EDP UNIVERSITY OF PUERTO RICO, INC.
RECINTO DE HATO REY
MAESTRÍA EN SISTEMAS DE INFORMACIÓN CON ESPECIALIDAD EN SEGURIDAD E INVESTIGACIÓN DE FRAUDE CIBERNÉTICO

FRAUDE MUNDIAL: ORGANIZACIÓN CRIMINAL INFRAUD

UNITED STATES OF AMERICA V. SVYATOSLAV BONDARENKO, 2018

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

MARZO, 2020

PREPARADO POR
NAOMI I. LLINÁS ROSA

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

FRAUDE MUNDIAL: ORGANIZACIÓN CRIMINAL INFRAUD

UNITED STATES OF AMERICA V. SVYATOSLAV BONDARENKO, 2018

Preparado por
Naomi I. Llinás Rosa

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

Marzo, 2020

Aprobado por:

Dr. Miguel A. Drouyn, Profesor

Tabla de Contenido

TABLA DE FIGURAS

I. INTRODUCCIÓN Y TRASFONDO

Introducción

A medida que pasan los años y el internet acapara más territorio, la seguridad de nuestra data cae más en riesgo. Esto es un tema preocupante, partiendo del punto de vista que los procesos se continúan digitalizando cada vez más. Es prácticamente imposible proteger nuestra data personal en todo momento. Como individuos podemos tomar medidas de protección y prevención, pero no podemos controlar el manejo de nuestra data por parte de las diferentes agencias y comercios con los cuales interactuamos a diario. El análisis y entendimiento de este caso ayudará a proveer otra perspectiva de los fraudes que pasan a diario y que muchos desconocen. Además, brindará recomendaciones sobre como las personas y entidades deben manejar la data de manera segura para minimizar el riesgo de ser víctimas de fraude.

Descripción del caso

Caso: United States of America V. Svyatoslav Bondarenko

Número de Caso: 2:17-cr-306-JCM-PAL

Acusados:

1. Svyatoslav Bondarenko, a.k.a Obnon, a.k.a Rector, a.k.a. Helkern
2. Sergey Medvedev, a.k.a. Stells, a.k.a. Segmed, a.k.a. Serbear
3. Amjad Ali, a.k.a. Amjad Ali Chaudary, a.k.a. RedruMZ, a.k.a. Amjad Chaudary

4. Roland Patrick N'Djimbi Tchikaya a.k.a. Darker, a.k.a. karke3r.cvv
5. Arnaldo Sanchez Torteya, Miroslav Kovacevic, a.k.a. Elroncoluna
6. Miroslav Kovacevic, a.k.a. Goldjunge
7. Frederick Thomas, a.k.a Mosto, a.k.a 1stunna, a.k.a. Bestssn
8. Osama Abdelhamed, a.k.a. MrShrnofr, a.k.a DrOsama, a.k.a. DrOsama1
9. Besart Hoxha, a.k.a. pizza
10. Raihan Ahmed, a.k.a. Chan, a.k.a. Cyber Hacker, a.k.a. Mae Tony, a.k.a. Tony
11. Andrey Sergeevich Novak, a.k.a Unicc, a.k.a. Faaxxx, a.k.a. Faxtrod
12. Valerian Chiochiu, a.k.a. Onassis, a.k.a. Flagler, a.k.a. Socrate, a.k.a Eclessiastes
13. John Doe #8, a.k.a, Aimless88
14. Genaro Fioretti, a.k.a Danny Logort, a.k.a Genny Fioretti
15. Edgar Rojas, a.k.a. Edgar Andres Viloria Rojas, a.k.a. Guapo, a.k.a. Guapo 1988, a.k.a. Onlyshop
16. John Telusma, a.k.a John Westley Telusma, a.k.a Peterelliot, a.k.a Pete, a.k.a Pette
17. Rami Fawaz, a.k.a. Rami Imad Fawaz, a.k.a Validshop, a.k.a Th3d, a.k.a. Zatcher, a.k.a Darkeyes
18. Muhammad Shiraz, a.k.a. Moviestar, a.k.a. Leslie

19. Jose Gamboa, a.k.a. Jose Gamboa-Soto, a.k.a. Rafael Garcia, a.k.a Rafael 101, a.k.a Memberplex2006, a.k.a Knowledge
20. Alexey Klimenko, a.k.a Grandhost
21. Edward Lavoile, a.k.a Eddie Lavoie, a.k.a Skizo, a.k.a Eddy Lavoile
22. Anthony Nnamdi Okeakpu, a.k.a. Aslike1, a.k.a. Aslike, a.k.a. Moneymafia, a.k.a. Shilonng
23. Pius Sushil Wilson, a.k.a. FDIC, a.k.a. TheRealGuru, a.k.a. TheRealGuruNYC, a.k.a. RealGuru, a.k.a Po1son, a.k.a Infection, a.k.a. Infected
24. Muhammad Khan, a.k.a CoolJ2, a.k.a. CoolJ, a.k.a. Secureroot, a.k.a. Secureroot1, a.k.a. Secureroot2, a.k.a Mohammed Khan
25. John Doe #7, a.k.a. Muad'Dib
26. John Doe #1, a.k.a. Carlitos, a.k.a TonyMontana
27. David Jonathan Vargas, a.k.a. Cashmoneyinc, a.k.a. Avb, a.k.a. Poony, a.k.a. Renegade11, a.k.a. DvdSVrgs
28. John Doe #2
29. Marko Leopard, a.k.a. Leopardmk
30. John Doe #3, a.k.a. Scottish
31. Aldo Ymeraj, a.k.a. Nii.in, a.k.a. Kubanezi, a.k.a. Yankeeman
32. John Doe #4, a.k.a. Best4Best, a.k.a. Wazo, a.k.a Modmod, a.k.a Alone1, a.k.a. Shadow, a.k.a. Banderas, a.k.a. Banadoura
33. Liridon Musliu, a.k.a. Ccstore, a.k.a. Bowl, a.k.a. Hulk

34. John Doe #5, a.k.a Deputat, a.k.a. Zo0mer
35. Mena Mouries Abd El-Malak, a.k.a Mina Morris, a.k.a Mena2341, a.k.a MenaSex
36. John Doe #6, a.k.a Goldenshop, a.k.a Malov

Abogados:

Dayle Elison – Abogada del distrito de Nevada de los Estados Unidos

Kelly Pearson – Abogado Litigante de la División de Crimen Organizado de los Estados Unidos.

Fiscales:

John P. Cronan – Fiscal Adjunto Interino de la División Criminal del Departamento de Justicia

Steven W Myhre – Fiscal Interino de los Estados Unidos

Chad W McHenry – Asistente Fiscal de los Estados Unidos

Juez:

Honorable Peggy A. Leen – Jueza Federal del magistrado de los Estados Unidos en el Distrito de Nevada.

Trasfondo

Según United States of America v. Svyatoslav Bondarenko (2018), Infraud es una organización cibercriminal dirigida a la venta y compra de data fraudulenta a gran escala. Esta

puede ser data personal como seguro social, nombre y dirección. También, puede ser data financiera, tarjetas de créditos falsificadas y credenciales de acceso a bancos. Pero, no solo se limitaban a esto, sino que también traficaban con malwares y diferentes scripts diseñados para violentar o dañar a sus víctimas.

Según se expone en United States of America v. Svyatoslav Bondarenko (2018), esta organización creaba un enlace entre compradores y vendedores potenciales de este tipo de datos. Estos actos criminales tuvieron víctimas principalmente en Nevada, pero también alrededor del mundo, incluyendo el United Kingdom Bank con un fraude total de aproximadamente $530 millones de dólares.

Fue fundada en octubre de 2010 por el ucraniano Svyatoslav Bondarenko aka *Obnon*, *Rector*, *Helkern* de aproximadamente 36 años de edad y su cofundador es Sergey Medvedev de nacionalidad rusa. Su creador, Bondarenko estableció unas normas de seguridad muy específicas para poder operar este website, dentro de estas normas lo estaban comunicarse únicamente en línea y utilizado alias, proteger su identidad, educar a los miembros de la organización para no cometer errores y evitar ser descubiertos. También tenían medidas de expulsión para los miembros que actuaban de manera extraña o en contra de los intereses de Infraud.

En el 2015 Bondarenko pierde su presencia en Infraud, este dejó de participar de la organización y desapareció. En abril del 2016 Medvedev se proclama dueño y administrador de Infraud y decide cambiar las normas de su operación con medidas menos severas para permitir el acceso a mayor cantidad de miembros. Esta decisión provocó que se realizaran varias

transacciones con agentes encubiertos y a la fecha de su disolución en 2018 ya contaban con aproximadamente 10,901 miembros en su red.

Descripción de los hechos

A continuación, se presenta un histórico de lo que fueron los sucesos ocurridos desde la creación de Infraud hasta que fue descubierta la organización.

1. En octubre del 2010 Svyatoslav Bondarenko fundó el *website* llamado Infraud para negocios a miembros potenciales prometiendo que este sería un lugar *cómodo y seguro* para unir profesionales para los cuales el *carding* y el *hacking* se convirtiera en un estilo de vida.
2. En noviembre del 2010 Bondarenko publicó lo que se conociera como las normas de conducta para los miembros de la Organización Infraud.
3. Entre octubre 2010 y marzo 2011 surgieron varios anuncios de venta y compras de tarjetas de crédito comprometidas, artículos ilícitos, servicios de *escrow.*
4. En marzo 2011 Bondarenko, como administrador de Infraud prohibió a los miembros de la organización la venta y compra de artículos de contrabando provenientes de Russia.
5. Entre marzo 2011 y septiembre 2012 se mantienen activos los anuncios, ventas y compras de artículos de contrabando, documentos de identificación falsificados, malwares, tarjetas de crédito comprometidas, websites de *carding* y credenciales de cuentas paypal.

6. En septiembre 2012, se estipula un proceso para nuevos vendedores mediante el cual serán verificados y aprobados por la Organización Infraud. En este proceso el vendedor en turno debía proveer una muestra de sus productos para validar la calidad de estos.
7. En octubre 2012 surge un nuevo anuncio por parte de uno de los miembros en el cual se ofrecen los servicios de *World Wide Travel Agency,* esto consiste en reservas de viajes, rentas de autos, hoteles entre otras cosas, a un costo menor del precio real.
8. Durante los años 2012 al 2016 continúan las transacciones activas de trafico de data en el foro de Infraud. En los cuales quedan expuestos otros *websites*, de venta en la Deep web.
9. En abril 16, 2016 Medvedev Cofundador de Infraud publica que Bondarenko está desaparecido y se proclama dueño y *administrador de la Organización Infraud.*
10. En Julio del 2016 Medvedev indica que ahora Infraud tiene una invitación abierta para que sus miembros puedan incluir a sus asociados a la organización siempre y cuando esto cumplan con unos requisitos mínimos.
11. En agosto 2017 uno de los miembros de la organización vendió a un agente encubierto de Investigaciones del Homeland Security más de quince (15) tarjetas de crédito comprometidas pertenecientes a residentes de Nevada. Esto se completó desde su AVS goldenshop.cc.
12. En agosto 2017 Novak miembros de la organización vendió a un agente encubierto de Investigaciones del Homeland Security quince (15) tarjetas de crédito comprometidas pertenecientes a residentes de Nevada. Esto se completó desde su AVS unicc.at.

13. En agosto 2017 Novak miembros de la organización vendió a un agente encubierto de Investigaciones del Homeland Security quince (54) tarjetas de crédito comprometidas pertenecientes a residentes de Nevada. Esto se completó desde su AVS unicc.at.

Acusaciones, cargos y penalidades

18 U.S.C. § 2 – Ayudar o incitar la comisión de una actividad criminal.

18 U.S.C. § 1028 – Fraude y Actividad relacionada con documentos de identificación y características de autenticación.

18 U.S.C. § 1028A – Robo de identidad agravado

18 U.S.C. § 1029 – Fraude y actividad relacionada con los dispositivos de acceso.

18 U.S.C. § 1343– Fraude por cable, radio o televisión

18 U.S.C. § 1344– Fraude Bancario

18 U.S.C. § 1543 – Falsificación o uso falso de pasaporte

18 U.S.C. § 1956 – Lavado de instrumentos monetarios

18 U.S.C. § 1961 – Actos delictivos

18 U.S.C. § 1962 – Actividades prohibidas

Definición de Términos

Sitio de Venta Automatizado (AVS) – Sitios que operan con un software de gestión automático que mantiene un seguimiento de todas las fases de una venta, según lo define (EGA futura, s.f.)

Carding – Falsificación de tarjeta de crédito en la cual esta, es codificada con la información de la cuenta real de la víctima (Pérez, 2019).

ICQ – Chat de mensajería instantánea.

CVV – Código de verificación de tarjeta, este código contiene data encriptada del titular de esta, esto puede incluir nombre completo, fecha de nacimiento, seguro social, dirección, teléfono y por consiguiente información bancaria (Nvindi, 2019).

Liberty Reserve – Moneda virtual utilizada por ciberdelincuentes para lavado proveniente de sus actividades ilegales, según se expone en (Department of Justice, 2016).

Malware – La Oficina de Seguridad del Internauta (2016), define que este es un programa informático ejecutado sin autorización del propietario del dispositivo infectado y permite ejecutar funciones por parte del atacante.

Ripper – Vendedor de productos ilícitos o de baja calidad, también aquel vendedor que no entrega los bienes acordados en la transacción (Thomas J Holt, 2011).

II. REVISIÓN DE LITERATURA

Introducción

En esta revisión de literatura se estará argumentando sobre los fraudes actuales del caso en cuestión y las consecuencias de esto a nivel estadístico. En adición se estarán evaluando brevemente las leyes y cargos aplicables según las acciones y actividades fraudulentas cometidas por la organización Infraud. Cabe resaltar que esta organización operaba bajo el lema "En el fraude Confiamos", "*In fraud we trust"* en inglés por tanto siempre declararon que estaban operando de manera ilegal.

Fraudes involucrados

Según ICE (2017), el fraude de documentos o identidad representa una vulnerabilidad de alta importancia ya que pudiera promover la entrada de terroristas, delincuentes y extranjeros indocumentados a los Estados Unidos o cualquier país y permanecer allí. También establecen que este fraude consiste en la creación, falsificación, manipulación, venta y uso de documentos de identidad.

Este hurto de documentos de identificación o la falsificación de ello conlleva directamente al robo de identidad. Según expone Douglas (2020), la FTC en el año 2019 tuvo reportes de 167,000 personas con tarjetas de crédito fraudulentas abiertas con su información. También las redes sociales contribuyen al robo de información, dada la cantidad de data que se expone públicamente. En los últimos años el robo de identidad proveniente de las redes sociales ha incrementado (ver Figura 1).

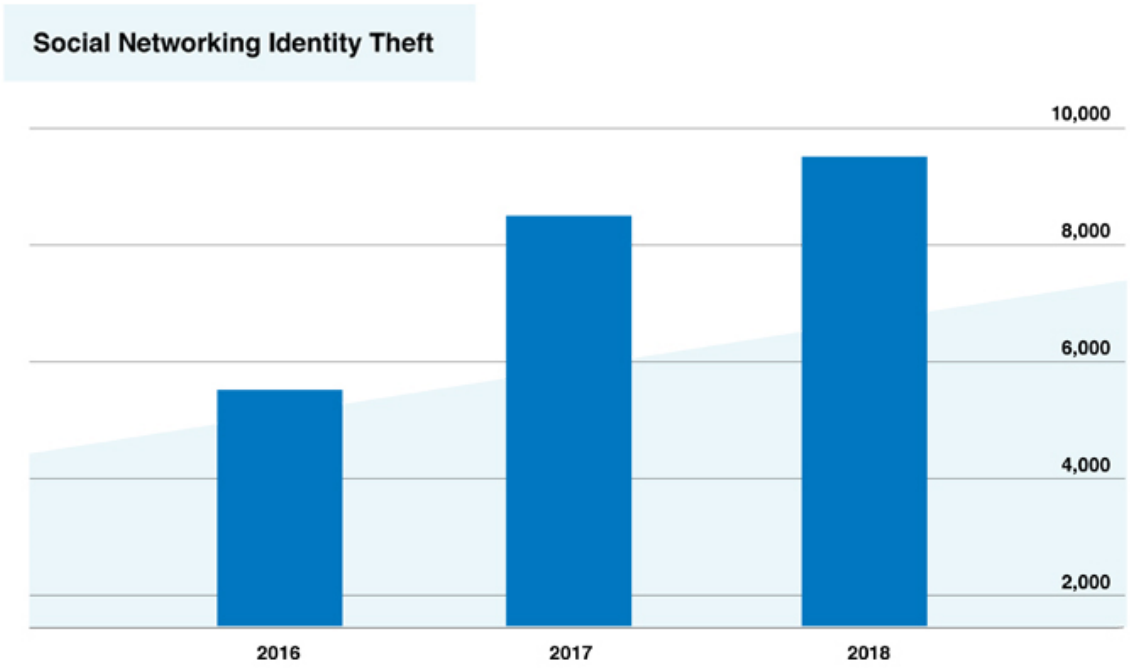


Figura 1: Estadística de Robo de Identidad. Recuperado de https://www.consumeraffairs.com/finance/identity-theft-statistics.html

De acuerdo con el Center of Victim Research (2016), 7-10 % de las personas en los Estados Unidos son víctimas de robo de identidad cada año de los cuales el 21% son víctimas de múltiples incidentes. Otro esquema en el que se considera robo de identidad es el fraude con tarjetas de crédito. Esto se debe a que de la tarjeta se puede obtener información como, nombre, número de tarjeta, fecha de vencimiento y otra información personal incluida en el perfil de data que contiene cada plástico.

Cornell Law School (s.f.) expone que este tipo de fraudes se clasifican en dos categorías generales, la solicitud fraudulenta que es en la cual el defraudador abre una cuenta utilizando información de otra persona y la apropiación fraudulenta que es cuando el atacante toma control y posesión de una cuenta ya existente; Esto ocurre frecuentemente mediante la clonación de tarjetas.

Leyes Aplicables

Las violaciones cometidas durante este fraude van todas en contra del Título 18 del código de los Estados Unidos, se incluyen las diferentes secciones aplicables.

1. 18 U.S.C. § 2 – Ayudar o incitar la comisión de una actividad criminal en contra de los Estados Unidos.

   Aquella persona o entidad que a sabiendas comete un delito en contra de los Estados Unidos, ayuda, incita, aconseja, ordena, induce o procura su comisión.

   Penalidades aplicables – No se trata de un delito independiente por consecuente el estatuto no establece penalidad.

2. 18 U.S.C. § 1028 – Fraude y Actividad relacionada con documentos de identificación y características de autenticación.

   Aquella persona o entidad que a sabiendas produce un documento de identificación falso; compra, vende o transfiere documentos de identificación falsos o robados con la intención de defraudar a los Estados Unidos.

   Penalidades Aplicables – 5 a 30 años de prisión y/o $250,000 de multa.

3. 18 U.S.C. § 1028A – Robo de identidad agravado

   Aquella persona que durante y en relación con cualquier violación de delito grave, transfiera o posea documentos de identificación de otra persona.

Penalidades Aplicables – 2 a 5 años de prisión consecutivos a cualquier otro termino de prisión imputado y/o $250,000 de multa.

4. 18 U.S.C. § 1029 – Fraude y actividad relacionada con los dispositivos de acceso.

   Aquella persona que a sabiendas y con intención de defraudar posee quince (15) o más dispositivos de acceso falsificados o no autorizados.

   Penalidades Aplicables – 10 a 20 años de prisión y/o $250,000 de multa.

5. 18 U.S.C. § 1343– Fraude por cable, radio o televisión

   Representaciones fraudulentas para obtener dinero o algún beneficio ilícito mediante cable, radio o televisión.

   Penalidades Aplicables – 20 a 30 años de prisión y/o $250,000 a $1,000,000 de multa.

6. 18 U.S.C. § 1344– Fraude Bancario

   Cualquiera que a sabiendas ejecute alguna acción con el propósito de defraudar una institución bancaria; para obtener, dinero, créditos, activos, seguridades y/o propiedades.

   Penalidades Aplicables – 30 años de prisión y/o $1,000,000 de multa.

7. 18 U.S.C. § 1543 – Falsificación o uso falso de pasaporte

   Aquel que intencionalmente use o proporcione a otro un pasaporte falsificado, mutilado o alterado.

Penalidades Aplicables – 25 años de prisión y/o $250,000 de multa.

8. 18 U.S.C. § 1956 – Lavado de instrumentos monetarios

   Conducta o intento de realizar transacciones financieras involucrando el producto de alguna actividad ilegal.

   Penalidades Aplicables – 20 años de prisión y/o $500,000 de multa o el doble de valor de la propiedad involucrada hasta $10,000 lo que sea mayor.

9. 18 U.S.C. § 1961

   Cualquier acto o amenaza que implique asesinato, secuestro, juego, incendio, premeditación, robo, soborno, extorsión, tráfico de material obsceno o tráfico de sustancias controladas.

   Penalidades Aplicables – Más de un año de prisión.

10. 18 U.S.C. § 1962 – Actividades prohibidas

    Recibo de cualquier ingreso derivado, directa o indirectamente de un patrón de actividades de crimen organizado.

    Penalidades Aplicables – 20 años de cárcel y/o $250,000 de multa.

Casos Relacionados

(United States of America v. Rafael Joaquin Beltre Beltre, 2012)

Al igual que en la investigación presentada esta acusación es en contra de una red de delincuentes que se dedicaban a traficar documentos de identidad en este particular las

víctimas eran personas de Puerto Rico. Su modo operatorio era hacer pasar el negocio ilícito como una tienda de ropa llamada Savarona Suppliers en la cual se referían a los documentos de féminas como "faldas" y a los documentos de masculinos como "pantalón"; para hacer referencia a las edades utilizaban tamaños de ropa, esto para protegerse en las comunicaciones vía telefónica. Otros términos utilizados por esta red eran "camisas", "uniformes" y "ropa". Al igual que en el caso de Bondarenko se les acusa de violación al código 18 U.S.C. § 1028 y 18 U.S.C § 1028A por venta, producción y transferencia de documentos de identificación falsos o hurtados. A diferencia de la red Infraud, estos utilizaban el servicio de correo postal de los Estados Unidos para hacer entrega de los documentos de identificación ilícitos con los cuales traficaban.

(United States of America v. Romeo Vasile Chita, 2011)

Este caso tiene similitud con el principal, ya que, los criminales son acusados de conspiración y lavado de dinero. Nueve individuos son acusados de enviar correos *Phishing* acompañados de un *keylogger* que les permitía capturar información sensitiva de los usuarios incluyendo información bancaria. Una vez adquirida la información financiera procedían a retirar y transferir dinero de estas entre múltiples cuentas para así encubrir el origen de los fondos. Entre los cargos presentados también se encuentran el 18 U.S.C § 1956 Y 18 U.S.C § 1962 por tráfico y transacciones financieras provenientes de medios ilegales.

(United States of America v. Arthur Budovsky, 2013)

En este caso, que se relaciona directamente con el de Infraud, Arthur Budovsky fundador de Liberty Reserve, moneda virtual utilizada por los miembros de la Organización

Infraud es acusado y declarado culpable por dirigir una empresa masiva de lavado de dinero. Budovsky tenía pleno conocimiento de que sus servicios eran principalmente utilizados por delincuentes que buscaban lavar sus ganancias provenientes de actividades criminales. A pesar de no estar acusados de los mismos cargos, esta fue una de las razones por las cuales los miembros de Infraud pudieron seguir cometiendo actos criminales, ya utilizando Liberty Reserve pudieron seguir lavando el dinero que generaban de sus actividades.

Herramientas de investigación

Las herramientas utilizadas para completar la investigación forense deben ser las adecuadas según la evidencia obtenida en el caso. En este particular se incautó una laptop a la cual se le realizó una imagen para extraer toda la data incriminatoria posible. Para realizar esta extracción se utilizará el programa Forensic Toolkit (FTK), este se utiliza para la creación de imágenes de disco y también permite recuperar datos previamente eliminados y archivos perdidos. En adición a esto y totalmente relevante FTK permite crear hashes para asegurar la integridad de la imagen y prevenir alteraciones en la evidencia (Access Data FTK, 2020).

Otra herramienta que se puede utilizar al realizar la investigación forense es el programa Autopsy, este permite investigar y extraer data de una imagen previamente obtenida. Es decir, en este programa de análisis se puede recuperar data activa o eliminada del disco que sea relevante y pertinente a la investigación según requerido. Este software permite realizar búsquedas por palabras claves. Y también permite ver otros atributos como la fecha y hora de creación del archivo que se esté analizando (Carrier, 2020).

III. SIMULACIÓN

Según se presenta en la figura 2 la organización *Infraud* contaba con un *website* criminal basado en diferentes foros segregados por categorías. Para almacenar toda esta data tenían unos servidores los cuales eran manejados por los administradores Svyatoslav Bondarenko y Sergey Medvedev, estos se encargaban de mantener la seguridad de estos utilizando conexiones VPN para proteger ese tráfico de data desde el *website* hasta los servidores y a su vez mantener el anonimato entre miembros y cualquier persona que lograra acceso al website.

Estos foros recibían insumo por parte de los miembros y vendedores mediante un proxy para protegerse a sí mismos. Los miembros pagaban por anuncios que eran publicados en la página web y servían para promocionar sus productos y dirigir el tráfico a sus páginas de venta automáticas. Por otro lado, también podían comprar cualquier cosa que se estuviese ofreciendo. Los vendedores eran los que se encargaban de adquirir los diferentes activos que se traficaban mediante el *website* de *Infraud*.

La organización Infraud al igual que cualquier empresa u organización legítima, contaba con una jerarquía en la cual cada parte tenía una tarea esencial en este esquema fraudulento para que el mismo tuviera lugar. Los títulos se clasificaban en seis categorías explicadas a continuación; administradores, super moderadores, moderadores, vendedores, miembros y miembros VIP. Los *Administradores* a.k.a. 4DMini57r470rz eran los de más alto rango en la organización *Infraud*; encargados de manejar el sitio, la organización y sus miembros. También se encargaban de reclutar vendedores *reputables* de contrabando para mantener siempre su sitio como uno de alta calidad ante esta sociedad de criminales.

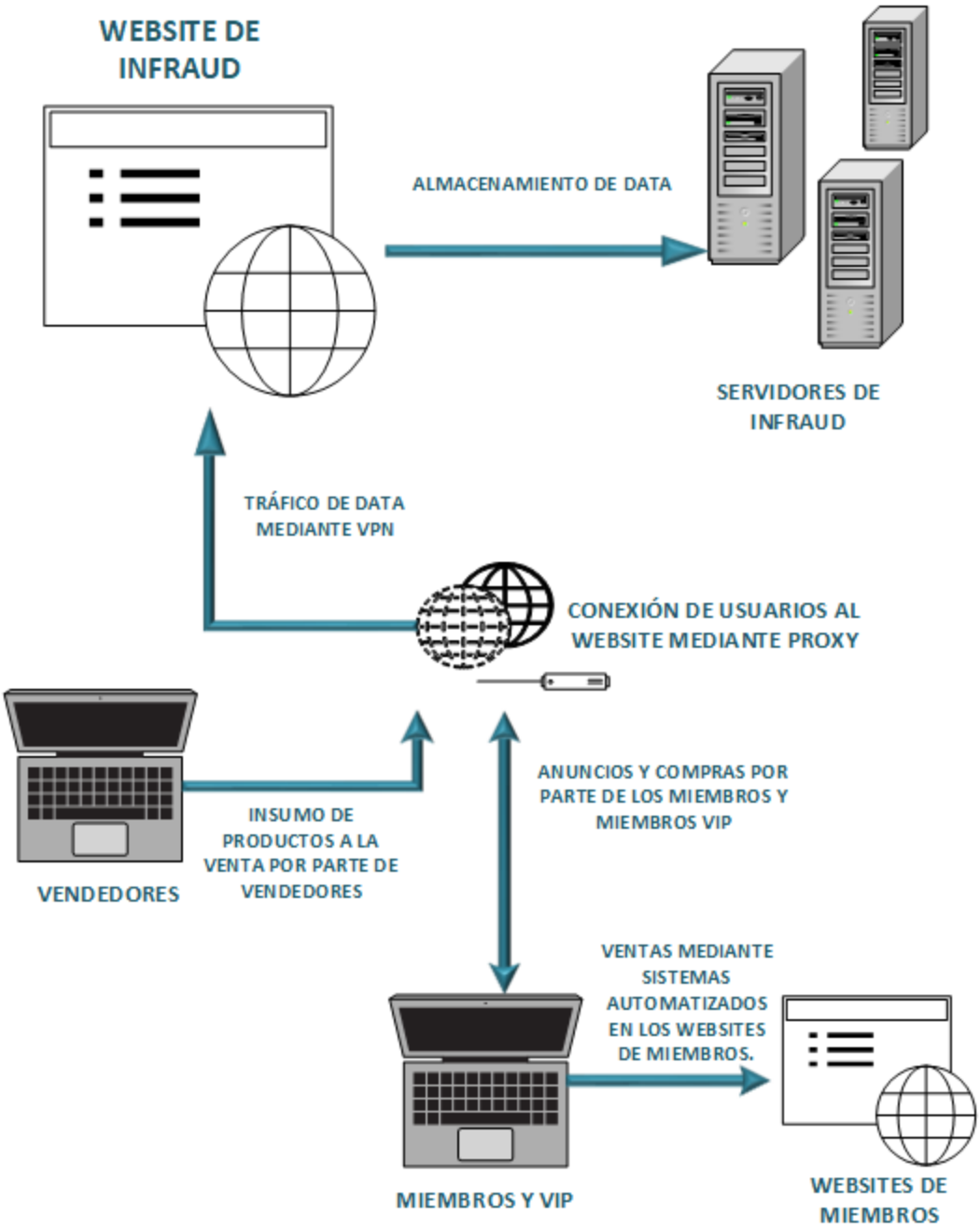


Figura 2: Diagrama de operación Organización Criminal Infraud.

Los administradores tomaban las decisiones importantes y decidían quien se convertía en miembro y quien dejaba de participar en el foro, al igual que los niveles y ascensos de éstos en la jerarquía. Se mantenían alertas a las acciones de sus miembros que demostraran algún

tipo de deslealtad o falta a sus principios como organización criminal creyente del *slogan* "*In Fraud We Trust*". Otras de sus funciones lo eran mantener la viabilidad del negocio e idear estrategias para prevenir ser detenidos en el mundo real y darle mantenimiento y seguridad a los servidores y página web de *Infraud*.

Los administradores se encomendaban a conseguir los mejores vendedores para traerlos a su red en la cual se podían conseguir documentos de identidad como certificados de nacimiento, números de seguro social, identificaciones y pasaportes; también se ofrecían tarjetas de débito y crédito comprometidas, credenciales de acceso a cuentas Paypal comprometidas, accesos a cuentas de banco y lo que se conoce como Carded Travel Services según United States of America v. Svyatoslav Bondarenko (2018), este consiste en ofrecer reservaciones de viajes, estadías, alquiler de transporte entre otras cosas típicas de unas vacaciones a un costo mucho menor del valor real, generalmente equivalente a un 20%-30% del costo total, estas reservas eran realizadas con tarjetas de crédito fraudulentas. Otras cosas ofrecidas en este *website* eran malwares y programas perjudiciales para provocar daños y pérdidas a las víctimas, entre otros bienes ilegales.

Por su parte, los *Super Moderadores* a.k.a. M0DER470R5 eran los responsables de brindar apoyo y servir como críticos de los productos en los cuales sus pericias les permitiese. En adición, tenían privilegios de eliminar publicaciones de miembros y editar lo que fuese necesario. Los *Moderadores* a.k.a. M0d3r470r2 tenían funciones similares a los Super moderadores, pero estos solo tenían privilegio de controlar contenido de las publicaciones en algunos foros asignados en la página web de la organización.

Como figuras esenciales los *Vendedores* a.k.a. Professors o Doctors realizaban la venta de sus productos ilícitos mediante sus propios *sites* de venta y mediante el foro de Infraud a los miembros de este. Los vendedores podían pagar y publicar anuncios en el foro de la organización para así dirigir el tráfico a sus sitios de venta automáticos (AVS). Los productos ofrecidos por los vendedores eran evaluados en el foro por los miembros de Infraud y los vendedores deficientes eran castigados por la administración.

Los miembros se clasificaban en dos grupos, los *Miembros VIP* a.k.a Fratello Masons o Miembros avanzados que eran los miembros principales y así clasificados por los administradores de la organización para ser distinguidos del resto. Y los *Miembros* a.k.a. Phr4Ud573r, estos eran miembros generales de la comunidad *Infraud* que utilizaban el *website* para compartir información de actividades criminales y participar de esquemas de fraude. Haciéndose parte de la organización mediante los foros en línea y la aprobación de los administradores. Compran material de los vendedores de la organización como tarjetas de crédito comprometidas, documentos de identidad falsificados, para contribuir a sus esquemas ilegales. Al igual que los vendedores los miembros pueden pagar y publicar anuncios en los foros de la organización.

Los administradores y moderadores se encargaban de educar a sus miembros para cumplir con medidas de seguridad establecidas de su parte y así proteger la organización. Tenían una metodología específica para todos sus procesos, entre estos los pagos que se efectuaban debían ser utilizando monedas virtuales en específico Liberty Reserve, de esta manera hacían el lavado de dinero que provenía de estas prácticas delictivas y prevenían ser detectados. Sus comunicaciones únicamente debían ser por mensajes directos utilizando la

plataforma de mensajería instantánea ICQ ya que esta identifica los perfiles por un número universal UIN por sus siglas en inglés; tenían prohibido comunicarse de manera telefónica ni utilizando sus nombres reales.

IV. INFORME FORENSE DEL CASO

Resumen Ejecutivo

El Departamento de Justicia Federal representado por el Fiscal John A Cronan ha contratado los servicios de investigación forense digital de NIL Forensics con sede en Puerto Rico. Esto para analizar una imagen de disco duro de una laptop incautada por el FBI. La acusación busca ubicar a Sergey Medvedev a.k.a Stells como participe de la organización criminal Infraud.

Como resultado de la investigación se hallaron varios archivos de texto, imágenes y correos electrónicos que relacionan al acusado con la organización y sus actividades. Una vez culminada la examinación de la evidencia suministrada se devuelve al Fiscal John A Cronan junto con la copia digital realizada para completar la investigación solicitada.

Objetivo

Esta investigación le fue solicitada a NIL Forensics por parte del Departamento de Justicia de los Estados Unidos y es llevada a cabo con el fin de hallar archivos, data y cualquier información que sirva como evidencia en el caso en curso, en la cual se les acusa de participar en una organización cibercriminal. El resultado de esta indagación brindará el conocimiento requerido para que el Departamento de Justicia pueda tomar una decisión justa sobre los acusados.

Alcance del trabajo

El 15 de febrero de 2020, el Fiscal Interino de la División Criminal del Departamento de Justicia de los Estados Unidos John P. Cronan le hizo entrega a la examinadora de NIL Forensics, Naomi I. Llinás Rosa una memoria USB marca Kingston. En esta se encontraba una imagen del disco duro marca Seagate incautado por parte de FBI al acusado Sergey Medvedev.

En cumplimiento con los estándares establecidos en la industria forense digital se procede a extraer el hash de la imagen recibida como evidencia y crear una copia de esta para asegurar su integridad. Luego se procede a ejecutar la examinación utilizando la herramienta FTK Imager versión 4.2.1.4 para obtener datos presentes en el disco.

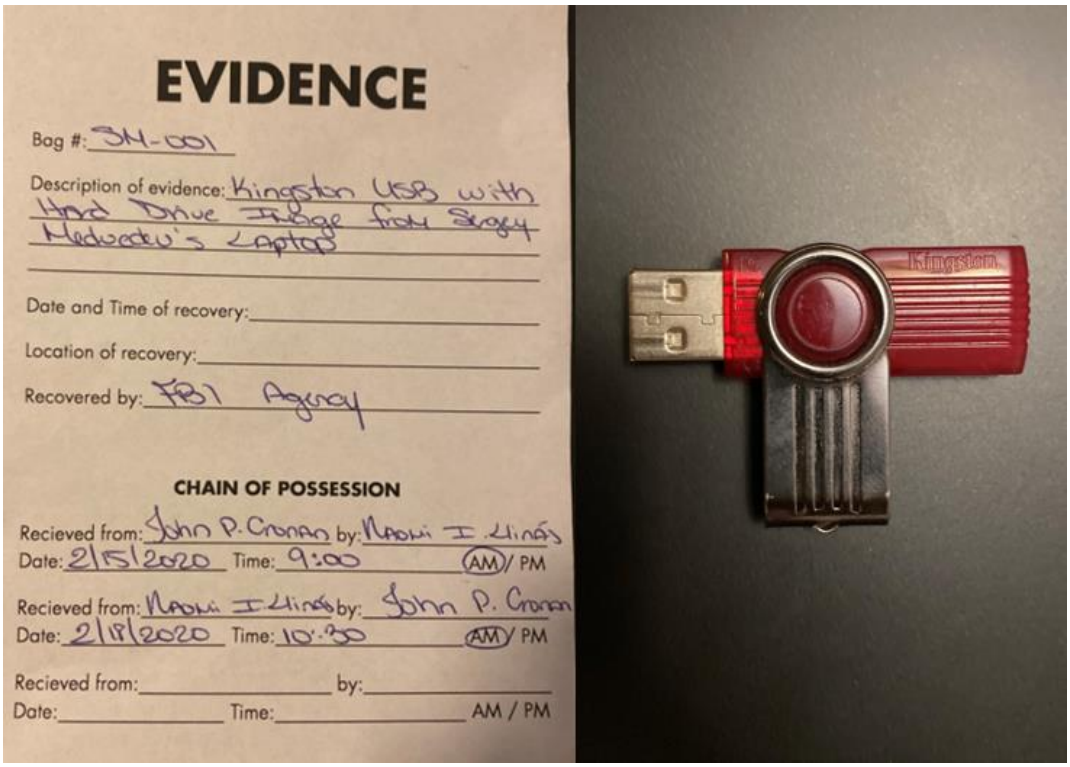


Figura 3: Evidencia Suministrada por el Fiscal John P. Cronan

Datos del Caso

Número del Caso: 2:17-cr-306-JCM-PAL

Investigador: Naomi I. Llinás Rosa

Cliente: Departamento de Justicia de los Estados Unidos

Representante del cliente: Steven W Myhre, Fiscal y Chad W McHenry, Asistente Fiscal.

Descripción de los dispositivos utilizados

Detalle de dispositivos utilizados durante el proceso de investigación.

1. Laptop Lenovo, modelo Flex 5-1570, con procesador Intel Core i7 de 1.8 GHz, 8 GB de RAM y sistema operativo Windows 10 - 64 bit, donde residen las herramientas y aplicaciones utilizadas en el proceso de examinación.
2. Memoria USB 2.0 marca Kingston con capacidad de 64 GB, identificado como evidencia SM-001.

Resumen de Hallazgos

Al concluir el análisis de la evidencia SM-001 utilizando la herramienta FTK Imager se hallaron diferentes archivos presentados a continuación:

1. Correo electrónico recibido por Sergey Medvedev a.k.a Stells de parte de Svyatoslav Bondarenko a.k.a Rector, en el cual este le indica que como administrador principal ha tomado la decisión de prohibir terminantemente hacer tráfico de data con víctimas provenientes de Rusia.

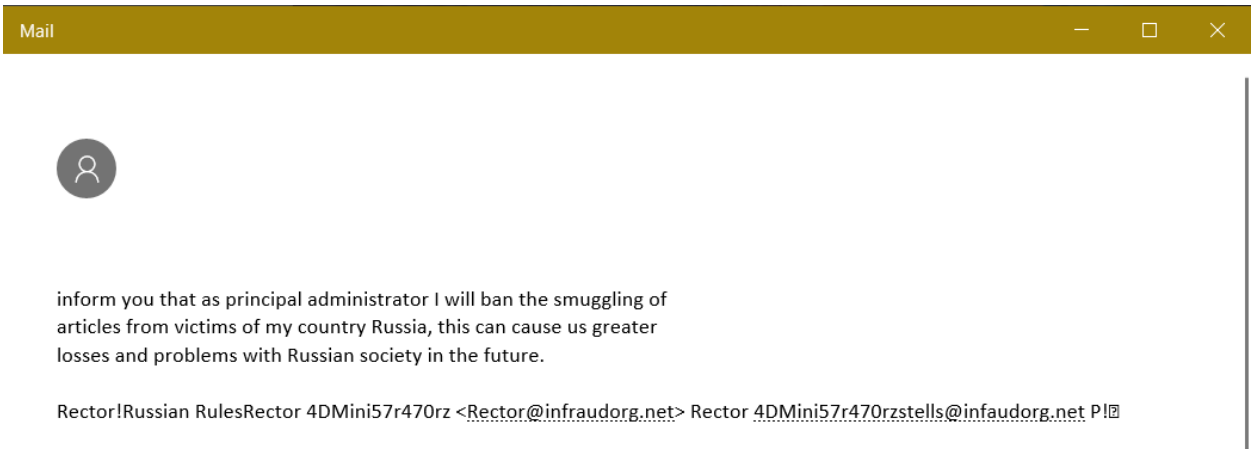


Figura 4: Correo electrónico recibido por parte de Rector.

2. Alerta automática mediante correo electrónico desde el foro de Infraud, solicitando aprobación para nueva publicación de Goldjunge en el foro de la Organización Infraud.

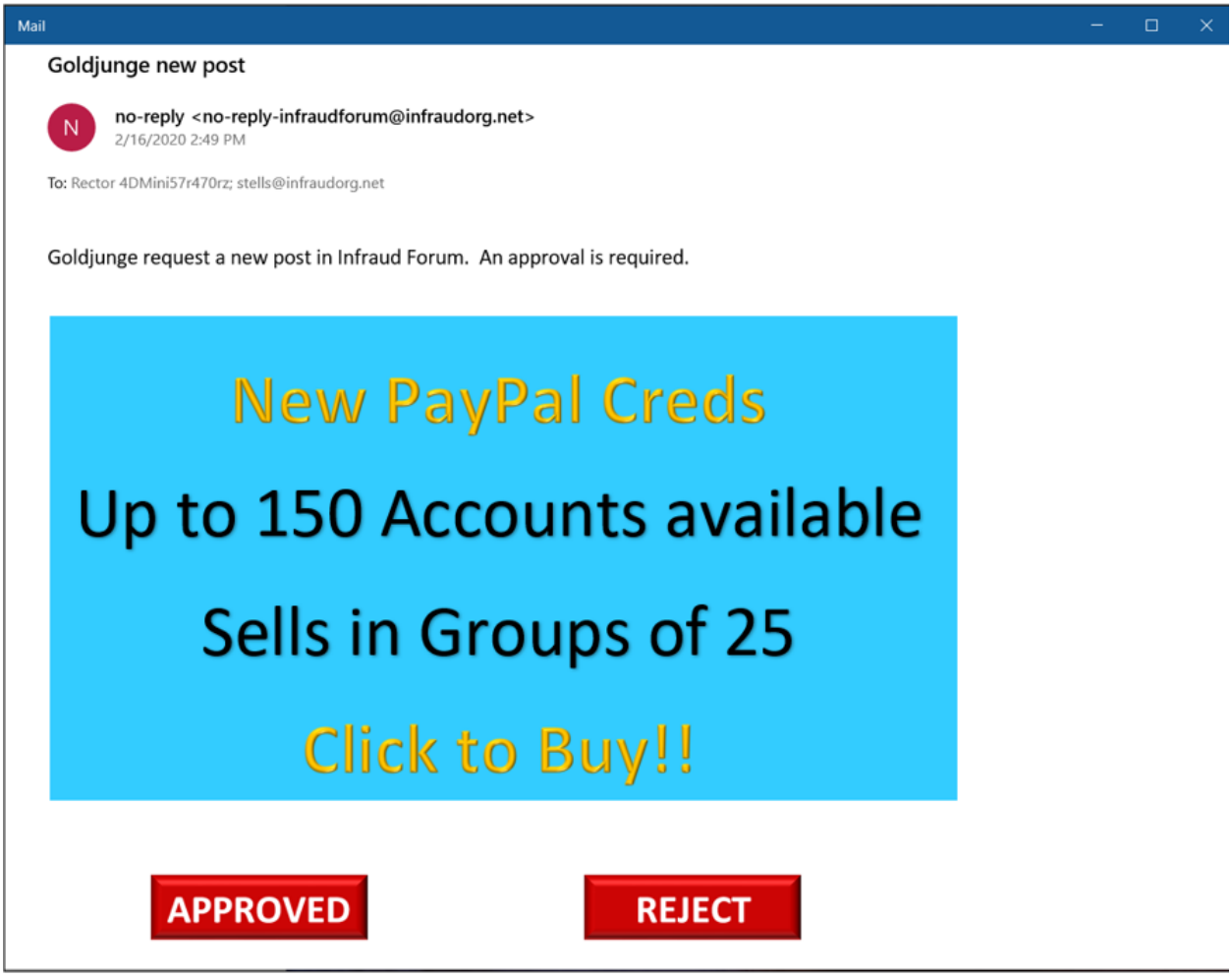


Figura 5: Alerta de publicación mediante correo electrónico.

3. Correo electrónico con tono amenazante por parte de Sergey Medvedev a.k.a. Stells a Bondarenko a.k.a. Rector. Este correo Sergey le reclama a Bondarenko porque no está activo en el foro y que, si no regresa a este, él tomara el cargo total del foro y sus miembros.

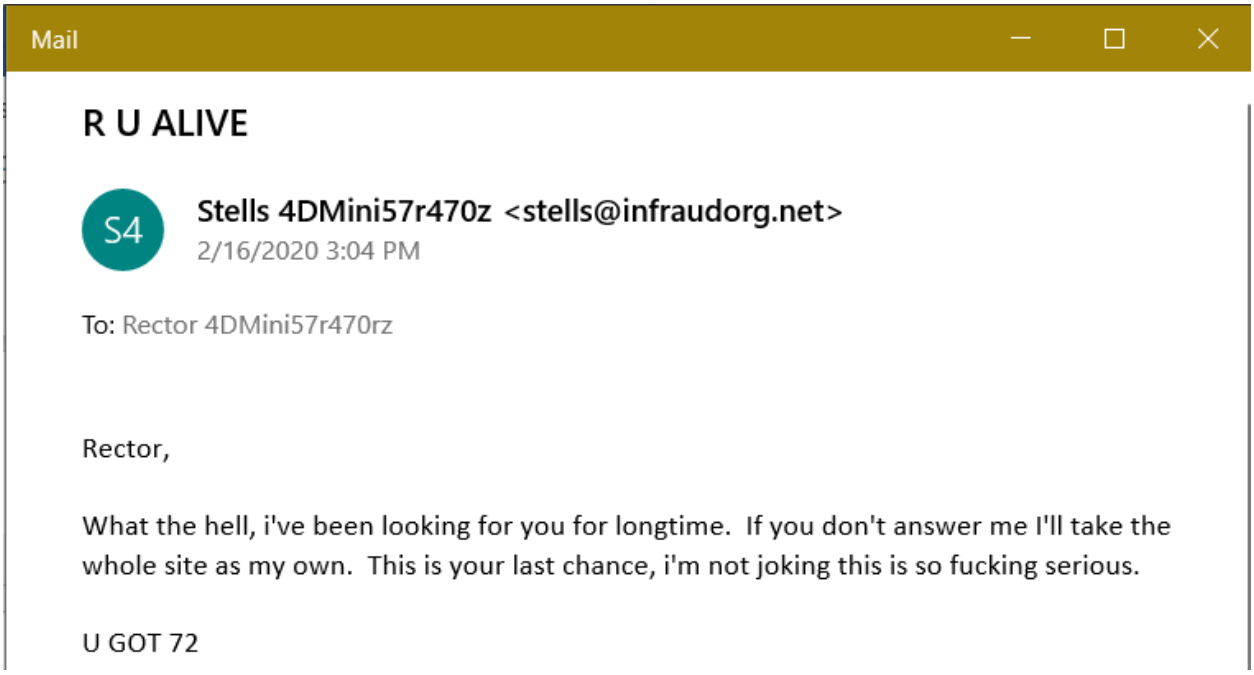
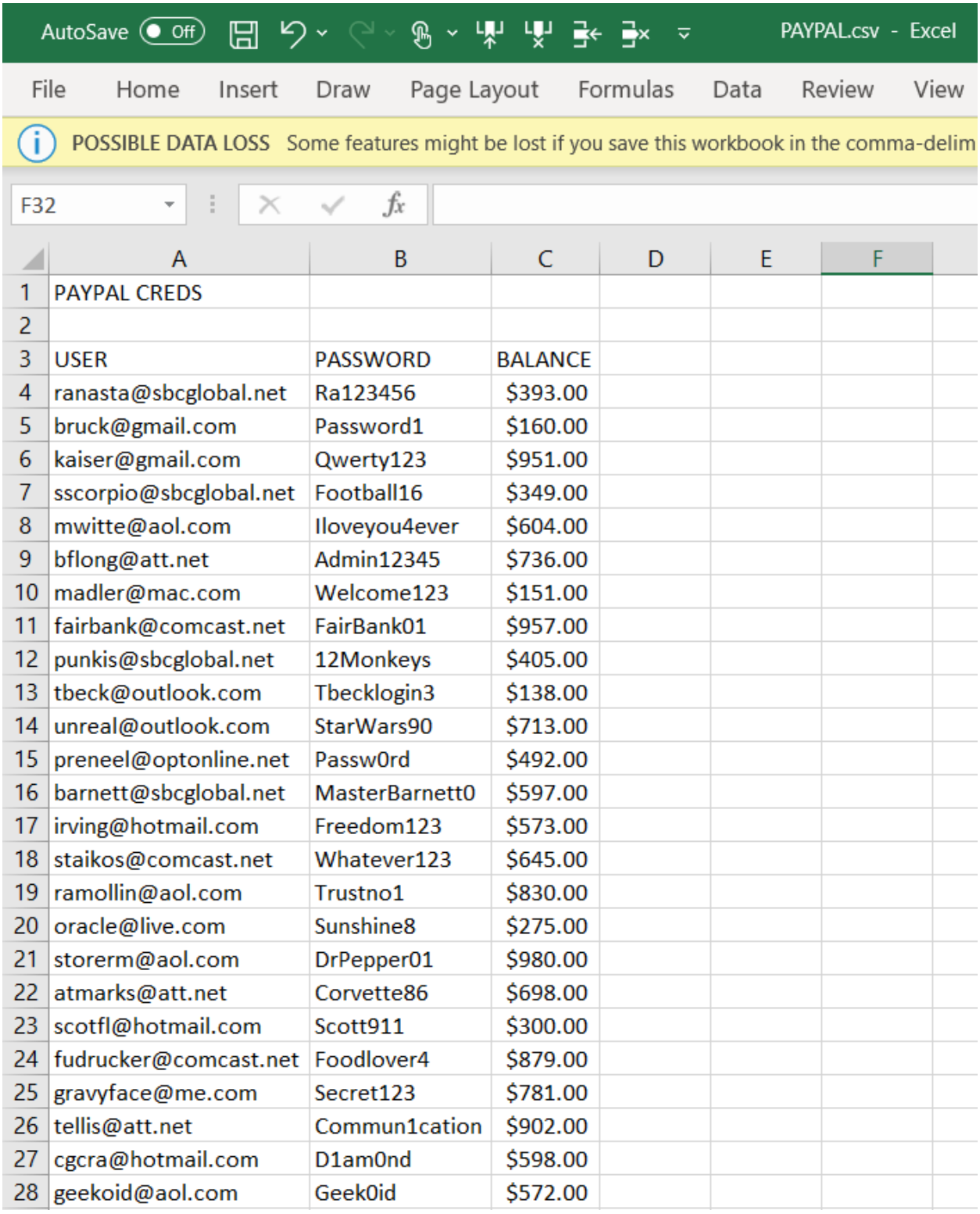


Figura 6: Correo electrónico enviado de Medvedev a Bondarenko.

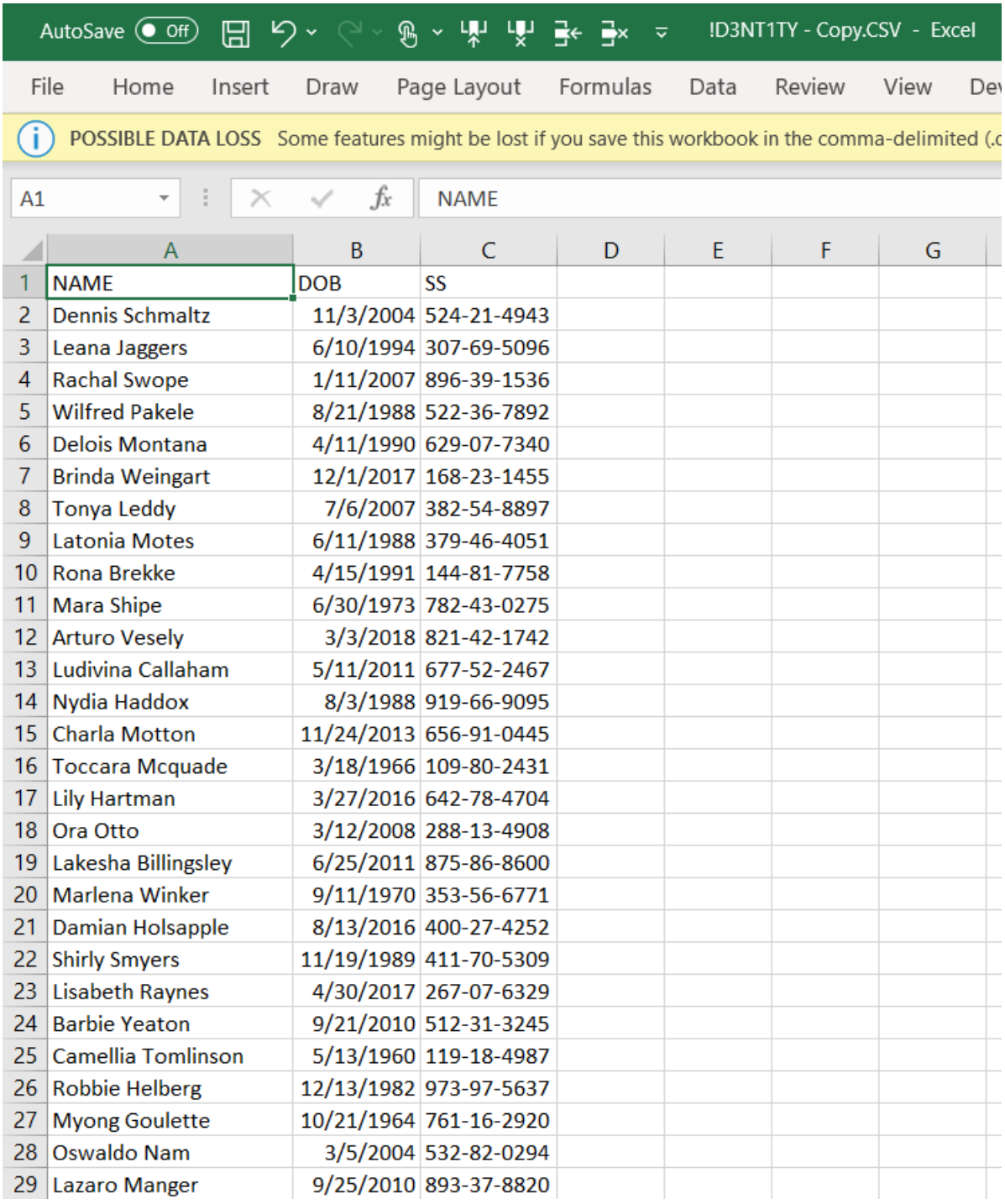
4. Archivo identificado como PayPal en el que se obtuvo información de cuentas paypal con credenciales de acceso y balances.



	A	B	C	D	E	F
1	PAYPAL CREDS					
2						
3	USER	PASSWORD	BALANCE			
4	ranasta@sbcglobal.net	Ra123456	$393.00			
5	bruck@gmail.com	Password1	$160.00			
6	kaiser@gmail.com	Qwerty123	$951.00			
7	sscorpio@sbcglobal.net	Football16	$349.00			
8	mwitte@aol.com	Iloveyou4ever	$604.00			
9	bflong@att.net	Admin12345	$736.00			
10	madler@mac.com	Welcome123	$151.00			
11	fairbank@comcast.net	FairBank01	$957.00			
12	punkis@sbcglobal.net	12Monkeys	$405.00			
13	tbeck@outlook.com	Tbecklogin3	$138.00			
14	unreal@outlook.com	StarWars90	$713.00			
15	preneel@optonline.net	Passw0rd	$492.00			
16	barnett@sbcglobal.net	MasterBarnett0	$597.00			
17	irving@hotmail.com	Freedom123	$573.00			
18	staikos@comcast.net	Whatever123	$645.00			
19	ramollin@aol.com	Trustno1	$830.00			
20	oracle@live.com	Sunshine8	$275.00			
21	storerm@aol.com	DrPepper01	$980.00			
22	atmarks@att.net	Corvette86	$698.00			
23	scotfl@hotmail.com	Scott911	$300.00			
24	fudrucker@comcast.net	Foodlover4	$879.00			
25	gravyface@me.com	Secret123	$781.00			
26	tellis@att.net	Commun1cation	$902.00			
27	cgcra@hotmail.com	D1am0nd	$598.00			
28	geekoid@aol.com	Geek0id	$572.00			

Figura 7: Archivo Paypal.

5. Archivo identificado como !D3NT1TY, en el cual se obtuvo data personal con nombres completos, números de seguro social y fechas de nacimiento.



	A	B	C	D	E	F	G
1	NAME	DOB	SS				
2	Dennis Schmaltz	11/3/2004	524-21-4943				
3	Leana Jaggers	6/10/1994	307-69-5096				
4	Rachal Swope	1/11/2007	896-39-1536				
5	Wilfred Pakele	8/21/1988	522-36-7892				
6	Delois Montana	4/11/1990	629-07-7340				
7	Brinda Weingart	12/1/2017	168-23-1455				
8	Tonya Leddy	7/6/2007	382-54-8897				
9	Latonia Motes	6/11/1988	379-46-4051				
10	Rona Brekke	4/15/1991	144-81-7758				
11	Mara Shipe	6/30/1973	782-43-0275				
12	Arturo Vesely	3/3/2018	821-42-1742				
13	Ludivina Callaham	5/11/2011	677-52-2467				
14	Nydia Haddox	8/3/1988	919-66-9095				
15	Charla Motton	11/24/2013	656-91-0445				
16	Toccara Mcquade	3/18/1966	109-80-2431				
17	Lily Hartman	3/27/2016	642-78-4704				
18	Ora Otto	3/12/2008	288-13-4908				
19	Lakesha Billingsley	6/25/2011	875-86-8600				
20	Marlena Winker	9/11/1970	353-56-6771				
21	Damian Holsapple	8/13/2016	400-27-4252				
22	Shirly Smyers	11/19/1989	411-70-5309				
23	Lisabeth Raynes	4/30/2017	267-07-6329				
24	Barbie Yeaton	9/21/2010	512-31-3245				
25	Camellia Tomlinson	5/13/1960	119-18-4987				
26	Robbie Helberg	12/13/1982	973-97-5637				
27	Myong Goulette	10/21/1964	761-16-2920				
28	Oswaldo Nam	3/5/2004	532-82-0294				
29	Lazaro Manger	9/25/2010	893-37-8820				

Figura 8: Archivo ¡D3NT1TY con data de identidades.

6. Imagen recuperada de los archivos eliminados en la cual se observa una tarjeta de seguro social de alguna persona ajena al acusado.

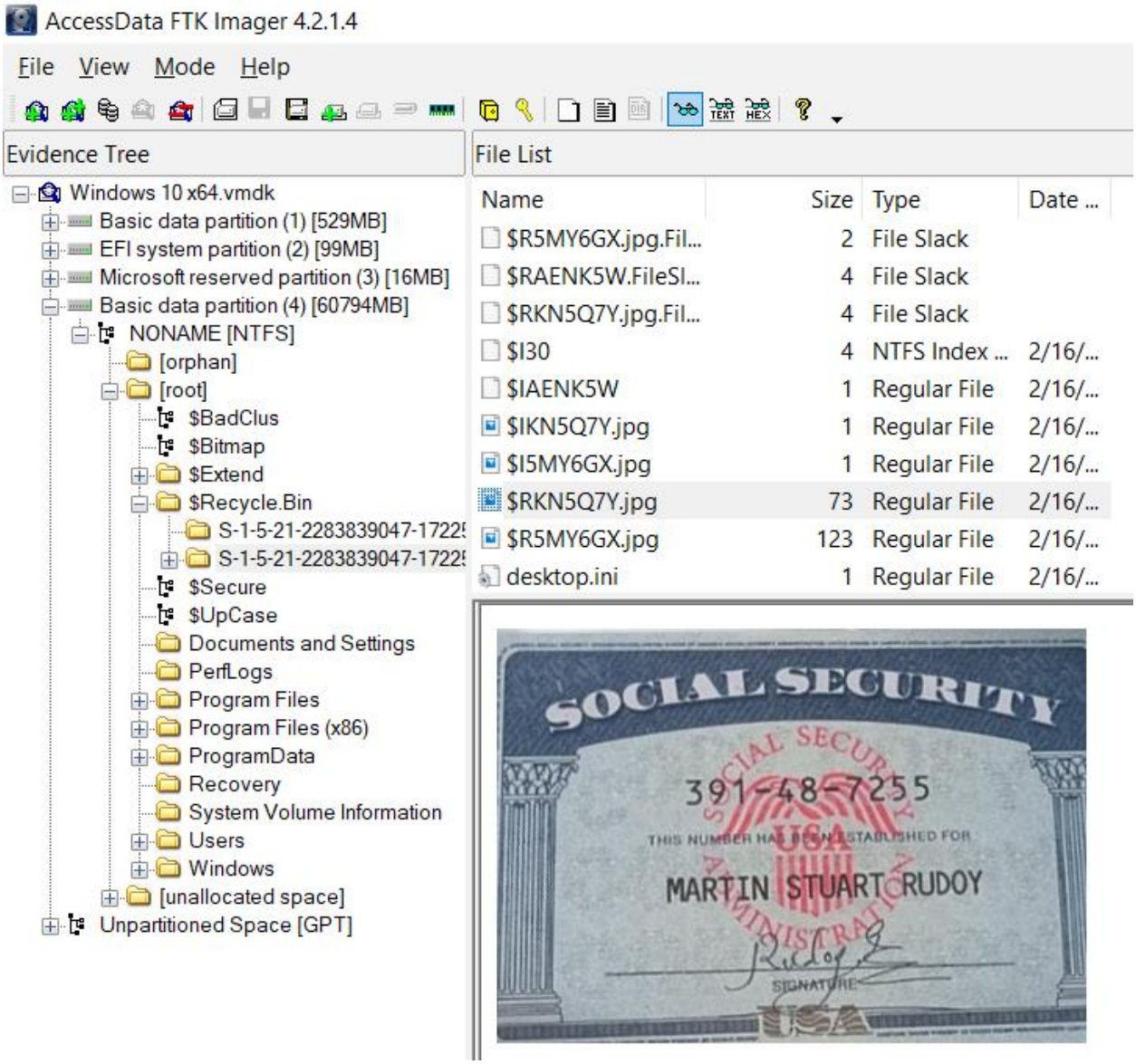


Figura 9: Foto borrada de seguro social.

7. Imagen recuperada de los archivos eliminados en la cual se observa otra tarjeta de seguro social de alguna otra persona ajena al acusado.

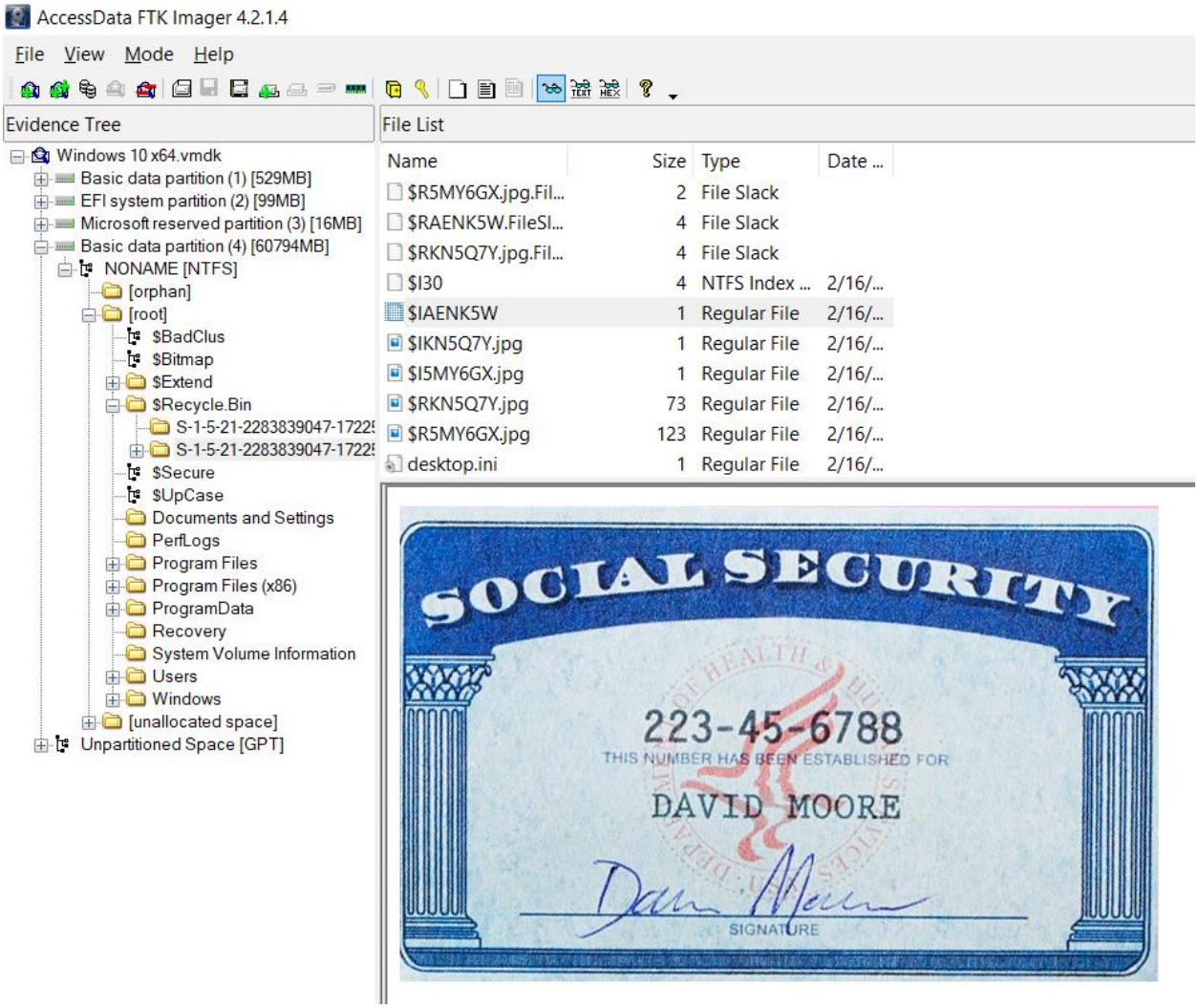


Figura 10: Foto borrada de seguro social.

Cadena de custodia

Primer Evento:

Descripción: Evidencia ofrecida por el Fiscal John P. Cronan a la examinadora Naomi I. Llinás Rosa. Dicha evidencia consiste en una imagen de un disco duro perteneciente a la maquina incautada al sospechoso Sergey Medvedev.

Evento Verificado por: Naomi I. Llinás Rosa y John P. Cronan

Numero de Evidencia: SM-001

Fecha y hora de comienzo: Febrero 15, 2020 – 9:00 AM

Fecha y hora de terminación: Febrero 15, 2020 – 9:30 AM

Lugar de Origen: Departamento de Justicia, Las vegas Nevadas

Destino: Laboratorio Forense – NIL Forensics, Puerto Rico

Segundo Evento:

Descripción: Creación de copia de imagen forense y almacenamiento de evidencia original

Evento Verificado por: Naomi I. Llinás Rosa

Numero de Evidencia: SM-001

Fecha y hora de comienzo: Febrero 16, 2020 – 10:14 PM

Fecha y hora de terminación: Febrero 16, 2020 – 10:20 PM

Lugar de Origen: Laboratorio Forense – NIL Forensics, Puerto Rico

Destino: Laboratorio Forense – NIL Forensics, Puerto Rico

Tercer Evento:

Descripción: Análisis y extracción de evidencia

Evento Verificado por: Naomi I. Llinás Rosa

Numero de Evidencia: SM-001

Fecha y hora de comienzo: Febrero 16, 2020 – 11:00 PM

Fecha y hora de terminación: Febrero 17, 2020 – 8:30 PM

Lugar de Origen: Laboratorio Forense – NIL Forensics, Puerto Rico

Destino: Laboratorio Forense – NIL Forensics, Puerto Rico

Cuarto Evento:

Descripción: Entrega de evidencia e Informe Forense al Fiscal

Evento Verificado por: Naomi I. Llinás Rosa y John P. Cronan

Numero de Evidencia: SM-001

Fecha y hora de comienzo: Febrero 18, 2020 – 10:30 AM

Fecha y hora de terminación: Febrero 18, 2020 – 11:30 AM

Lugar de Origen: Laboratorio Forense NIL Forensics, Puerto Rico

Destino: Oficina Administrativa FBI, Las Vegas Nevadas

Procedimiento

A continuación, se presentan en detalle los procedimientos realizados para realizar el análisis de la evidencia SM-001 y la extracción de la data.

1. Crear caso y copia de la imagen forense con la herramienta FTK Imager.

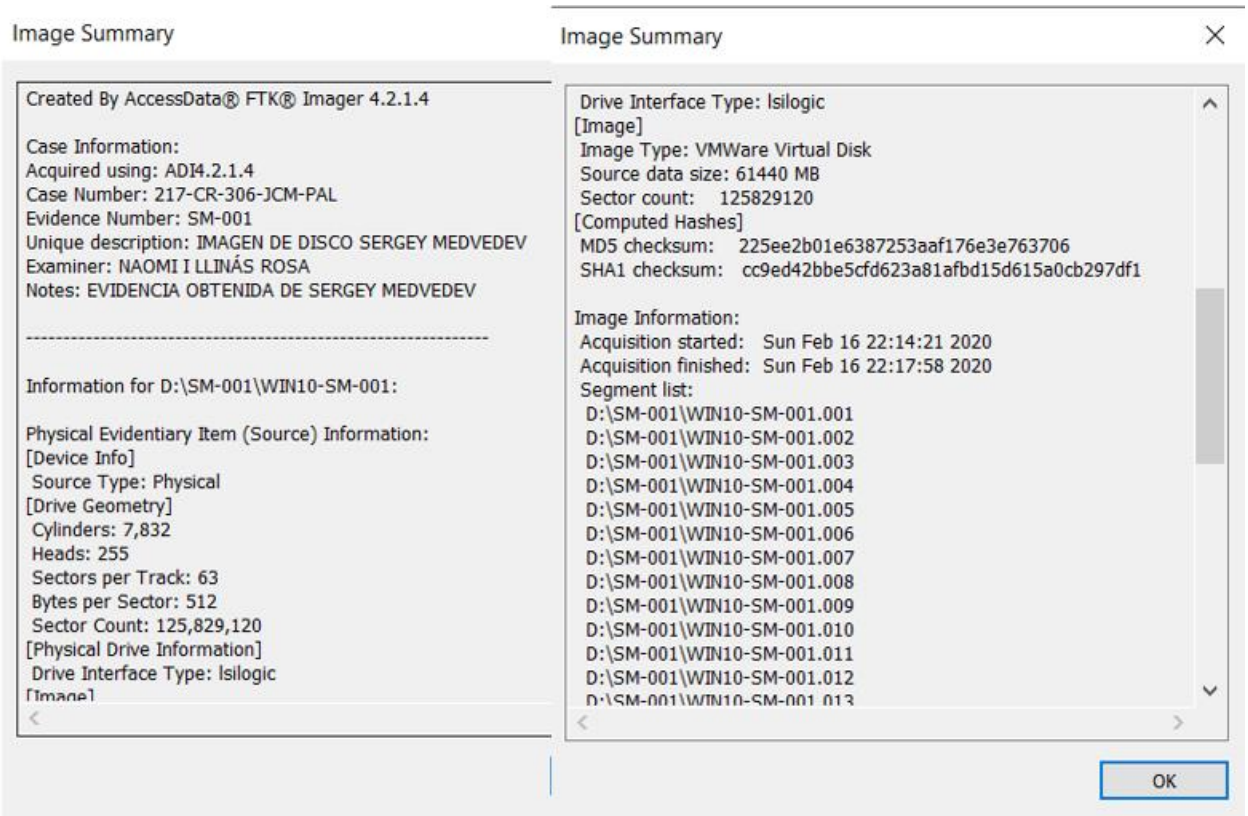


Figura 11: Caso creado con evidencia añadida y número de hash.

2. Examinación de archivos bajo el usuario Stells e identificación de correos electrónicos en la carpeta designada sin localidad. Cabe la posibilidad de que se guardaran estos archivos en esta partición en el disco para evitar ser descubiertos (Figuras 12 a la 15).

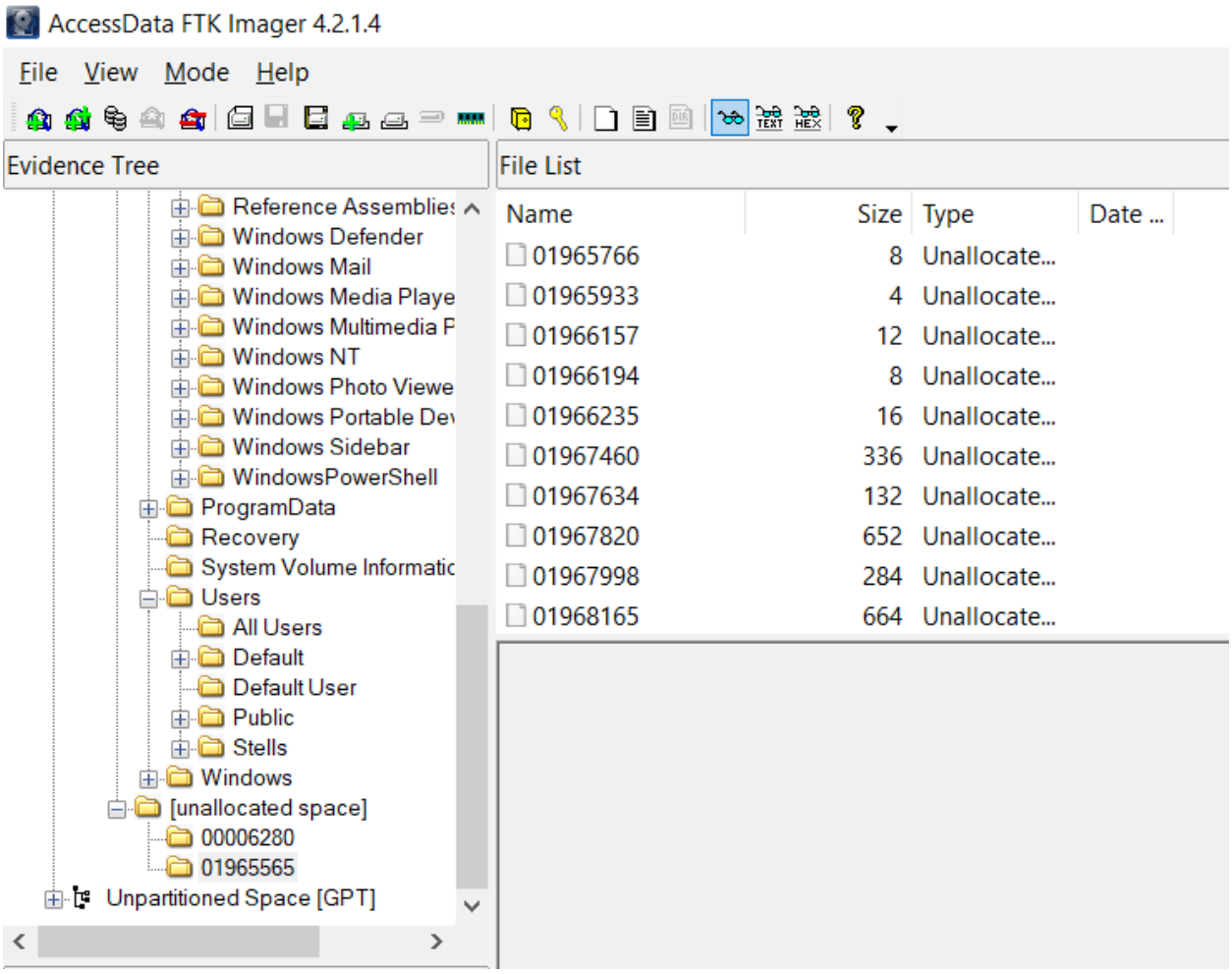


Figura 12: Examinación de carpeta unallocated space.

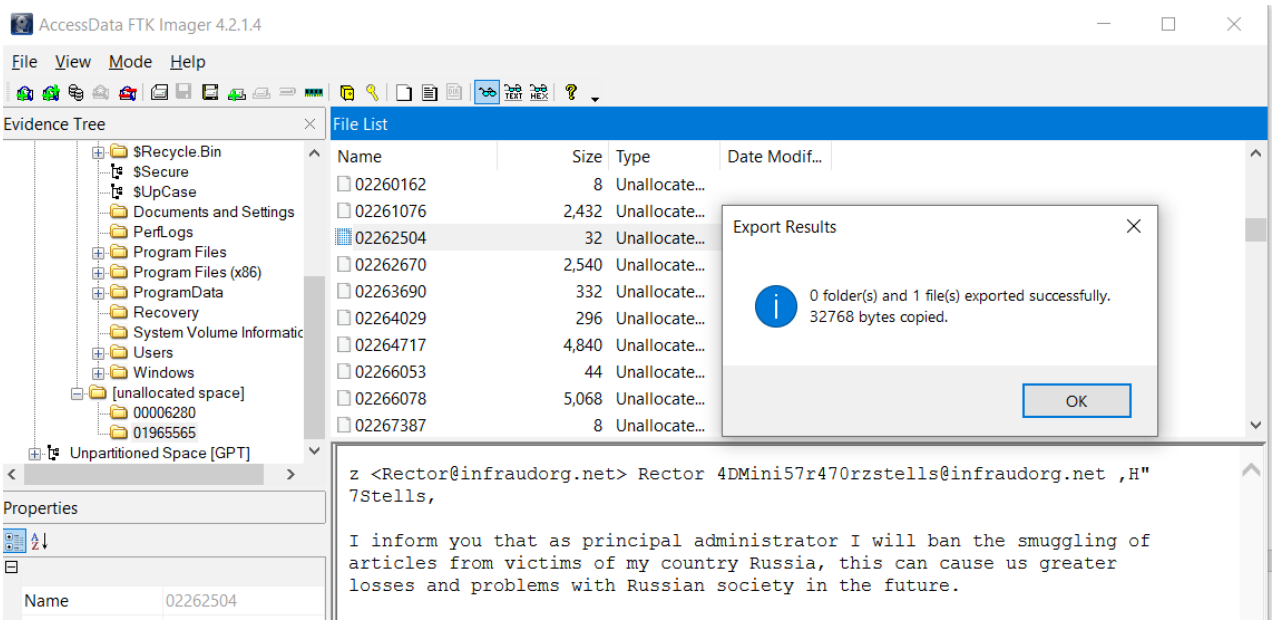


Figura 13: Exportación correo electrónico dirigido a Medvedev a.k.a Stells, proveniente de Bondarenko a.k.a Rector

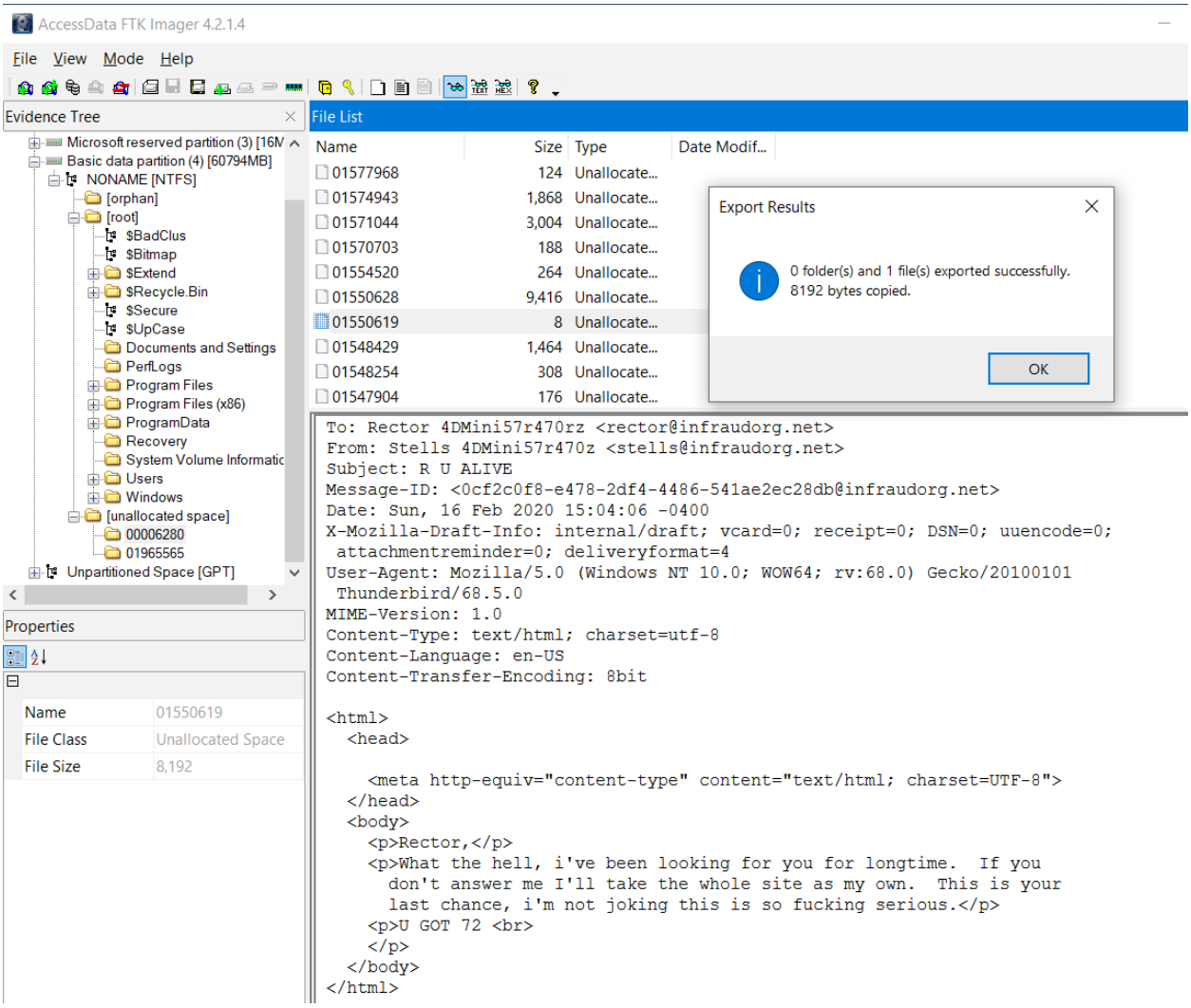


Figura 14: Exportación correo electrónico enviado por Medvedev a.k.a Stells, hacia Bondarenko a.k.a Rector.

3. Exportación de correo electrónico en el cual se incluye archivo png.

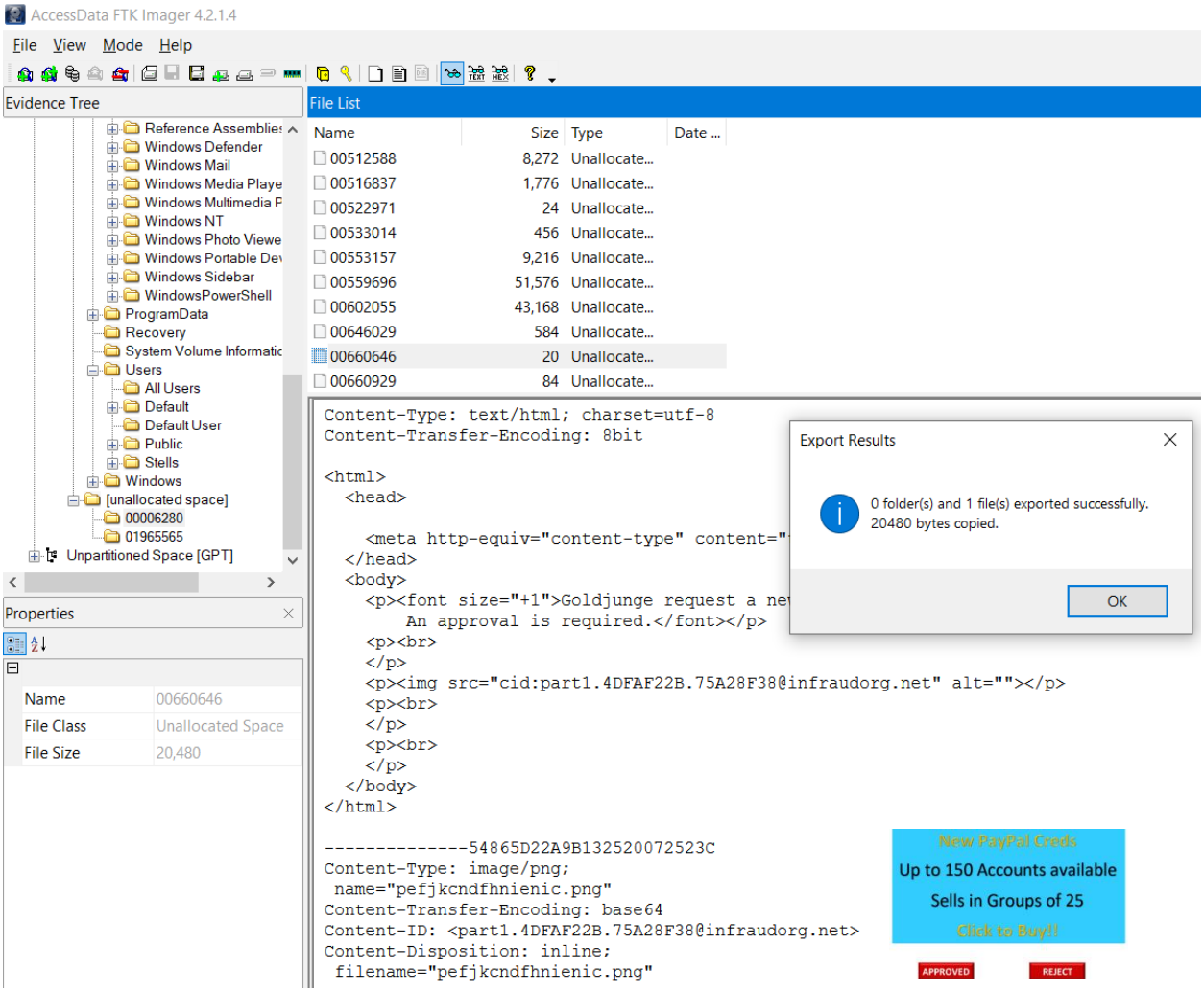


Figura 15: Exportación de archivo.

4. Cambio de extensión de archivos a .eml, formato de correo electrónico para abrir y obtener una imagen legible (Figuras 4 a la 6).

5. Examinación de archivos ubicados en la carpeta de documentos (Figuras 16 y 17).

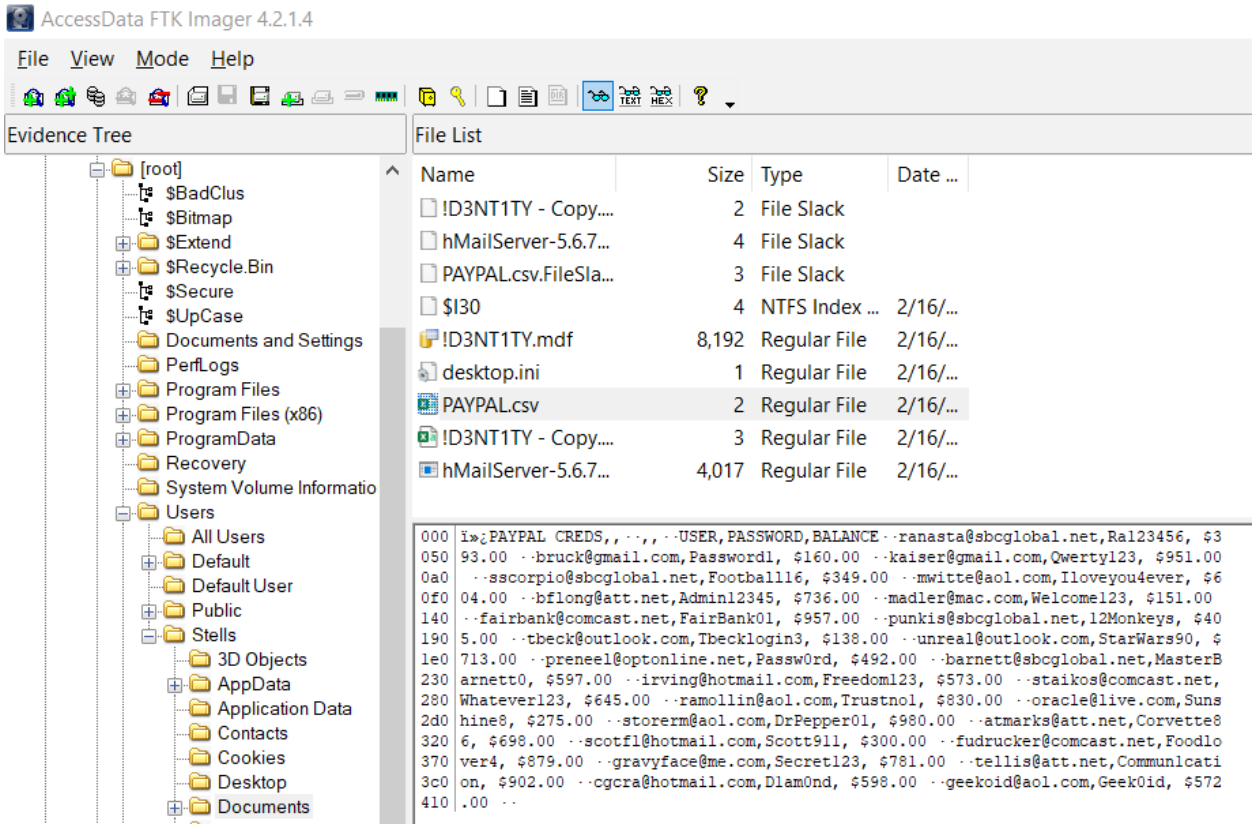


Figura 16: Archivo llamado Paypal identificado en la carpeta de documentos

.

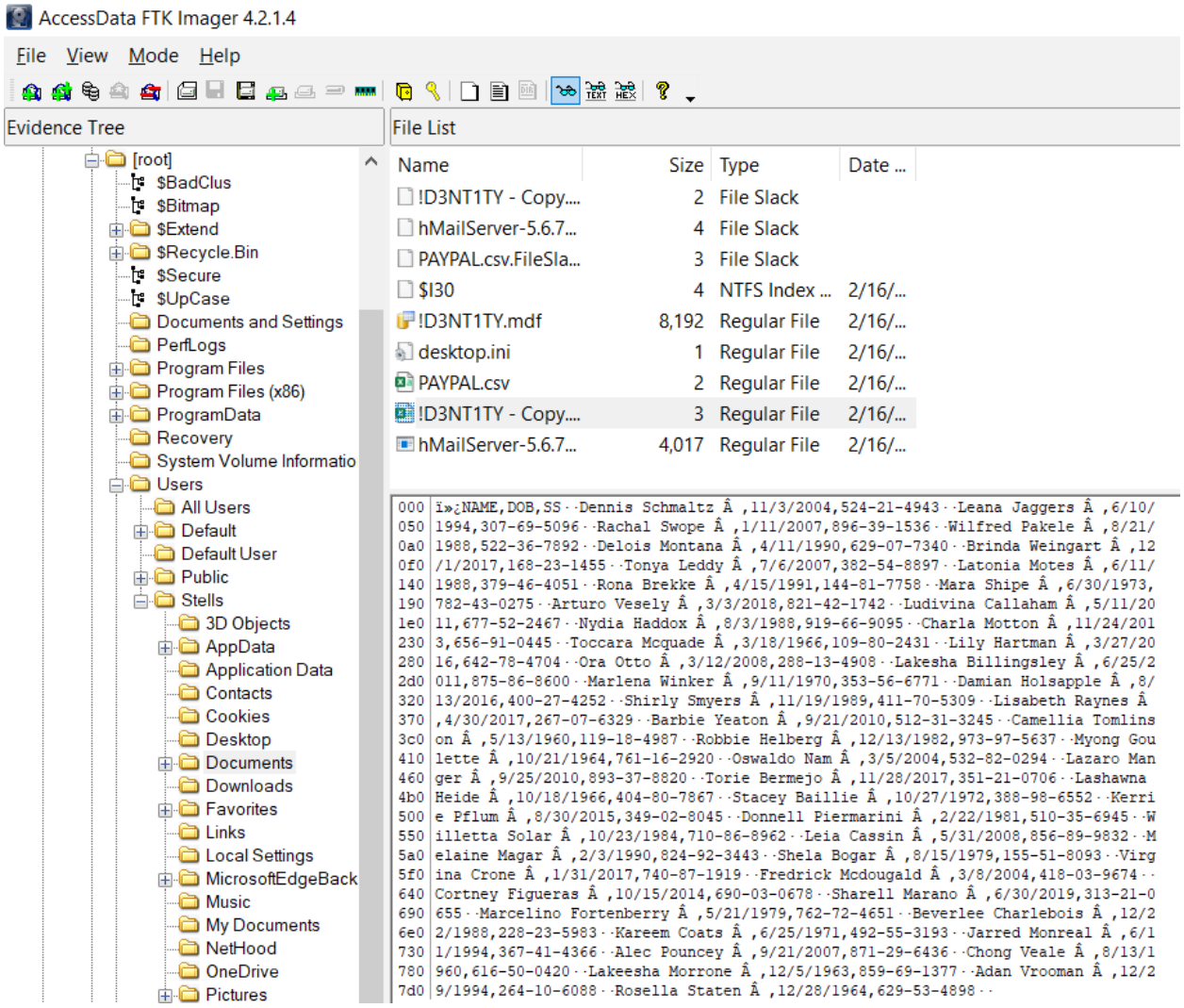


Figura 17: Archivo llamado Paypal identificado en la carpeta de documentos

6. Exportación de archivos en formato Excel nombrados ¡D3NTITY y Paypal. (Figuras 7 y 8)
7. Examinación de archivos eliminados, mediante la cual se hallaron dos tarjetas de seguro social. (Figuras 9 y 10)
8. Una vez concluida la examinación del disco se procede a validar el hash para asegurar la integridad de la imagen.

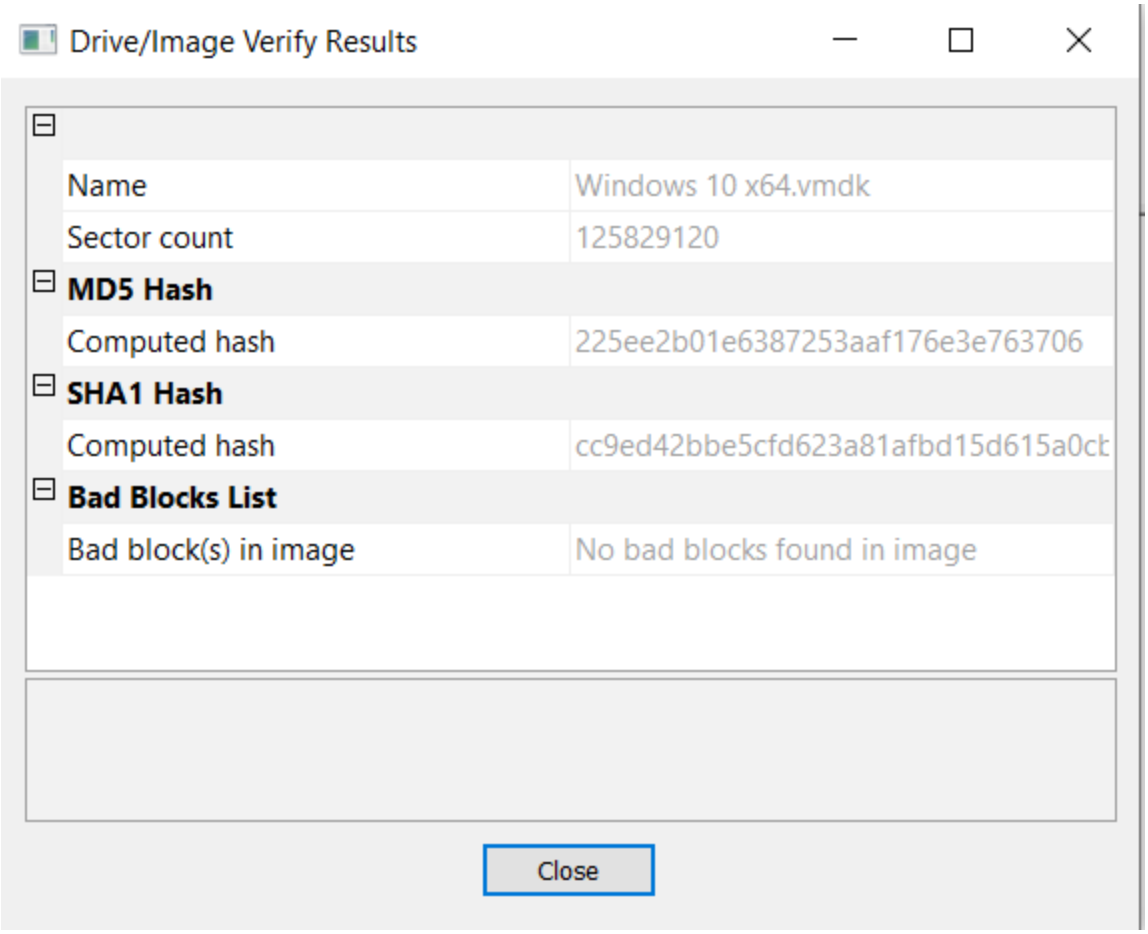


Figura 18: Confirmación de hash una vez culminada la examinación.

Figura 18: Confirmación de hash una vez culminada la examinación.

Conclusión

Una vez completada la examinación total y análisis de la evidencia suministrada, se determina por los hallazgos que existe relación directa entre el acusado y el esquema presentado. Se halló un usuario identificado como Stells, alias de Sergey Medvedev bajo el cual se identificaron diferentes archivos que lo ubican en la escena. Existen varios correos electrónicos que demuestran que Medvedev era uno de los administradores de la plataforma

Infraud. También se hallaron documentos con información sumamente relevante al caso en sus directorios principales. Mas aun, se hallaron dos (2) archivos que a pesar de los intentos por eliminar o sacar de las carpetas visibles aun residen en el disco, y estos son documentos con información de identidad ajenas a la del propietario de este equipo. Se concluye este reporte con hallazgos íntegros, confiables y en cumplimiento con los estándares de la industria y según lo establece el gobierno federal.

V. DISCUSIÓN DEL CASO

Los hechos llevados a cabo por los miembros de la organización criminal Infraud provocaron daños de una gran magnitud. Según se expone en el informe forense muchas de las acusaciones emitidas por el Departamento de Justicia en contra de dicha organización y sus miembros tienen una base fundada y evidencia que así lo demuestra. Existen archivos y conversaciones entre miembros que aclaran cualquier duda de relación existente.

Esta organización permaneció activa por siete (7) años consecutivos provocando pérdidas a un sin número de personas y organizaciones alrededor de mundo. Los países involucrados en este fraude hasta la fecha lo son Estados Unidos, Australia, Reino Unido, Francia, Italia, Kosovo y Serbia, lugares en los cuales han sido detenidos algunos de los miembros. Se estima que los daños provocados por la Organización Infraud son de aproximadamente $530 millones a individuos, comerciantes, e instituciones financieras. También se estima que esta organización sea la responsable de aproximadamente $2.2 billones en pérdidas adicionales.

Para las víctimas este ataque representa un problema mayor ya que no tan solo están teniendo pérdidas monetarias, sino que también su identidad y sus bienes están en un riesgo mayor. Según el análisis realizado esta organización tenía usuarios a nivel mundial por tanto su nivel de alcance maligno es bastante extenso, ya que contaban con aproximadamente 10,901 miembros en el año 2017. Tomando en consideración que de los 36 individuos acusados solo 13 están apresados, es una cifra alarmante. Las evidencias halladas contribuyen a la disolución

de este tipo de organizaciones y brindan herramientas a los respectivos departamentos de justicia para dar un alto en contra de este tipo de movimientos criminales.

VI. AUDITORÍA Y PREVENCIÓN

Trasfondo, alcance y objetivos

Esta auditoría está dirigida a los procedimientos llevados a cabo por individuos y compañías con relación al manejo de documentos personales e información sensitiva. Lo que se busca es identificar las fallas generales cometidas que llevan a una exposición de data mediante la cual se generan daños a terceros. Tal cual los miembros de Infraud llevaron a cabo, esta organización ciber criminal sacó provecho de unas vulnerabilidades ya existentes. Fue de esta manera que lograron una operación de tráfico de tarjetas de débito y crédito e identidades por siete años consecutivos evitando ser atrapados. Mediante esta auditoría se procura esclarecer como estos miembros se hacían de esta data para luego dejarla expuesta ante el mercado de la *Deep Web.*

Hallazgos detallados y recomendaciones

Hallazgo 1 – Medidas pobres contra Phising.

Condición – Falta de medidas en los correos electrónicos y poca educación por parte de los usuarios.

Criterio – Las compañías, deben contar con unas políticas establecidas en sus correos electrónicos que restringen el acceso de data conflictiva e identificada como posible phishing a su red.

Causa – Esto es provocado por una falla a nivel de compañías y a nivel de individuos una ausencia de control.

Efecto – Por consiguiente, esto puede provocar que se brinde información personal a personas desconocidas y ajenas a la compañía que solo buscan hacer daño.

Recomendaciones – No brindar información sensitiva vía teléfono o internet a personas desconocidas aun cuando estas se identifiquen como miembro de alguna organización conocida.

No acceder a páginas web conocidas mediante enlaces incluidos en comunicaciones electrónicas.

Utilizar herramientas diseñadas para controlar los correos phising.

Hallazgo 2 – Contraseñas no seguras

Condición – Usuarios con contraseñas comunes sin nivel de complejidad y una misma utilización para diferentes accesos.

Criterio – La contraseña segura debe cumplir con una cantidad de caracteres específicos y con unos requisitos especiales.

Causa – Esto es una falla de control provocada por el usuario.

Efecto – La utilización de una contraseña común lleva a ser descifrada con mayor facilidad y a su vez queda expuesta la data.

Recomendaciones – Se recomienda crear contraseñas un mínimo de 8 a 12 dígitos, incluyendo caracteres especiales, números, letras mayúsculas y minúsculas.

Hallazgo 3 – Accesos a conexiones Wi-Fi

Condición – En las bitácoras de historial se hallan varias conexiones Wi-Fi a puntos externos y sobre todo públicos.

Criterio – Para asegurar la integridad de un equipo se previene exponer el mismo a conexiones abiertas a todo público.

Causa – Establecer conexiones automáticas, de esta manera se pierde el control de ver y asegurar a donde se está exponiendo el equipo y la data.

Efecto – Data interceptada por terceros.

Recomendaciones – Hacer conexión solo en las redes conocidas y de preferencia que requieran clave de acceso.

Recomendaciones Adicionales

A fines de proteger la información personal de cada uno, La Comisión Federal de Comercio, (s.f.) brinda varias recomendaciones que contribuyen a minimizar el riesgo de ser víctima de fraude.

1. Al momento de desechar un dispositivo electrónico es de suma importancia destruir toda la data almacenada. Para lograr esto se deben restablecer el equipo a su configuración original, de manera que todo quede eliminado. En el caso que el equipo no encienda lo más recomendable es destruir el disco duro.
2. Instalar programas antivirus y firewall para proteger el tráfico de data desde y hasta el equipo.

3. No guardar información financiera junto con la conexión automática ya que eso va a provocar que en caso de que otra persona acceda al equipo también obtenga todas las credenciales y accesos.

VII. CONCLUSIÓN

Al finalizar toda la investigación del caso en contra de la Organización cibercriminal Infraud, y analizar toda la evidencia obtenida, llego a la conclusión de que en definitiva los acusados de este fraude, están totalmente vinculados a las acusaciones. Según se demostró los miembros de esta organización se dedicaban a traficar data de una manera natural sin importar el daño ocasionado por sus acciones. Cabe recalcar que estas personas no tenían ningún tipo de remordimiento ya que se dedicaron a esto por siete (7) años consecutivos, traficando data de hombres, mujeres, adolescentes y niños sin ninguna excepción provocando pérdidas y destrucción a las víctimas.

Desde un punto de vista oficial, los individuos y agencias deben tomar mas seriedad y sobretodo responsabilidad en el manejo y almacenamiento de la data. Todo el mundo se debe educar para protegerse de manera correcta ante este tipo de criminales y ataques cibernéticos. Hoy día la data ha adquirido gran valor en el mercado ilícito. Es decir, la información personal, de valor y confidencial se debe compartir meramente cuando sea requerido y de manera segura.

En lo personal, al realizar esta investigación puedo ver la magnitud del asunto. En realidad, si existe el peligro de ser atacado cibernéticamente, y la mayoría de las personas toma este tema sin la delicadeza de requiere. La humanidad se esta volviendo a lo tecnológico y así mismo se exponen unos a los otros, esto va desde lo mas simple que es crear un correo electrónico hasta establecer un acceso a cuentas bancarias. En general todas estas interacciones conllevan una conexión a internet en la cual siempre existirá un riesgo de que

nuestro tráfico de data sea interceptado por *hackers.* Entiendo que todos debemos en la manera posible proteger nuestra información y prevenir tener escapes de data siendo responsables y prudentes con el manejo de la data dentro y fuera del internet.

VIII. REFERENCIAS

Access Data FTK. (2020). *Access Data*. Obtenido de Forensic Toolkit: https://accessdata.com/products-services/forensic-toolkit-ftk

Carrier, B. (2020). *Sleuthkit Autopsy*.. Obtenido de Autopsy: https://www.sleuthkit.org/autopsy/

Center of Victim Research. (2016). *Center of Victim Research*. Obtenido de https://ncvc.dspacedirect.org/bitstream/item/1228/CVR%20Research%20Syntheses_Identity%20Theft%20and%20Fraud_Brief.pdf

Cornell Law School. (s.f.). *Cornell Law School*. Obtenido de Law Cornell: https://www.law.cornell.edu/wex/es/fraude_con_tarjeta_de_cr%C3%A9dito

Cornell Law School. (s.f.). *Cornell Law School*. Obtenido de Law Cornell: https://www.law.cornell.edu/uscode/text/18

Department of Justice. (2016). *The United States Department of Justice*. Obtenido de https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital

Douglas, R. (2020). *Consumer Affairs*. Obtenido de Consumer Affairs: https://www.consumeraffairs.com/finance/identity-theft-statistics.html

EGA futura. (s.f.). *EGA Futura*. Obtenido de https://www.egafutura.com/wiki-es/sistema-fuerza-ventas-sfa

ICE, D. d. (2017). *US Immigration and Customs Enforcement*. Obtenido de ICE: https://www.ice.gov/es/fraude-beneficios-identidad

La Comisión Federal de Comercio. (s.f.). *La Comision Federal de Comercio*. Obtenido de Información para consumidores: https://www.consumidor.ftc.gov/articulos/s0272-como-proteger-su-informacion-personal

Nvindi. (2019). *Mejores tarjetas de credito*. Obtenido de https://www.mejorestarjetasdecredito.es/codigo-de-seguridad-de-las-tarjetas-cvv/

Oficina de Seguridad del Internauta. (2016). *Oficina de Seguridad del Internauta*. Obtenido de OSI: https://www.osi.es/es/actualidad/blog/2016/10/11/malware-cual-es-su-objetivo-y-como-nos-infecta

Pérez, E. (2019). *Derecho de la red*. Obtenido de Derecho de la red: https://derechodelared.com/carding/

Thomas J Holt, B. H. (2011). Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications. En B. H. Thomas J Holt, *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (págs. 139-140). New York: IGI Global.

United States of America v. Arthur Budovsky, 13 cr 368 (United States District of New York 23 de May de 2013).

United States of America v. Rafael Joaquin Beltre Beltre, 3:11-cr-00589-GAG-MEL (United States District of Puerto Rico 22 de March de 2012).

United States of America v. Romeo Vasile Chita, 1:10CR392 (United States District of Ohio Eastern Division 20 de October de 2011).

United States of America v. Svyatoslav Bondarenko, 2:17-cr-306-JCM-PAL (United States District of Nevada 20 de January de 2018).