EDP University of Puerto Rico

Recinto de Hato Rey

Programa de Maestría en Sistemas de Información con Especialidad en Seguridad de Información e Investigación de Fraude

ACOSO CIBERNÉTICO

Análisis del caso: USA vs. Ryan S. Lin

Marzo, 2019

Preparado por:

Christopher Rodríguez Maldonado

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

ACOSO CIBERNÉTICO

Análisis de caso: USA vs. Ryan S. Lin

(1:18-cr-10092)

Preparado por: Christopher Rodríguez Maldonado

Ha sido aceptado como requisito parcial para el grado de:

Maestría en Sistemas de Información

Especialidad en Seguridad de Información e Investigación de Fraude

Marzo, 2019

_____

Miguel A. Drouyn Marrero, Director

Agradecimientos

Primordialmente le quiero dar las gracias a Dios por darme la fortaleza y voluntad de poder lograr las metas que me establezco en la vida. Por brindarme la salud para poder batallar con los obstáculos en el camino y seguir marchando hacia delante. Agradezco a mi familia quien me enseñó los valores más importantes de la vida. En especial a mi madre Ana, quien luchó contra viento y marea para poder brindarnos la mejor calidad de vida posible, hasta en sus últimos momentos. De quien aprendí a ser como soy hoy día y de lo cual jamás me arrepentiré, ya que estoy consciente que fuiste una guerrera y sin ti poco hubiera sido posible, te amo. A mi padre y hermanos, Ramón Sr., Ramón Luis y Christian, porque durante todo mi camino me recuerdan constantemente mis logros y a no dejarme vencer.

Quiero agradecerles a todos los profesores que fueron parte de esta etapa en mi vida. Todos me ayudaron a mejorar como persona y a no perder el interés en mis metas. Gracias al Dr. Drouyn por haberme aceptado y permitirme lograr mi grado de maestría junto a sus compañeros.

Como último, pero no menos importante, quiero agradecerles a mis compañeros de clase, quienes estuvieron junto a mí desde el principio y luchamos juntos para lograr nuestra meta. Gracias a Raúl Cordero, Janice Fuentes, Cathy Pinero y Wilmer D. Charmant por dejarme ser parte del mismo grupo, ayudarme con todos los proyectos que trabajamos juntos y por darme el honor de ser parte de sus amistades.

Tabla de contenido

Tabla de figuras

Sección 1: Introducción y trasfondo

Introducción

El tema del ciberacoso es serio y debe tomarse con más seriedad desde el primer indicio. Hoy día la facilidad en que las personas pueden ser atacadas cibernéticamente es preocupante. Recuerdo cuando había orientaciones en las escuelas con el fin de proteger nuestra información personal, pero en las redes sociales no se tomaba con seriedad. Según Katehakis (2015), cerca de 1 millón de mujeres y 400,000 hombres son acosados cada año en los Estados Unidos, la mitad de ellos suelen ser adultos jóvenes de menos de 25 años. También dijo que "el acoso cibernético es una compulsión que busca humillar, controlar, asustar, manipular, avergonzar, vengar, o lastimar a la víctima. La mayoría de estas personas son obsesivas, inestables, lastimados o están mentalmente desajustadas".

Expondré cómo esta persona utiliza los medios tecnológicos para cometer ciberacoso escondiendo su identidad de las víctimas y de los oficiales de la ley. La mayoría de los comportamientos anteriormente mencionados por la Dra. Katehakis fueron observadas en este caso.

Descripción del caso

Número del caso: 1:18-cr-10092

Caso: USA v. Ryan S. Lin

Partes en el caso:

Acusado

Ryan S. Lin

Víctima

Jennifer Smith

Investigadores

Jeffrey Williams, agente especial del FBI,

Abogados

1. Daniel J. Gaudet
2. Frances M Doran, Jr.
3. J.W. Carney, Jr.
4. Nathaniel Silver
5. Reyna M. Ramírez

Fiscales

1. Amy H. Burkart- Assistant United States Attorney for District of Massachusetts
2. Mona Sedky- U.S. Department of Justice Senior Trial Attorney Computer Crime & Intellectual Property Section.

Jueces

Andrew E. Lelling- United States Attorney for the District of Massachusetts

Trasfondo

Según el documento de USA v. Ryan Lin (2017), el agente Jeffrey Williams redacta que Lin tiene experiencia como programador de sistemas y sus estudios fueron en sistemas de información en una universidad prestigiosa, *Renssealer Polytechnic Institute*. Con esta experiencia el acusado abuso de su conocimiento para cometer los delitos. Ryan sabía cómo acceder a computadoras y obtener información confidencial sin autorización. Acosaba a las victimas enviando mensajes y fotos anónimamente utilizando servicios anónimos de mensajería.

Creo cuentas falsas con identidades de las víctimas con las que enviaba los mensajes y solicitaba encuentros sexuales. Luego, comenzó a realizar amenazas falsas de bombas y tiroteos haciéndose pasar por las víctimas en escuelas, centros comerciales, entre otros.

Según el documento de USA v. Ryan S. Lin (2018c), donde el Dr. Mendoza hace referencia al reporte psicológico realizado a Ryan Lin, Lin padece de ASD (Desorden del Espectro Autista) entre nivel 1 y 2. Según National Institute of Mental Health (2018), el desorden del espectro autista es una condición neurológica y de desarrollo que comienza en la niñez y dura toda la vida. Esta condición afecta como una persona se comporta, interactúa con otras personas, se comunica y aprende. Aunque en la evaluación Lin haya sido diagnosticado con ASD, esto no implica que la condena sugerida pueda disminuir. Otras condiciones que Mendoza pudo identificar en la conducta de Ryan fue su deficiencia social, dificultad al cambio, inflexibilidad y concentración en ciencia de computadoras. Por su gran conocimiento sobre computadoras es que pudo realizar los delitos sin ser detectado por tanto tiempo. Ryan consiguió acceso no autorizado a cuentas privadas de sus víctimas, publicó información privada de sus víctimas, creó cuentas en redes sociales haciéndose pasar por sus víctimas y realizó falsas amenazas de bombas y tiroteos con la identidad de sus víctimas.

Lin estaba totalmente consciente de que tendría consecuencias con la ley mientras cometía los delitos. Su forma de ocultar su identidad y cometer los delitos anónimamente es evidencia de que conocía que era ilegal y que tendría consecuencias de ser encontrado. Lin implementó diferentes técnicas para no ser detectado, por ejemplo, utilizando el internet mediante un servicio que anonimiza las direcciones IP de la computadora como TOR “*The*

Onion Router" (por sus siglas en inglés); utilizando servicios de VPN "*Virtual Private Network*" (por sus siglas en inglés); enviando mensajes de textos por servicios extranjeros anónimos; y utilizando proveedores extranjeros de emails encriptados.

Descripción de hechos

Según el documento de USA v. Ryan Lin (2017), en el affidavit incluido en este documento, el agente federal Jeffrey Williams quien fue el encargado de la investigación, declaró que desde abril de 2016 hasta octubre del 2017 el acusado Ryan S. Lin estuvo cometiendo crímenes de acoso cibernético. Ryan tenía diferentes víctimas que no estaban relacionadas, pero en este caso, además de la víctima principal, Jennifer Smith, también estuvieron involucrados sus familiares, amistades y compañeros de trabajo.

Todo comenzó cuando Ryan contestó una publicidad de cuarto vacante para solicitarlo. Para finales de abril y principios de mayo Ryan se mudó para el apartamento donde conoció a Smith. Aquí fue donde el acusado utilizó la laptop y entró a las cuentas de "Google" y "Apple" de Smith sin autorización para obtener información privada como fotos, videos y diarios. No concurrió mucho tiempo cuando el acusado comenzó a actuar extrañamente y ocasionó que la víctima se fuera del apartamento para el 30 de mayo del 2016. A varias semanas de Ryan haberse mudado, comenzó a enviarle a Smith mensajes de textos acosándola. Ryan le envió mensajes haciendo referencias al aborto de Smith, información personal que la víctima no compartía, pero lo tenía en su diario que estaba guardado en la laptop.

Luego de que Smith se fuera del apartamento, buscando alejarse de Ryan, comenzaron los acosos por mensajes de textos y correos electrónicos. Ryan les enviaba videos y fotos

sexuales a las amistades, compañeros de trabajo y familiares de Smith. Comenzó a acosar a todas las personas cercanas y relacionadas a Smith enviándoles fotos de pornografía infantil e inclusive fotos personales de sus cuentas en las redes con mensajes de contenido fuerte, amenazándolos con violación o asesinato. Comenzó a crear cuentas ficticias robando identidades para enviar amenazas de violaciones, asesinatos y bombas. Todo tipo de comunicación lo hacía mediante servicios anónimos de llamadas y mensajes que no permiten identificar el *IP address* o número de teléfono. De esta manera no podían rastrear quien enviaba los mensajes y amenazas.

Acusaciones, cargos y penalidades

Siete cargos por acoso cibernético 18 U.S. CODE § 2261A(2)(B)- Ryan Lin, mediante correos electrónicos, mensajes de textos, servicios de *Facebook*, *FetLife*, *CollarSpace*, *Backpage*, *Craiglist* y línea de emergencia policiaca, acosó e intimidó a las victimas causando angustia emocional desde mayo del 2016 hasta octubre del 2017. Se expone a las penalidades por este delito de:

1. Cadena perpetua si la victima resulta fallecida.
2. No más de 20 años si la victima resulta desfigurada permanentemente o lesión física que amenaza la vida
3. No más de 10 años si la victima resulta seriamente lesionada físicamente o si el perpetrador utiliza un arma seriamente peligrosa
4. No más de 5 años si la ofensa conduce al capítulo 109A.
5. No menos de 1 año si la persona acosa y viola cualquier orden de restricción o parecida.

Cinco cargos por distribución de pornografía infantil 18 U.S. CODE § 2252(a)(2)- Ryan Lin envió fotografías de pornografía infantil a sus víctimas y se expone a las penalidades de no menos de 5 años y no más de 20, pero si la persona ha sido convicto previamente no menos de 15 años y no más de 40 años. A continuación, las fechas en que envió dichas imágenes:

1. 16 de septiembre del 2016, por correo electrónico
2. 13 de julio del 2017, por mensajes de textos
3. 16 de septiembre del 2017, por correo electrónico

Nueve cargos por amenaza de bombas falsas 18 U.S. CODE § 844(e)- entre las fechas del 13 de julio 2017 al 2 de octubre del 2017 Ryan realizó las siguientes falsas amenazas de bombas por las cuales se expone a una penalidad de no más de 10 años de prisión:

4. Waltham Schools, el 13 de julio del 2017
5. Colonial Shopping Center, el 26 de julio del 2017
6. Waltham District Court, el 22 de septiembre del 2017
7. Waltham Government Center, el 15 de septiembre del 2017
8. Bentley University, el 15 de septiembre del 2017
9. Waltham Residential Address, el 30 de septiembre del 2017
10. Westin Hotel in Waltham, el 30 de septiembre del 2017
11. Holiday Inn Express, el 1 de octubre del 2017
12. Waltham Schools, el 2 de octubre del 2017

Tres cargos por fraude y abuso informático 18 U.S. CODE § 1030(a)(2)(C), (c)(2)(B)- sin autorización, Ryan obtuvo información entrando a la cuenta de la víctima de *Google* el 15 de

mayo del 2016, la cuenta de *Apple iCloud* el 28 de julio de 2016 y la cuenta de *Rover.com* durante el mes de julio del 2017. Se expone a una penalidad de no más de 5 años de prisión.

Un cargo por robo de identidad agravado 18 U.S. CODE $ 1028A- Ryan entró a las cuentas con los credenciales de otras personas, creó cuentas con nombres de otras personas y tenía conversaciones haciéndose pasar por la otra persona. Se expone a una penalidad de 2 años de prisión.

Definición de términos

Ciberacoso- amenazas, hostigamiento, humillación u otro tipo de molestias realizadas por un adulto contra otro adulto por medio de tecnologías temáticas de comunicación, es decir; internet, telefonía móvil, videoconsolas en línea, etc. (Stopbullying.gov 2018)

Programador de sistemas- controlan el funcionamiento interno de los ordenadores mediante programación. Traducen el idioma en un lenguaje que una computadora pueda leer. (IBM Knowledge Center 2018)

Sistemas de información- conjunto de mecanismos que su fin es la administración, recuperación, procesamiento fácil y rápido de datos y de información. (Zwass, V. 2011)

VPN (Virtual Private Network)- es una red privada virtual que las compañías utilizan para acceder a la red de forma remota. (Wells, J.T. 2013)

TOR (The Onion Router)- aplicación libre de costo utilizada para que no puedan supervisar las actividades realizadas en las redes. (What is Tor? 2018)

IP Address (Internal Protocol Address)- es un número identificador para cada equipo en el internet para poder comunicarse y saber la localidad del mismo. (Zwass, V. 2011)

ASD (Desorden del espectro autista)- serie de características con deficiencia en el comportamiento social e interacciones no verbales como el contacto visual, expresiones faciales, entre otros. (Park, et. Al 2016)

Software- instrucciones que dirigen a una computadora a realizar tareas, interactuar con el usuario, o procesar data. (Zwass, V. 2011)

Software de Seguridad- están diseñados para la protección de las computadoras de varias formas de acceso no autorizado y de softwares destructivos. (Zwass, V. 2011)

RAM- Random-Access Memory (por sus siglas en inglés), es donde se almacena la data para tareas a corto plazo que el procesador necesita. (Intel)

Sección 2: Revisión de literatura

Introducción

Según Mishra (2008), una encuesta de *Fortune 1000* encontró un aumento de 64% en ataques cibernéticos en el año. La unidad de terrorismo cibernético de la policía de Nueva York consideró el acoso cibernético como parte de la investigación. Este comportamiento ha sido reportado desde el siglo 19. El internet le ha provisto nuevas oportunidades a los usuarios para acosar, sin embargo, muchas personas no están conscientes de que muchas de las cualidades encontradas fuera del internet también se encuentran dentro del internet. Este problema de la invasión de privacidad y acoso en la tecnología ha incrementado. El ciberacoso es un problema global que ha ido creando incontables atacadores y víctimas. Usualmente, las víctimas de ciberacoso son usuarios nuevos en el internet o sin experiencia. Un 75% de las víctimas son mujeres y niños emocionalmente débiles pero varias veces los hombres también son acosados. El porcentaje proyectado es asumido ya que la mayoría de estos ataques no son reportados, ya sea por miedo de la víctima o porque no saben qué hacer.

Mishra nos identifica tres tipos de ciberacoso dependiendo la forma en que se utilice el internet. Los tres tipos de ciberacoso son:

1. **Acoso por correo electrónico**: Comunicación directa mediante correo electrónico. Es casi similar a la forma tradicional de acoso, se envían correos electrónicos con amenazas, contenido obsceno, o hasta con virus. Esta es la forma más sencilla de ciberacoso por la facilidad de anonimizar al que envía el correo electrónico, de esta manera los acosadores pueden esconder sus rastros con sencillez.

2. **Acoso en internet**: la comunicación por el internet es global y amplia. En comparación con el correo electrónico, el internet tiene más variedad y es más público. Dentro de la variedad de ciberacoso que el atacante puede realizar, el mismo puede postear mensajes amenazando con violar o matar a la víctima. Incluso pueden postear fotos íntimas con detalles personales.
3. **Acoso por computadora**: Este es el uso no autorizado de la computadora de la otra persona. Por ejemplo, el acosador utiliza el internet y el sistema operativo para asumir el control de la computadora de la víctima. De esta forma el atacante puede comunicarse directamente con la víctima tomando el control de su computadora y la única opción de la víctima es desconectar la computadora y abandonar la dirección IP actual.

No solo nos clasifica tres tipos de ciberacoso según la forma en que utilices el internet, sino que también nos clasifica los acosadores cibernéticos en tres tipos. Los tres tipos de acosadores identificados por Mishra son:

1. **El acosador común obsesionado**: Este tipo de acosador se declina a aceptar que la relación entre ellos ha terminado.
2. **El acosador delirante**: Este tipo de acosador padece de enfermedades mentales que los hace creer falsas ilusiones que los mantiene atados a la víctima. Asumen que la víctima los ama, aunque en ocasiones ni siquiera se conocen. Usualmente estos acosadores son personas solitarias y la mayoría de sus víctimas son celebridades, doctores, personas casadas, entre otros.

3. **El acosador vengativo**: este tipo de acosador está molesto con la víctima por razones mínimas ya sean reales o imaginativas. Se observa mucho en empleados disgustados y exparejas.

Fraudes Involucrados

Según Duggan (2017), en una encuesta reciente de aproximadamente 4,000 adultos en Estados Unidos se encuentra que el 41% han sido atacados por el acoso cibernético. Un 66% afirma que han sido testigos del acoso cibernético dirigido a otras personas. En algunos casos el acoso cibernético experimentado se limita a burlas o insultos que pueden ser ignorados y no afectan gravemente. Sin embargo, 1 de cada 5 (18%) han sido víctimas de acoso más severos como amenazas físicas, acoso constante por un largo periodo o acoso sexual. Otra de las encuestas muestra que más del 25% de los americanos deciden no subir contenido a las redes sociales luego de ser testigos del acoso a los demás. Luego de observar el acoso en los demás, un 28% ajusta las opciones de privacidad, un 27% deciden no subir algún contenido a sus redes, un 16% cambia alguna información de sus perfiles, un 13% deciden dejar de utilizar los servicios en línea y un 47% optó por uno o más de los escenarios anteriores.

Eke, Seto & William (2011) realizaron un estudio donde tomaron una muestra de 541 hombres registrados por la policía como ofensores de pornografía infantil y extendieron el periodo de seguimiento para observar el comportamiento. De la muestra el 34% tuvieron cargos por volver a cometer alguna ofensa, un 6% fueron cargados con contacto sexual contra niños y un 3% adicional fueron cargados con contacto sexual contra niños que no habían sido detectado antes. Para la muestra completa hubo un 32% de reincidencia, un 4% de los ofensores fueron

cargados con nueva ofensa de contacto sexual, un 2% adicional de los ofensores fueron cargados con ofensas de contacto sexual histórico y un 7% de los ofensores fueron cargados con nueva ofensa de pornografía infantil.

Andres (2014) nos informa que de una encuesta realizada entre 273 compañías, el 90% descubrió violaciones a la seguridad de sus sistemas. El 70% fueron violaciones serias como robo de información y equipos, fraude económico y ataques cibernéticos. El 74% tuvo pérdidas financieras de más de $265,589,940 y el promedio era de $120,240,180 en años anteriores. El 71% descubrieron que personas dentro de la empresa contaban con accesos no autorizados. La mayoría de los ataques se realizaron al sistema exterior, es decir al internet. El 79% abusa del acceso al internet ya sea viendo pornografía, pirateando o uso inapropiado. A su vez un 85% fueron contagiadas con virus.

Leyes aplicables

18 U.S. CODE § 2261A(2)(B) (Cyberstalking): Uso de correos electrónicos o/y cualquier equipo de electrónico como computadoras, con la intención de asesinar, lastimar, acosar o intimidar a una persona, causa, intenta causar o razonablemente espera causar estrés emocional a una persona, familiares cercanos de la persona o pareja íntima de la persona. El acusado se expone a las penalidades por este delito de:

4. Cadena perpetua si la victima resulta fallecida.
5. No más de 20 años si la victima resulta desfigurada permanentemente o lesión física que amenaza la vida

6. No más de 10 años si la victima resulta seriamente lesionada físicamente o si el perpetrador utiliza un arma seriamente peligrosa
7. No más de 5 años si la ofensa conduce al capítulo 109A.
8. No menos de 1 año si la persona acosa y viola cualquier orden de restricción o parecida.

18 U.S. CODE § 2252(a) (2) (Distribution of Child Pornography): Envío de contenido sexual de menores de edad mediante cualquier método incluyendo equipos electrónicos como computadoras. El acusado se expone a las penalidades de no menos de 5 años y no más de 20, pero si la persona ha sido convicto previamente no menos de 15 años y no más de 40 años.

18 U.S. CODE § 844(e) (Hoax Bomb Threats): Persona que mediante cualquier método de comunicación amenaza o maliciosamente brinda información falsa, a sabiendas, acerca de un atentado para lastimar, matar o intimidar a un individuo o destruir cualquier propiedad utilizando fuego o explosivos. El acusado se expone a la penalidad no más de 10 años de prisión.

18 U.S. CODE § 1030(a) (2) (C), (c) (2) (B) (Computer Fraud and Abuse): Acceder intencionalmente a una computadora protegida sin autorización y obtiene información privada. Por este delito el acusado se expone a la penalidad de no más de 5 años de prisión.

18 U.S. CODE $ 1028A (Aggravated Identity Theft): persona que conscientemente utiliza cualquier tipo de identificación de otra persona sin autorización mientras comete un delito. El acusado se expone a la penalidad de 2 años de prisión

18 U.S. CODE $ 982(a) (2), 1030(i) & 2253 (Forfeiture): La persona sentenciada debe entregar las propiedades mencionadas a los Estados Unidos.

Casos relacionados

USA v. Maliska, Case No. 1:18-cr-00162-TSC (Corte de Distrito de Columbia de USA);

Según el documento del Tribunal de Distrito de Columbia de USA v. Maliska *Indictment* (2018), Maliska fue sentenciado por delitos de robo de identidad y acoso cibernético. Maliska accedió sin autorización a la cuenta de Facebook de la víctima de donde consiguió las fotos personales. Utilizó las fotos para publicarlas en twitter y páginas pornográficas difamándola con mensajes, preferencias y experiencias sexuales. Publicó anuncios de la víctima como potencial escolta, lo que ocasionó que varias personas le escribieran a la víctima y llegaran a su trabajo solicitando sus servicios. La víctima eventualmente llenó una demanda civil contra Maliska, donde como parte del acuerdo de esa demanda civil el acusado admitió haber cometido las acusaciones de haber publicado declaraciones difamatorias de la víctima anónimamente en el internet, haber entrado sin permiso a las cuentas personales de *Facebook* y obtenido las fotos personales, haber alterado las fotos de la víctima para que sea vean en poses sexuales, publicó varias fotos en páginas en el internet, compartió información de la víctima en páginas pornográficas y dejó la información de contacto para que cualquier persona pudiera contactarla, que era responsable de muchas publicaciones sobre la víctima donde usó fotos robadas, y envió declaraciones falsas de contenido sexual a los padres de la víctima. Parte del acuerdo era que Maliska borraría todo contenido que fue creado y que tenga en sus equipos electrónicos acerca de la víctima y que no podrá publicar nada en ninguna parte refiriéndose a la víctima. Sin embargo, Maliska continuó con el acoso violando el acuerdo y las órdenes del juez.

Herramientas de investigación

Según Nelson, Phillips y Steuart, (2016), cuando se va a realizar una investigación forense debes mantener un comportamiento profesional en todo momento. Se debe trabajar con objetividad y confidencialidad durante la investigación, expandir tu conocimiento constantemente y mantenerte íntegro. Tu opinión debe ser basada en tu educación, entrenamiento, experiencia y la evidencia en tu trabajo. Debes evitar llegar a conclusiones sin antes analizar todos los posibles factores considerados. Evitar el prejuicio para mantener la integridad de tus hallazgos en todas las investigaciones. Tu responsabilidad es encontrar toda evidencia digital relevante al caso. Tu rol como profesional de forense digital es recolectar data del equipo del sospechoso y determinar si se encontró evidencia que señale que un crimen fue cometido o las políticas de una compañía o industria fueron violadas. Si la evidencia sugiere que un crimen fue cometido, se procede a crear un caso y recolectar toda la evidencia que puedas ofrecer a la corte. Todo este proceso debe ser realizado según las reglas y procedimientos establecidos para que la evidencia no se considere alterada o dañada.

Según Karbhari & Mane (2015), las herramientas de investigación han ayudado a que el proceso de investigación forense sea más efectivo y eficiente. Encontrar evidencia tomaba mucho tiempo, este proceso se ha facilitado gracias a las herramientas que día a día sus características mejoran. Al igual que las herramientas mejoran también lo hace el crimen. *WinHex* es una herramienta poderosa para análisis, recuperación y manipulación de data creada por *X-Ways Software Technology AG* en Alemania. Esta herramienta es útil para el campo de forense digital, procesamiento de data, recuperación de data y seguridad de tecnología de

información. Tiene la capacidad de editar cualquier archivo, recuperar data perdida o eliminada de equipos digitales. Adicional puede editar el RAM, disco e interpretación de data.

Según Jain & Kalbande (2014), la herramienta *Encase* para forense digital se utiliza para adquirir, analizar, clasificar, recuperar y reconstruir eventos pasados y crear reportes digitales de los hallazgos encontrados durante el proceso de la investigación forense. *Encase* es aceptada y reconocida por la corte de justicia y el mundo de forense digital. *Accesdata* creó una herramienta llamada FTK *Forensic Toolkit*. Esta herramienta se utiliza para adquirir, analizar y crear réplicas de la data que se esté investigando. Dentro del paquete de FTK se incluyen herramientas para recuperación de archivos borrados, analizar data de los emails, búsqueda y descifrar contraseñas.

Sección 3: Simulación

El esquema utilizado por Lin para acosar a sus víctimas era mediante servicios extranjeros que proveen números de teléfonos temporeros para enviar mensajes de textos, servicios extranjeros que proveen emails encriptados para enviar los correos electrónicos y creación de cuentas con nombres falsos y correos electrónicos creados únicamente para ese propósito. A continuación, se muestra un diagrama de como Lin realizaba sus actividades:

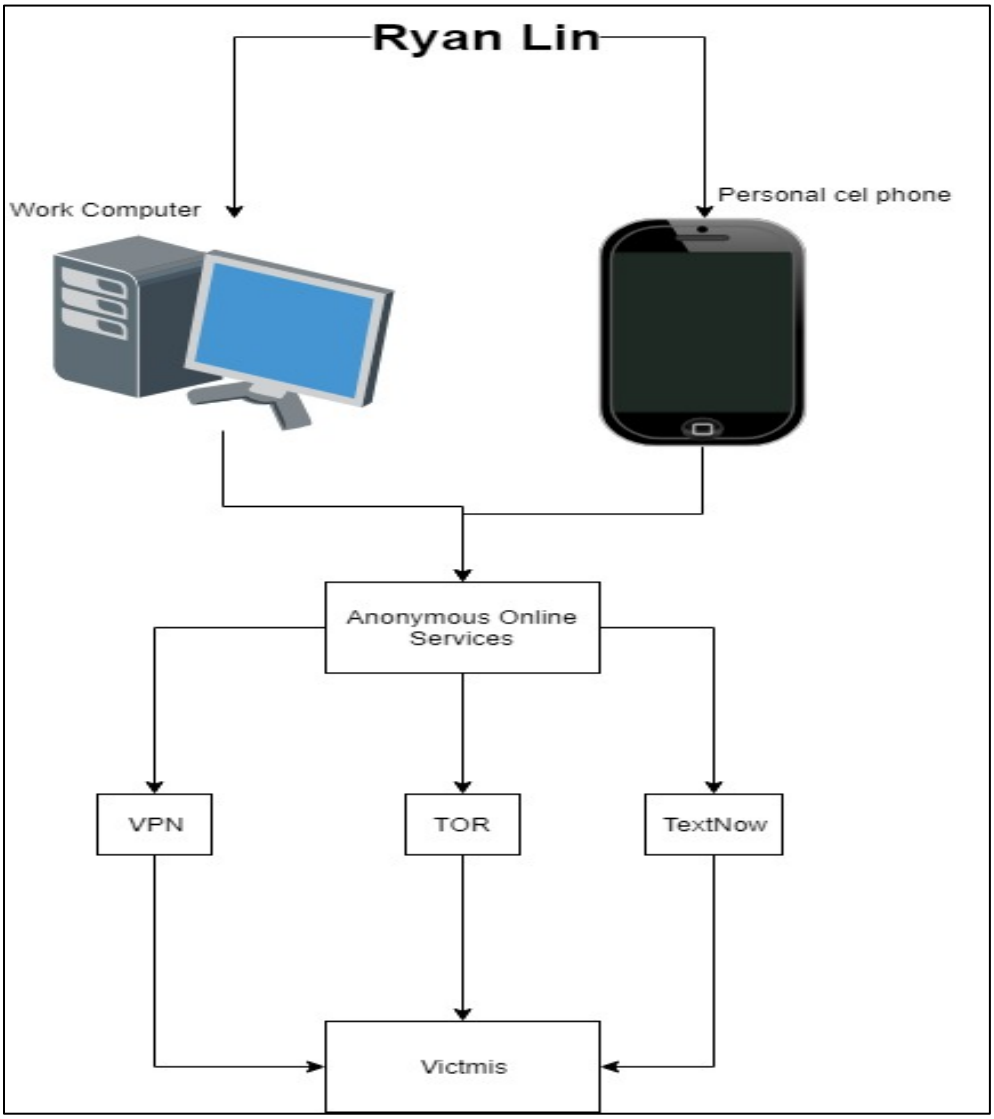

Figura 1: Diagrama de como Lin acosaba a sus víctimas.

Sección 4: Informe del caso

Resumen Ejecutivo

La asistente del Fiscal Federal, Amy Harman Burkart, solicitó el servicio de la compañía DFI (Digital Forensics Investigations) para analizar un Flash Drive que contiene una copia exacta del disco duro de la evidencia recogida en el caso de Ryan Lin v. United States of America. El equipo incautado por el agente Jeffrey Williams fue una DESKTOP COMPUTER BLACK S/N 1627FD34500500402, la cual era de la compañía donde trabajó Lin mientras cometía los delitos. Esta investigación solicitada por la corte del Distrito de Massachusetts es para recuperar posible evidencia en el proceso judicial del caso vinculado a fraude y acoso cibernético.

Objetivo

El análisis del *Flash Drive* fue delegado a la compañía DFI, quienes son expertos en el análisis forense de dispositivos electrónicos con especialización en recuperación de datos. Decisión bien tomada ya que Lin logro borrar la mayoría de la data relacionada al caso. DFI está a cargo de recuperar toda la evidencia posible para demostrar la culpabilidad del acusado en el caso cuyo número es 1:18-cr-10092, Ryan S. Lin v. USA.

Alcance de trabajo

El día 2 de junio de 2018 Amy Harman Burkart, entregó a la compañía DFI el dispositivo *IronKey Basic* S1000 64GB *Encrypted Flash Drive*, cuyo número de evidencia es el 2017-RSL-1, para la investigación y recuperación de datos borrados por la compañía donde Lin trabajaba

luego de ser terminado del puesto. El propósito es recuperar la data borrada y guardar una imagen íntegra para poder utilizarla como evidencia contra el acusado.

Las herramientas que utiliza la compañía *DFI* son importantes ya que son de confianza y aceptadas por el Gobierno Federal, estas herramientas son las de *Forensic Toolkit Access Data*. Con esta herramienta la compañía *DFI* podrá analizar, estudiar, recuperar y guardar la data investigada íntegramente para ayudar en la toma de decisiones en el caso de Ryan Lin v USA. La investigación está pautada para el día 13 de marzo del 2018, antes de la vista final. Los resultados de la investigación se estarán entregando en un informe de hallazgos donde se detallará la evidencia encontrada en el *USB Drive* entregado por el Gobierno Federal.

Datos del caso

Número de Caso: 1:18-cr-10092

Caso: Unites States of America v. Ryan S. Lin

Asunto: Acoso cibernético, robo de identidad agravado, amenaza de bombas, distribución de pornografía infantil, fraude y abuso de computadoras.

Acusado: Ryan S. Lin

Examinador: Christopher L. Rodríguez

Cliente: Departamento de Justicia de los Estados Unidos, Distrito de Massachusetts.

Representante: Amy Harman Burkart, Asistente del Fiscal Federal

Descripción de los dispositivos utilizados

A continuación, los equipos utilizados por la compañía *DFI* para la investigación:

Laptop marca Lenovo, procesador Intel(R) Core(TM) i3-5020U CPU @ 2.20GHZ 2.20GHz. Cuenta con una memoria interna de 8.00 GB (RAM) y un sistema operativo de 64-bit. Esta máquina tiene instadala las herramientas utilizadas para la investigación. Imagen de la pantalla principal de la maquina a utilizarse. (Véase figura 2 y 3).

Figura 2: Pantalla principal de la maquina utilizada.

Una imágen de las especificaciones del sistema operativo.

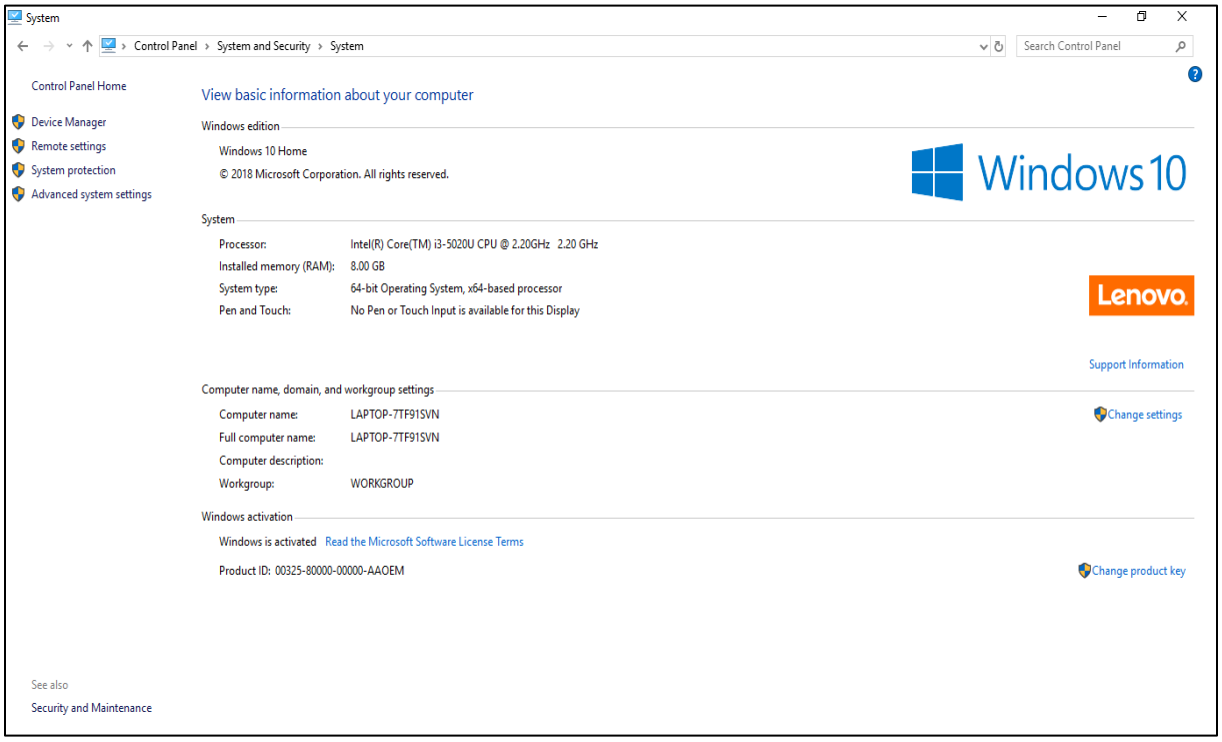

Figura 3: Imagen del sistema operativo Lenovo.

IronKey Basic S1000 64GB Encrypted Flash Drive, imagen del dispositivo a continuación.

(Véase figura 4)

Figura 4: Flash drive entregado por el Gobierno Federal para investigación.

Resumen de Hallazgos

Luego de culminar el procedimiento de investigación del Flash Drive entregado a *DFI* por parte del Gobierno Federal, se encontró una serie de hallazgos significativos para el caso USA v. Ryan S. Lin. Se logró recuperar evidencia que señalaba que el acusado tenía guardada unas imágenes acosando a varias de sus víctimas. A continuación, imágenes de contenido en las imágenes encontradas en el *Flash Drive.* (Véase figuras de la 5 a la 11).

Email que aparenta ser de Smith, pero en realidad fue Lin quien lo envió a Matthew (compañero de cuarto de Smith).

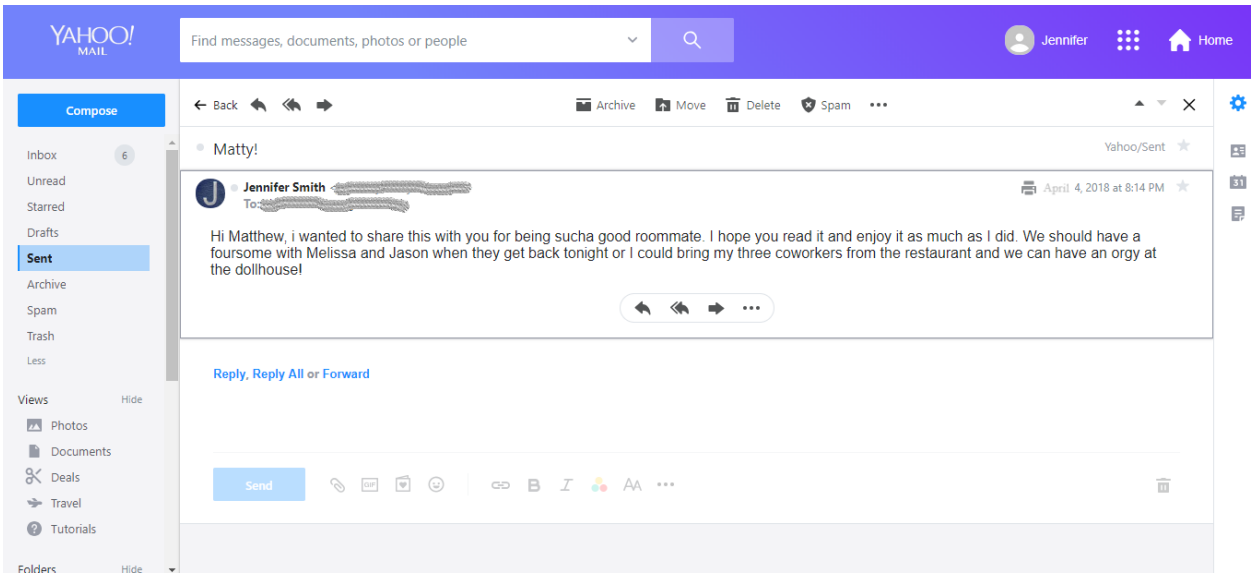

Figura 5: Email enviado por Lin.

Email que Lin envió al padre de Smith y a los compañeros de trabajo incluyendo la imagen del “collage” que Lin creo con fotos de Jennifer Smith.

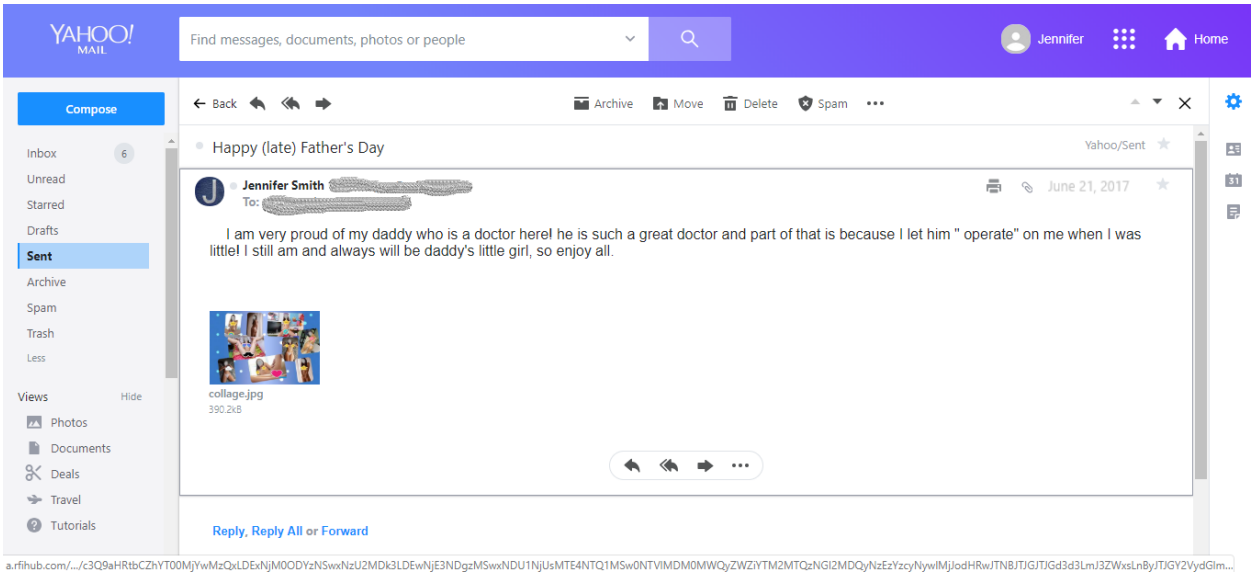

Figura 6: Email con imagen del “collage”.

Imagen del “collage” que Lin creo con las fotos de Smith y que compartió con muchas personas.

Figura 7: Collage.

Mensajes que Lin le envió a Smith anónimamente acosándola.

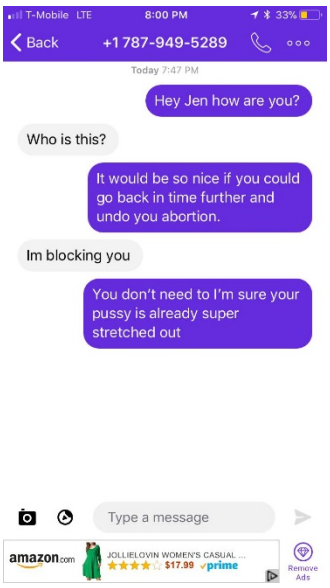

Figura 8: Mensajes desde número anónimo.

Mensajes anónimos que recibió Smith luego de compartir su número nuevo con "Ashley" quien era Lin realmente.

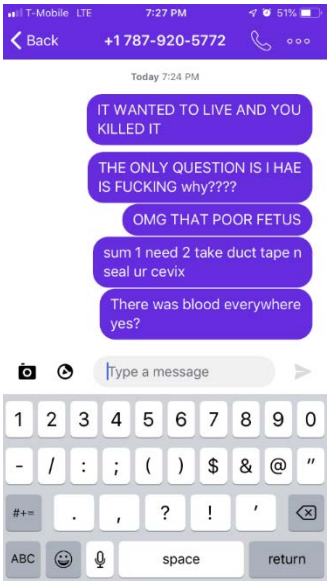

Figura 9: Mensajes anónimos enviados por Lin.

Mensaje anónimo que recibió jefa de Smith del restaurante donde trabajaba.

Figura 10: Mensaje anónimo enviado a la jefa de Smith.

Mensaje anónimo que recibió una amiga de Smith quien vivía en New Jersey.

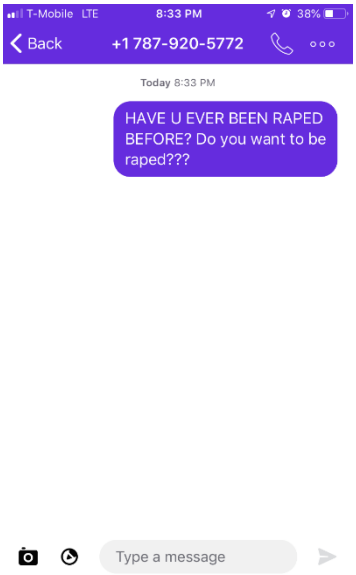

Figura 11: Mensaje que recibió amiga de Smith.

Cadena de Custodia

Primer evento:

- Descripción del evento: Entrega de Flash Drive por la asistente del fiscal Federal Amy Harman Burkart a Christopher Rodríguez, Examinador Forense de DFI. La evidencia se basa de un IronKey Basic S1000 64GB Encrypted Flash Drive cuyo número de evidencia es 2017-RSL-1
- Evento verificado por: Asistente del Fiscal Federal Amy Harman Burkart y el investigador forense Christopher Rodríguez
- Numero de evidencia: 2017-RSL-1
- Fecha de comienzo: 2 de junio del 2018 a las 10:00 a.m.
- Fecha de terminación: 2 de julio del 2018 a las 10:30 a.m.
- Lugar de Origen: USAO-DMASS (United States Attorney's Office for the District of Massachusetts)
- Destino: DFI Forensic Laboratory

Segundo evento:

- Descripción del evento: Creación de caso
- Evento verificado por: Christopher Rodríguez
- Numero de caso asignado: USARL2018
- Fecha de comienzo: 2 de julio del 2018 a las 10:40 a.m.
- Fecha de terminación: 2 de julio del 2018 a las 10:45 a.m.
- Lugar de Origen: DFI Forensic Laboratory
- Destino: DFI Forensic Laboratory

Tercer evento:

- Descripción del evento: Creación de réplica y análisis de la evidencia.
- Evento verificado por: Christopher Rodríguez (examinador forense)
- Numero de caso: USARL2018
- Fecha de comienzo: 2 de julio del 2018 a las 10:50 a.m.
- Fecha de terminación: 3 de julio del 2018 a las 1:00 p.m.
- Lugar de Origen: DFI Forensic Laboratory
- Destino: DFI Forensic Laboratory

Cuarto evento:

- Descripción del evento: Se le entrega análisis forense de la evidencia a la asistente Fiscal Federal Amy Harman Burkart. El examinador forense Christopher Rodríguez hizo entrega del reporte personalmente.
- Evento verificado por: Christopher Rodríguez y Amy Harman Burkart.
- Numero de caso: USARL2018
- Fecha de comienzo: 3 de julio del 2018 a las 1:45 p.m.
- Fecha de terminación: 3 de julio del 2018 a las 2:17 p.m.
- Lugar de Origen: DFI Forensic Laboratory
- Destino: USAO-DMASS

Quinto evento:

- Descripción del evento: Se le devuelve el *Flash Drive* a la asistente del Fiscal Federal Amy Harman Burkart. Esta fue entregada personalmente por el examinador forense Christopher Rodríguez.
- Evento verificado por: Christopher Rodríguez y Amy Harman Burkart.
- Numero de evidencia: USARL2018

- Fecha de comienzo: 3 de julio del 2018 a las 3:00 p.m.
- Fecha de terminación: 3 de julio del 2018 a las 3:34 p.m.
- Lugar de Origen: DFI Forensic Laboratory
- Destino: USAO-DMASS

Procedimiento

Para que la data recuperada y analizada se mantenga íntegra y pueda ser utilizada para el caso correctamente se realizan unos procedimientos rigurosos. La herramienta utilizada para esta investigación es prestigiosa y reconocida por entidades federales, por esta razón con las imágenes del procedimiento realizado que mostraremos a continuación se confirma que la misma es íntegra.

Para el análisis de la evidencia 2017-RSL-1, se utilizó la herramienta de *AccessData FTK Image* para crear una imagen idéntica a la evidencia entregada y analizarla. A continuación, procedimiento realizado para el análisis de la evidencia. (Véase figuras de 12 a la 35).

Al inicio de la aplicación seleccionas “Create Disk Image…"

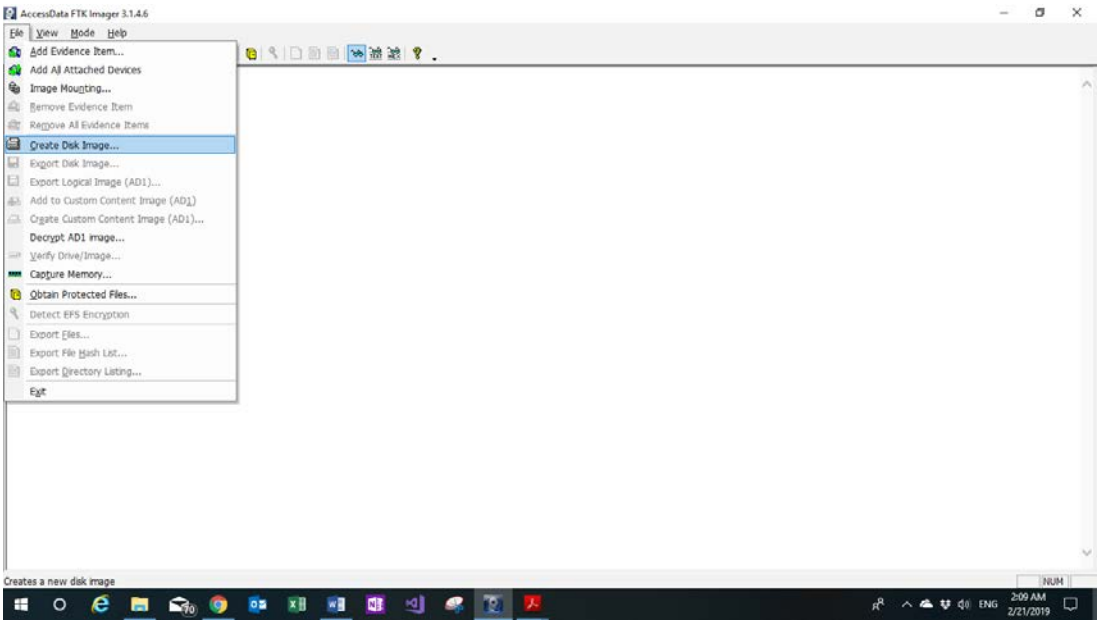

Figura 12: Comienzo del procedimiento creando imagen idéntica.

Luego selecciona la fuente de la evidencia.

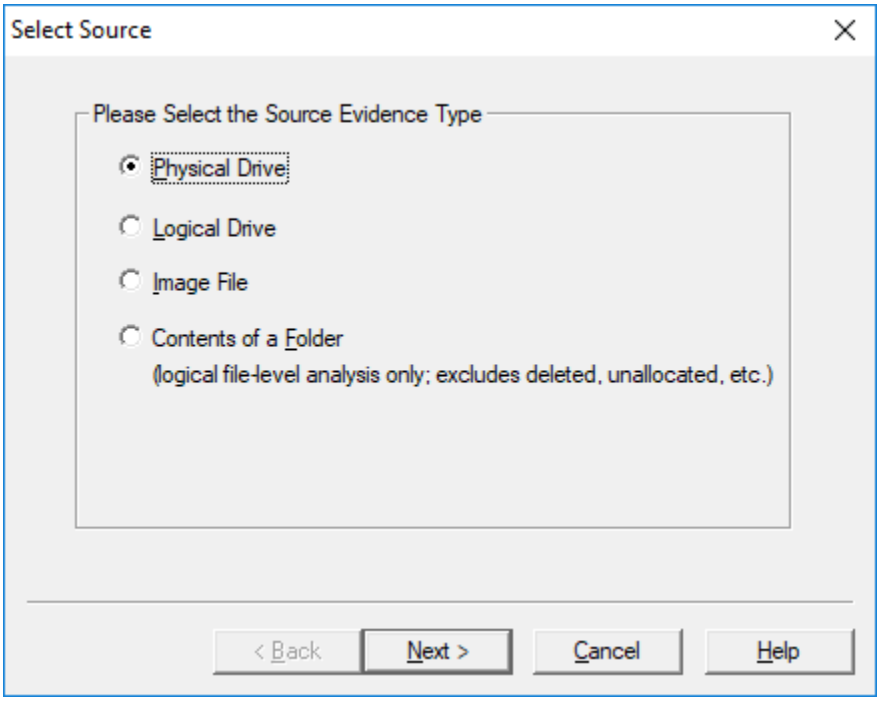

Figura 13: Tipo de fuente de la evidencia

Se procede a escoger el dispositivo a utilizarse por el examinador para crear la imagen para realizar la investigación.

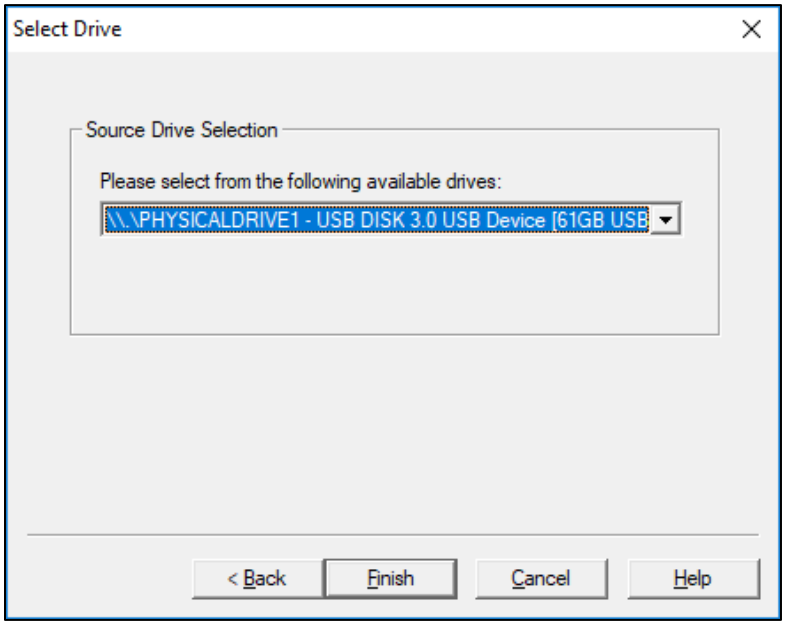

Figura 14: Se escoge el dispositivo indicado.

Luego se escoge la opción de “add” para añadir el destino de la imagen a crearse.

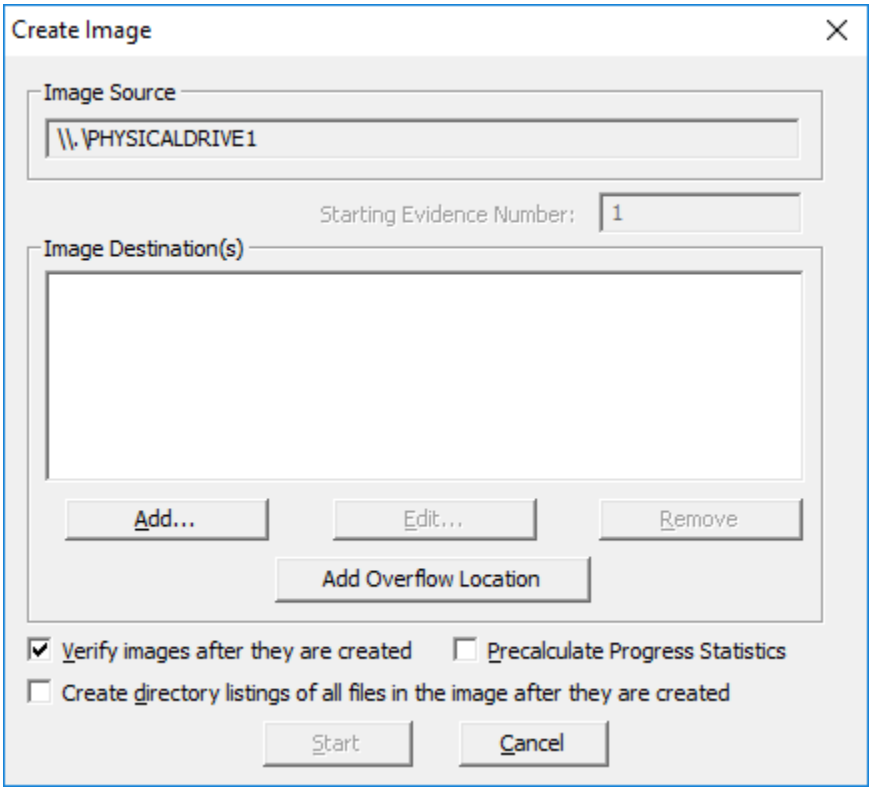

Figura 15: Opción para añadir el destino de donde desea crear la imagen

Cuando aparece esta opción escogemos el destino favorable, en mi caso será el Raw (dd).

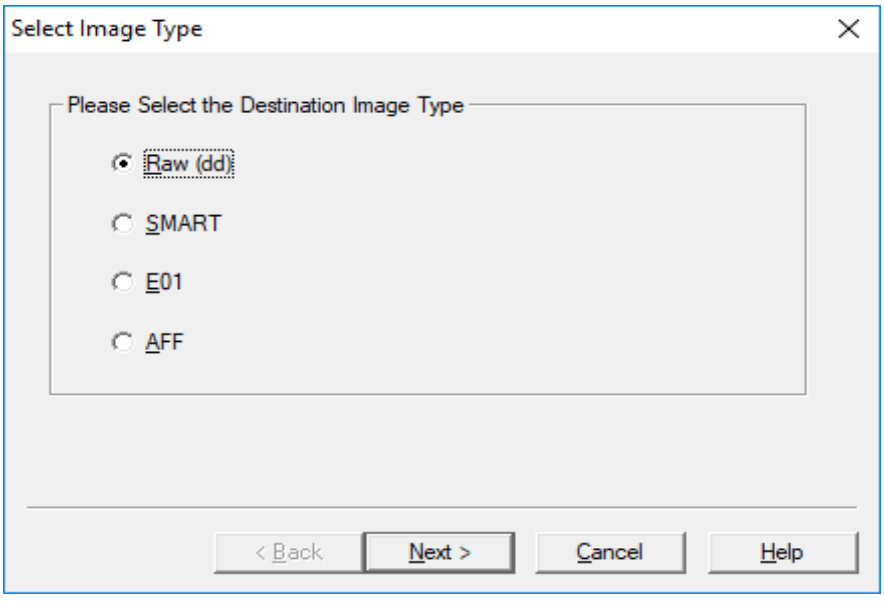

Figura 16: Opción escogida por el examinador del tipo del destino.

Al escoger el destino nos brinda la próxima pantalla para poblar con la información que quieras identificar el caso.

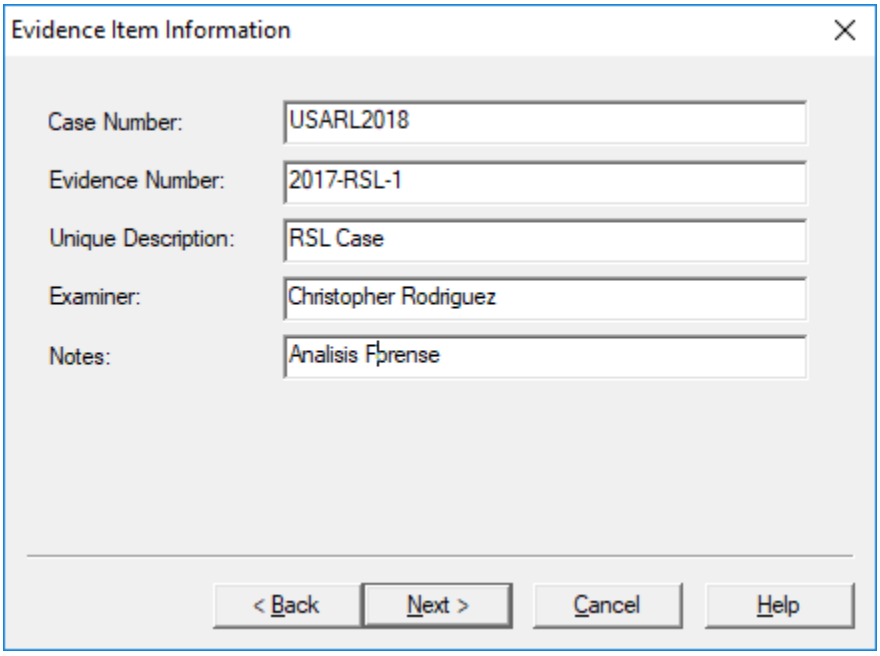

Figura 17: Se brinda información para documentación personal del examinador.

Luego debes escoger el destino donde quieres guardar la imagen a crearse, en adición le asignas el nombre al archivo de la imagen.

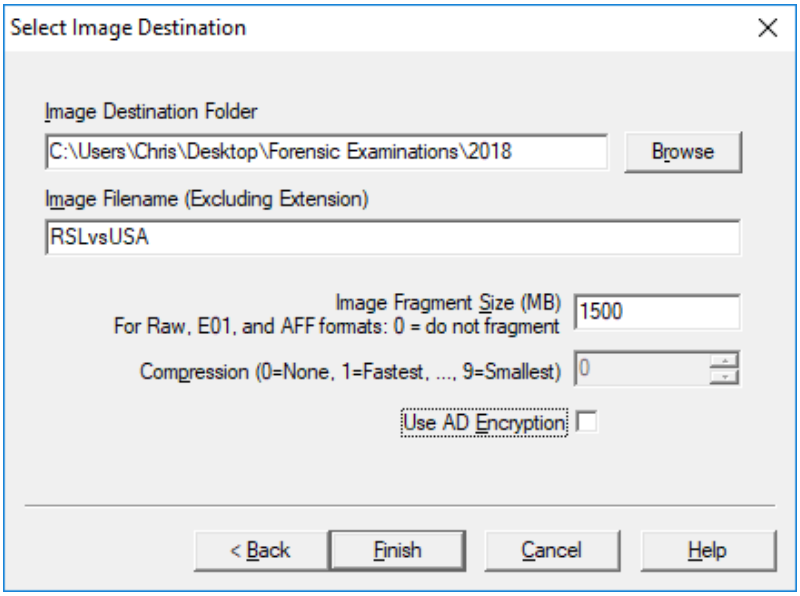

Figura 18: Se escoge destino y nombre del archivo.

Una vez presionas “Finish” comienza a crear la imagen, dejándote saber la fuente, destino y el estado del proceso.

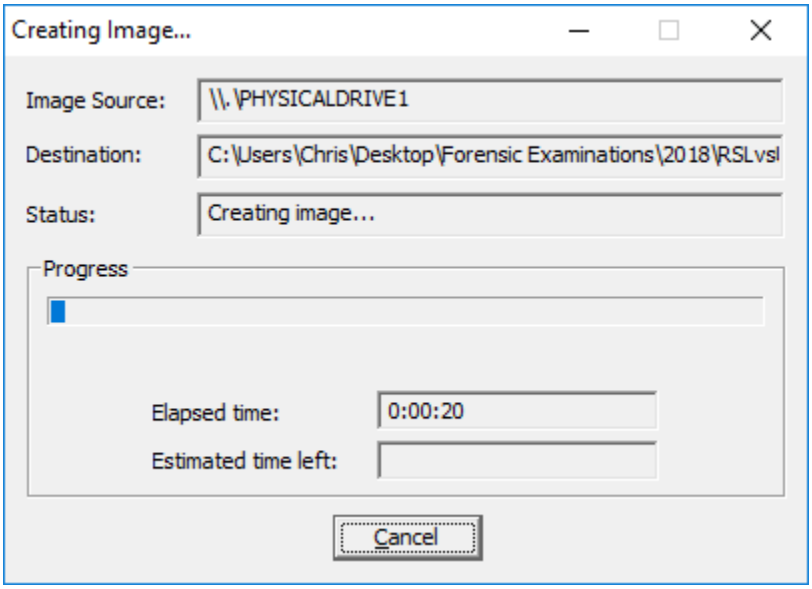

Figura 19: Comienza proceso de creación de imagen.

Una vez creado, procede a verificar que la imagen ha sido creada correctamente y te brinda el nombre del documento de la imagen según asignada.

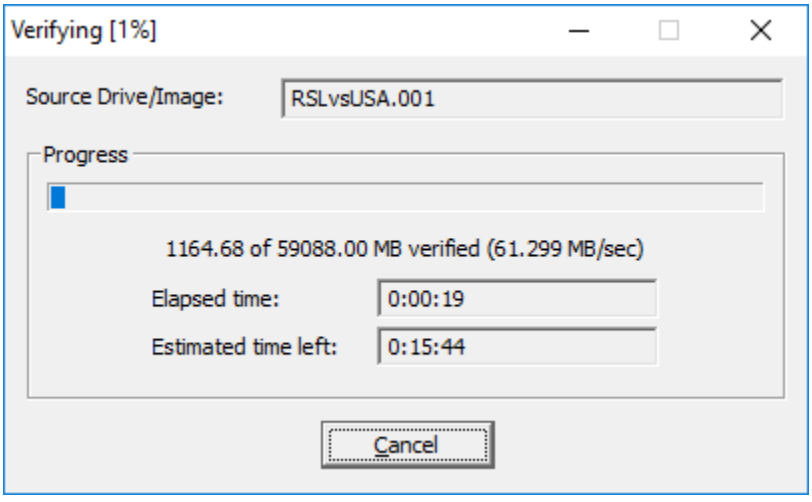

Figura 20: Verificación de la creación de la imagen.

Resultados luego de finalizar la creación de la imagen.

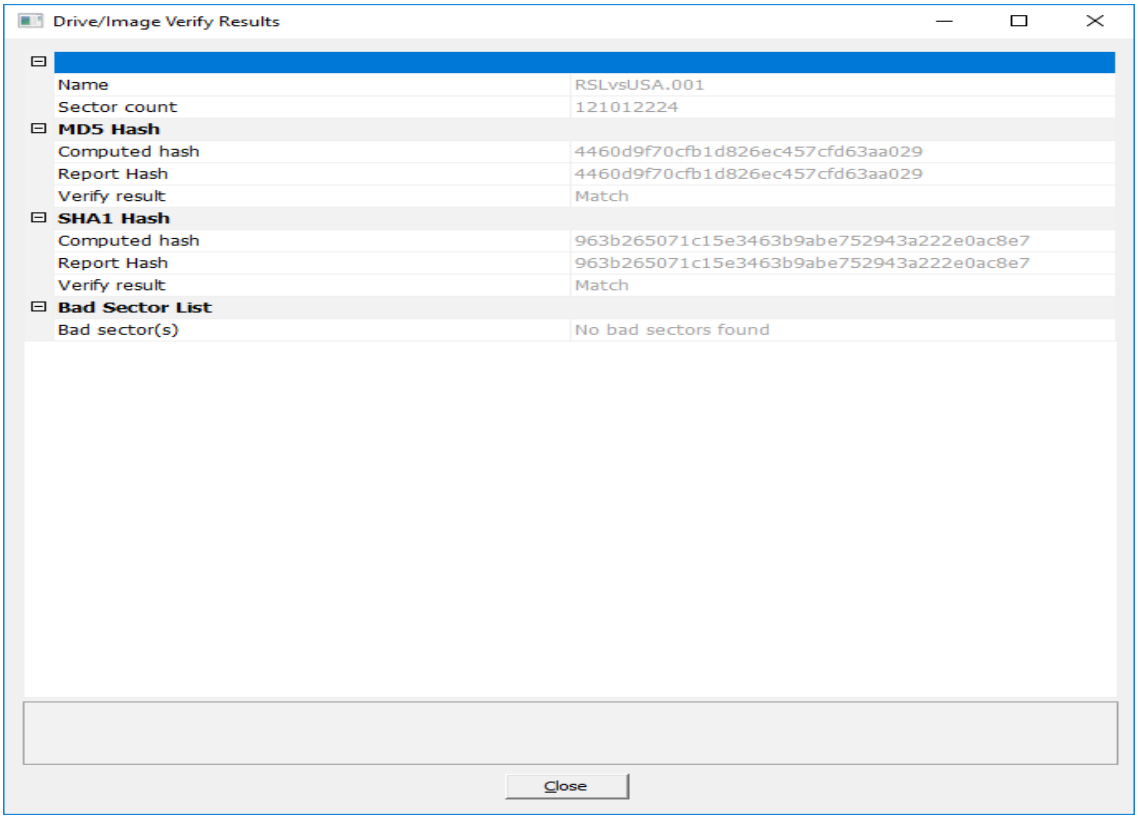

Figura 21: Resumen de los resultados de la creación de la imagen.

Documentos de la creación de la imagen en el destino asignado.

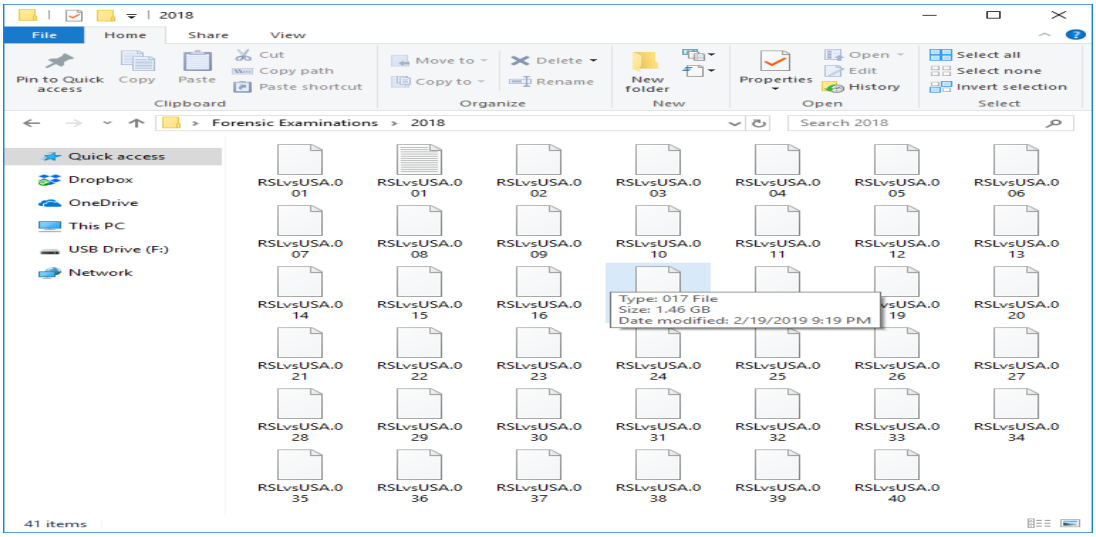

Figura 22: Documentos obtenidos luego de la creación de la imagen en el destino asignado.

Evidencia de la imagen creada y los detalles del documento.

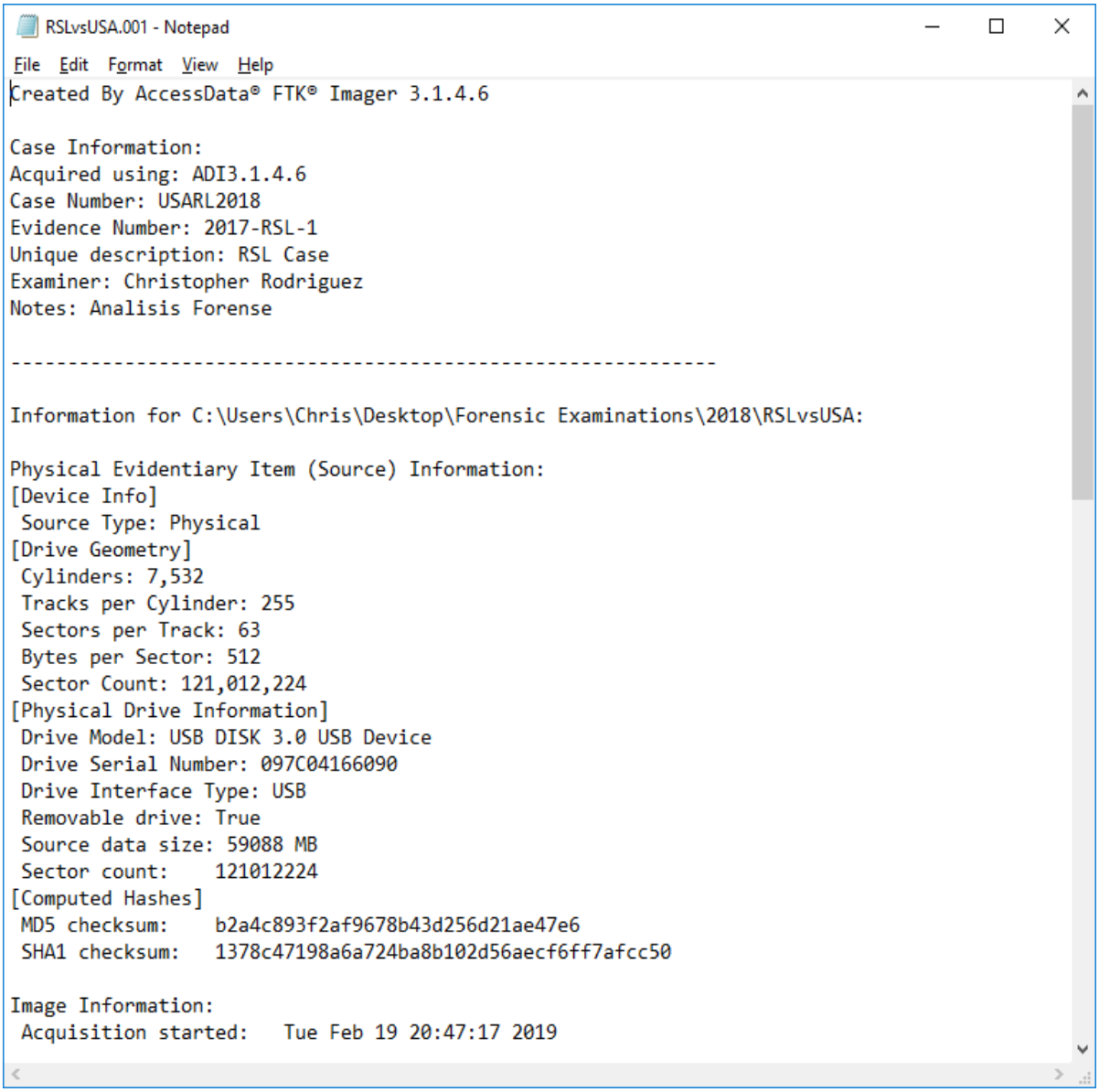

Figura 23: Información y detalles de la creación de la imagen.

Al finalizar la creación de la imagen, vamos a la opción de “Add Evidence Item…” para buscar el archivo creado de la imagen.

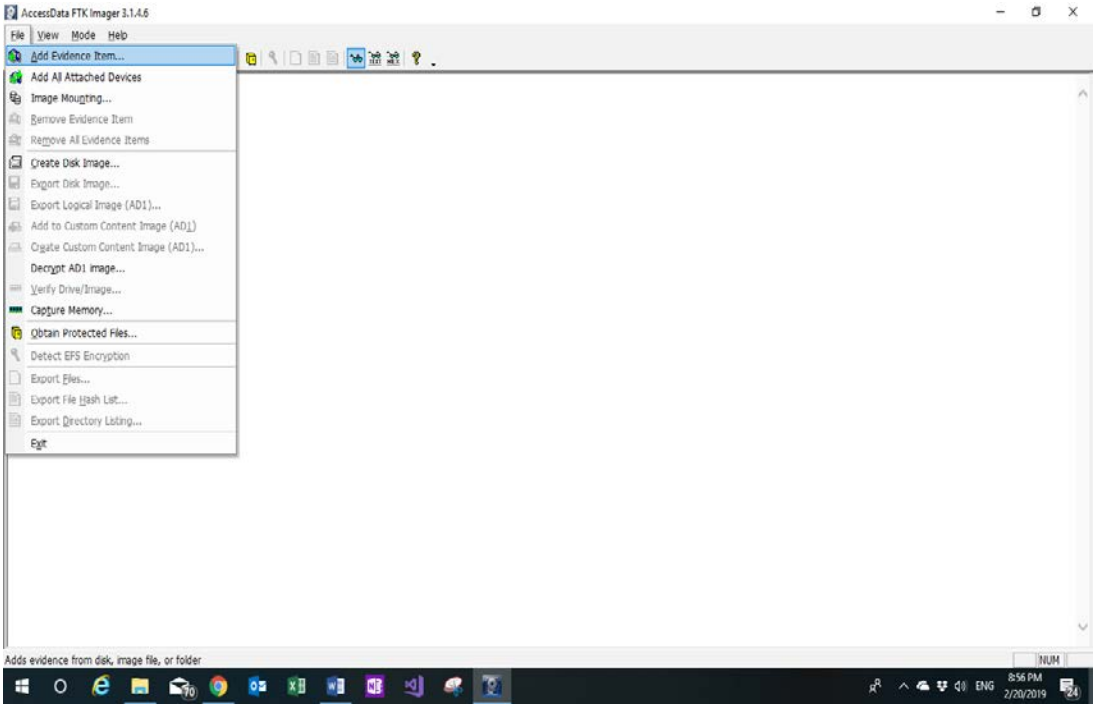

Figura 24: Se añade la evidencia para analizarla.

Se escoge la fuente del archivo a investigar.

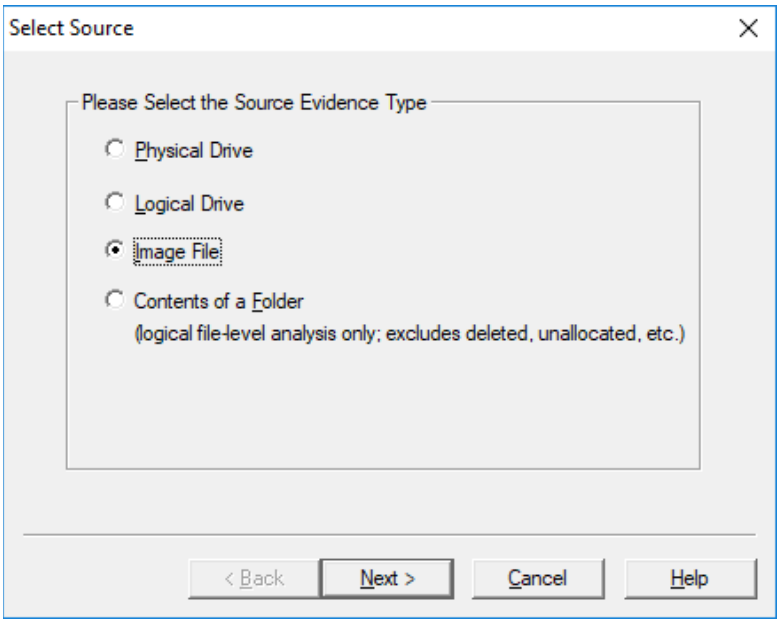

Figura 25: Selección de tipo de fuente.

Buscamos los documentos en el archivo creado para el destino de la creación de la imagen.

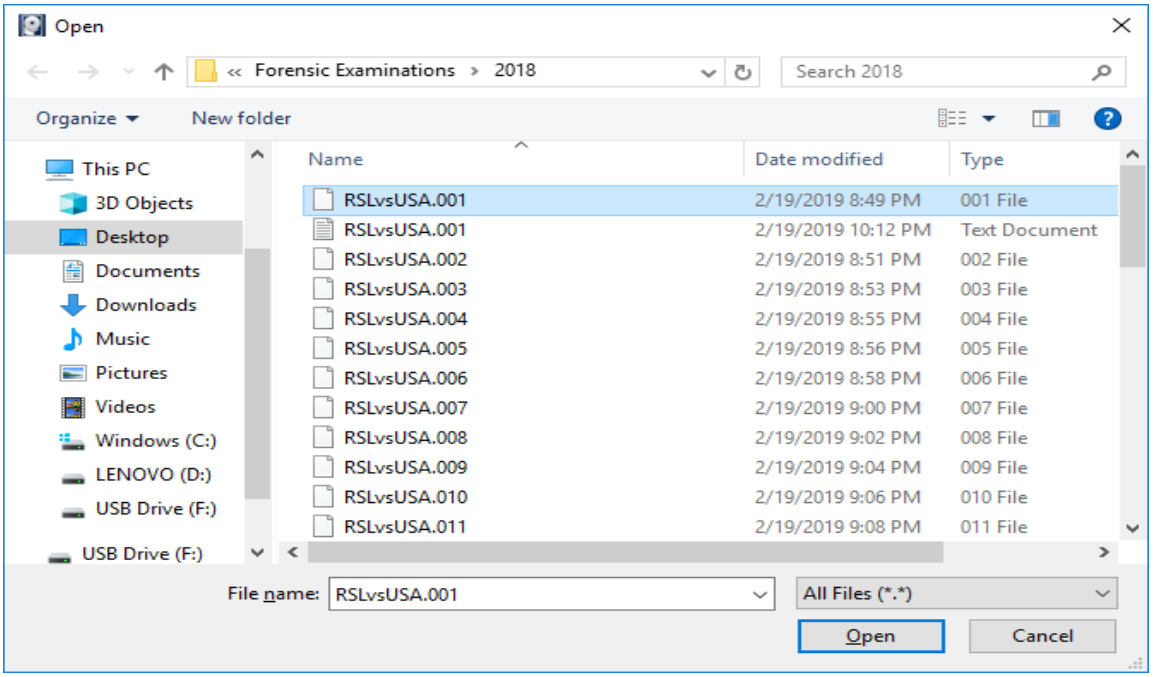

Figura 26: Selección de documento a investigar.

Luego de traer el archivo, encontramos todos los archivos y documentos dentro del mismo. La siguiente imagen muestra el “path” de las imágenes encontradas, podemos ver que se encontró bajo “Forensics”, “root”, “Game Codes”, “View Codes”, “Entertainment”, “You know who” y finalmente llegamos a “Messages”. Todas estas imágenes fueron eliminadas por Lin antes de que fuera arrestado. Este detalle adviene a conocimiento porque las imágenes se muestran con un “X” en el ícono de la imagen dejándonos saber que esas imágenes fueron borradas. La primera imagen es un correo electrónico que Lin envió, haciendo pasar por Smith, al compañero de apartamento Matthew.

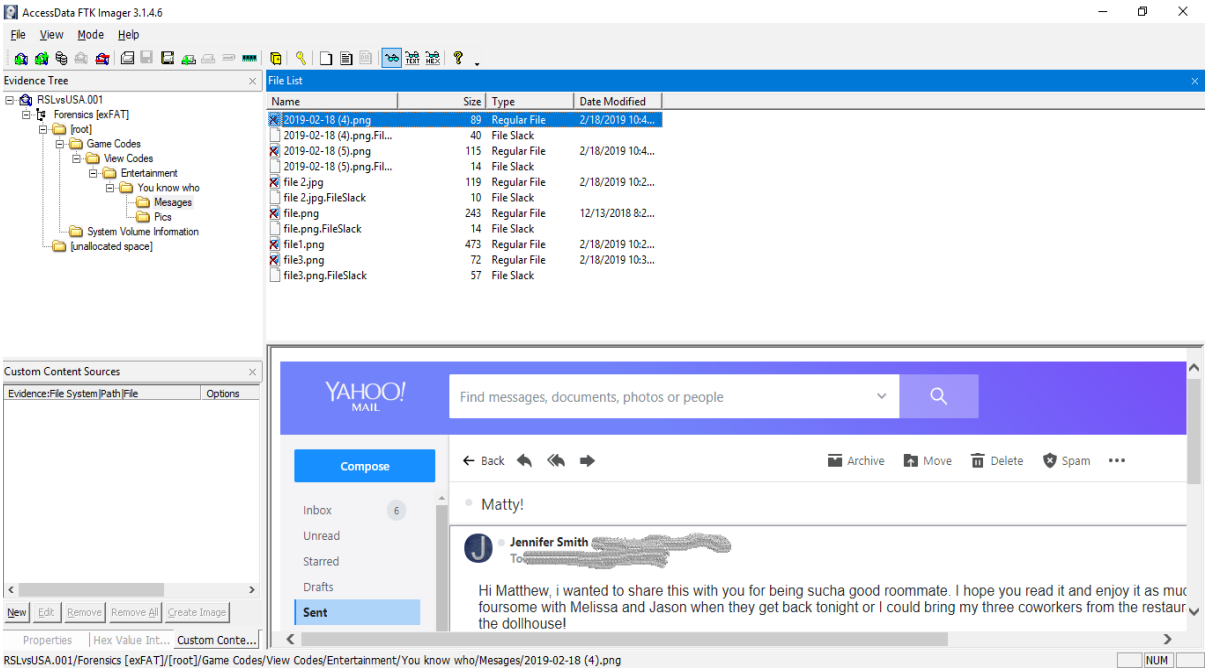

Figura 27: Imagen del correo envido por Lin a Matthew.

Correo electrónico que Lin envió al padre de Smith y sus compañeros de trabajo incluyendo un “collage” de fotografías de Smith desnudas.

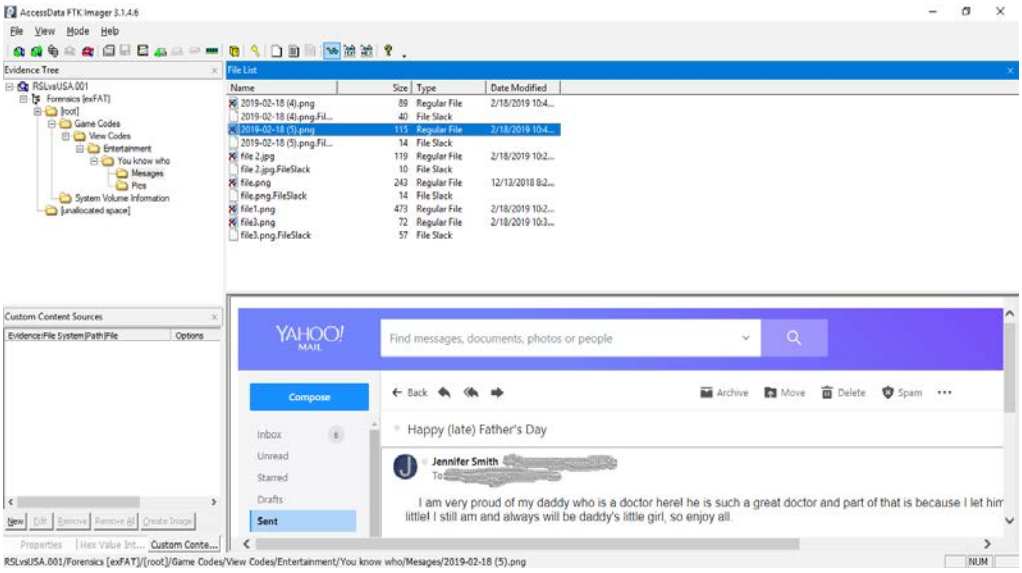

Figura 28: Imagen del email enviado al padre de Smith y sus compañeros con el “collage”.

Imagen recuperada del mensaje de texto enviado por Lin a Smith desde un número anónimo brindado por la aplicación de *Textnow*.

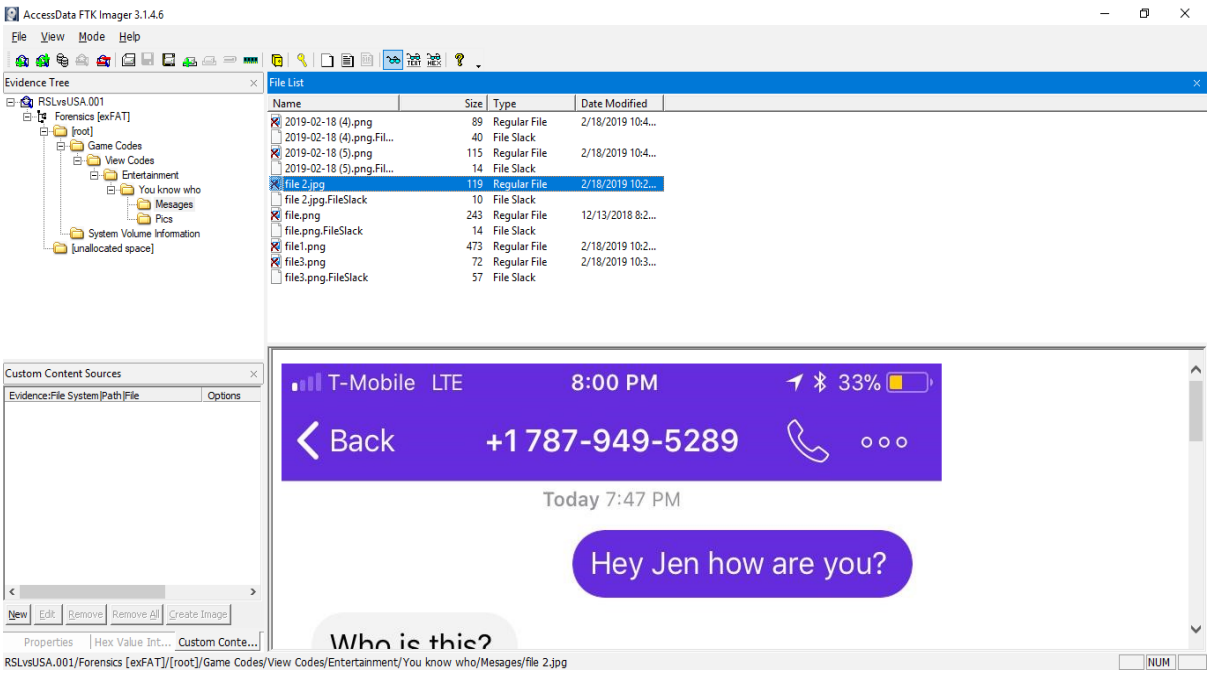

Figura 29: Imagen de mensaje enviado a Jennifer.

Imagen del mensaje que Lin le envió a Smith anónimamente, misma aplicación que después de pasar el tiempo te asigna un número nuevo.

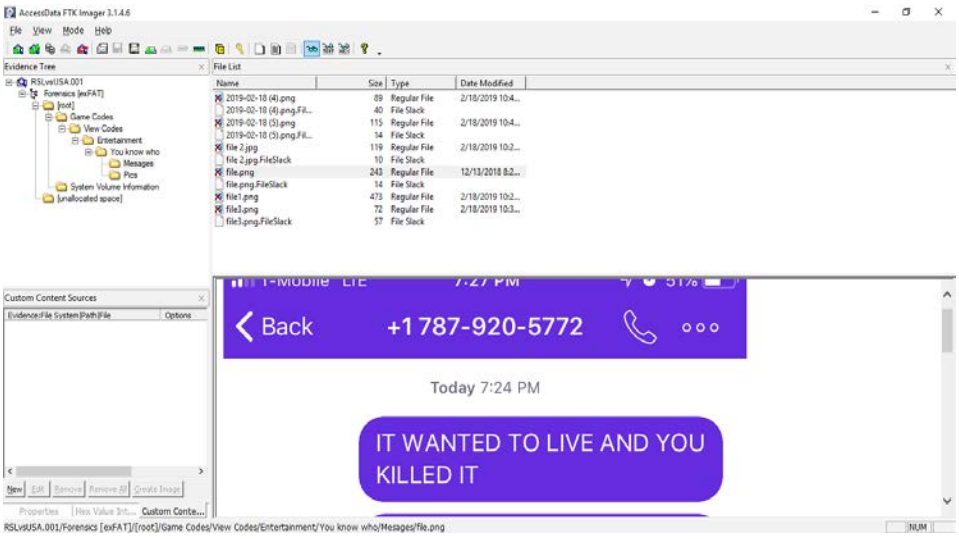

Figura 30: Imagen de mensaje enviado a Jennifer.

Imagen recuperada del mensaje enviado a la jefa de Smith en el trabajo antiguo.

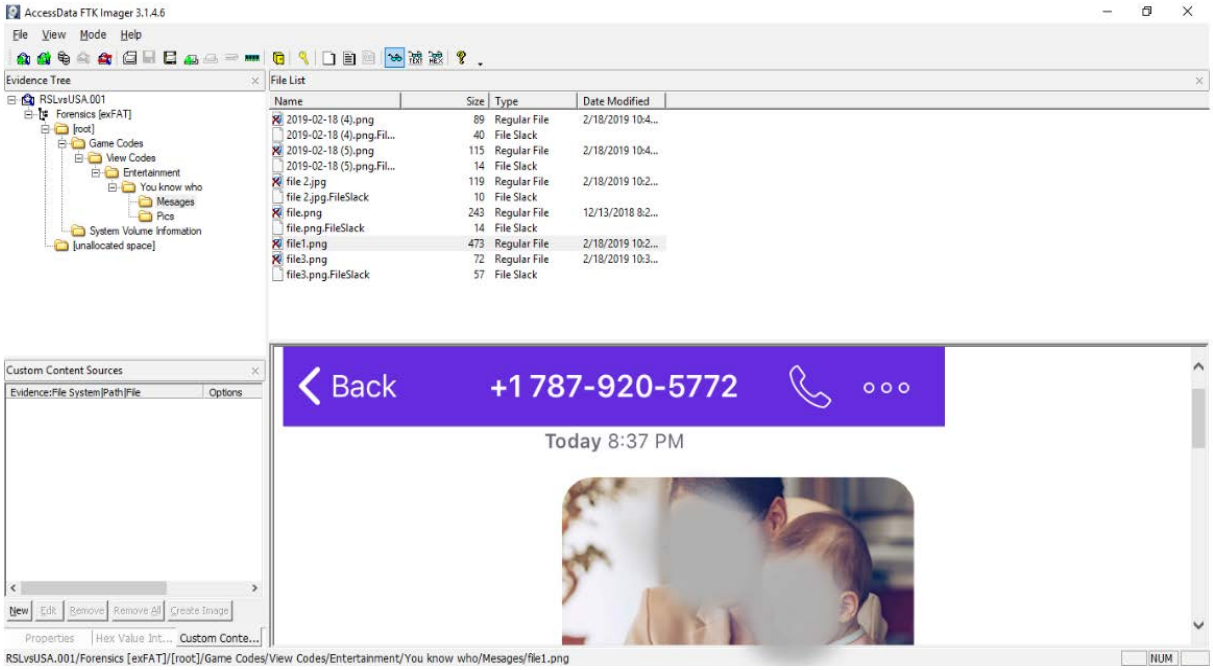

Figura 31: Imagen de mensaje enviado a la ex jefa de Jennifer.

Imagen recuperada del mensaje enviado a la amiga de Smith que vivía en New Jersey para ese tiempo.

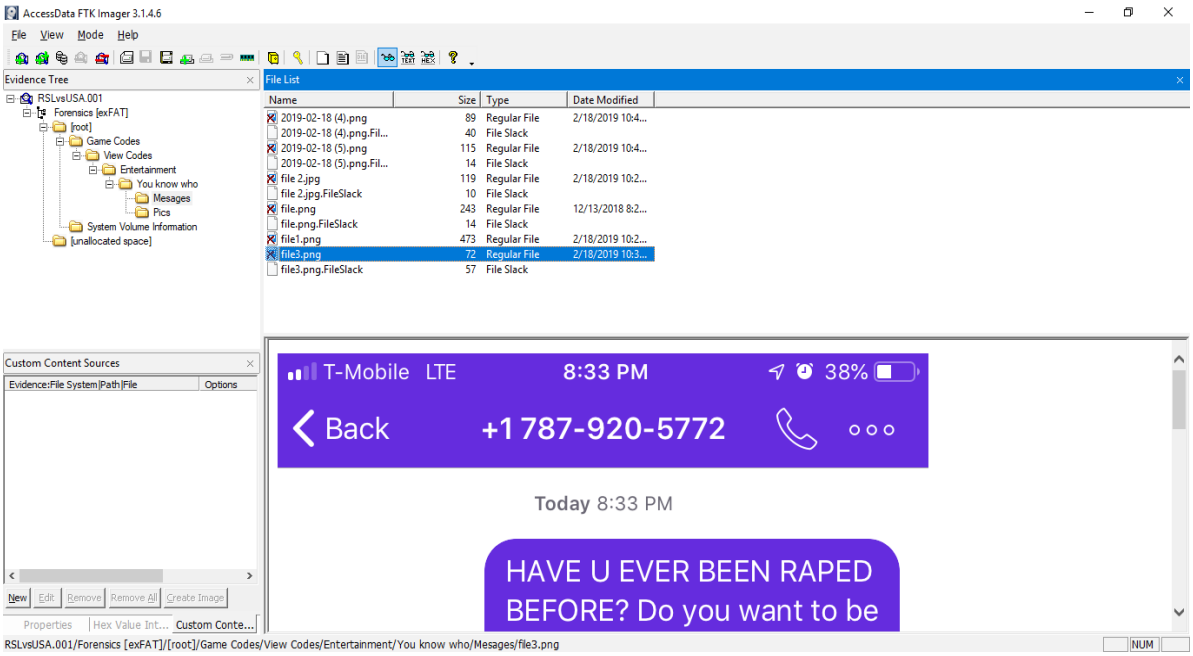

Figura 32: Imagen de mensaje enviado a amiga de Smith.

Luego de analizar el archivo de “Messages”, pasamos al archivo de “Pics” en el cual se logró recuperar el “collage” creado por Lin.

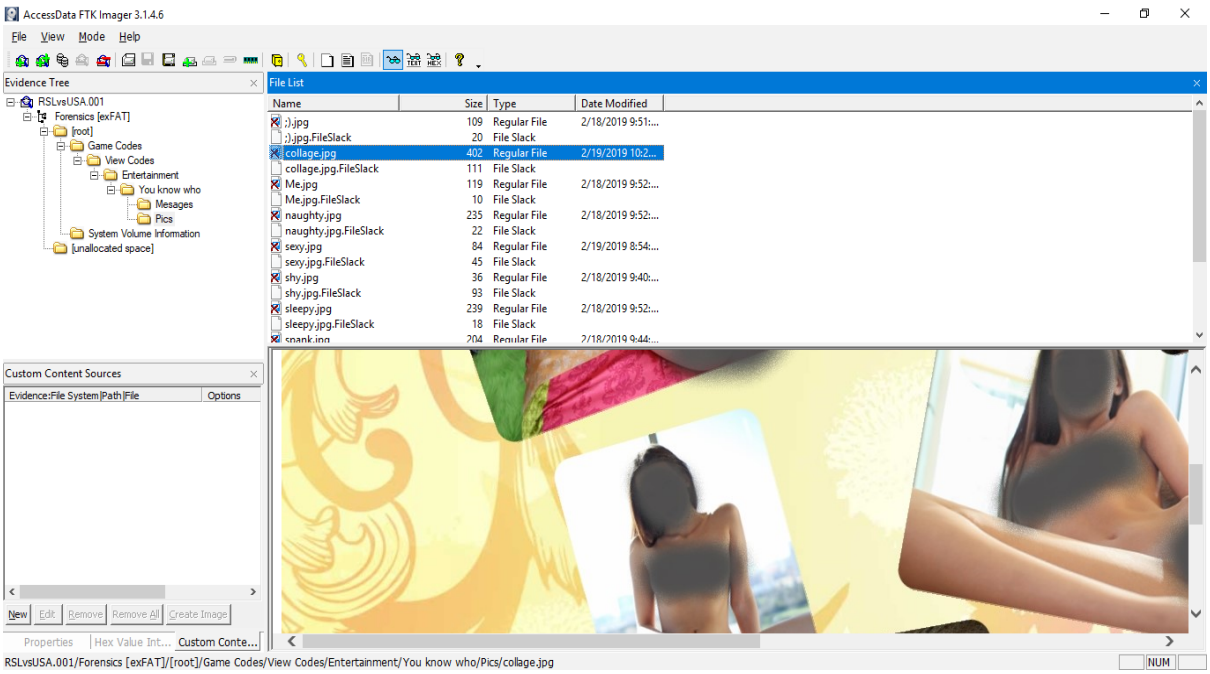

Figura 33: Imagen del “collage”.

Luego de analizar los documentos y encontrar imágenes importantes para el caso, se procede a crear un archivo para exportar y recuperar estas imágenes oficialmente. Esto para poder brindarle al FBI los resultados y las imágenes como evidencia.

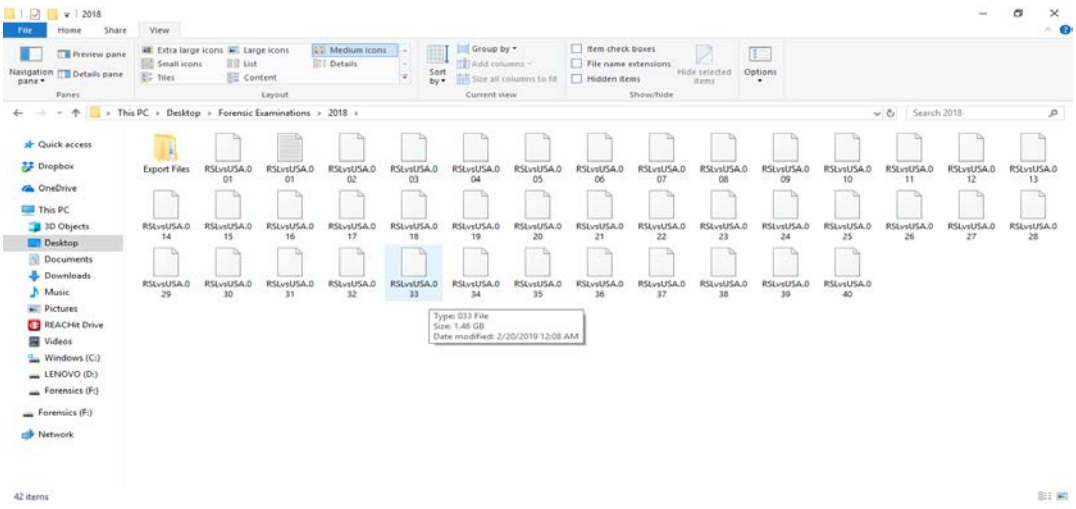

Figura 34: Archivo creado para exportar las imágenes recuperadas.

Archivo de “Messages” dentro del “Export Files” con las imágenes de los mensajes.

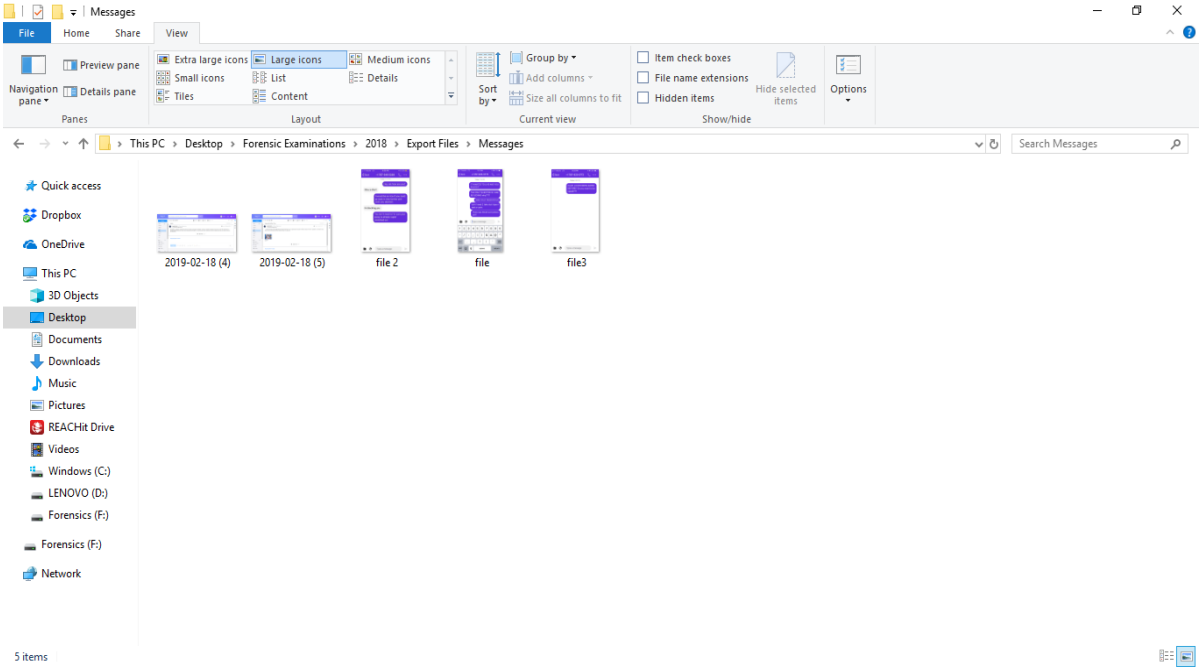

Figura 35: Imágenes de los mensajes recuperados en el archivo exportados.

Archivo de “Pics” dentro de “Export Files” con las imágenes del “collage” creado por Lin.

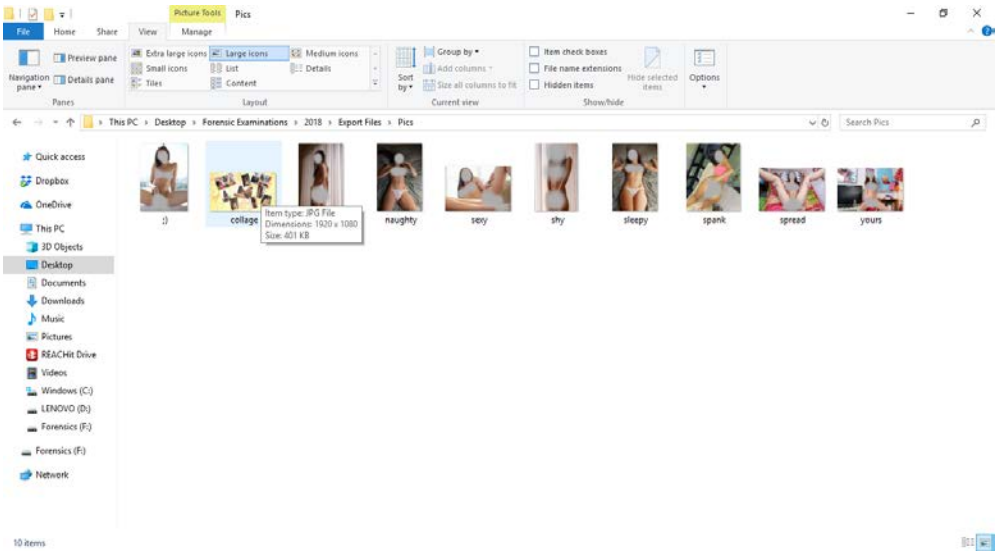

Figura 36: Imágenes de las fotografías recuperadas utilizadas para el “collage”.

Conclusión

De acuerdo con la investigación y análisis de los dispositivos entregados para examinación, se determina que la evidencia encontrada es concreta y que Ryan Lin cometió los delitos de los cuales fue acusado. Los documentos recuperados demuestran que Ryan Lin en efecto estuvo acosando a sus víctimas. En adición, cometió el delito de robo de identidad creando cuentas falsas y haciéndose pasar por las víctimas para perjudicar sus empleos o reputación. Creó cuentas ficticias ocasionándole a las victimas experiencias indeseables donde desconocidos se aparecían en su hogar solicitando servicios sexuales.

Como experto en investigación forense, certifico que Ryan S. Lin es la persona responsable de los mensajes enviados a las víctimas; desconocidos apareciendo en su hogar solicitando servicios sexuales y de la reputación de las víctimas en sus hogares; universidad; escuelas y empleo. La evidencia encontrada en el *Flash Drive* es suficiente para confirmar que el Sr. Ryan Lin es el responsable basado en mi experiencia en relación con la investigación forense digital.

Sección 5: Discusión del caso

Ryan S. Lin es acusado con 24 cargos de acoso cibernético, robo identidad agravada, abuso y fraude en computadoras, distribución de pornografía infantil y amenaza de bombas según el documento USA v. Ryan S. Lin (2018). Según los resultados encontrados al finalizar el análisis de la evidencia 2017-RSL-1 (IronKey Basic S1000 64GB Encrypted Flash Drive), Ryan Lin estuvo acosando a las víctimas, enviando los mensajes y fotos. Las imágenes demuestran claramente que Lin estuvo enviado dichos mensajes a las víctimas.

Todas las imágenes encontradas en el procedimiento corroboran que Ryan Lin guardó imágenes de varios de los delitos de los cuales se le acusa y logró eliminarlas. Esto comprueba que el realizar una investigación forense digital es viable para lograr recuperar y obtener la evidencia que pruebe los hechos más allá de duda razonable.

Sección 6: Auditoría y prevención

Según U.S. Department of Homeland Security Cybersecurity Strategy (2018) (DHS, por sus siglas en inglés), la dependencia en el internet ha aumentado sustancialmente. Este crecimiento en el uso de la tecnología también aumenta el riesgo progresivamente a nivel global. Esto ha abierto paso a las amenazas de terrorismo, crímenes individuales, crímenes organizacionales, y otros tipos de crímenes en el mundo digital. DHS cree que el internet puede ser seguro y resistente. Al igual que otras organizaciones, esta agencia gubernamental trabaja para minimizar las vulnerabilidades organizacionales de ataques maliciosos protegiendo sus propias redes. Todos los días se esfuerzan para identificar y manejar riesgos cibernéticos de índole nacional.

El DHS (2018) estima que más de 20 billones de equipos se encontrarán conectados al internet para el 2020. El incremento en riesgo dado al número y variedad de equipos se considera sustancial. Esta diversidad de amenazas puede impactar sistemas de información tanto federales como no federales. Los intentos a las redes del gobierno ocurren a diario; los números de incidentes han aumentado más de diez veces entre el 2006 y el 2015. En el 2015, una brecha a una sola agencia federal resulto en el compromiso de información personal de más de 4 millones de empleados federales y cerca de 22 millones de personas.

Para manejar este problema, el DHS ha creado una estrategia para combatir la seguridad nacional de los riesgos cibernéticos. Identificaron 5 pilares de los cuales establecieron 7 metas para asegurar la funcionalidad, innovación, comunicación y prosperidad económica de forma consistente con los valores nacionales y que protegen la privacidad de las personas. El DHS y la Oficina de *Strategy*, *Policy*, and *Plans* (PLCY, por sus siglas en inglés) (2018), lideraron el

desarrollo de la estrategia junto a todos los componentes del DHS y de acuerdo a la sección 1912 del 2017 *National Defense Authorization Act* que se demuestra a continuación:

Pilar 1: Identificación de Riesgo

Meta 1: Acceder a los riesgos de seguridad cibernética que están evolucionando

Objetivo 1.1: Mantener atención estratégicamente a las tendencias nacionales y sistemáticas de riesgo en la seguridad cibernética.

Pilar 2: Reducción de Vulnerabilidad

Meta 2: Proteger los sistemas de información federales.

Objetivo 2.1: Aumentar la seguridad cibernética de las empresas federales mediante mejoras en la gobernación, política de seguridad de información y vigilancia.

Objetivo 2.2: Proveer capacidad para proteger, herramientas y servicios alrededor de las empresas federales.

Objetivo 2.3: Desplegar capacidad y prácticas innovadoras para la seguridad cibernética y proteger el sistema de información del DHS.

Meta 3: Proteger infraestructura crítica.

Objetivo 3.1: Desarrollar ofrecimientos y compromisos de seguridad cibernética para señalar el riesgo nacional a la infraestructura.

Objetivo 3.2: Ampliar y mejorar el intercambio de indicadores de amenazas cibernéticas, medidas de defensa y otra información de ciberseguridad.

Objetivo 3.3: Mejorar la capacidad y recursos de seguridad cibernética disponibles para agencias, reguladores y creadores de políticas en específico.

Pilar 3: Reducción de amenaza

Meta 4: Prevenir y perturbar el uso criminal del ciberespacio.

Objetivo 4.1: Combatir crímenes financieros, perturbar y vencer crímenes de organizaciones.

Objetivo 4.2: Prevenir, perturbar y contraatacar las amenazas de seguridad cibernética para proteger personas, eventos especiales de seguridad y la infraestructura crítica.

Objetivo 4.3: Desarrollar relaciones y construir capacidad de cumplimiento de la ley para contraatacar el uso ilícito del ciberespacio.

Objetivo 4.4: Desarrollar capacidad y recursos para mejorar el esfuerzo investigativo y señalar los retos al cumplimiento de la ley en desarrollo.

Pilar 4: Mitigación de Consecuencias.

Meta 5: Responder eficientemente a incidentes cibernéticos.

Objetivo 5.1: Aumentar el reporte voluntario de incidente y las notificaciones de las víctimas para facilitar la asistencia de respuesta.

Objetivo 5.2: Expandir la capacidad de activos de respuesta para mitigar y manejar los incidentes cibernéticos.

Objetivo 5.3: Aumentar la cooperación entre los respondedores de incidentes para asegurar la complementación a la respuesta de amenazas y el esfuerzo de las respuestas de los activos.

Pilar 5: Habilitar los resultados de la ciberseguridad

Meta 6: Fortalecer la seguridad y fiabilidad del ecosistema cibernético.

Objetivo 6.1: Fomentar la seguridad cibernética mejorada en softwares, hardware, servicios, tecnología y la construcción de redes resistentes.

Objetivo 6.2: Priorizar la investigación, el desarrollo y la transición tecnológica de la ciberseguridad del DHS para respaldar los objetivos de la misión del DHS.

Objetivo 6.3: Expandir la colaboración internacional para avanzar con los objetivos y promover una red abierta, segura y confiable.

Objetivo 6.4: Mejorar el reclutamiento, educación, entrenamiento y retención de desarrollo mundial y fuerza laboral cibernética.

Meta 7: Mejorar el manejo de las actividades de seguridad cibernética del DHS.

Objetivo 7.1: Integrar el desarrollo de políticas de ciberseguridad, la estrategia y las actividades de planificación.

Objetivo 7.2: Priorizar y evaluar la efectividad de las actividades y programas de seguridad cibernética del DHS.

El DHS cree que el espacio cibernético puede ser uno seguro y salvo para la funcionalidad del gobierno, entrega de servicios esenciales y la vida cotidiana de las personas. Se mantendrá liderando las iniciativas para asegurar que la seguridad cibernética se está manejando de forma adecuada, que se estén mitigando las vulnerabilidades, que las amenazas estén reduciendo y estén siendo contraatacadas. Con la colaboración de los expertos en redes y la ley, la estrategia del DHS y el esfuerzo en las respuestas de incidentes se puede proveer un mejor espacio cibernético para las futuras generaciones.

Esta estrategia parece ser la más adecuada para poder prevenir o disminuir los incidentes cibernéticos. Es una estrategia real y con enfoque en lo más importante. Si el plan es llevado a cabo según está implementado, la seguridad de las personas está en buenas manos. Es importante

que cada persona aprenda a protegerse individualmente, pero cuando la información más privada la obtienen entidades federales también es importante que ellos protejan la información de cualquier persona con malas intenciones. Según mi experiencia y aprendizaje este plan de prevención puede ser la clave para el éxito de la seguridad cibernética.

Sección 7: Conclusión

El acoso cibernético no es atendido con la seriedad que se debería atender. Es un delito que las consecuencias podrían ser fatales como el suicidio o problemas mentales por el resto de la vida. Cuando se reporta un acoso cibernético se debe reaccionar con urgencia y tomar acción para que todas las personas estén conscientes de los problemas que están ocurriendo y sepan que se está tomando acción contra estos delitos. Si todas las personas que son afectadas por el acoso cibernético reportaran lo que les sucede, la cantidad de casos aumentaría más de lo que todos se imaginan. Las estadísticas que se obtienen sobre el porcentaje de las personas que han sido víctima o testigos de acoso cibernético están basadas en lo que se ha reportado, pero son muchas las personas que no lo reportan. Si le damos la seguridad a las personas que reportan el acoso cibernético y se tomara acción, tendremos mejores resultados.

El internet es parte de la tecnología que indiscutiblemente está en constante evolución. Es cierto que la evolución de la tecnología es para el bien global pero lamentablemente también evoluciona el mal uso de éste. Mientras la mayoría de las personas utilizan la tecnología para mejorar su vida cotidiana y hasta para constante comunicación, otras lo utilizan para cometer delitos y lucrarse de las personas que no están bien educados sobre la tecnología. Es por eso, que el desarrollo de herramientas y el conocimiento para combatir el crimen cibernético es importante y también está en constante evolución.

El gran avance del internet afecta tanto positiva como negativamente a la humanidad. Hoy día es importante estar informado y educado sobre la tecnología ya que son muchos los beneficios para las personas que no lo utilizan con mala intención. Parte de lo positivo es que en el internet puedes educarte de cualquier tema que desees aprender. La comunicación es mucho más sencilla y puedes comunicarte desde cualquier parte del mundo. No hay nada mejor que

encontrarse en persona y tener una buena conversación, pero lamentablemente no es posible hacerlo en todo momento con todas las personas. También muchos dejan de socializar en la vida real porque se les hace mucho más fácil tener una conversación por internet. De la misma manera que mucha gente utiliza el internet para asuntos productivos, también están los que lo utilizan para acosar, defraudar, robar, y hasta cometer insultos hacia otras personas. Varias de estas las podemos ver a diario, aunque no sea notorio cuenta.

Es importante recalcar que para estos delitos que aumentan y evolucionan con el internet, contamos con herramientas para combatirlo. Con la colaboración de todas las personas y los expertos en investigación se puede hacer un buen esfuerzo para contraatacar el acoso cibernético. Comenzando por establecer una penalidad mayor y orientar a las personas que si cometen el delito serán procesados contra la ley. Muchos de los que cometen los delitos son expertos que saben los procesos de investigación y como pueden ser encontrados. Es difícil capturar a estas personas, la mayoría de las veces son capturadas por errores mínimos cometidos por ellos mismos. La razón por la que es difícil o toman mucho tiempo en capturar a estas personas es porque la mayoría está bien educada y saben borrar evidencia. Queda de parte de las organizaciones, las instituciones gubernamentales y federales estar bien entrenados y experimentados para proteger el bien de la humanidad.

Sección 8: Referencias

Stopbullying.gov (2018). *¿Qué es el ciberacoso?*. Recuperado el 10 de noviembre de 2018, de https://espanol.stopbullying.gov/acoso-por-internet/qu%C3%A9-es/ur6/%C3%ADndice.html

Certain activities relating to material involving the sexual exploitation of minors, 18 U.S. Code § 2252 (1988).

Código Penal de Puerto Rico Ley Núm. 146 de 30 de julio de 2012 (2018). Recuperado el 14 de diciembre de 2018, de http://www2.pr.gov/ogp/Bvirtual/leyesreferencia/PDF/Justicia/146-2012/146-2012.pdf

Criminal forteiture, 18 U.S. Code § 982 (1988).

Duggan, M. (2017). *Online harassment 2017. Pew Research Center.* Recuperado el 5 de diciembre de 2018, de http://www.pewinternet.org/2017/07/11/online-harassment-2017/

Eke, Seto & Williams (2011), Examining the Criminal History and Future Offending of Child Pornography Offenders: An Extended Prospective Follow-up Study. *Law Human Behavior*. 35: 466. https://doi.org/10.1007/s10979-010-9252-2

Fraud and related activity in connection with computers, 18 U.S. Code § 1030 (1988).

Fraud and related activity in connection with identification documents, authentication features, and information, 18 U.S. Code § 1028 (1988).

IBM Knowledge Center. (2018). *Who is the system programmer?*. Recuperado el 10 de noviembre de 2018, de https://www.educaweb.com/profesion/programador-sistemas-informaticos-363/

Intel. *Computer and Laptop RAM- Intel.* Recuperado el 13 de diciembre del 2018, de https://www.intel.com/content/www/us/en/tech-tips-and-tricks/computer-ram.html

Intersate domestic violence, 18 U.S. Code § 2261 (1988).

Jain & Kalbande (2014). A Comparative Study based Digital Forensic Tool: Complete Automated Tool. IJoFCS, 22-29, doi: 10.5769/J201401003.

Karbhari & Mane (2015). *Comparative Study and Simulation of Digital Forensics Tools*. Recuperado de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.742.2594&rep=rep1&type=pdf

Katehakis, A. (2015). Cyberstalking: the growing crime. *Psychology Today*. Recuperado de https://www.psychologytoday.com/us/blog/sex-lies-trauma/201503/cyberstalking-the-fastest-growing-crime

Andres, J. (2014). Estadísticas sobre los delitos informáticos. *Legislación Informática*. Recuperado de http://legislacionunicesar2014.blogspot.com/2014/06/estadisticas-sobre-los-delitos.html

Mishra, A., (2008). *Cyber stalking: a challenge for web security.* Recuperado el 9 de diciembre de 2018, de https://www.researchgate.net/profile/Alok_Mishra5/publication/259148587_

Cyber_Stalking_A_Challenge_for_Web_Security/links/00b4952a0cd2e3ffda000000/Cyber-Stalking-A-Challenge-for-Web-Security.pdf

National Institute of Mental Health (2018). *Autism Spectrum Disorder*. Recuperado de https://www.nimh.nih.gov/health/topics/autism-spectrum-disorders-asd/index.shtml

Nelson, Phillips & Steuart (2016), *Guide to Computer Forensics and Investigations: Processing Digital Evidence.*

Park et. al. (2016). A short review on the current understanding of autism spectrum disorders. PubMed, 25(1), doi: 10.5607/en.2016.25.1.1.

Penalties, 18 U.S. Code § 844 (1988).

U.S. Department of Homeland Security Cybersecurity Strategy (2018). Recuperado de https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

USA v. Maliska, Corte de Distrito de Columbia de USA (2018). Obtenido de https://www.courtlistener.com/docket/7439540/1/united-states-v-maliska/

USA v. Ryan S. Lin, Corte de Distrito de Massachusetts de USA *Criminal Complaint* (2017). Obtenido de https://www.justice.gov/opa/press-release/file/1001841/download

USA v. Ryan S. Lin, Corte de Distrito de Massachusetts de USA *Parties and Attorneys* (2018a). Recuperado de https://www.courtlistener.com/docket/6358360/parties/united-states-v-lin/

USA v. Ryan S. Lin, Corte de Distrito de Massachusetts de USA *Information* (2018b). Recuperado de https://www.justice.gov/file/1050316/download

USA v. Ryan S. Lin, Corte de Distrito de Massachusetts de USA *Governement's Sentencing Memorandum* (2018c). Recuperado de https://www.universalhub.com/files/lin-pros.pdf

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

What is Tor? (2018). *Tor.* Recuperado el 5 diciembre de 2018, de https://www.torproject.org/

Zwass, V. (2011). Information system. *Encyclopedia Britanica.* Recuperado el 10 de noviembre de 2018, de https://www.britannica.com/topic/information-system