EDP UNIVERSITY OF PUERTO RICO, INC

RECINTO DE HATO REY

PROGRAMA DE MAESTRÍA EN SISTEMAS DE INFORMACIÓN

CON ESPECIALIDAD EN SEGURIDAD DE INFORMACIÓN E INVESTIGACIÓN DE FRAUDE

Acoso y Fraude Cibernético

Análisis del caso: USA v. Steve Waithe

Requisito Para La Maestría En Sistemas De Información

Con Especialidad En Seguridad De Información E Investigación De Fraude

AGOSTO, 2022

PREPARADO POR

JONATHAN W. CALDERAS MIRABAL

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

ACOSO Y FRAUDE CIBERNÉTICO

ANÁLISIS DEL CASO: USA V. STEVE WAITHE

Preparado por

Jonathan W. Calderas Mirabal

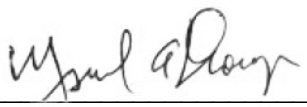
Ha sido aceptado como requisito parcial para el grado de

Maestría En Sistemas De Información

Con Especialidad En Seguridad De Información E Investigación De Fraude

Agosto, 2022

Aprobado por:



Prof. Miguel A. Drouyn Marrero, Ed.D., CISA, CFE

AGRADECIMIENTOS

Le quiero dar las gracias a mi familia entera quien me han enseñado los valores y modalidades que presento hoy día. Le agradezco en especial a mi padre, Walter Calderas, y madre, Yanice Mirabal quienes siempre han estado presentes para ayudarme salir hacia adelante en los aspectos académicos. Siempre han dado lo máximo de sus habilidades para brindar ayuda en cualquier situación que necesite. Los miro como modelos a seguir en esta vida ya que su fortaleza, dedicación, y enseñanzas me han dado las herramientas necesarias para llegar a esta etapa en el presente. Ha sido una bendición estar rodeado por una familia tan trabajadora y humilde.

También le quiero agradecer a unas personas muy importantes quienes me han dado ayuda para poder completar mis metas. Le agradezco a Carlos Calvo, Frank Maldonado, Kalash Jiménez, y Dr. Miguel Drouyn quienes sus guías y diálogos llenos de motivación e inspiración me propulsaron hacia la meta. Le quiero también agradecer a toda la facultad de EDP University quien me ha instruido y guiado por el camino del conocimiento. He podido aplicar cada una de las enseñanzas que me han brindado a mi carrera profesional gracias a sus experiencias y conocimientos extensos.

TABLA DE CONTENIDO

TABLA DE FIGURAS

SECCIÓN I: INTRODUCCIÓN Y TRASFONDO

Introducción

Una persona pasa por diferentes etapas de la vida, etapas que son imposibles de evitar. Nosotros nacemos y luego pasamos a ser cuidados por nuestros padres y madres. Durante ese periodo de tiempo, nuestros padres y madres se encargan de protegernos de cualquier situación o evento que sean negativas para nuestra salud. Luego pasamos a empezar la escuela K-12. Los maestros y administrativos tienen como misión la enseñanza, pero también la creación de un ambiente sano y saludable para la transformación de personas inmaduras hacia personas listas para enfrentar la realidad dura que es la vida. La siguiente etapa es la universidad.

La Universidad pasa a ser una etapa en la cual se espera que los estudiantes asuman un control mayor de su proceso educativo. Es entonces, la misión de cada una de las personas en defenderse y protegerse cada uno. Pero, aun así, eso no le da autoridad, permiso, ni el potencial de los profesores a abusar de los estudiantes. En los tiempos de antes, ese tipo de abuso pudiera haber sido peleas, abuso verbal, cartas con intenciones negativas, entre otros. Pero ahora en la era digital, ese abuso toma otra forma diferente.

Según Morgan & Truman (2022), nada más que hace 3 años atrás, 1.3% de toda la población en los Estados Unidos, o 3,419,710 personas fueron acosadas. De eso, 0.4% o 936,310 personas de toda la población de 16 años en adelante en los Estados Unidos, es víctima de algún tipo de acoso cibernético o *cyberstalking* en inglés. Por ese mismo camino, Morgan y Truman mencionan que de ese mismo 0.4% de la población que recibe acoso cibernético, 538,690 personas o el 0.2% fueron víctimas de acoso cibernético con la modalidad de recibir correos electrónicos o algún otro tipo de mensajería del internet o redes sociales.

Es muy importante la investigación de este caso ya que, con los análisis realizados y concluidos, pueden ser muy útiles para la población en general para poder tratar de controlar y minimizar los daños causados por el acoso cibernético realizado por maestros o profesores de una institución universitaria. Según Miller (2021), esos daños pueden ser: intenciones de suicidio, PTSD, depresión, estrés, miedo extremo, pérdida de control, sueño, hambre, familiares, y amistades, y el trauma que dura a través de los años. Las entidades en las que se beneficiarán del análisis de este caso son:

- Todas las instituciones educativas, escolares, y universitarias
- Padres, madres, familiares, y amistades de los estudiantes
- Los estudiantes de todos los niveles de educación
- Pasadas y futuras personas víctimas de acoso cibernético.

Descripción del caso

Caso: United States of America v. Steve Waithe

Número del caso: 1:21-cr-10342-PBS

Partes en el caso:

- **Acusado:** Steve Waithe
- **Víctimas:** 49 estudiantes femeninas anónimas de los estados de California, Colorado, Connecticut, Florida, Illinois, Indiana, Maryland, Massachusetts, Michigan, Minnesota, New Jersey, Pennsylvania, South Carolina, Texas, y Virginia.

Investigadores:

- Mark Wilson, agente especial del FBI
- Joseph R. Bonavolonta, Agente Especial a cargo del FBI división de Boston, MA

Abogado:

- Jack Corfman, abogado en representación de Steve Waithe

Fiscales:

- Nathaniel R. Mendell, Fiscal de la corte del estado de Massachusetts en Estados Unidos
- Adam W. Deitch, Asistente de la Unidad de Crímenes Mayores

Juez:

- Honorable Denise J. Casper, Corte Federal de Boston, Massachusetts

Trasfondo

Este trabajo investigativo se enfoca principalmente en el área del acoso y fraude cibernético donde se presentará un esquema fraudulento realizado por el acusado, proveniente de Chicago, Illinois. El caso de US v. Steve Waithe, 1:21-cr-10342-PBS (2021) ha sido uno de los más famosos en los años recientes dado su tema de abuso del poder y el acoso cibernético hacia mujeres. El acoso cibernético en especial ha sido uno de los esquemas más populares y dañinos para la salud mental.

Steve Waithe tenía 28 años en abril del 2021 cuando fue traído a la justicia, por lo que debe tener alrededor de 28 o 29 años al momento de realizar esta investigación. Según Bennett-Green (2014) su hermano, Stann Waithe, participó por Trinidad y Tobago en las olimpiadas de Beijing en 2008. Por otro lado, Steve Waithe participó por Trinidad y Tobago en 2012 en unas competencias en Barcelona. Se puede entonces deducir que es de decendencia de Trinidad y Tobago, pero nacido en los Estados Unidos con ciudadanía americana. Adicional, mide 6 pies y 2 pulgadas, lo cual lo ayudó muchísimo a destacarse deportivamente. Se reporta por Penn State University Athletics (n.d.) que fue un deportista universitario de excelencia en la universidad de Pennsylvania en el 2014 y 2015.

Según Meléndez & Hughes (2021) Waithe comenzó como entrenador interino en la universidad de Tennessee. Continúan mencionando que luego pasó a trabajar como entrenador de atletismo en las universidades de Pennsylvania e Illinois Institute of Technology. De ahí pasó a la universidad de Northeastern en Boston Massachusetts desde octubre 11 de 2018 hasta febrero 2019, donde empezó sus esquemas defraudadores. Luego procedió a trabajar como asistente de atletismo desde septiembre 16 de 2019 hasta enero 8 de 2020 en la universidad de Concordia en Chicago.

La actividad de fraude y acoso cibernético que había estado cometiendo Steve Waithe mientras laboraba en Northeastern como entrenador deportivo, comienza aproximadamente a finales del año 2018. Las estudiantes víctimas, que permanecen anónimas para preservar su seguridad, se dan cuenta de la actividad sospechosa de Waithe mediante la observación de que lo encuentran rebuscando en el teléfono personal de las victimas sin autorización. Lo denuncian a la universidad Northeastern que luego realiza una investigación de Titulo IX. Se termina declarando a Waithe culpable de acoso sexual. En consecuencia, Waithe pierde el trabajo, pero consigue otro

en otra universidad distinta, continuando su fraude digital hasta que lo traen a la justicia más adelante.

El documento de reporte investigativo US v. Steve Waithe, 1:21-mj-01209-DLC (2021) que destacan a Mark Wilson como el investigador del caso, menciona como logran traer a Waithe por fraude y acoso cibernético. Puedo inferir que comienza cuando una víctima quien estaba recibiendo mensajes sospechosos por Instagram o Snapchat lo reportó a las autoridades. Las autoridades luego rastrearon el IP address de las cuentas fraudulentas hacia su lugar de origen o creación, que en este caso sería la casa de Waithe. Indagaron sobre cual correo electrónico "email" y teléfono fue utilizado para la creación de las múltiples cuentas falsas para rastrearlo hacia información originada de Waithe. Finalmente, logrando acceso a los correos electrónicos controlados por el acusado que incluyen mensajes por Instagram mencionando la creación de esas cuentas fraudulentas.

Descripción de los hechos

Según el documento de US v. Steve Waithe, 1:21-cr-10342-PBS (2021) que destaca al Agente especial del FBI Mark Wilson como investigador principal del caso, se detalla el acusado, Steve Waithe, de cometer el crimen de acoso cibernético desde los años febrero 2020 hasta abril 2021. Durante esos años, Waithe tuvo aproximadamente 49 víctimas diferentes. La dificultad en casos de acoso cibernético es el temor de las victimas a salir adelante e identificarse. Además, es mejor de esta manera para así preservar la seguridad y anonimato de las víctimas.

Realmente se desconoce cuál fue la real razón de este comportamiento errático del entrenador de deportes. Todo comienza cuando Steve Waithe fue contratado en la Universidad de Northeastern en Boston Massachussetts en el año 2018. Luego de ser contratado, comenzando el

año 2019, empezó a demostrar unos comportamientos anti-éticos. Según ESPN (2021) ese comportamiento fue descrito por la abogada Kate McClelland como confianza agresiva y depredadora.

Durante el año 2019, las clases en la universidad Northeastern corrían común y corriente. El trabajo de Waithe era proveer su experiencia como entrenador deportivo, específicamente en el área de la pista. El Sr. Waithe se les acercaba a las mujeres atletas y se ofrecía a obtener el teléfono celular personal de las atletas femeninas con el propósito de grabarlas para que luego puedan utilizar esa filmación para estudiar su técnica y forma de correr para mejorar el rendimiento y efectividad de sus carreras. Las mujeres atletas entonces accedieron y aceptaron bajo esas condiciones. En vez de realmente filmar a las atletas, lo que el Sr. Waithe hacía era rebuscar sus teléfonos personales para fotos e información sensitiva en la cual el pudiera utilizar a su favor en un futuro. De la manera en que él lo hacía era, buscar la foto para luego enviárselas a sí mismo por correo electrónico y borrando cualquier rastro para evitar ser atrapado.

ESPN (2021) reporta que por lo menos una mujer observó a Waithe rebuscando en el teléfono en vez de filmar, que es la razón en la que se obtuvo el teléfono en primer lugar. Muchas de las veces, Waithe abandonaba las prácticas de las atletas a su cargo, todavía trabajando con los teléfonos. Al transcurso del año 2019, Waithe continuó sus prácticas sin ningún remordimiento ni pensamientos en consecuencias. A medida que las mujeres atletas se daban cuenta de lo que estaba pasando, fueron a la universidad de Northeastern a quejarse. La Universidad formuló una investigación en esta conducta inapropiada que finalmente resultó en el despido de Steve Waithe.

Continuando en el año 2020, un año desde que fue despedido, Waithe comienza a contactar a las personas a las cuales le robó información sensitiva mientras se encontraba “filmando”. Waithe creó al menos 5 cuentas con identidades falsas en el servicio social de Instagram para permanecer

anónimo. Waithe utilizó el anonimato para enviar mensajes directos por Instagram a las víctimas que contenían las fotos sensitivas que él había robado cuando ocupaba su teléfono para "filmar" Luego, utilizó esas fotos para orquestar una mentira basada en que había encontrado esas fotos en la internet, pero se ofrecía ayudar a buscar y removerlas si la victima le enviaba más fotos sensitivas. Continuó mencionando que las utilizaría para ayudar a pasarlas por una herramienta que analiza las fotos y busca similares en el internet. Según el documento acusatorio, Waithe envió sobre 100 mensajes a las víctimas. Pero, al ver que no conseguía suerte, decidió aumentar su esquema.

En paralelo, es decir, a la misma vez que utilizaba cuentas falsas en Instagran, Waithe también creó correos electrónicos falsos para solicitar fotos comprometedoras de las víctimas. Los correos electrónicos, provenientes de personas falsas Katie y Kathryn creadas por Waithe, solicitaban las fotos para un estudio corporal en el cual estudia el progreso y transformación de los cuerpos de mujeres atletas. Según el documento acusatorio, muchas mujeres realmente no contestaron, pero al menos 17 personas respondieron con sobre 350 fotos desnudas o semi desnudas. Este tipo de esquema se ve muchísimo de otra forma llamada *phishing*. En muchas ocasiones se parecen en el respecto de que los mensajes solicitan información sensitiva para obtener beneficios. El esquema de fraude se encuentra en su pico máximo.

Waithe ahora continua con la parte de acoso cibernético más agresiva. Como Waithe estaba ansioso de conseguir esas fotos de cualquier manera, pero realmente las víctimas no le respondían, trató de acudir a otras maneras. Se dedicó a entonces a personificar y crear cuentas falsas de técnicos de seguridad en la red de Instagram para enviar fotos sensitivas a las víctimas, las cuales les pertenecen las mismas víctimas, pero Waithe se las robó. También se dedicó a obtener teléfonos

celulares de las victimas para acosarlas e intimidarlas. Todo con el fin de seguir consiguiendo más fotos sensitivas. Pero, el esquema no termina ahí. Waithe sigue escalando su criminalidad.

Ahora Waithe comienza a indagar e investigar sobre la posibilidad de hackear las cuentas de Snapchat. Él logra conseguir a una persona que le puede asistir en ese aspecto. Waithe entonces le provee un pago, los usuarios, y los números de teléfonos de al menos 15 mujeres para poder lograrlo. Waithe y la otra persona, logran entrar en las cuentas de Snapchat sin autorización ni permiso. Resolvieron la situación de la autenticación de doble factor, personificando ser del apoyo técnico de Snapchat y solicitando el código y un PIN mediante un mensaje de texto proveniente de un número telefónico falso. Otra razón del porque este esquema tiene mucho en común con un esquema de *phishing*. Waithe logra robar fotos sensitivas de esas cuentas y las graba en almacenamientos propios. La codicia y malicia del acusado es tan grande, que continúa acosando sus víctimas luego de robar sus propias fotos de las cuentas *hackeadas* de Snapchat. Incluso, se centraliza en el acoso continuo y agresivo antes y después de la brecha de la cuenta de Snapchat de la víctima 6, y también al novio.

Para realmente finalizar la descripción de los hechos cometidos, Waithe consigue una página web llamada LeakedBB, a la cual ofrece vender o cambiar las fotos conseguidas para obtener beneficio monetario.

Acusaciones, Cargos, y Penalidades

Desde al menos del mes de febrero del año 2020 hasta el mes de abril del año 2021, Steve Waithe ha cometido los siguientes delitos criminales:

Cargos 1 – 12: Fraude electrónico (Wire fraud) | 18 U.S.C. § 1343

El cargo principal en que se basa el esquema de cometió Steve Waithe. Waithe obtuvo fotos de una manera en que el mintió sobre el propósito real de obtener el teléfono de las víctimas. Luego de un tiempo, utilizó esas fotos para enviárselas a las víctimas en el cual se las robó, con el propósito de dejarles saber que encontró esas fotos en el internet. Finalmente, ofrece servicios para eliminarlas de la internet si las victimas le envían más fotos para propósitos de búsqueda en reversa o ”reverse search”.

De otro modo similar, Waithe creó y asumió identidades falsas que luego las utilizó para solicitar más fotos de víctimas, esta vez por métodos de correo electrónico. Todo bajo el esquema fraudulento de ser de una compañía que realiza estudios corporales de atletas. Finalmente, utilizó estas fotos para venderlas en la “Dark Web” y obtener beneficios monetarios.

Se expone a una penalidad de hasta 20 años en prisión y multa de hasta $250,000.

Cargo 13: Acoso cibernético (Cyberstalking) | 18 U.S.C. § 2261A(2)(B)

Steve Waithe se encargó de crear un esquema de acoso e intimidación para forzar a que las víctimas caigan o cedan bajo presión. No solo eso, sino también se dedicó a buscar diferentes maneras en las que pudiera contactar a las víctimas si no responden por otro medio de comunicación. Primeramente, Waithe envió mensajes a través de Instagram y Snapchat a las víctimas solicitando más y más fotos sensitivas para ayudar a sacarlas del internet. También se dedicó a obtener fotos sensitivas de Snapchat y enviárselas a los novios/novias de las víctimas a través de mensajería instantánea para así crecer la campaña de acoso e intimidación. Finalmente, se dedicó a enviar mensajes de texto para acosar a las víctimas y novios/novias de las víctimas, ya que no le respondían por otros medios de comunicación.

Steve Waithe se expone a una penalidad de un máximo de 20 años si las víctimas han sufrido algún tipo de ataque físico mayor. Máximo de 10 años si la víctima ha sido agredida físicamente.

Cargo 14: Conspiración de cometer fraude de computadoras (Conspiracy to commit computer fraud) | 18 U.S.C. § 371

Steve Waithe necesitaba más fotos sensitivas para ambos sus usos personales y para seguir en el esquema fraudulento. Dándose cuenta de que las víctimas y/o los novios/novias de las victimas realmente no les respondían por la mensajería de Instagram, Snapchat, mensajes de texto, e email, decidió investigar un poco sobre la posibilidad de "hackear" las cuentas de Snapchat. Luego de realizar su investigación, llegó a la finalidad de contactar a una persona con la habilidad de "hackear" esas cuentas. Conspiración realmente se refiere a cuando 2 o más personas se colocan en acuerdo de realizar un acto criminal pero todavía no lo ha realizado

Waithe se expone a una penalidad de 5 años por su conspiración de tipo mayor.

Cargo 15: Fraude de computadoras | 18 U.S.C. § 1030(a)(4) y 2

Waithe le proveyó los "usernames" y números telefónicos de unas víctimas para que el contacto *hacker* pueda entrar a las cuentas de Snapchat ilegalmente. Finalmente, el contacto logró entrar a las cuentas de las víctimas y le proveyó los detalles resultantes de credenciales. Waithe entonces procede a robar la información sensitiva en las cuentas de Snapchat. Waithe se expone a una penalidad de máximo de 10 años por la (a)(4).

Definición de términos

Acoso cibernético: La utilización de quipos electrónicos como el teléfono celular, computadoras, y la internet para acosar o acechar (*stalk*) a una persona (Gordon, 2021).

PTSD: Conocido en inglés como el Post-traumatic Stress Disorder. Es un desorden mental o psiquiátrico causado por eventos traumáticos como una guerra, violación, robo, u otros que causan mucho estrés al cuerpo, específicamente la mente (Mayo Clinic, n.d). Los eventos se retienen en la mente y causan mucha ansiedad, terror, y miedo. Luego, la persona puede vivir esos momentos de forma retrospectiva, comúnmente en los sueños.

***Phishing*:** El acto de enviar mensajes, ya sean por correo electrónico, mensajes de textos, o llamadas telefónicas por entidades falsas imitando ser legítimas, para el propósito de obtener información (Phishing.org, n.d.).

Smishing: El nombre coloquial que se refiere solamente al envío de mensajes de texto fraudulentos con el propósito de obtener información sensitiva (Norton, 2022).

Instagram: servicio o red social en la cual se permite compartir fotos y videos para que las demás personas las vean (Instagram, n.d.).

Snapchat: servicio que permite enviar fotos o videos a personas, pero que se borran o eliminan automáticamente después de ser vista. También proveen espacio para comunicaciones de tipo "chats" (Bates, 2021).

Esquema de Fraude: Evento o actividad realizad en el cual se miente para obtener beneficios (ACFE, n.d.).

Anonimato o anonimizado: que se desconoce el origen, o que se trata de evitar ser reconocido (Merriam-Webster, n.d.).

Nombre de usuario o "username": identificación única que se utiliza para la identificación de una sola persona entre muchas (Tatum, 2022).

Búsqueda de imagen en reversa: Se refiere a la utilización de una imagen en una herramienta que la usa para analizarla y luego buscar más imágenes semejantes a la utilizada (Fisher, 2020).

***Hacker*:** entidad que se dedica a obtener acceso sin autorización o autenticación a lugares o sistemas protegidos (Cisco, n.d.).

Dirección IP: Conocido como *IP address* en inglés. Es una serie de caracteres únicos asignados a cada dispositivo conectado al internet. Su función es permitir la conexión entre los dispositivos (Fruhlinger, 2022).

SECCIÓN II: REVISIÓN DE LITERATURA

Introducción

Desde hace muchos años atrás, idealizábamos con un futuro altamente tecnológico. Imaginábamos relojes que nos permitían hacer llamadas, carros voladores, y mensajería instantánea. Moviendo el tiempo hacia adelante, estamos en esa época que deseábamos. Pero no todo es tan interesante o divertido como lo ansiábamos. El internet ha sido un área que promueve el crecimiento, estudio, crecimientos económicos, y la comunicación. Así mismo como se pueden utilizar para beneficios benignos, se pueden utilizar para beneficios nefastos.

El internet permite la facilitación y mejoría del crimen de acoso cibernético por la naturaleza anónima del internet y la falta de educación de la población. Se les hace mucho más fácil a los criminales esconderse detrás de una pantalla, teclado, y ratón. También se puede pensar de la siguiente manera. Los criminales no fueran criminales si no existiera la anonimidad en la internet. Realmente no hay un curso obligatorio que se ofrece para aprender a utilizar el internet. Cada persona es responsable de educarse en hábitos sanas sobre el uso del internet. Pero, para las personas muy jóvenes, este tipo de responsabilidad educativa en la internet le cae principalmente a los padres y madres. Así mismo, puedo decir que basado en mi observación extensa, están fallando considerablemente. Los encargados simplemente facilitan los equipos como las computadoras, tabletas, o teléfonos para navegar el internet, pero no monitorean su uso. Este tipo de comportamiento se replica y aumenta a través de los años y consigue la consecuencia de no saber controlar su uso ni su compartimiento de información personal.

Ya que es evidente de que hay un fallo en los usos correctos del internet, también se falla en el buen régimen de cuidado social. Me refiero a normativas para salvaguardar su identidad en

las redes sociales. Las personas deben practicar políticas de contraseñas seguras, educarse en esquemas de *phishing*, no prestar sus dispositivos tecnológicos a las personas no identificadas, no revelar información sensitiva, y actualizar sus primeras defensas en contra de los virus en la web. No solo es importante conocer las formas en que una persona puede evitar el acoso cibernético, sino también es importante conocer el perfil de los acosadores para lograr determinar la mejor manera de manejar el caso.

Según Hammond (2019) algunos perfiles de los acosadores son:

- Vengativo: Acosador está molesto con la víctima usualmente por razones sin base. Lo único que quieren es causar dolor agresivo. Actúan de manera errática, sangrienta, enojado, y obsesionado
- Calmada: Acosador de manera calmada. Simplemente comente el crimen por el gusto de hacerlo. Actúan de manera calmada, relajada, inteligente, pasiva, y paciente.
- Íntimo: Acosador quien no acepta la terminación o que otra persona no sienta los mismos sentimientos. Actúan de manera agresiva, depredadora, obsesionada, y posesiva.
- Colectivo: Puede ser una combinación de los anteriores. Pero se enfoca en un agrupo de personas, en vez de una persona individual que comete el delito. Actúan de manera agrupada, inteligente, obsesionada, dominante, y silenciosos.

Fraudes involucrados

El elemento fraudulento principal es el acoso cibernético. Para continuar el esquema de acoso cibernético, se utiliza el fraude de computadoras y electrónicos. Como ya establecido la

sección de Definición de Términos, el acoso cibernético es la utilización de equipos electrónicos como medios o vías para llevar a cabo el acto de acoso de una persona. El acosador goza de la modalidad de anonimato que se provee fácilmente en el espacio dentro del internet. Según Morgan & Truman (2022), aproximadamente un 3.4 millones o 1.3% de toda la población de los Estados Unidos o 260.7 millones fue víctima de acoso en el año de 2018 y 2019. Esos acosos incluidas en las estadísticas son: acoso regular (acoso físico), acoso con tecnología (acoso cibernético) y un acoso mezclado con ambas partes. Lo que distingue el acoso cibernético, el tema central de estudio en esta investigación, de las demás maneras de acoso es que se utiliza la tecnología para inducir amenazas a cualquier área de la salud humana (Grayson, n.d.). Las mismas estadísticas de Morgan & Truman dictan que 67% de todas personas recibieron acoso tradicional o físico, y que 80% de todas las personas recibieron acoso cibernético. De las personas que recibieron acoso cibernético, 66% fue por método de llamadas de teléfono y mensajes de texto, 55% por medio de correo electrónico y redes sociales, 32% fueron monitoreados por redes sociales, 29% fueron amenazados con publicación de información sensitiva en la internet, 22% fueron espiadas utilizando equipo electrónico, y 14% fueron seguidas. Las estadísticas tienen en consideración todas las personas (femeninas y masculinos) de una edad de 16 en adelante. Es realmente interesante de que existan estadísticas para el grupo de edad y sexo en la cual se enfoca esta investigación.

Las estadísticas presentadas por Morgan & Truman (2022) argumentan de que las mujeres fueron acosadas más del doble de las veces de acosos hacia los hombres. Esto representa un incidente altamente preocupante para la población femenina. De acuerdo con Bertazzo (2021), Jessica Vitak presenta la preocupación de que el mundo se vaya en la dirección del pensamiento de que el acoso cibernético ya es algo común y corriente en la vida de las mujeres. Begotti & Maran (2019) mencionan que las estrategias más comunes que utilizan los acosadores en contra

de las mujeres son: avances sexuales no deseados con un 20.2%, amenazas de violencias si no cumplen con lo solicitado que representa un 11.8%, y utilización de robo de identidad para personificar a otra persona con 12.2%. Por esa misma línea, los acosadores gozan de ventajas en contra de la víctima, ya que en el mismo reportaje se mencionan que el acosador es amistad hasta el 66.7% de las veces en avances sexuales no deseados, pareja o expareja hasta el 20% de las veces en acoso cibernético, y un extraño 57.1% de las veces en fraude de identidad. Dada la dirección de hoy día y las estadísticas presentadas, se podría pensar que el acoso cibernético ha aumentado exponencialmente, pero realmente es todo lo opuesto.

Bertazzo relata de que el crimen de acoso cibernético no ha aumentado, pero si se ha convertido en un crimen de repercusiones mucho más severas. Begotti & Maran (2019) hacen un estudio de 133 participantes y los resultados encontrados cuentan 58.1% cayeron en depresión, 42.8% caen en ansiedad, 22.0% en paranoia, 4.9% terminan con pensamientos de suicidio, 26.8% le cogen miedo a todo evento incómodo, 12.2% con ataques de pánico, y 12.2% con problemas de dormir. Todo representa implicaciones bastante severas que pueden permanecer por el resto de la vida de la víctima. Morgan & Truman (2022) comentan que 1.5 % de la población estadounidense había reportado acoso cibernético en el 2016, mientras que en el 2019 se reportó un 1.3%. Representa un decrecimiento del acoso cibernético en 3 años, pero sus implicaciones aumentan. Solo 5% de todas las víctimas de acoso cibernético solicitaron una orden de protección.

En acuerdo con el estudio de la firma Pew, descrito por Bertazzo, 41% de las personas mencionan que su acoso cibernético ha sido orquestado en al menos 2 medios como las redes sociales, mensajes instantáneos, correo electrónico, páginas web, video juegos, y aplicaciones de citas o “dating”. Pero, según Morgan & Truman (2022), solo 13% de las personas modificaron sus actividades diarias para poder evitar el acoso cibernético. Más importante, Duggan (2017)

menciona que al menos 27% de las personas en Estados Unidos prefieren no subir contenido en las redes sociales como consecuencia del acoso cibernético de otras personas. Por lo menos hay personas que toman este tema con seriedad y decidieron hacer algo al respecto.

Leyes aplicables

Cargos 1 – 12: Fraude electrónico (Wire fraud) | 18 U.S.C. § 1343

Ley que penaliza a una persona que intenta defraudar para obtener dinero por el método de una premisa o evento falso. El acto de defraudar puede ocurrir por radio, televisión, o internet con contenido de texto, sonido, señales, o imágenes para esquematizar el fraude. Se penaliza por un máximo de 20 años. Según Fraud by wire, radio, or television (1952) si el acto de fraude electrónico ocurre en beneficio de defraudar a un evento de desastre natural o emergencia, la penalidad es entonces una multa de $1,000,000 o prisión máxima de 30 años, o una combinación de ambos.

Cargo 13: Acoso cibernético (Cyberstalking) | 18 U.S.C. § 2261A(2)(B)

Ley que penaliza al atacante por uso de la tecnología (correos electrónicos, redes sociales, mensajes de textos, teléfonos, y computadoras) con la intención de matar, lastimar, acosar, o intimidar y tiene como consecuencia el trauma emocional o miedo razonable de lastima o muerte a la víctima principal, familiares, o pareja de la víctima.

Penalidades según Stalking (1996):

- Prisión de por vida si la victima fallece.
- No más de 20 si la victima termina desfigurada permanentemente.
- No más de 10 años si se utiliza un arma letal o víctima es lastimada seriamente.

- No menos de 1 año si el atacante viola cualquier orden de protección de la víctima.
- No más de 5 años en cualquier otra situación no cubierta en los puntos anteriores.

Cargo 14: Conspiración de cometer fraude de computadoras (Conspiracy to commit computer fraud) | 18 U.S.C. § 371

Ley que penaliza al acto de conspirar, o el convertirse de acuerdo para realizar un acto o evento, entre 2 o más personas. Con el propósito de cometer cualquier ofensa o defraudar de cualquier modo o métodos a cualquier entidad. Según Conspiracy to commit offense or to defraud United States (1948) la penalidad es de 5 años para cada integrante del acto de conspiración. Así mismo, si la ofensa que fue consecuencia de la conspiración es una ofensa menor, entonces la penalidad de esta ley no debe ser mayor de la ofensa.

Cargo 15: Fraude de computadoras | 18 U.S.C. §§ 1030(a)(4) y 2

La ley 1030 penaliza la entrada a propósito y sin autorización a un sistema computarizado de los Estados Unidos. La parte (a)(4) penaliza la entrada a propósito y sin autorización de una computadora protegida con el propósito de obtener objetos de valor, defraudar, y aumentar el esquema de fraude. Según Fraud and related activity in connection with computers (1984) se penaliza con no más de 5 años en prisión.

Junto con 18 U.S.C. § 2, que establece que cuando una persona (1) a propósitos promueve a que otra persona (2) haga una acción de parte de la persona (1), la persona (1) será tan culpable como la persona (2) que cometió el delito (Principals, 1948). Esta ley no tiene penalidades ya que su función principal es atar a una persona que ordena a otra como principal en el esquema.

Casos relacionados

Caso # 1: USA v. Ki Cheung Yau

Según Department of Justice. (2021) el tribunal de Minnesota ha acusado a Ki Cheung Yau, 27, por el delito de acoso cibernético o *cyberstalking* y robo de identidad. Ki Cheung Yau, un extranjero de China, pero viviendo y atendiendo una universidad en Los Ángeles California, ha tomado la tarea de acosar a mujeres sin ningún tipo de motivación previa. Comienza cuando se dedicó a investigar sobre posibles víctimas femeninas de una Universidad en Minnesota hasta que encontró a una persona. Luego, Yau creó perfiles en las redes sociales como Facebook, lugares pornográficos, Instagram, y otros con el propósito de personificar la víctima con su información sensitiva e identificativa. La manera en que logra esto no es expresado explícitamente, pero se puede asumir de que Yau obtuvo información de la víctima de las mismas redes sociales. Las redes sociales son un arma de doble filo por su accesibilidad (Siena, 2021). Permite socializar y comunicar, pero a la misma vez se expone información muy sensitiva.

Finalmente, Yau utiliza esos perfiles sociales fraudulentos para solicitar encuentros sexuales que parecen ser provenientes de la víctima. Pero en realidad no lo son. La mujer víctima relata que ha recibido múltiples acosos cibernéticos basados en muchas llamadas, mensajes de texto, por redes sociales y correo electrónico, y visitas físicas a su hogar como resultado de personas anónimas recibiendo mensajes del acusado. Yau, incluso, ayuda a las personas que aceptan el encuentro sexual a encontrar a la víctima real. Efectivamente promoviendo el acoso cibernético de muchas otras personas extrañas. La víctima reporta a la policía, que inmediatamente realizan su investigación hasta llegar al arresto del criminal.

En relación con el caso de USA v. Steve Waithe, se asimilan en que se puede apreciar que las personas estudiantes jóvenes confían demasiado en la tecnología. Publican demasiada

información que luego pueden ser usadas en su contra. En diferencia, el caso de selección presenta un acoso cibernético de profesor a estudiante mientras que en este caso se presenta una relación entre estudiante a estudiante en diferentes estados. También se diferencian en que este caso relacionado no incluye fraude de computadoras, pero si incluye un grado alto de robo de identidad.

Caso # 2: USA v. Sumit Garg

Según el documento acusatorio del caso USA v. Sumit Garg (2021), Garg fue acusado de cometer el delito de acoso cibernético principalmente hacia una compañera de vivienda "roommate". Está mirando a una sentencia máxima de 5 años por acoso cibernético, máximo de 5 años por acoso cibernético en violación de una orden de la corte por protección, y 5 años por conspiración de cometer el delito de acoso cibernético.

Según el documento acusatorio, Garg, que laboraba como consultor de seguridad cibernética, vivía con su esposa y un *roomate*. Cuando se mudó su compañera de vivienda, el acusado comenzó a rebuscar sus pertenencias personales para obtener más información. Utilizó esa información encontrada para dirigir mensajes de texto y de redes sociales de naturaleza sexual. También utilizó esa información para buscar familiares de la víctima, como el tío y el novio. Cuando tuvieron una discusión sobre visitas de amistades de la víctima, ella solicitó una orden de protección contra Garg en el cual se compromete a no continuar sus ataques de acoso sexual. Finalmente, la víctima se marchó inmediatamente del apartamento que compartían ellos 3.

El acusado ignoró la orden de protección. Pero, esta vez envió mensajes de correo electrónico hacia los familiares con intenciones de atacar e intimidar a la víctima. Envió mensajes de amenazas hacia el tío, que es abogado de la víctima. También al detective de la policía

responsable de la investigación del caso, fiscal responsable de traer a Garg a la justicia, y el juez en cargo del caso.

Este caso se asemeja con el investigado en respecto a cómo una persona que simboliza la autoridad puede abusar de sus especializades con tanta facilidad. En ambos casos, el acosador causó implicaciones emocionales graves. Garg tuvo conocimiento sobre la seguridad cibernética y la utilizó para esconder sus rastros en relación con sus amenazas de acoso por el internet. Aunque seguramente tiene el conocimiento extenso sobre cómo trabajar las seguridades de una cuenta en la red social, Garg pudo haber obtenido las credenciales de la víctima para aumentar su ataque. Pero no lo hizo. Es lo único que se diferencia en mi caso seleccionado.

Caso #3: USA v. Andrew T. Maliska

La Tribunal de Washington D.C. ha encontrado culpable a Andrew T. Maliska por cargos de acoso cibernético y robo de identidad hacia una amiga y estudiante colega de una Universidad en Washington D.C. Según el documento acusatorio de USA v. Andrew T. Maliska (2021), Maliska accedió sin autorización a la cuenta de Facebook de la víctima con el propósito de obtener información sensitiva. Tenía en la mira específicamente fotos comprometedoras. En este caso, es fraude de computadora por obtener acceso sin autorización a una cuenta de red social. Ese cargo no aparece registrado en este caso, pero es meritado mencionarlo. Luego de ese primer paso, Maliska procedió a subir las fotos conseguidas a una página web de foros y otra dedicada a la pornografía con el propósito de acosar e intimidar. Las fotos habían sido editadas para burlarse y fomentar la comunicación despectiva en contra de la víctima.

Los padres de la víctima habían sido enviados un enlace URL hacia las páginas web en donde se encontraban dichas fotos. Inmediatamente decidieron contactar abogados para que

ayudaran en la búsqueda del criminal responsable. Se logró encontrar el responsable y la víctima finalmente fomentó cargos en contra, en la cual se llegó a un acuerdo de cesar toda actividad criminal. Maliska, sin embargo, continuó sus actividades criminales. Incluyendo la creación de una página de Facebook personificando a la víctima.

Otra vez, se ven semejanzas en cómo los casos de acoso cibernético toman auge en el ámbito educativo, en donde las personas son de la edad más propensa para el crimen. Se debe a que es una etapa en donde comenzamos a ser independientes y colocamos nuestra confianza en las personas equivocadas. No hay muchas diferencias entre este y el caso seleccionado para mi investigación. Pero, sin hay diferencia en que, en este caso, el delito de acoso cibernético fue cometido por alguien de más confianza. Un amigo y estudiante colega. Mientras que, en mi caso seleccionado, es cometido por alguien de menos confianza y conocimiento. Un profesor de atletismo.

Herramientas de investigación

Una vez se hallan recopilado toda la información pertinente al caso en general, como lo son: el trasfondo, los acusados, las leyes aplicables, las fuentes de donde se investigará, se procede a utilizar las herramientas para iniciar la investigación y lograr llegar a una conclusión. Es de conocimiento general que las conclusiones de los casos no pueden ser puramente basados en especulaciones subjetivas. Hay que acudir a una investigación basada en herramientas que ayudan a minimizar errores, aumentar productividad, reducir pérdidas de tiempo, y poder llegar a conclusiones que se puedan recrear. Todo este procedimiento se encuentra administrado bajo una serie de reglas que todos utilizan.

Se utilizará el modelo de EDRM para propósitos de esta investigación de fraude digital. El modelo EDRM es un marco que determina los pasos estándares para la investigación, descubrimiento, recuperación, y análisis de la información digital (Callaghan, 2019). Según el EDRM, se persiguen los siguientes pasos en orden para conducir la investigación:

- Identificación: se identifica la información que se espera obtener.
- Preservación: Se localiza la información hacia un área fuera de cualquier peligro.
- Colección: Examinación de la información entera para lograr determinar si se puede utilizar.
- Revisión: Etapa en donde se extrae y examina la información.
- Producción: Los resultados o hallazgos son preparados en forma de reporte.

Se pueden utilizar las siguientes herramientas de forense digital para conseguir llevar a cabalidad los pasos descritos:

- **FTK Forensic Toolkit versión 1.81.6:** herramienta que permite examinar discos duros enteros para analizar archivos borrados, correos electrónicos, fotos, y más (Dodt, 2019).
- **Kali Linux:** sistema operativo en un ambiente seguro basado en Linux pre-preparado con una gran cantidad de herramientas para el análisis forense. Según Kumar (2022) tiene más de 100 herramientas diferentes para su uso de análisis.
- **VMware:** Sistema "software" que permitirá virtualizar la máquina de Kali Linux. En otras palabras, es el "software" que permite el manejo de Kali Linux en una computadora Windows 10.
- **FTK Pro Discover:** Permite la examinación completa de una imagen de un disco duro. Incluye funcionalidades como: la examinación de datos borrados,

documentos, fotos, y visualización de la localización de la data en el disco duro (ProDiscover, n.d.).

- **Autopsy:** Según Kumar (2022), Autopsy se especializa en el análisis de las imágenes de los discos duros de una computadora o disco externo. Primero se obtiene una imagen o copia exacta el disco dura en investigación y luego se incorpora a la herramienta para su análisis completo.
- **FTK Imager:** Permite la creación de imágenes de la data en una computadora sin alterarla ni modificarla de alguna manera. Es muy útil para también examinar la imagen que acaba de ser creada (Exterro, n.d.).

SECCIÓN III: SIMULACIÓN DEL CASO

El esquema del Sr. Steve Waithe comienza cuando fue contratado en la universidad de Northeastern en Boston, Massachusetts como entrenador, desde octubre 11 de 2018 hasta febrero 2019. Como parte de sus funciones de mejoría atlética, el entrenador de atletismo solicita que sus estudiantes mujeres atletas le prestaran su teléfono celular móvil para filmarlas. El propósito de esa filmación es que las estudiantes mujeres puedan luego verlas y poder ver en donde están cometiendo errores para mejorarlos. Pero realmente no filmaba.

A finales del 2018, el Sr. Waithe aprovechaba que tenía el teléfono móvil de las mujeres para rebuscar cualquier foto que las estudiantes tuvieran. Al encontrar información sensitiva, procedió a enviárselas a su correo electrónico para guardarlas. Las atletas se dieron cuenta de este comportamiento y se lo reportaron a la universidad, la cual inició una investigación que terminó en su despido en febrero de 2019. Waithe utilizó esas fotos robadas para usarlas en contra de las víctimas empezando en febrero 2020.

Desde febrero de 2020, utiliza su conocimiento y la relación profesor-estudiante para conseguir por lo menos 6 víctimas en la red social Instagram. El acusado creó las siguientes cuentas falsas en Instagram, junto con el día en que comenzó a utilizarlas:

1. Anon.4887 – 13 febrero 2020
2. Privacyprotecter – 12 junio de 2020
3. Theprivacyprotecter – 30 junio 2020
4. Privacyprotected – 30 julio 2020
5. privacyprotect1 – 30 junio 2020
6. Pvcyprotect – 3 octubre 2020

El propósito de la creación de estas cuentas recae en la intención de contactar anónimamente e intimidar a las víctimas hasta el punto en que continúen enviando más fotos sensitivas. El esquema de comunicación que utiliza con todas las cuentas falsas en Instagram sigue el patrón predecible siguiente:

- Hacer contacto.
- Enviar fotos sensitivas que se robó cuando tuvo acceso a los teléfonos personales, con el propósito de comunicar que las encontró por el internet.
- Ofrece ayudar a remover las fotos.
- Pero, necesita que se le envíe a Waithe más fotos sensitivas para ayudar en la búsqueda de otras fotos en el internet.

El acusado comienza acosando las mujeres atletas con la cuenta de anon.4887 en febrero de 2020. En adición, creó 2 correos electrónicos con perfiles falsos de Katie Janovich (janovichkatie@gmail.com) y otro de Kathryn Svoboda. Con estos 2 correos electrónicos, Waithe logró expandir el esquema en marzo de 2020. Ahora reclama que son personas realizando un estudio de cuerpos de atletas. El estudio se centra en la investigación continua de la relación entre las dietas y ejercicios con el peso, altura, y grasa corporal. Se requiere fotos sensitivas, preferiblemente desnudas para que se pueda realizar. 17 personas respondieron y las víctimas enviaron sobre 350 fotos desnudas. Luego continúa utilizando las cuentas del 2 al 5 en la lista anterior. Pero su codicia lo convierte en insatisfecho con lo logrado y desea más.

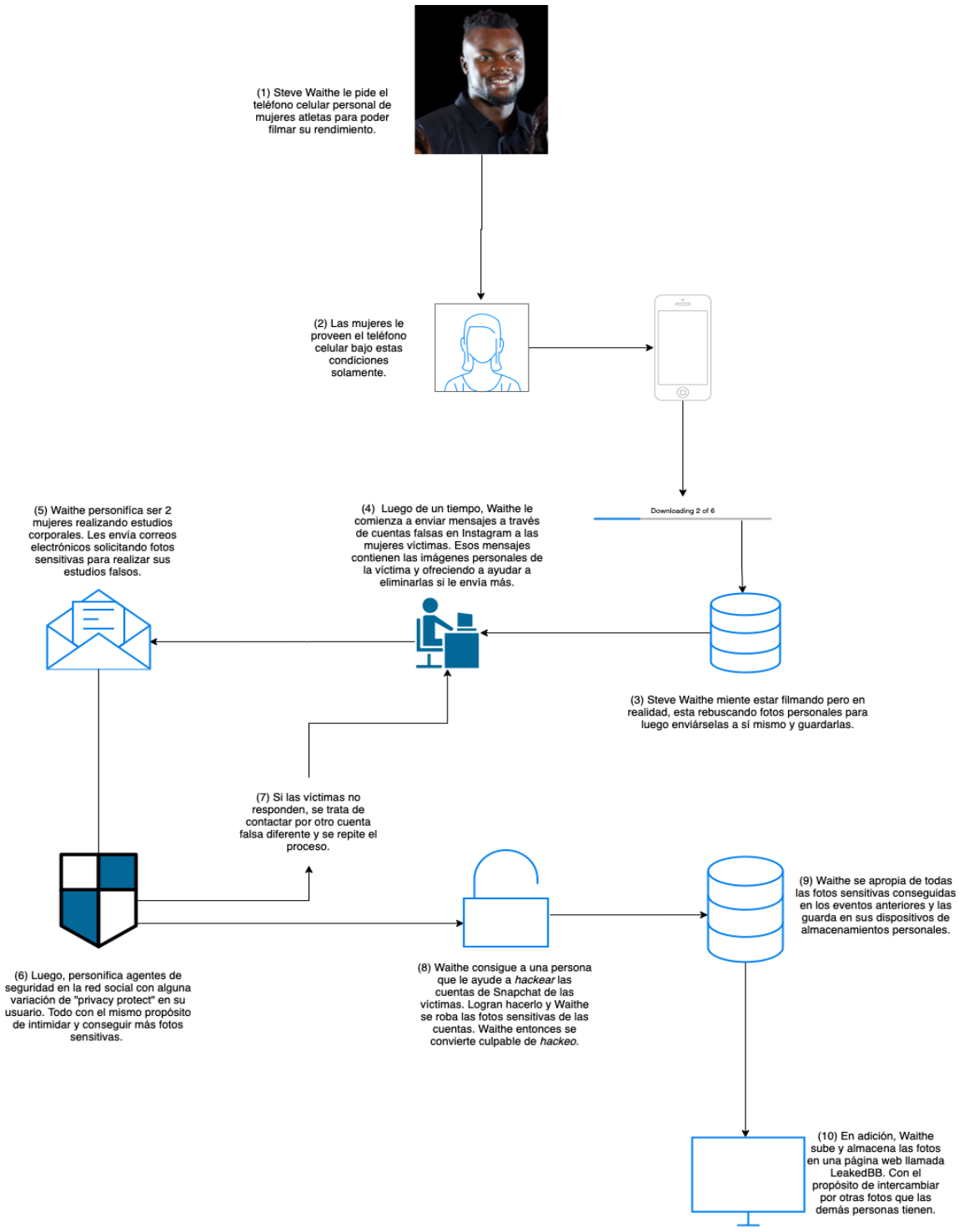
Comienza en mayo del 2020 y aumenta en octubre 2 de 2020 a rebuscar el internet sobre información de la posibilidad real de *hackear* cuentas de Snapchat. Termina obteniendo ayuda en una página web llamada LeakedBB de una persona que ya tiene experiencia haciéndolo. A principios de octubre se le provee los usuarios y números de teléfonos a la persona para ayudar en

la brecha de las cuentas. En el 3 de octubre del 2020 se creó al menos 4 números de teléfonos falsos con el servicio TextNow para que la víctima 6 recibiera 4 mensajes de textos diferentes falsos creados para solicitar el número de código de 6 caracteres y el PIN de 4 caracteres de seguridad. Es importante notar que Snapchat requiere estos códigos para la protección de la cuenta. Por lo menos la cuenta de la víctima 6 fue *hackeada* con éxito y Waithe le proveyó dinero por esos servicios. En la misma fecha, utiliza la cuenta de pvcyprotect en Instagram para acosar al novio de la víctima 6, enviándole fotos sensitivas de la víctima. También utiliza un número falso creado por TextNow para continuar enviándole fotos sensitivas para acosar la víctima. En ambos casos, las fotos enviadas fueron robadas de la cuenta *hackeada*.

Finalmente, Waithe reune todas las fotos obtenidas como parte de este esquema de fraude y acoso cibernético y las guarda en su dispositivo de almacenamiento personal. Utiliza las fotos para intercambios con otras personas en la página web LeakedBB en la fecha de 12 de octubre del 2020. La figura en la siguiente página representa la información de los hechos descritos, pero de una manera visual:

Figura 1

Esquema detallado de acoso cibernético y fraude a mujeres atletas estudiantes.



SECCIÓN IV: INFORME FORENSE DEL CASO

Resumen Ejecutivo

El asistente de la Unidad de Crímenes Mayores, Adam W. Deitch solicitó el servicio de la compañía Forensic Investigation Solutions para analizar un disco de almacenamiento de tipo Flash Drive o Thumb Drive que contiene una copia duplicada exacta del disco duro interno de un laptop recogido como evidencia del caso de US v. Steve Waithe. El agente especial del Federal Bureau of Investigation (FBI) encargado del caso, Mark Wilson, incautó una laptop Samsung Notebook modelo XE500C12 con el número serial 1BEF9FAG419150B como parte de su investigación. Luego extrajo toda la data en el disco duro interno y la colocó en un almacenamiento Flash Drive. La evidencia recolectada fue duplicada para mantener la original intacta y luego sometida a una serie de examinaciones utilizando las herramientas altamente aceptadas por la industria forense y la corte federal. Se revisaron todos los archivos contenidos y luego se revisaron para su veracidad. Los resultados finales demuestran que el acusado Steve Waithe fue el orquestador del esquema de fraude y acoso cibernético. Se utilizará por la corte del Distrito de Massachusetts para traer a justicia el caso.

Objetivo

El análisis del disco Flash Drive que ha sido preparado por el agente especial del FBI, Mark Wilson, ha sido encargado a Forensic Investigation Solutions para que utilicen su experiencia en recuperación de datos en un disco duro. Se manejará esta situación con las herramientas y equipos adecuados para dicho trabajo. Forensic Investigation Solutions está bajo obligación de investigar, analizar, recuperar, y proteger toda información encontrada como evidencia. Todo con el propósito

de encontrar evidencia incriminatoria para ser presentada en el caso. De encontrar evidencia incriminatoria, se presentará el reporte pericial para ser utilizada en la corte para sostener los cargos sometidos.

Alcance del trabajo

El día 1 de junio de 2021, Adam W. Deitch le entregó a Jonathan W. Calderas Mirabal, investigador de la compañía Forensic Investigation Solutions el equipo de almacenamiento Lexar JumpDrive M45 modelo LJDM45-64GABSLNA con 64 GB de espacio que contiene adentro la copia exacta del disco duro de la laptop Samsung Notebook modelo XE500C12 con el número serial 1BEF9FAG419150B recuperada del acusado. Este equipo de almacenamiento de evidencia es entregado al investigador a cargo con el propósito de analizar y extraer cualquier evidencia en respecto a las comunicaciones y las fotos que sostuvo en relación con las víctimas.

El investigador a cargo tiene la obligación de utilizar las herramientas provistas por la compañía de AccessData que es la corporación dueña de las herramientas FTK Forensic Toolkit e Imager. La herramienta para utilizar para esta investigación, AccessData FTK Imager, es altamente aceptada por el Gobierno Federal de los Estados Unidos por su historial de precisión y fiabilidad. Su funcionalidad de analizar, recuperar, examinar, y mantener la integridad de la data les permitirán a los fiscales presentarlo en la corte del distrito de Massachusetts para tomar las decisiones finales en respecto a las acusaciones de Steve Waithe. Los resultados de esta investigación se detallan en un informe de hallazgos.

Datos del caso

Número del caso: 1:21-cr-10342-PBS

Caso: United States of America v. Steve Waithe

Temas: Acoso cibernético (18 U.S.C. § 2261A(2)(B)), Fraude electrónico (18 U.S.C. § 1343), Conspiración de cometer fraude de computadoras (18 U.S.C. § 371), y Fraude de computadoras (18 U.S.C. § 1030(a)(4) y 2)

Acusado: Steve Waithe

Investigador: Jonathan W. Calderas Mirabal

Cliente: Departamento de la Justicia, Corte del Distrito de Boston Massachusetts

Representante del cliente: Adam W. Deitch

Descripción de los equipos utilizados

A continuación, se presentan los equipos utilizados por la compañía Forensic Investigation Solutions para la investigación del caso de US v. Steve Waithe:

Se cuenta con Laptop Apple Macbook Pro de 13 pulgadas del año 2020 con procesador Intel Core i5-8257U quad core con velocidad base de 1.40 GHz hasta un máximo de 3.90 GHz. Memoria RAM de 8 GB y disco SSD de 256 GB formateado a 95 GB para la partición de Windows 10. Se utiliza la herramienta de Boot Camp provista por Apple para la instalación de Windows 10 Education en una computadora MacBook Pro. Como nota profesional, la instalación y utilización de Windows 10 en una computadora Apple MacBook por medio de Boot Camp no presenta ninguna limitación. Se utiliza la herramienta *software* FTK Imager de AccessData en la partición de Windows 10 Education como de costumbre en una computadora Windows regular.

Figura 2

Computadora utilizada MacBook Pro 13 pulgadas del 2020 con Windows 10 Education instalado.

Figura 3

Información de la computadora utilizada.

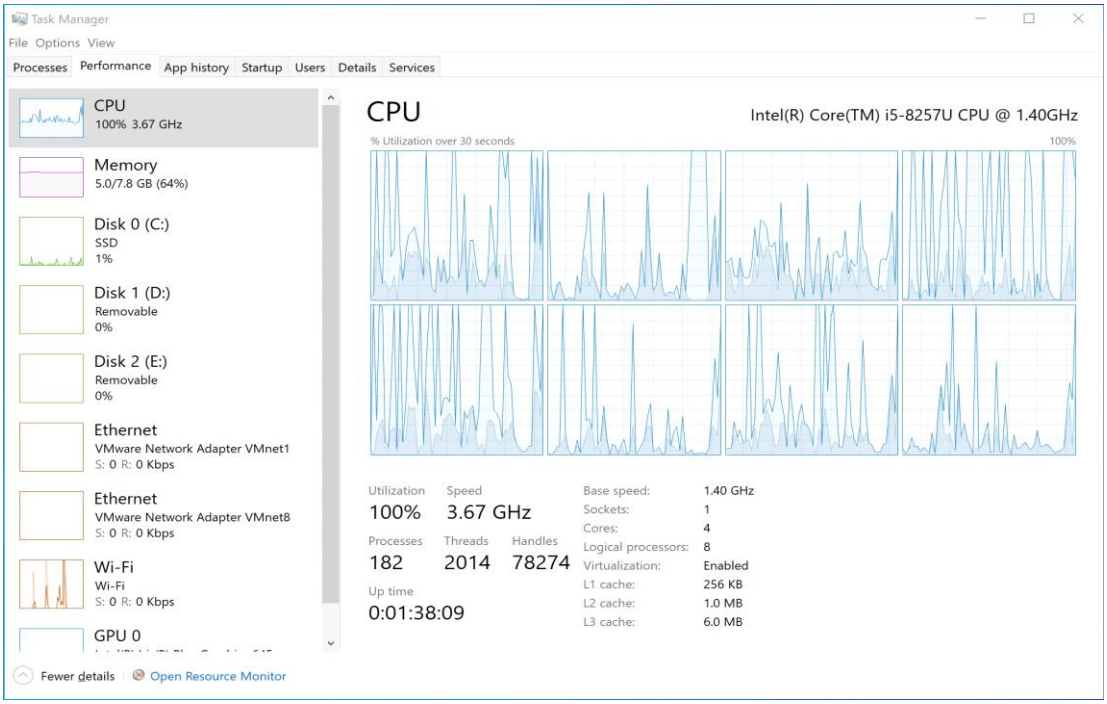
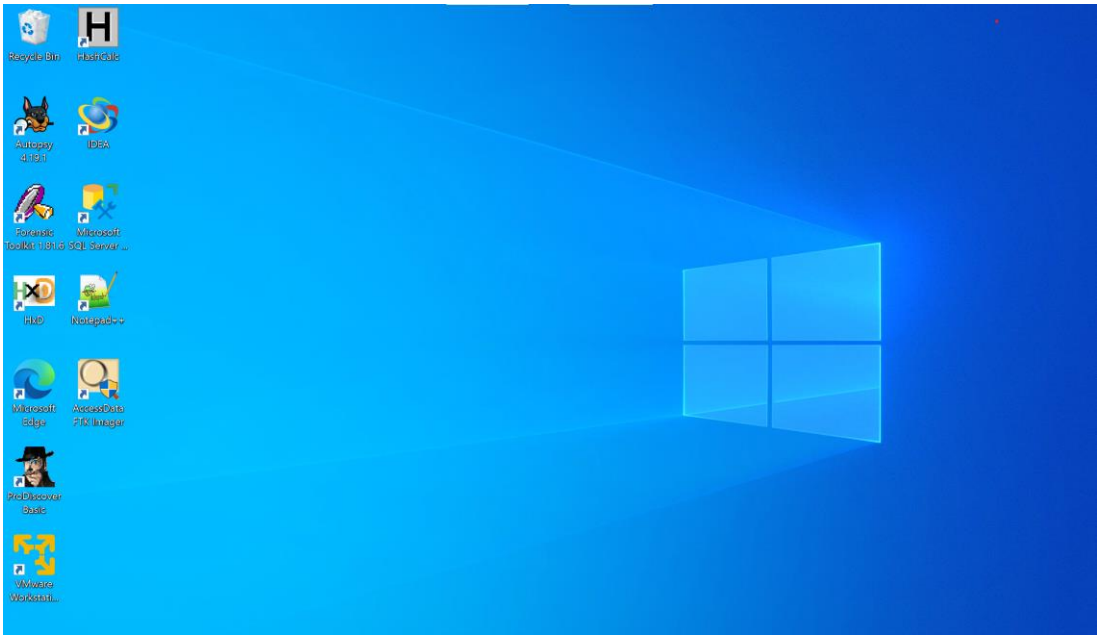


Figura 4

Pantalla principal de la computadora utilizada.



Se ve el icono de la lupa en color crema. Esa es la herramienta que se utiliza para la investigación.

Figura 5

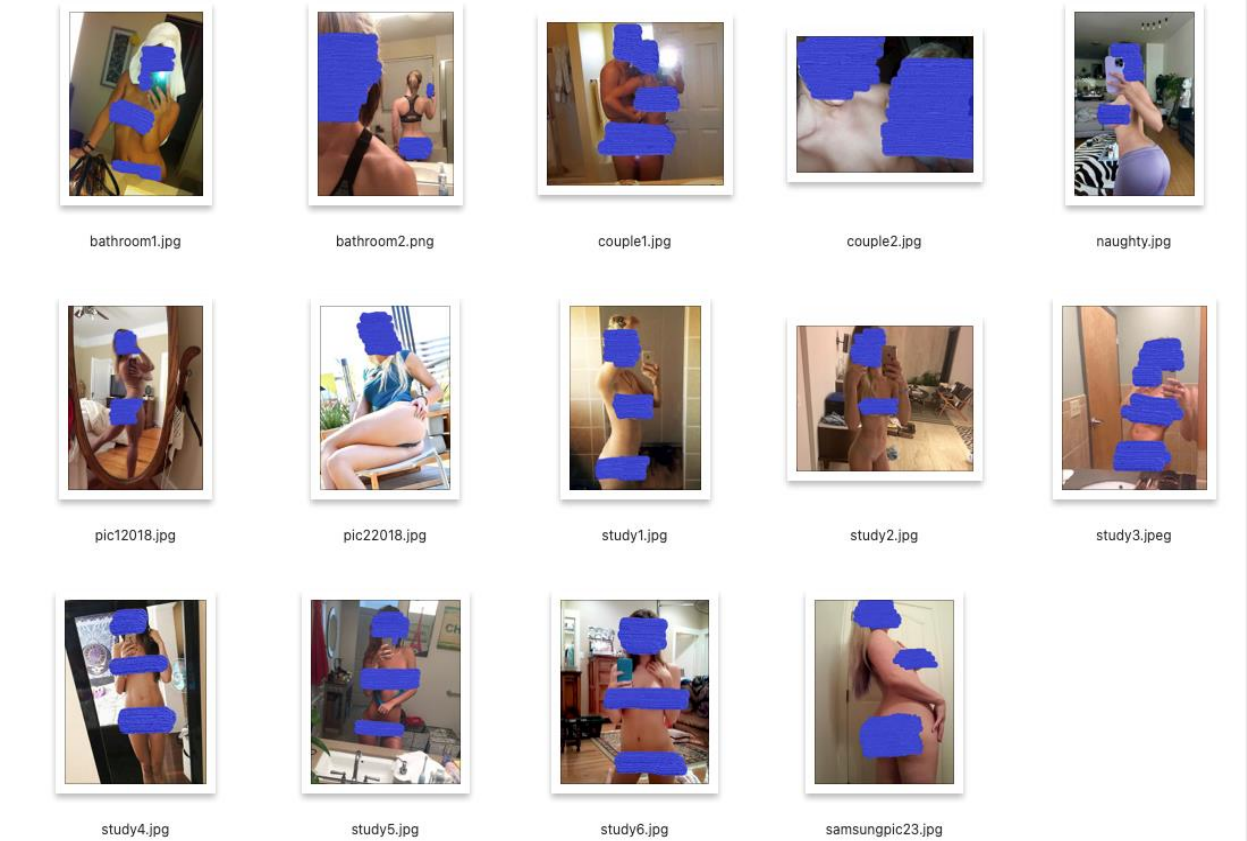
Dispositivo Lexar JumpDrive M45 entregado por Adam W. Deitch para ser investigado por Forensic Investigation Solutions.

Resumen de Hallazgos

Luego de finalizar el proceso investigativo del dispositivo Lexar JumpDrive M45 con 64 GB de almacenamiento que contiene la imagen del disco duro interno de la Samsung Notebook modelo XE500C12 con el número serial 1BEF9FAG419150B perteneciente del acusado, se encontraron una gran cantidad de hallazgos incriminatorios. Se reporta a continuación, una serie de archivos recuperados y exportados por el investigador, que contienen las fotos personales de las víctimas y mensajes en Instagram con propósitos de acoso y fraude.

Figura 6

Imágenes de las víctimas en posesión de Waithe.



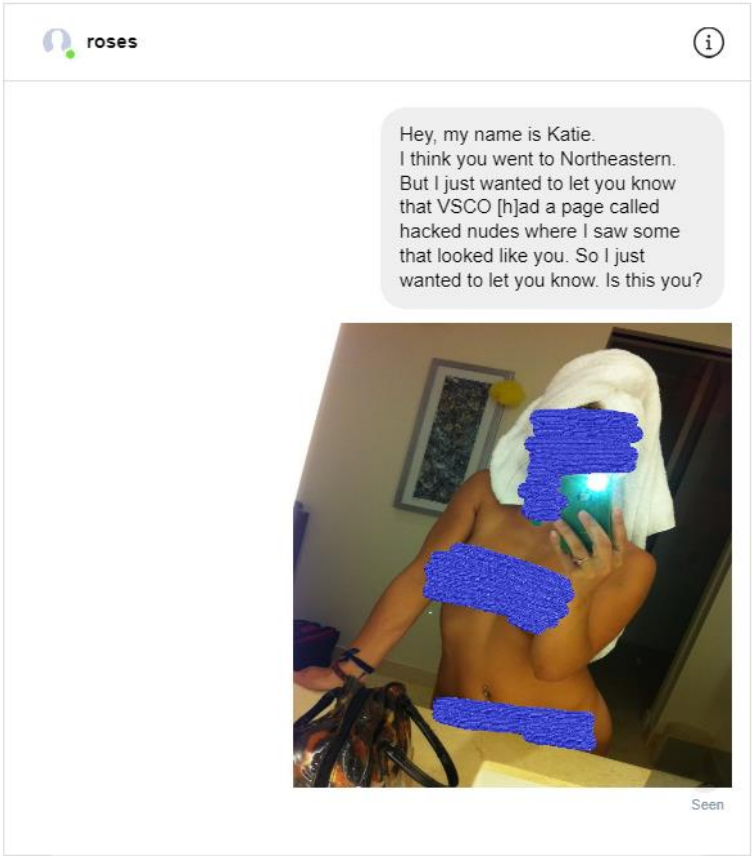
Las imágenes se consiguieron en posesión de Waithe. Se consiguió entrando al *folder* Windows (C), Users, Steve Waithe, Pictures, en un archivo llamado *naked*. Son imágenes que han sido certificadas por las víctimas, que son ellas certeramente. Waithe las obtuvo mediante el robo

de las fotos cuando era entrenador, *hackeo* de la cuenta de Snapchat, y los correos electrónicos fraudulentos personificando 2 mujeres en búsqueda de un estudio corporal. Se recuperaron como resultado de esta investigación y se extrajeron para salvaguardar.

En las próximas figuras 7 - 14, se puede observar todos los historiales de la aplicación de Instagram que fueron recuperadas. Contienen las conversaciones completas que Waithe tuvo con las víctimas. Se consiguieron entrando al *folder* Windows (C), Program Files, Instagram, Chat Log.

Figura 7

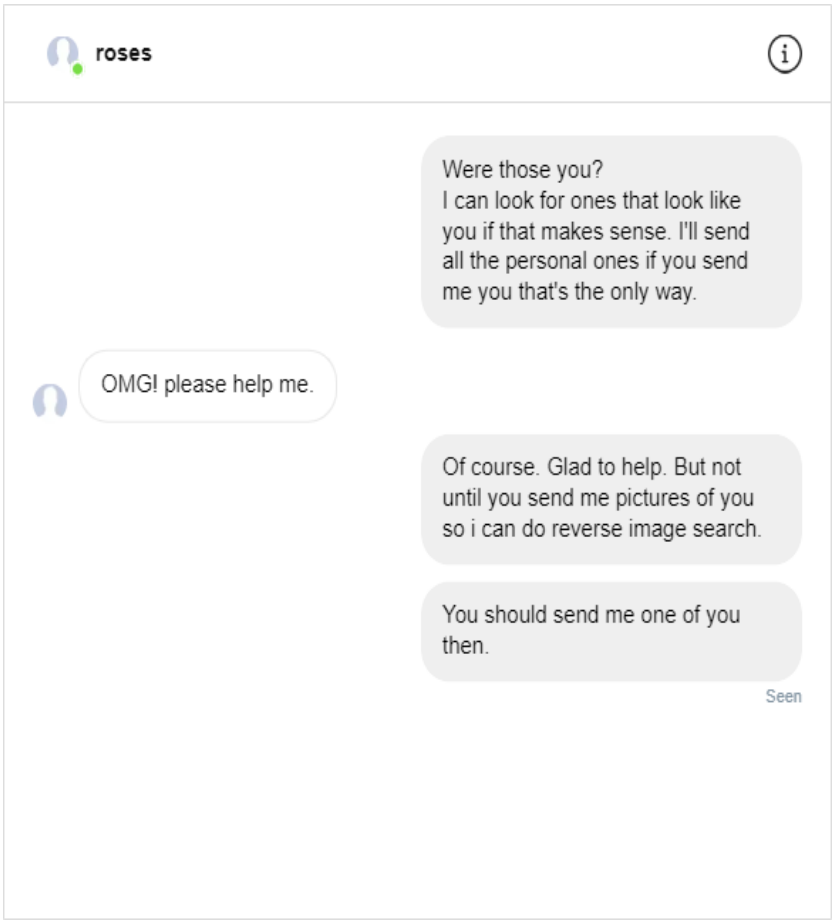
Mensaje por Instagram de Waithe hacia la víctima 1.



Mensaje que utiliza un patrón predecible de conversación en cada uno de los mensajes en Instagram. Steve Waithe utiliza una cuenta fraudulenta para anonimato en el internet.

Figura 8

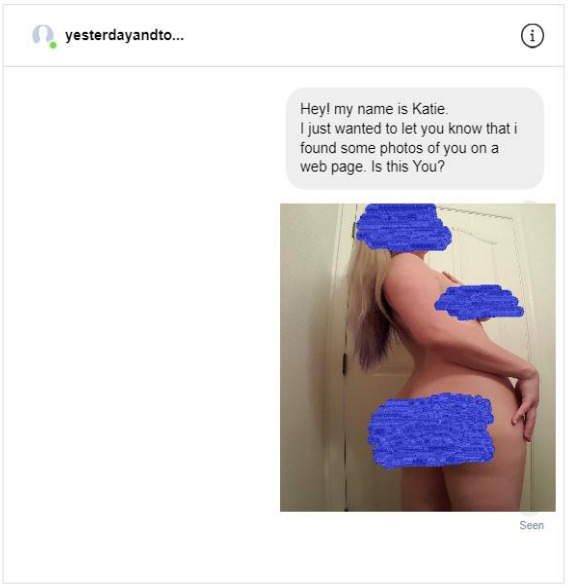
Continuación de mensaje por Instagram de Waithe hacia la víctima 1.



Se continua la conversación con la víctima 1, demostrando el patrón predecible.

Figura 9

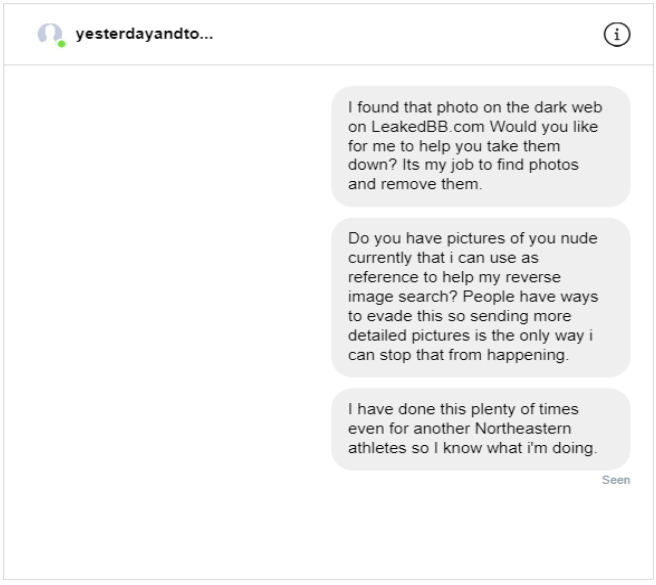
Mensaje por Instagram de Waithe hacia la víctima 2.



Mensaje en Instagram en el que Waithe utiliza una imagen robada para acosar a la víctima.

Figura 10

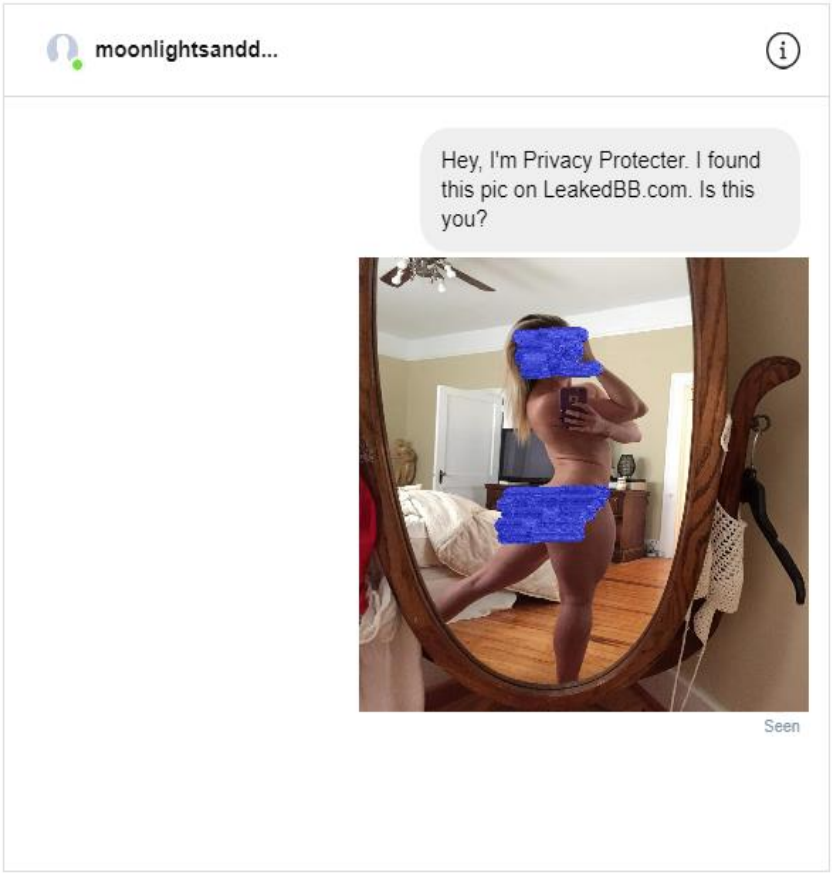
Continuación de mensaje por Instagram de Waithe hacia la víctima 2.



Mensaje fraudulento en el cual Waithe personifica un agente de seguridad que dice saber lo que hace. Puede inspirar un sentido de confianza entre la víctima y el acusado.

Figura 11

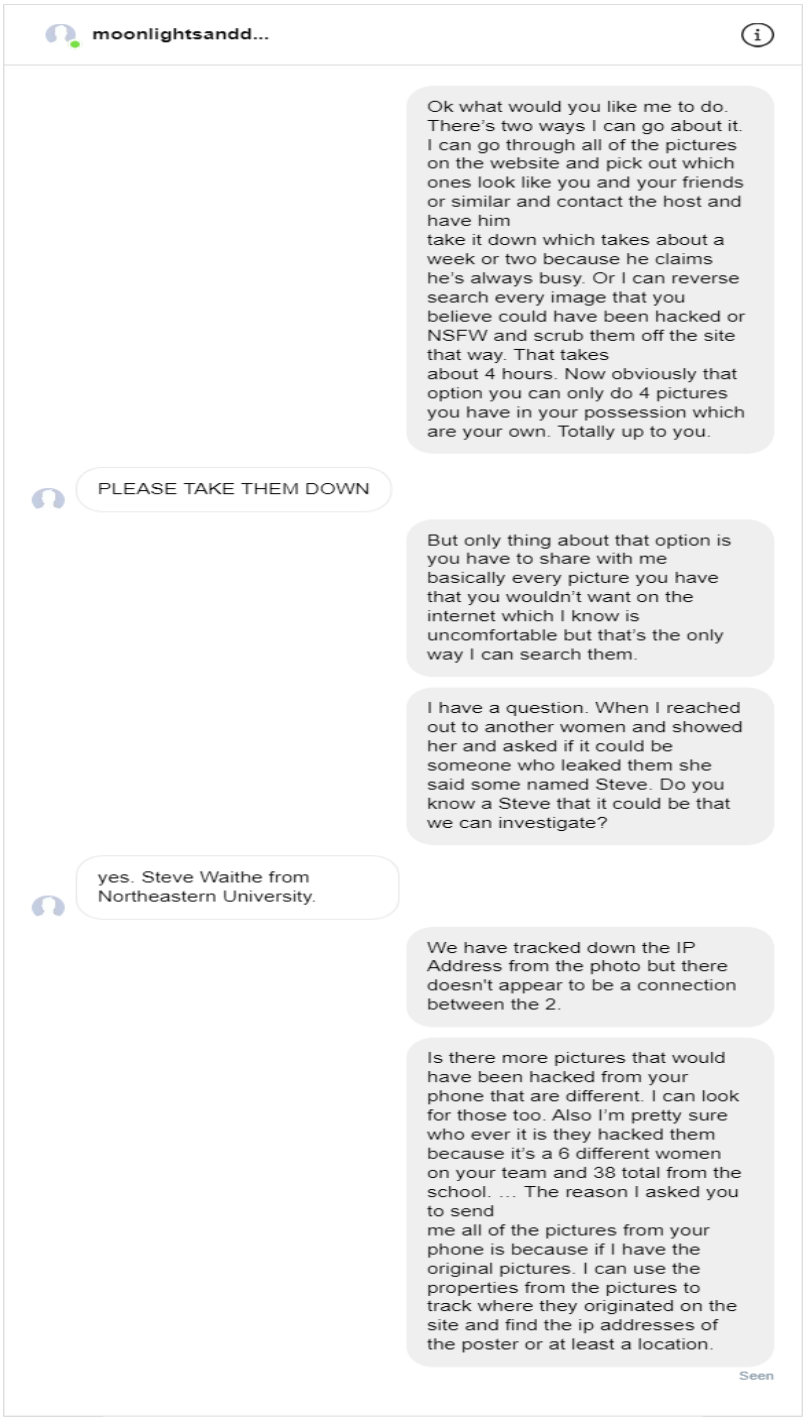
Mensaje por Instagram de Waithe hacia la víctima 5.



Se demuestra el mismo patrón de conversación que lleva con todas las víctimas. Se envía una imagen robada de la víctima para acosarlas e intimidarlas

Figura 12

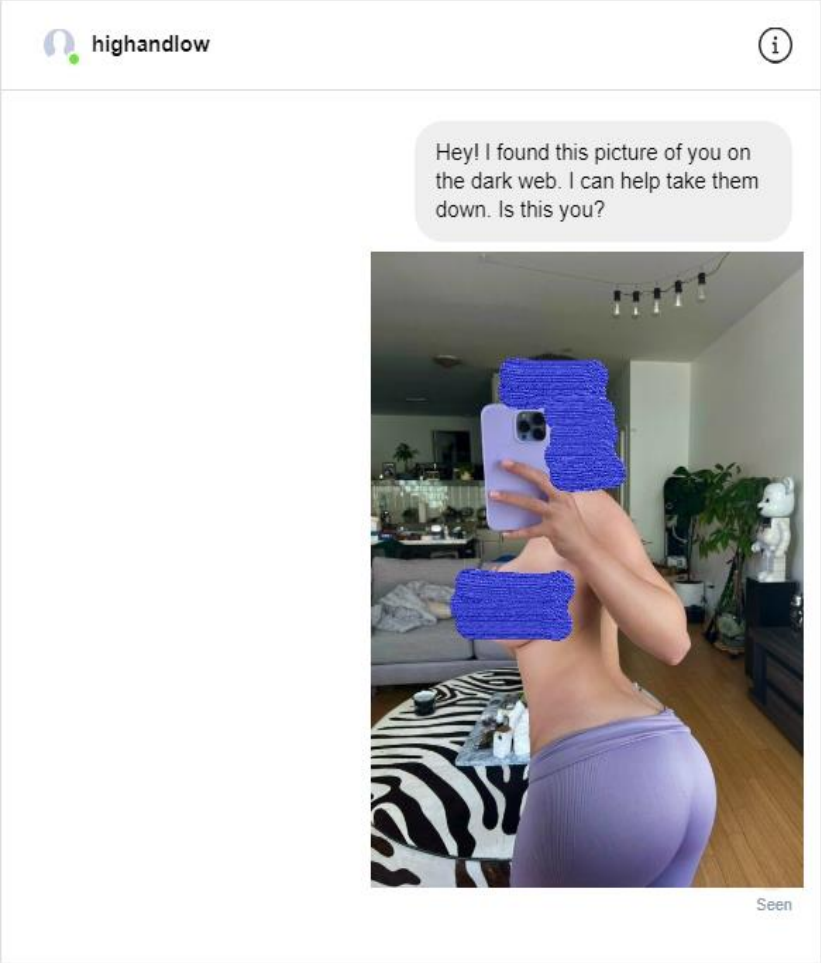
Continuación de mensaje por Instagram de Waithe hacia la víctima 5.



Mensaje largo que inspira confianza falsa entre víctima y Waithe. El acusado, incluso, se menciona el mismo, pero con motivos para tratar de eliminarse de las sospechas de la víctima.

Figura 13

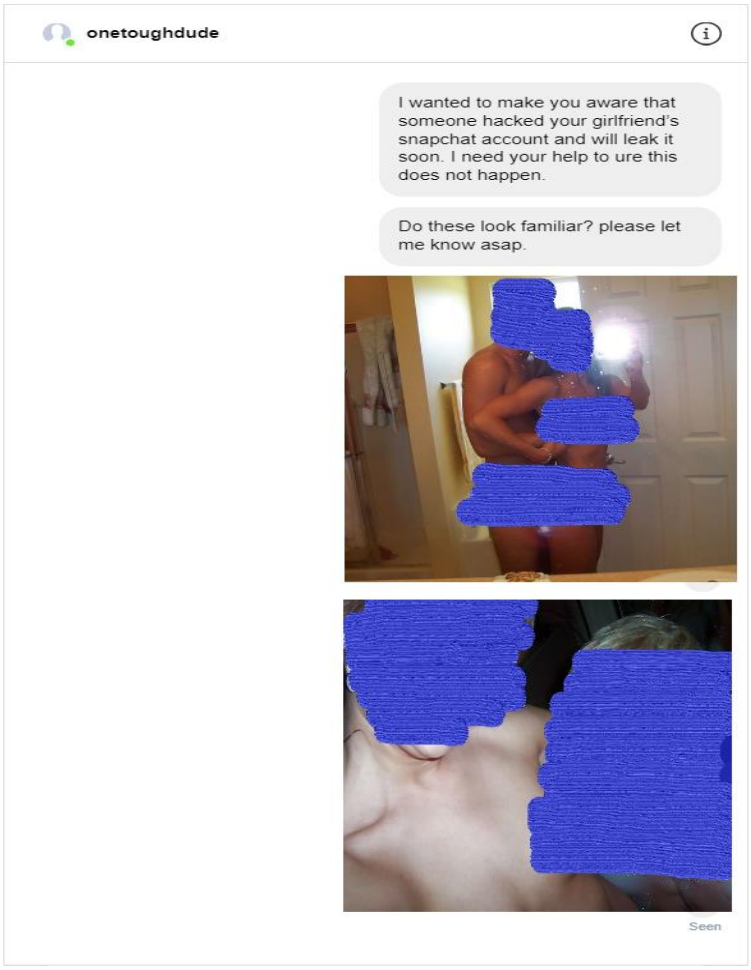
Mensaje por Instagram de Waithe hacia la víctima 6.



Mensaje de Instagram de parte de una cuenta falsa que presenta una foto que está en posesión de Waithe, pero utilizada para propósitos de acosar la víctima 6, a la cual le pertenece la foto.

Figura 14

Mensaje por Instagram de Waithe hacia el novio de la víctima 6.



Mensaje enviado por una cuenta falsa creada por Waithe, hacia el novio de la víctima 6.

Evidencia que demuestra el acoso extenso y agresivo, particularmente hacia la víctima 6.

Cadena de Custodia

Primer evento:

Descripción del evento: USB Lexar JumpDrive M45 64 GB entregado por Adam W. Deitch, recibido por Jonathan W. Calderas Mirabal en Forensic Investigation Solutions.

Evento verificado por: investigador Jonathan W. Calderas Mirabal y fiscal Adam W. Deitch

 # de evidencia: SW-05-23-2021

Fecha de comienzo: 1 de junio de 2021 - 8:00 AM

Fecha de terminación: 1 de junio de 2021 - 8:30 AM

Lugar de origen: Oficina del fiscal en el Distrito de Massachusetts

Destino: Laboratorio en Forensic Investigation Solutions

Segundo evento:

Descripción del evento: Creación de caso y asignación de evidencia.

Evento verificado por: Jonathan W. Calderas Mirabal.

 # de evidencia: evidencia SW-05-23-2021 asignada al caso USvSW-05-23-2021

Fecha de comienzo: 1 de junio de 2021 - 9:00 AM

Fecha de terminación: 1 de junio de 2021 - 9:30 AM

Lugar de origen: laboratorio en Forensic Investigation Solutions

Destino: laboratorio en Forensic Investigation Solutions

Tercer evento:

Descripción del evento: Comienzo de duplicación y luego preservación.

Evento verificado por: Jonathan W. Calderas Mirabal

 # de evidencia: evidencia SW-05-23-2021 asignada al caso USvSW-05-23-2021

Fecha de comienzo: 1 de junio de 2021 - 10:30 AM

Fecha de terminación: 4 de junio de 2021 - 9:00 AM

Lugar de origen: laboratorio en Forensic Investigation Solutions

Destino: laboratorio en Forensic Investigation Solutions

Cuarto evento:

Descripción del evento: Comienzo de análisis de la data.

Evento verificado por: Jonathan W. Calderas Mirabal

 # de evidencia: evidencia SW-05-23-2021 asignada al caso USvSW-05-23-2021

Fecha de comienzo: 4 de junio de 2021 - 10:00 AM

Fecha de terminación: 7 de junio de 2021 - 10:00 AM

Lugar de origen: laboratorio en Forensic Investigation Solutions

Destino: laboratorio en Forensic Investigation Solutions

Quinto evento:

Descripción del evento: Comienzo de revisión de resultados obtenidos.

Evento verificado por: Jonathan W. Calderas Mirabal

 # de evidencia: evidencia SW-05-23-2021 asignada al caso USvSW-05-23-2021

Fecha de comienzo: 7 de junio de 2021 - 10:30 AM

Fecha de terminación: 7 de junio de 2021 - 7:00 PM

Lugar de origen: laboratorio en Forensic Investigation Solutions

Destino: laboratorio en Forensic Investigation Solutions

Sexto evento:

Descripción del evento: Creación del informe. Fue entregado a Adam W. Deitch por el investigador Jonathan W. Calderas Mirabal.

Evento verificado por: investigador Jonathan W. Calderas Mirabal y fiscal Adam W. Deitch

 # de evidencia: reporte de evidencia SW-05-23-2021 asignada al caso USvSW-05-23-2021

Fecha de comienzo: 8 de junio de 2021 - 8:00 AM

Fecha de terminación: 8 de junio de 2021 - 1:00 PM

Lugar de origen: laboratorio en Forensic Investigation Solutions

Destino: Oficina del fiscal en el Distrito de Massachusetts

Séptimo evento:

Descripción del evento: Devolución de la evidencia USB Lexar JumpDrive M45 64 GB hacia el fiscal Adam W. Deitch. Fue entregada por el investigador Jonathan W. Calderas Mirabal.

Evento verificado por: Jonathan W. Calderas Mirabal y fiscal Adam W. Deitch

 # de evidencia: evidencia SW-05-23-2021 asignada al caso USvSW-05-23-2021

Fecha de comienzo: 8 de junio de 2021 - 1:30 PM

Fecha de terminación: 8 de junio de 2021 - 1:40 PM

Lugar de origen: Forensic Investigation Solutions

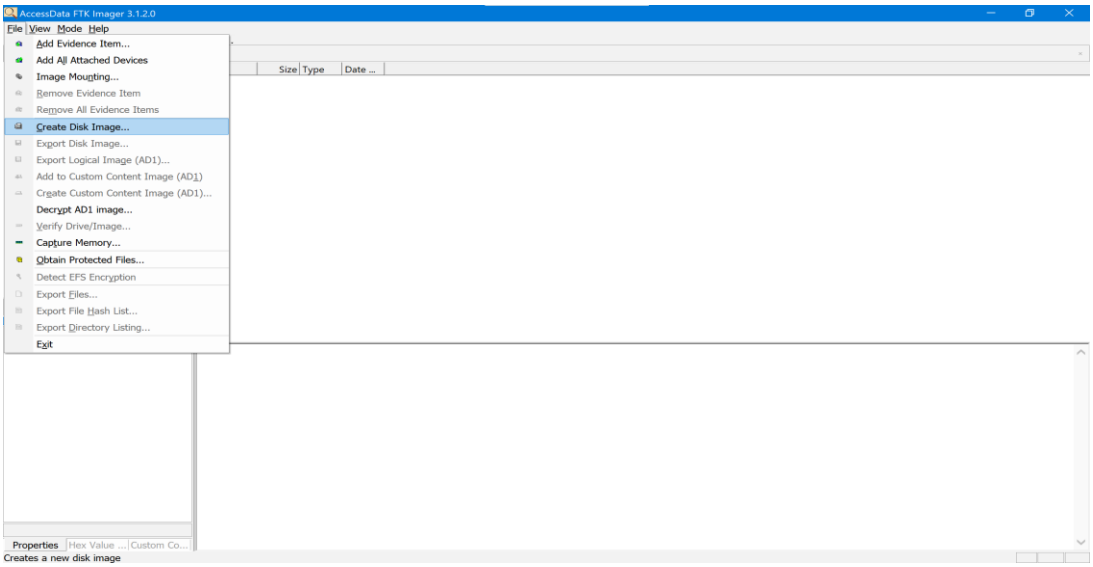
Destino: Oficina del fiscal en el Distrito de Massachusetts

Procedimiento

Para realizar una investigación sensitiva, es muy importante utilizar las herramientas correctas que han sido aprobadas para su uso por las entidades gubernamentales. Una vez entregada la evidencia SW-05-23-2021 a Forensic Investigation Solutions se comienza su duplicación. Se utilizó la herramienta de AccessData FTK Imager para crear una imagen idéntica y exacta a la evidencia entregada. Luego se comienza la etapa de análisis, obtención de resultados, y revisión de resultados. se utiliza la herramienta de AccessData FTK Imager para la examinación confiada de la imagen creada.

Figura 15

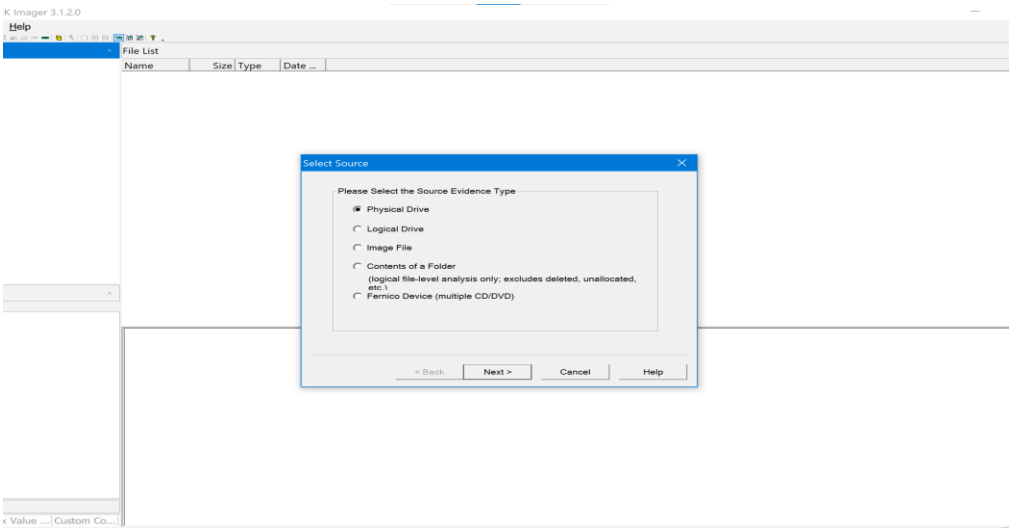
Utilización de FTK Imager para la creación de imagen duplicada de evidencia.



Se selecciona la opción de *Create Disk Image* para comenzar.

Figura 16

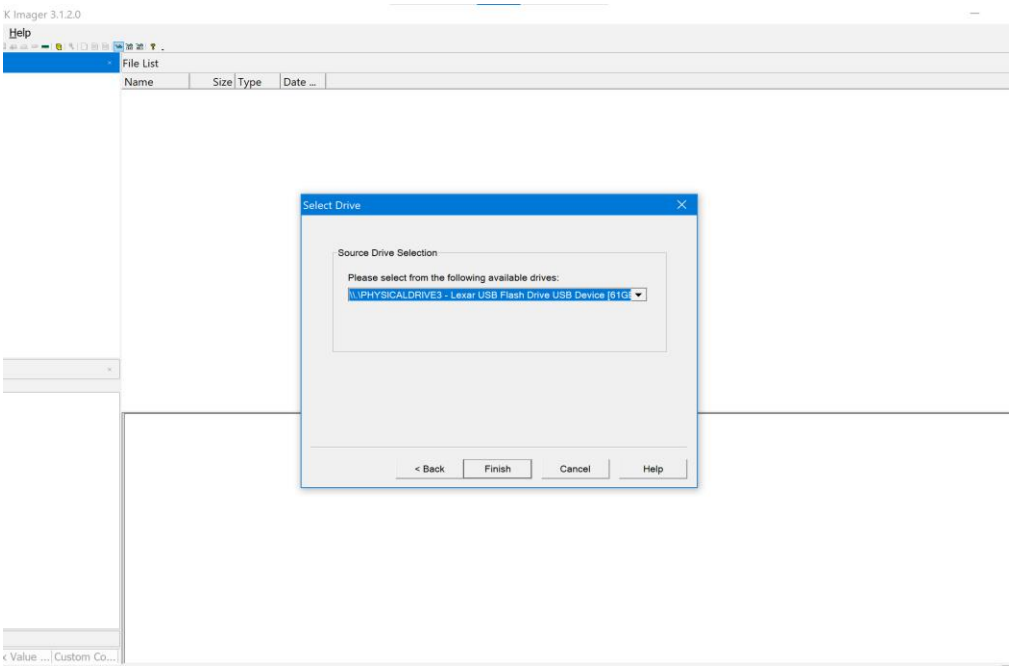
Selección del tipo de fuente.



Se procede a seleccionar el tipo de fuente de la evidencia.

Figura 17

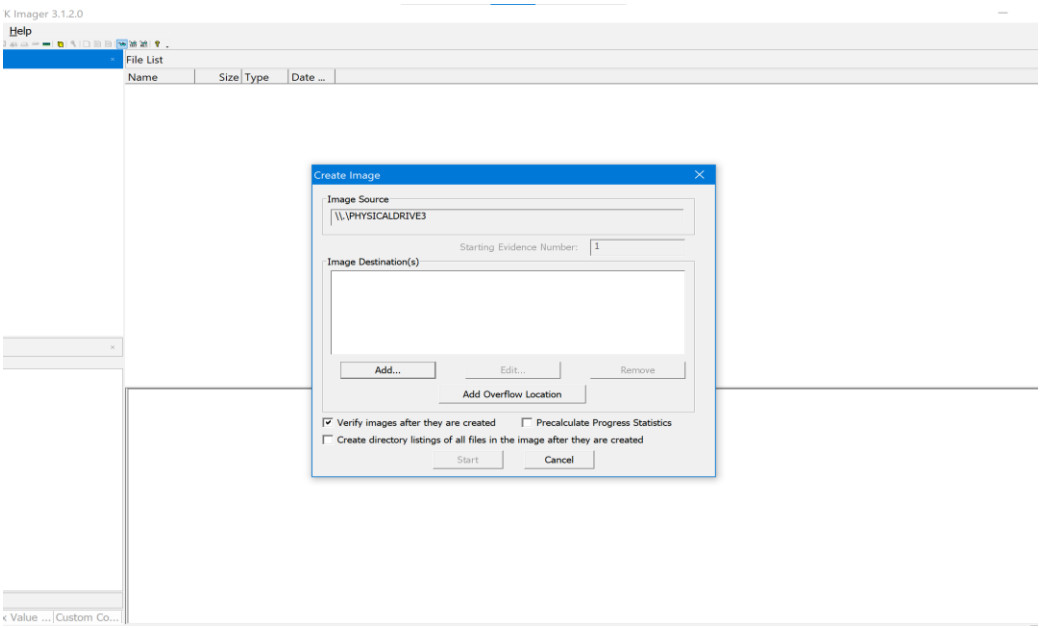
Selección del disco USB Lexar JumpDrive M45 64 GB.



Se selecciona el disco USB provisto por Adam W. Deitch.

Figura 18

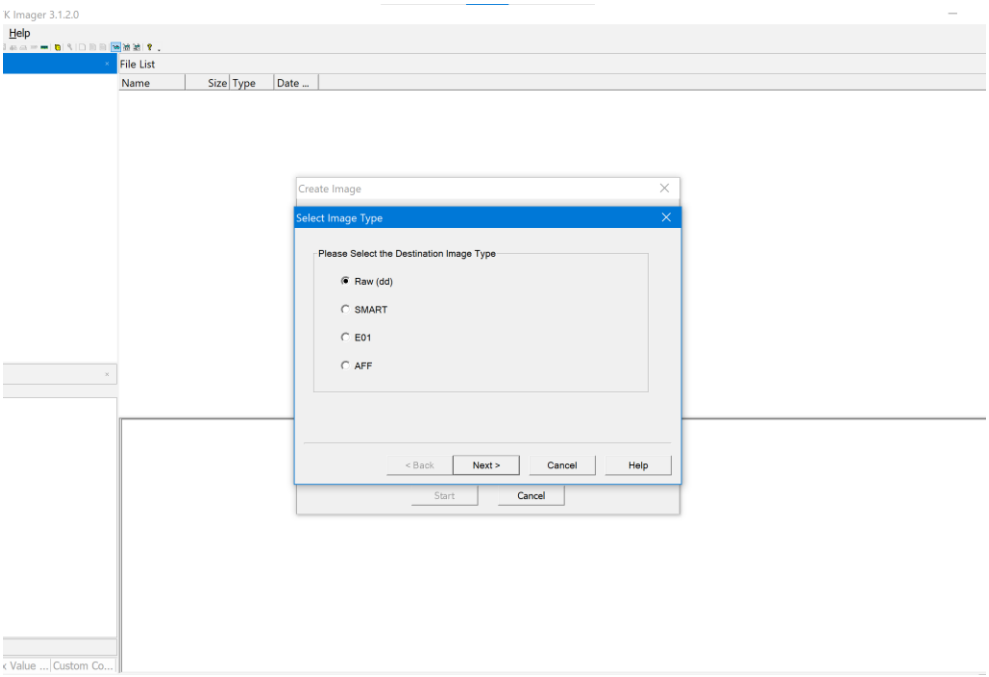
Selección del destino en donde se crea la imagen duplicada.



Se selecciona *Add…* para comenzar la selección del destino en donde se creará la imagen.

Figura 19

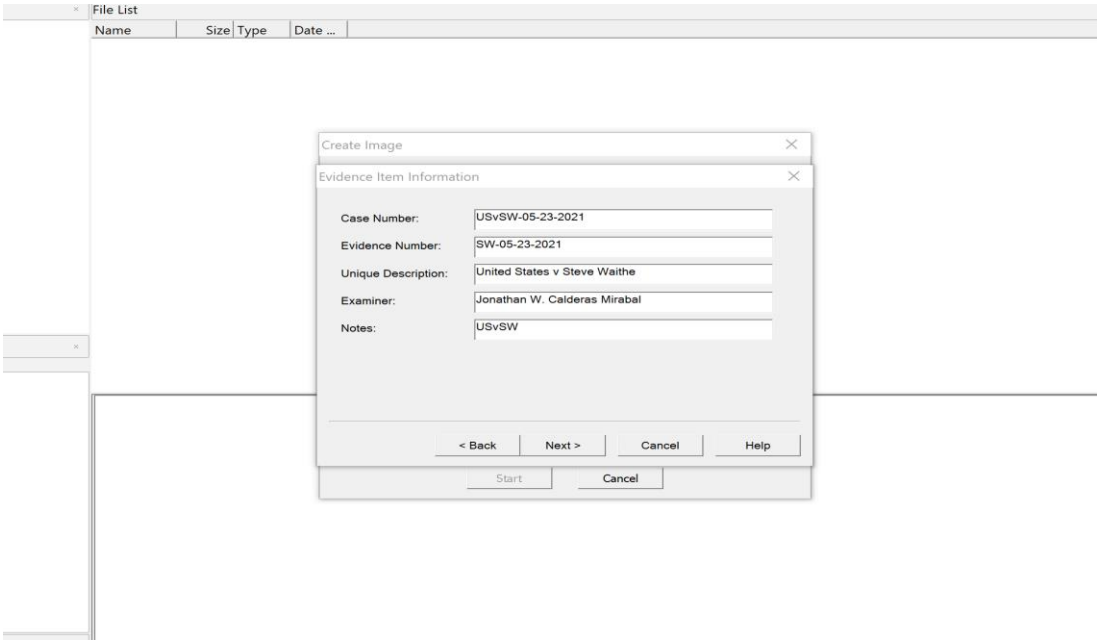
Selección de formato de la imagen.



Se selecciona la extensión formato para la imagen. Raw (dd) es el preferido por FTK Imager.

Figura 20

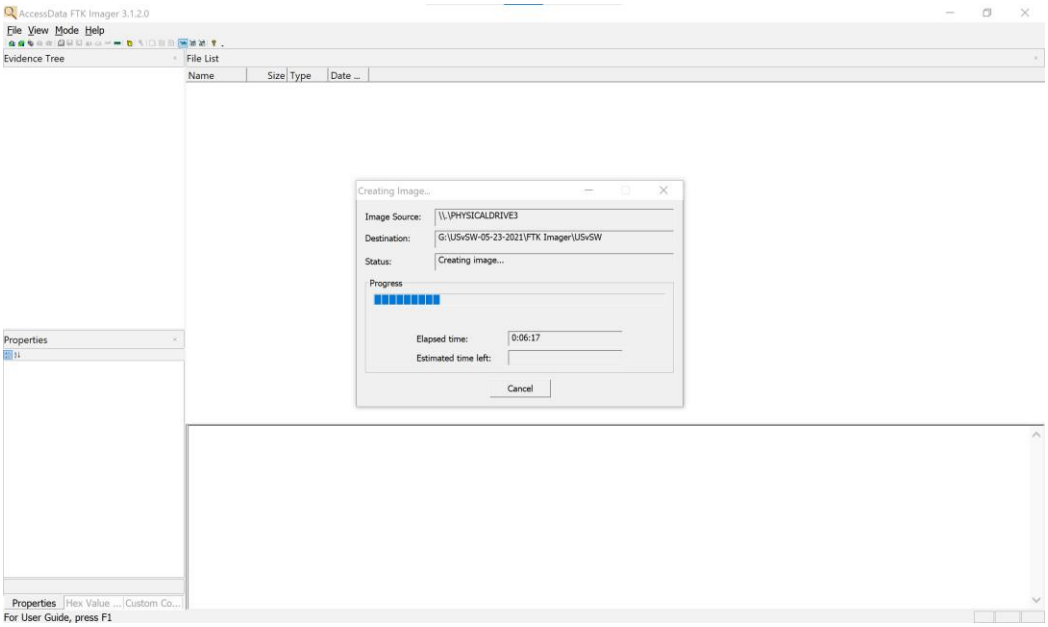
Creación del caso.



Se procede a la próxima pantalla en donde se proveen los detalles de la imagen creada.

Figura 21

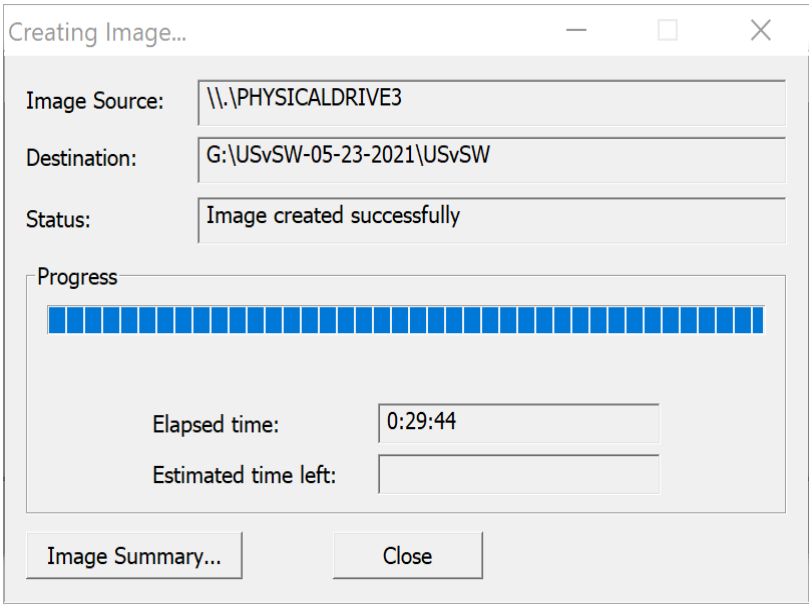
Fuente, destino, y progreso de la imagen duplicada a crear.



Luego, se presiona *Finish* y comienza la duplicación de la evidencia en el destino escogido.

Figura 22

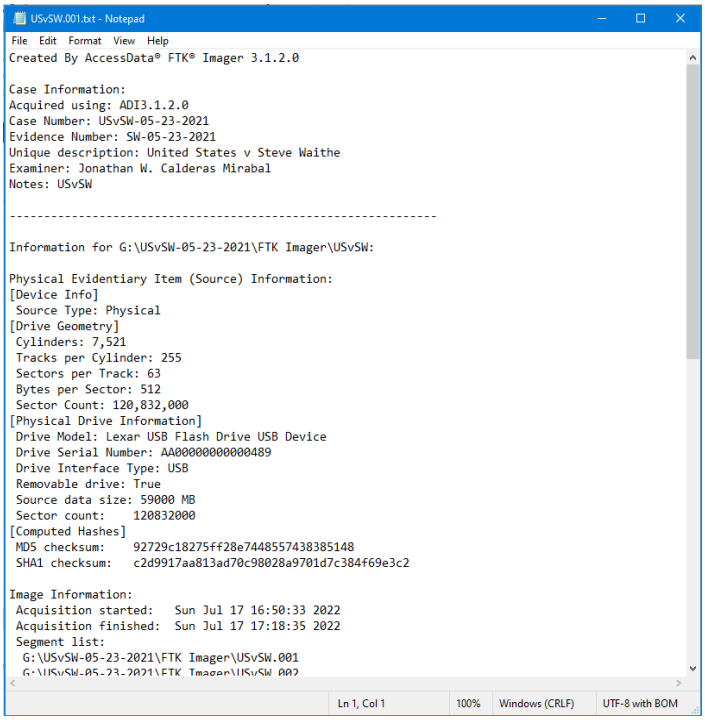
Creación de imagen con éxito.



Creación de la imagen ha sido creada con éxito.

Figura 23

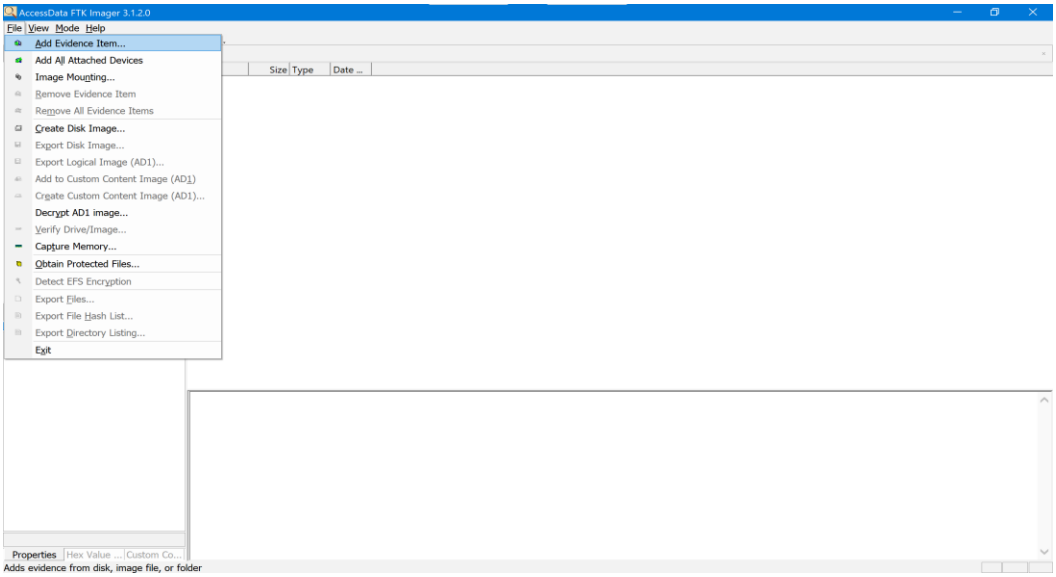
Detalles de la imagen creada.



Evidencia de la creación de la imagen.

Figura 24

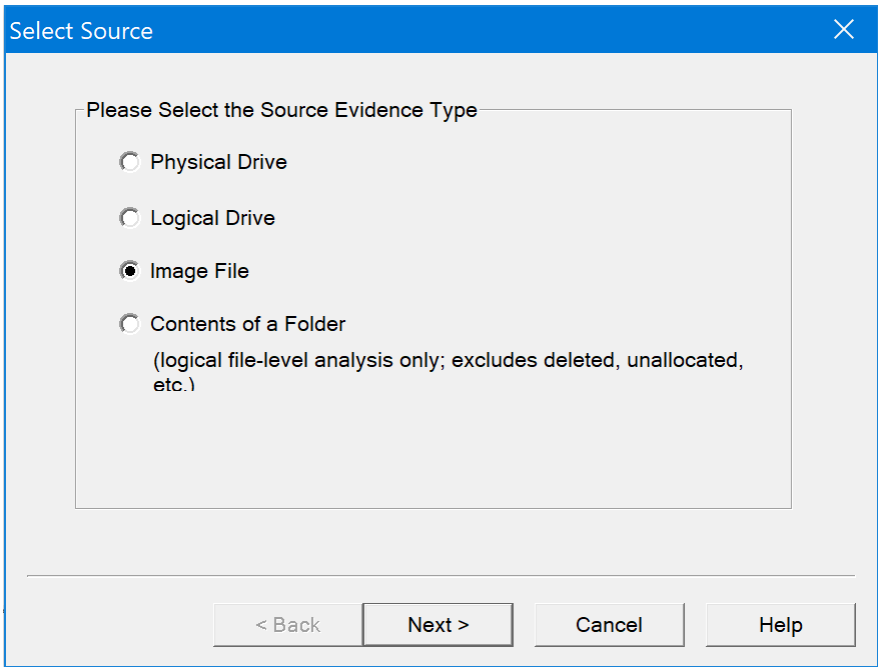
Añadiendo la imagen que se acaba de crear en FTK Imager para investigarla.



Se selecciona *Add Evidence Item…* para comenzar la montura de la evidencia.

Figura 25

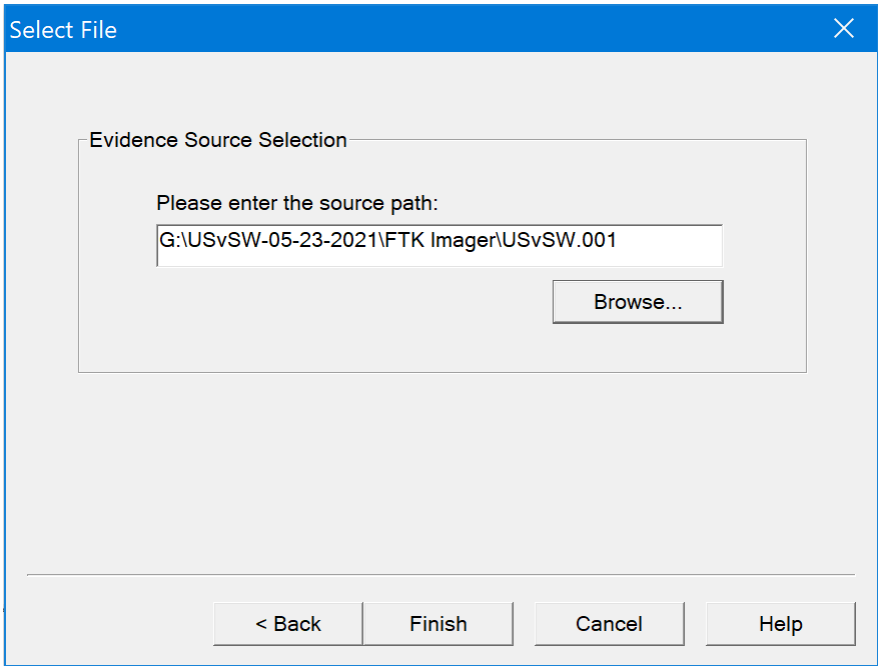
Se escoge el tipo de imagen.



Selección de *Image File* significa que se montará un archivo de tipo imagen.

Figura 26

Fuente de la imagen a analizar.



Se selecciona la Fuente o localización en donde se encuentra la imagen y se presiona *Finish*.

En las próximas figuras 27 – 34, se ven conversaciones de Instagram por medio de archivos *logs* que mantienen un récord de todas las conversaciones realizadas por la aplicación de Instagram en la computadora. Se logra entrando en el disco Windows (C) que es directorio padre de todo el sistema operativo. Luego se procede al directorio de Program Files que contiene archivos relacionados a las aplicaciones instaladas, y se localiza el *folder* de Instagram para investigar sus contenidos. Se encuentra una serie de archivos de tipo *log* que contienen la fecha en que se grabó y una codificación única. Todas las figuras 27 -34 se encuentran en el mismo directorio.

Figura 27

Archivo (log) que muestra una conversación en Instagram con la víctima 1.

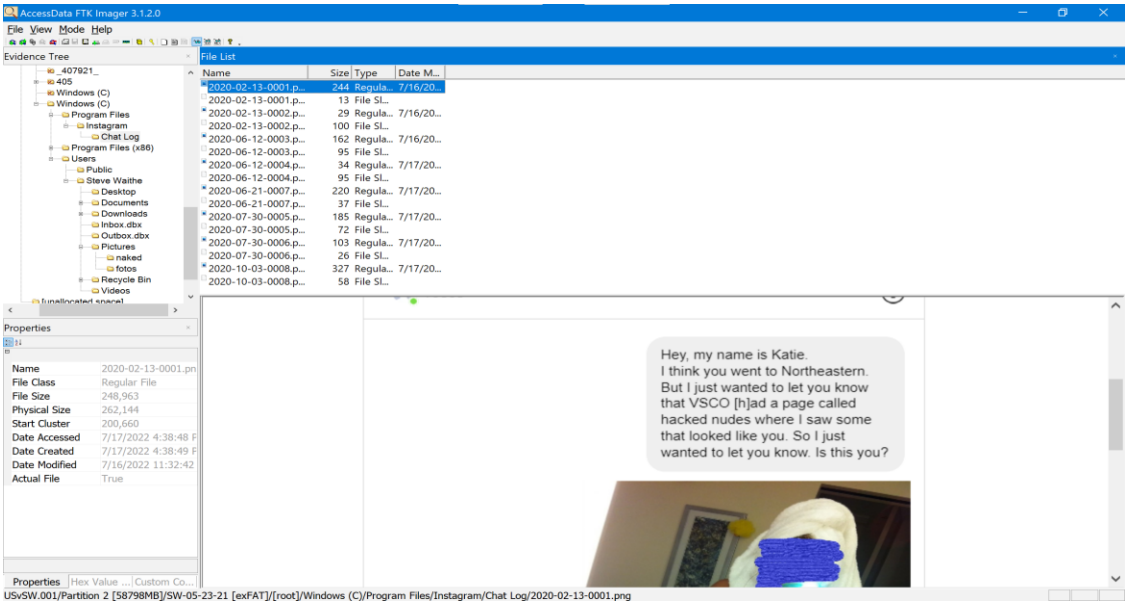
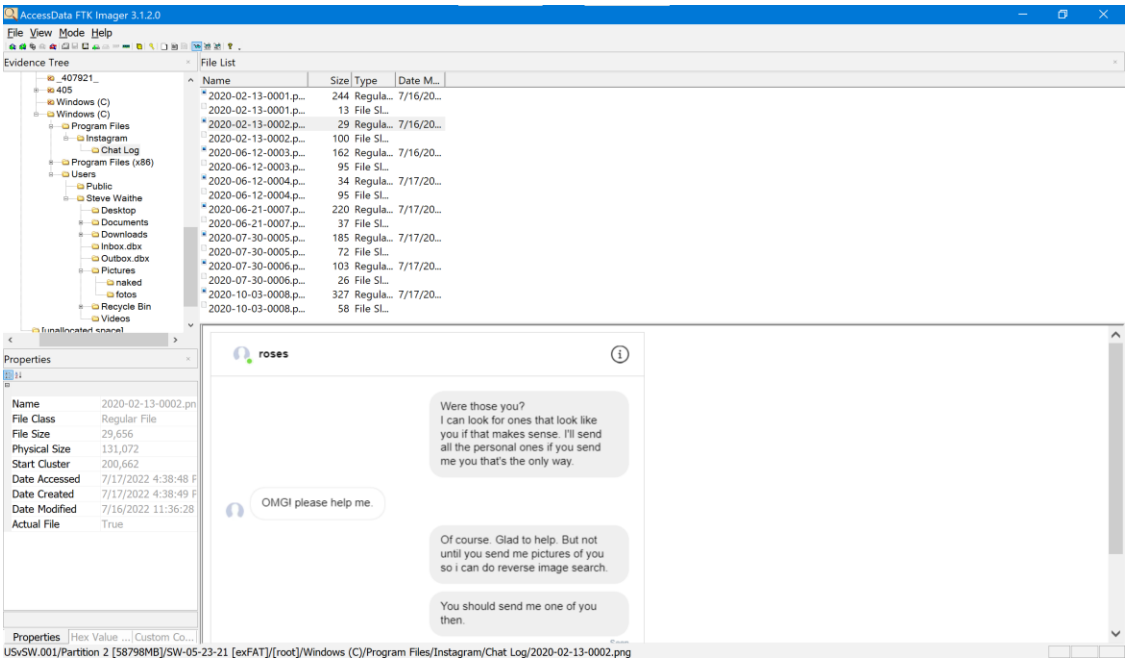


Figura muestra una conversación entre una cuenta falsa de Instagram, la víctima, y fotos sensitivas de la víctima, pero en posesión de Waithe.

Figura 28

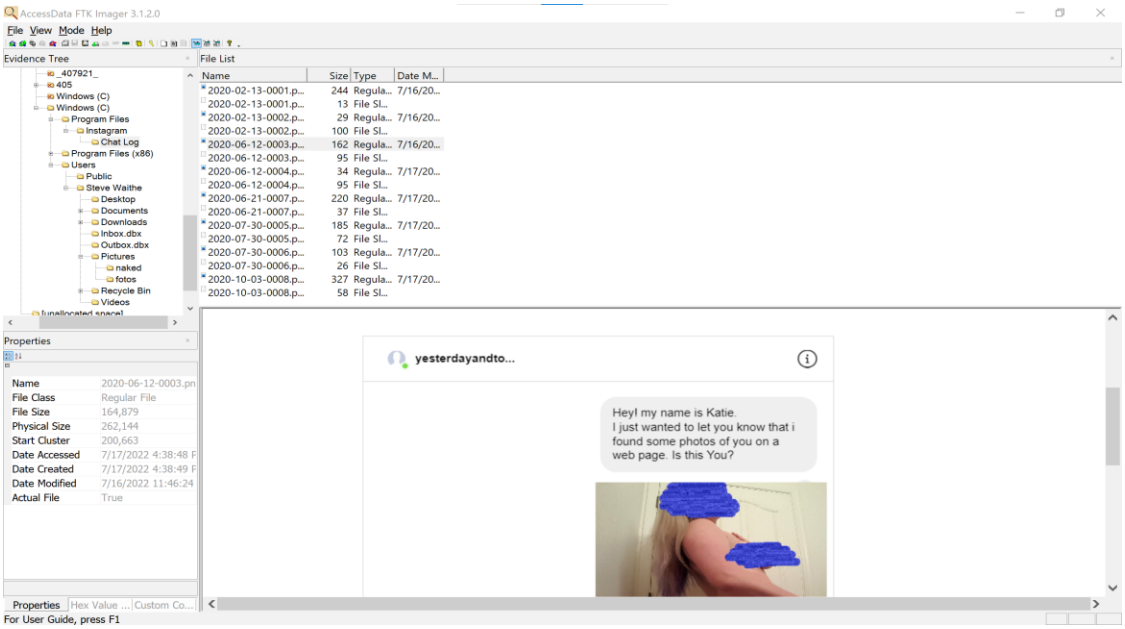
Continuación de la conversación el Instagram con la víctima 1.



Se muestra una conversación depredadora.

Figura 29

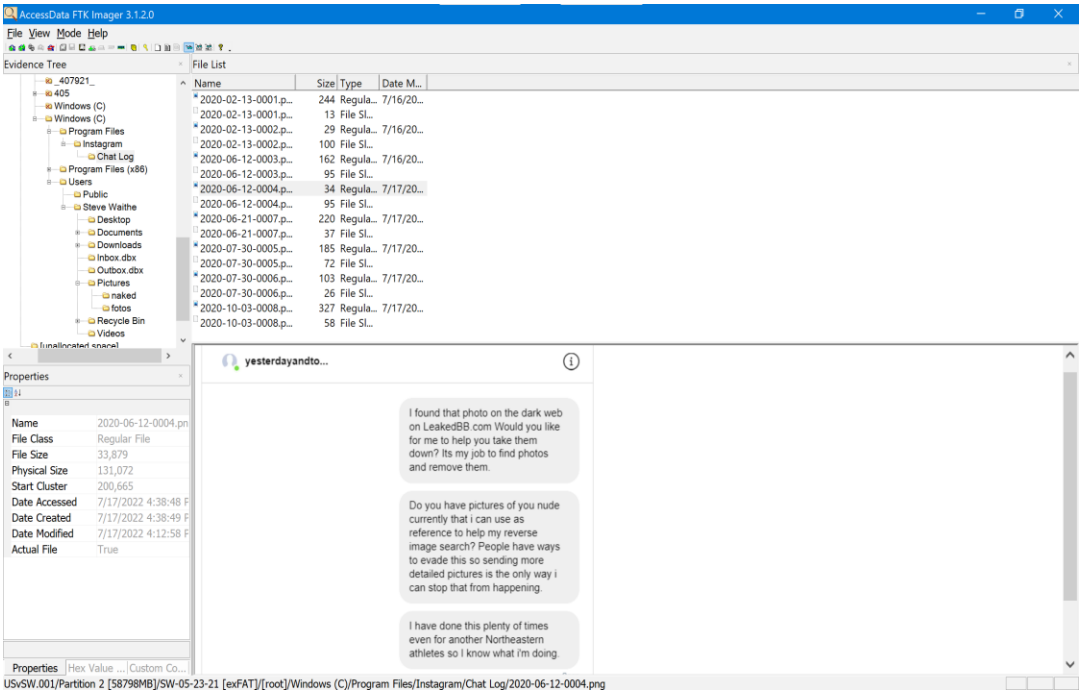
Conversación en Instagram con la víctima 2.



Conversación que demuestra el mismo comportamiento de la víctima 1.

Figura 30

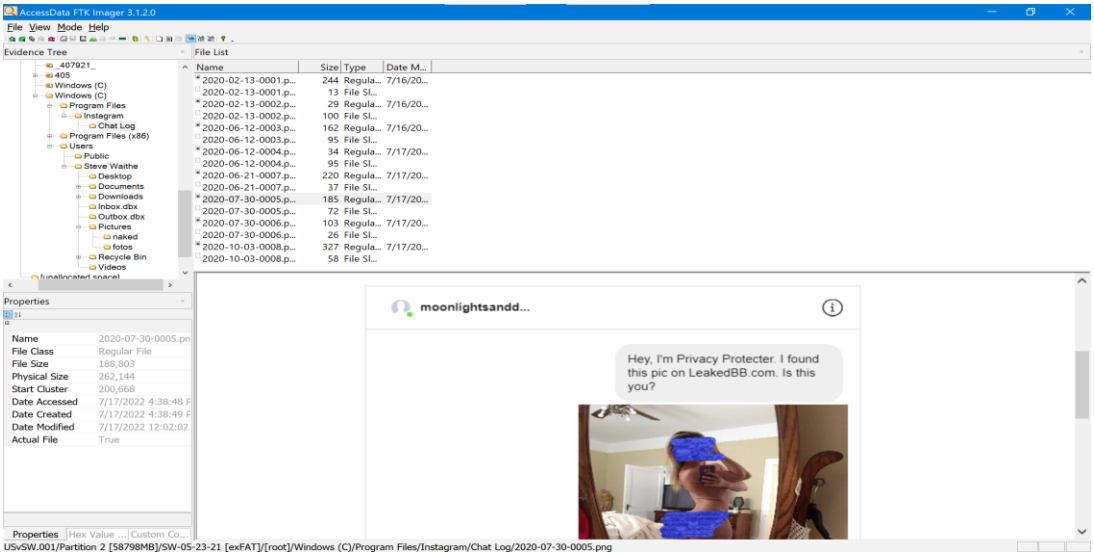
Continuación con el acoso con la víctima 2.



Se continua el patrón de acoso con gran cantidad de mensajes agresivos.

Figura 31

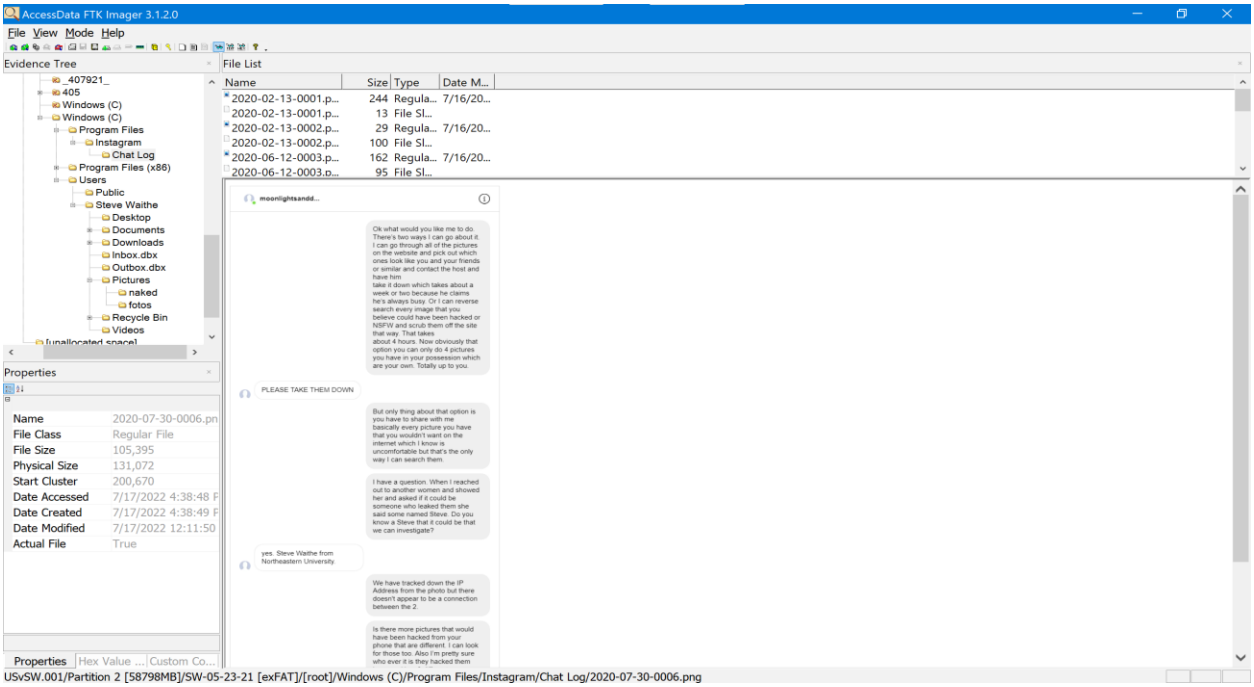
Acoso de la víctima 5.



Waithe continúa contactando víctimas de las cuales se había robado fotos sensitivas cuando laboraba en Northeastern Univesity en Boston.

Figura 32

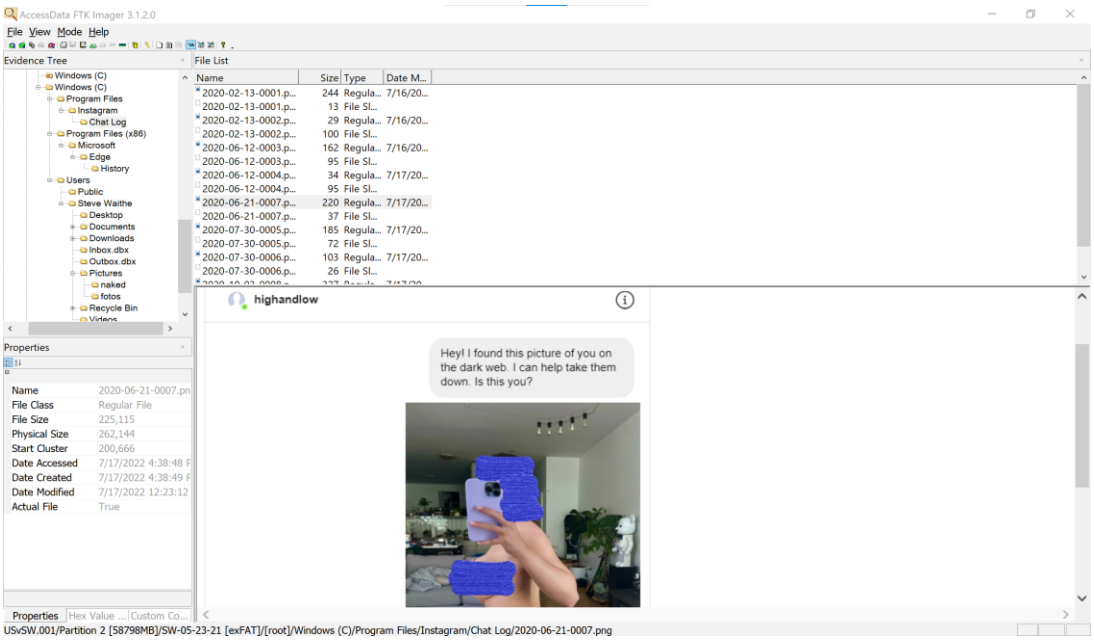
Continuación de acoso de la víctima 5.



Se nota una conversación más viva que las demás, pero aun la víctima no cae en el esquema.

Figura 33

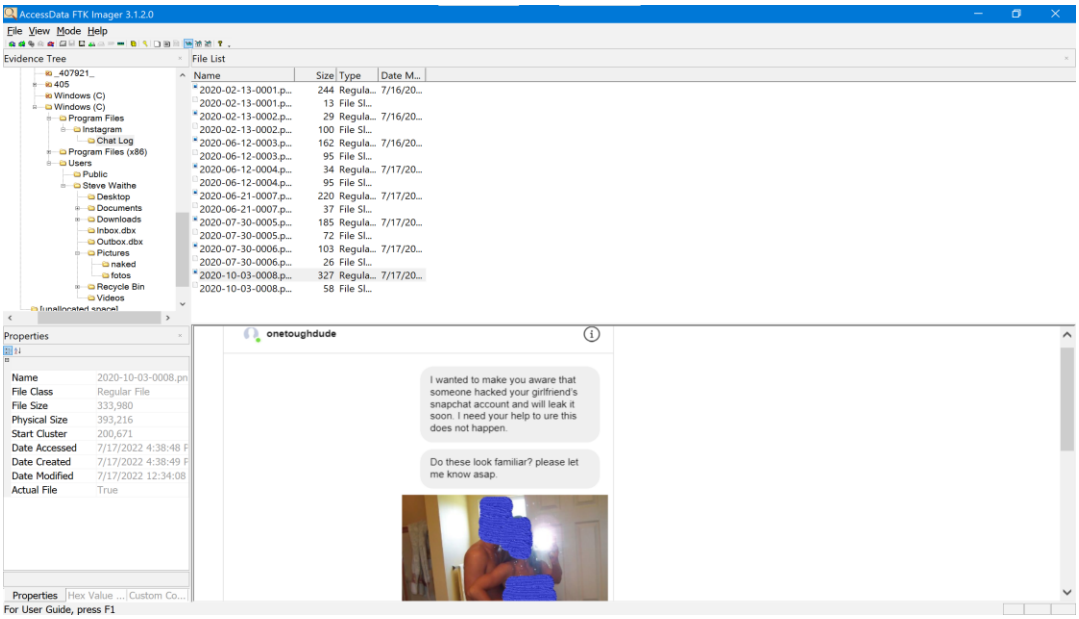
Acoso de la víctima 6.



Se demuestra que Waithe mantiene el mismo patrón de conversación con la víctima 6.

Figura 34

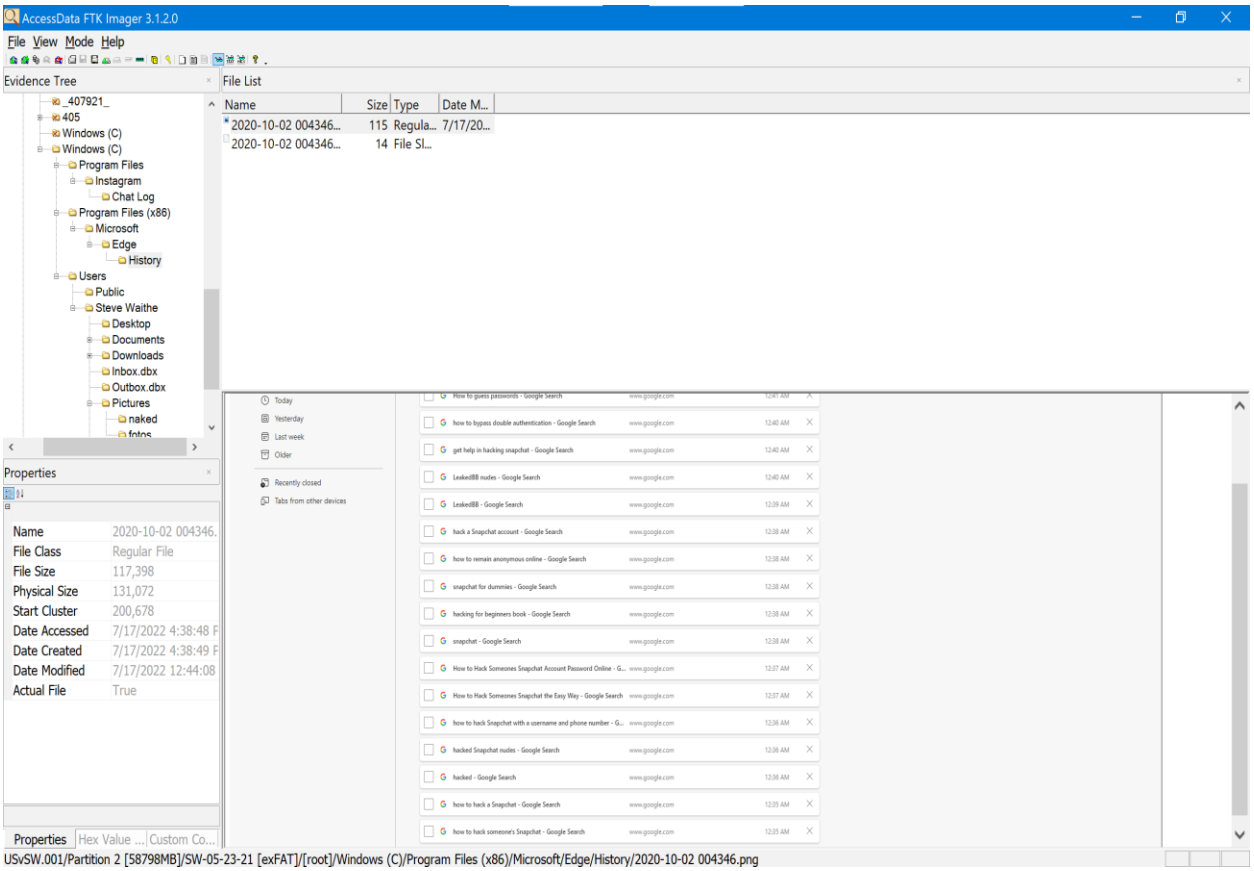
Acoso al novio de la víctima 6.



Waithe logra robar fotos sensitivas en la cuenta de Snapchat *hackeada* de la víctima 6 y las utiliza para acosar al novio de la víctima 6.

Figura 35

Una imagen encontrada en la data del navegador Edge.

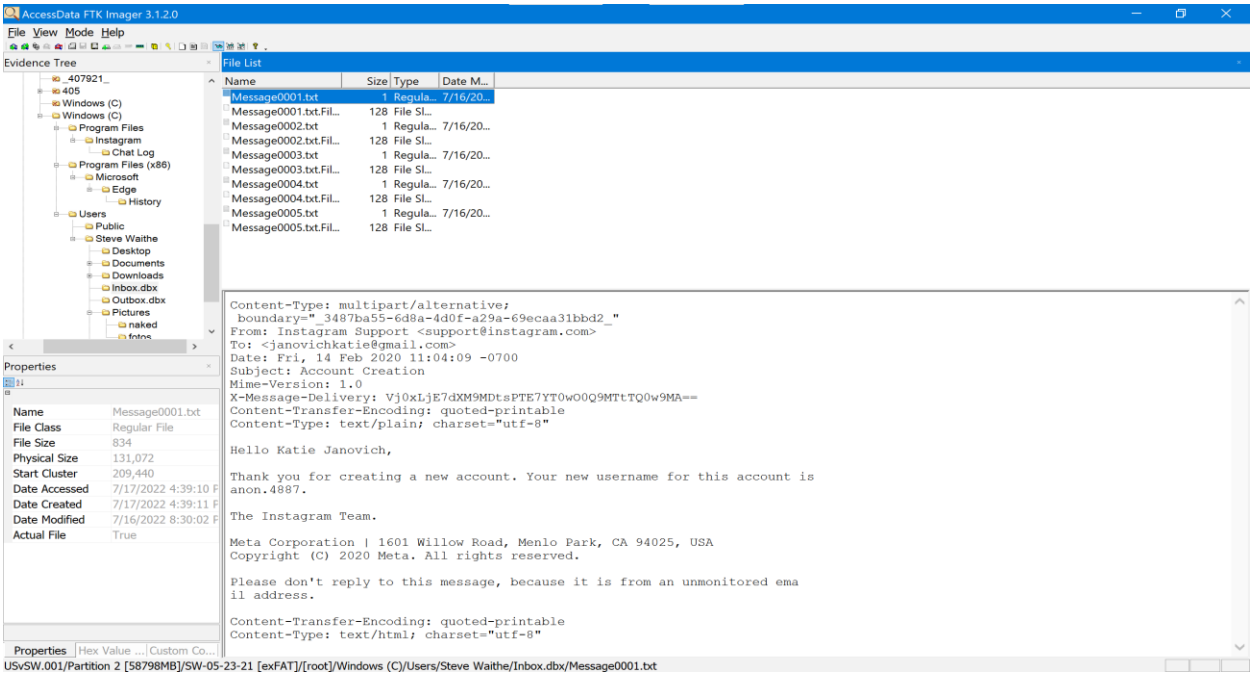


Se procede al archive de Program Files (x86) que es muy parecido al investigado anteriormente de Program Files. Se logra conseguir todos los archivos relacionados a la aplicación de navegador web Edge. En ese mismo archivo, se logró conseguir un *snapshot* o una imagen en un tiempo determinado, enseñando el historial que realizó el acusado en 2 de octubre de 2020.

En las próximas figuras 36 – 38, se muestran evidencia de comunicaciones entre Instagram y correos electrónicos vinculados a Waithe. Se procede a entrar en el *folder* de Users dentro de Windows (C). Se entra al usuario de Steve Waithe y se encuentra en el archivo de Inbox correos electronicos en relación con el uso de cuentas falsas en Instagram. También, en las figuras 39 y 40 se encuentran varios correos electrónicos en el *folder* Outbox personificando a personas falsas para obtener más fotos comprometedoras.

Figura 36

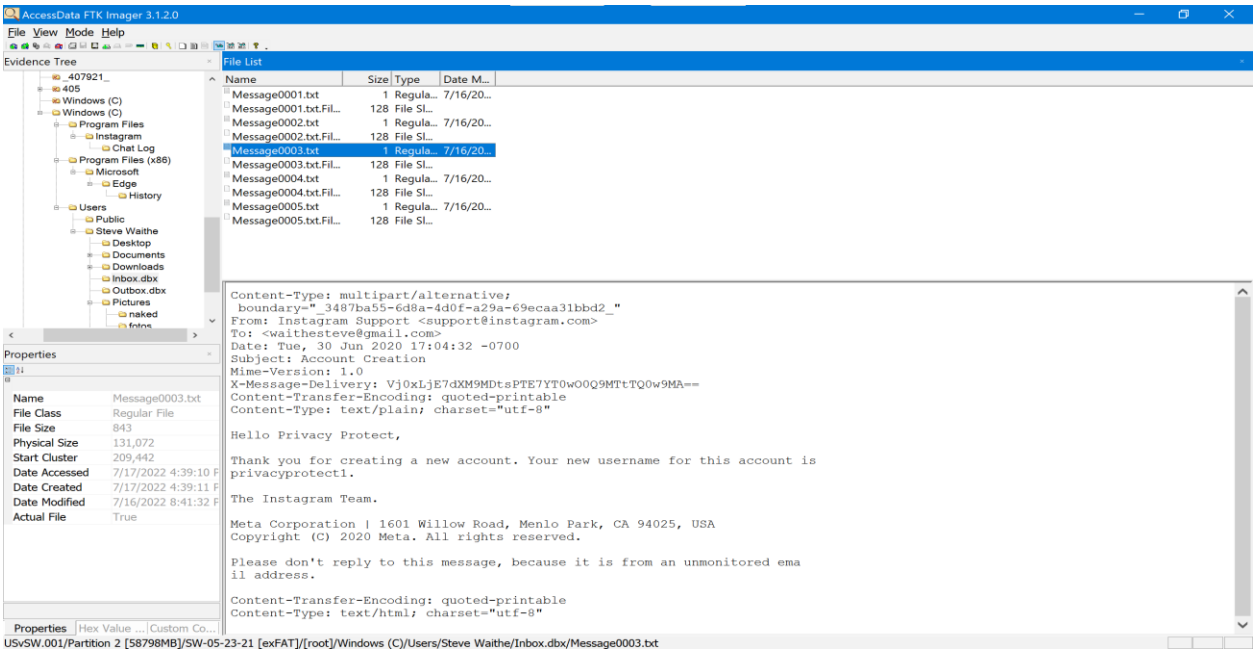
Correo electrónico enviado por Instagram hacia Waithe.



Comunicación con Instagram en relación con una cuenta asociada al acoso cibernético

Figura 37

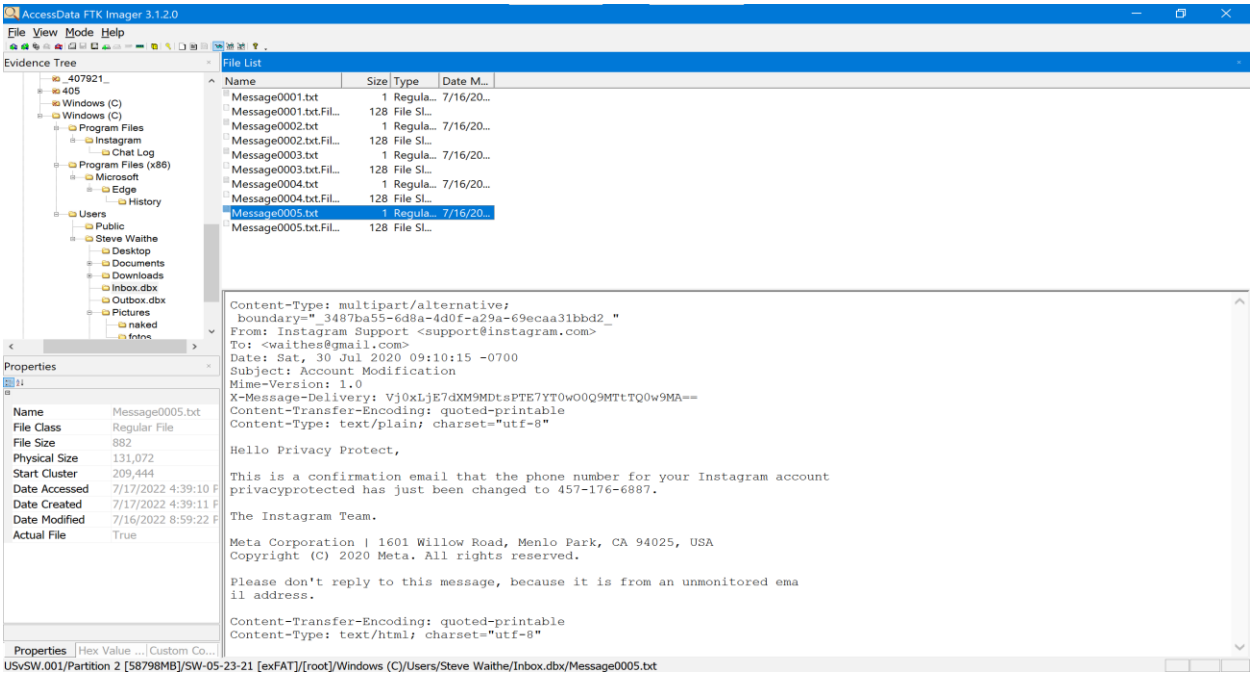
Correo electrónico de parte de Instagram en respecto a la creación de una cuenta en Instagram.



Comunicación con Instagram sobre la creación de una cuenta asociada al acoso.

Figura 38

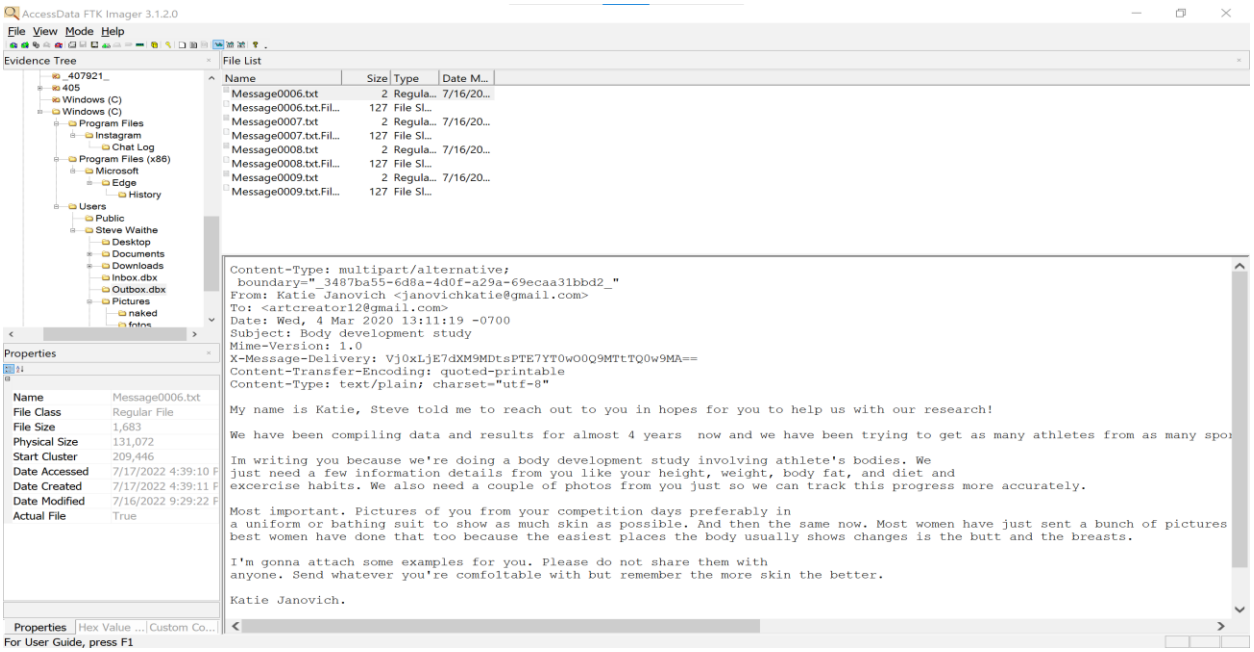
Cambio de número telefónico de una cuenta relacionada al acoso, al número móvil de Waithe.



Comunicación con Instagram.

Figura 39

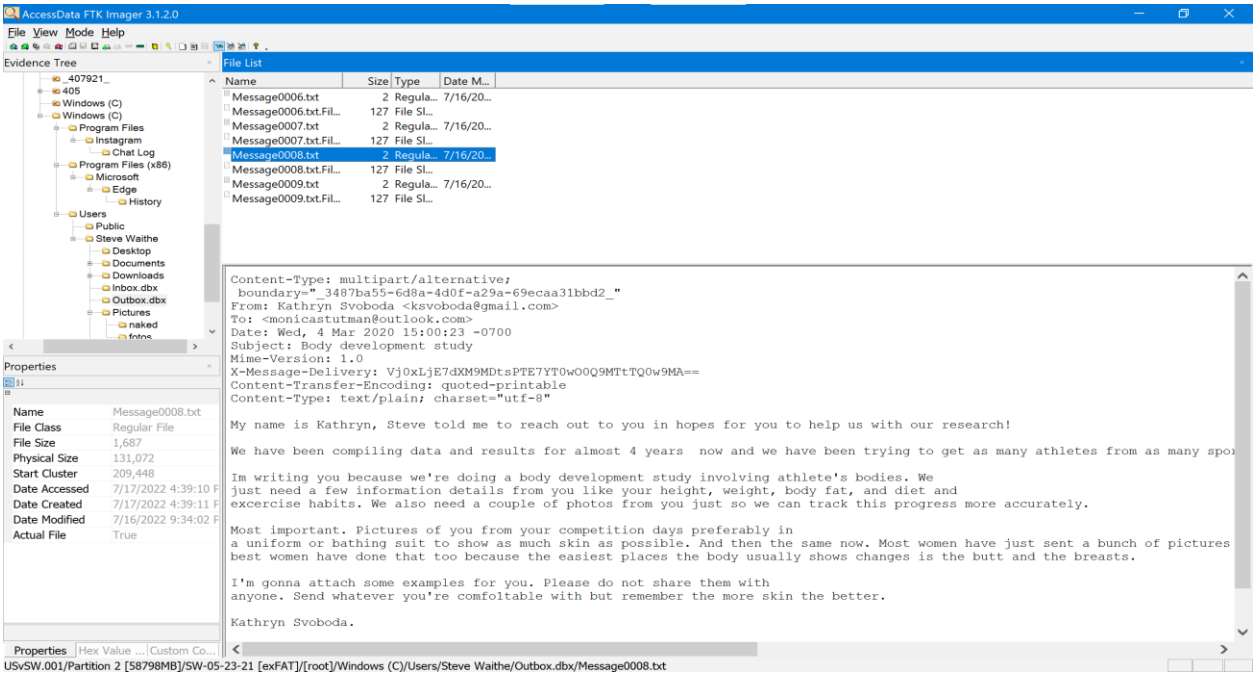
Correo electrónico fraudulento solicitando fotos sensitivas.



Personificación fraudulenta de Katie Janovich.

Figura 40

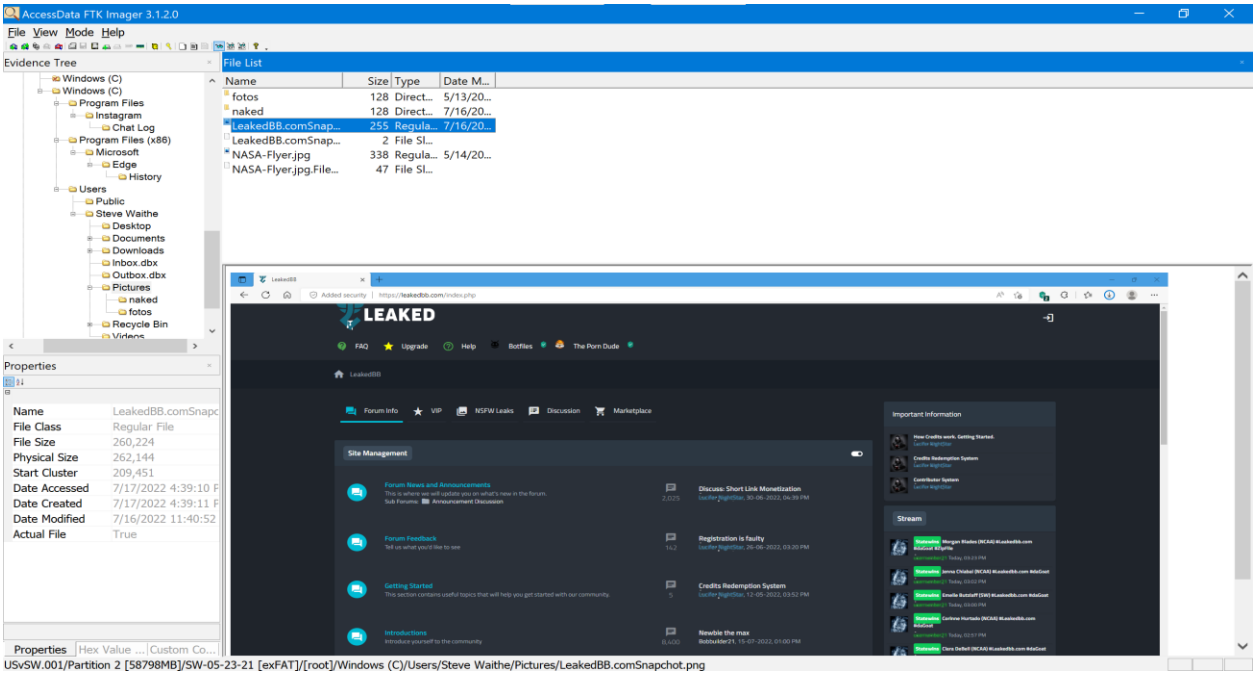
Otro correo electrónico fraudulento bajo el mando del acusado en búsqueda de fotos sensitivas.



Personificación fraudulenta de Kathryn Svoboda.

Figura 41

Screenshot encontrado donde hace referencia a la página LeadkedBB.



Se consigue evidencia de *screenshot* de una página web titulada LeakedBB. LeakedBB es la página web en donde Waithe luego ofreció las fotos obtenidas como producto del esquema de fraude y acoso cibernético. Se consiguió entrando al *folder* Windows (C), Users, Steve Waithe, Pictures.

Conclusión

De acuerdo con la investigación exhaustiva y completa que se ha hecho al dispositivo USB Lexar JumpDrive M45 entregado por Adam W. Deitch, se determina que la evidencia encontrada es indicadora de que el acusado Steve Waithe realmente cometió los delitos al cual fue acusado. Luego de haber identificado las víctimas, las cuales han permanecido anónimas en esta investigación, se encuentran evidencia de conversaciones en Instagram en donde se presentan las fotos de las víctimas y actitudes agresivas y depredadoras de parte de Waithe (Véase las figuras 27 - 34). En adición, se encuentra evidencia mediante la extracción de correos electrónicos de la computadora de Waithe, de la creación de las cuentas de Instagram que son asociadas y reportadas por las víctimas (Véase las figuras 36 - 38). La investigación finalizada, proveyó resultados de confirmación de fotos de las víctimas en la posesión de Waithe (Véase la figura 6). La posesión de estas fotos no fue autorizada por las víctimas.

Como investigador principal de Forensic Investigation Solutions, con más de 10 años de experiencia en el área de la forense, programación, auditoría, y seguridad, concluyo que la evidencia es certificadora de la culpabilidad de Steve Waithe.

SECCIÓN V: DISCUSIÓN DEL CASO

Según el documento del pliego acusatorio, se radican 12 cargos de fraude electrónico, 1 cargo de acoso cibernético, y 2 cargos de fraude de computadoras. Según los resultados de los análisis realizados al disco duro de la computadora de Steve Waithe, se concluye que el mismo Waithe sostuvo múltiples cuentas de Instagram en el cual personifica agentes de seguridad encargados de proteger la privacidad en la internet (Véase las figuras 36 - 38) y 2 mujeres que solicitan fotos sensitivas para llevar a cabo un estudio vía correo electrónico (Véase las figuras 39 - 40). Todo comienza bajo unas premisas falsas y continúa escalando. En acorde con el cargo de fraude electrónico. Se utilizan estas cuentas falsas para seguir solicitando más fotos.

Los resultados de esta investigación demuestran que Steve Waithe presentó intenciones de utilizar las cuentas y perfiles de personas falsificadas para continuar su esquema. Basada en la evidencia, las víctimas en Instagram no cayeron en el esquema. Por lo que luego, sigue creando más cuentas fraudulentas para lograr establecer comunicación con las víctimas. No solo esto, sino que el acusado continúa enviando cientos de mensajes a través de Instagram y correos electrónicos a pesar de que las víctimas no presentan interés en enviar más fotos. Todo finalizando en comportamiento de acoso cibernético. Finalmente, al tener codicia de obtener más y más fotos, busca ayuda en el Internet.

Waithe realiza una seria de búsquedas en el Internet, evidenciado por el historial en el navegador Web (Véase figura 35). Consigue ayuda de una persona extraña en el cual obtiene éxito en *hackear* las cuentas de Snapchat. Conducente al cargo de fraude de computadoras. Se apoya en la evidencia recolectada como producto de esta investigación y se hace la afirmación de que Steve Waithe es culpable de los cargos sometidos.

Según el documento acusatorio y varias entrevistas, todas las víctimas sufrieron daños emocionales. Tales como: ansiedad, depresión, insomnio, humillación, estrés, fatiga, tendencias suicidas, y cambios en personalidades. La víctima 6, en particular, sufrió daños doblemente severos que las otras víctimas ya que el nivel de severidad del acoso cibernético fue más fuerte. Waithe la acosó con más empeño por Instagram, mensajes de textos, y a su novio. Daños causados a todas las víctimas, excepto la 6, son estimados en $50,000 por cada una. Mientras que la víctima 6 es estimado en $110,000 en daños emocionales extremos.

SECCIÓN VI: AUDITORÍA Y PREVENCIÓN

El uso de la tecnología ha crecido substancialmente durante los últimos años. Ha crecido tanto que nosotros dependemos cada vez más y más de la tecnología para los usos diarios. Confiamos tanto, que guardamos información como: usuarios, contraseñas, información bancaria, mensajería, fotos, localizaciones, y más. Esta confiabilidad en la tecnología es un arma de doble filo ya que trae la facilidad del manejo de tanta información que sería casi imposible. Pero, también presenta un riesgo de robo de información sensitiva si esa tecnología cae en las manos equivocadas.

Muchos de los controles tecnológicos diseñados para evitar el robo de información sensitiva están diseñados transparentemente por los mismos vendedores o creadores de tecnología. Sin embargo, hay muchos otros controles que corresponden a cada persona que está en posesión de la tecnología, como lo es un teléfono celular. A continuación, se presentan los hallazgos encontrados en el transcurso de la investigación del caso US v. Steve Waithe, 1:21-cr-10342-PBS (2021) que demuestran lo mencionado, y otros que pensábamos que serían robustos.

A continuación, se presentan los hallazgos encontrados que fueron los factores clave en la realización del esquema de acoso y fraude cibernético. Los hallazgos 1 – 4 son relacionados a fallas de las víctimas y el hallazgo 5 es falla relacionado a la Universidad.

Primer hallazgo:

Condición: Las estudiantes atletas no estuvieron pendientes a lo que hacía Steve Waithe con sus teléfonos celulares. Los teléfonos celulares de hoy día contienen casi toda la información sensitiva en respecto a su dueño/dueña.

Criterio: Las estudiantes atletas debieron estar pendientes a lo que Steve Waithe hacía con sus teléfonos. En otro lado, las estudiantes debieron mejor no prestar el teléfono personal y solicitar que se grabaran sus rendimientos con una cámara oficial de la Universidad.

Causa: La condición fue causada por la ausencia en los controles personales sobre el cuido de la información sensitiva en los teléfonos personales.

Efecto: El impacto de la ausencia en los controles de esta condición llevó a la pérdida o robo de información sensitiva, principalmente fotos de naturaleza sensitiva y personal. También hubo robo de información personal como el número de teléfono, correos electrónicos, y más.

Recomendación: Las estudiantes no deben prestar sus teléfonos personales para ningún motivo, especialmente hacia una persona extraña. Deben siempre estar pendientes en la localización, seguridad bajo contraseña, y el tipo de contenido en sus teléfonos. La Universidad Northeastern debe comprar, proveer, y enforzar el uso de cámaras de grabación específicamente para rendimientos deportivos. La Universidad debe crear y enforzar políticas sobre el uso de teléfonos dentro de la Universidad. La política específicamente le debe prohibir a los facultativos el uso completo de celulares proveniente de otra persona que no sea el mismo facultativo.

Segundo hallazgo:

Condición: Al menos una víctima, la víctima 6, decidió guardar información sensitiva en el servicio social de Snapchat. La víctima 6 en todo su poder, a sabiendas, y con toda debida autorización guardó fotos comprometedoras en el archivo de *My Eyes Only*. Ese archivo es para guardar fotos o video que se desean guardar bajo seguridad en Snapchat. La finalidad es evitar que se coloquen públicamente.

Criterio: Todo lo que se publica en el internet es prácticamente del dominio público de alguna manera u otra. La víctima 6 debió reconocer que nadie puede ver esas fotos en ese archivo, pero Snapchat nunca describe si ellos mismos tampoco pueden verlas. En otras palabras, Snapchat resguarda la contraseña que salvaguarda ese archivo protegido y no menciona explícitamente si el mismo Snapchat tiene acceso o no (Smart GEN Society, 2021). La víctima debió abstenerse de publicar información personal.

Causa: El problema es causado por una falla en los controles de las víctimas al no leer debidamente los términos de Snapchat.

Efecto: El impacto de esta falla en los controles de la víctima se refleja en el robo de las fotos sensitivas de la víctima por Steve Waithe.

Recomendación: Leer cuidadosamente los términos de uso y la política de privacidad de Snapchat. También se debe reconocer un potencial de *hackeo* de los servicios de Snapchat y la posibilidad de que esa información finalice en manos equivocadas (Norton 360, n.d.). No se debe publicar información extremadamente sensitiva en ningún lado en el internet ya que siempre es propensa a robo, aunque sea protegida (Kidscape, n.d.). Es mejor mantenerlo en almacenamiento local y fuera del dominio del internet.

Tercer hallazgo:

Condición: Las estudiantes atletas víctimas de Waithe no fueron diligentes en comprobar la certificación, autenticidad, o veracidad de los correos electrónicos fraudulentos enviados por el acusado. Resultando en un esquema de *phishing* para escalar el esquema mayor de acoso cibernético.

Criterio: Las víctimas debieron haber hecho su tarea de autenticar de que los correos electrónicos recibidos realmente son provenientes de una fuente legítima y no fraudulenta. Finalizando en el descarte de todos esos correos electrónicos.

Causa: La condición fue causada por ausencia en controles personales de instrucción sobre esquemas populares actuales que son fraudulentos.

Efecto: El efecto de esta condición es que las víctimas cayeron en el esquema tipo *phishing* orquestado por Waithe que proviene de una fuente y premisa falsa que solicita fotos sensitivas. El efecto es que 17 víctimas respondieron y enviaron sobre 350 fotos comprometedoras que terminaron en posesión de Waithe.

Recomendación: Según National Cyber Security Centre (n.d.b) y Norton (2021) las víctimas deben realizar lo siguiente:

- Instalar un programa de antivirus con apoyo para protección en el internet que incluye la filtración de correos electrónicos de tipo *spam*.
- Leer cuidadosamente todos los correos electrónicos (sin presionar algún hipervínculo) y verificar para discrepancias o errores. Los correos electrónicos falsos usualmente contienen errores ortográficos y gramaticales.
- Leer detenidamente y verificar si solicitan y de qué manera solicitan alguna información. De ser de manera agresiva, usualmente son falsos.
- Mantener la contraseña de los correos electrónicos al día, siguiendo las más altas recomendaciones para su creación.
- Evitar responder a la conversación.
- Reportar a las autoridades si se sospecha de fraude *phishing*.

Cuarto hallazgo:

Condición: Las víctimas no fueron diligentes en comprobar la autenticidad de los mensajes de textos fraudulentos enviados por Waithe que solicitan el código de seguridad de la cuenta en Snapchat. Finalizando en *smishing.*

Criterio: Las víctimas debieron haber hecho su tarea de autenticar de que los mensajes de textos recibidos realmente son provenientes del equipo de apoyo de Snapchat. Certificando la efectividad del mecanismo de doble autenticación y deteniendo el *hack* de la cuenta de Snapchat al descartar el mensaje de texto fraudulento.

Causa: La condición fue causada por fallas en controles personales de instrucción sobre esquemas populares actuales como el *phishing* mediante mensajería de texto.

Efecto: El efecto de esta condición es que al menos 1 víctima proveyera su código de seguridad, como consecuencia de la activación de la doble autenticación, a Waithe y la persona ayudándolo a *hacker* la cuenta de Snapchat. Finalmente, Waithe obtiene acceso de la cuenta de la víctima y le roba todas las fotos personales y comprometedoras. Todo para continuar el esquema de acoso cibernético con ayuda de fraude de computadoras.

Recomendación: Según Kaspersky (n.d.) y Norton (2022) las víctimas deben seguir las siguientes recomendaciones:

- Leer detenidamente los mensajes de texto. Los mensajes fraudulentos usualmente contienen errores ortográficos y gramaticales.
- Leer las políticas de uso de los servicios que se posee. Ninguna organización solicita que se le envíe códigos de seguridad por mensaje de texto.
- Nunca responder a un mensaje de texto si parece ser fraudulento.

- Nunca presionar los hipervínculos encontrados dentro del texto.
- Reportar el mensaje al proveedor de servicio telefónico.
- Borrar el mensaje de texto si parece, aunque sea un poco, ser falso.
- De aparentar ser el mensaje de Snapchat, consultar y verificar directamente con la compañía para asegurar si los mensajes son verídicos o falsos.

Quinto hallazgo:

Condición: La Universidad Northeastern en Boston despidió a Waithe en 2019 por una investigación que terminó acusado por acoso sexual. La Universidad de Concordia en Chicago le ofreció trabajo a Waithe en 2019. Se demuestran de una probabilidad alta de que las Universidades están fracasando en su proceso de reclutamiento. No se están realizando las investigaciones necesarias y podrían terminar en casos como este.

Criterio: La Universidad que contrató a Steve Waithe debió hacer sus investigaciones correctamente para poder así evitar la repetición de situaciones como la establecida en este caso.

Causa: La condición fue causada por la falla en los controles de reclutamientos dentro de las Universidades.

Efecto: El efecto de este hallazgo se ve reflejado en la continuación y facilitación del esquema de acoso cibernético orquestado por Waithe ya que tuvo acceso a más víctimas.

Recomendación: Las Universidades deben revisar, solidificar, y hacer cumplir con las políticas y procedimientos de reclutamiento de su facultativo más importantes tal y como lo hace la Universidad Columbia en New York (n.d.):

- Hacer una verificación de antecedentes criminales, registro de ofensas sexuales, educación, y trabajos anteriores.

- Verificación de récord con uso de drogas, automóvil, huellas digitales, y problemas monetarios.

SECCIÓN VII: CONCLUSIÓN

Muchas personas deliberan que el acoso cibernético es simplemente unas pocas interacciones indeseadas, pero la gran realidad es que es incorrecto. Incluso, es muy peligroso plantear esa mentalidad. Es importante mencionar nuevamente lo que las estadísticas resultan. Estas son: 58.1% cayeron en depresión, 42.8% caen en ansiedad, 22.0% en paranoia, 4.9% terminan con pensamientos de suicidio, 26.8% le cogen miedo a todo evento incómodo, 12.2% con ataques de pánico, y 12.2% con problemas de dormir. Estos son implicaciones extremadamente complejas y serias lo cual pueden permanecer por el resto de la vida de la víctima. Por otro lado, el acoso cibernético ha bajado un poco en un periodo de 3 años, pero, sin embargo, la severidad de los casos ha aumentado significativamente. ¿Pudiera ser que las repercusiones para los autores del delito son muy flojas? ¿Puede ser que no se le provee un espacio seguro para que las víctimas lo reporten? Hay que atender estas situaciones si realmente deseamos una mejor sociedad.

El internet ha evolucionado rápidamente en estos últimos 20 años. Mientras que la gran mayoría de las personas la utilizan para comprar, estudiar, trabajar, escuchar música, jugar, y más, otros la utilizan para abusar de esta tecnología y cometer delitos. No puedo estresar lo suficiente lo importante que es en educarse sobre las tecnologías de redes sociales disponibles para así estar al tanto de las maneras en que una persona puede obtener el beneficio para la oportunidad para causar daño. El origen, escalación, y facilidad de este caso es evidenciado en los resultados que demuestran la falta de conocimiento de la protección en el espacio del internet. Se hubiese podido haber evitado situaciones, como este caso, desde un principio. Por eso es por lo que la constante

educación en la tecnología ayudará a aumentar el conocimiento para combatir el acoso y fraude cibernético.

Realmente ya se cuenta con una gran selección de herramientas y métodos para combatir esos crímenes que afectan la calidad de la vida humana desde una perspectiva forense digital. Pero, es importante que el lado de los aspectos éticos y legales evolucionen con igual velocidad. Actualmente, pienso que las repercusiones legales son muy pasivas. Se deben aumentar las penalidades para así, efectivamente, poder controlar y bajar la cantidad de cargos por acosos cibernéticos que se están cometiendo. El cargo de fraude electrónico contiene repercusiones demasiado blandas. Por esta razón es que se cometen tantos delitos de fraudes electrónicos como lo son: el robo de identidad, activos, corrupción, contribuciones, soborno, estados financieros, y *hackeos*.

Por otro lado, la cultura organizacional juega un papel muy importante que la mayoría de las veces olvidamos. Se ha vuelto una costumbre sobre-trabajar a los empleados sin las debidas recompensas que se merecen. O, también, se crea unos valores o costumbre equivocados en un ámbito laboral. Esto, en turno, empuja a las personas a buscar otros métodos de recompensas o continuar las tradiciones que les enseñaros. Entonces aquí es donde comienza el motivo de los diferentes tipos de fraudes.

Es la responsabilidad de las organizaciones y empresas a reevaluar sus valores éticos para que se mejoren las condiciones laborales. De esta manera, se logra disminuir los casos de acoso y fraude electrónico. También es responsabilidad de cada profesional forense y examinador de fraude a educarse sobre la evolución de los métodos para cometer dichos delitos. Finalmente, recae principalmente en las manos de cada uno de los integrantes de la sociedad a educarse en las

maneras que se cometen los delitos cibernéticos para poder evadirlos y protegerse efectivamente de daños psicológicos.

SECCIÓN VIII: REFERENCIAS

ACFE. (n.d.). *Fraud 101: What Is Fraud?* https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud

Bates, P. (2021, septiembre 27). *What Is Snapchat and How Does It Work?* MakeUseOf. https://www.makeuseof.com/tag/what-is-snapchat/

Begotti, T & Maran D. A. (2019, mayo 22). *Characteristics of Cyberstalking Behavior, Consequences, and Coping Strategies: A Cross-Sectional Study in a Sample of Italian University Students*. Future Internet. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjKhcSGlYH5AhXBtYQIHcWAB2QQFnoECCMQAQ&url=https%3A%2F%2Fwww.mdpi.com%2F1999-5903%2F11%2F5%2F120%2Fpdf&usg=AOvVaw1SZcl6YCQQpoVltGdzBP6H

Bennett-Green, B. (2014, enero 23). GoPSUsports. *BLOG: One Summer – Steve Waithe.* https://gopsusports.com/news/2014/1/23/BLOG_One_Summer_Steve_Waithe

Bertazzo, S. (2021, junio 28). *Online Harassment Isn't Growing – But It's Getting More Severe.* PEW. https://www.pewtrusts.org/en/trust/archive/spring-2021/online-harassment-isnt-growing-but-its-getting-more-severe

Callaghan, P. (2019, noviembre 14). *What is the EDRM (Electronic Discovery Reference Model)?* Pagefreezer. https://blog.pagefreezer.com/what-is-ediscovery-reference-model-edrm

Cisco. (n.d.). *What Is a Hacker?* https://www.cisco.com/c/en/us/products/security/what-is-a-hacker.html

Conspiracy to commit offense or to defraud United States, 18 U.S.C. § 371 (1948). https://www.law.cornell.edu/uscode/text/18/371

Department of Justice. (2021, noviembre 17). *Chinese National Arrested and Charged with Cyberstalking.* https://www.justice.gov/usao-mn/pr/chinese-national-arrested-and-charged-cyberstalking

Dodt, C. (2019, julio 6). *Computer forensics: FTK forensic toolkit overview [updated 2019].* Infosec. https://resources.infosecinstitute.com/topic/computer-forensics-ftk-forensic-toolkit-overview/

Duggan M. (2017, julio 11). *Online Harassment 2017.* Pew Research Center. https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

ESPN. (2021, abril 7). *Ex-Northeastern track coach Steve Waithe arrested, accused of trying to*

trick female athletes into sending nude photos. https://www.espn.com/college-sports/story/_/id/31210397/ex-northeastern-track-coach-steve-waithe-arrested-accused-trying-trick-female-athletes-sending-nude-photos

Exterro. (n.d.). *FTK Imager.* https://www.exterro.com/ftk-imager

Fisher, T. (2020, enero 16). *How to Do a Reverse Search to Find Something Online.* Lifewire. https://www.lifewire.com/how-to-reverse-search-logic-3482669

Fraud and related activity in connection with computers, 18 U.S.C. § 1030 (1984). https://www.law.cornell.edu/uscode/text/18/1030

Fraud by wire, radio, or television, 18 U.S.C. § 1343 (1952). https://www.law.cornell.edu/uscode/text/18/1343

Fruhlinger, J. (2022, mayo 25). *What is an IP address? And what is your IP address?* Network World. https://www.networkworld.com/article/3588315/what-is-an-ip-address-and-what-is-your-ip-address.html

Gordon, S. (2021 agosto 16). *What Is Cyberstalking?* Verywellmind. https://www.verywellmind.com/what-is-cyberstalking-5181466

Grayson, J. (n.d.). *Cybercrimes On A Personal Level: What Is Cyberstalking.* Crime Victim

Center of Erie County. https://cvcerie.org/additional-resources/cyberstalking/

Hammond, C. (2019, septiembre 19). *23 Ways You Could be Cyberstalked.* PsychCentral. https://psychcentral.com/pro/exhausted-woman/2019/09/23-ways-you-could-be-cyberstalked#1

Instagram. (n.d.). *What is Instagram?* https://help.instagram.com/424737657584573

Kaspersky. (n.d.). *All About Phishing Scams & Prevention: What You Need To Know.* https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips

Kumar C. (2022, mayo 5). *22 herramientas de investigación forense GRATIS para expertos en seguridad de TI.* Geekflare. https://geekflare.com/es/forensic-investigation-tools/

Mayo Clinic. (n.d.). *Post-traumatic stress disorder (PTSD).* https://www.mayoclinic.org/diseases-conditions/post-traumatic-stress-disorder/symptoms-causes/syc-20355967

Melendez, P. & Hughes, S. (2021, abril 7). *Elite University Track Coach Stole Athletes' Nudes Then Extorted Them: DOJ.* Yahoo! Finance. https://uk.finance.yahoo.com/news/elite-university-track-coach-stole-160440890.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJJEK62jTAe2sXeJUcWEl9YCtaDIVoTuSxWZHOQMQ

9hIjnLRtHwIOLIn0XO-mc6Zw-sTGSw5L918X-vgoQkJTHe-yTJrJsVp5f1PHfTZldMlhikSnOjoVKnsar5-WUttxZBBNumFIfotUY1r0SMBjzJ0IEKqd1d255CZBLPVLtDs

Merriam-Webster. (n.d.). *anonymous. https://www.merriam-webster.com/dictionary/anonymous*

Miller, G. (2021 junio 15). *The Horrifying Truth of Cyberstalking.* The Signal. https://georgiastatesignal.com/the-horrifying-truth-of-cyberstalking/

Morgan, R. E. & Truman, J. L. (2022, febrero). *Stalking Victimization, 2019.* U.S. Department of Justice. https://bjs.ojp.gov/content/pub/pdf/sv19.pdf

National Cyber Security Centre. (n.d.). *Step 5 – Avoiding phishing attacks.* https://www.ncsc.gov.uk/collection/small-business-guide/avoiding-phishing-attacks

Norton 360. (n.d.). *15 Social Networking Safety Tips To Remember.* https://www.nortonlifelockpartner.com/security-center/15-social-networking-safety-tips.html

Norton. (2021, septiembre 23). *What is phishing? How to recognize and avoid phishing scams.* https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html#

Norton. (2022, mayo 4). *What is smishing + smishing attack protection tips for 2022.*

https://us.norton.com/internetsecurity-emerging-threats-smishing.html

Penn State University Athletics. (n.d.). *Steve Waithe.* https://gopsusports.com/sports/track-and-field/roster/steve-waithe/4277

Phishing.org. (n.d.). *What Is Phishing?* https://www.phishing.org/what-is-phishing

Principals, 18 U.S.C. § 2 (1948). https://www.law.cornell.edu/uscode/text/18/2

ProDiscover. (n.d.) *ProDiscover at a Glance.* https://prodiscover.com

Smart GEN Society. (2021, abril 7). *My Eyes Only Doesn't Mean Your Eyes Only.* https://www.smartgensociety.org/press/article/my-eyes-only

Siena, N. (2021, noviembre 19). *Chinese National Allegedly Created Fake Sexual Profiles Of Minnesota Woman, Charged With Cyberstalking.* Latin Times. https://www.latintimes.com/chinese-national-allegedly-created-fake-sexual-profiles-minnesota-woman-charged-495024

Stalking, 18 U.S.C. § 2261A (1996). https://www.law.cornell.edu/uscode/text/18/2261A

Tatum, M. (2022, mayo 24). *What is a Username?* EasyTechJunkie. https://www.easytechjunkie.com/what-is-a-username.htm

Universidad Columbia en New York. (n.d.). *Human Resources.*
https://humanresources.columbia.edu/content/hiring-process

USA v. Andrew T. Maliska, 1:18-cr-00163-TSC (District of Columbia 2018).
https://www.courtlistener.com/docket/7439540/1/united-states-v-maliska/

USA v. Sumit Garg, 2:21-cr-00045-JJCC (Disctrict of Washington 2021).
https://www.justice.gov/usao-wdwa/press-release/file/1377086/download

US v. Steve Waithe, 1:21-mj-01209-DLC (District of Massachusetts 2021).
https://www.justice.gov/usao-ma/press-release/file/1384226/download

US v. Steve Waithe, 1:21-cr-10342-PBS (District of Massachusetts 2021).
https://www.justice.gov/usao-ma/page/file/1452966/download