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

# Estudio de fraude al Medicare: El caso de Andrew Chmiel

Requisito Para La Maestría En Sistemas De Información
Con Especialidad En Seguridad De Información E Investigación De Fraude

DICIEMBRE, 2019

PREPARADO POR

ANGEL R. MERCDO ROBLES

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

**Estudio de fraude al Medicare: El caso de Andrew Chmiel**

Preparado por

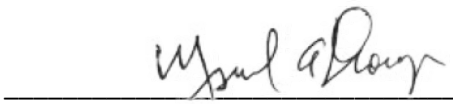
Angel R. Mercado Robles

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

Diciembre, 2019

Aprobado por:



Dr. Miguel A. Drouyn Marrero, Profesor

TABLA DE COTENIDO

LISTA DE FIGURAS

Figura 32. Entrar la clave de usuario y la dirección de correo de Andrew Chmiel requería del uso de Nirsoft (Nirlauncher). Del listado de programas, se utilizó la opción llamada WebBrowserPassView. Se identifica la dirección donde se sitúa el programa Nirsoft (Nirlauncher).

Figura 33. Del listado, se escoge la opción llamada WebBrowserPassView.

Figura 34. Con la información de correo obtenida, se ingresa a la misma utilizando algún explorador de internet.

Figura 35. Backuptrans Android SMS Backup and Restore.

Figura 36. Uso de Backuptrans Android SMS Backup and Restore. Pantalla inicial.

Figura 37. Conectar el celular de Andrew Chmiel a la laptop de forense.

Figura 38. Backuptrans Android SMS Backup and Restore comienza cargando los mensajes.

Figura 39. Backuptrans Android WhatsApp se utiliza para cargar los mensajes del celular de Andrew Chmiel. Los textos por WhatsApp son la prioridad. Se ejecuta el programa inicialmente.

Figura 40. Se conecta el celular de Andrew Chmiel a la laptop de forense.

Figura 41. El programa comienza a extraer los textos.

# 1. INTRODUCCIÓN Y TRASFONDO

## Introducción

En estos tiempos de grandes avances y logros en tecnología, debemos tener en cuenta que todavía, en gran medida, el factor humano sigue detrás de todo acontecimiento y función de los medios y mecanismos que se supone sean los que nos ayuden a progresar. Dentro de tales mecanismos, el bienestar del ser humano es contrapuesto al bienestar económico de muchos que quieren aprovecharse de buenas intenciones, medidas, tanto como fallos en programación y medios de hacer que todo un sistema funcione. Casos como este nos permiten entender por qué a los contribuyentes les suben las primas, porque hay tantos documentos a escribir y firmar, por qué existen tantas fugas de dinero y la importancia de encontrar fallas a los sistemas a tiempo. Nos permite conocer la realidad de cómo se llevan a cabo estos trabajos ilegítimos, las personas envueltas y la manera de pensar para ejecutar tales acciones. Todos en general nos podemos beneficiar, ya sean, los pacientes, los que pagamos impuestos, los que quieren hacer negocios con el gobierno federal, los negocios de aparatos y dispositivos médicos que puedan caer bajo las leyes y políticas federales.

## Descripción del caso

### Número del caso

3:19-299

### Partes del caso

Acusado – Andrew Chmiel.

Victimas – Beneficiarios de Medicare, Programa de Medicare, Medicare.

Investigadores – Medicare Strike Force, FBI, U.S. Department of Health and Human Services Office of the Inspector General, Center for Program Integrity, Assistant Director Robert Johnson del FBI Criminal Investigative Division, Deputy Inspector General for Investigations Gary Cantrell del U.S. Department of Health and Human Services Office of Inspector General, Chief Don Fort del IRS Criminal Investigation and Deputy Administrator and Director of CPI Alec Alexander del CMS/CPI, Health Care Fraud Unit del Criminal Division Fraud Section.

Fiscales – Abogado Asistente General Brian A. Benczkowski, Abogada de U.S. Sherri A. Lydon, Abogado de U.S. Craig Carpenito, Abogada de U.S. María Chapa López.

Juez – Honorable Joseph F. Anderson, Corte de Distrito, Carolina del Sur

Trasfondo

Hay empresas que utilizan doctores de telemedicina a distancia, tanto como lugares de DME o Durable Medical Equipment que suplen y no están limitados a sillas de rueda, camas de hospitales, equipos de tracción, máquinas para riñones, maquinaria para personas que requieren dispositivos de alta calidad para poder caminar y/o mantener quieta algún área del cuerpo que tienen dañada o en mejora. Entonces tenemos a Medicare, con las cubiertas tipo A, B y C. Algunas de tales cubiertas tratan con empresas DME para ayudar a costear por los equipos que los pacientes requieran de esa índole. Para que esas empresas DME puedan ayudar a brindar servicio/equipo para los pacientes, tienen que ser también referidos por los doctores que en específico puedan firmar, recomendar y hasta poder justificar que ese paciente particular requiere de esos servicios/equipo y a su vez el DME pueda cobrarlo al Medicare. Estas DME, doctores y servicios toman acción en diversos

estados, tales como Carolina del Sur, Nueva Jersey, Florida y llegando hasta las Filipinas (Department of Justice, 2019, abril).

Como parte de los doctores que se les hizo el acercamiento para llevar a cabo estas firmas y envío de pacientes para recibir estos servicios y prueba para recibirlos (sean servicios que les hagan o no falta) tenemos al doctor Hilton Head, entre otros, que notaron ciertas anomalías de pedido y oferta, lo cual, provoco que lo anunciaran al FBI para mayor atención e investigación. Todo esto llevo al descubrimiento de un esquema a gran escala, en donde varias empresas, dueños y codueños fueron hallados en tener que ver en acciones de conspiración, desvió de fondos, uso de cuentas "Shell", "Straw Owner" y diversos mecanismos para defraudar a Medicare, DME y el uso de empresas de tele mercadeo para interactuar con los pacientes y llevar a cabo la venta de servicios y equipo, lo cual, para mala noticia de los pacientes, eran equipo de baja calidad de China y por ende, bajo costo, aunque los cobros a Medicare fueron como si fuesen equipos de alta calidad de DME autorizados. Esto también iba de la mano con cuentas en altamar en Filipinas, sobornos a médicos, dueños de empresas DME, lavado de dinero, propietarios ocultos y miles de equipos de realmente no eran requeridos ni necesarios por los pacientes. Tales conspiraciones y sobornos generaron alrededor de mil millones de dólares en pagos ilegales por parte de Medicare a los DME y conspiradores. Esto llevo a una de las personas clave en este trasunto, un hombre de 43 años de edad, que vive en Mount Pleasant, llamado Andrew Chmiel, del cual se desprende cargos por lavado de dinero, fraude de correos, conspiración y hacer declaraciones falsas (Monk, 2019, abril).

Esto significa que miles de pacientes envejecientes y discapacitadas fueron atraídas a este esquema criminal y ordenaron tanto braces, dispositivos de cuello, sillas de rueda,

dispositivos para brazos y piernas lo cual eran totalmente innecesarias para ellos. Por ello ya ha habido más de 80 pedidos de registro en 167 distritos federales y que han sido servidos (Department of Justice, 2019, mayo).

Las ganancias ilícitas han sido utilizadas para la compra de yates, carros exóticos y casas de lujo. La conspiración utilizó anuncios en la televisión y anuncios en la red de internet, tanto como "call centers" internacionales para llevar a cabo las llamadas y pedidos. El caso todavía está en espera de otras vistas ya que todavía el mismo no ha culminado y esta información es hasta ahora la que se ha logrado capturar (Department of Justice, 2019, abril).

Descripción de los hechos

1- El acusado Andrew Chmiel defraudo a los Estados Unidos, Medicare y pacientes de Medicare mediante un esquema de contragolpe que situaba las ganancias por encima del cuidado a los pacientes.
2- El acusado Andrew Chmiel tiene interés de propietario de las siguientes compañías DME:
    a- Advantage Orthopedic Systems, Inc.
    b- B&L Medical Supply, Inc.
    c- Cumberland Medical Equipment, Inc.
    d- D2 Medical, LLC.
    e- In-Home Senior Care, LLC.
    f- Family Home Medical Equipment & Supplies, LLC.
    g- Magnolia Medical Supply Inc.

h- Medical Equipment Solutions of Southeast Florida, LLC d/b/a Medical Equipment Solutions.

i- Triana Enterprises, LLC d/b/a Triana Medical Supplies.

j- Wren Senior Services, LLC d/b/a Dogwood Medical.

3- El acusado Andrew Chmiel tiene interes de propietario de las siguientes companies "drop-ship" o almacen de entrega directa:

a- Bentley Medical Products.

b- Jacmart Medical.

4- El acusado Andrew Chmiel tiene interés de propietario de las siguientes compañías lo cual tenían la habilidad de venta y cobro a Medicare:

a- DO Delivery, a/k/a "Doctor Order Delivery".

b- Pain Center, LLC.

5- Andrew Chmiel es acusado de infringir en el Anti-Kickback Statute.

6- Andrew Chmiel es acusado de Conspiración.

7- Andrew Chmiel es acusado de utilizar medios del correo para envío de concepto personal y de las empresas para propósitos ilícitos.

8- Andrew Chmiel es acusado de llevar a cabo actividades criminales a conciencia y ejecutados hacia Medicare para defraudar los programas de servicio de salud.

9- Andrew Chmiel es acusado de mentirle a un agente federal mediante una investigación, en donde dijo, a conciencia, que no sabía que sus compañías/empresas habían utilizado prescripciones médicas de la telemedicina o tele-doctores para el envío de tales datos a Medicare.

10- Andrew Chmiel es acusado de mentirle a un agente federal al decir que había llevado a cabo actos ilícitos con la sobrina de un amigo filipino cuando en realidad era la hija de uno de los co-conspiradores de tales actos.

11- Andrew Chmiel es acusado de cometer actos de conspiración y lavado de dinero.

Acusaciones, cargos y penalidades

1- Conspiración

Violación de 18 U.S.C. § 287, 1341, 1343 y 1347.

Deben entregar a los Estados Unidos toda propiedad, real o personal, derivada por lo que proceda de lo obtenido por tales actos.

Multa de $250,000 y no más de 3 años de cárcel.

2- Fraude al Correo

Violación del título 18, Código de Estados Unidos, Sección 1341.

Debe entregar toda propiedad real o personal derivada del uso del mismo.

Multa de $250,000 y no más de 20 años de cárcel.

3- Fraude al Health Care

Violación del título 18, Código de Estados Unidos, Sección 1347.

Debe entregar toda propiedad real o personal derivada del acto ilícito llevado a cabo.

Multa de $250,000 y no más de 20 años de cárcel.

4- Declaraciones Falsas

Violación del título 18, Código de Estados Unidos, Sección 1001.

Debe entregar toda propiedad real o personal derivada de las declaraciones falsas.

Multa de $250,000 y no más de 10 años de cárcel.

5- Lavado de Dinero

Violación del título 18, Código de Estados Unidos, Sección 1956.

Debe entregar toda propiedad real o personal derivada de los actos ilícitos llevados a cabo y las ganancias de las mismas.

Multa de $250,000 y no más de 10 años de cárcel.

6- Las entregas de propiedad y bienes incluyen, pero no son limitadas a:

18 U.S.C. §§ 981(a)(1)(C), 982(a)(1) y 982(a)(7) y 28 U.S.C. §2461(c).\

Multa de $250,000 y no más de 10 años de cárcel.

7- Procedencias de Cash/Forfeiture Judgment:

U.S.C. §§ 371, 287, 1001, 1341, 1343 y 1347.

Multa de $250,000 y no más de 5 años de cárcel.

Definición de términos

1- DME – Durable Medical Equipment. Consiste en los lugares y empresas que brindan servicios y equipo como sillas de rueda, camas de hospitales, entre otros.
2- Shell Company – Medio por el cual puede ser utilizado para esconder la identidad del dueño, activos y es legal, en cuestión de protección del dueño (EGPD, 2019).
3- Drop Shipping – Cadena de manejo de suplido el cual el retailer o detallista no mantiene en stock o guardado en mercancía los dispositivos o aparatos a vender. Deja que el lugar haga tanto el encargo y envío de los mismos.
4- Retail – Proceso de vender bienes o servicios a un consumidor por distintos canales.

5- Straw Owner – Alguien que es dueño legalmente de una propiedad o apariencia legal, escondiendo por medios legales el dueño real, sea por propósitos legales o ilegales.
6- Kickback Scheme – Esquema de contragolpe. Es el pago ilícito a entes por el cual se dan intercambios de favores y se reciben pagos por el mismo. La remuneración se habla de antemano y ofrece una ventaja competitiva ilícita.
7- Ownership Interest – Interés del propietario. Indica por medio de certificados o medios legales el ser dueño de tales activos o propiedad.

## 2. REVISIÓN DE LITERATURA

### Introducción

En este trabajo realizado tomamos en cuenta diversos datos que provienen de investigaciones presentadas en corte, también tomando en cuenta lo que otros cuerpos de investigación hallaron. Desde el momento que se trajo a atención sobre unos actos que aparentemente estaban ocurriendo, sobre un esquema de fraude a Medicare y el cómo estaba siendo llevado a cabo, múltiples grupos fueron involucrados, tanto de seguridades, auditorias, gobierno, tanto como en diversos estados. Los recursos envueltos, tanto como los datos y mecanismos empleados en tales fraudes, se van estudiando para recapitular los comportamientos llevados a cabo por quien este acusado. El caso continúa y se siguen dilucidando detalles del mismo. Se discutirán los temas de relevancia, tales como el esquema de fraude al sistema de Medicare, sobornos, debilidades de procedimientos, incentivos ilegales y mecanismos legales que utilizan las compañías para protegerse, pero ser tergiversados para actos delictivos.

## Fraudes Involucrados

### Fraudes al Cuidado de Salud

El National Health Care Anti-Fraud Association (NHCAA por sus siglas en inglés, 2018) estima que los delitos por fraudes al cuidado de salud están en los miles y millones de dólares cada año. Se tenga un seguro patrocinado por el empleador o si se paga un seguro privado, los daños causados a corto o largo plazo son incalculables. Se le llama efecto dominó. Esto a su vez lleva a primas más altas y mayores gastos al consumidor, tanto como a reducción de coberturas y beneficios.

Cuando se trata del fraude al cuidado de salud, se puede encontrar personas que fueron víctimas de fraudes de manera individual, pacientes que tienen artefactos que pagaron o dieron su firma para tener, pero no les hacía falta. También podemos tener pacientes que han sido explotados al pasar por procedimientos médicos innecesarios y hasta inseguros. Aunque el fraude a la atención medica es llevada a cabo y/o cometida por un grupo pequeño de proveedores, las acciones de los mismos son vistas como actos que empañan la reputación de muchos otros lugares que no lo llevan a cabo. El miedo colectivo entonces se toma en cuenta como parte de las razones por la cual las personas no tienen seguro médico.

Los mecanismos empleados por los que cometen el fraude se les hace fácil ya que conocen las variables e información del paciente que utilizará como parte de su esquema. Por ello es que existe un patrón de los fraudes cometidos constantemente. Tenemos los fraudes por facturación de servicios que no fueron prestados. Esto ocurre mediante el uso de información que se tiene del paciente, sea brindada por el mismo o por medio de robo de identidad, para fabricar reclamos que son completos o con los blancos que hacen falta para

llenar formularios, sea de servicios como procedimientos. También se lleva a cabo facturación por servicios o procedimientos más caros de los que realmente se proporcionan o realizan. A esto se le llama “mejora”, o sea, facturar falsamente un procedimiento o tratamiento de mayor precio del que se proporcionó realmente (llamado también inflación) (NHCAA, 2018).

Los crecientes pagos, primas y servicios limitados son parte del impacto generado por el fraude del servicio de cuidado. Según NHCAA (2018), $2.27 trillones de dólares fueron gastados en servicio de cuidado y más de cuatro mil millones en reclamos de seguro. Se presenta una lista de quienes son los que sufren, victimas del fraude. Los métodos perpetrados para cometer tales actos ilícitos se resumen de la siguiente manera:

- Cobro por servicios no prestados.
- Cobrar más caro de lo establecido.
- Falsa representación de servicios provistos.
- Falsificación de diagnóstico del paciente.
- Fraude de sobornos.

Otro caso relacionado envuelve a 600 personas, de los cuales 165 eran profesionales de la medicina, fueron encontrados culpables por someter reclamos de prescripciones innecesarias, a su vez, no siendo entregadas a los pacientes ni compradas (LaPointe, 2018, junio). A su vez, según LaPointe (2018), en el 2017, las agencias federales anunciaron que, por promedio, estos fraudes traen pérdidas de hasta $1.3 mil millones en pérdidas.

Fraude por Cable o Correo

Se trata de esquemas de fraude a víctimas que tienen el derecho de recibir servicios honestos. Los estatutos del fraude por cable o correo son esencialmente los mismos, excepto por el medio físico de transporte y comunicación. Como consecuencia, las interpretaciones de uno son consideradas a ser aplicadas al otro. Para las cortes declarar que una comunicación constituye un esquema para defraudar al gobierno, se tiene que demostrar que el acusado, a conciencia, utiliza la comunicación de manera calculada para engañar a las personas. Si no, se ataca las intenciones y mecanismos del acusado para engañar (Department of Justice, 2019).

El Congreso (Doyle, 2019, febrero) establece que “el defraudar” y la frase “para obtener dinero, bienes y/o propiedades” no representan crímenes por separado, sin embargo, la frase “obtener dinero o propiedad” describe lo que constituye un esquema para defraudar. El fraude por cable o correo claramente protege en contra de privación de propiedad tangible, incluyendo algunos no tangibles, como derechos de propiedad. Se establecen tales fraudes bajo materialidad, intento de, lo que son servicios honestos y bajo “ayudando e incitando, intento y conspiración”. Por eso, la conspiración a cometer fraude de cable bajo 18 U.S.C. § 1349 requiere a un jurado que encuentre que dos personas o más quedaron de acuerdo con cometer tales fraudes y que el culpable a conciencia haya querido ser parte del intento para llevar a cabo tal esquema (Doyle, 2019, febrero).

El fraude por el uso indebido del servicio de correo y de envió por cable, aunque acarrean muchos temas en sí, se utilizan en casos de manera intercambiable. Según Doyle (2019, febrero) lo que cambia es el medio de transporte utilizado y la tecnología envuelta.

Estos actos datan del siglo XIX con los famosos capitalinos. Las sentencias cambian según las definiciones establecidas por el congreso y la corte suprema.

Existen lecturas que exponen a los lectores a concientizar sobre diferentes tipos de fraudes y el cómo evitarlos. Wolters Kluwer (2019) alerta sobre incidencias ocurriendo al recibo de facturas falsas, subastas en línea que son falsas y hasta del robo de cartas que contienen cheques.

Fraude al Cuidado de Salud y Declaraciones Falsas

El gasto en salud en los Estados Unidos continúa disparándose. Aunque muchos dependen de planes de seguro de salud con fondos privados, millones de estadounidenses están asegurados, en todo o en parte, por un seguro de salud pagado con fondos del gobierno federal o estatal. Los planes de salud patrocinados por el gobierno son los programas de Medicare y Medicaid. Estos dos programas brindan cobertura de atención médica de hasta 95 millones de estadounidenses, a un costo estimado de más de $ 900 mil millones (Pietragallo, 2019).

Debido al gran volumen de reclamos de atención médica presentados en nombre de los millones de estadounidenses asegurados en virtud de estos programas, el gobierno por sí solo no puede combatir eficazmente el fraude en la atención médica. Los denunciantes de irregularidades federales y estatales han demostrado ser la mejor arma del gobierno para detectar y perseguir el fraude en la atención médica. Los denunciantes suelen estar en la mejor posición para detectar conductas fraudulentas y sacarla a la luz presentando una demanda por qui tam en nombre del gobierno (Department of Justice, 2019).

Existen diversas maneras para defraudar, cobrar servicios no brindados, pacientes fantasmas, los sobornos, cambiar de código ciertos servicios, quedarse con reembolsos, certificaciones falsas, baja o ninguna necesidad médica, quedarse con los *grant* brindados para investigaciones médicas, reportar costos inflados, entre otros.

La responsabilidad bajo la Ley Federal de Reclamos Falsos ocurre cuando un acusado (1) presenta a sabiendas (o hace que se presente) un reclamo de pago falso o fraudulento; (2) a sabiendas hace, usa o hace que se haga o use un registro falso o material de declaración para un reclamo falso o fraudulento; (3) conspira con otros para cometer una violación de la Ley de Reclamaciones Falsas (4) a sabiendas hace, usa o hace que se haga o use un registro o declaración falsa para ocultar, evitar o disminuir la obligación de pagar dinero o transmitir propiedad del gobierno federal (Auerbach & White, 2019).

Artículos relacionados al tema:

El acta de Reclamos Falsos ocurre cuando un acusado presenta, a sabiendas, un reclamo falso o fraudulento, de pago, cobro, un registro falso o material de declaración para un reclamo falso o fraudulento (Auerbach & White, 2019). Existe lo que es la Ley Severa, 42 U.S.C. § 1395nn, también llamada *Physician Self-Referral Law.* La misma establece que si un médico tiene algún tipo de relación financiera, directa o indirecta con la entidad que proporciona servicios designados, el medico no puede derivar pacientes a tal entidad (Auerbach & White, 2019).

## Leyes Aplicables

### Conspiración 18 U.S. § 287

Consiste en llevar a cabo cualquier reclamo, a sabiendas, que sea falso, ficticio y/o fraudulento (Cornell, 2019).

El fraude, el despilfarro y el abuso comprenden, entre otras cosas, malversación de fondos, uso o apropiación indebidos de fondos o propiedad y declaraciones falsas, ya sea por parte de organizaciones o de individuos. Entre los ejemplos están robo de fondos para uso personal; utilizar los fondos para fines no relacionados con la subvención; robo de propiedad federal o de propiedad adquirida o arrendada a través de una subvención; cobrar alquileres del edificio inflados en un edificio propiedad del beneficiario; presentar informes financieros falsos; y presentar datos financieros falsos en las licitaciones presentadas al beneficiario (para un posible pago de conformidad con la subvención)

Los despilfarros, fraudes y abusos comprenden en apropiaciones indebidas de propiedad, fondos, para uso personal. Inflar cobros, tanto como los informes falsos son parte de los fraudes (Hhs.gov, 2019).

### Fraudes y Estafas 18 U.S. § 1341

Toda intención en llevar a cabo esquemas fraudulentos a sabiendas para asi obtener dinero y/o beneficio. El uso a su vez de transportes mediante el correo también puede ser multado y ser parte del fraude. (Cornell.com, 2019).

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

Cualquier acto engañoso a través de medios visuales, radio y televisión.

Quien haya ideado o tenga la intención de idear cualquier esquema o artificio para defraudar, o para obtener dinero o propiedad por medio de pretensiones, representaciones o promesas falsas o fraudulentas, transmite o hace que se transmita por medio de comunicación por cable, radio o televisión. en el comercio interestatal o extranjero, cualquier escritura, letrero, señal, imagen o sonido con el propósito de ejecutar dicho esquema o artificio, será multado bajo este título o encarcelado no más de 20 años, o ambos. Si la violación ocurre en relación con, o involucra algún beneficio autorizado, transportado, transmitido, transferido, desembolsado o pagado en relación con un desastre o emergencia mayor declarado por el presidente (como esos términos se definen en la sección 102 de Robert T. Stafford La Ley de Asistencia de Emergencia y Socorro en Desastres (42 USC 5122), o afecta a una institución financiera, dicha persona será multada con no más de $ 1,000,000 o encarcelada no más de 30 años, o ambas (Cornell.com, 2019).

Fraude en la atención médica 18 U.S. § 1347

Se refiere a quien intenta o ejecuta cualquier acto delictivo o fraudulento a programas de atención médica.

(a) Quien a sabiendas y deliberadamente ejecuta, o intenta ejecutar, un esquema o artificio:

(1) defraudar a cualquier programa de beneficios de atención médica; o

(2) para obtener, por medio de pretensiones falsas o fraudulentas, representaciones o promesas, cualquier parte del dinero o propiedad de, o bajo la custodia o control de, cualquier programa de beneficios de atención médica,

en relación con la entrega o el pago de beneficios, artículos o servicios de atención médica, serán multados bajo este título o encarcelados por no más de 10 años, o ambos. Si la

violación resulta en lesiones corporales graves (como se define en la sección 1365 de este título), dicha persona será multada bajo este título o encarcelada por no más de 20 años, o ambos; y si la violación resulta en la muerte, dicha persona será multada bajo este título, o encarcelada por cualquier término de años o de por vida, o ambos.

(b) Con respecto a las violaciones de esta sección, una persona no necesita tener un conocimiento real de esta sección o una intención específica de cometer una violación de esta sección (Cornell.com, 2019).

Fraude por Correo 18 U.S. § 1341

Abusos de Comunicaciones o fraude en las telecomunicaciones o cualquier mal uso del sistema postal.

Abusos de Comunicaciones, existes dos normas fundamentales que se ocupan de su regulación, de gran utilidad, a priori, frente al delito informático: la referida al fraude postal (The mail fraud statute, sección 1341 del federal code) y la que se ocupa del fraude por telecomunicaciones (wire fraud statute,sección 1343). El mail fraud statute se aplica a cualquier uso del sistema postal para perpetrar un proyecto fraudulento. La norma contiene los dos elementos esenciales del delito:

La utilización de sistema postal con la intención de ejecutar
Un fraude o ardid para obtener dinero o propiedad por medio de una falsa representación.

Según la interpretación que la justicia federal ha hecho de este precepto, no existiría, en principio, inconveniente para su aplicación a un delito informático fraudulento (M.G. 1991).

Fraude al Cuidado de Salud 18 U.S. § 1347

Fraude a proveedores médicos o programas de beneficios de atención médica.

El gobierno federal tiene muchas herramientas diferentes para procesar a los proveedores de atención médica sospechosos de defraudar a Medicare, Medicaid, Tricare y otros programas de beneficios de atención médica. Desde la Ley Stark hasta la Ley de Reclamaciones Falsas, las leyes que son específicas y no específicas para el cuidado de la salud imponen sanciones por todo, desde la aplicación incorrecta de las pautas de facturación de Medicare, hasta ofrecer sobornos y hacer las llamadas "autorreferencias" de los médicos.

Pero una de las herramientas más poderosas del gobierno en las investigaciones de fraude en la atención médica es 18 U.S.C. Sección 1347, el estatuto federal de fraude a la atención médica. Las prohibiciones de este estatuto son extraordinariamente amplias y sus sanciones son extremadamente severas. Afirma:

(a) Quien a sabiendas y deliberadamente ejecuta, o intenta ejecutar, un esquema o artificio:

(1) defraudar a cualquier programa de beneficios de atención médica; o

(2) obtener, por medio de pretensiones, representaciones o promesas falsas o fraudulentas, cualquier parte del dinero o propiedad que posea, o esté bajo la custodia o control de cualquier programa de beneficios de atención médica, en relación con la entrega o el pago por beneficios, artículos o servicios de atención médica, serán multados bajo este título o encarcelados no más de 10 años, o ambos. Si la violación resulta en lesiones corporales graves (como se define en la sección 1365 de este título), dicha persona será multada bajo este título o encarcelada por no más de 20 años, o ambos; y si la violación resulta en la

muerte, dicha persona será multada bajo este título, o encarcelada por cualquier término de años o de por vida, o ambos.

(b) Con respecto a las violaciones de esta sección, una persona no necesita tener un conocimiento real de esta sección o una intención específica de cometer una violación de esta sección (Federal-Lawer.com, 2019).

Declaraciones Falsas Título 18 U.S. § 1001

Declaraciones o entradas en general- ocultar información o cualquier declaración falsa.

(a) Salvo que se disponga lo contrario en esta sección, quien, en cualquier asunto dentro de la jurisdicción de la rama ejecutiva, legislativa o judicial del Gobierno de los Estados Unidos, a sabiendas y deliberadamente:

(1) falsifica, oculta u oculta mediante cualquier truco, esquema o dispositivo un hecho material;

(2) hace cualquier declaración o representación materialmente falsa, ficticia o fraudulenta; o

(3) hace o usa cualquier escritura o documento falso sabiendo que contiene cualquier declaración o entrada materialmente falsa, ficticia o fraudulenta;

serán multados bajo este título, encarcelados no más de 5 años o, si el delito involucra terrorismo internacional o doméstico (como se define en la sección 2331), encarcelados no más de 8 años, o ambos. Si el asunto se relaciona con un delito bajo el capítulo 109A, 109B, 110 o 117, o la sección 1591, entonces el período de prisión impuesto bajo esta sección no será mayor de 8 años.

(b) La subsección (a) no se aplica a una parte en un procedimiento judicial, o al abogado de esa parte, para declaraciones, representaciones, escritos o documentos presentados por dicha parte o abogado a un juez o magistrado en ese procedimiento.

(c) Con respecto a cualquier asunto dentro de la jurisdicción del poder legislativo, el inciso (a) se aplicará solo a:

(1) asuntos administrativos, incluyendo un reclamo de pago, un asunto relacionado con la adquisición de propiedades o servicios, personal o prácticas de empleo, o servicios de apoyo, o un documento requerido por ley, norma o reglamento para ser presentado al Congreso o cualquier oficina u oficial dentro del poder legislativo; o

(2) cualquier investigación o revisión, realizada de conformidad con la autoridad de cualquier comité, subcomité, comisión u oficina del Congreso, de conformidad con las normas aplicables de la Cámara o el Senado (Cornel.com, 2019).

Lavado de Dinero

Lavado de Instrumentos Monetarios Título 18 U.S. § 1956

El método más común de sancionar la utilización delictiva de fondos mal habidos consiste en la aplicación de leyes sobre lavado de dinero, tales como 18 U.S.C. §§1956 y 1957. La sección 1956(a) define tres tipos de actos delictivos: 1) transacciones de lavado de dinero en la esfera interna (§1956(a)(1)); 2) transacciones de lavado de dinero en el ámbito internacional (§1956(a)(2)), y 3) transacciones de lavado de dinero encubiertas "por incitación" (§1956(a)(3)). Este resumen se refiere al lavado de dinero en la esfera interna dentro de los Estados Unidos.

Para incurrir en culpabilidad penal conforme a 18 U.S.C. § 1956(a)(1), el acusado debe haber realizado o intentado realizar una transacción financiera a sabiendas de que los bienes a los que ella se refiere representan el producto de alguna actividad ilícita, con una de las cuatro intenciones específicas que más abajo se mencionan, y los bienes en efecto deben provenir de una actividad ilícita especificada. Además, el acusado debe saber que los bienes de que se trata eran el producto de cualquier delito grave previsto por leyes estatales, federales o extranjeras.

En §1956(c)(4) se define como "transacción financiera" una transacción que afecta al comercio interestatal o exterior y: (1) supone la movilización de fondos por vías cablegráficas y otras vías; (2) comprende la utilización de un instrumento monetario; o (3) supone la transferencia o el título de bienes raíces, vehículos terrestres, navíos o una aeronave; o (4) supone la utilización de una institución financiera que se ocupa de actos de comercio interestatal o exterior, o cuyas actividades afectan a esas modalidades de comercio.

Al realizar la transacción financiera el acusado debe haber actuado con alguna de las cuatro intenciones específicas siguientes:

- Sección 1956(a)(1)(A)(i): Intención de promover la realización de una actividad ilícita especificada;

- Sección 1956(a)(1)(A)(ii): Intención de realizar actos de evasión o fraude tributarios;

- Sección 1956(a)(1)(B)(i): Conocimiento de que la transacción estaba destinada a ocultar o desfigurar la naturaleza, ubicación, fuente, propiedad o control del producto de la actividad ilícita especificada; o

- Sección 1956(a)(1)(B)(ii): Conocimiento de que la transacción estaba destinada a eludir la obligación de declarar una transacción conforme a la legislación estatal o federal [por ejemplo en violación de 31 U.S.C. §§ 5313 (Declaración de Transacciones en Moneda) o 5316 (Declaración sobre Instrumentos de Moneda y Monetarios), o 26 U.S.C. § 6050I (Formulario 8300 del Servicio de Ingresos Internos)] (Oas.org, 2019).

La Entrega de Propiedades y Bienes

Decomiso civil (Civil Forfeiture). Título 18 U.S. § 981

(1) La siguiente propiedad está sujeta a confiscación a los Estados Unidos:

(A) Cualquier propiedad, real o personal, involucrada en una transacción o intento de transacción en violación de la sección 1956, 1957 o 1960 de este título, o cualquier propiedad rastreable a dicha propiedad.

(B) Cualquier propiedad, real o personal, dentro de la jurisdicción de los Estados Unidos, que constituya, se derive o pueda rastrearse a, cualquier producto obtenido directa o indirectamente de un delito contra una nación extranjera, o cualquier propiedad utilizada para facilitar dicho delito.

Si el delito:

(i) implica el tráfico de tecnología o material de armas nucleares, químicas, biológicas o radiológicas, o la fabricación, importación, venta o distribución de una sustancia controlada

(como se define ese término para los fines de la Ley de Sustancias Controladas), o cualquier otra conducta descrita en la sección 1956 (c) (7) (B);

(ii) sería punible dentro de la jurisdicción de la nación extranjera con la muerte o prisión por un período superior a 1 año; y (iii) sería punible según las leyes de los Estados Unidos con una pena de prisión de más de 1 año, si el acto o actividad que constituye el delito hubiera ocurrido dentro de la jurisdicción de los Estados Unidos.

(C) Cualquier propiedad, real o personal, que constituya o se derive de los ingresos atribuibles a una violación de la sección 215, 471, 472, 473, 474, 476, 477, 478, 479, 480, 481, 485, 486, 487 , 488, 501, 502, 510, 542, 545, 656, 657, 670, 842, 844, 1005, 1006, 1007, 1014, 1028, 1029, 1030, 1032 o 1344 de este título o cualquier delito que constituya "especificado actividad ilegal ”(como se define en la sección 1956 (c) (7) de este título), o una conspiración para cometer dicho delito (Cornell.com, 2019).

Decomiso penal (Criminal Forfeiture) Título 18 U.S. § 982

(7) El tribunal, al imponer una sentencia a una persona condenada por un delito federal de atención médica, ordenará a la persona que pierda bienes, reales o personales, que constituyan o se deriven, directa o indirectamente, de ingresos brutos atribuibles a la comisión de la ofensa (Cornell.com, 2019).

Modo de recuperación (Mode of recovery) Título 28 U.S. § 2461

Si una persona es acusada en un caso penal el congreso está autorizado a confiscar propiedades como parte de la sentencia.

a) Siempre que se prescriba una multa civil, pena o confiscación pecuniaria por la violación de una Ley del Congreso sin especificar el modo de recuperación o ejecución de la misma, puede recuperarse en una acción civil.

(b) A menos que la Ley del Congreso disponga lo contrario, siempre que se prescriba una confiscación de bienes como sanción por violación de una Ley del Congreso y la incautación tenga lugar en alta mar o en aguas navegables dentro del almirantazgo y la jurisdicción marítima de los Estados Unidos. Los estados, tal decomiso puede ser ejecutado por difamación en almirantazgo, pero en casos de incautaciones en tierra, la confiscación puede imponerse mediante un procedimiento por difamación que se ajustará lo más posible a los procedimientos en almirantazgo.

(c) Si una persona es acusada en un caso penal de una violación de una Ley del Congreso para la cual está autorizada la confiscación de bienes civiles o penales, el Gobierno puede incluir un aviso de la confiscación en la acusación o información de conformidad con las Reglas Federales de procedimiento penal. Si el acusado es condenado por el delito que dio lugar a la confiscación, el tribunal ordenará la confiscación de la propiedad como parte de la sentencia en el caso penal de conformidad con [1] las Reglas Federales de Procedimiento Penal y la sección 3554 del título 18, Código de los Estados Unidos. Los procedimientos en la sección 413 de la Ley de Sustancias Controladas (21 USC 853) se aplican a todas las etapas de un procedimiento de decomiso penal, excepto que la subsección (d) de dicha sección se aplica solo en los casos en que el acusado sea condenado por una violación de dicha Ley (Cornell.com, 2019).

Procedencias de Cash/Confiscación Título 18 U.S. § 371

Conspiración para cometer un delito o defraudar a Estados.

Si personas conspiran para cometer un delito en estados unidos con cualquier propósito cada uno será multado o encarcelado 5 años o menos.

Si dos o más personas conspiran para cometer un delito contra los Estados Unidos, o para defraudar a los Estados Unidos, o cualquier agencia de los mismos de cualquier manera o para cualquier propósito, y una o más de esas personas realizan cualquier acto para hacer el objeto de la conspiración, cada uno será multado bajo este título o encarcelado no más de cinco años, o ambos.

Sin embargo, si el delito, cuya comisión es el objeto de la conspiración, es solo un delito menor, el castigo por tal conspiración no excederá el castigo máximo previsto para dicho delito menor (Cornell.com, 2019).

Casos Relacionados

Fraude a los Cuidados Médicos

EX CFO y 3 cirujanos fueron acusados en esquemas de contragolpe, en los roles que resultaron en la sumisión de más de $950 millones de dólares en reclamos fraudulentos, en su mayoría al sistema de compensación de trabajadores de California Ellison, 2018, Julio).

Operador de Hospicio paga $8.5 Millones de dólares para resolver una demanda del False Claims Act. Caris Healthcare retuvo a conciencia sobrepagos de pacientes que no eran elegibles para el Medicare hospice benefit (BeckersHospitalReview.com, 2019).

# 3. SIMULACIÓN

En este caso particular, el fraude y los medios ilícitos utilizados por Andrew Chmiel, serán expuestos, partiendo de las investigaciones llevadas a cabo hasta el momento, ya que el caso sigue en pie y no ha culminado. Andrew Chmiel trabaja con equipo médico y cobra según el monto de pacientes que tenga, equipos que se le compren y de los pagos que provengan de Medicare. Él logra amasar buen capital y crea múltiples compañías, muchas de ellas LLC, que trabajen con equipos DME o Durable Medical Equipment. Una LLC es una compañía de responsabilidad limitada, lo cual funge como estructura de negocio permitido y conforme a estatutos del estado (IRS, 2019) Al querer expandir sus servicios y cobros, acude a otras empresas DME.

Para atraer con buenas ofertas a esas otras empresas, le ofrece *sobornos,* sin competir en subastas e incentivar cada compra de equipo. Se buscan pacientes para adjudicarle la aparente necesidad y compra de equipo médico. Acuden a los pacientes que serán los que den su firma, luego para la adquisición de los equipos. Andrew Chmiel acude al pago de compañías de telecomunicaciones y radio para anuncios y empresas de telemercadeo para llamar a los pacientes de los cuales ya tienen su información, desde sus números de teléfono hasta las complicaciones de salud que tienen, Andrew Chmiel lleva a cabo un acercamiento con sus ofertas a diversos doctores. Algunos acceden y otros no. Los que acceden, también tendrán pagos de soborno como incentivo de la entrega de información privada de sus pacientes.

A su vez, los doctores hacían promoción de los servicios de tales equipos y servicios médicos remotos. Entre los doctores y Andrew Chmiel, tenían documentos con listados de posibles pacientes interesados o meras victimas que simplemente se dejan

llevar, para las firmas y luego los procedimientos a llevar a cabo con Medicare. Esto abre también otra brecha para los doctores y para Andrew Chmiel ya que también están cobrando por servicios que no se han dado. Los pedidos de equipo se envían desde el doctor del paciente hasta las empresas DME, incluyendo las empresas DME del cual Andrew Chmiel el dueño. Luego llenan los documentos para Medicare y llevan a cabo los pedidos. Según como mejore el tráfico de pacientes, van entrando al panorama más empresas DME, más doctores, más lugares pagados de telecomunicaciones y radio.

Las ganancias cada vez más son abrumadoras. Andrew Chmiel desea mantener tales ingresos bajo el radar. Acude a cuentas de banco en otros países, tanto como empresas *shell*. Al no existir record de su nombre como dueño y de sus empresas como parte de los esquemas de las cuentas *Shell*, asimismo evita las sospechas. Para bajar los costos de equipo médico, Andrew Chmiel acude a la compra de equipo médico de baja calidad, que proviene de China. Todo el esquema sigue fluyendo hasta que la queja de uno de los doctores se lleva al FBI.

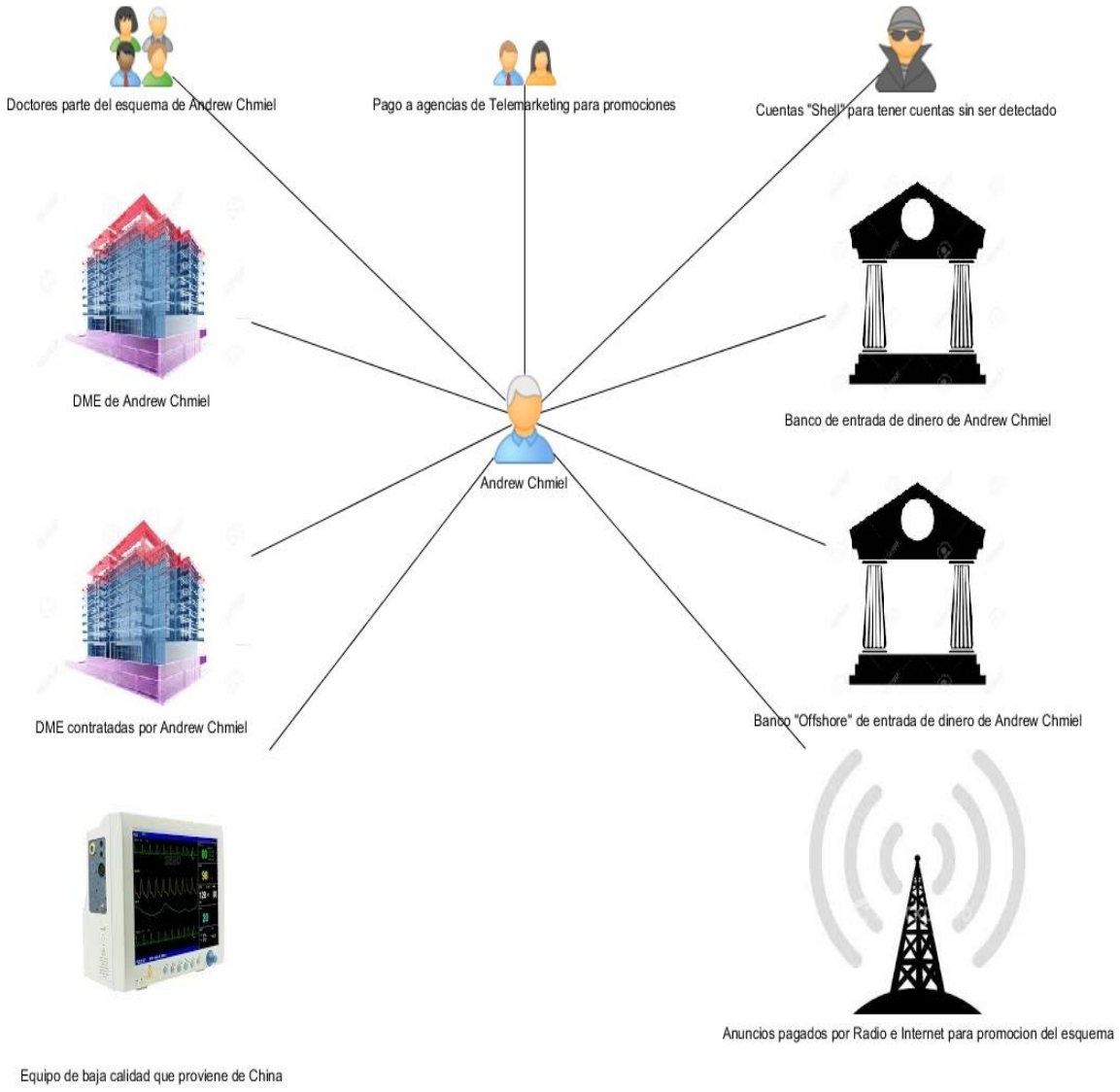



Figura 1. Simulación recreacional del caso sobre el fraude de Andrew Chmiel.

# 4. INFORME DEL CASO

## Resumen Ejecutivo

Este caso trata de Andrew Chmiel y los cargos de fraude que le acarrean. Los datos que se recuperen de sus distintos dispositivos electrónicos tendrán gran peso a la hora de continuar el caso. El mismo todavía no ha terminado. Hasta ahora las investigaciones apuntan a Andrew Chmiel tener cuentas de bancos, propiedades y negocios que son sustentadas con dinero obtenido de manera ilícita. Significa que se requieren de datos que ayuden a demostrar que todo fue a conciencia y de modo continuo. Todas las herramientas que Andrew Chmiel ha utilizado fueron con datos electrónicos. Gracias a los programas de hoy día se puede llevar a cabo una recopilación de todo lo que Andrew Chmiel pudo crear y continuar desde que comenzó con el fraude.

Las herramientas que se utilizan para extraer los datos son compatibles con lo que Andrew Chmiel creó. Son datos con extensiones genéricas, sea documentos de Word, Excel, fotos, videos y hasta pdf. Al todo ser creado con herramientas conocidas, la investigación será más llevadera. La corte requería de un investigador forense que tuviese su propio laboratorio, lo cual, a su vez, tomase en cuenta la cadena de custodia de los aparatos electrónicos que así lo albergan. Se escoge a la empresa Hammu Designs para la tarea. Inmediatamente los dispositivos llegan al laboratorio, el trabajo de investigación comienza. La extracción de datos no es llevada a cabo de inmediato ya que se llevaron a cabo copias a discos duros y pendrives externos para no manipular datos del disco original, ya que eso puede invalidar toda la investigación por completo y alertar a su abogado para que los hallazgos sean obviados.

Al lograr cargar el sistema operativo de Andrew Chmiel en plataformas Virtuales, en Live CD y con las aplicaciones que duplican su sistema, se logran encontrar la información requerida para la corte. Todo lo que se encuentre debe ser copiado a un pendrive o disco duro externo al cual se le configura que lo que sea escrito una vez ya no se le pueda rescribir. Esto aumenta el nivel de confianza de los datos. Todo lo que se ha logrado fue gracias a los programas de forense. En el caso del celular de Andrew Chmiel se logra configurar la computadora forense de tal manera que sea compatible con los datos a recibir del mismo. Lo encontrado en el celular tiene que pasar por el mismo método de otros discos duros. Esto significa que debe ser colocado en un dispositivo con las seguridades de no ser rescrito.

Luego de encontrar toda fuente requerida, se le entrega a la fiscal para que su transporte sea seguro y la cadena de custodia de datos y dispositivos sea lo más corto posible. Todo fue encontrado para que el caso continúe.

## Objetivo

En este caso particular se buscan datos que sean relevantes al caso escogido. Los mismos deben ser en formatos lo cual regularmente se utilicen en conversaciones, sea mediante envíos de correos, documentos, minutas, reuniones y hasta contratos. A su vez se espera encontrar videos, formatos de imágenes y todo lo que logre atar a Andrew Chmiel con las imputaciones con las cuales se le señala.

## Alcance del Trabajo

Las herramientas utilizadas para la investigación del caso son las siguientes:

- Nirsoft LastActivityView.

- OSForensics.
- HBCD PE x64 (Hirens Boot CD)
- Nirsoft Utilities (NirLauncher)
- Dispositivos externos (Discos Duros, CD/DVD, Pendrives)
- Backuptrans Android SMS Backup and Restore
- Backuptrans Android Whatsapp Transfer
- Lazesoft Recover My Password

Procedimientos llevados a cabo como parte de la investigación:

- Copia del disco duro original.
- Extracción de datos específicos a USB y protegerlos para no ser re-escritos.
- Utilizar herramientas que cargan un sistema operativo al RAM para verificar otras áreas del sistema operativo de Andrew Chmiel.
- Utilizar herramientas para ingresar a su usuario local (laptop).
- Extraer anotaciones del sistema operativo que indiquen el comportamiento de los últimos actos llevados a cabo en la computadora.
- Investigar datos de su celular.
- Verificación del sistema operativo de la computadora de Andrew Chmiel.
- Anotar lugares de conexión remota.

Personas Entrevistadas:

- Andrew Chmiel
- Doctores
- Bart Daniel, abogado de Andrew Chmiel

- Victimas aleatorias

Datos del Caso

- Número del caso – 3:19-299
- Investigadores – Garry Cantrell, Robert Johnson, Don Fort
- Solicitantes de la investigación – Sherri A. Lydon, United States Attorney
- Representantes de los solicitantes – Sherri A. Lydon

Descripción de los dispositivos utilizados

- Nirsoft LastActivityView – LastActivityView v1.35, Copyright © 2012-2019 Nir Sofer.
- Lazesoft (2019).
- OSForensics – OSForensics versión 7.0.10016 (64-bit) 2018-2019.
- HBCD PE x64 (Hirens Boot CD). V 1.0.1. Copyright 2010-2019.
- Nirsoft Utilities – Version 1.23.6, Last Updated 2019-November-25. (Nir Sofer, 2019).
- Backuptrans Android SMS Backup and Restore (2019) Version 2.14.37.
- Backuptrans Android Whatsapp Transfer (2019) Version 3.2.130.
- Disco duro externo – Toshiba MK6475GSX S/N 12VBSJA7S 640GB.
- Disco duro externo – Toshiba MQ01ABD100M S/N 86P7S55CS 1TB.
- Disco duro externo – Samsung ST640LM001 P/N HN-M640MBB/M.
- CD-R TDK52x 80min 700MB (Deft-2).
- CD-R TDK 52x 80min 700MB.

- Lexar USB Flash Drive USB Device [Hard drive] (16.01 GB) -- drive 1, s/n 901060F080A0 (HBCD_PE_64).
- Lexar USB Flash Drive USB Device [Hard drive] (16.00 GB) -- drive 2, s/n AA1J1M9CJ3GB7910 (CAINE).
- CENTON DS Pro USB Device [Hard drive] (32.46 GB) -- drive 2, s/n 11090119001111.
- Lexar USB Flash Drive USB Device [Hard drive] (64.02 GB) -- drive 1, s/n AA00000000000489.

Para la extracción de datos, tanto de la laptop como del celular, se llevó a cabo el uso de diversas herramientas, según compatibilidad, fácil manejo y la totalidad de datos que se requerían y fuesen a su vez de pruebas para la corte. A continuación, las herramientas, procedimientos y el producto final de los datos buscados/extraídos:

Resumen de Hallazgos

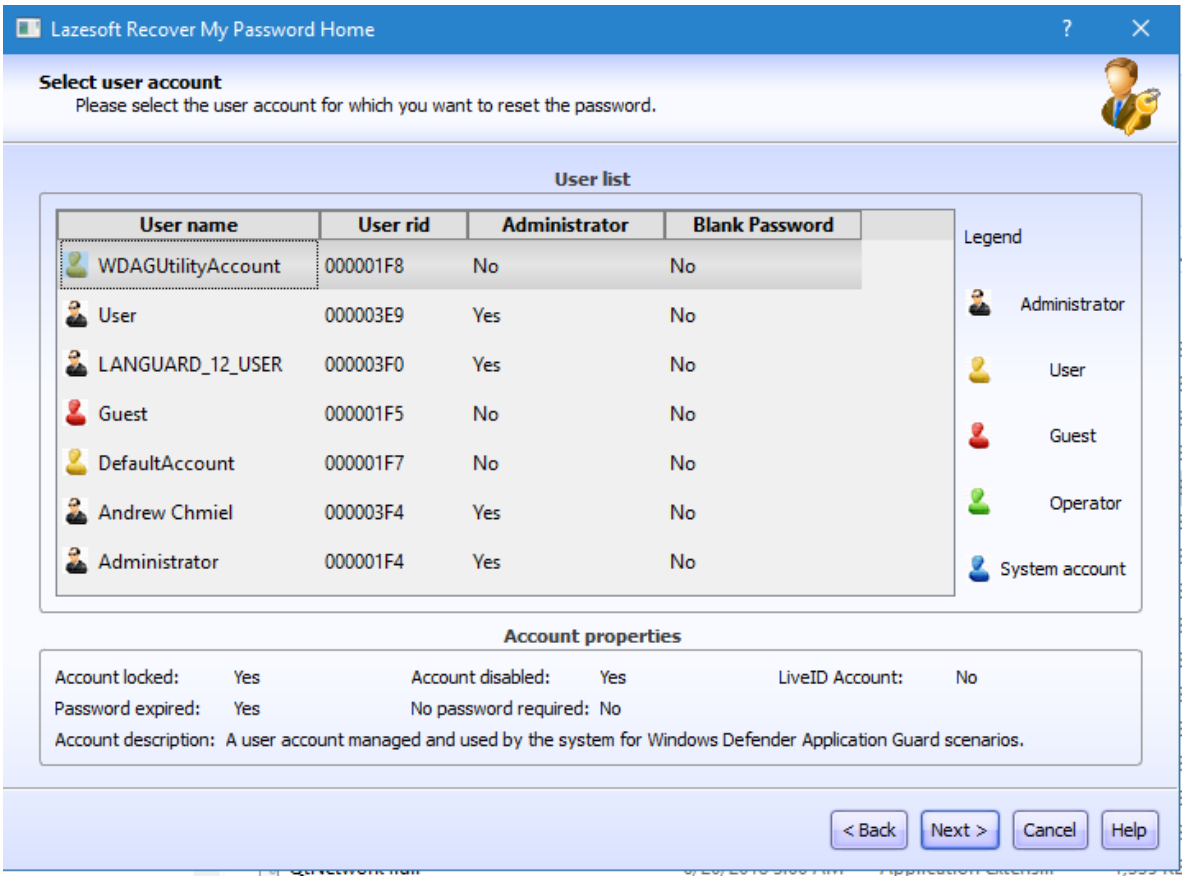



Figura 2. Herramienta para el cambio de clave de usuario.

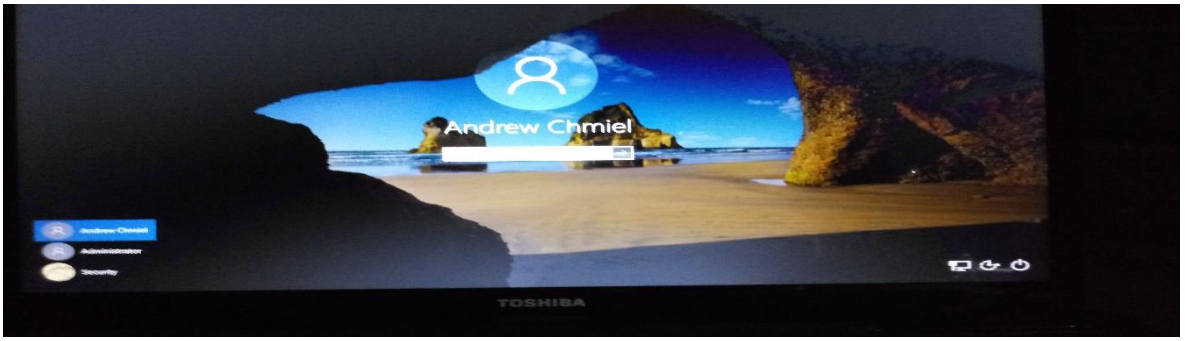



Figura 3. Ingreso al usuario de Andrew Chmiel.

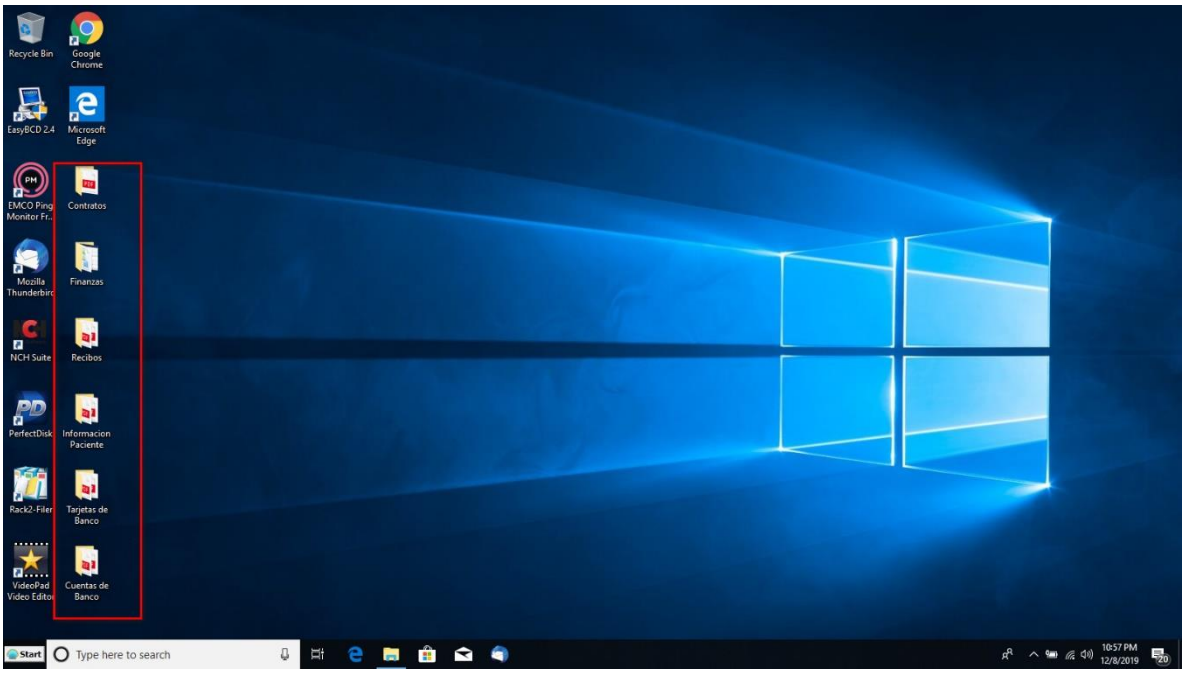



Figura 4. Desktop de Andrew Chmiel con datos.

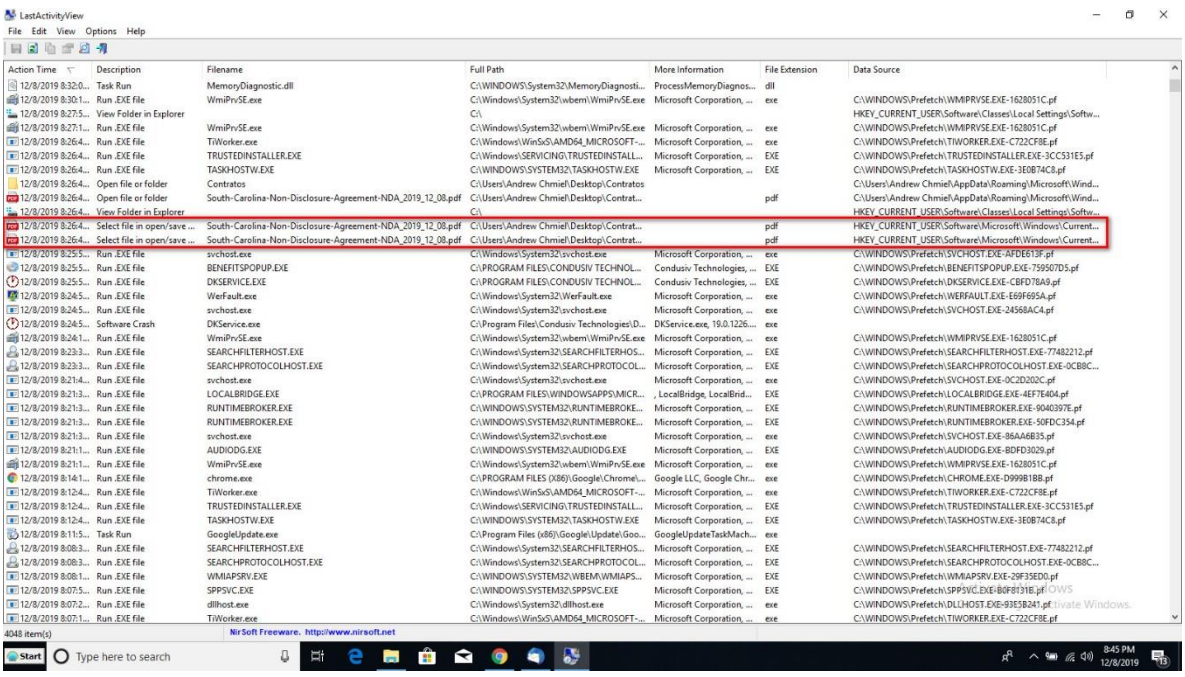



Figura 5. Last Activity View, hallazgo de lo último accesado que contiene la localización y datos importantes.

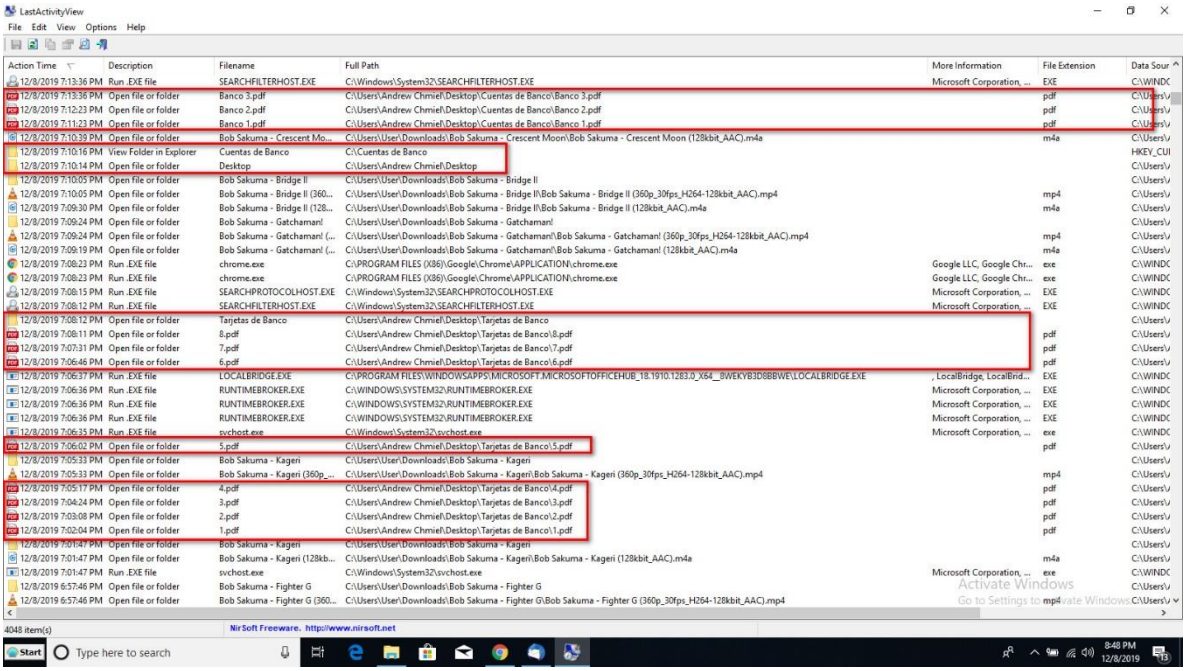



Figura 6. Last Activity View, hallazgos adicionales de carpetas y datos.

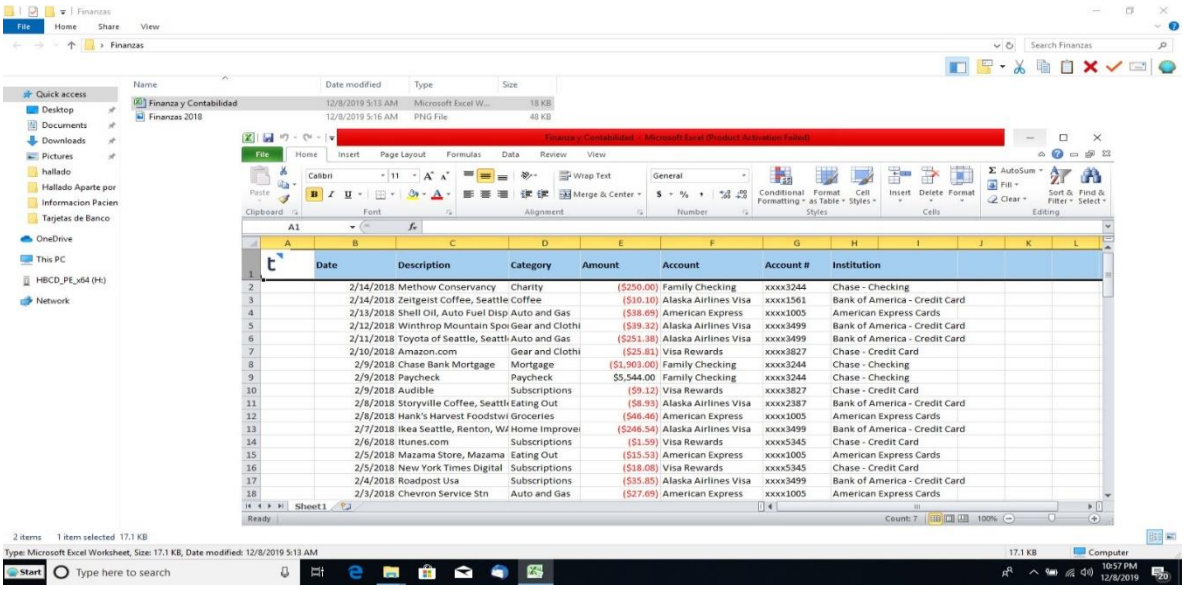



Figura 7. Hallazgo de carpetas con datos sobre finanzas.

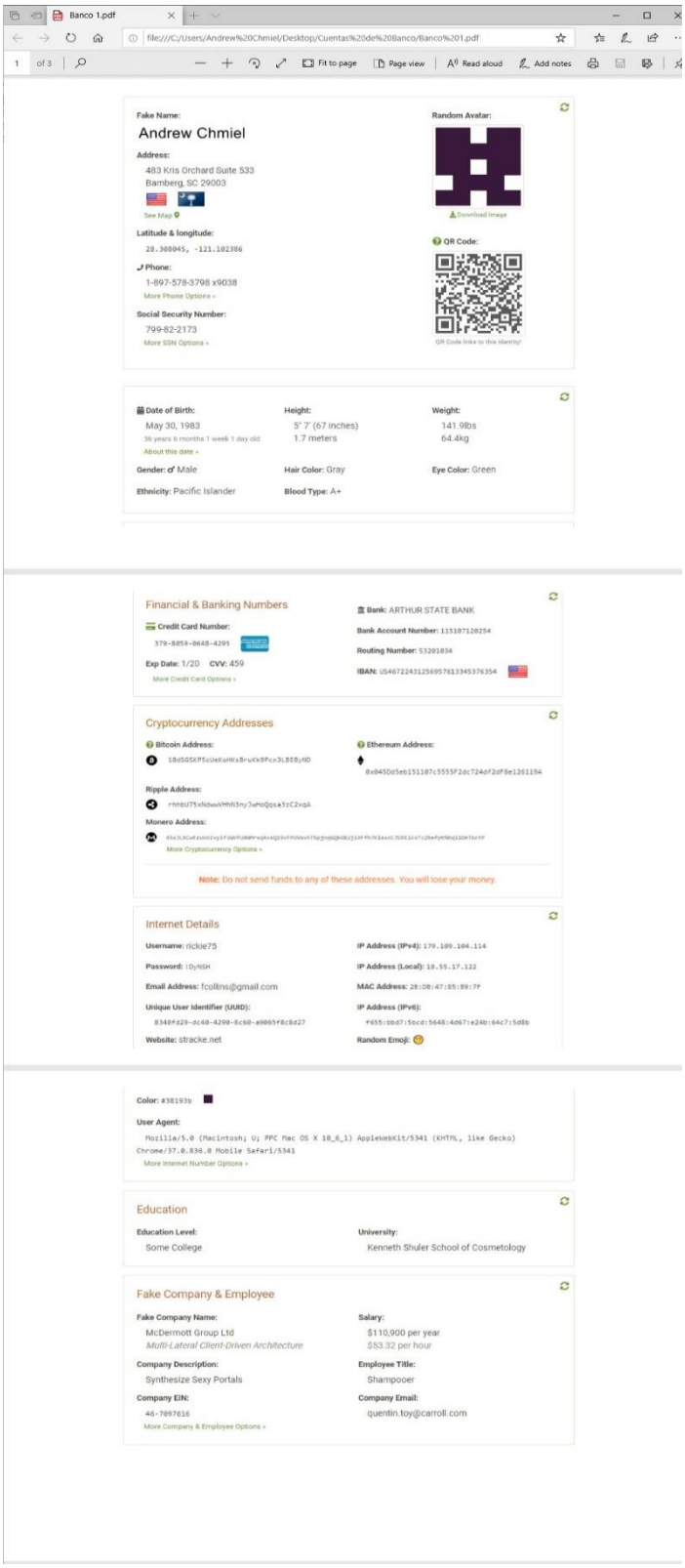



Figura 8. Hallazgo de carpetas con datos sobre cuentas de banco.

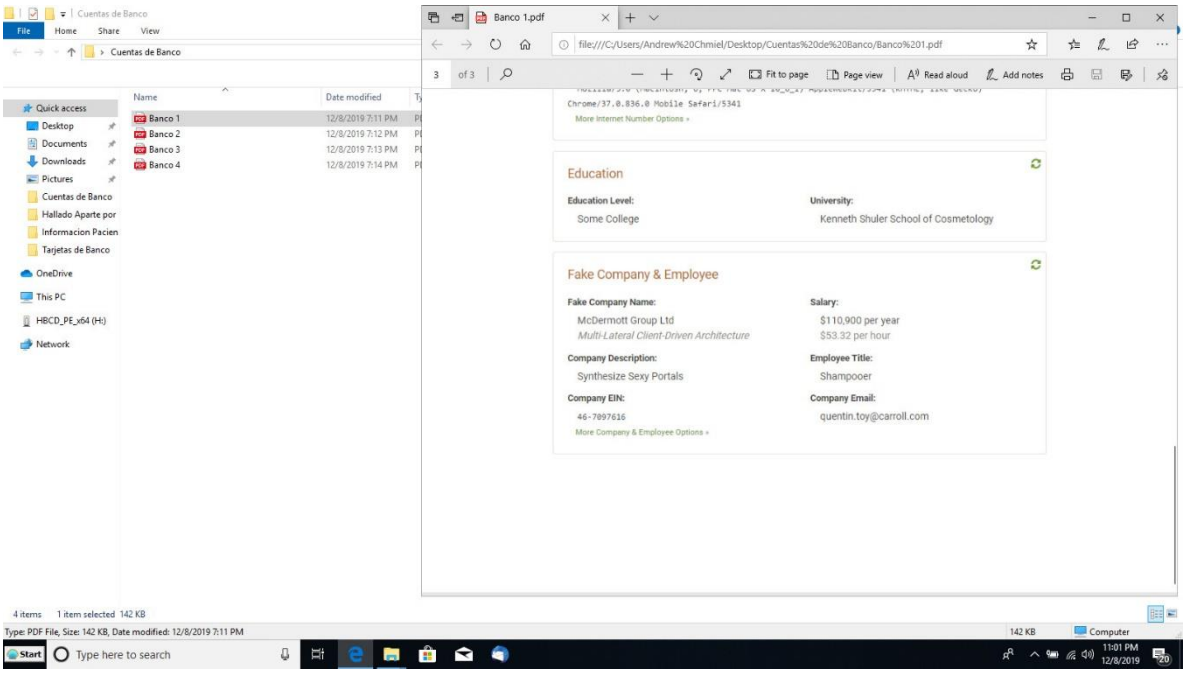



Figura 9. Carpeta con información adicional sobre cuentas de banco.

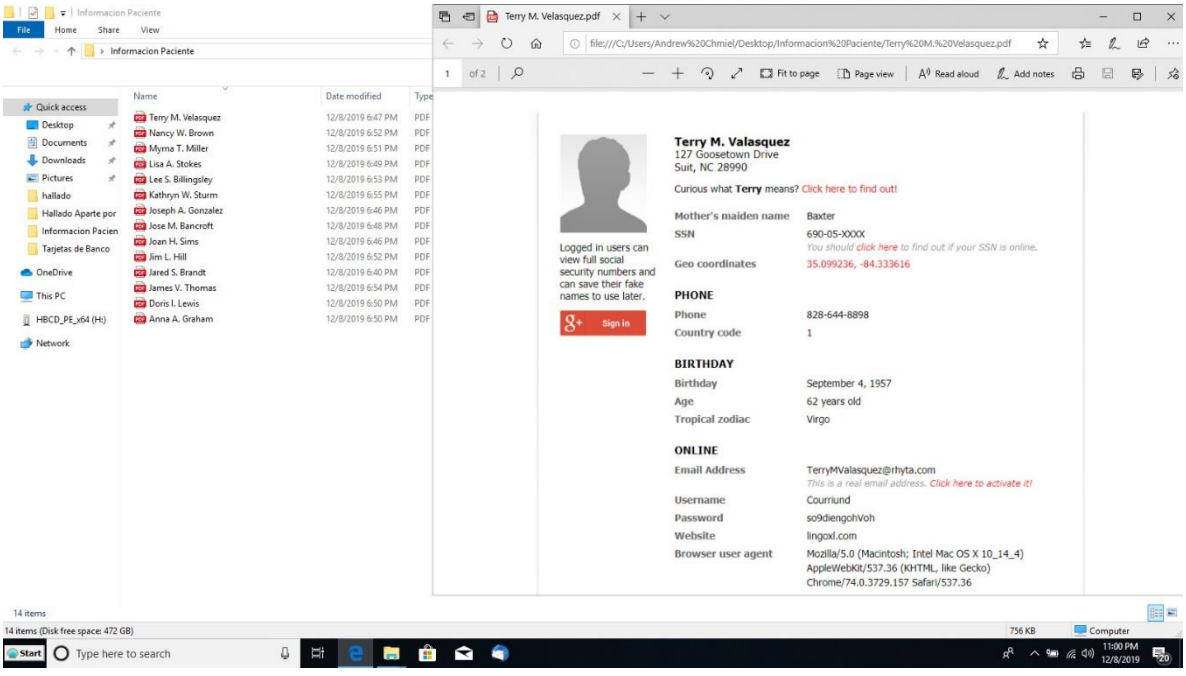



Figura 10. Carpeta con información de pacientes.

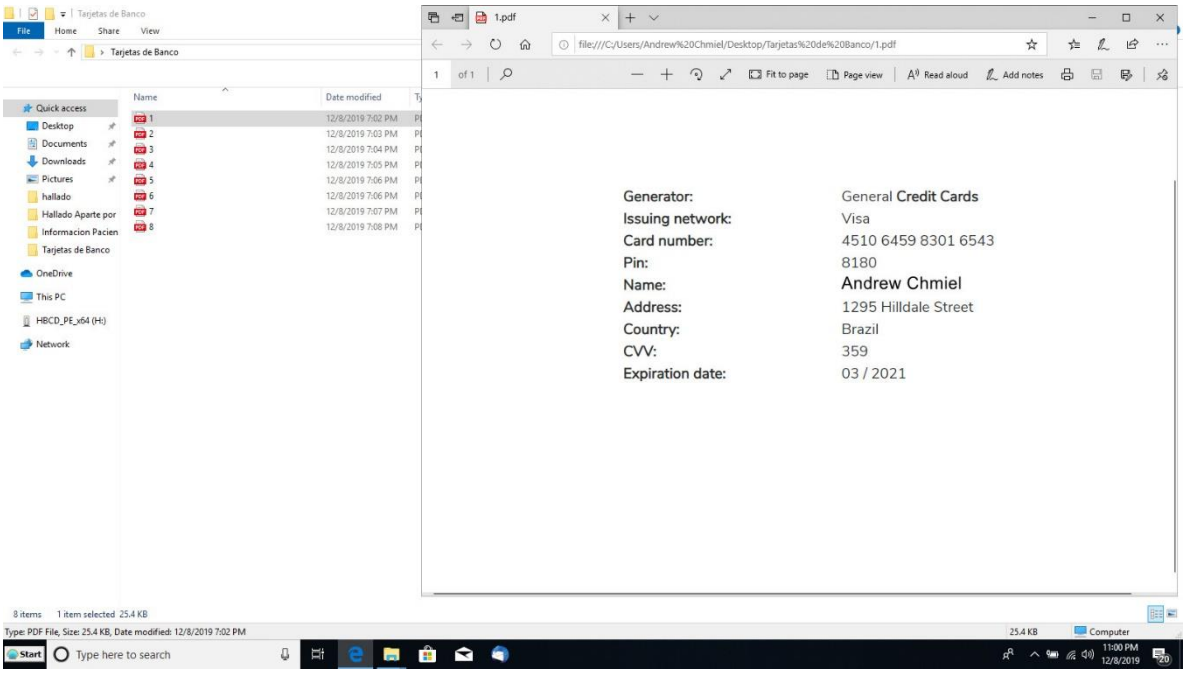



Figura 11. Carpeta con información de tarjetas de banco.

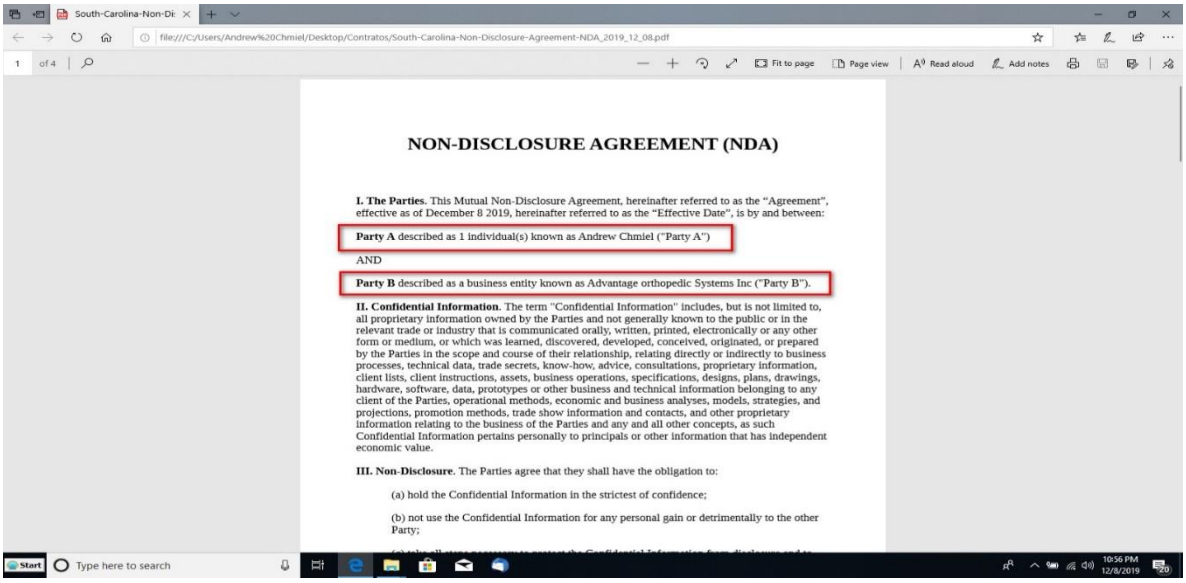



Figura 12. Contrato sobre no divulgación.

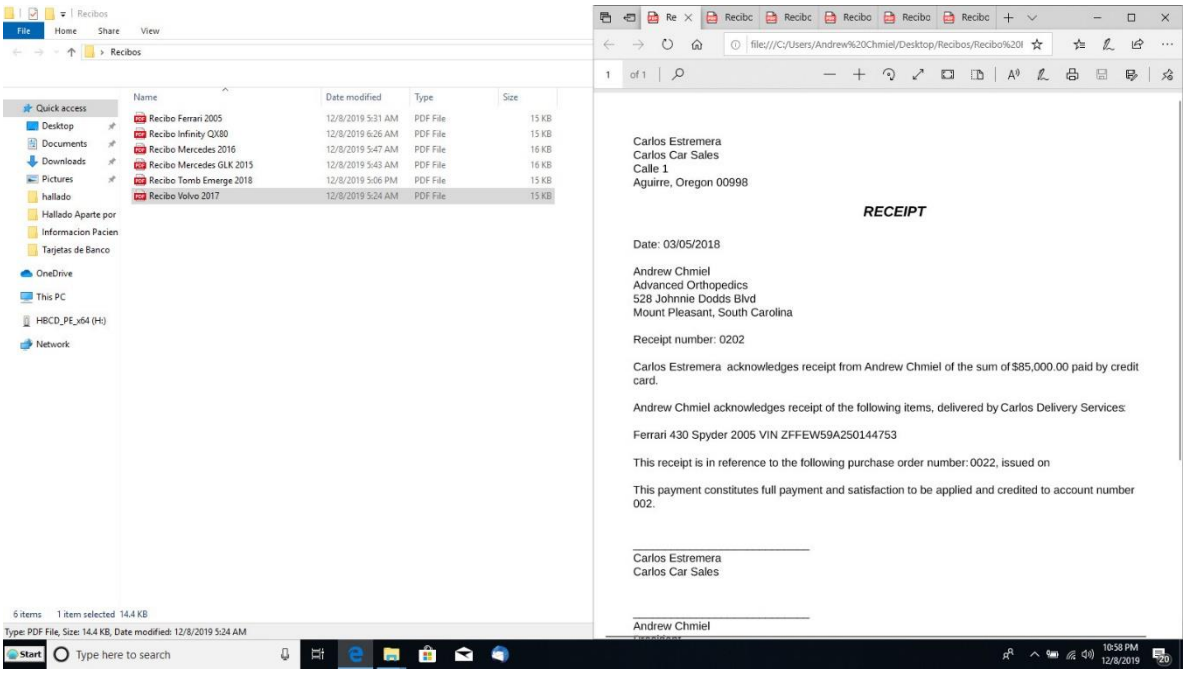



Figura 13. Recibo de compras de autos.

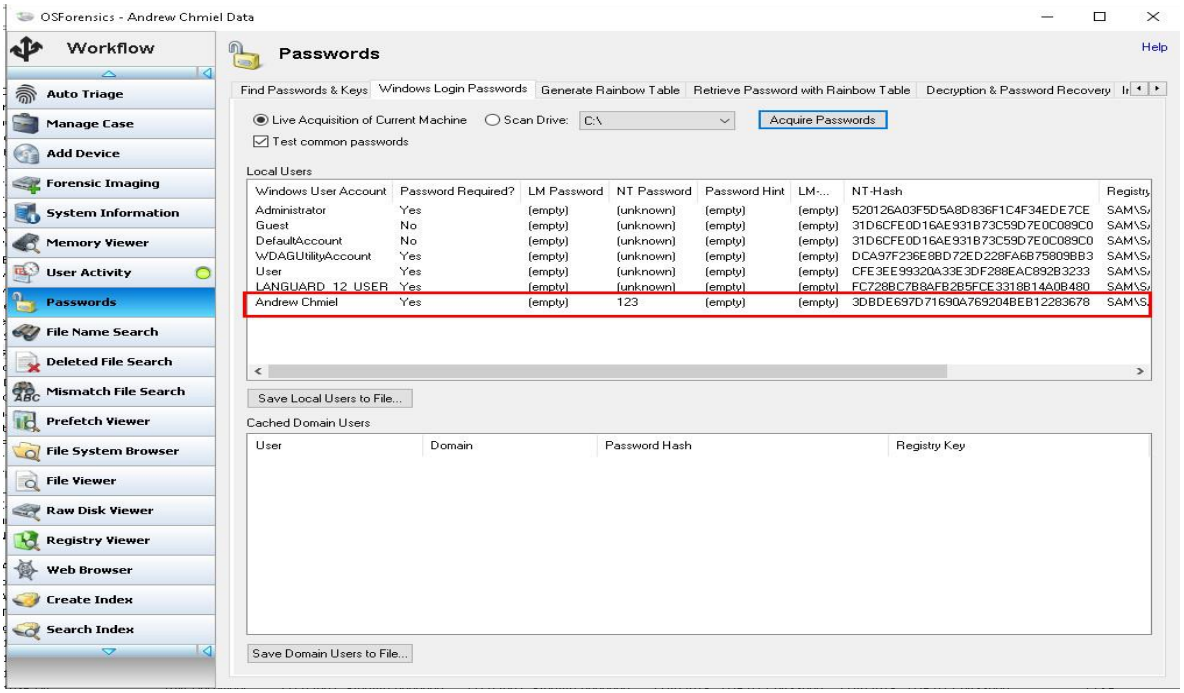



Figura 14. OsForensics. Hallazgo de claves de acceso sobre usuario de Andrew Chmiel.

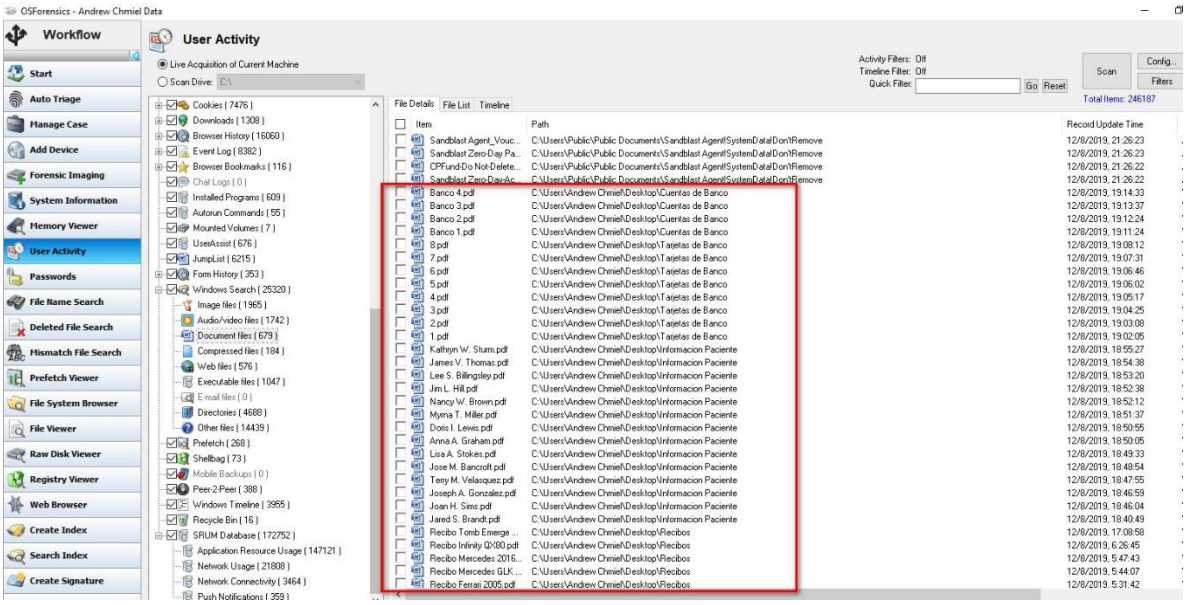



Figura 15. Nirsoft (Nirlauncher). Hallazgo de direcciones locales de carpetas y datos importantes.

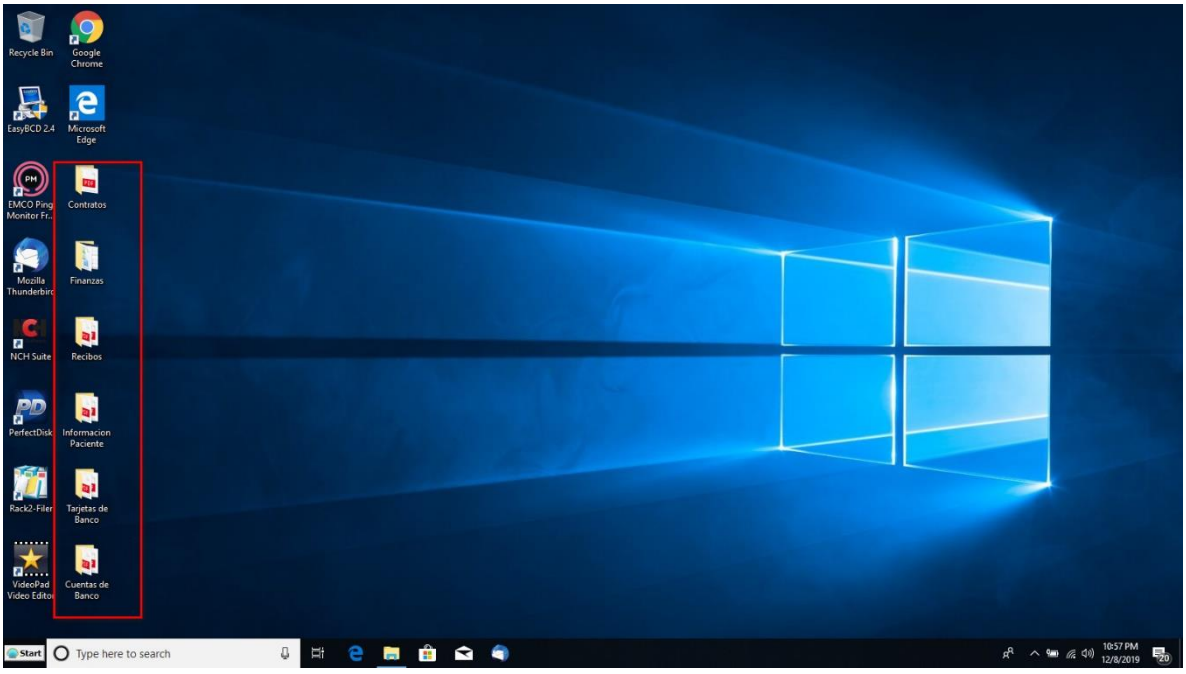



Figura 16. Hallazgo de las carpetas con datos importantes y su localización.

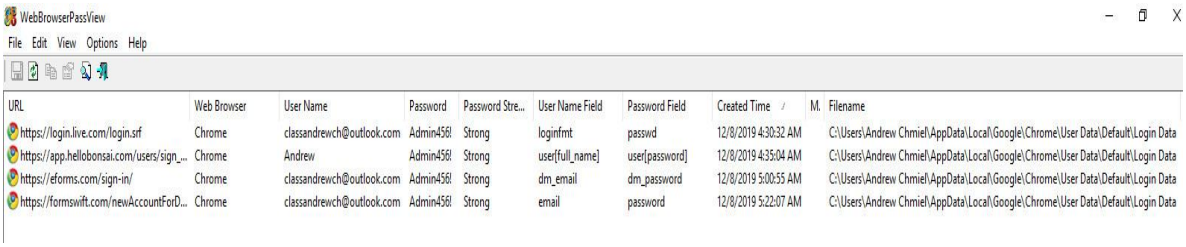



Figura 17. Hallazgo de clave e email de Andrew Chmiel.

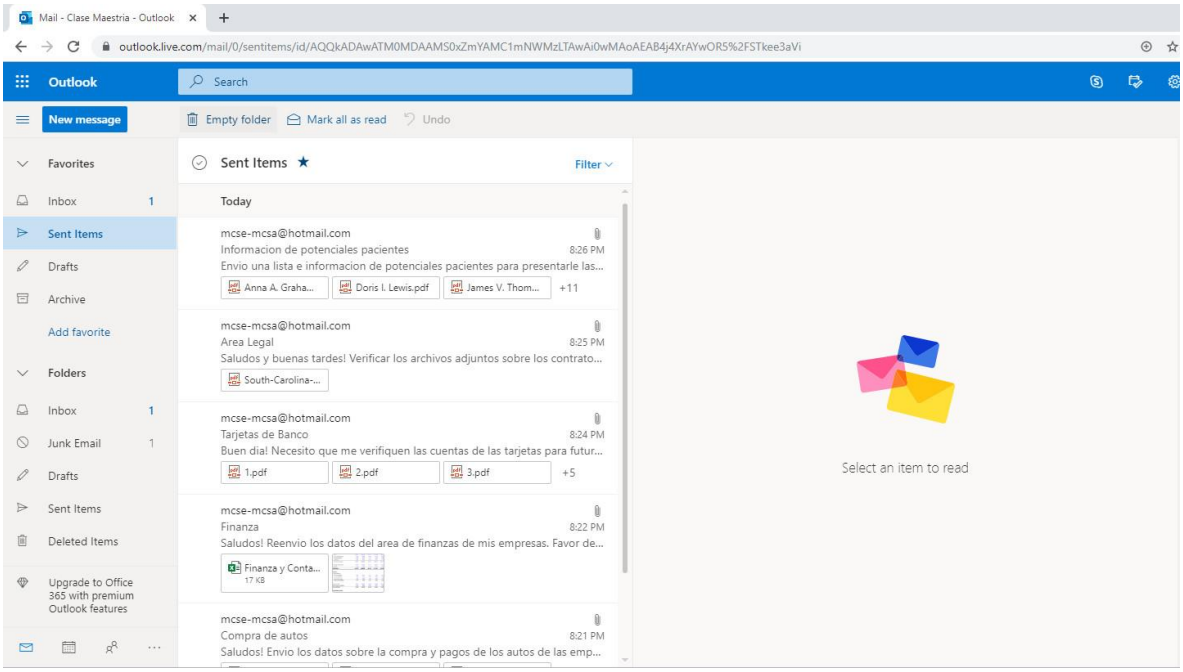



Figura 18. Ingreso al email de Andrew Chmiel y correos enviados con archivos importantes encontrados en su laptop.

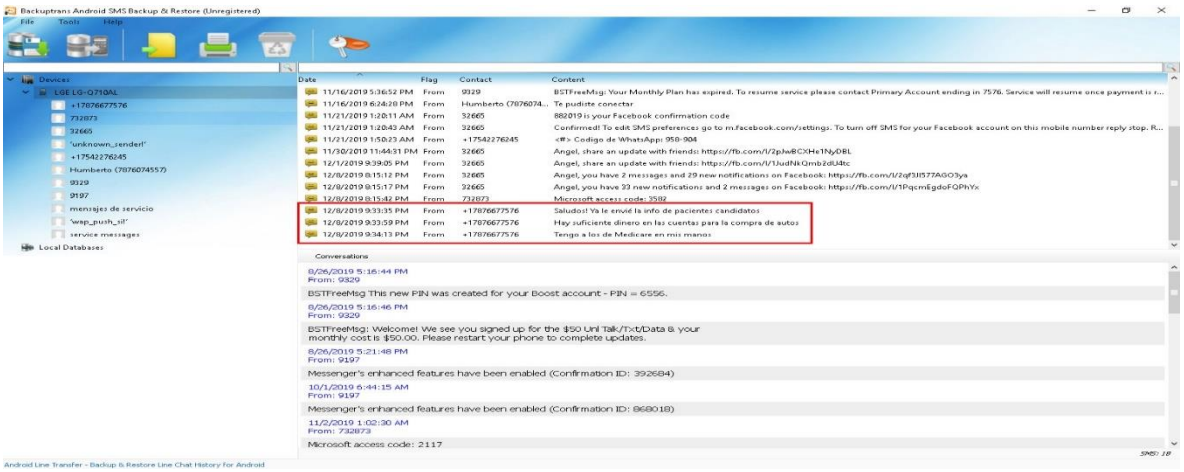


Figura 19. Backuptrans Android Texts. Hallazgo de textos regulares del celular.

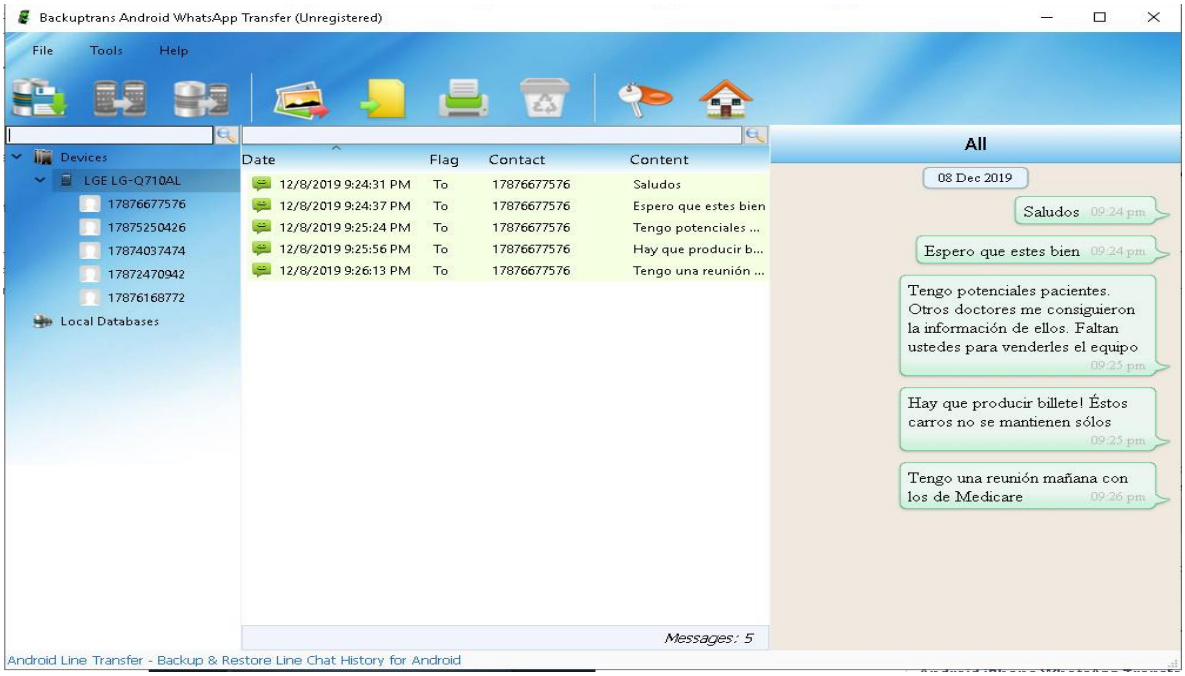



Figura 20. Backuptrans Android Whatsapp. Hallazgo de conversación en Whatsapp.

Cadena de Custodia

Primer Evento

Descripción del Evento: Entrega de la laptop de Andrew Chmiel (Laptop Toshiba Satellite l775, PSK3SU-09903T, Intel Core i5-2430 CPU @ 2.4GHz, 2 Cores, 4 Logical Processors) al laboratorio de Hammu Designs.

Evento verificado por: Sherri A. Lydon, United States Attorney.

Número de la evidencia: Ev-001

Fecha y Hora de comienzo: enero 1, 2019, 1:00PM.

Fecha y Hora de terminación: abril 4, 2019, 1:00PM.

Lugar de Origen: Propiedad de Andrew Chmiel, 528 Johnnie Dodd #3, Mt. Pleasant, South Carolina, Parcel No. 514-00-00-176.

Destino: Hammu Designs (Laboratorio de Forense), Calle Marginal D-10, Bahía Vistamar, Carolina, P.R., 00983.

Segundo Evento

Descripción del Evento: Entrega del celular de Andrew Chmiel (LG Stylo4 Modelo LG-Q710AL S/N 906VTDN2043122) Evento verificado por: Sherri A. Lydon, United States Attorney.

Número de la evidencia: Ev-002.

Fecha y Hora de comienzo: enero 1, 2019, 1:00PM.

Fecha y Hora de terminación: abril 4, 2019, 1:00PM.

Lugar de Origen: Propiedad de Andrew Chmiel, 528 Johnnie Dodd #3, Mt. Pleasant, South Carolina, Parcel No. 514-00-00-176.

Destino: Hammu Designs (Laboratorio de Forense), Calle Marginal D-10, Bahía Vistamar, Carolina, P.R., 00983.

Tercer Evento

Acceso a la bóveda donde permanecen guardados los equipo (Laptop y Celular) de Andrew Chmiel para la realización del servicio forense. Evento verificado por: Sherri A. Lydon, United States Attorney.

Número de la evidencia: Ev-003.

Fecha y Hora de comienzo: enero 1, 2019, 1:00PM.

Fecha y Hora de terminación: abril 4, 2019, 1:00PM.

Lugar de Origen: Propiedad de Andrew Chmiel, 528 Johnnie Dodd #3, Mt. Pleasant, South Carolina, Parcel No. 514-00-00-176.

Destino: Hammu Designs (Laboratorio de Forense), Calle Marginal D-10, Bahía Vistamar, Carolina, P.R., 00983.

Cuarto Evento

Descripción del Evento: Regreso del equipo investigado por los servicios de forense (Laptop y Celular de Andrew Chmiel). Evento verificado por: Sherri A. Lydon, United States Attorney.

Número de la evidencia: Ev-004.

Fecha y Hora de comienzo: abril 4, 2019, 1:00PM.

Fecha y Hora de terminación: abril 4, 2019, 1:00PM.

Lugar de Origen: Propiedad de Andrew Chmiel, 528 Johnnie Dodd #3, Mt. Pleasant, South Carolina, Parcel No. 514-00-00-176.

Destino: Hammu Designs (Laboratorio de Forense), Calle Marginal D-10, Bahía Vistamar, Carolina, P.R., 00983.

Quinto Evento

Descripción del Evento: Entrega de la laptop de Andrew Chmiel y celular a la corte.

Evento verificado por: Sherri A. Lydon, United States Attorney.

Número de la evidencia: Ev-001 y Ev-002.

Fecha y Hora de comienzo: abril 4, 2019, 1:00PM.

Fecha y Hora de terminación: abril 4, 2019, 1:00PM.

Lugar de Origen: Hammu Designs (Laboratorio de Forense), Calle Marginal D-10, Bahía Vistamar, Carolina, P.R., 00983.

Destino: Corte Federal, Clerk's Office, United States District Cour, Room 150 Federal Bldg 150 Carlos Chardon Avenue, San Juan, P.R. 00918-1767.

Procedimiento

Para ingresar al usuario, se requirió de una herramienta para el cambio de clave.


Figura 21. Herramienta Hirens Boot Cd.

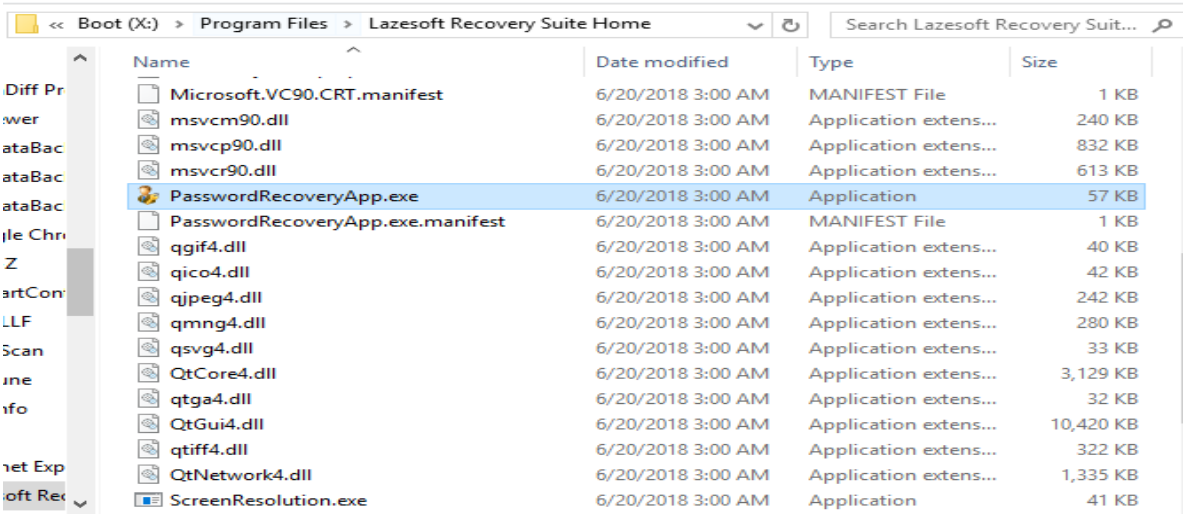



Figura 22. Utilizar la herramienta de Lazesoft Recovery My Password Home, incluida dentro de la suite de herramientas de Hirens Boot CD.

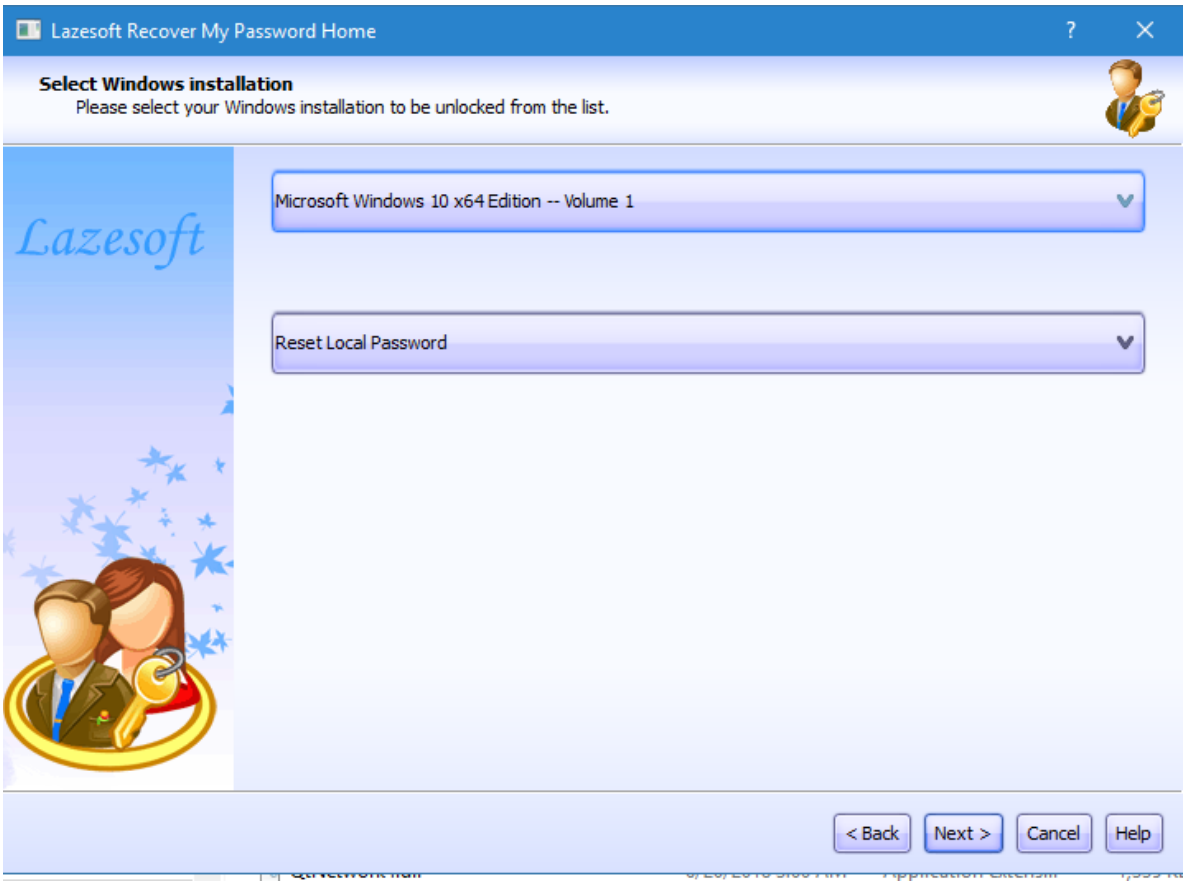



Figura 23. Escoger opciones.

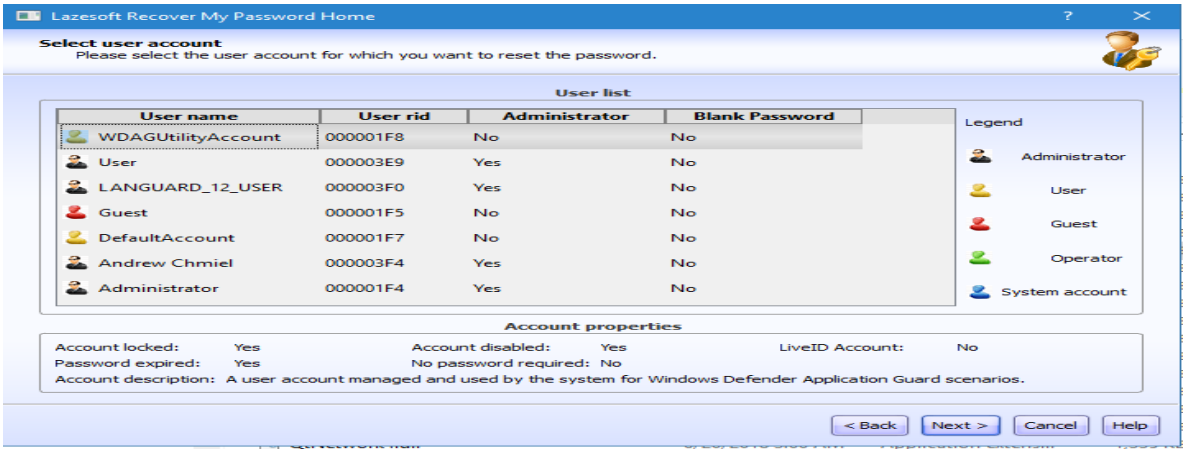



Figura 24. Escoger usuario para el cambio de clave.

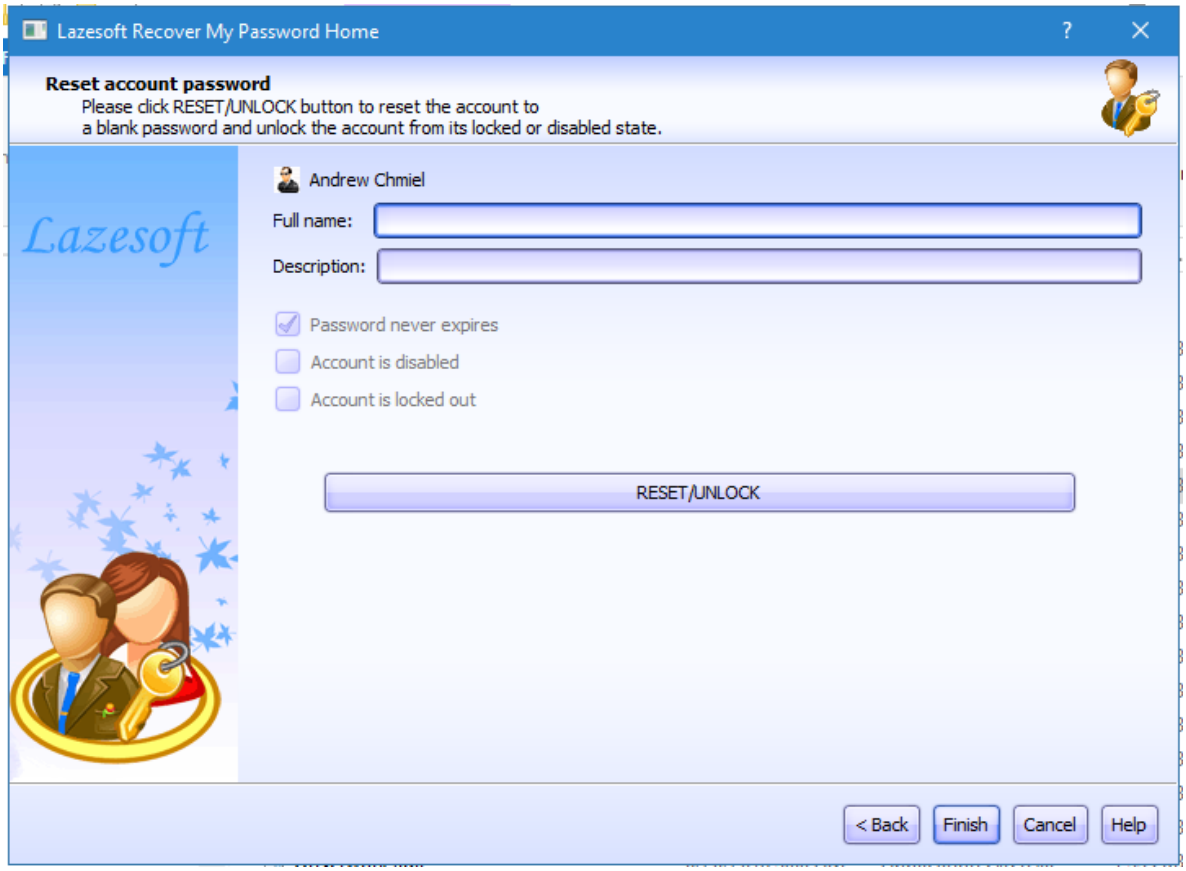



Figura 25. Cambiar la clave mediante *Reset/Unlock*.

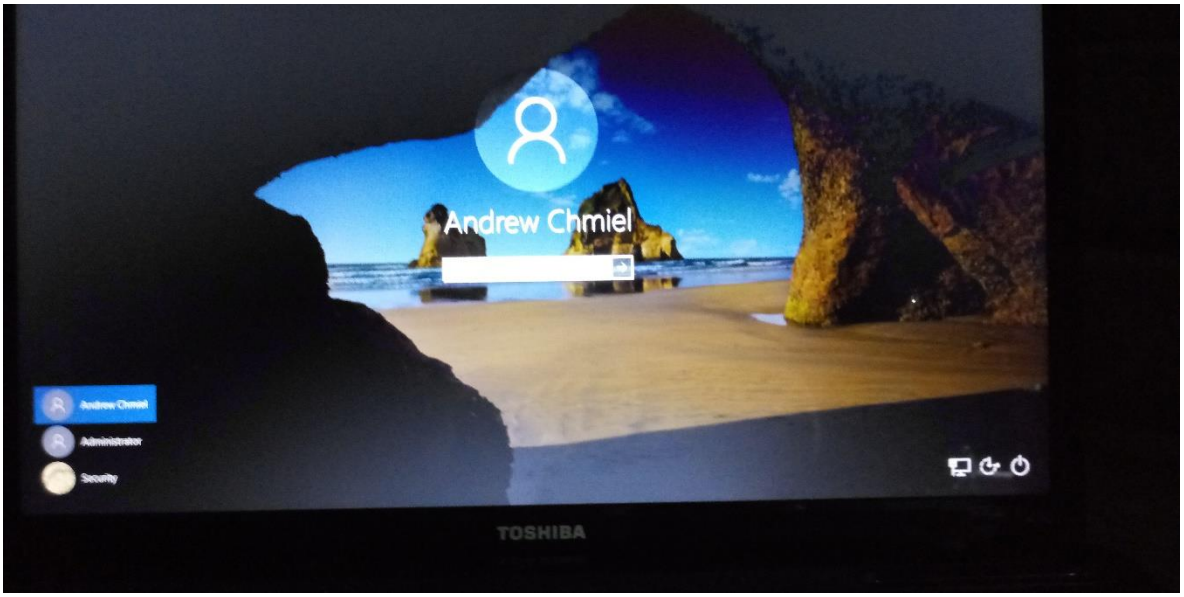



Figura 26. Ingreso al usuario Andrew Chmiel.

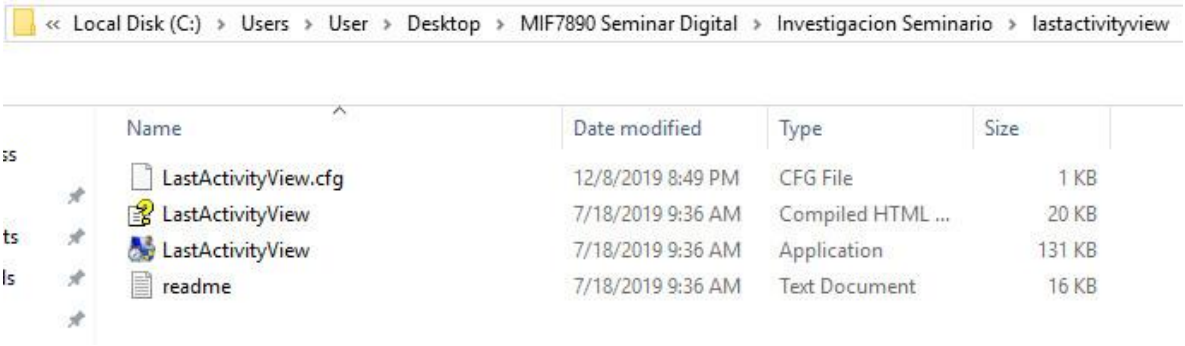



Figura 27. Ejecutar el programa Last Activity View

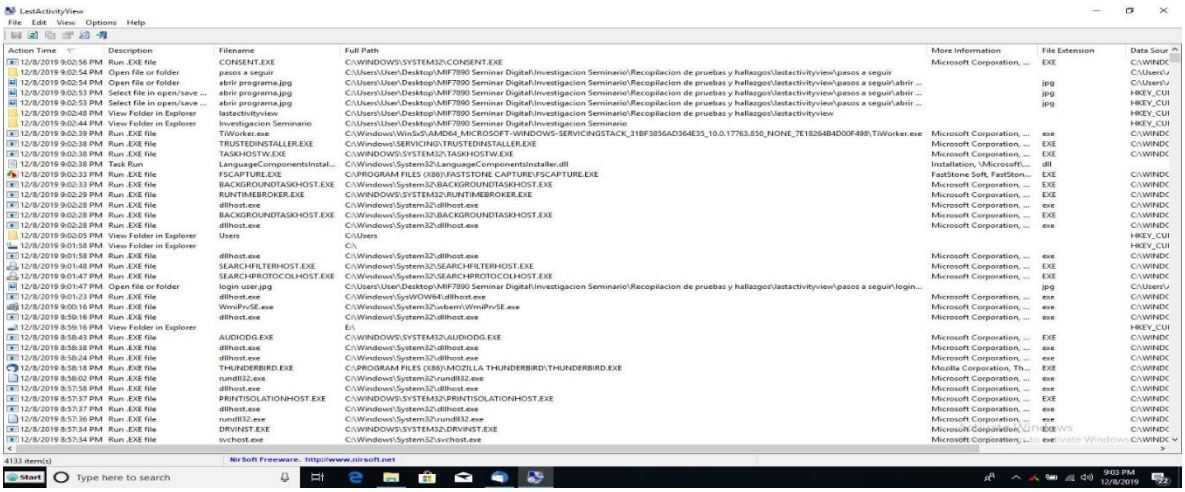


Figura 28. Pantalla inicial del programa. Se comienza la búsqueda del nombre de carpetas con nombres de datos importantes y su localización

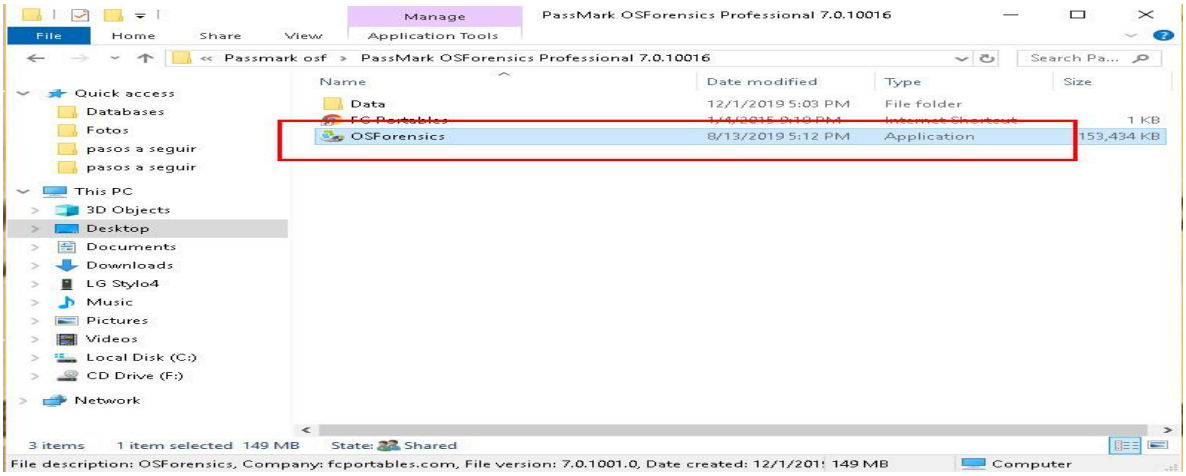


Figura 29. OSForensics. Dentro del usuario se verifica la clave para ingreso al usuario Andrew Chmiel. Se ejecuta el programa inicialmente.

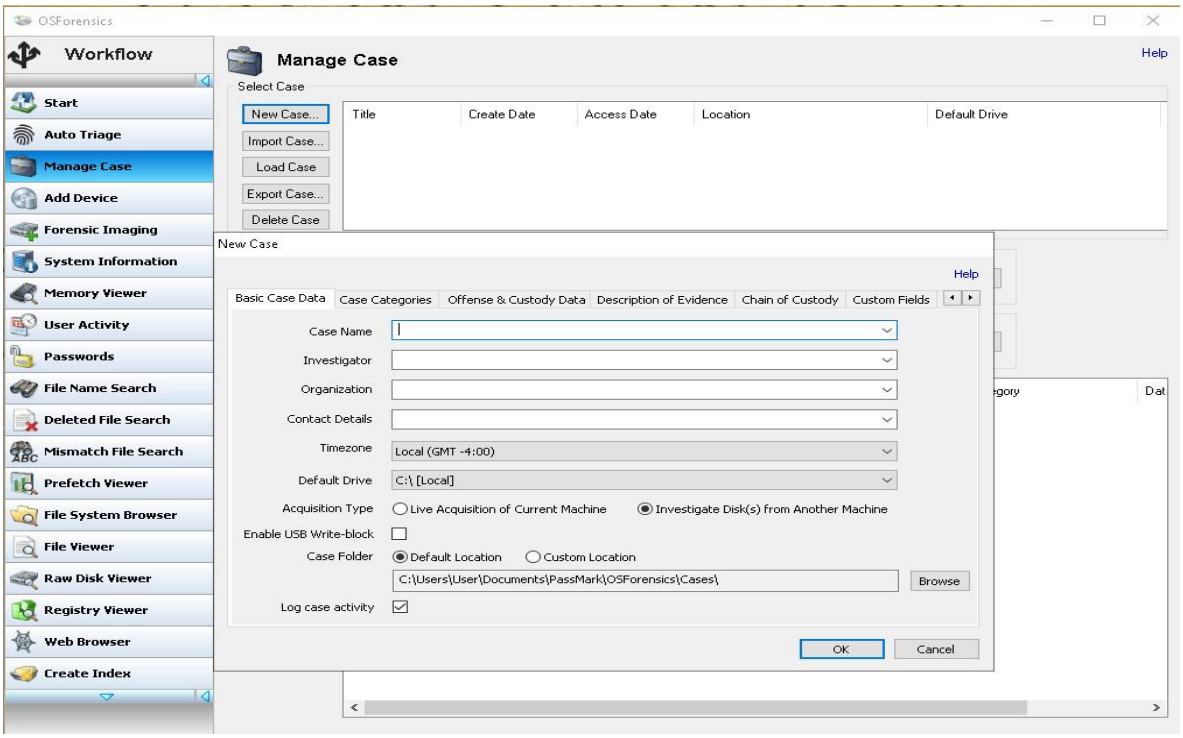



Figura 30. Se crea un caso.

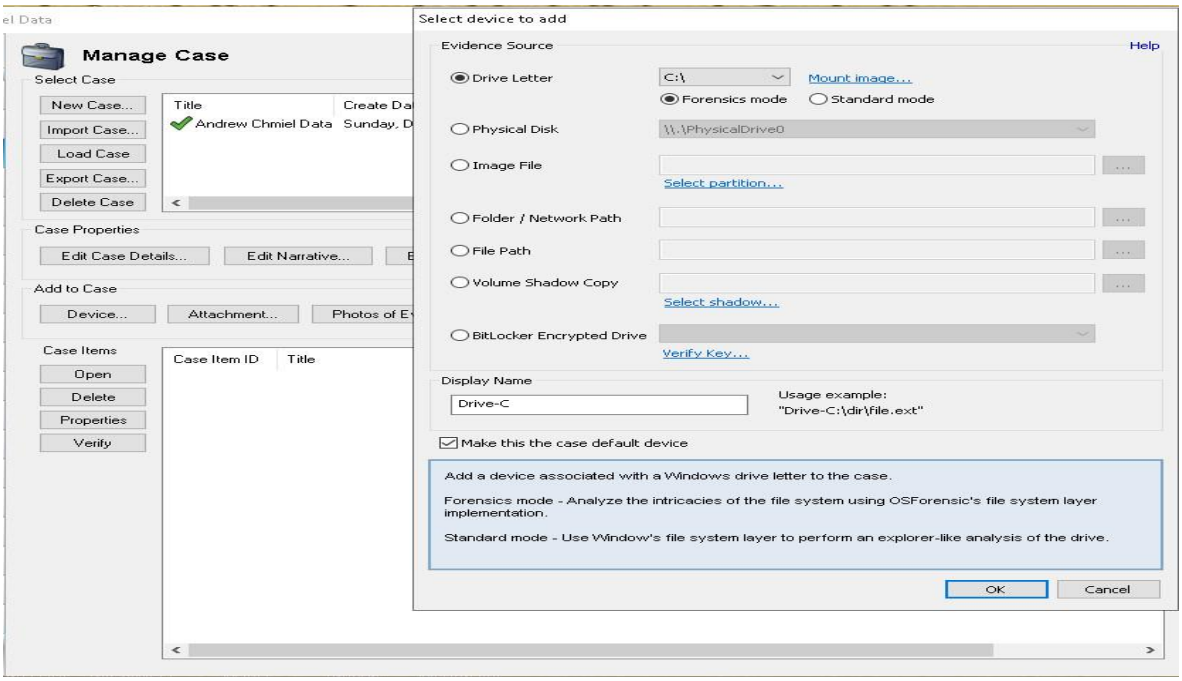


Figura 31. Se define el dispositivo a investigar. En este caso el disco duro C.

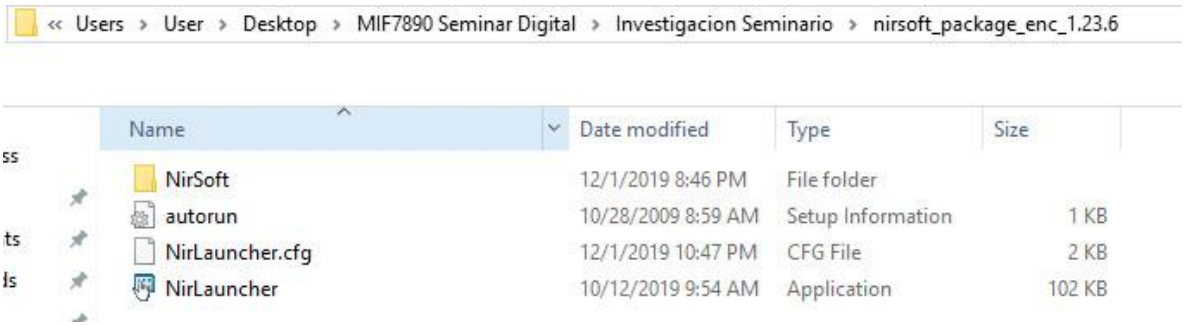



Figura 32. Entrar la clave de usuario y la dirección de correo de Andrew Chmiel requería del uso de Nirsoft (Nirlauncher). Del listado de programas, se utilizó la opción llamada WebBrowserPassView. Se identifica la dirección donde se situa el programa Nirsoft (Nirlauncher).

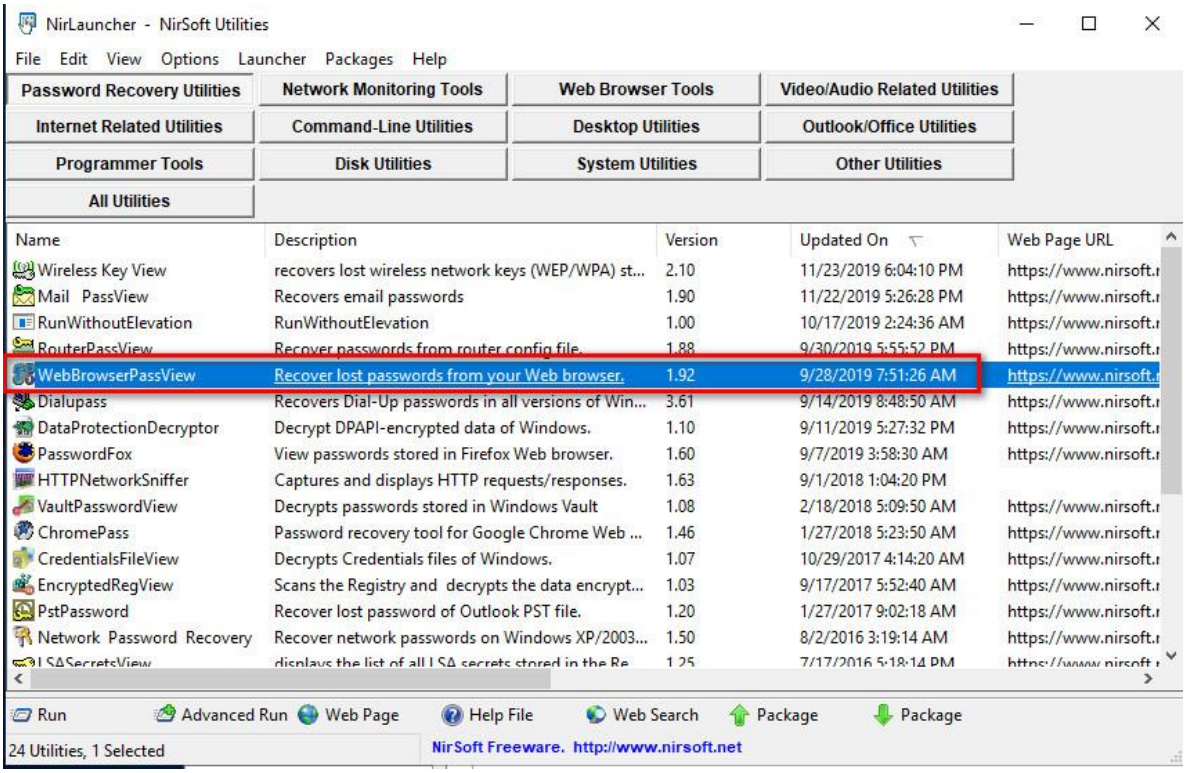



Figura 33. Del listado, se escoge la opcion llamada WebBrowserPassView.

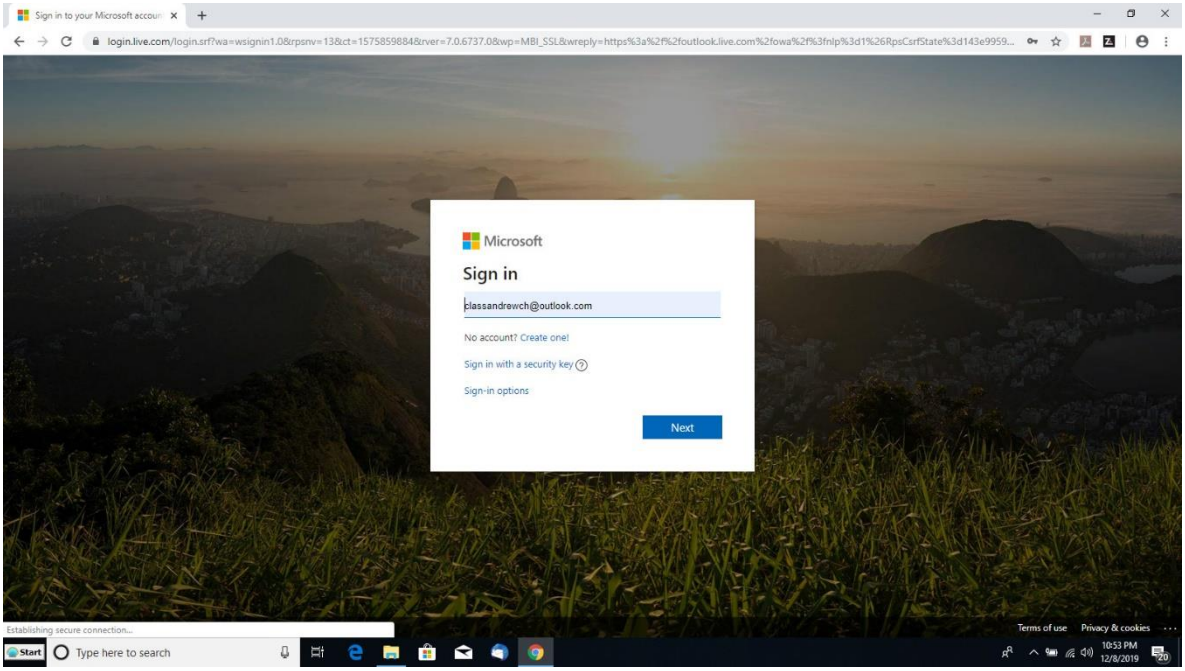
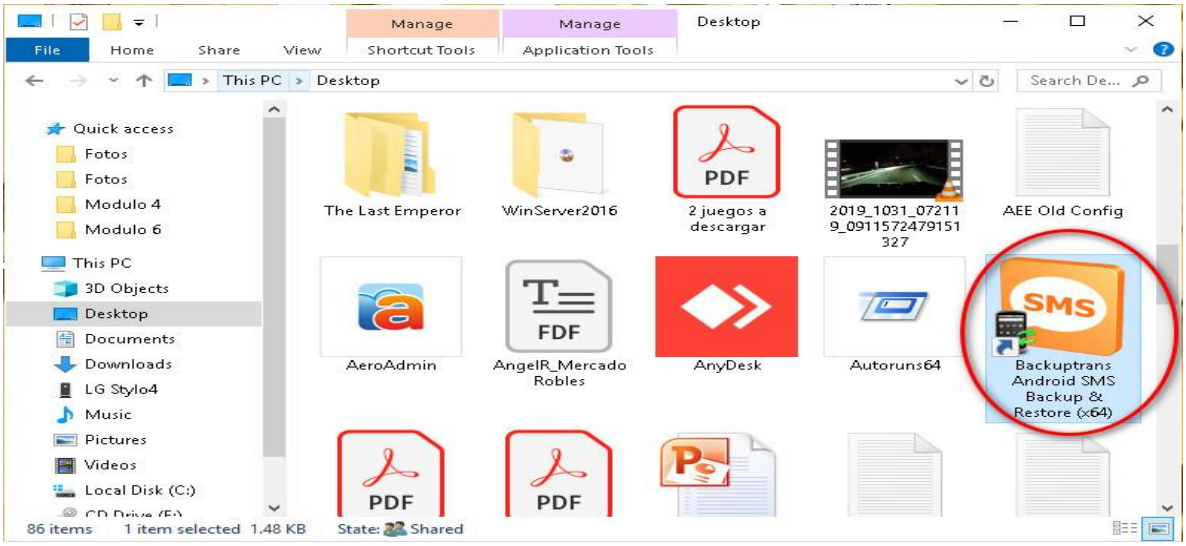



Figura 34. Con la información de correo obtenida, se ingresa a la misma utilizando algún explorador de internet.




Se comienza el trabajo de forense en el celular de Andrew Chmiel. Los datos de interés se concentran en los textos enviados por medio de Whatsapp y por medio de la aplicación de fábrica del celular. Se utilizan dos programas para el acceso a los textos.

Figura 35. Backuptrans Android SMS Backup and Restore.

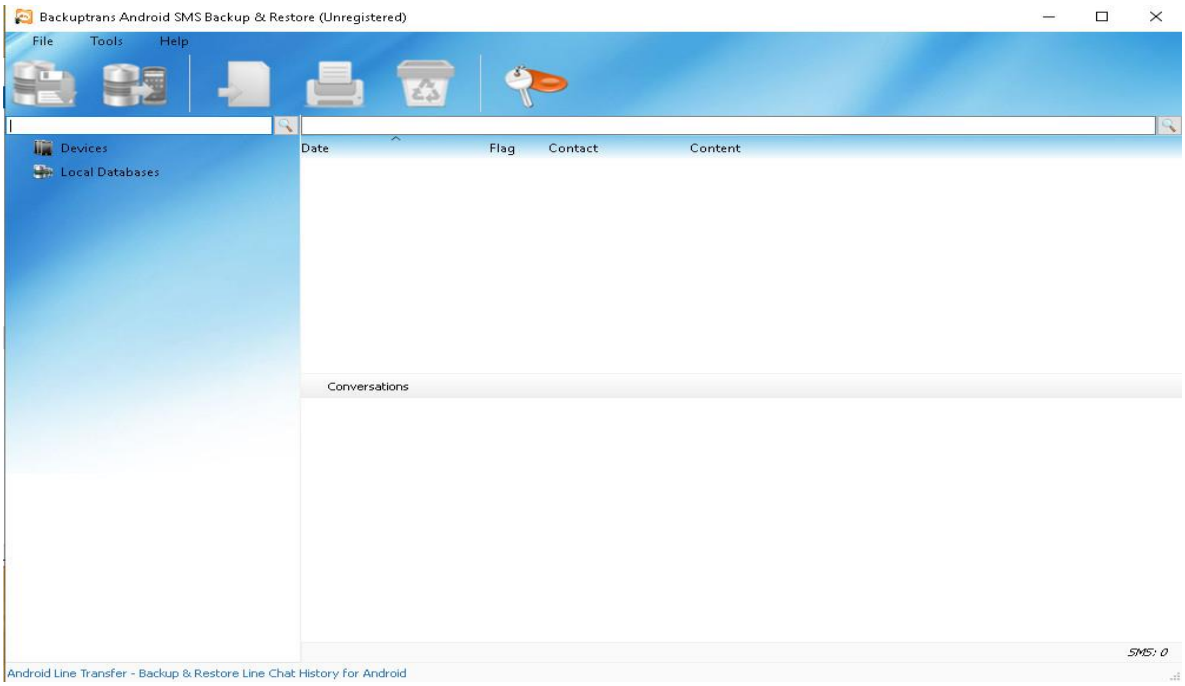



Figura 36. Uso de Backuptrans Android SMS Backup and Restore. Pantalla inicial.Figura


37. Conectar el celular de Andrew Chmiel a la laptop de forense.

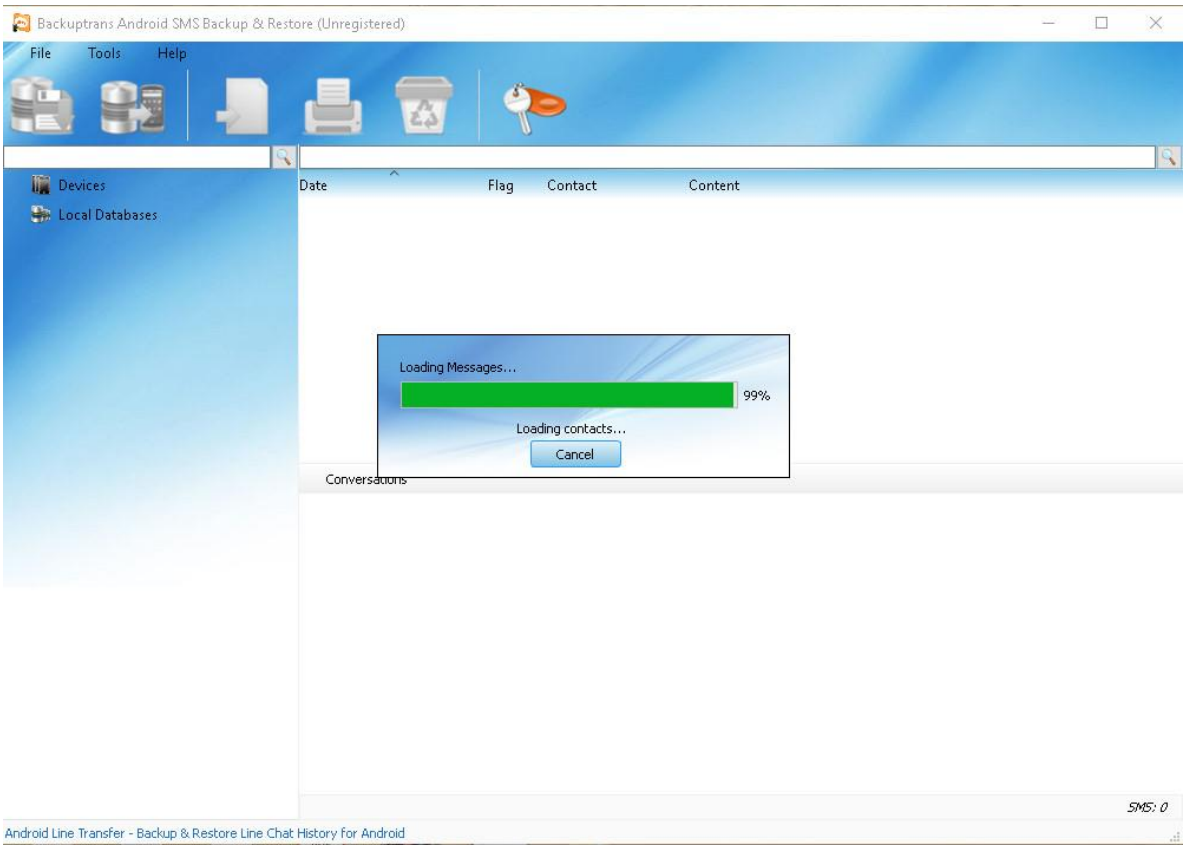



Figura 38. Backuptrans Android SMS Backup and Restore comienza cargando los mensajes.

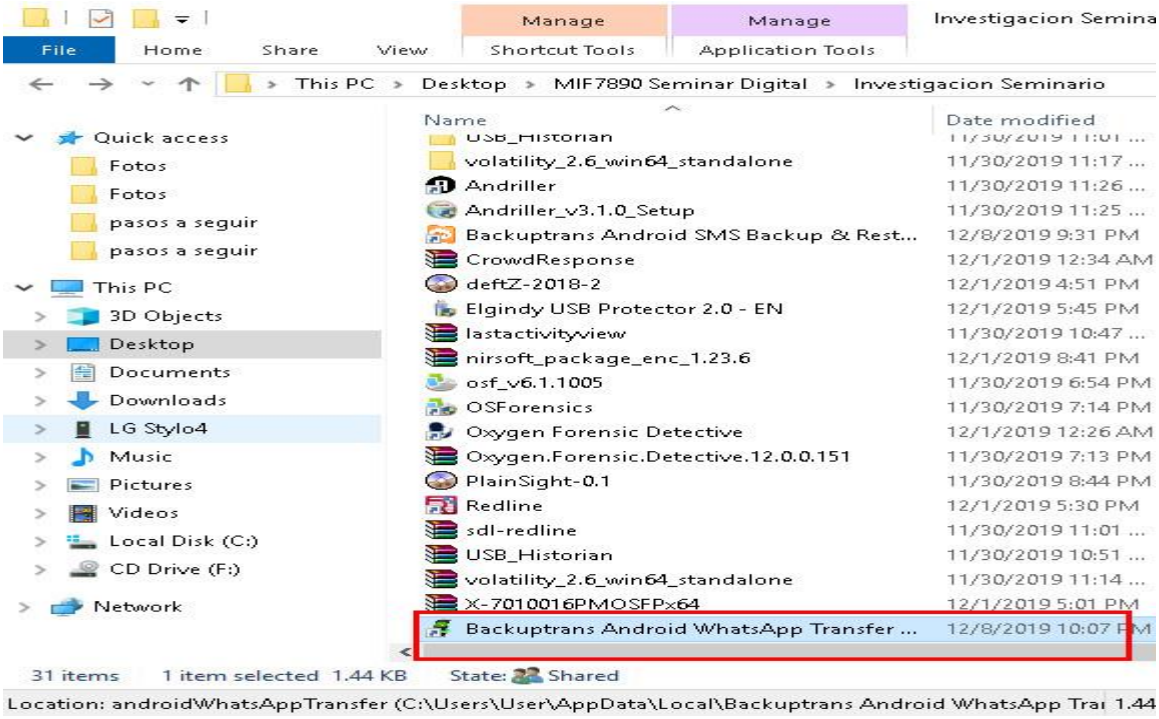



Figura 39. Backuptrans Android Whatsapp se utiliza para cargar los mensajes del celular de Andrew Chmiel. Los textos por Whatsapp son la prioridad. Se ejecuta el programa inicialmente.


Figura 40. Se conecta el celular de Andrew Chmiel a la laptop de forense.

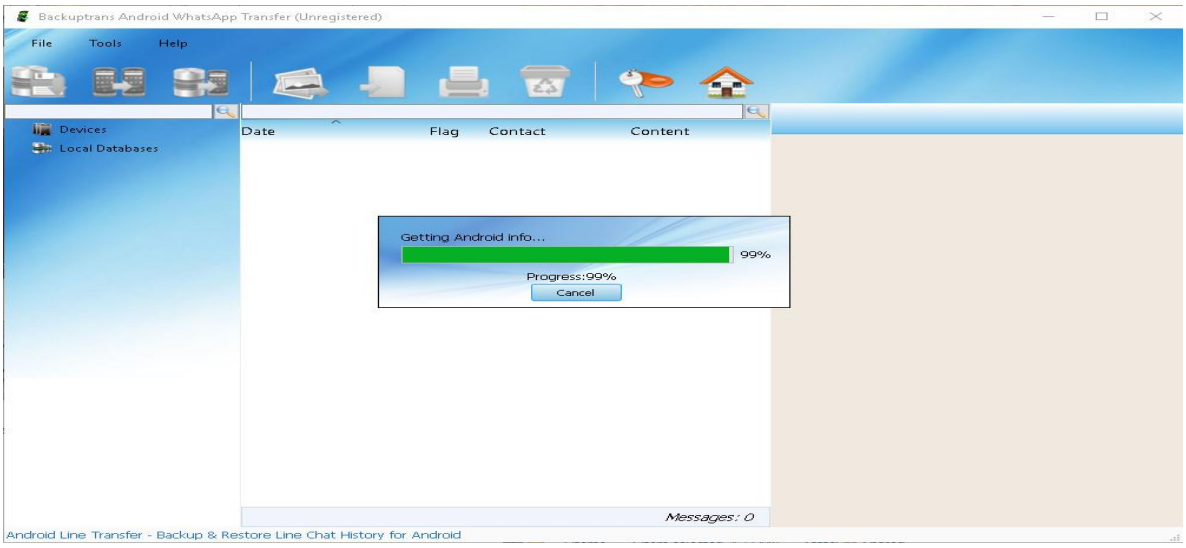



Figura 41. El programa comienza a extraer los textos.

## Conclusión

La información creada por Andrew Chmiel fue encontrada en su totalidad. Lo encontrado en su laptop tanto como en su celular es clave para la continuación del caso en cuestión. En un momento dado se utilizaron herramientas para lograr cargar su sistema en dispositivos externos. Luego de llevar a cabo las copias de su disco duro, se continuó con las copias y luego con los diversos programas que lograron capturar todo documento creado. Para lograr atar los documentos a su creación y a Andrew Chmiel, se verificó el uso de la computadora y los horarios, tanto, así como la conexión y uso de sus puertos usb.

El patrón de uso que Andrew Chmiel le daba a su computadora se pudo recobrar con las herramientas de forense. Esto a su vez presentaba los lugares y accesos a las diversas cuentas que el acusado tenía. Lo obtenido de su celular estaba en armonía con lo detallado de su computadora. Se logra con ello crear los eslabones que hacían falta para probar los comportamientos expuestos en corte.

# 5. DISCUSIÓN DEL CASO

Según el caso de corte, Andrew Chmiel crea cuentas “Shell” para su anonimato y entradas de dinero. A su vez logra entablar negocios con doctores, telemarketing en diversos países, contratos con lugares DME, cobros a Medicare, compras constantes de equipo proveniente de China y constante acceso a los datos personales de los pacientes. Todo el andamiaje es posible gracias a la constante comunicación con diversos entes, mediante correos electrónicos, creación de documentos personales y el recibir correos con los documentos de los pacientes. Todo lugar frecuentado por Andrew Chmiel mediante su explorador de internet fue grabado en su sistema.

Cuando los programas son utilizados para crear documentos, para navegar el internet y para conectar dispositivos externos, el sistema operativo guarda los cambios y mantiene una bitácora de lo llevado a cabo. Con las herramientas forenses podemos hallar esos comportamientos y encaminarnos al lugar específico en donde se encuentren los datos en cuestión. Al leer los escritos creados por Andrew Chmiel y lo recibido por su contraparte, las acusaciones se convierten en hechos.

Los daños causados por los fraudes imputados a Andrew Chmiel fueron de manera directa e indirecta hacia los pacientes que fueron la víctima principal. Las pérdidas en dinero de Medicare fueron por una totalidad en cifras de billones. Los pacientes también tienen su baja y lo más que se pierde es la confianza en los DME, los doctores y en las medidas de seguridad que se han tenido hasta ahora.

# 6. AUDITORIA Y PREVENCIÓN

## Trasfondo

El caso de Andrew Chmiel se enfoca en las vulnerabilidades sobre manejo de información y procesos entre los DME (Durable Medical Equipment), doctores, documentos y Medicare. Los pacientes que recibieron los equipos de los DME tuvieron que llenar documentos de información personal y brindar sus firmas para que los doctores refieran su caso. Sin embargo, los pacientes recibieron equipo médico para condiciones que no tienen. A su vez se les cobraba por servicios que no recibieron o les cobraban demás.

Estos acontecimientos se llevaban a cabo por Andrew Chmiel, las empresas del cual era dueño, doctores que fueron sobornados y por pacientes que no estaban debidamente informados en cómo manejar estas situaciones. Los doctores solo requieren del permiso de los pacientes, los doctores refieren pacientes a los DME y los DME llevan a cabo el encargo de los equipos médicos. Luego de los servicios ser prestados, Medicare reembolsaba el dinero, los DME y Andrew Chmiel les pagaba a los doctores y así continuaba la cadena del fraude. Las promociones de servicios de tele mercadeo al que Andrew Chmiel se mantenía invirtiendo, llevaban a cabo las llamadas al listado de pacientes que les eran referidos.

## Alcance

Se presentará el caso tomando en cuenta los mecanismos utilizados para llevar a cabo el pedido de servicios, mecanismos actuales de documentación, cadena de pasos antes y después de llevar a cabo el pedido de equipos médicos. Se utilizará como consulta los conceptos de auditoria, vulnerabilidades encontradas y posibles soluciones.

Objetivo

Estos casos son estudiados para mejorar deficiencias que presentan diversos servicios ofrecidos por parte del gobierno federal a los pacientes. Los fallos en comunicación, documentación y educación son los temas que se discutirán. Esto incluye lo ocurrido, lo que se pudo prevenir y lo que se puede mejorar. El enfoque trata de controles no llevados a la práctica y como cada etapa tuvo su manera de ser prevenida. Se pretende brindar enfoque en mejores prácticas y herramientas que se debieron utilizar. Esto significa que, de ocurrir nuevamente, se pueda adaptar cualquier empresa o paciente que se encuentre en medio de un fraude o potencial fraude.

## Hallazgos detallados

Condición

La tendencia de acudir a personas envejecientes para estos tipos de fraude sigue en aumento. Este caso no es la excepción. Las víctimas eran por lo general personas convalecientes o envejecientes (Ap, 2019). Muchas personas no están debidamente educadas en temas sobre fraude y que hacer en tales momentos. Esto resume el primer hallazgo sobre el fraude del caso en cuestión. En segundo lugar, Medicare no estaba dudando de las prácticas de pagos y reembolsos llevados a cabo, ya que no ofrecieron el llevar a cabo una auditoria. Según Brooke Andrus (2014), existe un listado de comportamientos que debes evitar para que Medicare no sospeche de tus acciones como proveedor de algún tipo de servicio. Significa que las personas que llevan a cabo acciones ilícitas se actualizan constantemente para no sonar ningún tipo de alarma.

Los doctores que fueron parte de este esquema fueron parte de las debilidades de todo el sistema. Se requería de ellos la información de los pacientes, permiso de los

pacientes y sus firmas. El próximo paso es que cada DME compre los equipos médicos, de baja calidad, para ser enviado a los pacientes. Si los pacientes no notaban algo raro o simplemente no cuestionaban las acciones de sus doctores y entrega de equipo innecesario, el esquema continuará sin ser detectado. Como paso final, los DME piden su reembolso a Medicare.

Criterio

Si los controles estuviesen en vigor, Medicare hubiese llevado a cabo una auditoria. Parte de los signos que pueden llamar la atención, que también ocurría en este esquema de fraude, son los siguientes (Andrus, 2014, Julio):

- Para utilizar más dinero del límite impuesto, se llevaban a cabo modificadores KX, lo cual indican que se tenía que llevar a cabo ese cambio en el documento para poderse cobrar según la condición del paciente.
- Múltiples doctores cobrando bajo un mismo número de proveedor.
- Cobrar utilizando números de código por encima del promedio, según las fechas de servicio.

  Sin embargo, los DME no causaban dudas al llevar a cabo lo siguiente (Andrus, 2014, Julio):

- No perdían ni dejaban de enviar los certificados de los planes de los pacientes.
- Daban buena supervisión al paciente.
- Estaban cumpliendo con los créditos requeridos por Medicare.
- No enviaban documentos sin las firmas de los doctores.
- Enviaban toda documentación requerida y completa.
- Le brindaban los historiales médicos completos y a tiempo a Medicare.

- Cobraban lo requerido, según el estatus e información del paciente.

Causa

Fue causada por falta de rigurosidad en los controles por los cuales los DME y Medicare se rigen. La operación que se llevaba a gran escala era para haberse auditado, aunque no diese razón para causar dudas. Si cada cierto tiempo se llevase a cabo auditoria en diversos lugares que generan mucha entrada de dinero, estos casos fuesen de menor ocurrencia.

Efecto

El impacto en la organización, en este caso Medicare, a causa de la condición, se resume de la siguiente manera:

- Pérdida de $2 mil millones de dólares.
- Aumento en primas.
- Quitar algunos servicios.
- Pasos más rigurosos para el pago de algunos procedimientos.
- Pérdida de dinero en constantes investigaciones, después de las perdidas por fraude surgir.

Recomendaciones

- Auditorias cada 3 años.
- Auditorias cada cantidad de dinero generado.
- Pedir listado de doctores y auditar sus referidos.
- Auditoria de expedientes médicos digitalizados.

- Pedir listado de pacientes por recibir y recibiendo equipo médico, verificando si van acorde a su cuadro e historial.
- Entrevistar a los pacientes.

# 7 CONCLUSIÓN

Los datos obtenidos muestran fallas en tanto los mecanismos de detección de fraude de Medicare, auditorias requeridas, abuso de poder de los doctores y de los DME (Durable Medical Equipment). Otro factor que se encuentra vulnerable es el sector de personas envejecientes. El caso de Andrew Chmiel presenta un cuadro en donde se conglomera un panorama que requiere de atención.

Medicare no lleva a cabo auditorias de rutina (Indest, 2019). Si se lleva a cabo alguna actividad en la que Medicare sospeche de algún tipo de actividad cuestionable, entonces acuden a una auditoria. Andrew Chmiel, mediante el uso de sus DME, los doctores que por medio de sobornos utilizaba, los cobros a Medicare y la entrega de equipo chino de baja calidad, fueron llevados a cabo sin inicial ningún tipo de duda. La incomodidad provino de doctores que decidieron alertar al FBI sobre el posible fraude.

Andrew Chmiel evitaba llamar la atención de Medicare. Significa que no llevaba a cabo el *copiar y pegar* de documentación del paciente y requerido por Medicare, no utilizaba códigos de servicios y cobros tan distintos a los utilizados por otros DME, se enfocaba en la decisión del doctor primario del paciente, utilizaba personal certificado para llenar documentos y especificaba los procedimientos que parecían ser necesarios (Roberts, 2014, noviembre).

Este caso muestra lo vulnerable que un sistema puede estar; Se detalla el fraude por etapa; Las herramientas utilizadas como parte de la investigación forense demuestran la capacidad tecnológica y de conocimiento que se requiere; Destaca la importancia de las auditorias de rutina y ayuda en la mejoría de los controles dentro y fuera de Medicare. Aunque la perdida de dinero fue cuantiosa, el aprendizaje y cambios que se deben implementar dan cabida a futuras mejoras para los tiempos venideros.

# REFERENCIAS

Andrus, B. (2014, Julio, 16).

*AP*. (2019, mayo, 6). Obtenido de https://apnews.com/fad086a48fef4ee292028f6ed56f6065.

Auerbach & White, N. (2019). *Whistle Blower Firm*. Retrieved from https://www.whistleblowerfirm.com/qui-tamfalse-claims-act/what-is-a-false-claim/.

*BackupTrans*. (2019). Obtenido de https://www.backuptrans.com/download.html#ax2.

*BackupTrans*. (2019). Obtenido de https://www.backuptrans.com/download.html#ax2.

*CBS*. (2019, noviembre, 15). Obtenido de https://baltimore.cbslocal.com/2019/11/15/nicole-williams-tawanna-gaines-maryland-house-of-delegates/.

*Click On Detroit*. (2019, noviembre 14). Obtenido de https://www.clickondetroit.com/news/2019/11/14/metro-detroit-jeweler-joseph-dumouchelle-facing-federal-wire-fraud-charges/.

*CMS*. (2019). Obtenido de https://www.cms.gov/Medicare/Compliance-and-Audits/Part-C-and-Part-D-Compliance-and-Audits/Downloads/Program_Audit_Process_Overview.pdf.

*Cornell*. (2019). Obtenido de https://www.law.cornell.edu/uscode/text/18/287.

*Cornell*. (2019). Obtenido de https://www.law.cornell.edu/uscode/text/18/1341#.

*Cornell*. (2019). Obtenido de https://www.law.cornell.edu/uscode/text/18/981.

*Cornell*. (2019). Obtenido de https://www.law.cornell.edu/uscode/text/18/371.

*Cornell*. (2019). Obtenido de https://www.law.cornell.edu/uscode/text/28/2461.

*Cornell*. (2019). Obtenido de https://www.law.cornell.edu/uscode/text/18/1001.

*Cornell*. (2019). Obtenido de https://www.law.cornell.edu/uscode/text/18/1347.

*Cornell*. (2019). Obtenido de https://www.law.cornell.edu/uscode/text/18/1343.

*Cornell*. (2019). Obtenido de https://www.law.cornell.edu/uscode/text/18/982.

Doyle, C. (2016, enero 20). *FAS*. Obtenido de https://fas.org/sgp/crs/misc/R41223.pdf.

Doyle, C. (2018, mayo, 11). *FAS*. Obtenido de https://fas.org/sgp/crs/misc/98-808.pdf.

Doyle, C. (2019, febrero, 11). *FAS*. Obtenido de https://fas.org/sgp/crs/misc/R41930.pdf.

Doyle, C. (2019, febrero, 11). *FAS*. Obtenido de https://fas.org/sgp/crs/misc/R41930.pdf.

Ellison, A. (2018, Julio, 2). *Beckers Hospital Review*. Obtenido de https://www.beckershospitalreview.com/legal-regulatory-issues/15-latest-healthcare-industry-lawsuits-settlements-070218.html.

*EPGD Law*. (2019, enero, 16). Obtenido de https://www.epgdlaw.com/what-are-some-of-the-benefits-of-having-a-shell-company/.

*FBI Gov*. (2019). Obtenido de https://www.fbi.gov/investigate/white-collar-crime/health-care-fraud/health-care-fraud-news.

*FBI Gov*. (2019). Obtenido de https://www.fbi.gov/investigate/white-collar-crime/news.

*Federal Lawyer*. (2019). Obtenido de https://federal-lawyer.com/federal-health-care-fraud-statute/.

*Head Start*. (2018, marzo, 21). Obtenido de https://eclkc.ohs.acf.hhs.gov/es/gestion-fiscal/articulo/fraude-desperdicio-y-abuso.

*Hirens Boot CD*. (2019). Obtenido de https://www.hirensbootcd.org/download/.

Indest, G. F. (2019). *The Health Law Firm*. Obtenido de https://www.thehealthlawfirm.com/resources/health-law-articles-and-documents/medicare-audits.html.

*Justice Gov*. (2018, noviembre 21). Obtenido de https://www.justice.gov/usao-sdfl/pr/man-pleads-guilty-laundering-proceeds-romance-and-cyber-scams.

*Justice Gov*. (2019). Obtenido de https://www.justice.gov/usao-nh/pr/hampton-woman-pleads-guilty-mail-fraud-scheme.

*Justice Gov*. (2019). Obtenido de https://www.justice.gov/usao-sdfl/pr/broward-county-resident-charged-wire-fraud-mail-fraud-and-money-laundering-relating.

*Justice Gov*. (2019, octubre, 11). Obtenido de https://www.justice.gov/usao-sdfl/pr/broward-county-resident-charged-wire-fraud-mail-fraud-and-money-laundering-relating.

*Justice Gov*. (2019, abril, 29). Obtenido de https://www.justice.gov/usao-ma/pr/former-united-states-postal-service-manager-pleads-guilty-bribery-witness-tampering-and.

*Justice Gov*. (2019, abril, 11). Obtenido de https://www.justice.gov/usao-dc/pr/washington-based-lawyer-indicted-charge-making-false-statements-department-justice.

*Justice Gov*. (2019, noviembre, 13). Obtenido de https://www.justice.gov/usao-ndok/pr/10-men-involved-nigerian-romance-scams-indicted-money-laundering-conspiracy.

*Justice Gov*. (2019, octubre, 10). Obtenido de https://www.justice.gov/usao-sdny/pr/18-members-international-fraud-and-money-laundering-conspiracy-charged-manhattan.

Justice, D. o. (2019, Abril, 9). *Department of Justice*. Obtenido de Federal Indictments & Law Enforcement Actions in One of the Largest Health Care Fraud Schemes Involving Telemedicine and Durable Medical Equipment Marketing Executives Results in Charges Against 24 Individuals Responsible for Over $1.2 Billion in Losses: https://www.justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes

Justice, D. o. (2019, Mayo, 11). *Department of Justice*. Obtenido de DOCUMENTS AND RESOURCES FROM THE APRIL 9, 2019 PRESS RELEASE ON HEALTH CARE FRAUD: https://www.justice.gov/opa/documents-and-resources-april-9-2019-press-release-health-care-fraud

*Justive Gov*. (2018, diciembre, 19). Obtenido de https://www.justice.gov/usao-ndil/pr/9-defendants-charged-chicago-international-investigation-targeting-romance-scams-and.

Kluwer, W. (2019). *Biz*. Obtenido de https://www.bizfilings.com/toolkit/research-topics/running-your-business/fraud-protection/recognizing-and-avoiding-mail-and-wire-fraud-schemes.

*Lazesoft*. (2019). Obtenido de https://www.lazesoft.com/contact.html.

*Medium*. (2019, junio 25). Obtenido de https://medium.com/kyc-io-scalable-kyc-management-solutions/the-5-largest-money-laundering-scandals-of-all-time-so-far-d30ff4abee10.

Monk, J. (2019, Abril, 9). *The Herald*. Obtenido de Billion-dollar Medicare fraud ring investigation started in South Carolina; feds say: https://www.heraldonline.com/latest-news/article229013389.html

*NHCAA*. (2018, febrero). Obtenido de https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx.

*NHCAA*. (2018). Obtenido de https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx.

*Passmark Software OSForensics*. (2019, diciembre, 2). Obtenido de https://www.osforensics.com/osforensics.html?gclid=CjwKCAiA5o3vBRBUEiwA9PVzagZD4XBujUxCASmngYGRd-t7tsXkm7p7S3jwgVkO2oT1tmbkUFFOwBoCHPQQAvD_BwE.

Pietragallo, G. (2019). *False Claim Act*. Retrieved from https://www.falseclaimsact.com/common-types-of-fraud/health-care-fraud.

*Rama Judicial*. (2019). Obtenido de http://www.ramajudicial.pr/.

*Rev Cycle Intelligence*. (2018, junio 28). Obtenido de https://revcycleintelligence.com/news/over-600-individuals-charged-in-2018-healthcare-fraud-takedown.

Roberts, L. W. (2014, Noviembre 13). *Physicians Practice*. Retrieved from https://www.physicianspractice.com/audits/six-ways-avoid-rac-audit.

Sofer, N. (2019). *NirLauncher*. Obtenido de https://launcher.nirsoft.net/downloads/index.html.

Sofer, N. (2019). *NirLauncher*. Obtenido de https://launcher.nirsoft.net/downloads/index.html.

Sofer, N. (2019). *Nirsoft*. Obtenido de http://www.nirsoft.net/utils/computer_activity_view.html.

Sofer, N. (2019). *NirLauncher*. Obtenido de https://launcher.nirsoft.net/downloads/index.html.

*WSJ*. (2015, junio 9). Obtenido de https://www.wsj.com/articles/prosecutors-broadly-use-mail-fraud-wire-fraud-statutes-1433870788.