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

ROBO DE BITCOINS Y FRAUDE ELECTRÓNICO

ANÁLISIS DE CASO: (USA Vs. MARK FORCE Y SHAUN BRIDGES)

Caso Número: 3:15-70370

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Especialidad en Seguridad de Información e Investigación de Fraude

PREPARADO POR:

MIGUEL FABREGAS RUIZ

Julio, 2018

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

ANÁLISIS CASO DE ROBO DE BITCOINS Y FRAUDE ELECTRÓNICO EN ESTADOS UNIDOS DE AMÉRICA

(USA Vs. MARK FORCE & STEPHAN BRIDGES)

Caso Número: 3:15-cr-00319

Preparado por:

Miguel Fabregas Ruiz

Ha sido aceptado como requisito parcial para el grado de:

Maestría en Sistemas de Información:

Especialidad en Seguridad de Información e Investigación de Fraude

Julio, 2018

Aprobado por:

Dr. Miguel A. Drouyn Marrero, Director

TABLA DE CONTENIDO

SECCIÓN 1: INTRODUCCIÓN Y TRASFONDO 1

Introducción 1

Descripción del caso 2

Trasfondo 3

Descripción de los hechos 5

Acusaciones – Cargos – Penalidad 9

Definición de términos 9

SECCIÓN 2: REVISIÓN DE LITERATURA 11

Introducción 11

Fraudes involucrados 13

Leyes aplicables 16

Casos relacionados 18

Herramientas de investigación 19

SECCIÓN 3: SIMULACIÓN 21

SECCIÓN 4: INFORME DEL CASO 24

Resumen Ejecutivo 24

Objetivo 24

Alcance del Trabajo 24

Datos del Caso 24

Descripción de los Dispositivos Utilizados 25

Resumen de Hallazgos 25

Cadena de Custodia 25

Procedimiento 27

Conclusión 39

SECCIÓN 5: DISCUSIÓN DEL CASO 40

SECCIÓN 6: AUDITORIA Y PREVENCIÓN 41

SECCIÓN 7: CONCLUSIÓN 42

SECCIÓN 8: REFERENCIAS 43

TABLA DE FIGURAS

FIGURA 1: Organigrama de Silk Road como se conectaban 22

FIGURA 2: Esquema de Fraude de Bitcoin a Mt. Gox 23

FIGURA 3: Inicio del Procedimiento 27

FIGURA 4: Crear la Imagen 28

FIGURA 5: Selección de fuente correspondiente 29

FIGURA 6: Destino de la Imagen 30

FIGURA 7: Tipo de Imagen a crear 31

FIGURA 8: Ingresar información de la evidencia 32

FIGURA 9: Definir la carpeta donde se almacena la imagen creada 33

FIGURA 10: Resumen de las opciones 34

FIGURA 11: Proceso de creación 35

FIGURA 12: Verificación de imagen 36

FIGURA 13: Resultados finales 37

FIGURA 14: Archivo de texto de imagen creada 38

FIGURA 15: Evidencia encontrada 39

SECCIÓN 1: INTRODUCCIÓN Y TRASFONDO

Introducción

Según Swartz (2015), un agente del servicio secreto estadounidense Shaun Bridges y otro agente de la DEA, Mark Force se declararon culpable por robar más de $800,000 dólares en bitcoins, estos estaban encargados de una investigación sobre el mercado de drogas en línea Silk Road.

Según el pliego acusatorio Silk Road operó durante más de dos años hasta que se cerró en octubre de 2013, después que el gobierno federal incauto y desactivo la Red (TOR). Esta generó más de $ 214 millones en ventas de drogas y otros bienes ilícitos y solo utilizando bitcoins como modo de moneda de transacción, según los fiscales del caso Melinda Haag y David Callaway del District Court of Northern California. Otro implicado en el caso y principal acusado Ross Ulbricht, dueño y el creador de Silk Road, Utilizó el alias Dread Pirate Roberts para disuadir a las autoridades vendiendo material ilícito y fue sentenciado a cadena perpetua luego de que un jurado federal en Manhattan lo declarara culpable de cargos que incluían la distribución de drogas a través de ventas en línea.

Shaun Bridges pertenecía al Servicio Secreto federal con sede en la cuidad de Baltimore, Maryland el cual investigó Silk Road. Otro miembro que ayudo en la investigación, el ex agente de la Agencia Antidrogas de Estados Unidos (DEA), Carl Force, el cual admitió los cargos de extorsión, lavado de dinero y obstrucción de la justicia.

En el tribunal, El caso en contra de Bridges este admitió que robo una suma alta de bitcoins que eran de la Ruta de la cebolla (TOR) y con este hecho Ulbricht revelo su identidad. Bridges invento el hecho que otro individuo estaba robando bitcoin en Silk Road y con estos

actos ayudó a que Ulbricht intentara contratar a alguien para matar a esa persona. Este señalamiento fue presentado en la sentencia de Shaun Bridges al cual fue sentenciado en noviembre 2015.

Descripción del caso

Número Del Caso CRIMINAL NO. 3-15-70370

Acusados son:

- Carl Mark Force IV, Case No. 3-15-70370
- Shaun Bridges, Case 3:15-CR 00319

Investigador.

- Agente Especial Tigran Gamgaryan IRS-Criminal Investigador

Abogados.

- Abogados de Mark Force Steven Hale Levin, y Levin & Curlett LLC,
- Abogados de Stephan Bridges Craig S. Denney Snell & Wilmer L.L.P. Snell & Wilmer L.L.P

Fiscal.

- Melinda Haag United States Attorney, District court of Northern California
- David R. Callaway Chief, Criminal Division District court of Northern California
- Kathryn Haun Assistant United States Attorney, District court of Northern California
- William Frentzen Assistant United States Attorney, District court of Northern California

Juez.

María-Elena James, United States Magistrate Judge, Northern district California

Trasfondo

Según el pliego acusatorio en el caso de USA vs Carl Force y Shaun W. Bridges (2015), a los acusados se les imputa robo de propiedad del gobierno, fraude electrónico, lavado de dinero, conflicto de interés cometidos en ambos lados de la nación norteamericana. Este caso fue manejado en la oficina del fiscal del norte de California y la oficina de la integridad pública ubicada en Washington D.C. En esta investigación fue coordinada junto a otras agencias del gobierno Federal a incluir agentes del Servicio Secreto y personal del Federal Bureau of Investigación (FBI) división de San Francisco, escuadrón dedicada a la Corrupción pública. Los cuales investigaron la violación de leyes criminales a incluir fraude, soborno, extorción, conflicto de interés y malversación de fondos públicos. También se incluyó en la investigación al Departamento de Justicia, oficina del inspector general (DOJ OIG) y la oficina del Departamento de Homeland Security oficina del inspector general (DHS OIG) ambos investigaron el proceso de abuso y fraude por los agentes oficiales.

El Agente Tigran Gamgaryan IRS-Criminal Investigador de la División de Investigación Criminal del Servicio de Rentas Internas (IRS), en el Distrito Norte de California, fue el enlace de la Unidad de Delitos Cibernéticos del grupo. Antes de eso, su experiencia fue como auditor para la Junta de Impuestos de Franquicias de California, donde investigó refugios fiscales abusivos. Su capacitación y experiencia incluyen, entre otras, investigaciones relacionadas con el lavado de dinero, fraude de empleados administrativos, corrupción pública, crimen organizado y

violaciones de la Ley de Secreto Bancario y el código impositivo. Desarrolló una especialidad en delitos informáticos digitales y cibernéticos.

El agente Especial Tigran Gamgaryan IRS-Criminal Investigador, investigó a los integrantes de la unidad que tenían asignada la tarea de investigar a los de la Ruta de la Seda (SILK ROAD) de Baltimore, incluía al ex agente de la DEA, Carl Mark FORCE IV (FORCE) y al ex agente del Servicio Secreto Shaun BRIDGES (BRIDGES). Esta es una investigación que cubría la cuidad de Maryland y hasta la sede en la ciudad de San Francisco. El curso de la investigación fue manejado por la Oficina del Fiscales de los Estados Unidos para el Distrito Norte de California y la Sección de Integridad Pública en Washington D.C. En esta investigación, se unieron varios agentes, para incluir Agentes Especiales y un Especialista en Operaciones de Personal del Escuadrón de Corrupción Pública de la División de San Francisco de la Oficina Federal de Investigaciones (FBI), que investiga el abuso de cargos públicos en violación del derecho penal para incluir fraude, soborno, extorsión, conflictos de interés y malversación de fondos. También se unió a esta investigación la Oficina del Inspector General (DOJ OIG) del Departamento de Justicia y la Oficina del Inspector General del Departamento de Seguridad Nacional (DHS OIG), que investigan y procesan el fraude y el abuso por parte de funcionarios federales.

Todos los hechos fueron provistos en una declaración jurada de todas las observaciones personales que el agente Tigran Gamgaryan IRS-Criminal Investigador obtuvo en su investigación. Sus años de entrenamientos y su experiencia como investigador hicieron toda la información y evidencia obtenida de otros agentes y testigos fuera suficiente para que la declaración jurada que mostrarse que había suficiente evidencia para causa probable y la radicación de cargos con las garantías requeridas por ley.

Descripción de hechos

Según lo que se desprende del pliego acusatorio del caso (2015), el gobierno realizó múltiples investigaciones en el mercado de Silk Road, una empresa subterránea de mercado negro que permitía a vendedores y compradores realizar transacciones ilegales a través de la Internet. Una de estas investigaciones se llevó a cabo en el Distrito Sur de Nueva York, y la otra se llevó a cabo en el distrito de Baltimore en Maryland. Tanto FORCE como BRIDGES se asignaron a la investigación de Baltimore y no a la de Nueva York.

Durante 2012 y 2013, tanto FORCE como BRIDGES tuvieron importantes responsabilidades relacionadas a la investigación de Silk Road en Baltimore. En esta capacidad, Force fue el agente encubierto principal con comunicación con D.P.R, Dread Pirate Robert, el propietario, administrador y operador de la página de web llamado Silk Road. BRIDGES fue el experto en informática forense en la misma investigación de la cuidad de Baltimore. Su calidad de miembro del Task Force con la asignación sobre la Ruta de la Seda (SILK ROAD) en Baltimore, tanto FORCE como BRIDGES tuvieron una exposición significativa y experiencia desarrollada en la moneda digital conocida como Bitcoin. Como se describirá más adelante en este documento, FORCE y BRIDGES abusaron de sus posiciones como agentes federales y se involucraron en un plan para defraudar a una variedad de organizaciones, el público y el gobierno, todos para su propio enriquecimiento financiero.

Con respecto a la Agencia Antidrogas (DEA) Agente Especial FORCE, esta investigación relevó entre otras cosas que, FORCE creó ciertas personas ficticias, que no estaban oficialmente autorizadas, para comunicarse con el D.P.R, que era el objetivo de la investigación de FORCE. Usando una de estas personas ficticias, FORCE extorsiona D.P.R buscando un pago monetario a cambio de información y que este no proporcionara al gobierno cierta información.

D.P.R pagó $ 250,000 por el servicio que Force le ofreció y que actuara que su papel como agente en la Tarea de Ruta de la Seda (SILK ROAD) se descubriera. Force creó una personalidad ficticia llamada "French Maid", Operando como "francés" Hasta el 1 de octubre de 2013. D.P.R era conocido por FORCE y el resto del Baltimore Silk Road Task Force solo por su apodo en línea "Dread Pirate Roberts" o "D.P. R". Ulbricht era conocido en el sitio de Silk Road con el apodo de "Dread Pirate Roberts" (D.P.R) y en lo sucesivo se lo denominará indistintamente como "D.P. R" y "Ulbricht".

Force presentó fraudulentamente a D.P.R cierta información concerniente a la verdadera identidad de" French Maid " y se ofreció a vender información del D.P.R sobre la investigación que el gobierno conducía en Silk Road a cambio de aproximadamente $ 100,000 en valor de bitcoin, que el D.P.R pagó y FORCE depositó en sus cuentas personales. FORCE robó y convirtió para su propio uso una cantidad considerable de bitcoins que el D.P.R envió a FORCE en su capacidad encubierta y oficial. En lugar de entregar esos bitcoins al gobierno, FORCE los depositó en sus propias cuentas personales;

FORCE participó en una serie de transacciones complejas y varias cuentas de Bitcoin (conocidas como direcciones de Bitcoin), sus cuentas de moneda digital personal y sus cuentas bancarias personales, incluyendo un cable de $ 235,000 dólares a una cuenta en el extranjero en Panamá, todo en un esfuerzo por lavar y ocultar la verdadera fuente del producto obtenido ilegalmente; FORCE utilizó su posición oficial como agente de la DEA para ejecutar ilegalmente los controles de antecedentes penales de personas en beneficio de una empresa de intercambio de moneda digital de terceros, CoinMKT, en la que FORCE había invertido personalmente aproximadamente $ 110,000 en bitcoin; FORCE funcionó como Director de Cumplimiento de facto para CoinMKT todo el tiempo empleado como agente de la DEA, incluso permitiéndose

aparecer en los "pabellones" de CoinMKT para la inversión de capital de riesgo y permitir figurar el lavado de dinero y / o conformidad de CoinMKT. Una compañía en la cual FORCE había invertido.

FORCE, CoinMKT indebidamente dirigida a congelar una de las cuentas de sus clientes individuales que contiene una gran cantidad de moneda digital, por valor de aproximadamente $297,000 dólares, aunque carecía de una base legal suficiente para hacerlo, FORCE entonces incauto ilegalmente esos fondos y los transfirió a su propia cuenta personal. FORCE usó el sello de firma de su supervisor, sin autorización, en un departamento oficial de los EE. UU. Citación judicial y envió la citación a una compañía de pagos, ordenando a la compañía que descongele su propia cuenta personal, que previamente había sido congelada debido a cierta actividad sospechosa. FORCE luego trató de ocultar la evidencia de su uso indebido de una citación oficial al ordenar a la compañía que no contactara a la DEA y que intentara destruir copias de la citación. Cuando la empresa no cumplió, FORCE solicitó a otro agente de Baltimore Silk Road Task Force, un agente del IRS, que colaborara con él para apoderarse de las cuentas bancarias de esa compañía.

Con respecto a BRIDGES del servicio secreto de EE. UU. (USSS), la investigación revelo, entre otras cosas, que, a fines de enero de 2013, miembros de la Fuerza de Tarea Baltimore Silk Road, que incluía a BRIDGES y FORCE, obtuvieron acceso a una cuenta de administrador de la página web de Silk Road, ellos obtuvieron esas cuentas administrativas por el arresto de un ex empleado de Silk Road. El 25 de enero de 2013, la página de web de Silk Road sufrió un robo de bitcoins cuantiosa y fueron trasladados a Mt. Gox, un intercambio de divisas digital con sede en Japón; segundo. El 12 de febrero de 2013, BRIDGES formó y registró una compañía de responsabilidad limitada personal llamada "Quantum International Investments,

LLC" (Quantum) y, el 22 de febrero de 2013, BRIDGES abrió una cuenta en Fidelity Investments (Fidelity) en nombre de Quantum, Según los registros obtenidos de Fidelity, BRIDGES financió su cuenta de Quantum Fidelity exclusivamente con depósitos bancarios de Mt. Gox en Japón. Específicamente, entre el 6 de marzo de 2013 y el 7 de mayo de 2013, la cuenta Quantum Fidelity de BRIDGES en los Estados Unidos recibieron nueve (9) transferencias electrónicas de Mt. Gox por un total de aproximadamente $ 820,000. A pesar de haberse beneficiado personalmente de la cantidad de $ 820,000 en una cuenta de Mt. Gox y recibir un depósito el 7 de mayo de 2013 desde la cuenta de Mt. Gox, y solo dos días después del 9 de mayo de 2013, BRIDGES sirvió como affiant en una orden de incautación multimillonaria para Mt. Gox.

La incautación de Mt. Gox y las cuentas bancarias de su propietario fue el motivo fundado a que se abriera una investigación. Cuando BRIDGES al enterarse de la investigación criminal del gobierno sobre la Fuerza de Tarea de la Ruta de la Seda de Baltimore basada en el Distrito Norte de California, y luego de una entrevista del FBI como parte de la investigación criminal, BRIDGES transfirió más de $ 250,000 de su cuenta de Quantum Fidelity a otra cuenta bancaria mantenida por él mismo y un tercero. Y es por eso por lo que esta declaración jurada es para el propósito limitado de establecer la causa probable de los crímenes propuesto para ser cargado en este momento, no incluye ciertos hechos adicionales, la investigación del gobierno continúa.

Acusaciones, Cargos y Penalidades

Según los hechos expuestos en una declaración jurada, es probable que existan los motivos para creer que FORCE cometió infracciones a la ley para incluir violación al Título 18 del Código de los Estados Unidos, Sección 1343 (Fraude electrónico), Título 18, Código de Estados Unidos, Sección 641 (Robo de propiedad del gobierno), 10 Título 18, Código de los Estados Unidos, Sección 1956 (Lavado de dinero) y Título 18, Código de los Estados Unidos, Sección I 208 (Conflicto de intereses). También hay causa probable para creer que BRIDGES cometió violaciones a la ley para incluir el Título 18, Código de los Estados Unidos, la Sección 1343 (Fraude electrónico) y el Título 18, 13 del Código de los Estados Unidos, Sección 1956 (Lavado de dinero).

Definición de Términos

Bitcoins, es un protocolo, una red de pagos y una moneda Originalmente se propuso como concepto en 2008, pero fue lanzada en enero de 2009

D.P.R, Dread Pirate Robert, nombre ficticio utilizado por Ross Ulbricht

French Maid, nombre ficticio utilizado por Mark Force.

DEA, Drug Enforcement agency.

USSS, United States Secret Service.

Fraude: Consiste en una falsa representación ya sea por palabras o por conducta, por acusaciones falsas o engañosas, o por ocultamiento de lo que debería haber sido divulgado, que engaña y tiene la intención de engañar a otro para que el individuo actúe sobre ella.

Fraude Electrónico: Fraude cometido utilizando medios electrónicos, tales como el uso de un teléfono, de un modem, o de una computadora.

Silk Road, pagina web que se dedica a vender y comprar contrabando ilegal con pagos de monedas de Bitcoin

SECCIÓN 2: REVISIÓN DE LITERATURA

Introducción

Según Oroyfinanza.com (2015), Bitcoin utiliza la tecnología peer-to-peer para funcionar sin autoridad central o bancos; gestión de operaciones y la emisión de bitcoins se lleva a cabo conjuntamente por la red. Bitcoin es una fuente abierta; su designación es publica, nadie posee ni controla Bitcoin y todos pueden participar. Ahora se analizará más a fondo el fraude cometido por Mark Force y Stephan Bridges en el delito que ambos se declararon culpable antes los tribunales. Bitcoin es una forma de moneda virtual convertible descentralizada que existe mediante el uso de un en línea, sistema de libro mayor descentralizado. Mientras que Bitcoin existe principalmente como una forma de moneda basada en Internet, es posible "imprimir" la información necesaria e intercambiar Bitcoin a través del medio físico. La moneda no es emitida por ningún gobierno, banco o empresa, sino que se genera y se controla a través de un software que opera a través de una red descentralizada. Para adquirir bitcoins, un usuario típico los comprará de un vendedor de Bitcoin o "intercambiador. También es posible" minar "bitcoin por verificar las transacciones de otros usuarios. Bitcoin es solo un tipo de moneda digital, y hay un número significativo de otras monedas digitales. Los intercambiadores de Bitcoin generalmente aceptan pagos de moneda fiduciaria (moneda que deriva su valor de la regulación o ley gubernamental) u otras monedas virtuales convertibles para obtener bitcoins.

Cuando un usuario desea comprar bitcoins de un intercambiador, el usuario generalmente enviará el pago en la forma de Fiat u otra moneda virtual convertible a un intercambiador, generalmente a través de cable o ACH, para el número correspondiente de bitcoins basado en un tipo de cambio fluctuante. El intercambiador, a menudo por una comisión, típicamente intentará intermediar la compra con otro usuario del intercambio que sea tratando de vender bitcoins, o, en

algunos casos, actuará como el vendedor mismo. Si el intercambiador puede colocar un comprador con un vendedor, entonces la transacción puede completarse.

Cuando un usuario adquiere bitcoins, se los envía a la dirección Bitcoin del usuario. Esto es algo similar a un número de cuenta bancaria, que se compone de una cadena de letras sensible a mayúsculas y 6 números que suman un total de 26 a 35 caracteres. El usuario puede luego realizar transacciones con otros usuarios de Bitcoin transfiriendo bitcoins a sus direcciones de Bitcoin a través de Internet. La poca o ninguna información de identificación personal sobre el pagador o beneficiario se transmite de Transacción Bitcoin. Las transacciones de Bitcoin ocurren usando una clave pública y una clave privada. Una clave pública es utilizada para recibir bitcoins y una clave privada se utiliza para permitir retiros de una dirección de Bitcoin. Solo se necesitan la dirección de Bitcoin de la parte receptora y la clave privada del remitente para completar la transacción, que por sí solos raramente reflejan información de identificación.

Todas las transacciones de Bitcoin se registran en lo que se conoce como la cadena de bloques. Esto es esencialmente un libro público distribuido que realiza un seguimiento de todas las transacciones de Bitcoin, entrantes y salientes, y actualizaciones aproximadamente seis veces por hora. La cadena de bloques registra cada dirección de Bitcoin que alguna vez recibió bitcoins y mantiene registros de cada transacción y todos los saldos conocidos para cada dirección de Bitcoin.

Las monedas digitales, incluido Bitcoin, tienen muchos usos legítimos conocidos. Sin embargo, al igual que el efectivo, los bitcoins pueden usarse para facilitar transacciones ilícitas y blanquear ganancias criminales, dada la facilidad con la que pueden usarse para mover dinero de forma anónima. Sin embargo, como se demuestra en este documento, en algunas circunstancias,

los pagos de bitcoin pueden remontarse a cuentas en instituciones financieras tradicionales que utilizan la cadena de bloques.

Fraudes involucrados

Las estafas y el fraude en el mundo financiero no son nada nuevo. Y el ecosistema de las criptomonedas no es una excepción. Basta con echar un vistazo a la breve historia de Bitcoin para darse cuenta de ello. Shane (2018) argumenta que la tecnología Bitcoin no ofrece ningún beneficio adicional a los estafadores sobre el dinero en efectivo o PayPal, por ejemplo, y a pesar de la complejidad técnica asociada a Bitcoin puede beneficiar la actividad de estafadores La prevalencia de las estafas en el ecosistema es más una consecuencia de la marginación de las instituciones jurídicas y financieras en una tecnología naciente. Mitos generalizados de por qué Bitcoin facilita el fraude, muchos presuponen que la tecnología Bitcoin es el culpable de la alta tasa de fraude, principalmente por su naturaleza supuestamente anónima e imposible de rastrear. Muchos usuarios tempranos de Bitcoin, incluyendo los criminales, también han confiado en esto, y con frecuencia en su propio perjuicio.

La naturaleza de Bitcoin es que es dinero rastreable. Todas las transacciones Bitcoin quedan registradas, de manera totalmente transparente y abierta, en la cadena de bloques y en miles de copias distribuidas por todo el mundo que pueden ser inspeccionadas por las víctimas, los investigadores y las autoridades. En los primeros días de Bitcoin, todavía no se habían desarrollado herramientas y técnicas sofisticadas para hacer conexiones entre las transacciones y facilitar el rastreo de la actividad económica, pero ahora mismo es un espacio en el que numerosos startups del ecosistema están focalizando su atención como por ejemplo Coín analíticos.

Por otro lado, Bitcoin no es anónima. Es cierto que los usuarios de la red no proporcionan su nombre u otra información de identificación en la propia red, pero sin embargo sí suele ser necesaria la identificación para la compra de bienes y servicios o intercambiar criptomonedas por dinero. Todas las transacciones quedan registradas, las víctimas del fraude o las autoridades pueden seguir el hilo de una transacción para rastrear todos sus movimientos. Para permanecer en el anonimato, el estafador debe convertir todas sus ganancias en bienes o servicios o a otra moneda sin que nadie conozca su identidad.

Además, más allá del análisis forense de la cadena de bloques, el porcentaje de operaciones en bitcoin que llevan a cabo el Know your Costumer (KYC) y este cumplimiento van en aumento, haciendo cada vez más difícil el intercambio a efectivo de forma anónima. de hecho, fue un informe realizado por la casa de cambio Bitstamp la que ayudó a las autoridades en el caso del agente de la DEA Carl Force, acusado de lavado de dinero y fraude electrónico durante su trabajo en las investigaciones en Silk Road.

Si la tecnología Bitcoin ya no hace que sea más fácil para los estafadores y timadores que desaparezcan con el dinero, ¿tiene alguna manera de facilitar las propias estafas? la primera investigación académica sobre las estafas Bitcoin se identificaron en cuatro categorías de estafas relacionadas con la criptomoneda: “programas de inversión de alto rendimiento, estafas en inversiones mineras, estafa en servicios de carteras y estafas en las casas de cambio”. Estas categorías se pueden condensar aún más en dos: inversiones fraudulentas y malas conductas de custodia, en las que un proveedor de servicios huye con los fondos que se había comprometido a mantener a salvo. En ambos casos, la estafa es perpetrada por convencer a las víctimas de confiar al estafador con sus fondos, y posteriormente los fondos no se utilizan para los fines previstos.

¿Hay algo en la tecnología o el código Bitcoin que ofrece a los estafadores la capacidad de engañar a los usuarios finales en la toma de buenas decisiones sobre dónde almacenar o invertir sus fondos? Está claro que no, pero tampoco se puede negar que la complejidad de Bitcoin puede ser una ventaja para los estafadores. Las víctimas sin tantos conocimientos tecnológicos y del mundo de los negocios son a menudo incapaces de evaluar si el producto que se ofrecen es técnicamente factible o si una empresa en busca de su inversión tiene un plan realista para aprovecha una necesidad genuina del mercado. Sin embargo, esto no pueden ampliarse a la tecnología de las monedas digitales como tal.

Como ha señalado el experto en Bitcoin Andreas Antonopoulos (2016), “los seres humanos han utilizado los controles de seguridad física durante miles de años. En comparación, nuestra experiencia con la seguridad digital es de menos de 50 años”. Al carecer de la capacidad técnica para mantener sus propios fondos en monedas digitales seguros, muchas personas han confiado sus tenencias a carteras o exchanges de custodia. Sin establecer las mejores prácticas, con la autorregulación del sector, sin la concesión de licencias del gobierno, o sin un sistema de reputación efectivo, los usuarios finales han debido identificar por su cuenta las instituciones de custodia de confianza, y no se puede negar que su trayectoria ha sido mala. La gran mayoría de estas empresas han perdido históricamente, al menos, algunos de los fondos de sus usuarios, ya sea por incompetencia o por robo descarado.

Afortunadamente la seguridad en las monedas digitales es un campo en rápida evolución. Avances significativos a nivel técnico, sobre todo el surgimiento de esquemas multiforme, que dividen el control de los fondos entre varios dispositivos y / o entidades. Nuevos proveedores de seguridad para empresas como BitGo ayudan a las instituciones de custodia a frenar a los hackers externos y al fraude por información privilegiada, además de que los usuarios finales

pueden ahora almacenar sus propios fondos en dispositivos de hardware especialmente diseñados para ello, como Trezor o Case.

En resumidas cuentas, los custodios que desaparecen con fondos no es nada nuevo. Sin embargo, la innovación puede disminuir la necesidad de custodios y ayudar a los custodios bienintencionado para que presten los servicios a sus clientes sin ningún contratiempo, pero ninguna tecnología puede detener al ingenuo de entregar su dinero a un estafador. La combinación de educación, mejores prácticas, reputación y / o certificación será necesaria para que el objetivo de evitar la mala conducta en la custodia se materialice.

Leyes aplicables

Las leyes violadas en el caso United States v. Shaun Bridges y Mark Force (2015) son las siguientes:

- **Título 18 U.S.C. 641** prohíbe el desfalco, el robo o la conversión de bienes pertenecientes a los Estados Unidos vale más de $ 1, 000. Los elementos esenciales de esta ofensa son:

(1) el acusado a sabiendas malversó, robó o convirtió al uso del demandado o el uso de otro el dinero o la propiedad de valor con la intención de privar al propietario del uso o beneficio del dinero o propiedad;

(2) el dinero o la propiedad pertenecían a los Estados Unidos; y

(3) el valor del dinero o la propiedad era más de $ 1, 000.

- **Título 18 U.S.C. 1343** prohíbe el fraude electrónico. Los elementos esenciales de esta ofensa son:

(1) el acusado participó deliberadamente, ideó o tuvo la intención de diseñar un plan o plan para defraudar, o un plan o plan para obtener dinero o propiedad por medio de pretextos falsos o fraudulentos, representaciones o promesas;

(2) las declaraciones hechas o los hechos omitidos como parte del esquema eran materiales, es decir, tenían una tendencia natural a influir, o eran capaces de influir, en una persona a parte con dinero o propiedad;

(3) el acusado actuó con la intención de defraudar, es decir, la intención de engañar o hacer trampa.

(4) el acusado usó, o hizo que se usara, una comunicación por cable para llevar a cabo. o intento para llevar a cabo una parte esencial del plan.

- **Título 18 U.S.C. 1956 (a) (1) (B) (i)** prohíbe el lavado de activos de "actividades específicas de desvinculación" (SUA). Los elementos esenciales son:

(l) el demandado llevó a cabo o tenía la intención de realizar una transacción financiera que involucrara propiedad que representaba el producto de una actividad legal específica;

(2) el demandado sabía que la propiedad representaba el producto de una actividad ilegal específica;

(3) el demandado sabía que la transacción se diseñó en su totalidad o en parte para ocultar o disfrazar la naturaleza, ubicación, fuente, propiedad o control del producto de la actividad ilegal específica; y

(4) el acusado hizo algo que fue un paso sustancial para cometer el crimen. El estatuto de lavado de dinero identifica específicamente ambos cables 1343 fraude y 641 robo de propiedad del gobierno como "actividad ilícita especificada".

- **Título 18 U.S.C. 208** prohíbe a los empleados federales tomar ciertos actos que afecten un interés financiero personal. la jurisprudencia establece que los elementos esenciales son:

(1) el demandado era un funcionario o empleado de la Rama Ejecutiva de los Estados Unidos;

(2) el acusado participó personal y sustancialmente como empleado del gobierno a través de la decisión, aprobación, desaprobación, recomendación, prestación de asesoramiento, investigación o de otro modo en un asunto; y

(3) el demandado sabía que tenía un interés financiero en el particular asunto en el que estaba participando.

Casos Relacionados

En el caso de Mark Force y Stephan Bridges no son los únicos casos que agentes de orden público cometan violaciones de ley en sus funciones. Diariamente un agente del orden público es arrestado por cometer delitos hacia el gobierno federal y estatal.

En el caso de United States of América v. Sheldon Silver Caso número 1:15-cr-00093-VEC, estableció que el uso de poder de Sheldon que era congresista en el estado de Nueva York al cual tomo juramento para trabajar con la gente y este uso su influencia para llenar su bolsillo

de dinero. Sheldon recibía dinero de desarrolladores para que este los refiriera y los contratara. El monto fue de más de 3 millones de dólares. Sheldon fue sentenciado a 7 años de prisión.

En el Caso de United States of América v. Miguel León Bejarano Caso número 6:18-cr-00064-RAW, durante noviembre 2017 y marzo 2018 en el distrito de Oklahoma, Miguel León con conocimiento y en conspiración de otros a transmitir comunicaciones fraudulentas que tenía el objetivo de recibir dinero por los escritos, fotos, señales etc. Miguel León se declaró culpable y espera a la sentencia que podría ser de 30 años de prisión y una multa de no más de un millón de dólares

El Caso de United States of América v. Michael Richo, Caso número 3:16-mj-464-SALM. Michael Richo se dedicaba a enviar online phishing para obtener los nombres de usuario y contraseña para robar los Bitcoins. Richo se robó un estimado de un millón de dólares en bitcoins.

Herramientas de investigación

FTK Imager de Access Data es una herramienta para realizar réplicas y visualización previa de datos, la cual permite una evaluación rápida de evidencia electrónica para determinar si se garantiza un análisis posterior con una herramienta forense como Access Data Forensic Toolkit. FTK Imager también puede crear copias perfectas (imágenes forenses) de datos de computadora sin realizar cambios en la evidencia original.

Recibí un USB marca Scandisk blanco con información relacionado a la investigación, en el mismo contenía un supuesto email que era información valiosa para la investigación. Se utilizo esta herramienta porque mantenía la información en el USB sin cambiar o afectar cualquier otra DATA que pudiera ayudarnos en la investigación. Para prevenir la manipulación

accidental o intencional de la evidencia original, FTK Imager realizar una imagen duplicado bit a bit del medio. La imagen forense es idéntica en cualquier forma al original, incluyendo espacio de holgura o residual y espacio sin asignar o espacio libre de la unidad. Esto permite almacenar el medio original en un lugar seguro de daño mientras se procede con la investigación utilizando la imagen forense.

SECCIÓN 3: SIMULACIÓN

Según el pliego acusatorio United States V. Mark Force, Stephen Bridges el esquema fue de la siguiente manera:

1. Mark Force vio la oportunidad de defraudar al gobierno de Estados Unidos utilizando los Bitcoins provistos por el mismo estado para comprar y vender suministros a la página de Silk Road.
2. Mark se acercó a Stephan Bridges y le ofreció la oportunidad de unirse a la investigación, pero con motivos fundados de defraudar a los de Silk Road y al gobierno.
3. El esquema era tan falso que Stephan le dio información a Ulbricht que otra persona se había robado sus Bitcoins y este mando a matar al responsable el cual era el mismo Stephan
4. Los acusados jugaban con las cuentas de Bitcoin y vendían y compraban casi al mismo tiempo para crear inestabilidad en el mercado y así vender y sacar más dinero de los programados.
5. Ambos acusados se apropiaron de los Bitcoin del Gobierno de los Estados Unidos de Norte América para enriquecerse. Mark Force y Stephan Bridges compraron y pagaron sus cuentas con las ganancias en el Bitcoin.
6. Crearon cuentas bancarias y realizaron transferencias electrónicas desde Mt. Gox a Quantum internacional con el motivo de lavar dinero

Demostración de cómo Force se conectaba y comunicaba con Ulbricht en el TOR client y compraba y vendía sus bitcoins

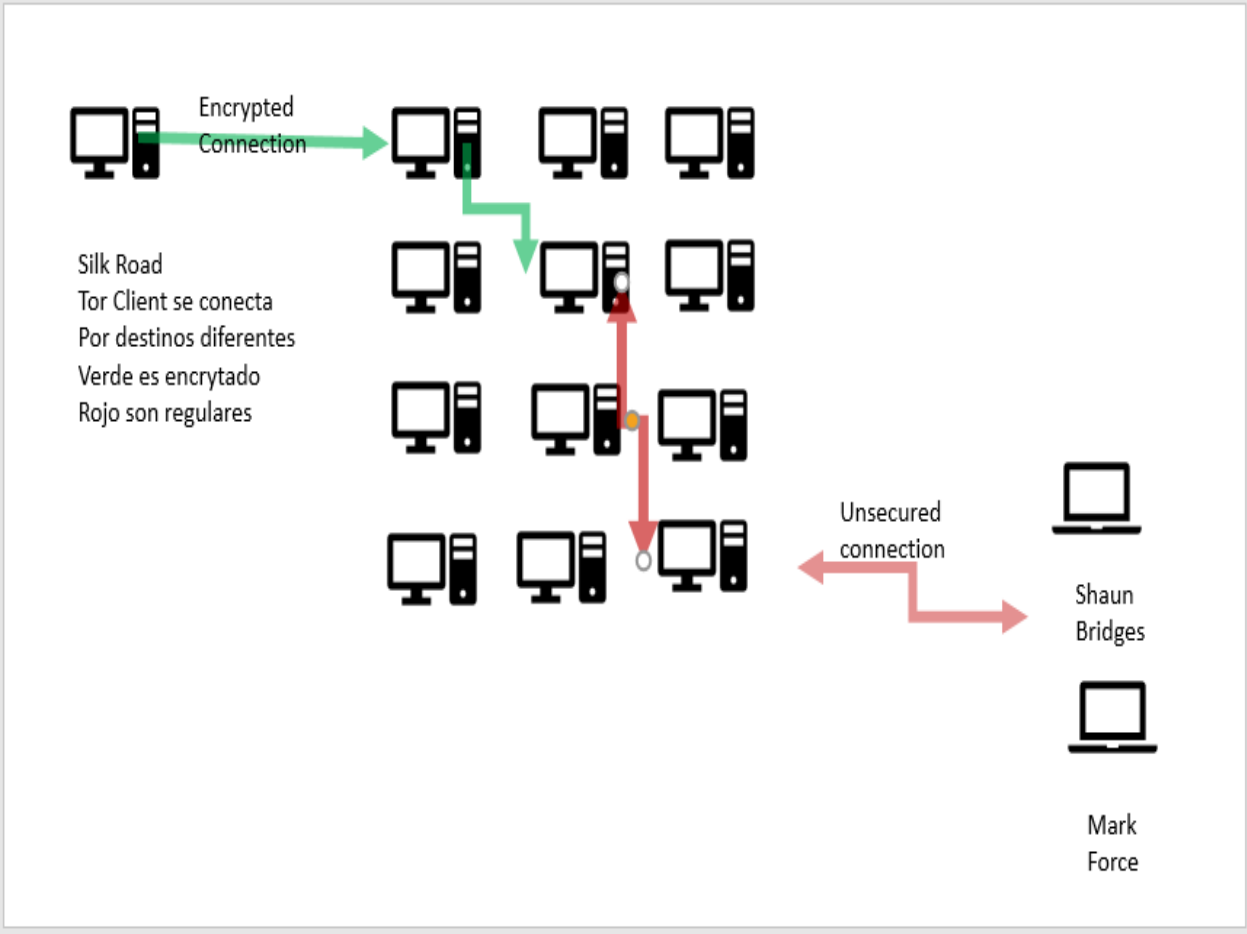
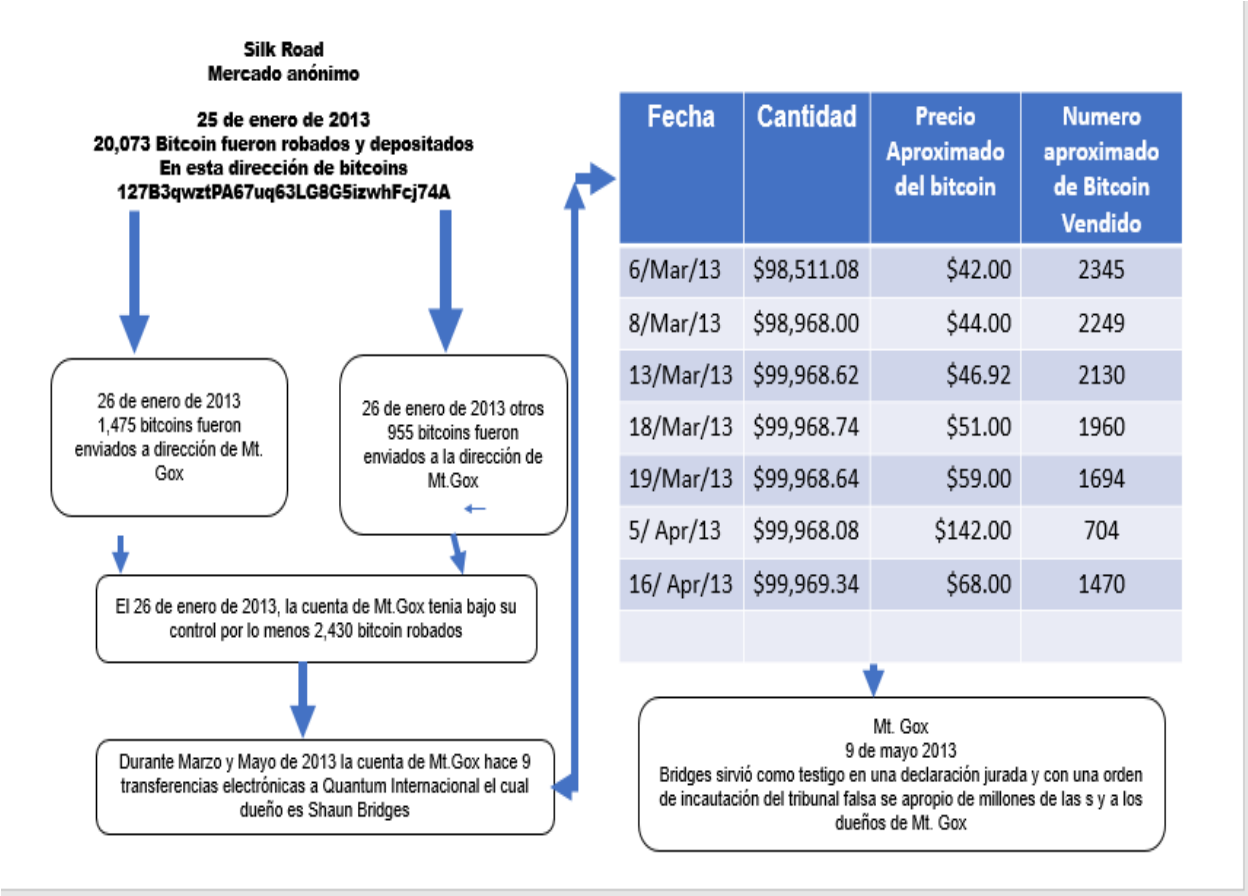


FIGURA 1: Organigrama de Silk Road como se conectaban

Shaun Bridges se apropiaba de los bitcoins con el uso credenciales administrativos de ex empleado de Silk Road y movían los Bitcoins a un banco llamado Mt. Gox y luego a sus cuentas personales. Con el uso de una orden de incautación falsa Bridges se apropió de la cuenta del dueño de Mt. Gox que era Multi-millonaria.



Fecha	Cantidad	Precio Aproximado del bitcoin	Numero aproximado de Bitcoin Vendido
6/Mar/13	$98,511.08	$42.00	2345
8/Mar/13	$98,968.00	$44.00	2249
13/Mar/13	$99,968.62	$46.92	2130
18/Mar/13	$99,968.74	$51.00	1960
19/Mar/13	$99,968.64	$59.00	1694
5/ Apr/13	$99,968.08	$142.00	704
16/ Apr/13	$99,969.34	$68.00	1470

Figura 2: Esquema de Fraude de Bitcoin a Mt. Gox

SECCIÓN 4: INFORME DEL CASO

Resumen Ejecutivo

Las circunstancias descritas en los expedientes del caso de United States v. Carl Mark Force & Stephen Bridges, llego a una conclusión que es necesario de contratar los servicios de un perito forense digital para que la evidencia provista sea admisible en el tribunal. Tigran Gamgaryan voluntariamente entrego un USB que es con la que Mark Force utilizaba como sus recursos y guardaba información en ella. Por la sensibilidad de la evidencia se procede hacer una copia del USB con FTK para no dañar o alterar la evidencia en el USB.

Objetivo

Se contrato el servicio de MFR Forensic con el objetivo de analizar, copiar y recuperar cualquier información que se pueda utilizar como evidencia del caso.

Alcance del Trabajo

En la fecha del 10 de mayo de 2018, la fiscal Melinda Haag hacen entrega al investigador forense Miguel Fabregas Ruiz de la compañía MFR Forensic un USB Color Blanco de la marca Scandisk donde se presume existe evidencia necesaria relevante que ayude esclarecer el caso. Todo el análisis será realizado en el USB para buscar alguna evidencia de utilidad para el caso.

Datos del Caso

1. Número del Caso: E-1-2017-04-22
2. Caso: United Sates v. Mark Force, Shaun Bridges
3. Investigador: Miguel Fabregas Ruiz

4. Representante del cliente: Melinda Haag y Kathryn Haun, William Frentzen Fiscales designados de Distrito Norte de California

Descripción de los dispositivos utilizados:

1. Desktop Dell con todas las herramientas necesarias para conducir una investigación forense.
2. FTK Imager, para realizar una copia que no perjudique la evidencia en el USB para poder analizarlo.
3. USB Cruzer Glide 16GB Color Blanco serie SDCZ60-016G

Resumen de Hallazgos

El análisis pericial de la evidencia es un evento de magnita integridad en el proceso. El uso de herramientas que permitan la extracción e integridad de la evidencia promueve que el proceso judicial no se encuentre en perjuicio. Después de analizar la prueba se encontró evidencia suficiente que los cargos sean sostenible en el Tribunal.

Cadena de Custodia

Evidencia recogida en la biblioteca de EDP University. Evidencia entregada por el Agente Tigran Gamgaryan IRS-Criminal Investigador y recogida por el Sr. Miguel Fabregas Ruiz, estudiante EDP.

Evento Verificado por: Miguel Fabregas

de evidencia: E-1-2017-04-22

Fecha de comienzo: marzo 22, 2018 – 9:09 a.m.

Fecha de Terminación: mayo 22, 2018 – 9:40 a.m.

Lugar de Origen: Biblioteca EDP University

Destino: Biblioteca, EDP University

Segundo Evento:

Descripción del Evento:

Creación de numero de caso y asignación de evidencia al mismo.

Evento Verificado por: Miguel Fabregas Ruiz

de evidencia: E-1-2017-04-22 Asignada al caso # C-1-2017-04-22

Fecha de comienzo: mayo 22, 2018 – 9:48 a.m.

Fecha de Terminación: mayo 22, 2017 –3:45 p.m.

Lugar de Origen: Biblioteca, EDP University

Destino: Biblioteca, EDP University

Pedir manual de políticas, verificar si es permitido remover equipos propiedad de ACME sin el conocimiento o consentimiento del empleado. Acuérdate de validar la evidencia de que el empleado firmo el acuse de recibo y entendimiento de las políticas o si hay evidencia de Trainings al respecto y la aprobación de estos.

Procedimiento

Al iniciar el programa se introduce el USB a la computadora y se comienza el proceso de extraer la información del expediente.

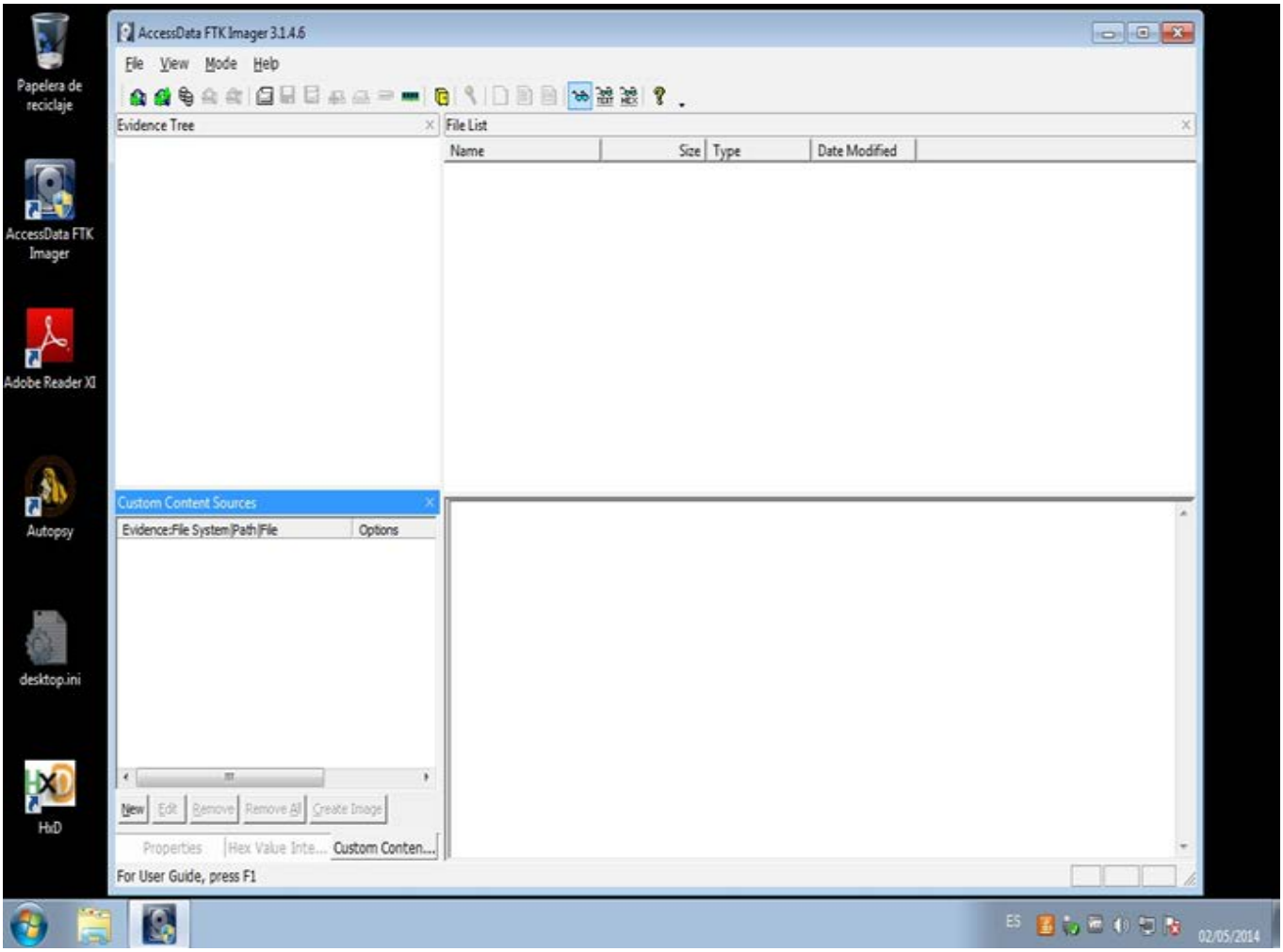


Figura 3- Inicio del Procedimiento

Se comienza el proceso de copiar la imagen del USB para mantener la integridad del expediente. Hacer clic en la opción “File -> Créate Disk Image” o Archivo -> Crear Imagen de Disco. Se presentará una nueva ventana donde se requiere definir la Fuente. Para propósito de la presente práctica se creará una imagen forense de toda una unidad USB o Memory Stick, por lo tanto, se selecciona la opción “Physical Drive” o Unidad Física. Luego hacer clic en el botón “Siguiente”. En una nueva ventana se muestra un menú desplegable, en el cual se selecciona la Unidad Fuente correspondiente, para luego hacer clic en el botón “Finish” o Finalizar.

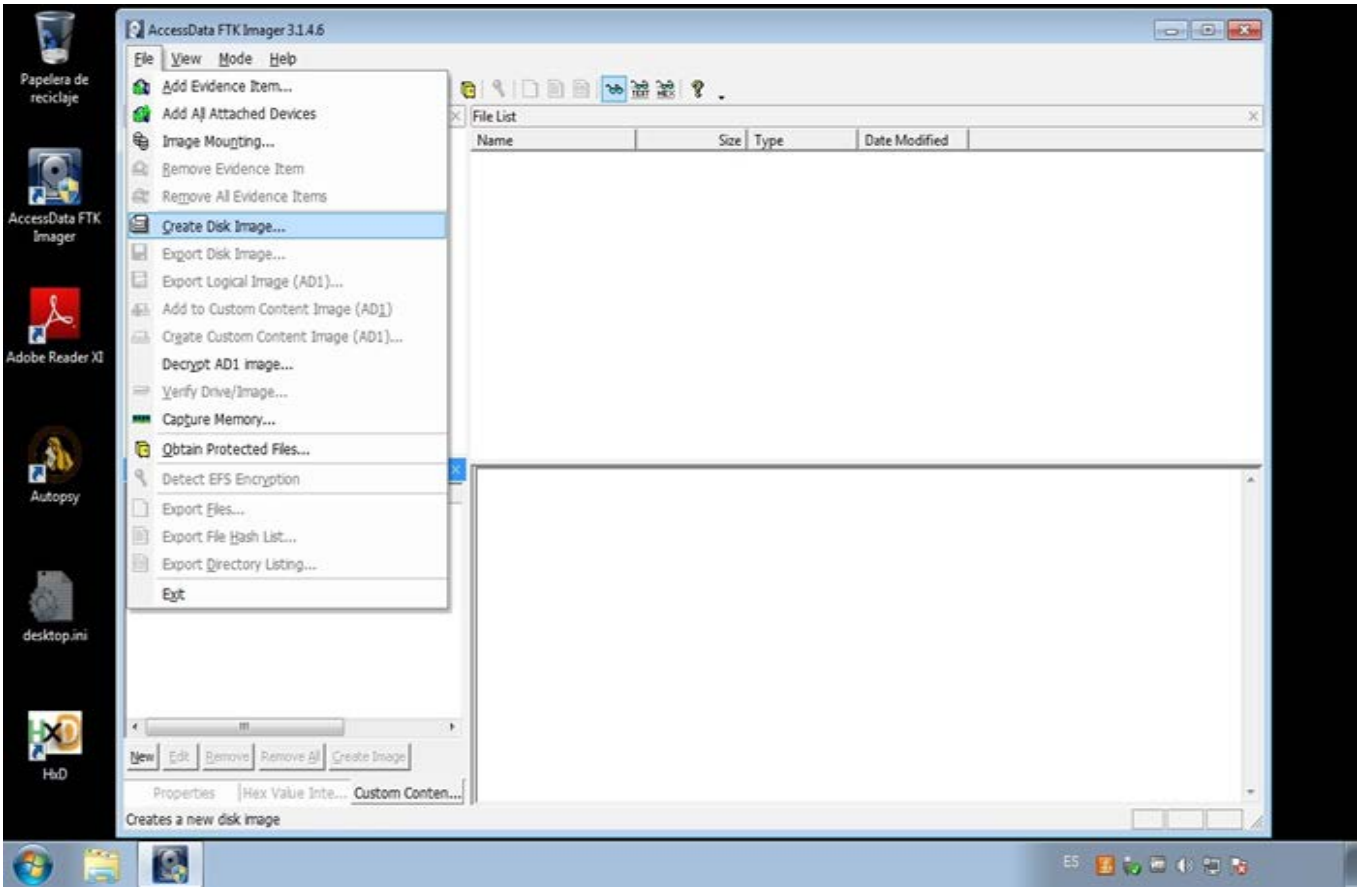


Figura 4: Crear la Imagen

En una nueva ventana se muestra un menú desplegable, en el cual se selecciona la Unidad Fuente correspondiente, para luego hacer clic en el botón “Finish” o Finalizar.

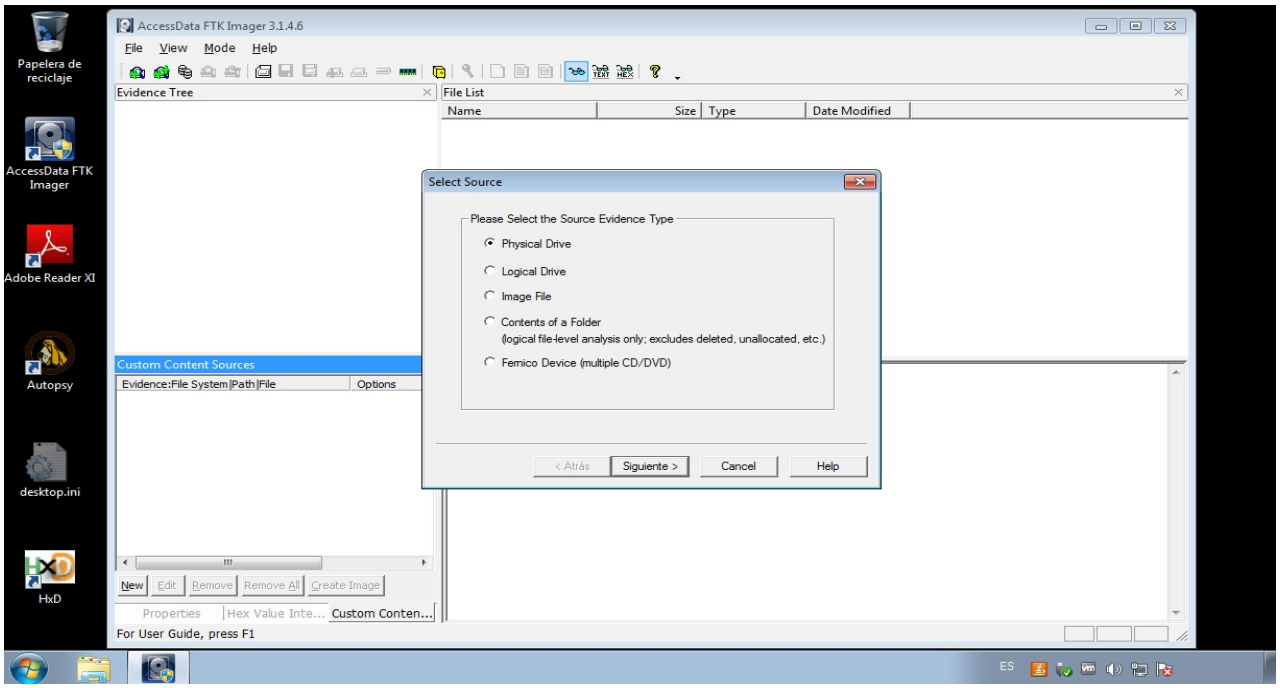


Figura 5: Selección de fuente correspondiente

La siguiente ventana permite definir un Destino para la Imagen. Para esto es necesario hacer clic en el botón “Add...”

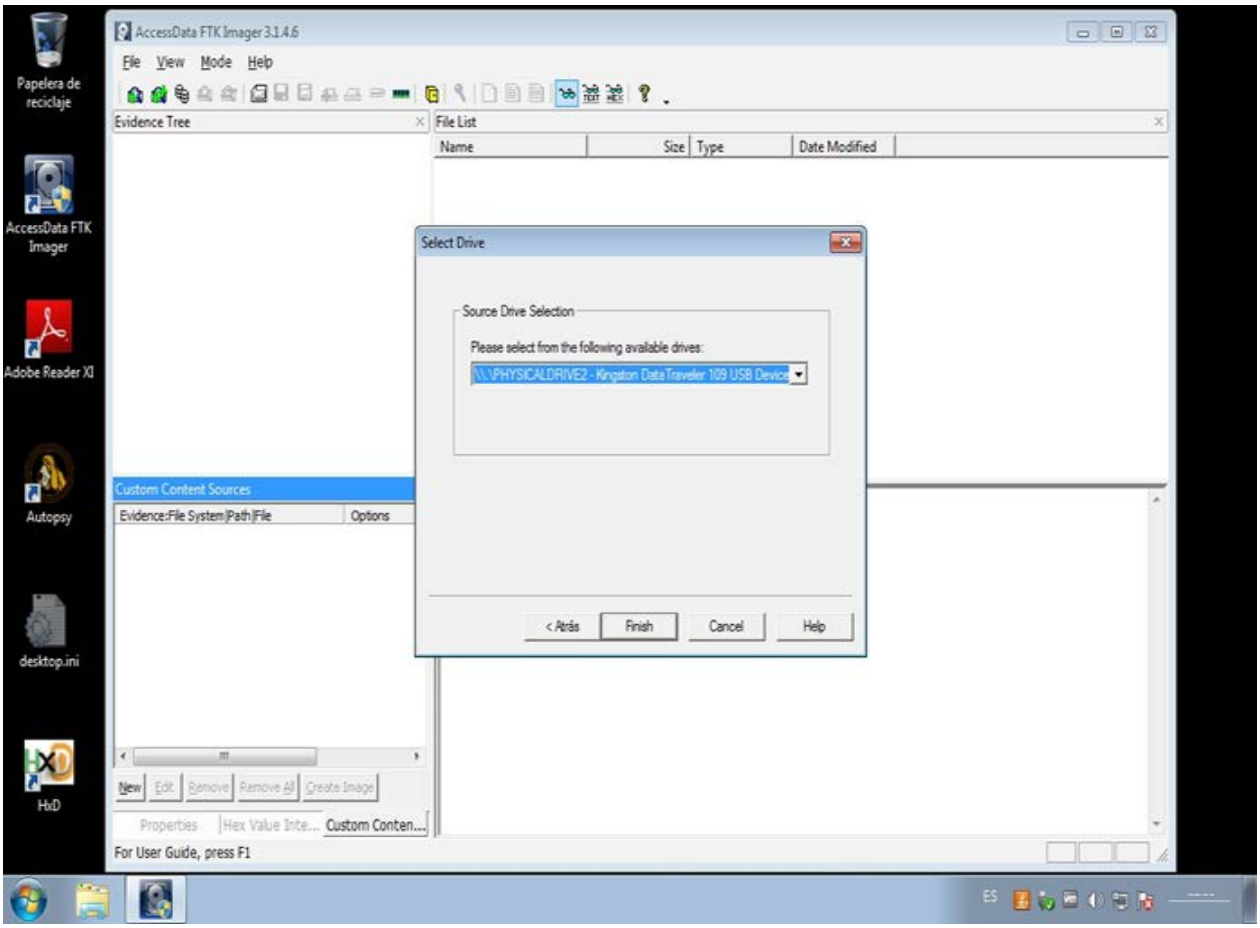


Figura 6: Destino de la Imagen

En esta ventana se define el tipo de la imagen de destino a crear. Para el caso de la presente práctica será una imagen “Raw” o en bruto, es decir tal y como sería creada utilizando una herramienta como dd o dcfldd. Revisar la publicación de título “Crear la Imagen Forense desde una Unidad utilizando dd”.

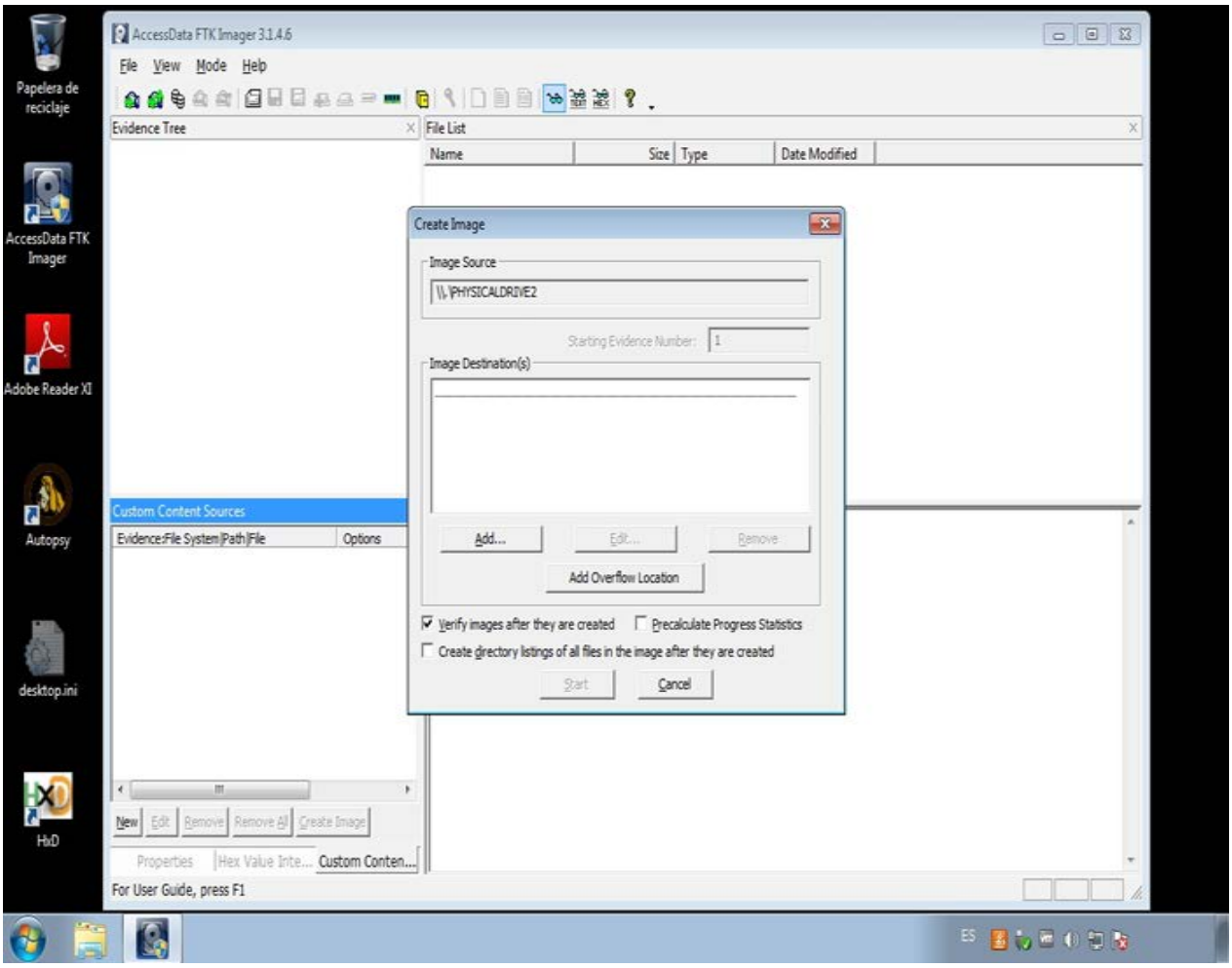


Figura 7: Tipo de Imagen a crear

La siguiente ventana solicita ingresar información sobre el ítem de evidencia. Al completar la información hacer clic en el botón “Siguiente”.

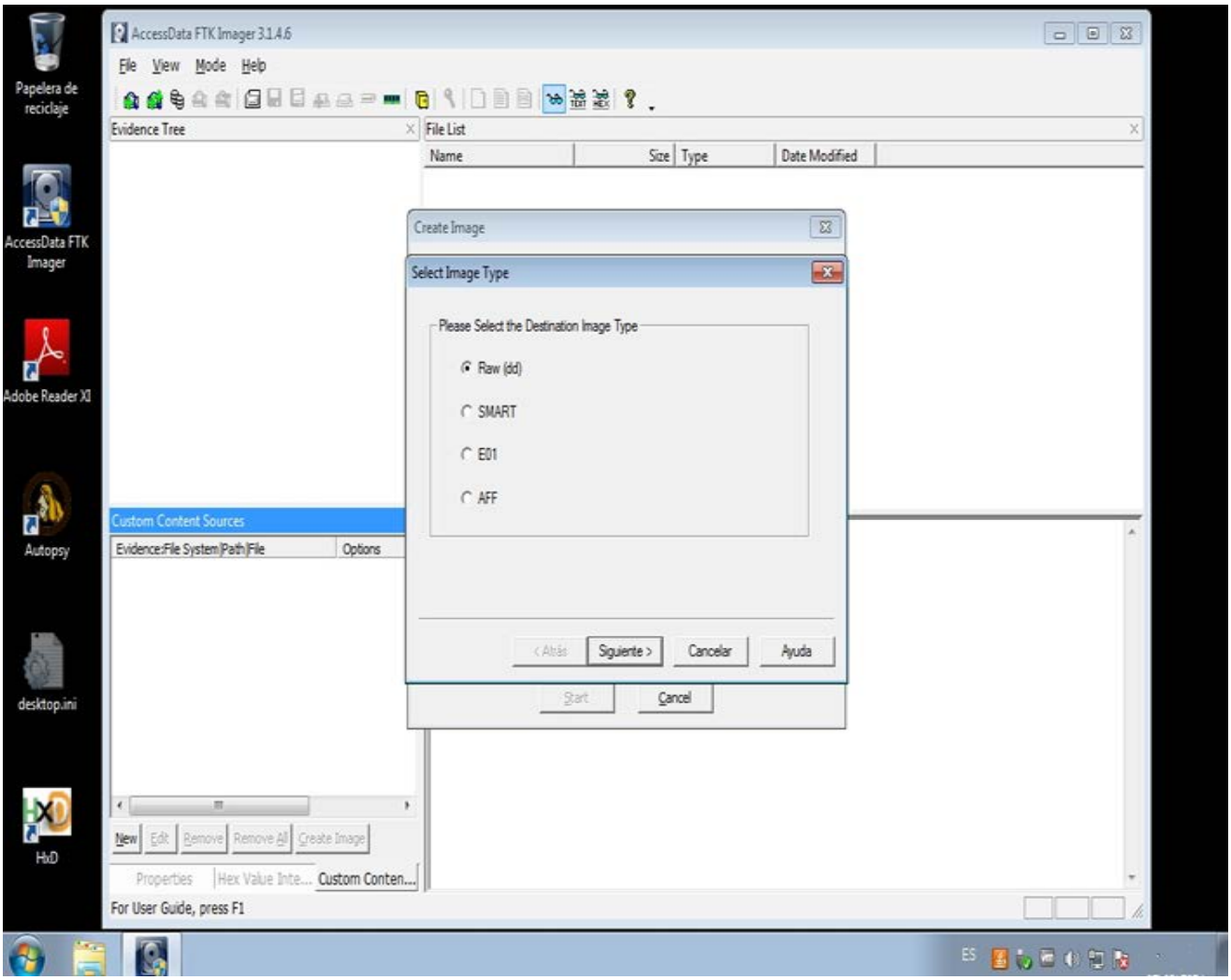


Figura 8: Ingresar información de la evidencia

Se requiere definir la carpeta donde se almacenará la imagen forense. La cual es seleccionada haciendo clic en el botón “Browse” o Navegar. A continuación, se requiere nombrar la imagen forense (UnidadUSBKR). Y opcionalmente definir si la imagen resultante será dividida en varias partes o sino no será fragmentada. Para el caso de la presente práctica no será divida, por lo tanto, se define el valor “0” en el campo “Image Fragment Size (MB)” o Tamaño del Fragmento de la Imagen.

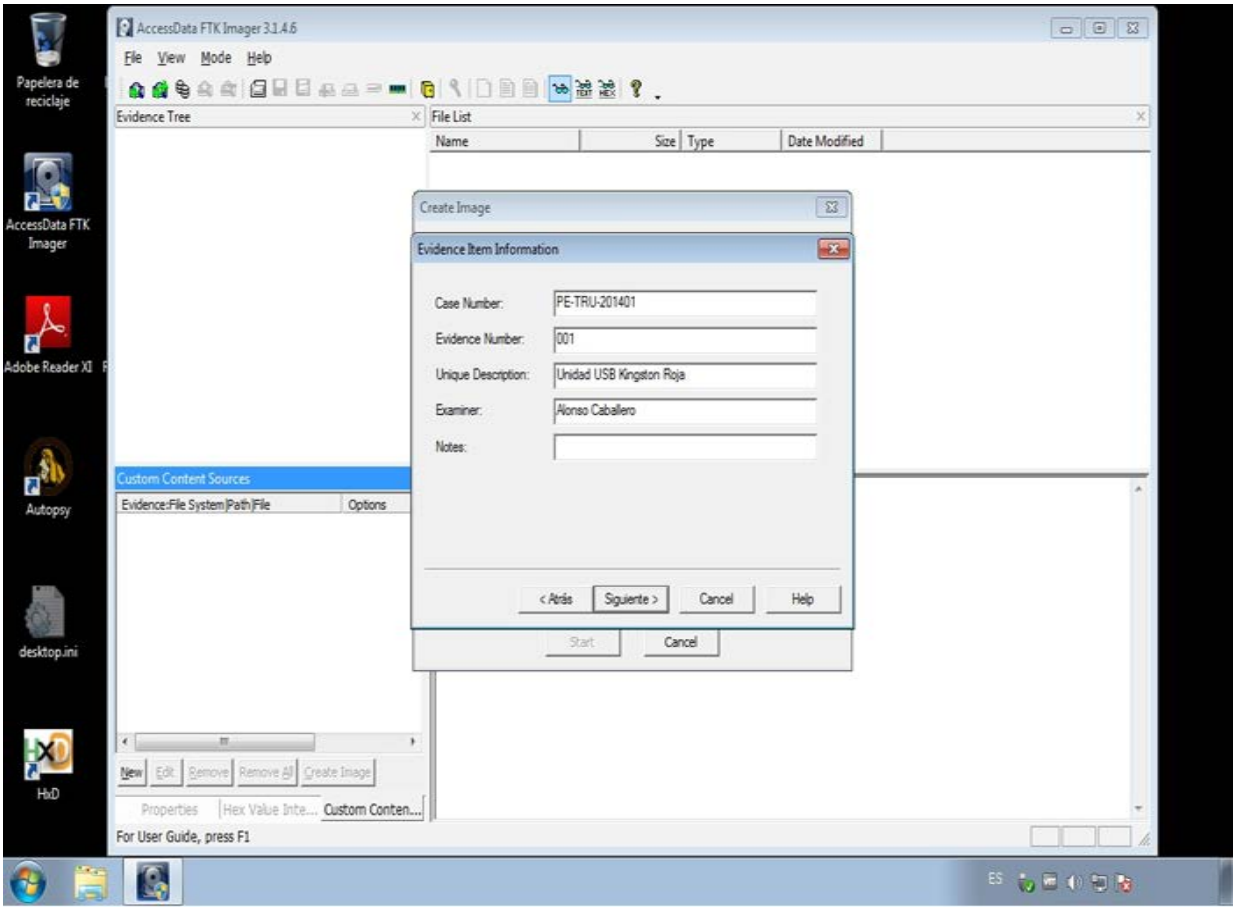


Figura 9: Definir la carpeta donde se almacena la imagen creada

Al Hacer clic en el botón “Finish”. Se mostrará un resumen de las opciones seleccionadas.

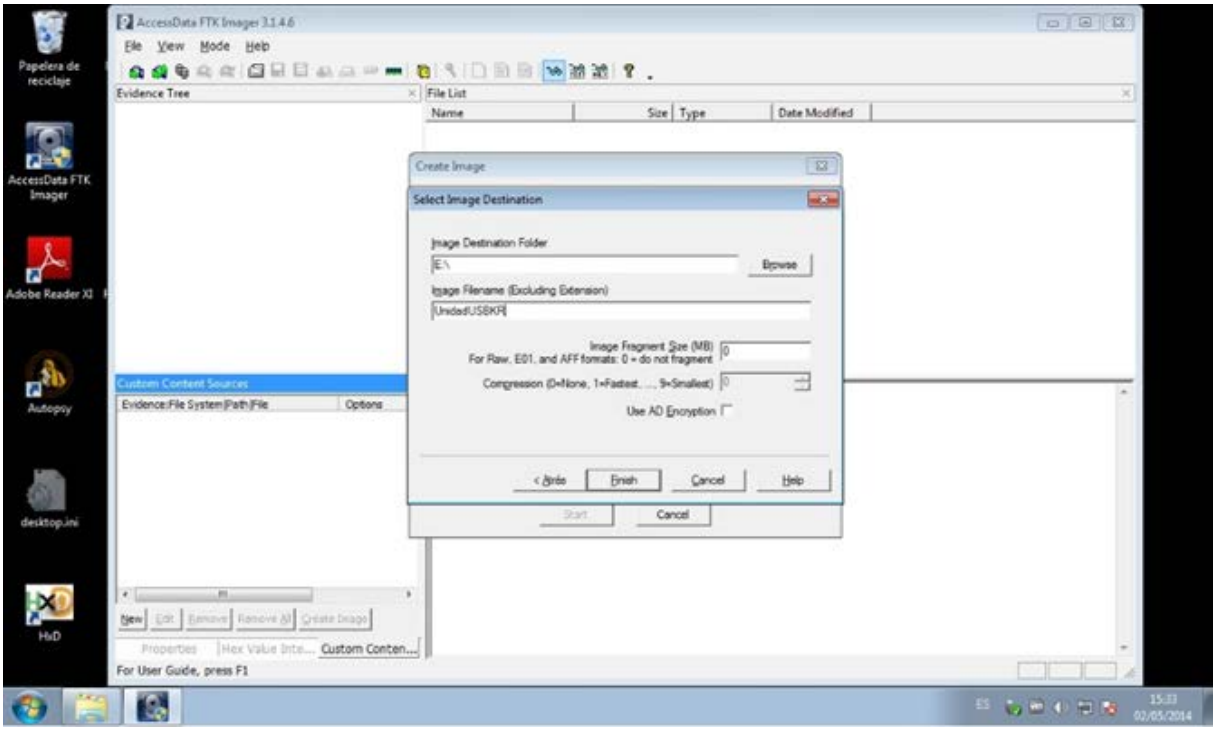


Figura 10: Resumen de las opciones

El proceso de creación de la imagen forense desde la unidad USB o Memory Stick iniciará al hacer clic en el botón “Start” o Iniciar.

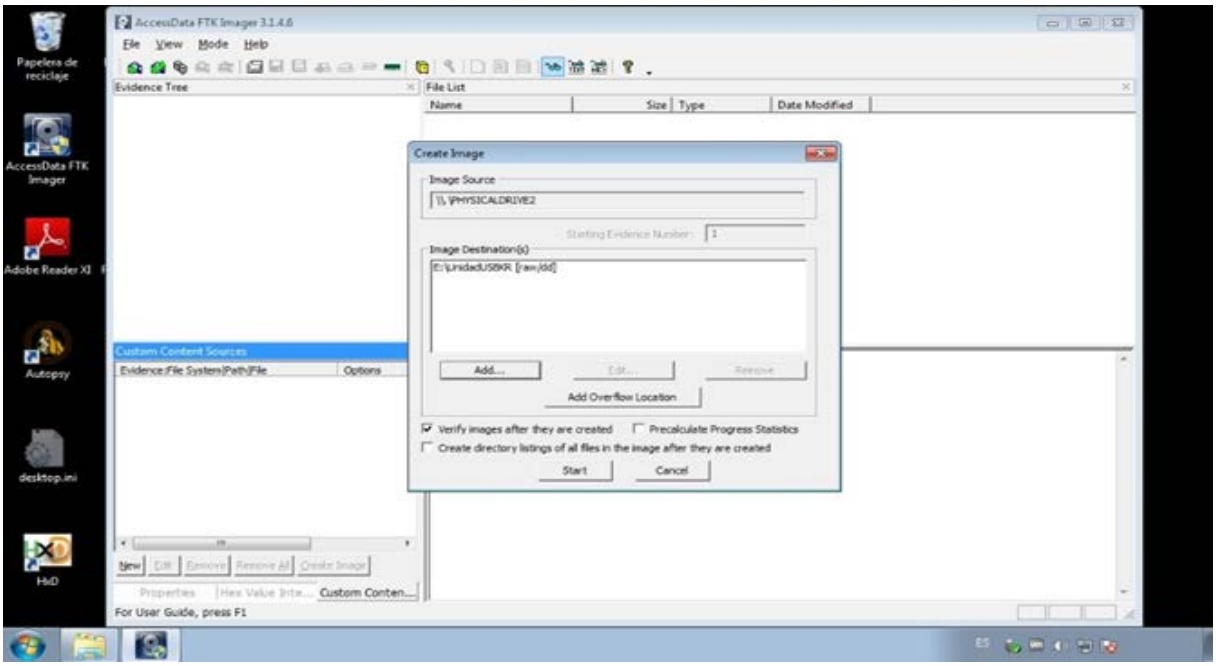


Figura 11: Proceso de creación

Finalizada la creación de la imagen forense, inicia la verificación de la imagen creada.

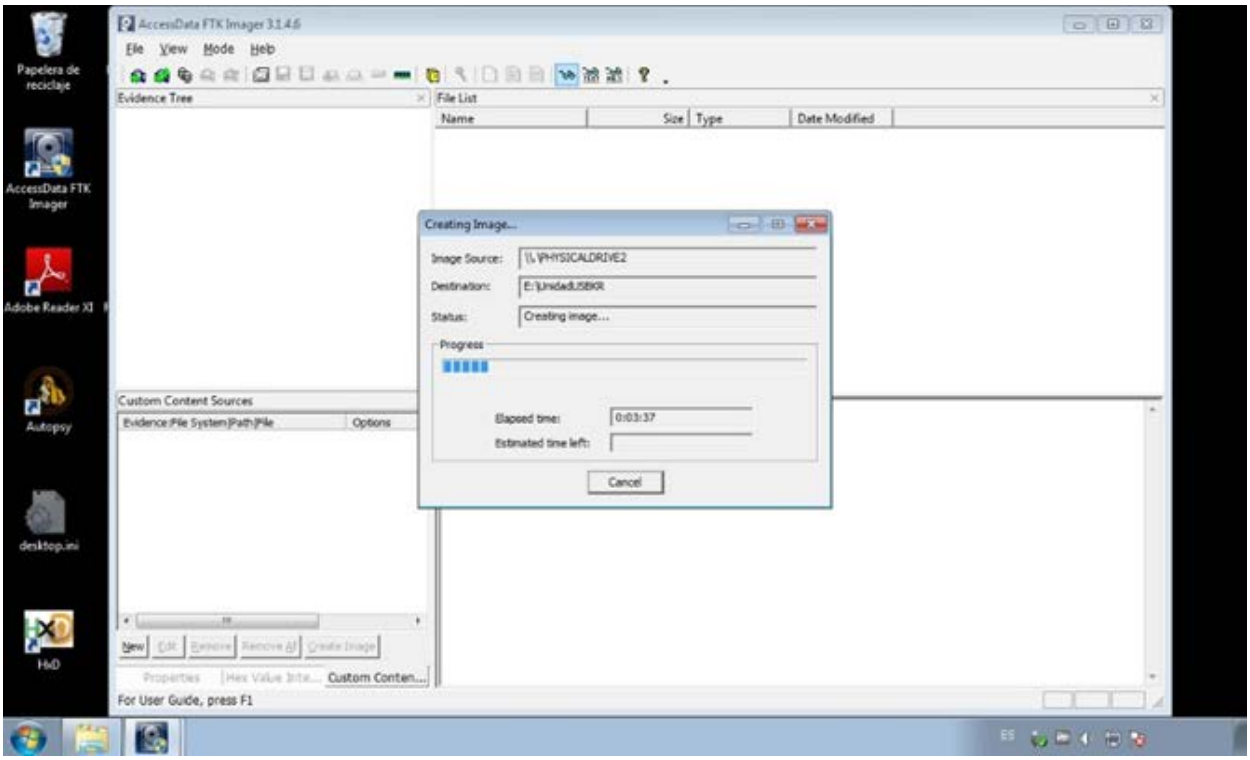


Figura 12: Verificación de Imagen

Al finalizar todo este procedimiento se presentan algunos resultados finales. Los resultados muestran el número de sectores copiados. La generación de un Hash MD5 y un Hash SHA-1. Anotar la coincidencia entre el campo “Computed Hash” o Hash Calculado, es decir el hash obtenido desde la unidad USB o Memory Stick, y el campo “Report Hash” o Hash Reportado, el cual se genera desde la imagen forense creada de nombre “unidadUSBKR.001”. Anotar también que no se han detectado sectores Malos.

.

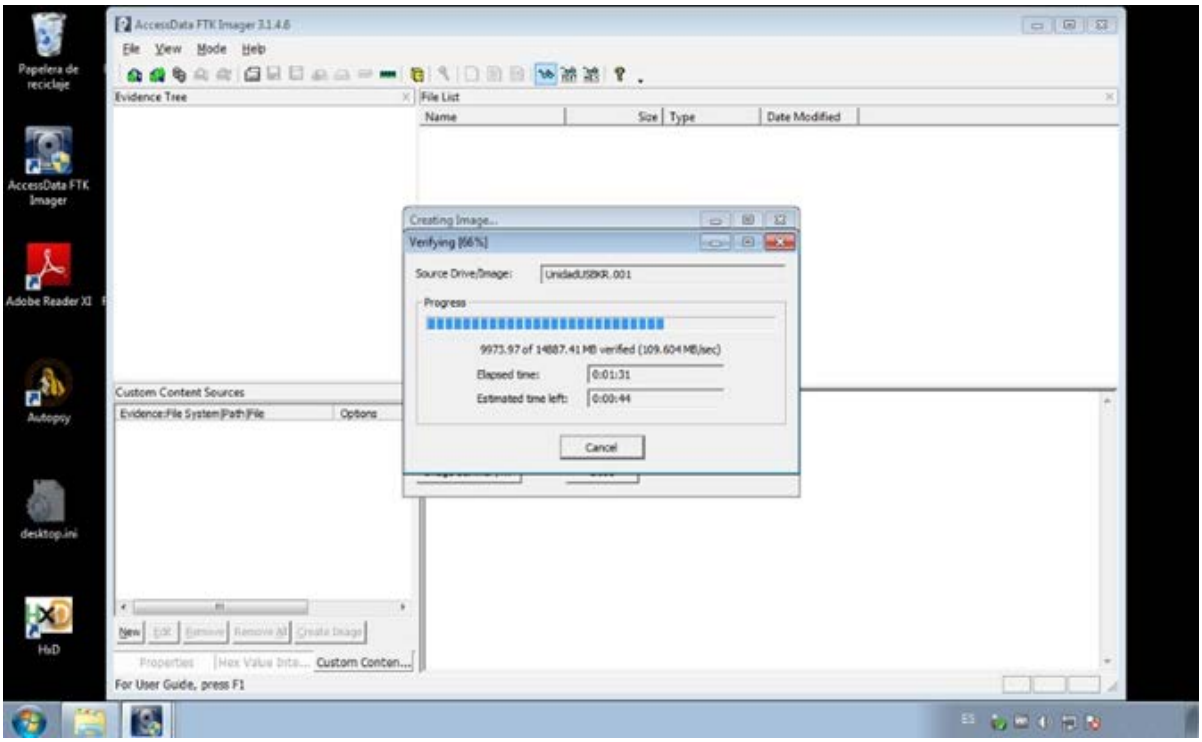
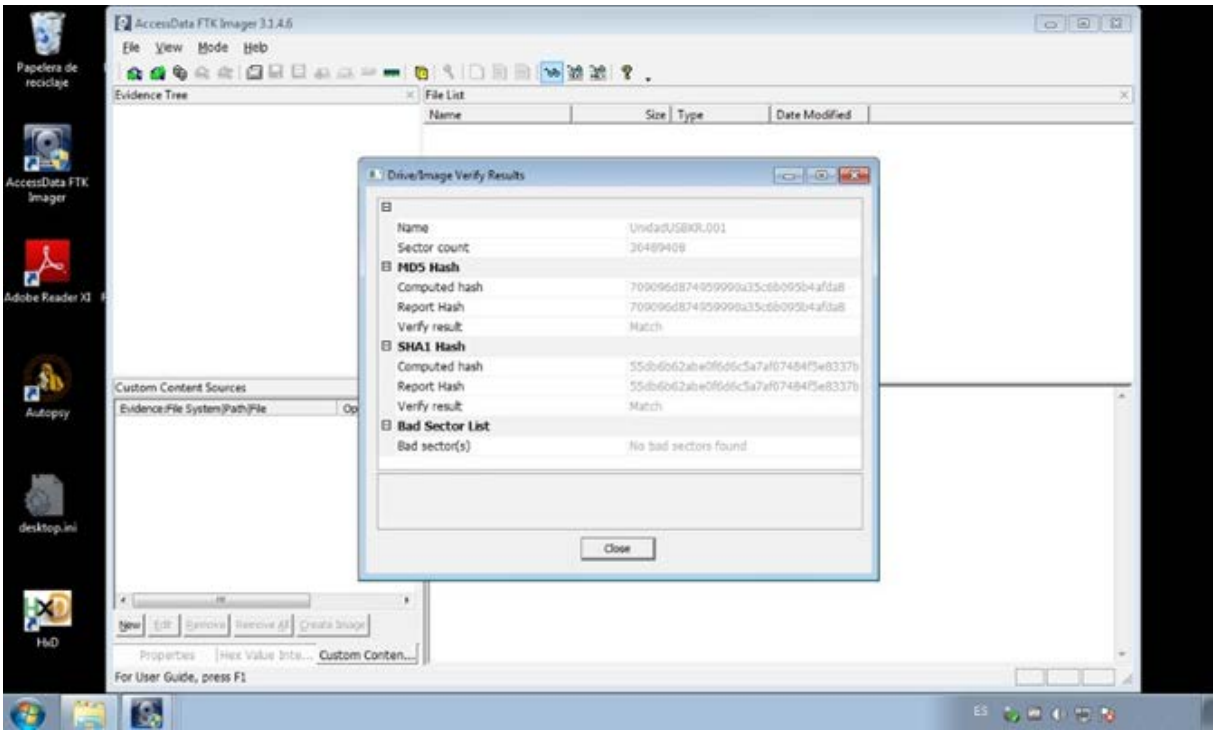


Figura 13: Resultados finales

En el mismo directorio o unidad donde se ha creado la imagen forense, se encontrará un archivo de texto con el mismo nombre de la imagen forense creada (UnidadUSBKR.txt), en el cual reside toda la información detallada del proceso realizado.



.

Figura 14: Archivo de Texto de imagen creada

Evidencia encontrada en el USB que auto incrimina y la misma fue utilizada en contra de Mark Force, Stephen Bridges y Ross Ulbricht.

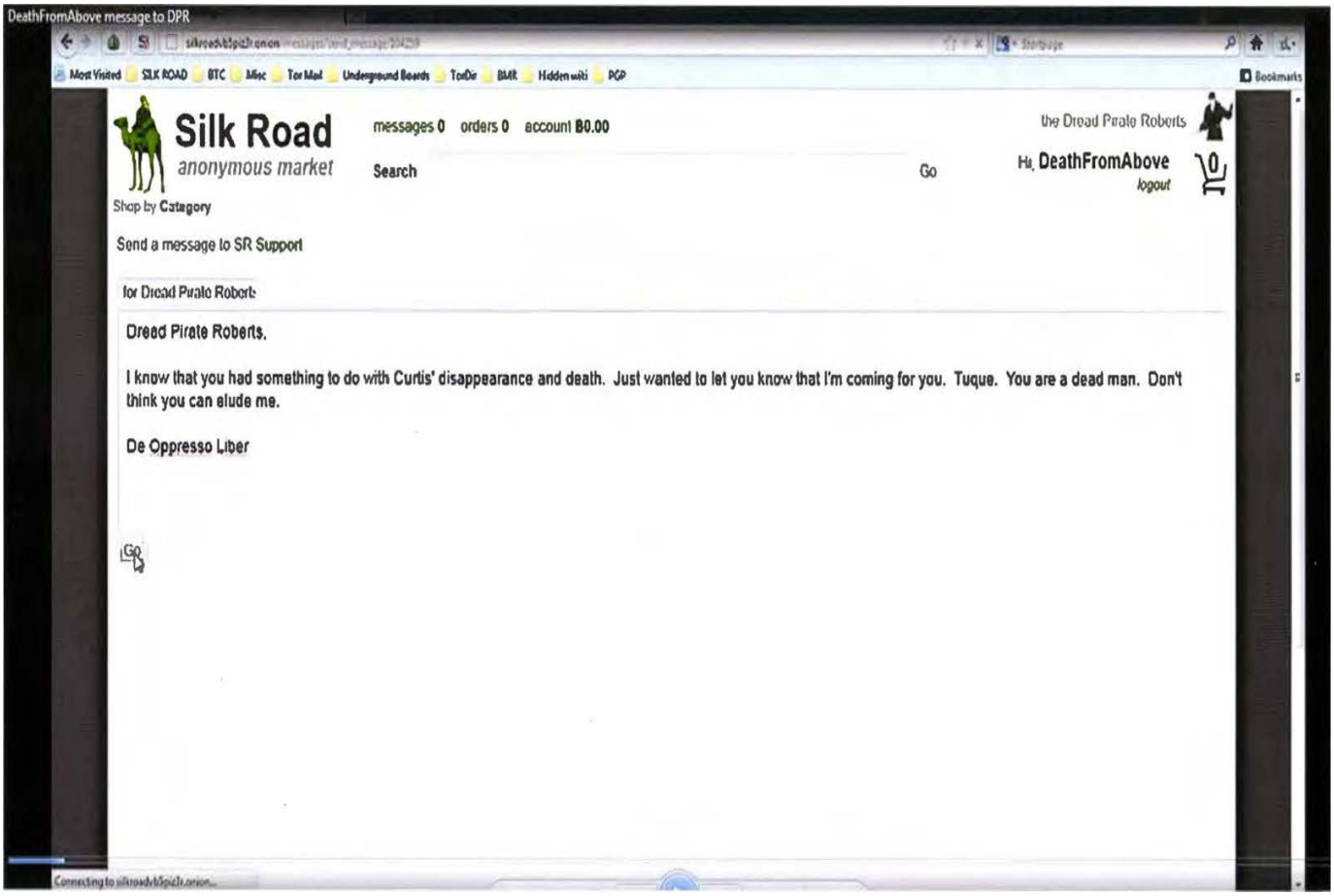


Figura 15: Evidencia encontrada

Conclusión

La cadena de custodia se establece para la integridad y seguridad de los acusados con la intención de proteger sus derechos. Después de un análisis rigorosa de la evidencia se encontró que Mark Force y Shaun Bridges establecieron un sistema que defraudaba al gobierno con solo comprar y vender Bitcoin y transferir las ganancias a sus cuentas personales con el propósito de enriquecerse.

SECCIÓN 5: DISCUSIÓN DEL CASO

Según lo que describe el pliego acusatorio y documentos analizados del caso United States v. Mark Force y Shaun Bridges (2015), a los acusados cometieron, Robo de propiedad de gobierno, lavado de dinero, fraude electrónico y conflicto de intereses.

Luego del análisis provisto por la agencia de MFR Forensic se llega a la determinación que la evidencia en el USB era de tal magnitud que los acusados cometieron los delitos antes mencionados. En adición se encontró evidencia que Ross Ulbricht cometió una amenaza de muerte y Muerte por contrato al cual fue acusado y cumpliendo en estos momentos en una penitenciaria en California.

SECCIÓN 6: AUDITORIA Y PREVENCIÓN

En esta sección se estudió todas las posibles maneras de asegurar que la compra y venta de Bitcoin sea segura y de confiable seguridad que cuando usted los compre no seas objeto de fraude o engaño. El hecho de que Bitcoin es una moneda digital ya lo hace susceptible a fraude, porque cualquier compañía le puede vender una dirección fatula. Los registros de direcciones de Bitcoins a pesar de que son registrados en un número de servidores son atacados numerosas veces por los hackers y son vulnerable. Pero como todo mercado de inversión capital hay un riesgo siempre en el mercado, recomiendo si vas a invertir en Bitcoin no te arriesgues tanto con capitales grandes y así no sea objeto de ser una víctima más en esta modalidad.

Hallazgos Detallados

Como parte de la auditoría realizada a Quantum Internacional y Mt. Gox se encontró los siguientes hallazgos relacionados al caso.

1. No se tienen un sistema que valide transferencias electrónicas.
    a. Condición: No existe un registro de transferencias electrónicas a menos entre a todas las cuentas.
    b. Criterio: con el registro se puede validar las transferencias electrónicas y cantidades no sean extremas.
    c. Causa: sin ningún control en los fondos transferidos electrónicamente se puede violar muchas leyes que la institución sea responsables por aceptar eso fondos ilegales.
    d. Efecto: Banco puede ser responsable de recibir fondos ilegales y pagar multas que pueden ser de millones y hasta perder los fondos transferidos.
    e. Recomendación: implementar sistema que registre y valide todas transacciones de fondos electrónicos

SECCIÓN 7: CONCLUSIÓN

Para poder llegar al extremo de cometer un fraude en contra del gobierno solo se necesita una oportunidad y el conocimiento para cometerlo. Las investigaciones toman tiempo y dinero, pero por lo más hábil y listo que seas siempre te van a detener y pasaras una vergüenza que tus hijos y familia nunca te lo perdonaran. Por solo ser oficiales del orden público y el gobierno te da esa libertad para investigar y utilizar sus recursos que son muchos en la investigación, no te da la autoridad de defraudar y enriquecerse ilegalmente con el dinero que es del pueblo.

Aquí se observó como una investigación de una página de web se torna en una investigación hasta de amenaza de muerte por los fuerte vínculos que el mismo gobierno presento y por la ambición del dinero y fortunas sin límites ocurren todo tipo de fraudes, robos y hasta casi la muerte.

Para concluir, el comportamiento de los agentes del orden público en este caso no es aceptable y denigrante hacia las agencias que depositaron la confianza en que iban a descubrir la manera de estafar y destruir la imagen del gobierno.

SECCIÓN 8: REFERENCIAS

American Psychological Association. (2012). Publication Manual of the Psychological Association. (6ta Ed.) Washington, DC: Library of Congress

Antonopoulos, A (2016). Why Dumb Networks are Better, Recuperado Junio 2018 https://medium/@aantonop/latest

Oroyfinanza.com (2015) Porque hay muchas estafas y fraudes en Bitcoins, Recuperado de https://www.oroyfinanzas.com/2015/12/por-que-hay-muchas-estafas-fraudes-bitcoin/

Schwartz, M. (2015). Former Secret Service Agent Pleads Guilty to $800K Bitcoin Theft, Recuperado May 2018 https://www.bankinfosecurity.com/former-secret-service-agent-pleads-guilty-to-800k-bitcoin-theft-a-8513

Shane, D. (2018) Un robo de criptomonedas por 530 millones de dólares puede ser el más grande de todos, Recuperado de https://cnnespanol.cnn.com/2018/01/29/robo-criptomonedas-coincheck-asia-japon/

United States District Court, Northern District of California. (2015) 3:15-cr-00319: USA v. Shaun Bridges, Recuperado de https://cryptome.org.2015/12/bridges-093.pdf

United States District Court, Northern District of California. (2015) 3:15-cr-70370. USA v. Carl Mark Force IV, et al, Recuperado de https://antilop.cc/sr/files/2015_03_25_FORCE_criminal_complaint.pdf

United States District Court, Southern District of New York (2018) 1:15-cr-00093-VEC: USA v. Sheldon Silver, Recuperado de https://www.pacer.gov/

United States District Court for the District of Connecticut (2016) 3:16-mj-464-SALM: USA v. Michael Richo, Recuperado de https://www.pacer.gov/

United States District Court, Eastern District of Oklahoma (2018) 6:18-cr-00064-RAW: USA v. Miguel León Bejarano, Recuperado de https://www.pacer.gov/