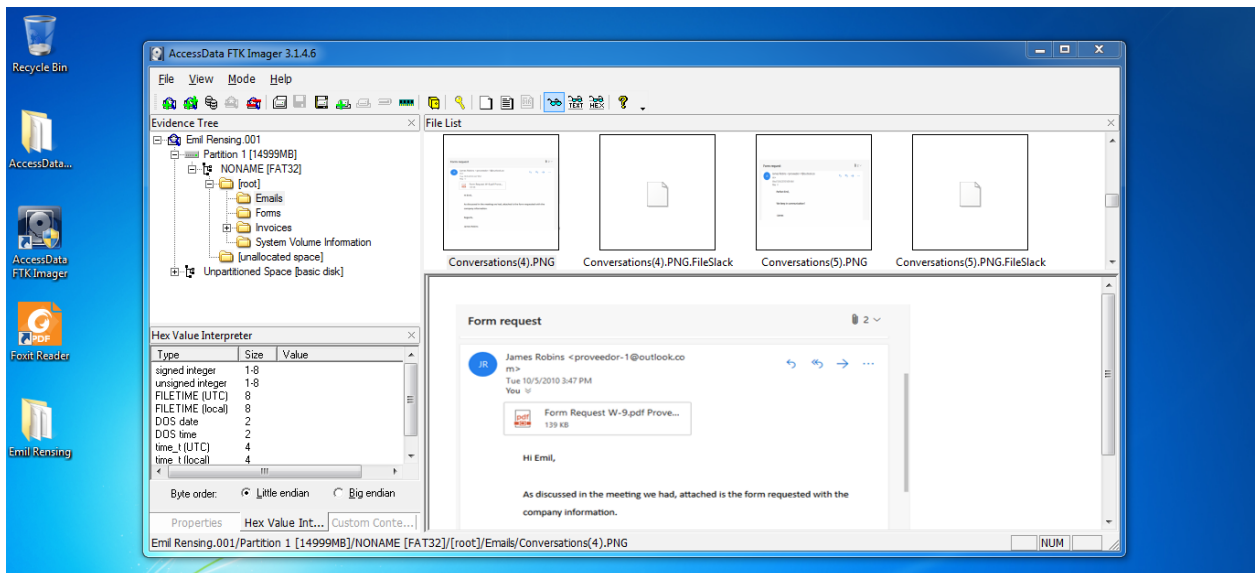


Figura # 45: Correo electrónico enviado por a James Robins a Emil Rensing.

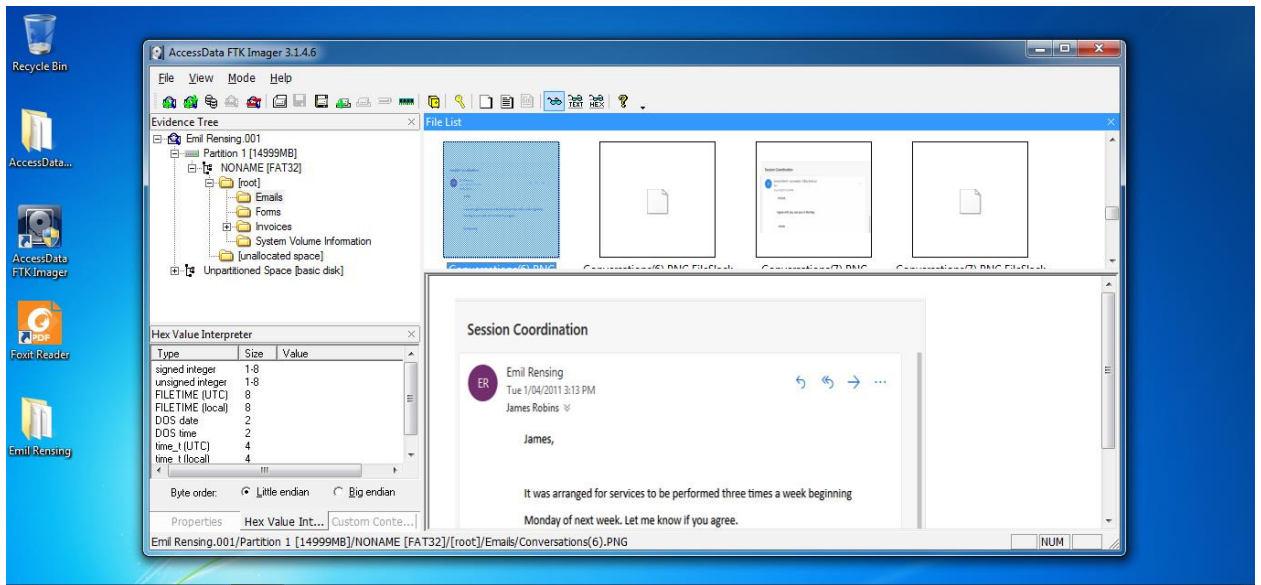


Figura # 46: Correo electrónico para coordinar sesiones de servicio.

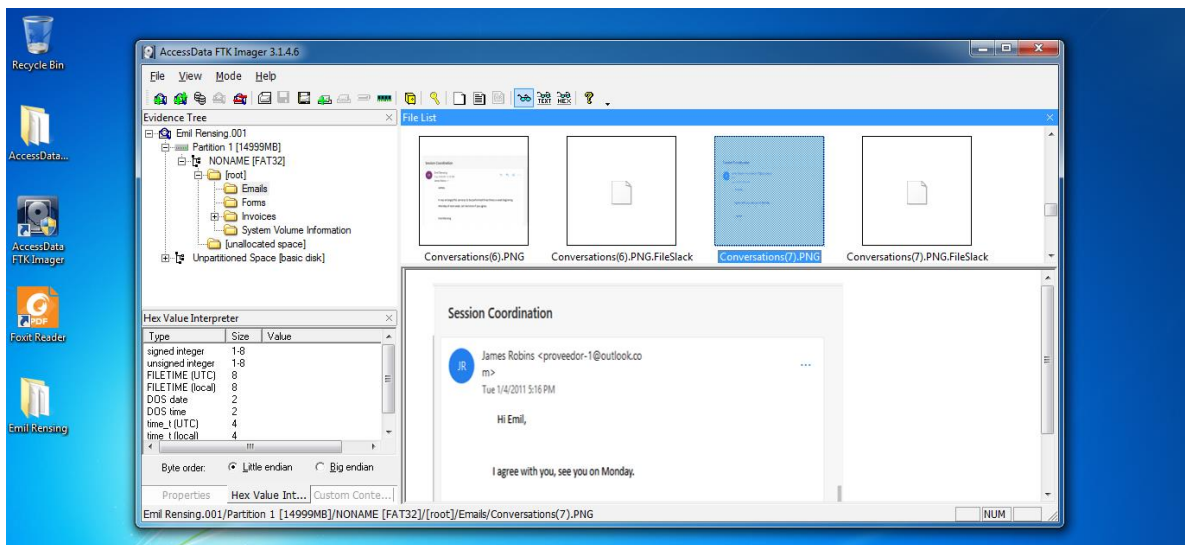


Figura # 47: Correo electrónico de confirmación de las sesiones de servicios.

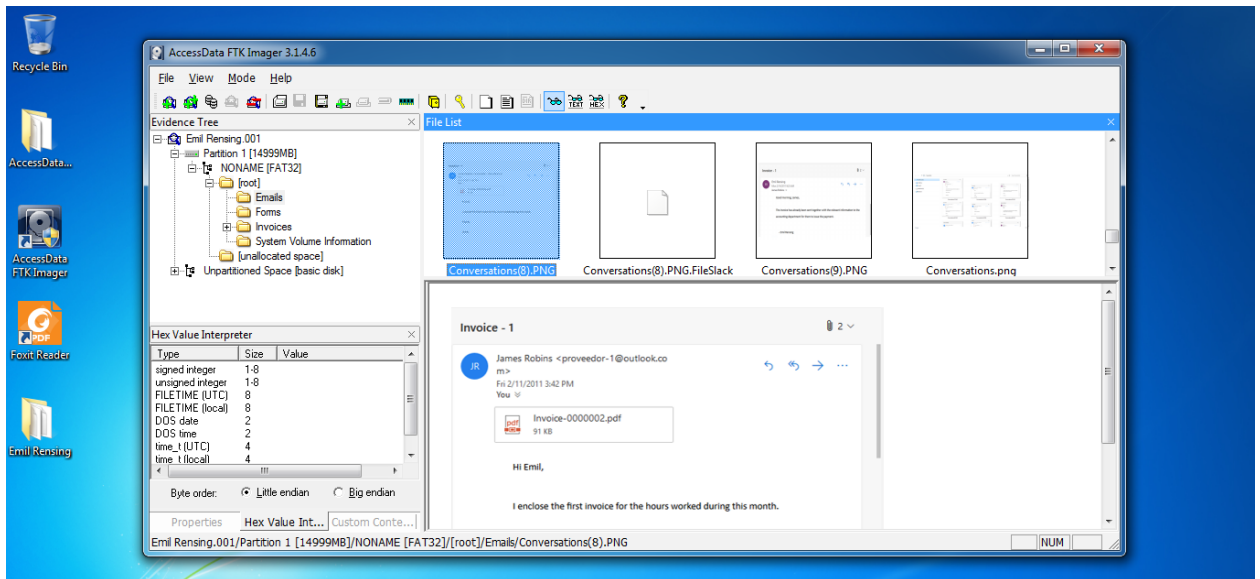


Figura # 48: Correo electrónico de James Robins con la primera factura de servicio.

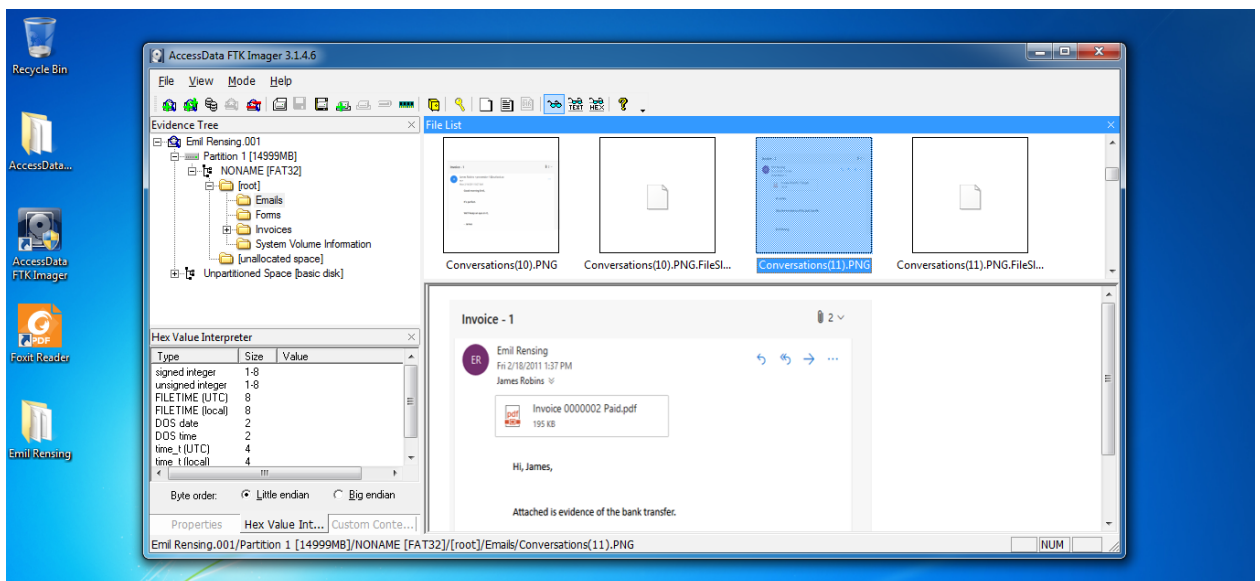


Figura # 49: Correo electrónico de Emil Rensing confirmando transferencia de pago.

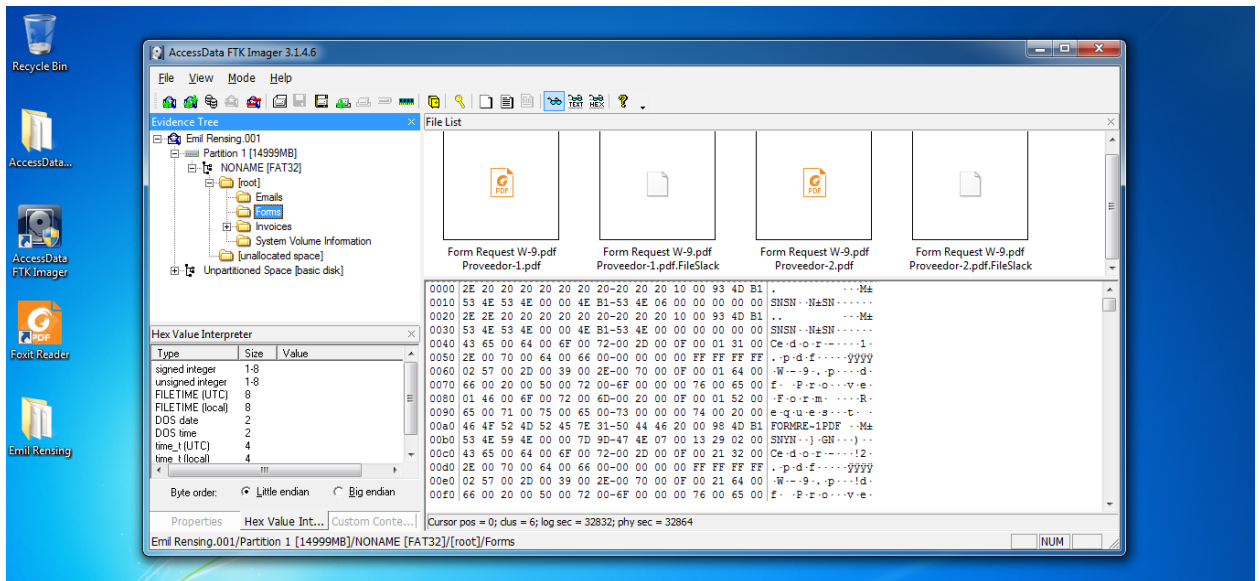


Figura # 50: Folder encontrado con formularios

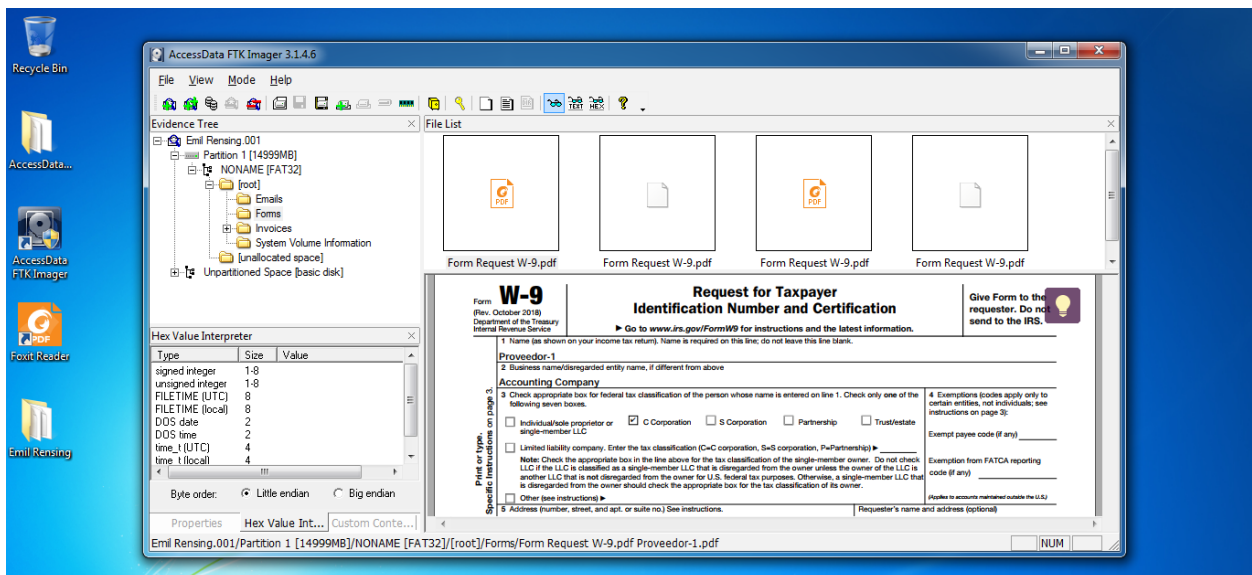


Figura # 51: Formulario del W-9 del IRS de Accounting Company.

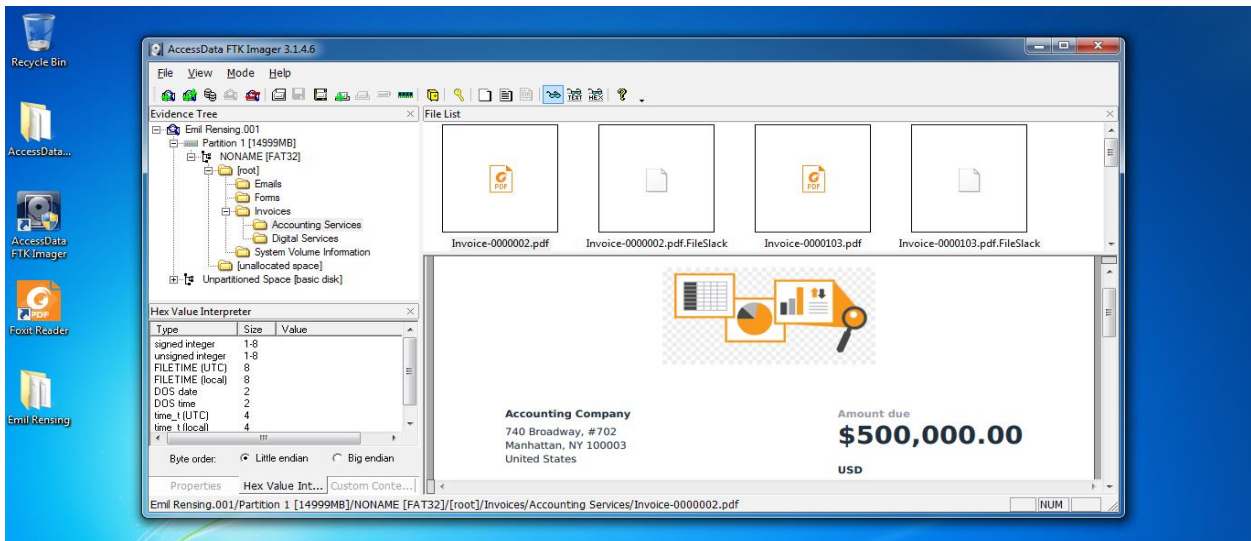


Figura # 54: Factura No.0000002 a nombre de Accounting Company

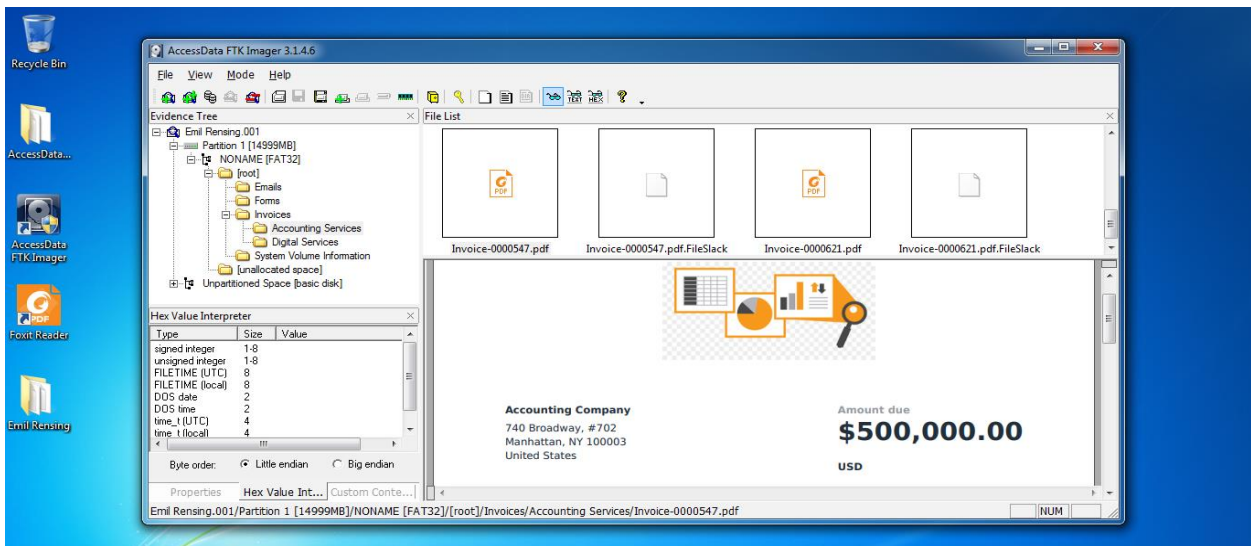


Figura # 55: Factura No.0000547 a nombre de Accounting Company

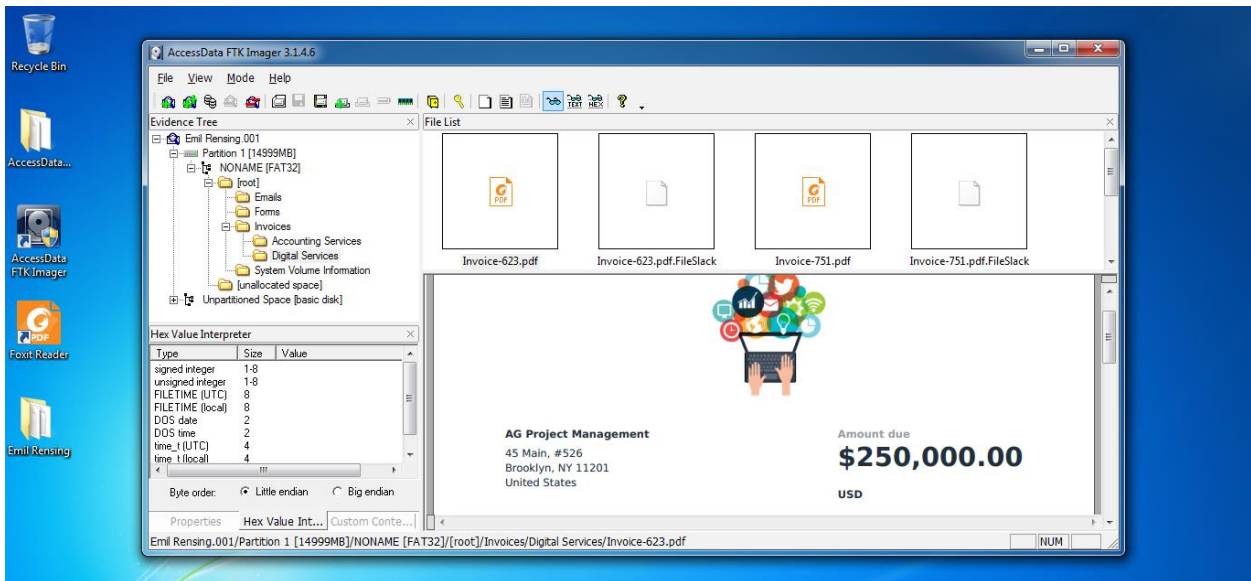


Figura # 56: Factura No.623 a nombre de AG Project Management

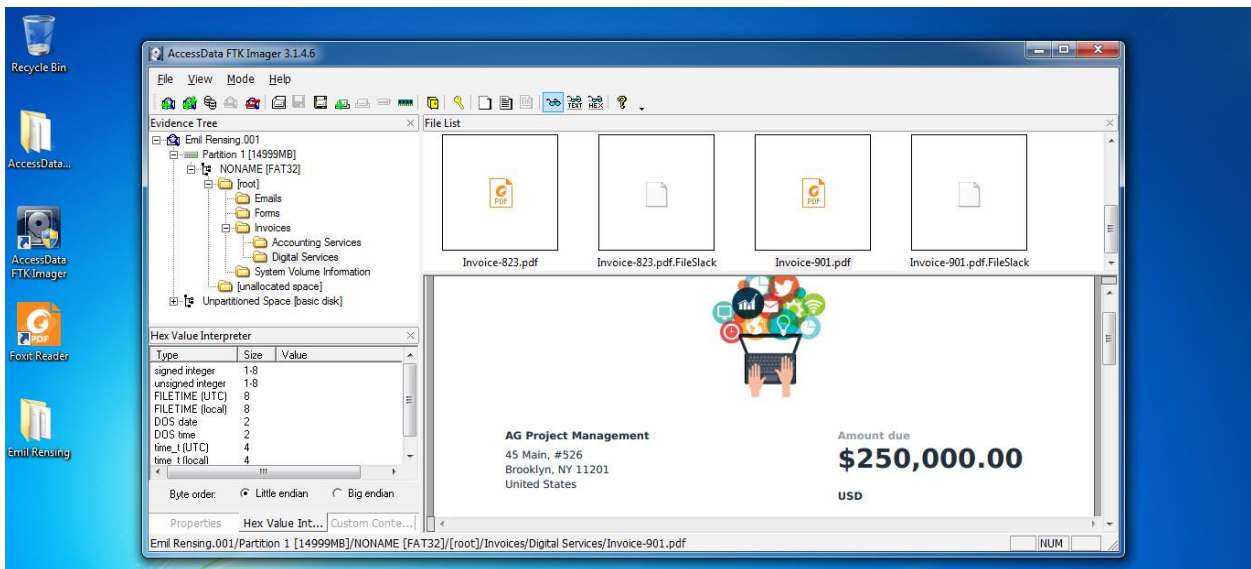


Figura # 57: Factura No.901 a nombre de AG Project Management

Conclusión

En el informe del caso pudimos identificar todos los hallazgos que se encontraron en la evidencia incautada la cual se nos fue entregada en un USB. En este se encontraron

varios documentos, entre ellos, facturas, formularios y correos electrónicos que muestran el esquema de fraude de Emil Rensing.

5. Discusión del caso

Según la información obtenida de los documentos legales del caso United States of America v. Emil Rensing, número 1:16-cr-00442-VM, al acusado se le imputan dos cargos, uno por robo de identidad y otro por fraude por cable a la compañía Epix donde este trabajaba. Rensing abusando de su puesto de Director Digital estableció un esquema de fraude contra su patrono por el cual se declaró culpable.

Este esquema de fraude consistía en crear proveedores falsos los cuales se supone que realizarían servicios técnicos y servicios contables, pero en realidad estos servicios nunca se realizaron. En dicho esquema Rensing estafó a la compañía Epix por más de \$7 millones. Él era la persona a cargo detrás de dichos proveedores.

Rensing creó cuentas de correo electrónico falsas, además de que con dichas cuentas elaboraba conversaciones aparentemente con los proveedores en las cuales se coordinaban reuniones, se enviaban formularios y se recibían facturas de los servicios que aparentemente se habían realizado. Cabe señalar que el personal designado en los contratos de los proveedores para realizar dichos servicios, eran antiguos socios comerciales y profesionales de Rensing, y estos no tenían ni la más mínima idea de que este estaba utilizando sus nombres para realizar el esquema.

6.Auditoria y prevención

Introducción

La auditoría es la revisión oficial de los estados contables de una institución para comprobar la exactitud de los apuntes contables y los criterios utilizados al realizarlos. (Expansión, 2018). Esta tiene como fin el asegurar que se han registrado todas las transacciones económicas y que los estados financieros reflejan lo más fidedignamente posible la verdadera situación patrimonial y económica de la entidad y se presentan de acuerdo con los principios de contabilidad generalmente aceptados (PCGA). La auditoría puede ser limitada o completa, según su alcance, y externa o interna, según la realice la propia empresa u otra firma (Expansión, 2018).

También se refiere a la profesión y la actividad de los auditores. Los auditores son aquellos profesionales encargados de llevar a cabo la auditoría de la empresa y pueden ser externos o internos: los auditores externos están empleados generalmente en una firma de auditoría, mientras que los auditores internos son empleados de la propia empresa auditada. Los auditores deben realizar el informe de auditoría, documento que contiene la opinión del auditor sobre la fidelidad y exactitud de las cuentas examinadas. Normalmente va dirigido a los accionistas y a los miembros del consejo de administración si son las cuentas anuales, o a quien le haya hecho el encargo si se trata de una auditoría específica, por ejemplo, antes de llevar a cabo una adquisición (Expansión, 2018).

Las auditorías siempre se han considerado como el examen y control de la situación económica de la empresa, para saber qué cosas van mal, qué cosas van bien y cómo se puede mejorar en cualquiera de los puntos clave de la empresa. Auditar, se entiende así,

como someter las cuentas de una empresa a examen para saber cómo está actualmente la empresa para saber hacia dónde debe ir a partir de ese momento. (Emprende pyme, 2018)

Sin embargo, en la actualidad son muchos los aspectos que se pueden auditar en una empresa sin necesidad de realizar un examen general de la empresa. Es decir, que se pueden realizar controles de algún sector de la empresa concreto, o de algún ámbito organizacional del que se quiera obtener una fotografía que represente el momento actual, para saber si se están haciendo bien las cosas o si se puede mejorar algún aspecto. (Emprende pyme, 2018)

Entre los objetivos de las auditorías podemos encontrar:

- Conocer la situación actual y exacta de la empresa en general o en algo concreto
- Dar credibilidad y confianza frente a posibles inversores o entidades financieras
- Detectar fraudes que se estén cometiendo en la empresa
- Comprobar la legalidad de todos los productos y actuaciones
- Detectar errores técnicos que se estén realizando
- Observar si se el sistema de trabajo de la empresa está siendo eficaz y eficiente
- Recabar la máxima información posible para tomar decisiones que mejoren el rendimiento

Resumen y hallazgos

Según la investigación realizada sobre este caso hay varios elementos fundamentales que fueron los que propiciaron que Rensing pudiera cometer este esquema de fraude millonario contra su empleador Epix. Aparentemente Rensing fue sacudido en el 2009 por el final de su matrimonio de 13 años con su novia de la escuela secundaria y el

inicio de problemas de salud no revelados. Por otro lado, la muerte inesperada de su hermana fue otra experiencia traumática, según los documentos judiciales (Littleton, 2018).

Los abogados de Rensing previo a la sentencia ante el juez, escribieron que Rensing “Sentía que su compensación no era lo suficientemente alta para el trabajo o el valor que entregaba; creía que tenía la aprobación tácita de la gerencia; que la cultura corporativa lo alentó mientras produjera resultados; y las reglas no eran tan importantes en ese negocio” (Littleton, 2018)

Durante el proceso de investigación se encontraron ciertas deficiencias por parte de la compañía Epix. A continuación, se detallan las mismas y se hacen algunas recomendaciones.

- Hallazgo # 1 Ausencia de segregación de funciones

Recomendación: Segregar las funciones de los empleados para evitar que estos puedan o tengan oportunidad de cometer algún tipo de fraude

- Hallazgo #2 Monitoreo del Sistema

Recomendación: Realizar monitoreos preventivos mensual o trimestralmente de los sistemas para ver que todo esté bajo control

- Hallazgo #3 Corroborar información e identidad de los proveedores

Recomendación: Confirmar la identidad de los proveedores antes de contratar los servicios y no hacer ningún tipo de negocios hasta tener toda la documentación completa.

- Hallazgo #4 Confirmar identidad de las cuentas bancarias

Recomendación: Confirmar la identidad de las cuentas bancarias de cada proveedor antes de emitir cualquier tipo de pago.

7. Conclusión

Según la investigación realizada en el caso USA v. Emil Rensing. La evidencia recopilada muestra que en efecto Emil Rensing sí ideó un esquema de fraude para robarle a Epix. Los hallazgos muestran que desde que Rensing comenzó en el 2010 a trabajar en Epix como Director Digital, ya estaba llevando a cabo el esquema de fraude.

Desde un principio él fue amoldando los procesos de la compañía, para poder ejecutar de manera perfecta el plan que tenía. Rensing hizo que la directiva sin saberlo le pusiera todo en bandeja de plata. Esto con la creación de los proveedores falsos, con nombres de sus conocidos, correo electrónico falsos, direcciones físicas falsas, pudo pasar desapercibido por un periodo de cinco años. Además de crear las facturas y formularios falsos. Rensing estuvo cobrando en sus cuentas personales por unos servicios que se supone que se realizaran en la compañía Epix, pero nunca fueron prestados.

Ningún fraude es perfecto y siempre quedará rastro de todo. Debido a esto fue que pudieron parar el esquema de fraude de Rensing.

8.Referencias

- ACFE (2018). Árbol del fraude. Recuperado de <https://acfe-spain.com/recursos-contrafraude/que-es-el-fraude/arbol-fraude>
- Cano, M. (s.f.) Fraude y estafa en los negocios. Recuperado de <http://interamerican-usa.com/articulos/Auditoria/Fraud-Estaf-Neg.htm>
- Case Ware (2018) Idea. Recuperado de <https://idea.caseware.com/>
- Castellnou R. (2018). Como afrontar el fraude interno en tu empresa. Recuperado de <https://www.captio.net/blog/los-5-tipos-de-fraude-interno>
- Confirma Sistemas (2016). El fraude interno, un problema en aumento. Recuperado de <https://www.confirmasistemas.es/es/contenidos/canal-estrategia/el-fraude-interno-un-problema-en-aumento>
- Gordon (2014). Como utilizar el kit de extracción de datos para Outlook. Recuperado de <https://www.outlooktransfer.com/es/how-to-use-data-extraction-kit-for-outlook/>
- Hernando, S. (2009) Análisis forense con AccessData FTK Imager. Recuperado de <http://www.sahw.com/wp/archivos/2009/03/09/analisis-forense-con-accessdata-ftk-imager/>
- Inter Economía (2016). El 65% de los fraudes a las compañías proviene de sus empleados. Recuperado de <https://intereconomia.com/tendencias/empleo/65-los-fraudes-las-companias-proviene-empleados-20161128-2055/>
- JPMorgan Chase & Co. (2018) Robo de identidad. Recuperado de <https://www.chase.com/es/digital/resources/privacy-security/questions/identity-theft>
- Julián Pérez Porto y María Merino. Publicado: 2008. Actualizado: 2008.
- Definicion.de: Definición de correo electrónico (<https://definicion.de/correo-electronico/>)

Julián Pérez Porto y María Merino. Publicado: 2009. Actualizado: 2013.

Definicion.de: Definición de fraude (<https://definicion.de/fraude/>)

Julián Pérez Porto y María Merino. Publicado: 2011. Actualizado: 2014.

Definicion.de: Definición de simulación (<https://definicion.de/simulacion/>)

Kenton, W. (2018). Wire Fraud. Recuperado de

<https://www.investopedia.com/terms/w/wirefraud.asp>

Littleton, C. (2018). El ex ejecutivo de Epix, Emil Rensing, fue sentenciado a cuatro años de

prisión por fraude: Recuperado de <https://variety.com/2018/tv/news/emil-rensing-epix-executive-sentencing-7-7-million-fraud-1202827421/>

Oficina de seguridad internauta (2011). El Robo de identidad y sus consecuencias. Recuperado

de <https://www.osi.es/es/actualidad/blog/2011/06/02/el-robo-de-identidad-y-sus-consecuencias>

Pepenella, S. FTK Imager step by Step: FTK Imager, More Than an Just an Imager

eForensics Magazine, 3 (8) 8-15

Raymond, N. (2016). Former Epix cable executive arrested on charges that he defrauded the

network of more than \$8 million. Recuperado de <https://www.businessinsider.com/former-epix-executive-arrested-on-fraud-charges-2016-4>

US Department of Justices (2017). CEO Indicted for Wire Fraud And Aggravated Identity

Theft. Recuperado de <https://www.justice.gov/usao-md/pr/ceo-indicted-wire-fraud-and-aggravated-identity-theft>

US Department of Justices (2019). Judge Sentences Businessman for Wire Fraud and

Aggravated Identity Theft. Recuperado de <https://www.justice.gov/usao-wdtx/pr/judge-sentences-businessman-wire-fraud-and-aggravated-identity-theft>

US Department of Justice (2017). Newark Women Sentenced to 4 Years Imprisonment in Embezzlement Case Recuperado de <https://www.justice.gov/usao-de/pr/newark-woman-sentenced-4-years-imprisonment-embezzlement-case-0>

US Department of Justice (2017). Chief Digital Officer of Premium Cable Network Pleads Guilty In Manhattan Federal Court To Defrauding His Employer of More Than \$7 Million Recuperado de <https://www.justice.gov/usao-sdny/pr/chief-digital-officer-premium-cable-network-pleads-guilty-manhattan-federal-court>

US Department of Justice (2018). United States of America v. Emil Rensing, 1:16-cr-00442-VM (D. NY 2016). Recuperado de <https://www.justice.gov/usao-sdny/file/845881/download>

US Department of Justice (2018a). Chief Digital Officer Of Cable Network Sentenced To 51 Months In Prison For Defrauding His Former Employer Of More Than \$7 Million. Recuperado de <https://www.justice.gov/usao-sdny/pr/chief-digital-officer-cable-network-sentenced-51-months-prison-defrauding-his-former>

US Department of Justice (2018b). Former Chief Digital Officer Of Premium Entertainment Network Charged With \$8 Million Fraud. Recuperado de <https://www.justice.gov/usao-sdny/pr/former-chief-digital-officer-premium-entertainment-network-charged-8-million-fraud>

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