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

EL COLECTIVO APOPHIS SQUAD Y SU DEDICACIÓN AL FRAUDE DIGITAL

ANÁLISIS DE CASO:
UNITED STATES V. TIMOTHY DALTON VAUGHN, AND GEORGE DUKE-COHAN

Número de caso: 2:**19-cr-00071-ODW**

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÓN CON

ESPECIALIDAD EN SEGURIDAD DE INFORMACIÓN E INVESTIGACIÓN DE FRAUDE

PREPARADO POR:

Ángel M. Pérez González

Marzo, 2020

Sirva la presente para certificar que el proyecto de investigación titulado:

EL COLECTIVO APOPHIS SQUAD Y SU DEDICACIÓN AL FRAUDE DIGITAL

Preparado por:

Ángel M. Pérez González

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

Marzo, 2020

Aprobado por:

Dr. Miguel A. Drouyn Marrero, Profesor.

Tabla de Contenidos

Tabla de Figuras

1. Introducción y Trasfondo.

Introducción:

La década del 2010 fue una que vio de manera exagerada un incremento en amenazas y ataques cibernéticos. Con el avance de las computadoras vino de la mano la sofisticación de las personas que las utilizan para hacer daño. Estos ataques cibernéticos crean una preocupación ya que, usualmente atacan entidades que tienen o información confidencial o mucha gente involucrada. En el caso expuesto se hicieron amenazas a aeropuertos, escuelas y entidades corporativas. Esto resulta alarmante ya que, ¿Cómo identificamos que son reales o no estás amenazas? y ¿Cómo podemos sentirnos seguros al ocurrir este tipo de eventualidad?

Es de suma importancia poder analizar situaciones como estas, ya que podría incurrir en daños de cifras altas. Tanto las escuelas, aeropuertos, las entidades e instituciones pueden beneficiarse del análisis de este caso ya que es una incidencia común hoy día. La idea es crear un nivel de conciencia ante esto, sobre todo en las escuelas para manejar el pánico que podría generarse ante la amenaza.

Descripción del caso:

- Número del caso: 2:19-cr-00071-ODW
- Acusados:
    - Timothy Dalton Vaughn
    - George Duke-Cohan
- Víctimas:
    - Escuelas en Estados Unidos y Reino Unido.
    - Hoonigan Industries

- Colombian University Colegio Nueva Granada
- FBI Omaha, Nebraska Field Office
- Los Angeles International Airport
- VeltPVP
- Zonix
- Mineplex
- ProtonMail
- San Francisco International Airport

- Investigadores:

  Ryan White - Fiscal Asistente de Sección de crímenes cibernéticos y de propiedad intelectual

  - Jennie L. Wang
    - Fiscal Asistente de Sección de crímenes cibernéticos.

- Abogados:
  - Julia S. Choe

- Fiscales:
  - Nicola T. Hanna
    - Fiscal de la corte del distrito central de California.

- Juez:
  - Otis D. Wright, II. de la corte del distrito central de California.

Trasfondo:

Los Estados Unidos está acusando a Timothy Dalton Vaughn y a George Duke-Cohan por conspiración y fraude a los Estados Unidos, amenazas a comercio interestatal, daños a computadoras y extorción. Timothy Dalton Vaughn de 21 años y residente de Winston-Salem en Carolina del Norte, se declaró culpable de cargos federales por hacer amenazas de ataques a escuelas en los Estados Unidos y el Reino Unido. Adicional, se declaró culpable de hacer reportes falsos sobre terrorismo e infiltraciones a aviones. Vaughn, tenía varios alias en la internet incluyendo "WantedbyFeds" y "Hacker_R_US" lo cual permitió vincularlo al grupo de hackers colectivo "Apophis Squad". El colectivo "Apophis Squad" se encarga de hacer llamadas telefónicas para extorsionar, enviar correos electrónicos a escuelas con amenazas y hacer ataques "DDoS" a páginas web.

George Duke-Cohan, de 19 años, residente de Hertfordshire en el Reino Unido, hoy día está cumpliendo sentencia en una cárcel en Gran Bretaña por amenazas a aerolíneas. Duke-Cohan tenía alias como "DigitalCrimes" y "7R1D3N7". Fue parte de los ataques de "swatting" y "DDoS" a varias entidades corportativas y escuelas. Duke-Cohan incurrió a hacer amenazas a la oficina del FBI en Omaha, Nebraska e inclusive, diciéndole al operador que atendió la llamada que violaría a su esposa y la mataría, según United States v. Vaughn and Duke-Cohan (2019).

Descripción de los hechos:

Según los documentos del caso USA vs. Timothy Dalton Vaughn, and George Duke-Cohan (2019).

1. En o alrededor de enero del 2018, Vaughn y Duke-Cohan lograron hackear la página www.cng.edu de la "Colombian University Colegio Nueva Granada".

2. Enero 14, 2018, se realizó un ataque “DDoS” a la página www.hoonigan.com dejando la página inoperable por tres días consecutivos.
3. Enero 15, 2018, Vaughn declaró en un chat que había realizado un ataque DDoS a la página www.hoonigan.com
4. Enero 28, 2018, Duke-Cohan hace una llamada a la oficina de Omaha en Nebraska del FBI. Duke-Cohan amenaza con enviar ébola o “anthrax” al lobby de la oficina del FBI y amenazó al operador de la llamada con violar y matar a su esposa. Luego llama para amenazar con una bomba en el aeropuerto de Los Ángeles.
5. Duke-Cohan alardea sobre sus hazañas en *Twitter* el 29 de enero de 2018 y publican una foto de la página www.cng.edu jaqueada con una foto de Adolfo Hitler.
6. Utilizando correos electrónicos parecidos a los de *VeltPVP* enviaron amenazas a escuelas y solicitaban un pago de $5,000 para no llevar a cabo los ataques. Estos hechos ocurrieron entre marzo 16 y 19 de 2018.
7. En marzo 28, 2018 Duke-Cohan vuelve a alardear por *Twitter* sobre los actos ilícitos cometidos.
8. Abril 8 y 9 de 2018, Duke-Cohan y varios miembros del *Apophis Squad* enviaron correos electrónicos a escuelas con amenazas, esta vez utilizando cuentas parecidas a las de *Zonix*.
9. En abril 10 de 2018 Vaughn en un chat *IRC* sostiene una conversación con Duke-Cohan sobre las amenazas. Duke-Cohan ese mismo día fue parte de una entrevista en el chat donde habla sobre sus ataques y los alias que utiliza.
10. El 7 y 8 de mayo de 2018 Duke-Cohan y varios miembros de *Apophis Squad* vuelven a realizar ataques a escuelas en el área central del distrito de California.

11. Duke-Cohan realiza un ataque *DDoS* de una semana a *ProtonMail* el 27 de junio de 2018, luego procede a hablar de los actos en su cuenta de *Twitter*.
12. El 9 de agosto de 2018 Duke-Cohan y su cómplice Vaughn llamaron al departamento de la policía de San Francisco para notificar que había una bomba en el avión UAL 949. La llamada ocasiono el aterrizaje de emergencia del avión.

Acusaciones, cargos y penalidades:

Amenaza de hacer daño a comercio interestatal (18 U.S.C. § 875(c))

Conspiración (18 U.S.C. § 371)

Amenazas interestatales involucrando explosivos (18 U.S.C. § 844(e))

Intencionalmente dañando computadoras (18 U.S.C. § 1030 (a) (5) (A), (c) (4) (B) (i), (c) (4) (A) (i) (I))

Amenazas de ataque a una computadora protegida con intención de extorción (18 U.S.C. § 1030(a) (7) (A), (c) (3) (A))

Ayudando e instigando (18 U.S.C. § 2(a))

Definición de términos:

- *DDoS* (“*Denial-Of-Service-Attack*”)
    - Un ataque que tiene como objetivo inhabilitar un servicio, infraestructura o un servidor. Se hace sobrecargando el sistema para prevenir la entrada de tráfico real.
- *Swatting*
    - Crear una emergencia falsa que incurre al pánico o alteración de la norma.

- Dirección IP
    - Números que identifican de forma lógica que se encarga de establecer comunicación en la mayoría de las redes.
- *FTK*
    - Herramienta (*Software)* utilizado para extraer información de un disco duro.
- *Proton Mail*
    - Un servicio que envía correos electrónicos encriptados.
- *Skype*
    - Una aplicación de telecomunicaciones utilizada para llevar a cabo llamadas de video desde un dispositivo con conexión a internet.
- *Snapchat*
    - Red social para enviar mensajes y videos. La aplicación suele descargarse a dispositivos móvil.
- *Twitter*
    - Red social en el internet para hablar sobre temas recientes y enterarse de lo que pasa en el mundo.

- *IRC (Internet Relay Chat)*
    - Facilita la comunicación entre usuarios en forma de texto.
- *Ransomware*
    - Es un tipo de infección cibernética que se usa para extorsionar a la víctima con su data o limitar el funcionamiento de su dispositivo.
- *Cloudflare*

    - Un servicio de seguridad cibernética que ofrece mitigación contra ataques *DDoS*.

- Cryptodrop
    - Un servicio de seguridad cibernética que ofrece protección contra ataques de *Malware.*
- *ProDiscover Basic*
    - Una herramienta para examinar el contenido de un disco duro y generar reportes de los hallazgos.

2. Revisión de Literatura

Introducción:

El crimen cibernético es uno que constantemente evoluciona, con el paso del tiempo se ha vuelto más común y quienes cometen estos actos ilícitos son aún más sofisticados. Esto, no solamente a ganado la atención de muchos, si no que creó una necesidad de personas dispuestas a proteger y monitorear constantemente sistemas de ataques y vulnerabilidades. "En la actualidad la mitad de los ataques cibernéticos son a negocios pequeños y solamente un 10% son reportados en los Estados Unidos cada año. Hay ataques de *ransomware* cada 14 segundos y se estiman $6 trillones de dólares en daños para el 2021" (Powell, 2019).

Utilizar el término crimen cibernético resulta ambiguo, en nuestro caso, el enfoque es en las amenazas cibernéticas. El propósito de las amenazas cibernéticas es explotar vulnerabilidades en un sistema y de ahí causar el mayor daño posible. Según NIST (n.d.), cualquier circunstancia o evento con el potencial de impactar una operación organizacional, bienes o individuos a través de un sistema de información y sin acceso autorizado. Exponemos a continuación un caso que cumple en su totalidad con la descripción anterior.

Fraudes involucrados:

Los actos ilícitos involucrados en este caso son comunes en la actualidad. Según Powell (2019), "existen alrededor de 2 billones de sitios web", en otras palabras, 2 billones de oportunidades para un jáquer explotar vulnerabilidades como lo hicieron los acusados. Powell señala que un estudio realizado por *Cybint*, encontró que alrededor del 60% de las compañías han sufrido ataques de *DDoS"* como el que sufrió *Hoonigan* a manos de los acusados.

Comparándolo con un crimen en persona, es relativamente fácil mantenerse anónimo en la web con el uso de VPNs para cometer los actos. Bitcoins, aunque generó un sistema económico asombroso también se volvió el enfoque de muchos de estos ataques. En el artículo de *CPO Magazine,* Powell *(2019),* expresa que 76 billones de dólares en Bitcoin son adquiridos de manera ilegal. En nuestro caso se utilizó la extorción a varias entidades, incluyendo aeropuertos en donde la amenaza requería pagos en Bitcoins para no llevarlo a cabo.

Según informa Newman (2018), *Github,* tan reciente como febrero del 2018, sufrió el ataque más grande documentado en la historia de DDoS. El mismo fue de 1.3 Tbps, y mantuvo a *Github* fuera de servicio de 15 a 20 minutos. Estos ataques DDoS forman parte estratégica de los planes de extorción implementados por los jáquer para obtener criptomonedas como las de Bitcoin. Una nueva modalidad es, según Lindsey (2019), comenzar con *ransomware,* el cual una vez infectado el sistema se combina con ataques DDoS que sólo se acabarán si se recibe una cantidad determinada de criptomonedas.

Un ataque *DDoS* (*Distributed Denial of Service* por sus siglas en inglés) atenta interrumpir los servicios de una página web dirigiendo una cantidad masiva de tráfico hacia ella. Los atacantes explotan las vulnerabilidades creando una red de computadoras virtuales que estarán constantemente entrando al sitio web. Esto hace que el tráfico sobrepase la cantidad límite del servidor e interrumpa el servicio, Petters (2019).

Leyes aplicables:

Conspirar a estafar a los Estados Unidos – La 18 U.S.C. § 371, es cuando dos personas o más conspiran a cometer una ofensa o estafa contra los Estados Unidos o alguna de sus agencias. La ofensa tiene una penalidad máxima de hasta 5 años de cárcel. (Justice.gov)

Amenazas al comercio interestatal – La 18 U.S.C. § 875 (c): estipula que cualquier intento de extorción por una persona amerita cargos y/o hasta un total de 20 años de cárcel. (law.Cornell.edu)

Amenazas interestatales involucrando explosivos – 18 U.S.C. § 844 (e): Utilizar correos electrónicos, llamadas o cualquier instrumento para afectar el comercio interestatal a través de amenazas o falsa información maliciosa. La sentencia incluye una penalidad y/o hasta un total de 10 años de cárcel. (law.Cornell.edu - B)

Daños intencionales a una computadora a través de una conexión – 18 U.S.C. § 1030 (a) (5) (A), (c) (4) (B) (i), (c) (4) (A) (i) (I): Transmisión de un código, programa o información para causar daños de manera intencional. Las penalidades podrían sumar a un total de 35 años de cárcel. (law.Cornell.edu - C)

Amenazas interestatales a computadoras protegidas con intención de extorción – 18 U.S.C. § 1030(a) (7) (A), (c) (3) (A): Lograr acceso a una computadora sin autorización para hacer daños. Causar daños a una computadora protegida y obtener información de esta. La sentencia incluye penalidades que podrían sumar a 30 años de cárcel. (law.Cornell.edu - D)

Ayudar e instigar - 18 U.S.C. § 2(a): Cometer una ofensa contra los Estados Unidos, sea directa o indirectamente. Penalidades pueden sumar hasta 3 años de cárcel. (law.Cornell.edu – E)

Casos Relacionados:

United States v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, Omid Ghaffarina, Sina Keissar y Nader Saedi (2016).

En este caso, 7 iraníes fueron acusados por atacar bancos de los Estados Unidos. Los acusados son miembros del gobierno iraní e incurrieron a entrar a computadoras privadas con data confidencial e interrumpir operaciones. Adicional, lanzaron varios ataques DDoS para interrumpir el servicio de 46 instituciones financieras dejando cientos de miles de clientes sin acceso a sus cuentas de banco, Zapotosky, Nakashima (2016). Es similar en la metodología utilizada para interrumpir servicios con los ataques DDoS al igual que se hizo en el caso que está siendo presentado.

United States of America v. Zhu Hua y Zhang Shilong (2018).

Ambos se encuentran acusados de robar información personal y propietaria de compañías mundiales, el FBI y el departamento de justicia. Zhu Hua y Zhang Shilong son parte del grupo *Advanced Persistent Threat 10* el cual está vinculado a el gobierno de China. Según el FBI (2018), sobre 45 organizaciones fueron afectadas, se robaron cientos gigabytes de información confidencial y hasta de la NASA. Es similar al caso que estoy investigando en que ambos son colectivos que se dedican a realizar ataques y que en ambas ocasiones el FBI fue víctima de los ataques.

United States of America v. Wu Zhiyong, Wang Qian, Xu Ke y Liu Lei (2019).

Cuatro miembros del ejército de la liberación de personas en China jaquearon la agencia de reportes de crédito *Equifax*. Tras infiltrar la base de datos lograron robar información personal de aproximadamente 145 millones de americanos. Hay nueve cargos incluyendo robo de

información privada y sensitiva, entrar sin autorización a una red privada y jaquear con intención de difundir la data. El ataqué afecto a 34 servidores en 20 lugares diferentes. La similitud con el caso que presento es en la explotación de vulnerabilidades para lograr acceso a información confidencial.

Herramientas de investigación:

a. *Cloudflare*
    a. Añade seguridad a las capas 3 y 4 lo cual previene un ataque DDoS antes que llegue al servidor, según la página web de Cloudflare (s.f.).
b. *Cryptodrop*
    a. Es una herramienta que puede hacer un análisis del sistema basándose en cómo era antes de estar comprometido. Al conseguir *ransomware* suspende las posibles amenazas y permite recuperar la data encriptada, (Rubenking, 2018).
c. *ProDiscover Basic*
    a. Es una herramienta que permite localizar data en el disco de una computadora y a la misma vez proteger evidencia, (Chandel, 2015).

3. Simulación Experimental del Esquema de Fraude

Descripción narrativa:

Timothy Dalton Vaughn y George Duke-Cohan creaban correos electrónicos los cuales contenían amenazas con bombas y armas de fuego. Los mismos serían enviados a cientos de escuelas en los distritos de Estados Unidos y Los Reinos Unidos. A través de *spoofing* hacían que los correos electrónicos parecieran reales y como si fueran enviados por entidades como *VeltPVP, Zonix* o haciéndose pasar como agencias gubernamentales de Londres. Junto a otros miembros del *Apophis Squad*, Vaughn y Duke-Cohan lanzaban ataques de *DDoS* a sitios web para extorsionar a sus víctimas.

Los eventos en secuencia comenzaron en enero de 2018 cuando Vaughn y Duke-Cohan se pusieron de acuerdo para atacar la página web de la *Colombian University,* Colegio Nueva Granada, www.cng.edu. Luego de ser exitosos en tumbar la página previamente mencionada, pasaron a un un ataque *DDoS* a la página web www.hoonigan.com el cual deshabilitó la misma por 3 días. Tras ese ataque el 14 de enero de 2018, Vaughn entró el 15 de enero de 2018 a un chat en *IRC* a hablar sobre el ataque a *www.hoonigan.com*. En enero 28 de 2018 Duke-Cohan hace una llamada a la oficina del FBI en Omaha, Nebraska y hace una amenaza de ébola o ántrax a la misma. El operador que atendió la llamada, al no responder fue amenazado con la violación y asesinato de su esposa.

Varias horas después del evento anteriormente mencionado Duke-Cohan vuelve a llamar a la oficina del FBI en Omaha amenazando con bombas en el Aeropuerto Internacional de Los Ángeles. Utilizando el alias de “7R1D3N7”, Duke-Cohan puso una captura de pantalla en *Twitter* de la página *www.cng.edu* con una foto de Adolf Hitler con el mensaje escrito de

"jaqueada por el *Apophis Squad"*. Luego el 29 de enero de 2018 volvieron a publicar por *twitter* sobre el ataque a www.cng.edu. 30 de enero de 2018 Duke-Cohan estaba *Catfishing* a una persona de Florida y junto a Vaughn hicieron la llamada a la oficina de Omaha del FBI. Ambos procedieron a decir que la llamada y la acción fue de parte del *Apophis Squad* para coger crédito.

Los eventos siguieron intensificando y para el 16 y 19 de marzo de 2018, ambos enviaron correos electrónicos a escuelas amenazando con bombardeos y haciéndose pasar por *VeltPVP*. El método de extorción fue pidiendo $5,000.00 dólares americanos o si no, un estudiante detonaría una bomba en 3 horas. Luego el 19 de marzo, procedieron a dar gracias a todos por participar del evento por *Twitter* y firmaron con un alias, Pl3x3lt. Para el 28 de marzo de 2018, amenazaron a las escuelas con matar a los estudiantes con un carro y de evacuar a los estudiantes iban a disparar. Lograron cerrar la escuela ese día y pusieron un mensaje en *Twitter* celebrando el acto.

Para abril 8, de 2018 Duke-Cohan recibe un listado de escuelas de Vaughn y pasaron a advertir que atacarían las escuelas de los Reinos Unidos cuando se acabaran las vacaciones. Ese día pasaron a amenazar por *Twitter* a la compañía *ZonixUS* y dijeron que harían ataques de *Doxing & Swatting.* Entonces enviaron correos electrónicos a los cuales de contestar le llegarían a *Zonix* amenazando varias escuelas con enviar un estudiante con 3 bombas y una pistola de calibre .22. Cerca del 10 de abril de 2018, Vaughn creó un usuario en *IRC* para comunicarse con Duke-Cohan y otros conspiradores.

Desde el 10 de abril hasta el 15 de abril de 2018 continuaron con el ciclo de amenazar escuelas, hacer llamadas y mencionar por *Twitter* los eventos en los que formaban parte. Se mantuvieron un poco menos activos hasta el 5 de mayo de 2018 donde comenzaron a pedir solicitudes por *Twitter* de estudiantes para cerrar escuelas. El 7 de mayo de 2018 pasaron a cumplir con las solicitudes enviando correos electrónicos a las escuelas haciéndose pasar por el

director general de la NCA de los Reinos Unidos o el oficial ejecutivo de *Marz Media*. Habría bombas colocadas en los transportes públicos de estudiantes de no recibir $5,000.00 dólares americanos al correo electrónico *cbrady350@gmail.com*.

Para el 26 de junio de 2018 repitieron el acto, esta vez a diferentes escuelas y amenazando con lanza misiles. El 27 de junio del mismo año, hicieron un ataque masivo de *DDoS* a *Protonmail* por una semana. Por los próximos días documentarían a través de la cuenta @apophissquadv2 en *Twitter* los sucesos del ataque contra *Protonmail.* El 9 de agosto 2018 Duke-Cohan hace un comentario por *Twitter* en el que estipula que a Vaughn la policía trató de entrar a la casa, pero no tenían querella.

Finalmente, el mismo día, hicieron una llamada al aeropuerto de San Francisco diciendo que un pasajero del vuelo tenía cuatro personas a bordo con bombas. Esto causó que el avión se pusiera en un área en cuarentena al aterrizar. El mismo se mantuvo estacionado por horas hasta que la seguridad lo verificara. Pasaron a escribir en *Twitter* que el avión UAL 949 no pudo salir ese día.

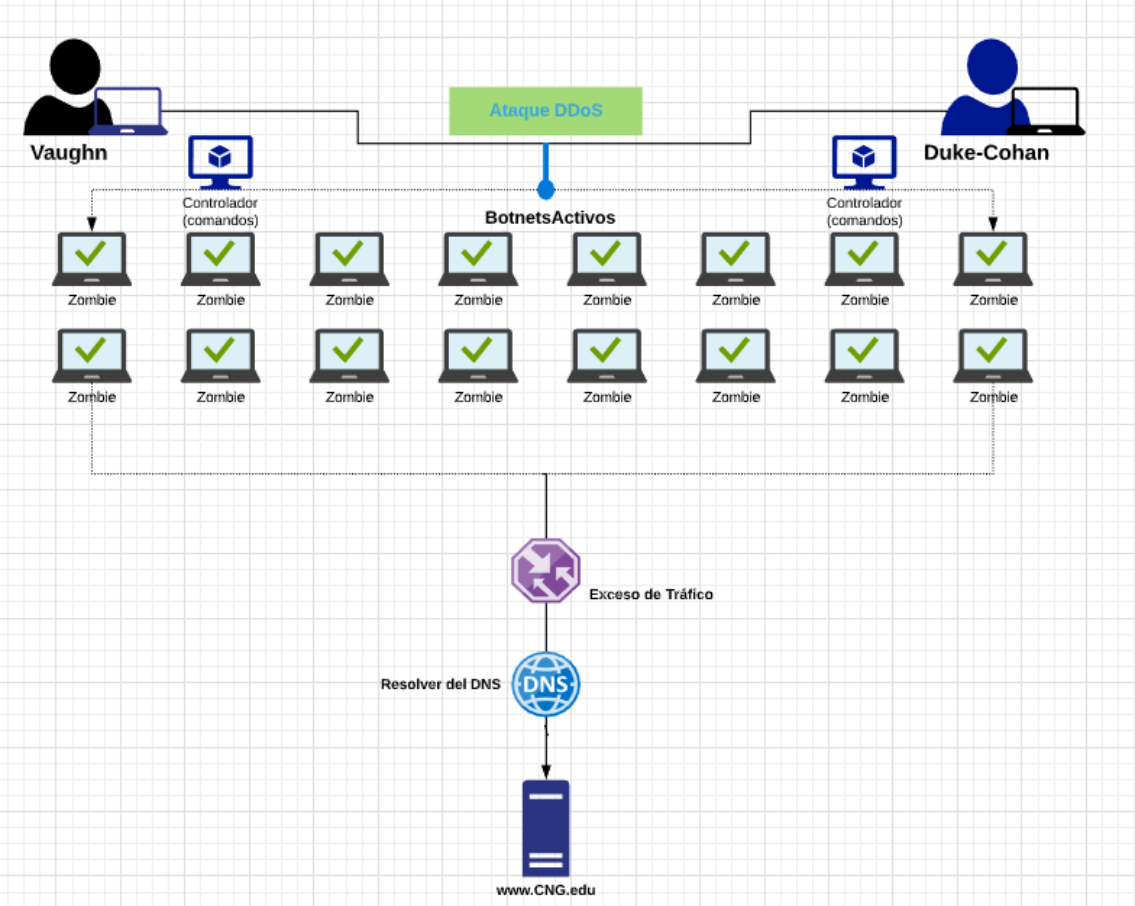


Figura 1 - Recreación de ataque DDoS

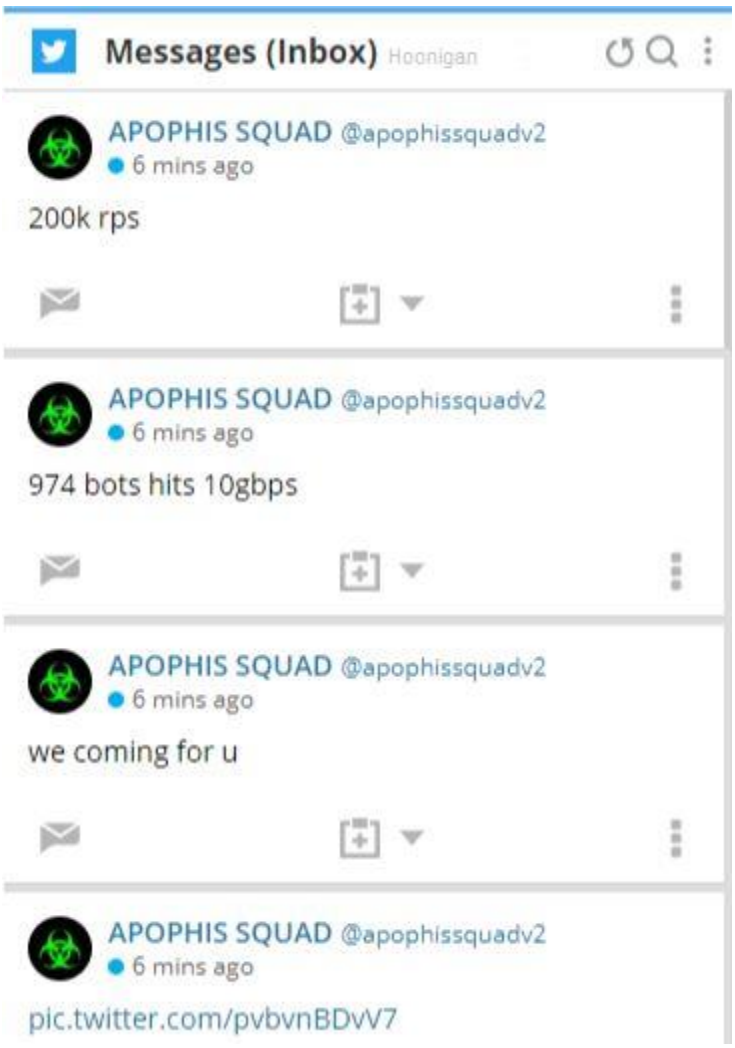


Figura 2– Mensajes de extorsión a *Hoonigan*.

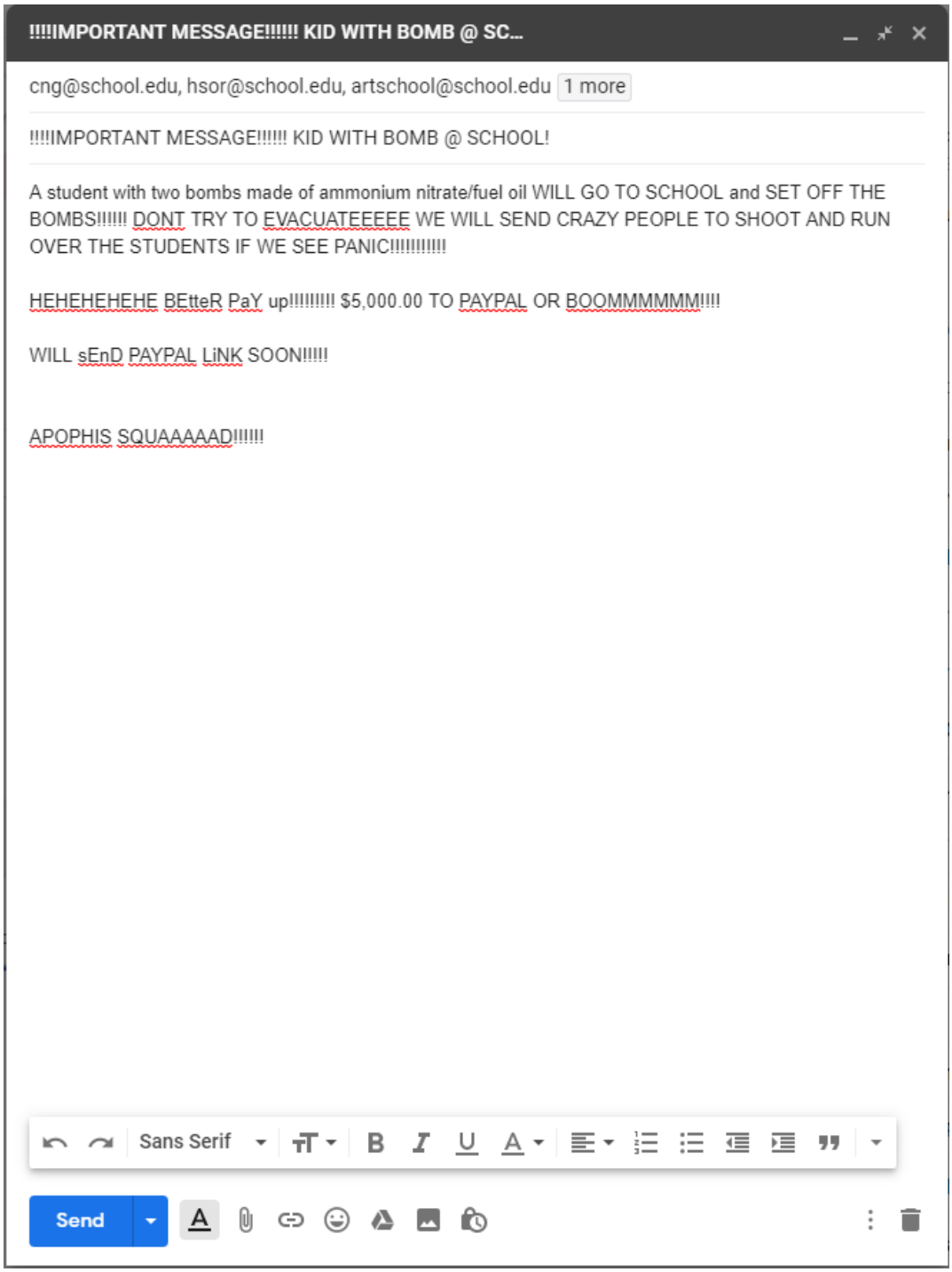


Figura 3 – Amenaza a diferentes escuelas extorsionando por dinero.

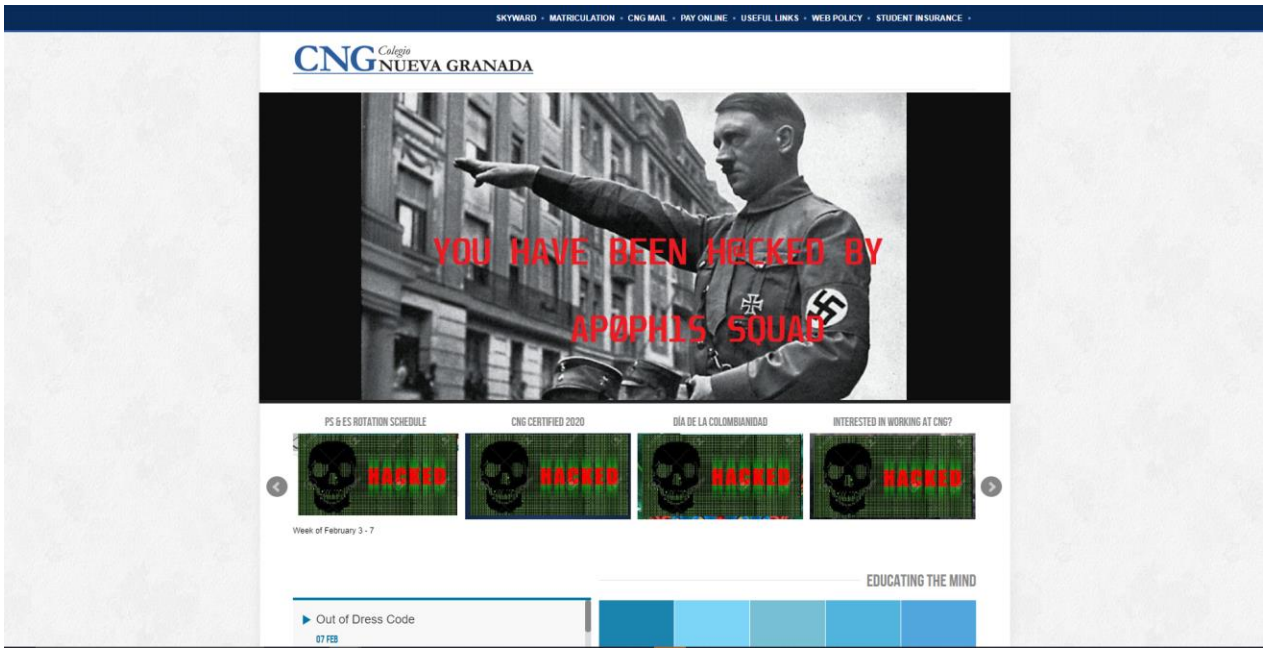


Figura 4 – Recreación de mensaje enviado en Twitter cuando jaquearon www.cng.edu.

4. Informe del Caso

Resumen Ejecutivo:

Ryan White, asistente fiscal de la división nacional de seguridad de la sección de crímenes cibernéticos y propiedad intelectual hizo entrega a QNTM Forensix de un dispositivo móvil y un disco duro portátil a ser analizados. El celular y el disco duro portátil fueron incautados durante un allanamiento realizado por el FBI en *Winston-Salem North Carolina*. Según se indica, estas piezas de evidencia corresponded a una investigación relacionada a unos ataques cibernéticos y amenazas terroristas.

De la examinación realizada al celular se identificaron conversaciones que comprometen al autor del crimen con su cómplice y la planificación detrás de los crímenes. Se incluye archivos, bitácoras de conversaciones y grabado en la memoria los correos electrónicos asociados con las cuentas de *Twitter, Town of Salem* y los *IRC chat rooms*. En el disco duro portátil se encontró instalado los juegos que frecuentaban para reclutar y hacer amenazas.

Tras completada la examinación del celular y el disco duro portátil, se devolvieron a Ryan White. Junto a las piezas de evidencia, se entregaron copias digitales de los hallazgos y el informe del análisis.

Objetivo:

Se solicitó los servicios de QNTM Forensix por la fiscalía de la Corte del Distrito Central de California para la ejecución de una examinación forense al contenido del dispositivo móvil y el disco duro portátil incautados por el FBI como parte de la investigación. El motivo detrás es identificar evidencia posiblemente vincular los crímenes cometidos de atentados terroristas y ataques *DDoS* con Timothy Dalton Vaughn y George Duke-Cohan.

Alcance del trabajo:

El 9 de diciembre de 2019, el asistente fiscal de la división nacional de seguridad de la sección de crímenes cibernéticos y propiedad intelectual Ryan White hizo entrega de lo incautado al examinador forense Ángel M. Pérez. Dentro de los artículos, un disco duro portátil marca San Disk, identificado como *Item* No. 2019-EV-00 (Figura 5) y un celular Samsung Note 8 identificado como *Item* No. 2019-EV-01 (Figura 6). Los dispositivos fueron extraídos de *Winston Salem* en *North Carolina* por el FBI.

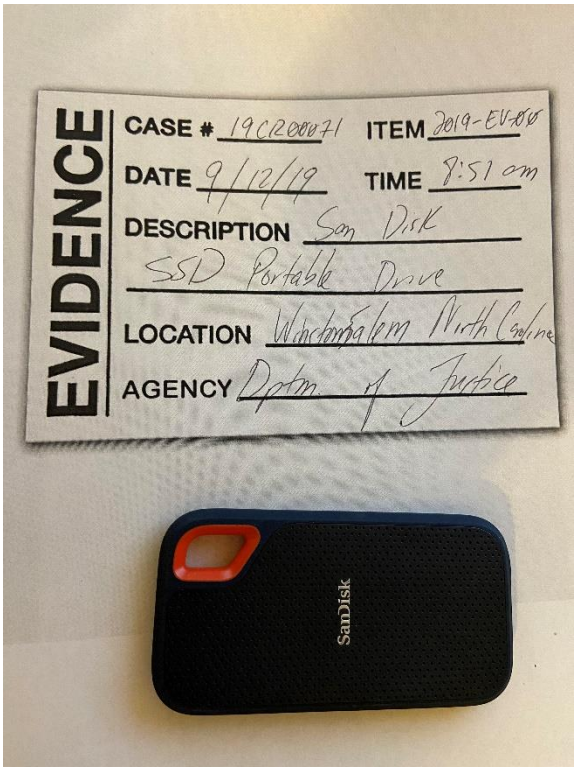


Figura 5 - Disco duro portátil marca SanDisk junto identificación de evidencia.

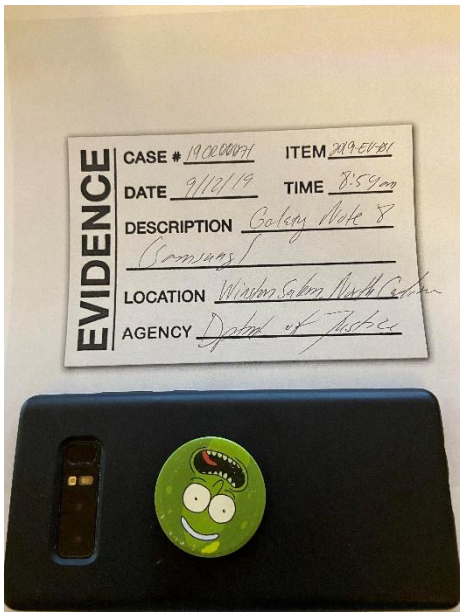


Figura 6 – Dispositivo móvil junto a identificación de evidencia.

La entrega se hizo para buscar información y extraer la mayor evidencia posible del disco duro y del dispositivo móvil. Conforme a los estándares de la investigación forense digital, esta tarea se ejecuta utilizando las herramientas Forensic Toolkit (FTK), MPE+ Nfield y FTK Imager.

Datos del caso:

1. Número de caso: 19-CR-00071
2. Investigador: Ángel M. Pérez
3. Cliente: Departamento de Justicia de Estados Unidos
4. Representante del cliente: Ryan White, asistente fiscal de la división nacional de seguridad de la sección de crímenes cibernéticos y propiedad intelectual

Descripción de los dispositivos utilizados:

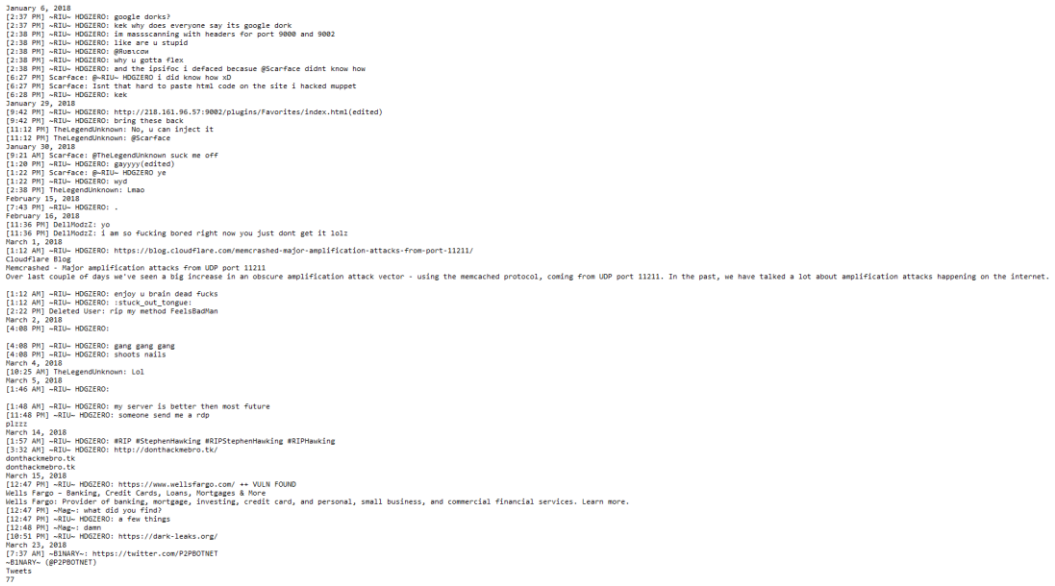
A continuación, detallados los dispositivos utilizados en el proceso de examinación forense:

1. Computadora Dell Inspiron 7000, con procesador Intel Core i5 de 2.5 Ghzm 8GB de RAM, sistema operativo Windows 10. Contiene instalados todos los programas que fueron utilizados en el proceso de examinación forense.
2. Disco duro portátil San Disk de 256 GB de capacidad, *Item* No. 2019-EV-00 (Figura 1)
3. Cable convertidor de USB a Tipo-C
4. Samsung Galaxy Note 8, *Item* No. 2019-EV-01 (Figura 2)

Resumen de hallazgos:

A continuación, se presentan los hallazgos identificados durante la examinación forense del dispositivo móvil (*Item* No. 2019-EV-01) entregado por Ryan White, asistente fiscal de la división nacional de seguridad de la sección de crímenes cibernéticos y propiedad intelectual.

1. Log encontrado de una conversación que estaba sosteniendo con su alias HDGZERO (Figura 7, 8 y 9). Está haciendo referencia a su cuenta de twitter *Wantedbyfeds* y mencionando a *ApophisSquad* vinculándose a ellos y los actos de *DDoS* cometidos.



```
January 6, 2018
[2:37 PM] ~RIU~ HDGZERO: google dorks?
[2:37 PM] ~RIU~ HDGZERO: kek why does everyone say its google dork
[2:38 PM] ~RIU~ HDGZERO: im massscanning with headers for port 9000 and 9002
[2:38 PM] ~RIU~ HDGZERO: like are u stupid
[2:38 PM] ~RIU~ HDGZERO: @Rumcox
[2:38 PM] ~RIU~ HDGZERO: why u gotta flex
[2:38 PM] ~RIU~ HDGZERO: and the ipsifoc i defaced becasue @Scarface didnt know how
[6:27 PM] Scarface: @~RIU~ HDGZERO i did know how xD
[6:27 PM] Scarface: isnt that hard to paste html code on the site i hacked muppet
[6:28 PM] ~RIU~ HDGZERO: kek
January 29, 2018
[9:42 PM] ~RIU~ HDGZERO: http://218.161.96.57:9002/plugins/Favorites/index.html(edited)
[9:42 PM] ~RIU~ HDGZERO: bring these back
[11:12 PM] TheLegendUnknown: No, u can inject it
[11:12 PM] TheLegendUnknown: @Scarface
January 30, 2018
[9:21 AM] Scarface: @TheLegendUnknown suck me off
[1:20 PM] ~RIU~ HDGZERO: gayyyy(edited)
[1:22 PM] Scarface: @~RIU~ HDGZERO ye
[1:22 PM] ~RIU~ HDGZERO: wyd
[2:38 PM] TheLegendUnknown: Lmao
February 15, 2018
[7:43 PM] ~RIU~ HDGZERO: .
February 16, 2018
[11:36 PM] DellModzI: yo
[11:36 PM] DellModzI: i am so fucking bored right now you just dont get it lolz
March 1, 2018
[1:12 AM] ~RIU~ HDGZERO: https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/
Cloudflare Blog
Memcrashed - Major amplification attacks from UDP port 11211
Over last couple of days we've seen a big increase in an obscure amplification attack vector - using the memcached protocol, coming from UDP port 11211. In the past, we have talked a lot about amplification attacks happening on the internet.

[1:12 AM] ~RIU~ HDGZERO: enjoy u brain dead fucks
[1:12 AM] ~RIU~ HDGZERO: :stuck_out_tongue:
[2:22 PM] Deleted User: rip my method FeelsBadMan
March 2, 2018
[4:08 PM] ~RIU~ HDGZERO:

[4:08 PM] ~RIU~ HDGZERO: gang gang gang
[4:08 PM] ~RIU~ HDGZERO: shoots nails
March 4, 2018
[10:25 AM] TheLegendUnknown: Lol
March 5, 2018
[1:46 AM] ~RIU~ HDGZERO:

[1:48 AM] ~RIU~ HDGZERO: my server is better then most future
[11:48 PM] ~RIU~ HDGZERO: someone send me a rdp
plzzz
March 14, 2018
[1:57 AM] ~RIU~ HDGZERO: #RIP #StephenHawking #RIPStephenHawking #RIPHawking
[3:32 AM] ~RIU~ HDGZERO: http://donthackmebro.tk/
donthackmebro.tk
donthackmebro.tk
March 15, 2018
[12:47 PM] ~RIU~ HDGZERO: https://www.wellsfargo.com/ ++ VULN FOUND
Wells Fargo - Banking, Credit Cards, Loans, Mortgages & More
Wells Fargo: Provider of banking, mortgage, investing, credit card, and personal, small business, and commercial financial services. Learn more.
[12:47 PM] ~Mag~: what did you find?
[12:47 PM] ~RIU~ HDGZERO: a few things
[12:48 PM] ~Mag~: damn
[10:51 PM] ~RIU~ HDGZERO: https://dark-leaks.org/
March 23, 2018
[7:37 AM] ~B1NARY~: https://twitter.com/P2PBOTNET
~B1NARY~ (@P2PBOTNET)
Tweets
??
```

Figura 7 - Log conseguido en el dispositivo móvil.

```
Twitter
March 25, 2018
[4:50 PM] Lampshademodz: 76.115.212.229 here you go an ip that is online but cant be pinged I ddosed him a few times have fun with it
March 26, 2018
[7:15 PM] Lampshademodz: @~RIU~ HDGZERO ^
[7:16 PM] ArcticNetwork: what you need Lamps?
[7:16 PM] ArcticNetwork: Zeros internet was limited but ill txt him
[7:17 PM] ~RIU~ HDGZERO: Zeros internet is indeed limited but hes currently taped into a fiber line that runs near his house and mac spoofing to the use it as i was the neighbors
[7:18 PM] ~RIU~ HDGZERO: If i*
[7:22 PM] ~RIU~ HDGZERO: also hacked a ems trucks wifi cuz why not
[7:29 PM] Lampshademodz: Wtf zero
[7:29 PM] Lampshademodz: XD
March 27, 2018
[11:09 AM] alva: tbh
[11:09 AM] alva: magician
April 6, 2018
[6:18 AM] ~RIU~ HDGZERO: https://isitupordown.net/health.gov
Oh no! health.gov is down. | isitupordown.net
The availability results for health.gov. | isitupordown.net
[6:18 AM] ~RIU~ HDGZERO: https://check-host.net/check-report/70d5c5akc4c
Ping server, ping website: Check host - online website monitoring
Ping server and website online: website monitoring with usefull tools, Check IP, Check website
[6:18 AM] ~RIU~ HDGZERO: https://check-host.net/check-report/70d5c6dk5fe
Check website perfomance and response: Check host - online website...
Website checking for speed and availability with servers around the world: website monitoring with usefull tools, Check IP, Check website
[6:18 AM] ~RIU~ HDGZERO: https://twitter.com/wantedbyfeds/status/982196488334790656

                         WantedbyFeds (@wantedbyfeds)
https://t.co/ZHxr2koRoV
https://t.co/iu4p3ywMSq
#TangoDown
@ApophisSquad
Only Temporary
~ Wanted

Twitter
[6:19 AM] ~RIU~ HDGZERO: https://twitter.com/wantedbyfeds/status/982200290727247875

                         WantedbyFeds (@wantedbyfeds)
https://t.co/VTskUl9TA3
https://t.co/zgCLOTY6kR
#TangoDown
@ApophisSquad @SkyNews
~ Wanted

Twitter
[6:19 AM] ~RIU~ HDGZERO: https://twitter.com/wantedbyfeds/status/982156973167730689

                         WantedbyFeds (@wantedbyfeds)
@UVA Hows your website, OOPS
https://t.co/rVCU2GYhqV
#TangoDown
https://t.co/M1PM84GZGG
@FBI @ApophisSquad
~ Wanted

Twitter
[6:19 AM] alva: good morning hun
[6:19 AM] ~RIU~ HDGZERO: 'https://twitter.com/wantedbyfeds/status/982063203864731649

                         WantedbyFeds (@wantedbyfeds)
HMM
@cbrady350
Would this happen 2 be you?
https://t.co/gINHAubeBs
#TangoDown
https://t.co/sMvUNPFjTE
@ApophisSquad
```

Figura 8 - Continuación del log

```
#TangoDown
https://t.co/M1PM84GZGG
@FBI @ApophisSquad
~ Wanted

Twitter
[6:19 AM] alva: good morning hun
[6:19 AM] ~RIU~ HDGZERO: 'https://twitter.com/wantedbyfeds/status/982063203864731649

                              WantedbyFeds (@wantedbyfeds)
HMM
@cbrady350
Would this happen 2 be you?
https://t.co/gINHAubeBs
#TangoDown
https://t.co/sMvUNPFjTE
@ApophisSquad

Twitter
[6:19 AM] ~RIU~ HDGZERO: morning :heart:
[6:20 AM] alva: hehe
[6:20 AM] ~RIU~ HDGZERO: https://twitter.com/wantedbyfeds/status/981231657071054848

                              WantedbyFeds (@wantedbyfeds)
Oh no! https://t.co/UehLenM47c is down. https://t.co/LyfRbLl5Wb #isitupordown
Only Temp Getting shit ready for them
~ Wanted

Twitter
[6:20 AM] ~RIU~ HDGZERO: https://twitter.com/wantedbyfeds/status/981005721029537792

                              WantedbyFeds (@wantedbyfeds)
https://t.co/HMzvhWeJHg
https://t.co/jRUp0NwYQu
#TangoDown
@ApophisSquad

Twitter
[6:20 AM] ~RIU~ HDGZERO: https://twitter.com/wantedbyfeds/status/980943867959791616

                              WantedbyFeds (@wantedbyfeds)
#TANGODOWN
https://t.co/O5MYryPpUj
https://t.co/Qqm7cidA59
@ApophisSquad

Twitter
[6:20 AM] ~RIU~ HDGZERO: https://twitter.com/wantedbyfeds/status/969646257206685696

                              WantedbyFeds (@wantedbyfeds)
Oh no! https://t.co/1x45zB1n5T is down. https://t.co/UlvTOV19Lu #isitupordown

#OFFLINE GET REKTED JUST CUZ I CAN!

Twitter
[6:21 AM] ~RIU~ HDGZERO: https://twitter.com/wantedbyfeds/status/955262773742616577(edited)

                              WantedbyFeds (@wantedbyfeds)
https://t.co/AZxo2cuYA0
#OFFLINE
@outagereportsa @outagereportca
report on that haha

meme @120FPS

Twitter
[6:21 AM] ~RIU~ HDGZERO: https://twitter.com/wantedbyfeds/status/955201598933864449
```

Figura 9 - Continuación del log.

2. Se encuentran *screenshots* tomados de los *tweets* hechos por la cuenta de *ApophisSquad* mencionando los ataques de *DDoS* y señalando otros usuarios (Figura 10, 11 y 12).

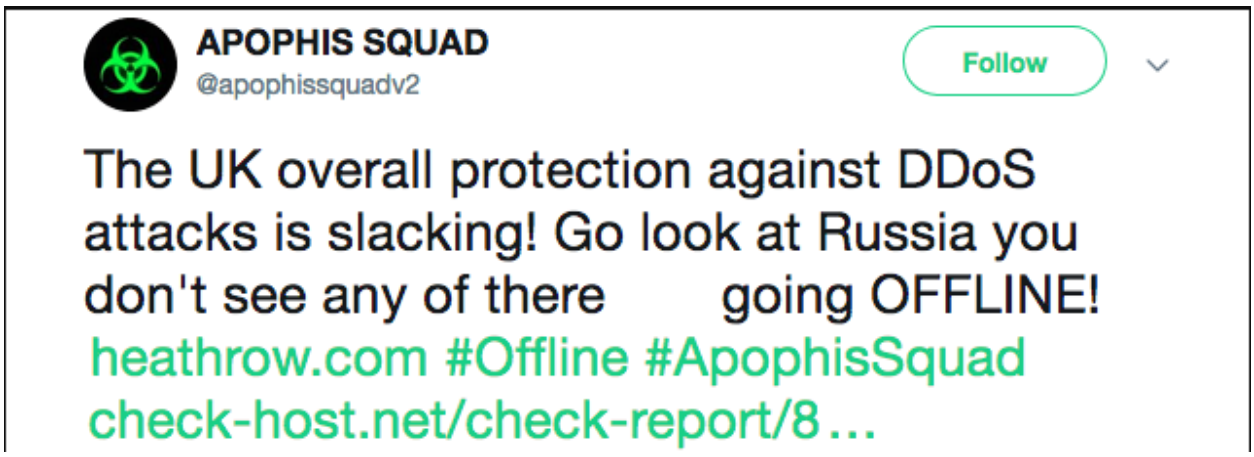


Figura 10 - *ApophisSquad* hablando sobre la pobre protección de los Reinos Unidos contra ataques DDoS

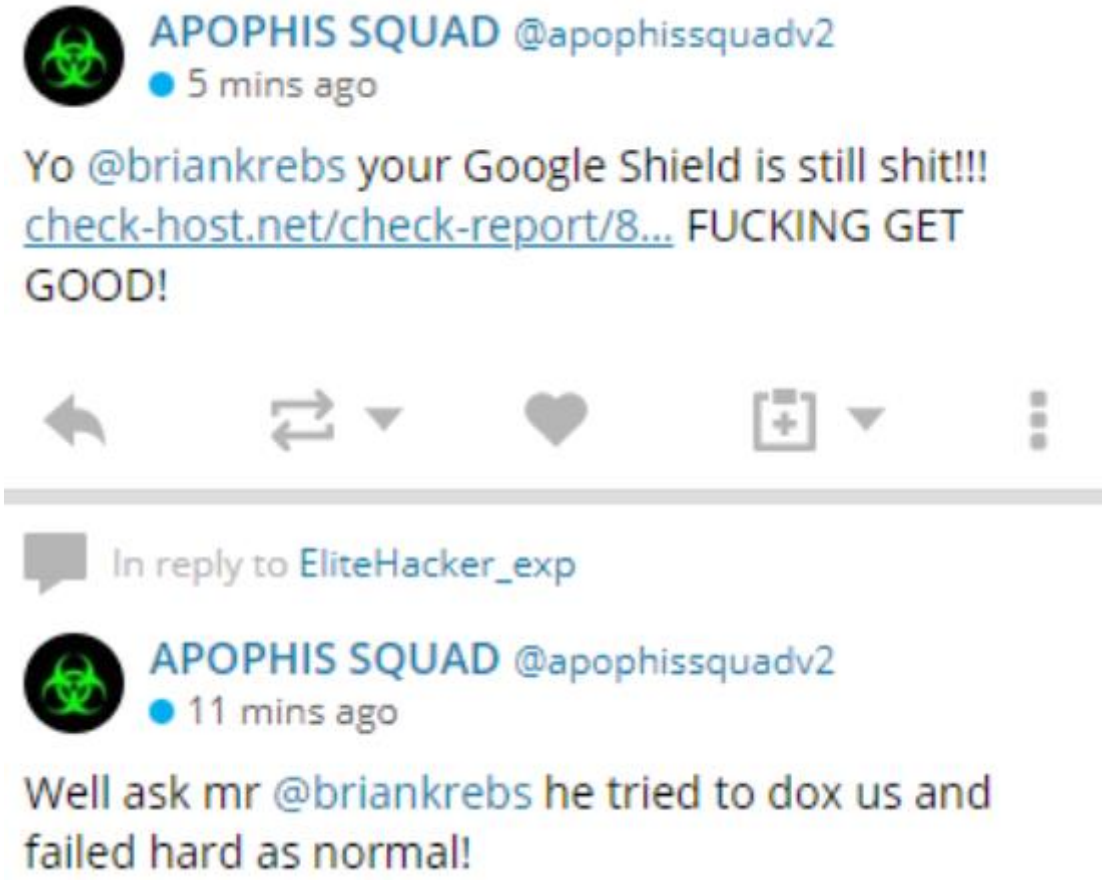


Figura 11 - Relatan ataque a Brian Krebs.

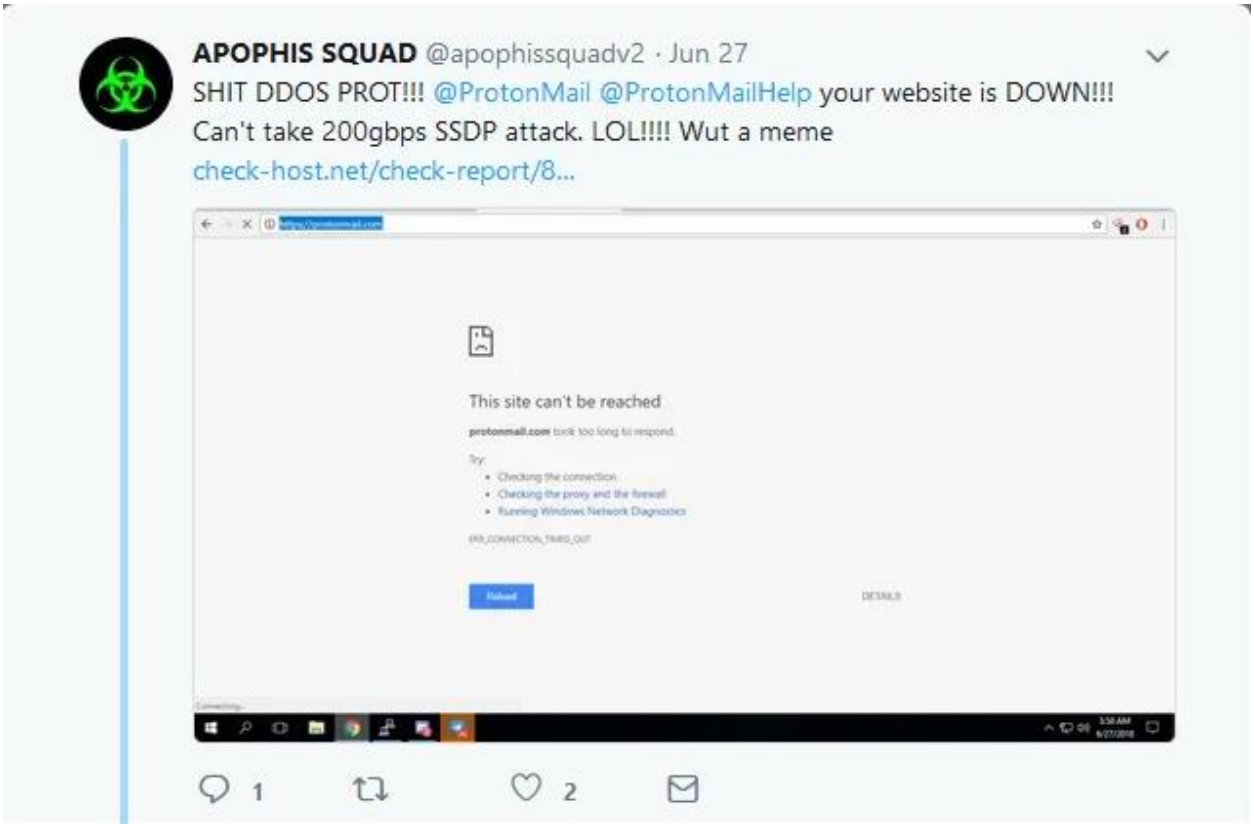


Figura 12 - Hablan sobre la pobre protección contra ataques *DDoS* que tiene *Proton Mail.*

A continuación, se presentan los hallazgos identificados durante la examinación forense del disco duro portátil (*Item* No. 2019-EV-00) entregado por Ryan White, asistente fiscal de la división nacional de seguridad de la sección de crímenes cibernéticos y propiedad intelectual.

1. Un archivo en formato texto simple conteniendo todos las cuentas, contraseñas y correos electrónicos utilizados en los eventos ilícitos (figura 13, 14 y 15).

```
Ran by: X_X#4746
Reason Doxed: fucking retard, i wouldnt care for reuploading the doxes i made on them. i am also currently doing doxes for free contact me
for more
information.

Name: Timothy Dalton Vaughn
Age: 20
Location: Winston-Salem, North Carolina
Current Address:
Current Number:
Alias(s)/Handle(s): ["Hacker_r_us", "wantedbyfeds", "HDGZERO", "Zero", "Xavier Farbell", "Timtim7719"]
Password(s): ["tt395151", "dr.pepper", "stopman1"]
Email(s): ["xavierfarbel@gmail.com", "hdgzero@gmail.com", "hdgzero@outlook.com", "hacker1284@yahoo.com", "hdgzero77@outlook.com", "hdgze-
ro7777@outlook.com", "hdgzero77777@outlook.com", "pleasebabydontleaveme@outlook.com", "fbisuspendedme@outlook.com", "t3951tim@free.fr",
"rootking77@gmail.com", "tinytimtim88@gmail.com", "tnationgaming@gmail.com", "tnationgaming@hotmail.com", "timothy.vaughn79@gmail.com", "tim-
othy.vaughn79@gmail.com", "timothyvaughn88@gmail.com", "t3951tim@gmail.com"]

Location History: ["2403 Summer Place Drive South West,Supply,28462,NC", "329 Steller Road,Jacksonville,28540,NC", "2403 Summer Place Drive
South West,Supply,28462,NC"]
Contact Information: ["(714) 417-1207", "(910) 455-0325", "(910) 842-7606", "(•••) •••-••66", "(206) 479-2209", "(206) 479-1209"]
Winston-Salem, North Carolina
Schooling: East Forsyth High School
School Address: 2500 W Mountain St, Kernersville, NC 27284
School Number: (336) 727-2265
Article 1: https://www.justice.gov/usao-cdca/pr/members-hacker-collective-face-federal-charges-attacking-computer-systems-emailing-mass
Article 2: https://www.zdnet.com/article/fbi-arrests-second-apophis-squad-hacker-in-the-us/

Backup Emails:
Email:"tnationgaming@gmail.com" || Backup Email:"rootking77@gmail.com"      || Last Available Password:"tt395151"
Email:"xavierfarbel@gmail.com"  || Backup Email:"xav••••••••••@gmail.com" || Last Available Password:"tt395151"
Email:"t3951tim@gmail.com"      || Backup Email:"tim•••••••@hotmail.com"    || Last Available Password:"tt395151"

Past IP Logs:
47.38.93.254    47-38-93-254.dhcp.unas.mo.charter.com   United States flag United States    NC  Lenoir              Charter Communications
AS20115 (Latest)
152.26.68.39                                            United States flag United States    NC  Durham             MCNC    AS19718
98.74.159.27    adsl-98-74-159-27.ilm.bellsouth.net     United States flag United States    NC  Leland              BellSouth.net Inc.
AS6389
76.6.15.142     nc-76-6-15-142.dhcp.embarqhsd.net       United States flag United States    NC  Mount Gilead        Qwest Communications Com-
pany, LLC   AS209
208.54.5.216    md80536d0.tmodns.net                    United States flag United States    CA  Sacramento          T-Mobile USA, Inc.
AS21928

Social Media:
Snapchat: xfarbel
```

Figura 13 - Correos electrónicos, IPs, alias.

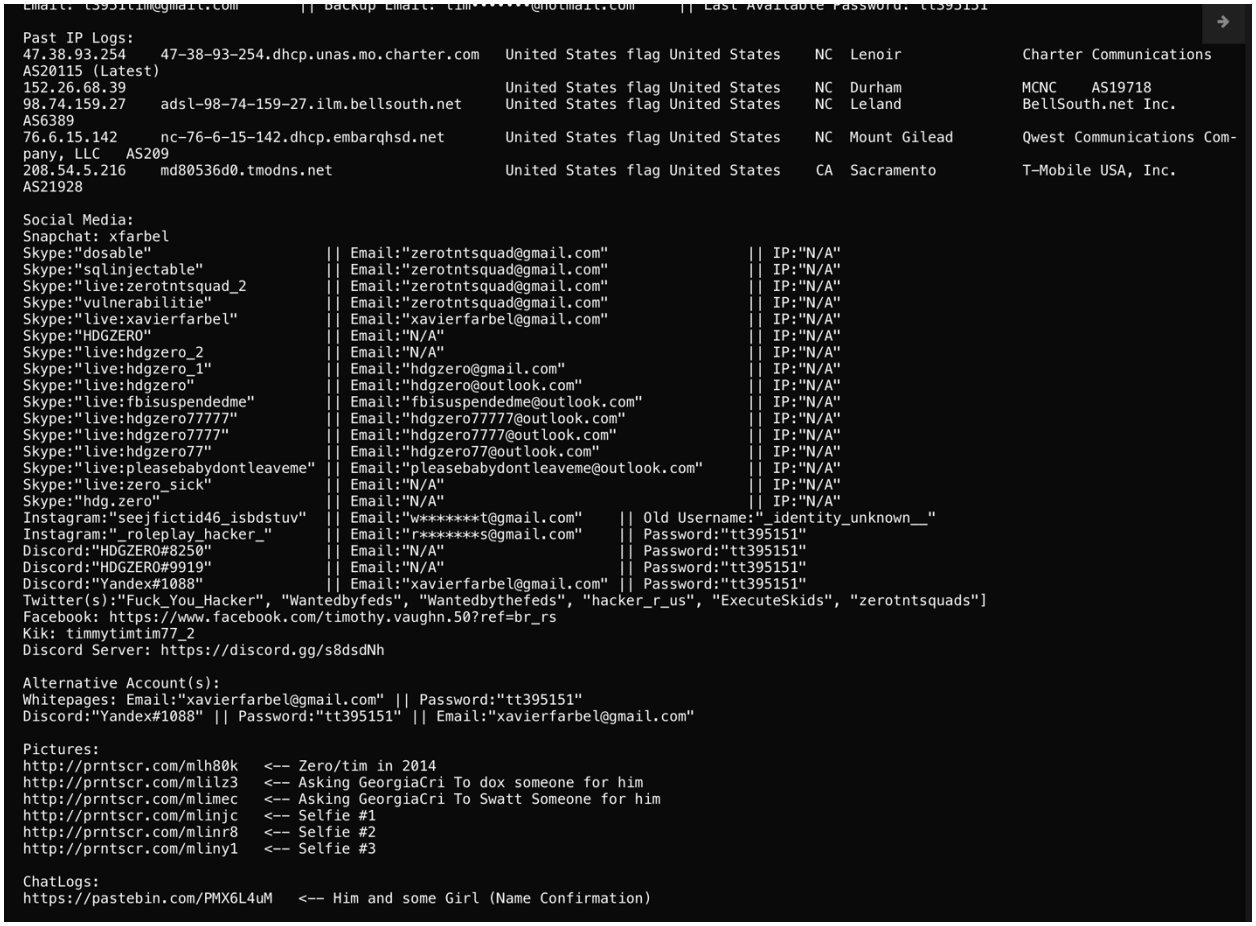


Figura 14 - Cuentas de *Skype, Snapchat* y cuentas alternas.

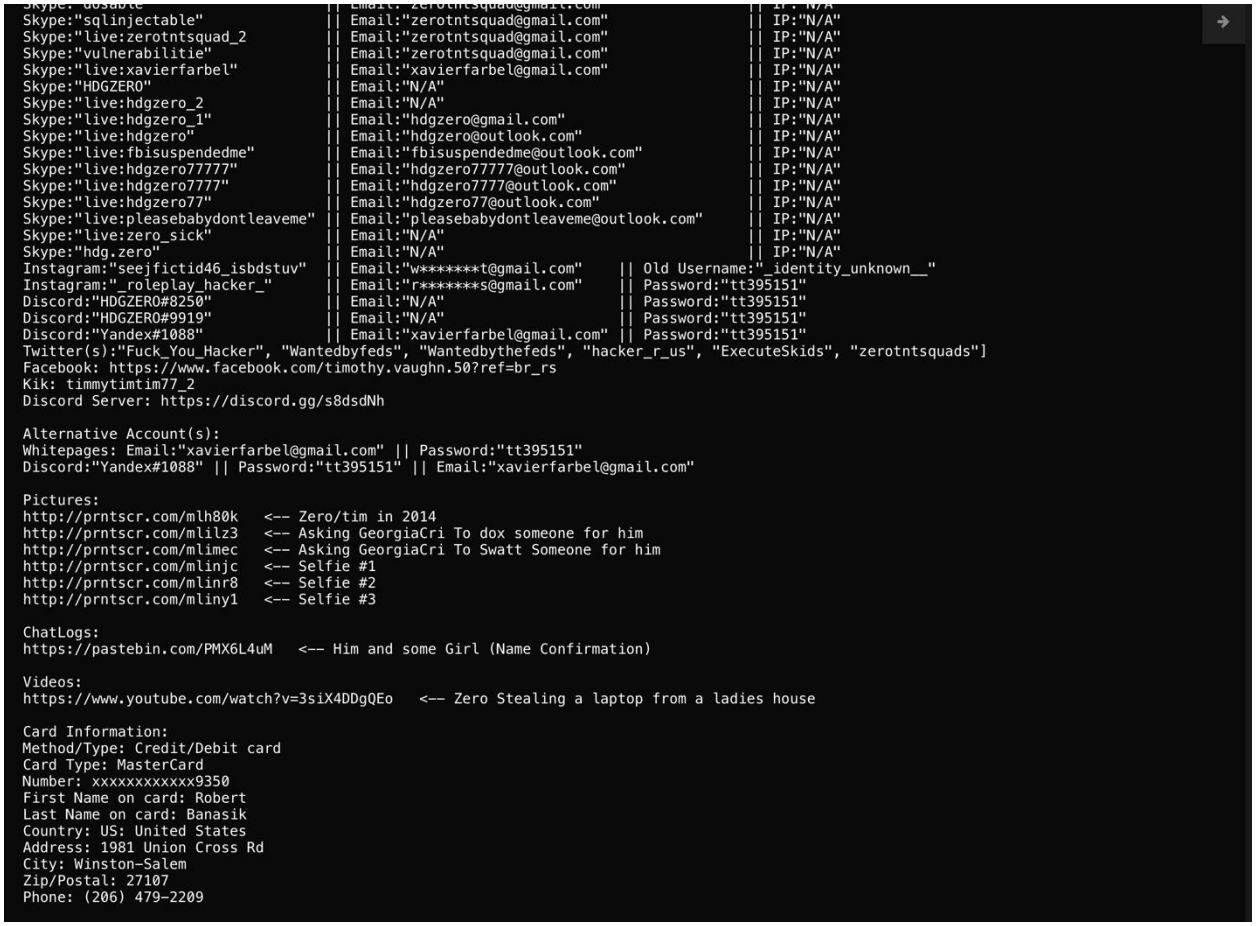


Figura 15 - Continuación de figura 10 y tarjetas de crédito utilizadas.

Cadena de custodia:

Los procedimientos estándares de operación de QNTM forensix indican la documentación de las etapas de adquisición, procesamiento y control de la evidencia analizada. La razón es mantener integridad del documento.

Primer evento

- Descripción: Evidencia fue entregada por Ryan White al examinador Ángel Pérez. Evidencia es un disco duro portátil *Item* no. 2019-EV-00 y un dispositivo móvil *Item* no. 2019-EV-01

- Verificado por: Ángel Pérez y Ryan White
- Fecha de comienzo: 12 de septiembre de 2019 – 1:49 p.m.
- Fecha de terminación: 12 de septiembre de 2019 – 2:54 p.m.
- Lugar de origen: Oficina del FBI, Distrito Central de California
- Destino: Laboratorio forense – QNTM Forensix, Puerto Rico

Segundo evento

- Descripción: Creación de número de caso a evidencia recibida
- Verificado por: Ángel Pérez
- Fecha de comienzo: 14 de septiembre de 2019 – 8:01 a.m.
- Fecha de terminación: 14 de septiembre de 2019 – 8:04 a.m.
- Lugar de origen: QNTM Forensix, Puerto Rico.
- Destino: QNTM Forensix, Puerto Rico.

Tercer evento

- Descripción: Proceso de imagen y análisis de evidencia recibida
- Verificado por: Ángel Pérez
- Fecha de comienzo: 15 de septiembre de 2019 – 8:04 a.m.
- Fecha de terminación: 15 de septiembre de 2019 – 10:33 a.m.
- Lugar de origen: QNTM Forensix, Puerto Rico.
- Destino: QNTM Forensix, Puerto Rico.

Cuarto evento

- Descripción: Entrega de la evidencia y el informe de análisis forense a Ryan White.
- Verificado por: Ángel Pérez y Ryan White.
- Fecha de comienzo: 22 de septiembre de 2019 – 4:33 p.m.
- Fecha de terminación: 22 de septiembre de 2019 – 5:01 p.m.
- Lugar de origen: QNTM Forensix, Puerto Rico.
- Destino: Oficina del FBI, Distrito Central de California.

Procedimiento:

A continuación, se describe los pasos que fueron ejecutados como parte del proceso de análisis forense realizado a la evidencia recibida.

1. Procedimiento: Creación del caso
    a. Herramienta: AccessData FTK
    b. Fecha de comienzo: 15 de septiembre de 2019 – 7:00 a.m.
    c. Fecha de terminación: 15 de septiembre de 2019 – 8:22 a.m.
    d. Descripción: Asignar número de caso a la evidencia adquirida con la herramienta FTK. (Figura 16)

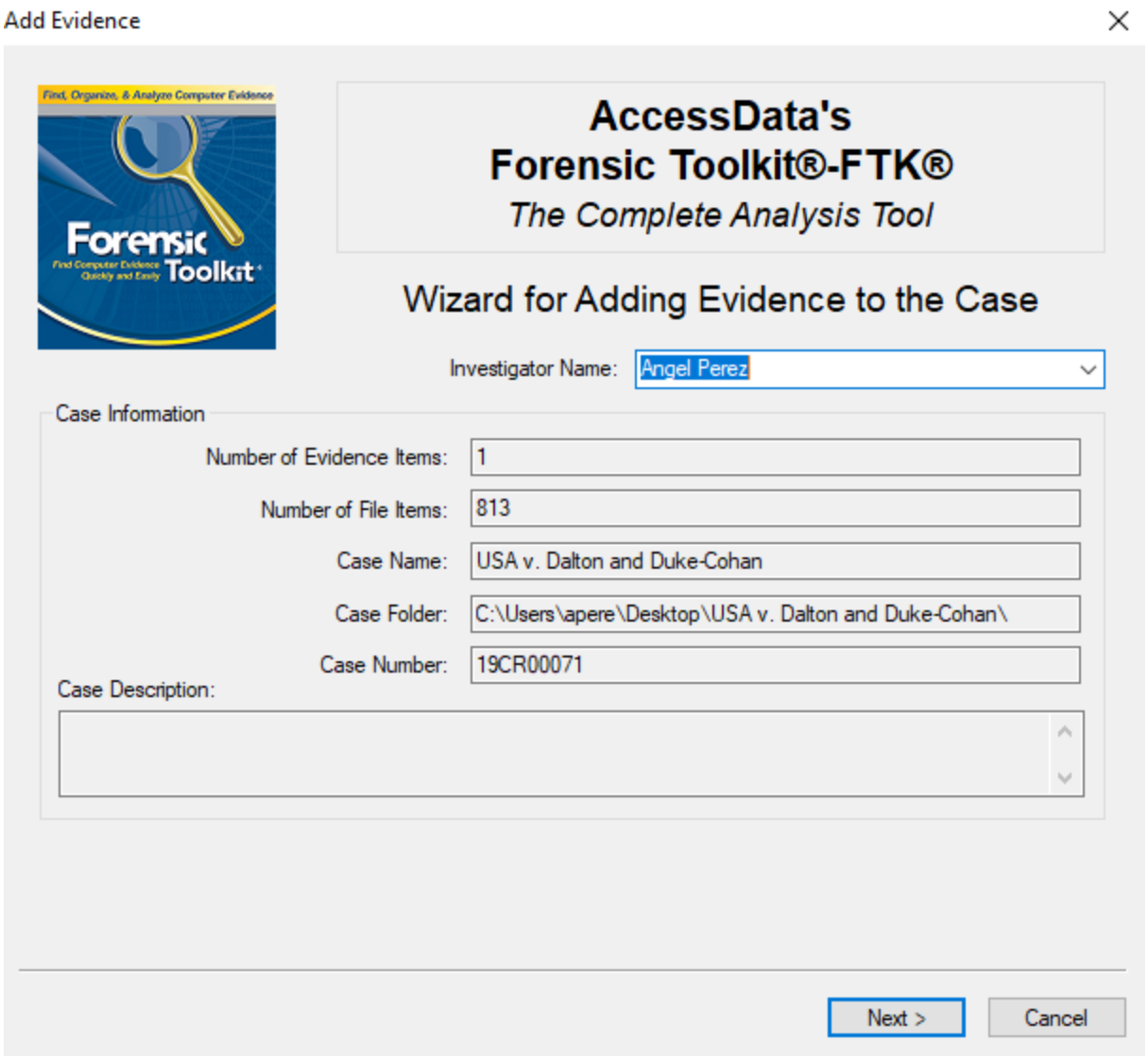


Figura 16 - Asignando número de caso a la evidencia.

2. Procedimiento: Creación de imagen original del dispositivo móvil.
    a. Herramienta: FTK Imager
    b. Fecha de comienzo: 15 de septiembre de 2019 – 10:04 a.m.
    c. Fecha de terminación: 15 de septiembre de 2019 – 10:44 a.m.
    d. Descripción: Proceso de captura de imágenes con la herramienta FTK Imager (Figura 17).

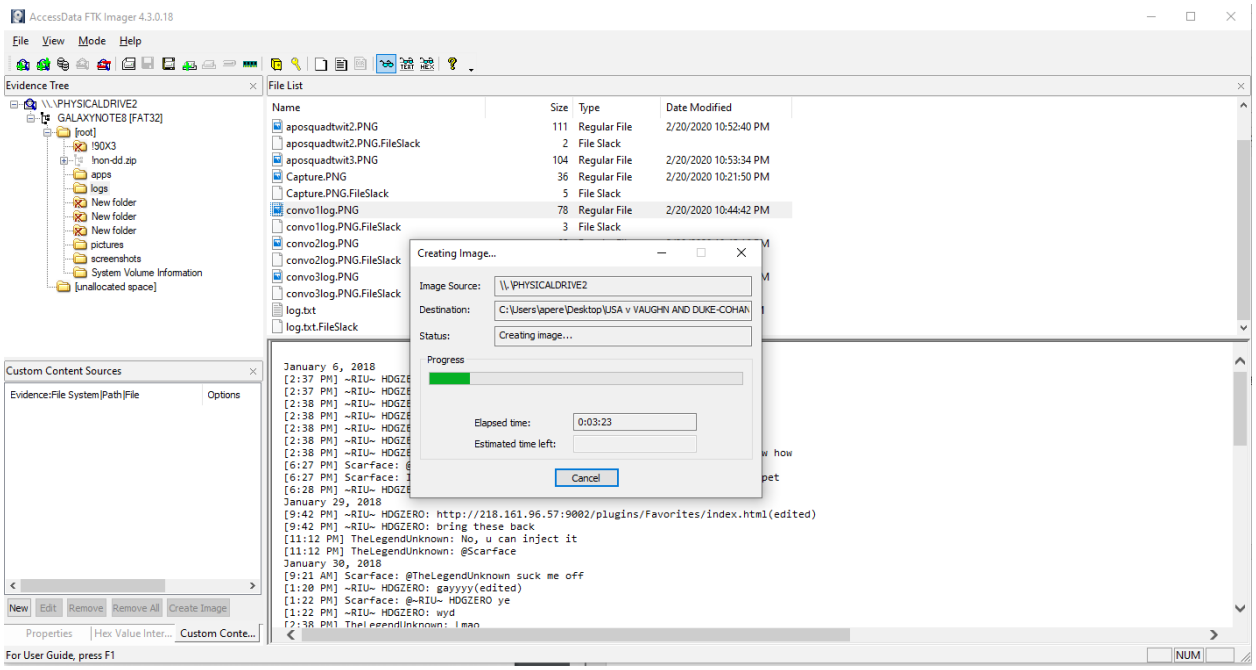


Figura 17- Creación de la imagen con *FTK Imager*

3. Procedimiento: Extrayendo información del dispositivo móvil

    a. Herramienta: FTK forensic toolkit

    b. Fecha de comienzo: 16 de septiembre de 2019 – 8:01 a.m.

    c. Fecha de terminación: 16 de septiembre de 2019 – 9:33 a.m.

    d. Descripción: Se realizó una búsqueda en la memoria del dispositivo móvil encontrando imágenes de publicaciones y un log de una conversación (Figura 18).

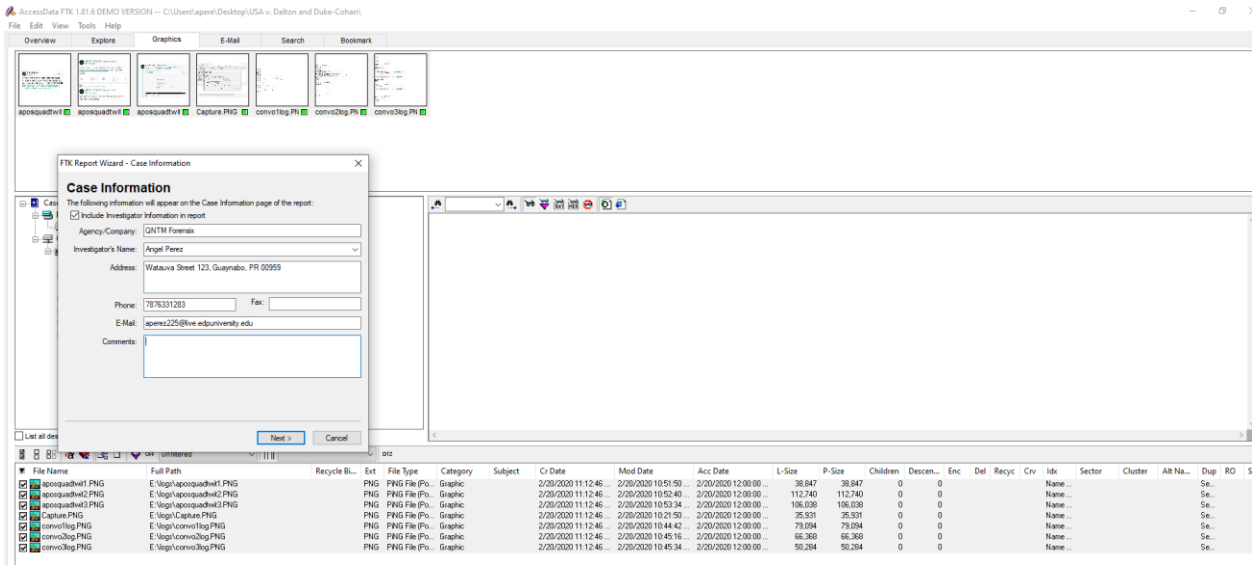


Figura 18 - Archivos encontrados en el dispositivo móvil.

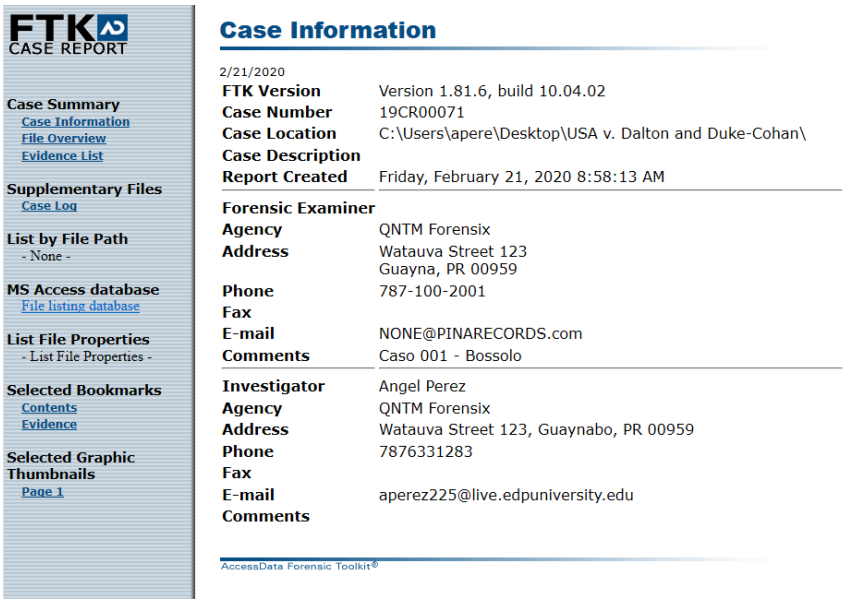
4. Procedimiento: Creando reporte por FTK

    a. Herramienta: FTK Forensic Toolkit

    b. Fecha de comienzo: 16 de septiembre de 2019 – 10:01 a.m.

    c. Fecha de terminación 16 de septiembre de 2019 – 10:38 a.m.

    d. Descripción: Se utilizó la herramienta para generar un reporte de los hallazgos (Figura 19, 20, 21, 22, 23, 24).



FTK CASE REPORT

Case Summary
Case Information
File Overview
Evidence List

Supplementary Files
Case Log

List by File Path
- None -

MS Access database
File listing database

List File Properties
- List File Properties -

Selected Bookmarks
Contents
Evidence

Selected Graphic Thumbnails
Page 1

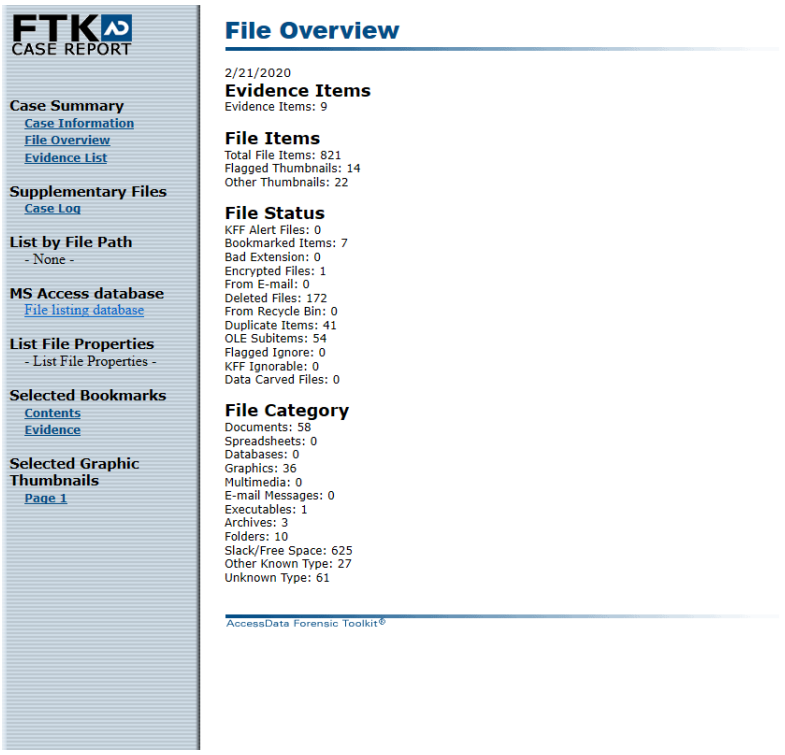
Case Information

2/21/2020

FTK Version	Version 1.81.6, build 10.04.02
Case Number	19CR00071
Case Location	C:\Users\apere\Desktop\USA v. Dalton and Duke-Cohan\
Case Description	
Report Created	Friday, February 21, 2020 8:58:13 AM
Forensic Examiner	
Agency	QNTM Forensix
Address	Watauva Street 123 Guayna, PR 00959
Phone	787-100-2001
Fax	
E-mail	NONE@PINARECORDS.com
Comments	Caso 001 - Bossolo
Investigator	Angel Perez
Agency	QNTM Forensix
Address	Watauva Street 123, Guaynabo, PR 00959
Phone	7876331283
Fax	
E-mail	aperez225@live.edpuniversity.edu
Comments	

AccessData Forensic Toolkit®

Figura 19 - Reporte del caso por *FTK*.



FTK CASE REPORT

Case Summary
Case Information
File Overview
Evidence List

Supplementary Files
Case Log

List by File Path
- None -

MS Access database
File listing database

List File Properties
- List File Properties -

Selected Bookmarks
Contents
Evidence

Selected Graphic Thumbnails
Page 1

File Overview

2/21/2020

Evidence Items
Evidence Items: 9

File Items
Total File Items: 821
Flagged Thumbnails: 14
Other Thumbnails: 22

File Status
KFF Alert Files: 0
Bookmarked Items: 7
Bad Extension: 0
Encrypted Files: 1
From E-mail: 0
Deleted Files: 172
From Recycle Bin: 0
Duplicate Items: 41
OLE Subitems: 54
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0

File Category
Documents: 58
Spreadsheets: 0
Databases: 0
Graphics: 36
Multimedia: 0
E-mail Messages: 0
Executables: 1
Archives: 3
Folders: 10
Slack/Free Space: 625
Other Known Type: 27
Unknown Type: 61

AccessData Forensic Toolkit®

Figura 20 - Reporte del caso por *FTK* (continuación), un overview.

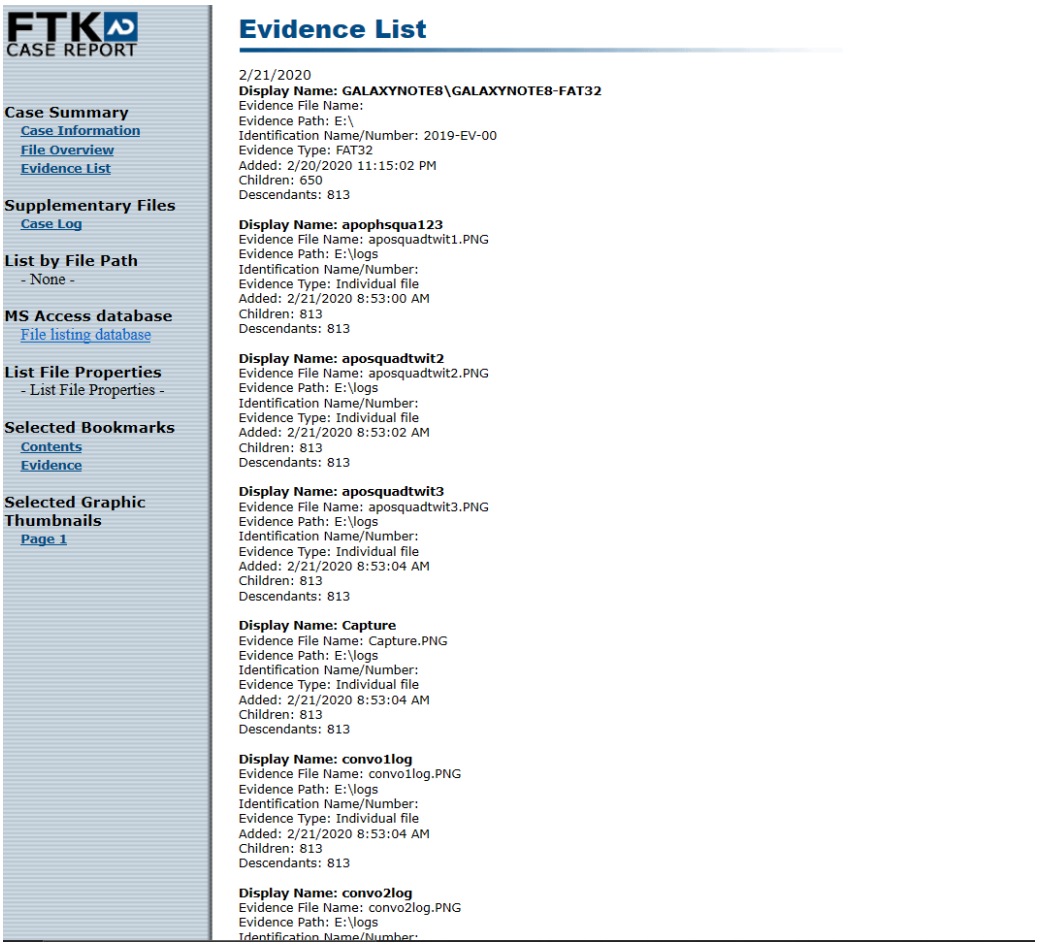


Figura 21 - Reporte del caso por *FTK* (continuación) lista de evidencia.

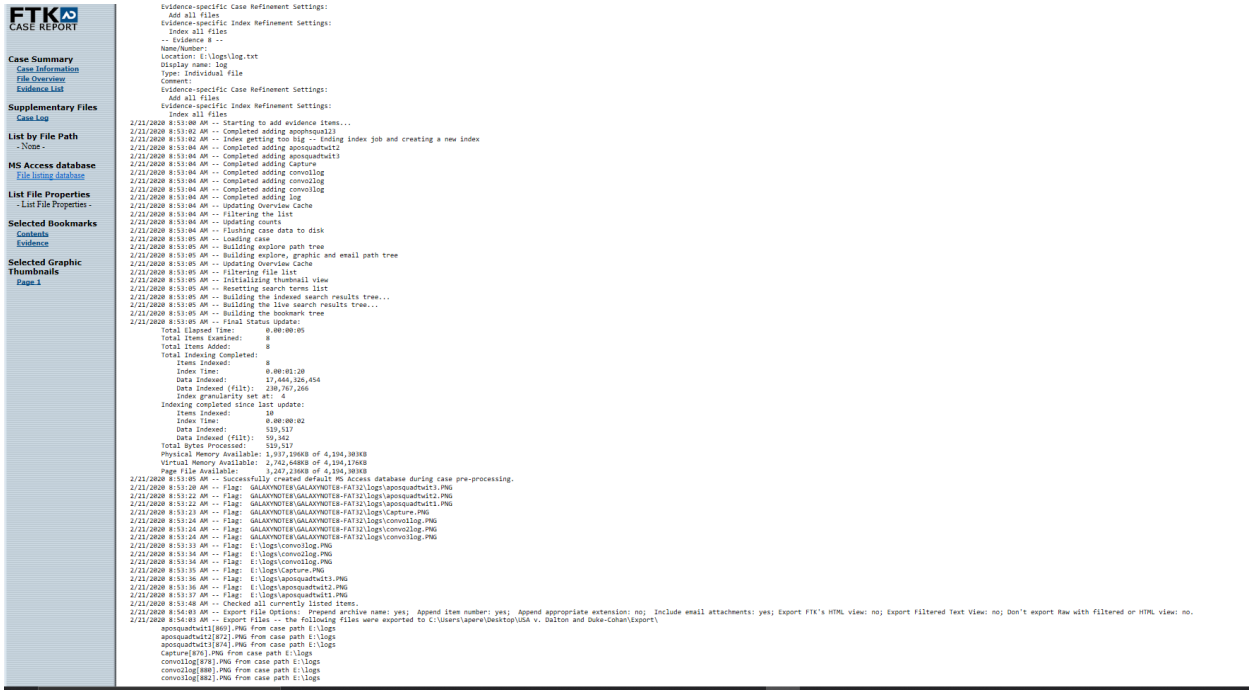


Figura 22- Reporte del caso por *FTK* (continuación), lista detallada de evidencia.

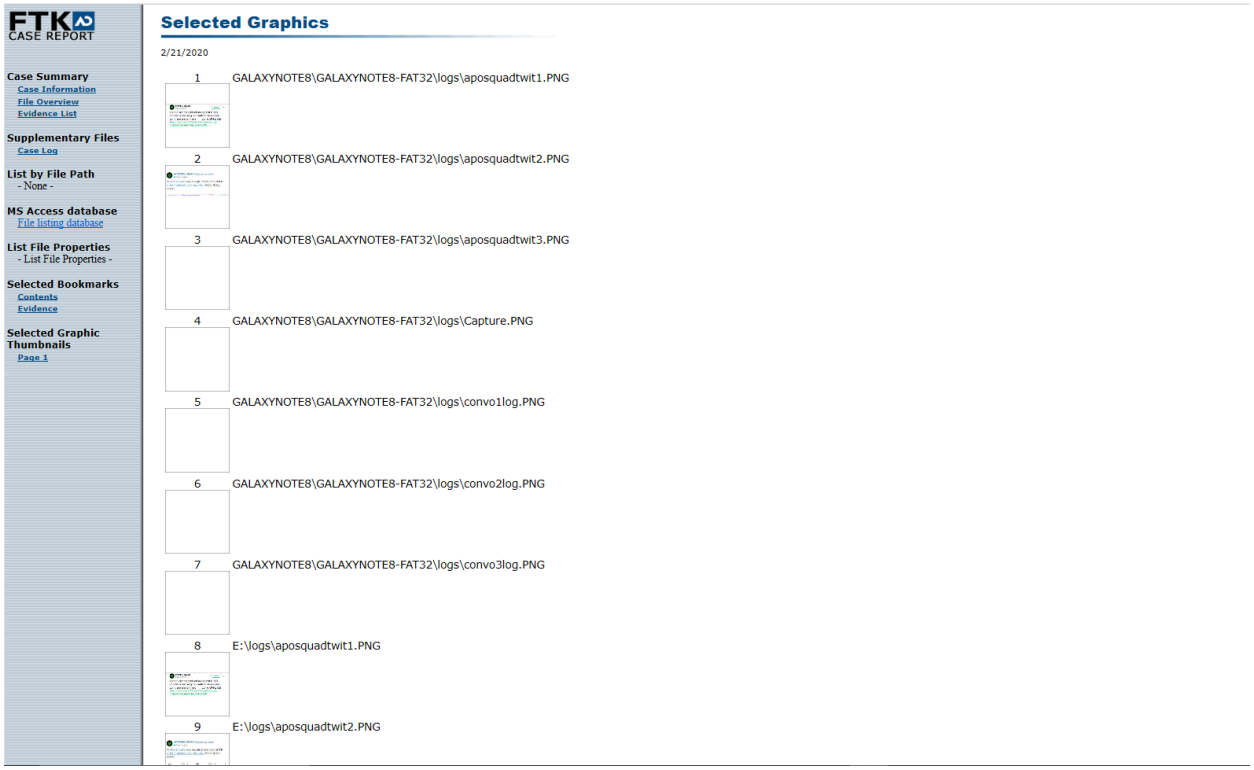


Figura 23 - Reporte del caso por *FTK* (continuación) gráficas encontradas

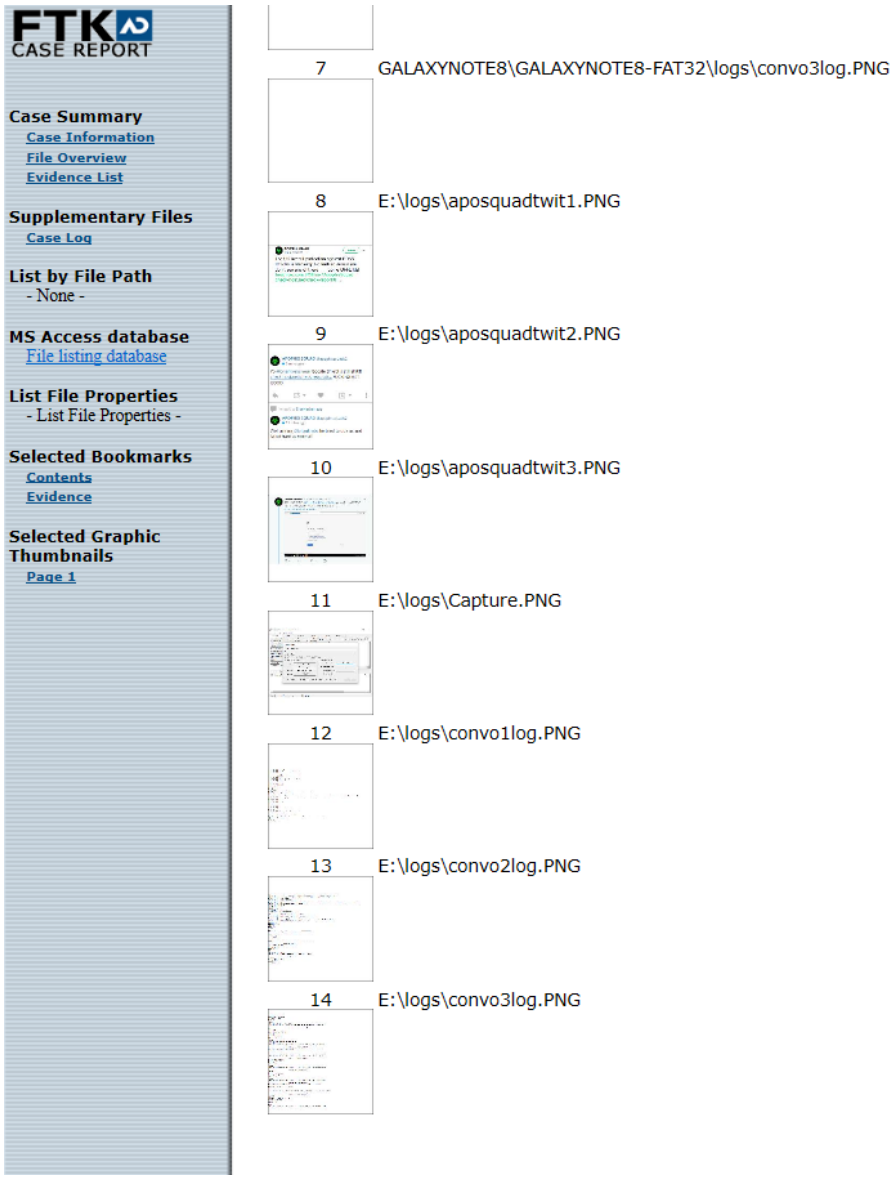


Figura 24 - Reporte del caso por *FTK* (continuación) logs encontrados.

5. Procedimiento: Creación de imagen del disco duro portátil.
    a. Herramienta: FTK Imager
    b. Fecha de comienzo: 17 de septiembre de 2019 – 9:33 a.m.
    c. Fecha de terminación: 17 de septiembre de 2019 – 10:11 a.m.
    d. Descripción: Proceso de captura de imágenes con la herramienta FTK Imager (Figura 25).

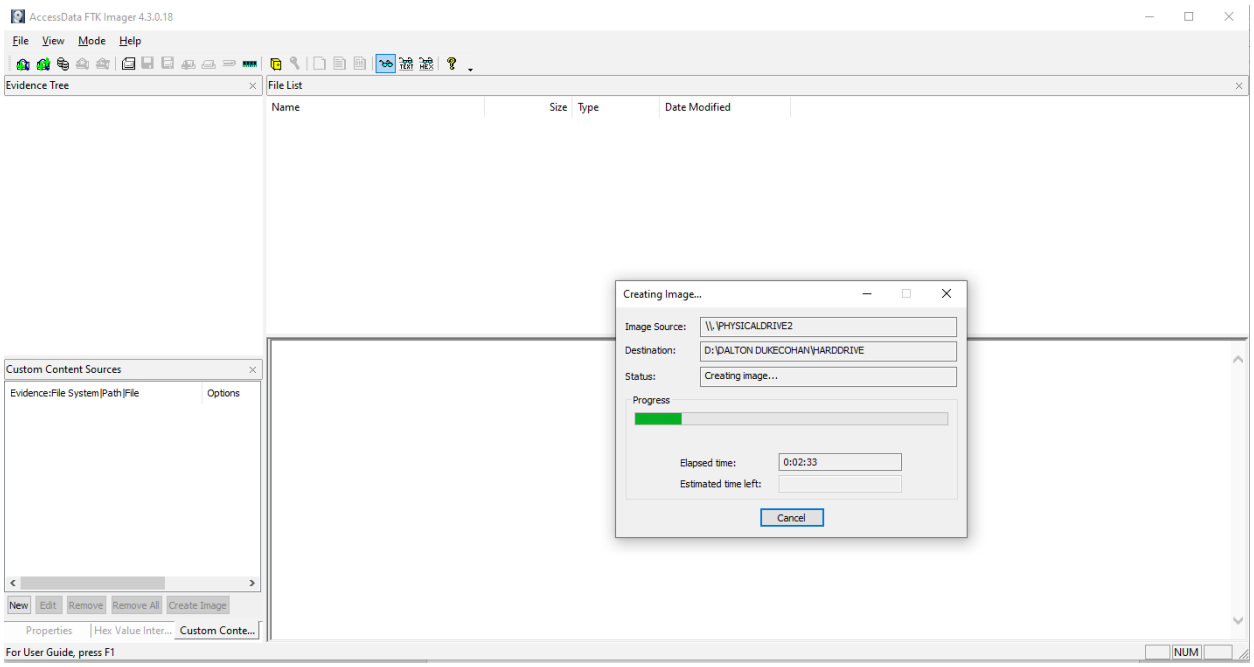


Figura 25 - Creando imagen con *FTK Imager*.

6. Procedimiento: Extrayendo información del disco duro portátil.

    a. Herramienta: FTK forensic toolkit

    b. Fecha de comienzo: 17 de septiembre de 2019 – 1:22 p.m.

    c. Fecha de terminación: 17 de septiembre de 2019 – 4:53 p.m.

    d. Descripción: Se realizó una búsqueda en la memoria del disco duro portátil encontrando datos de sus cuentas, direcciones de ip y los juegos en donde cometió los crímenes (Figura 26 y 27).

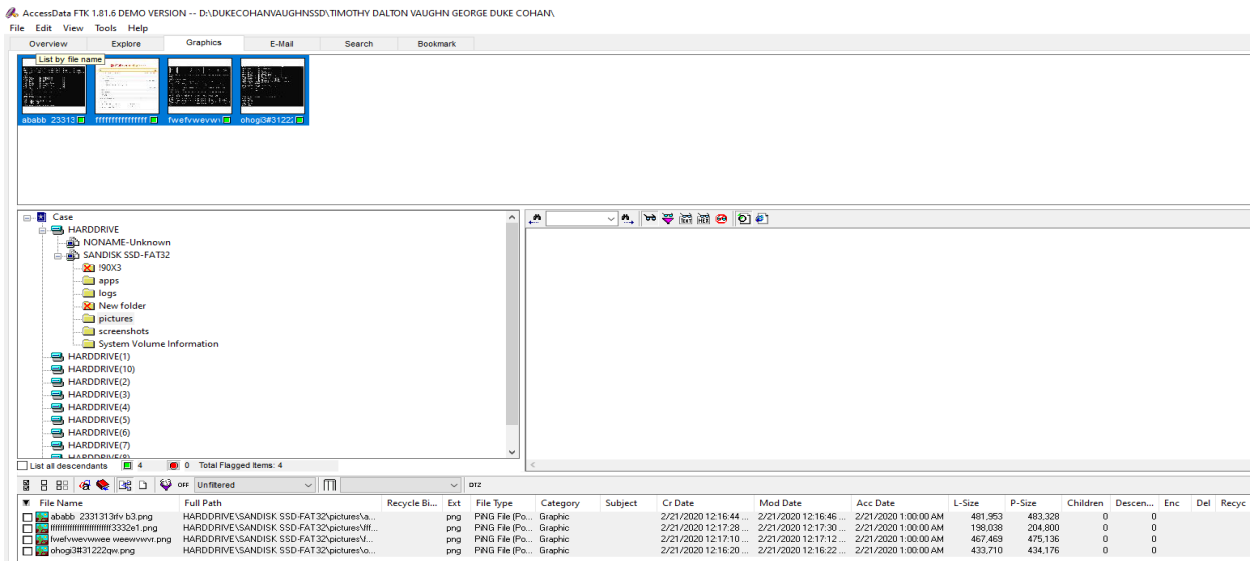


Figura 26 - Imágenes con las cuentas, usuarios y direcciones de IP que utilizaba.

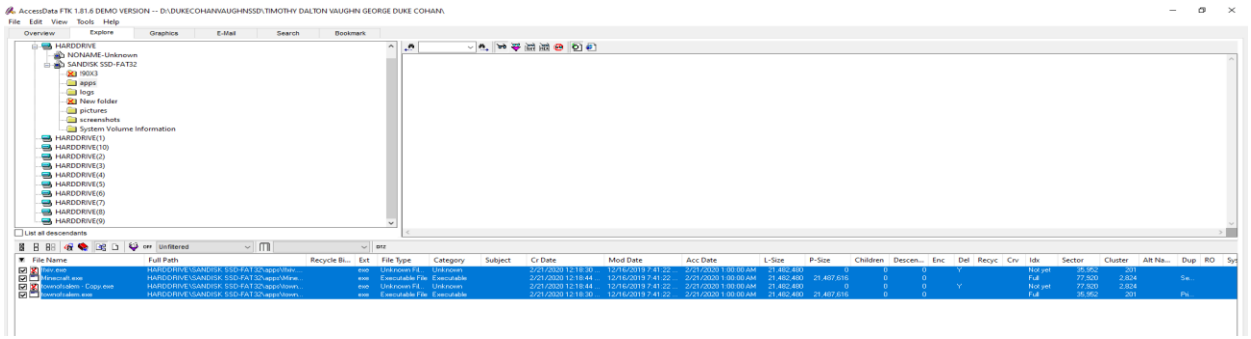


Figura 27 - Las aplicaciones donde se cometieron los crímenes.

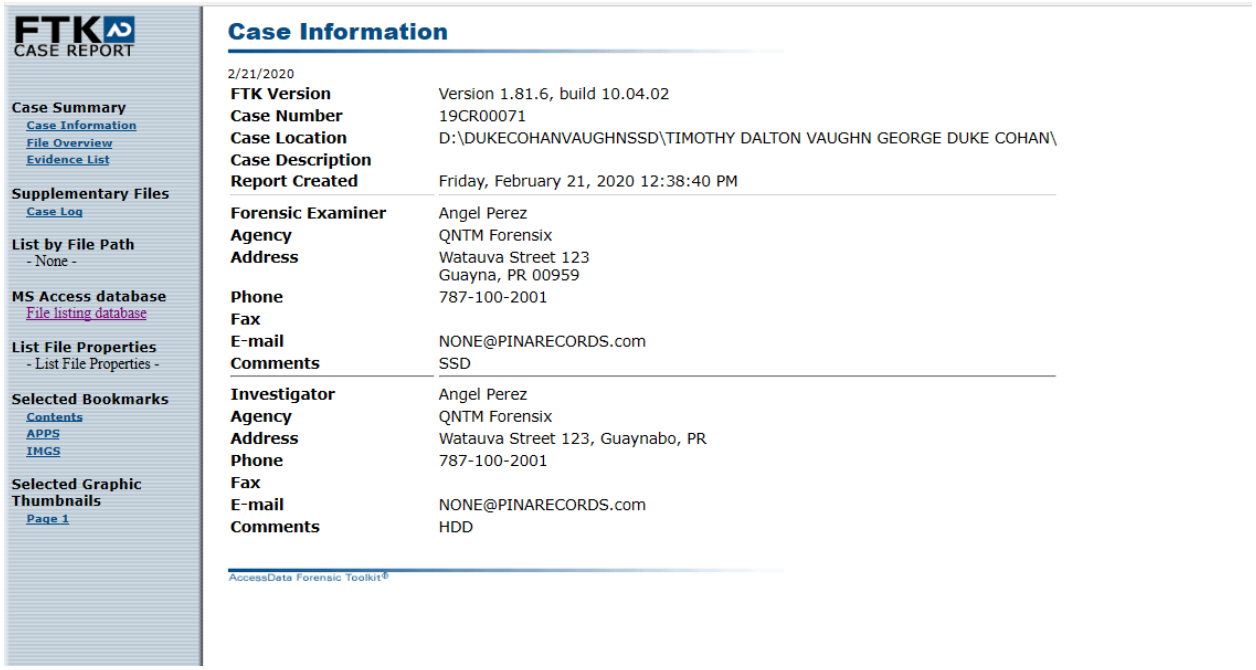
7. Creación del reporte

    a. Herramienta: FTK Forensic Toolkit

    b. Fecha de comienzo: 18 de septiembre de 2019 – 8:49 a.m.

    c. Fecha de terminación: 18 de septiembre de 2019 – 10:01 a.m.

    d. Descripción: Se utilizó la herramienta para generar un reporte de los hallazgos (Figura 28, 29, 30, 31, 32).



FTK CASE REPORT

Case Summary
Case Information
File Overview
Evidence List

Supplementary Files
Case Log

List by File Path
- None -

MS Access database
File listing database

List File Properties
- List File Properties -

Selected Bookmarks
Contents
APPS
IMGS

Selected Graphic Thumbnails
Page 1

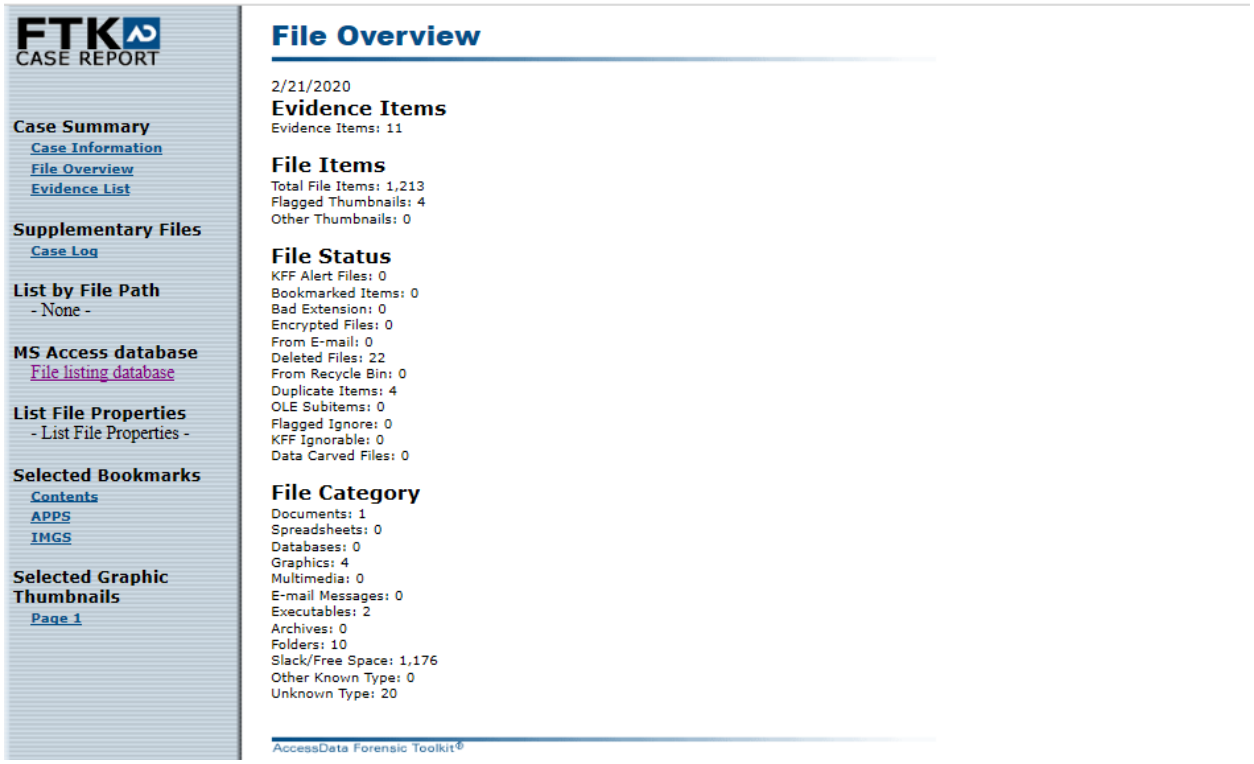
Case Information

2/21/2020

FTK Version	Version 1.81.6, build 10.04.02
Case Number	19CR00071
Case Location	D:\DUKECOHANVAUGHNSSD\TIMOTHY DALTON VAUGHN GEORGE DUKE COHAN\
Case Description	
Report Created	Friday, February 21, 2020 12:38:40 PM
Forensic Examiner	Angel Perez
Agency	QNTM Forensix
Address	Watauva Street 123 Guayna, PR 00959
Phone	787-100-2001
Fax	
E-mail	NONE@PINARECORDS.com
Comments	SSD
Investigator	Angel Perez
Agency	QNTM Forensix
Address	Watauva Street 123, Guaynabo, PR
Phone	787-100-2001
Fax	
E-mail	NONE@PINARECORDS.com
Comments	HDD

AccessData Forensic Toolkit®

Figura 28 - Información del caso en el reporte.



FTK CASE REPORT

Case Summary
Case Information
File Overview
Evidence List

Supplementary Files
Case Log

List by File Path
- None -

MS Access database
File listing database

List File Properties
- List File Properties -

Selected Bookmarks
Contents
APPS
IMGS

Selected Graphic Thumbnails
Page 1

File Overview

2/21/2020

Evidence Items
Evidence Items: 11

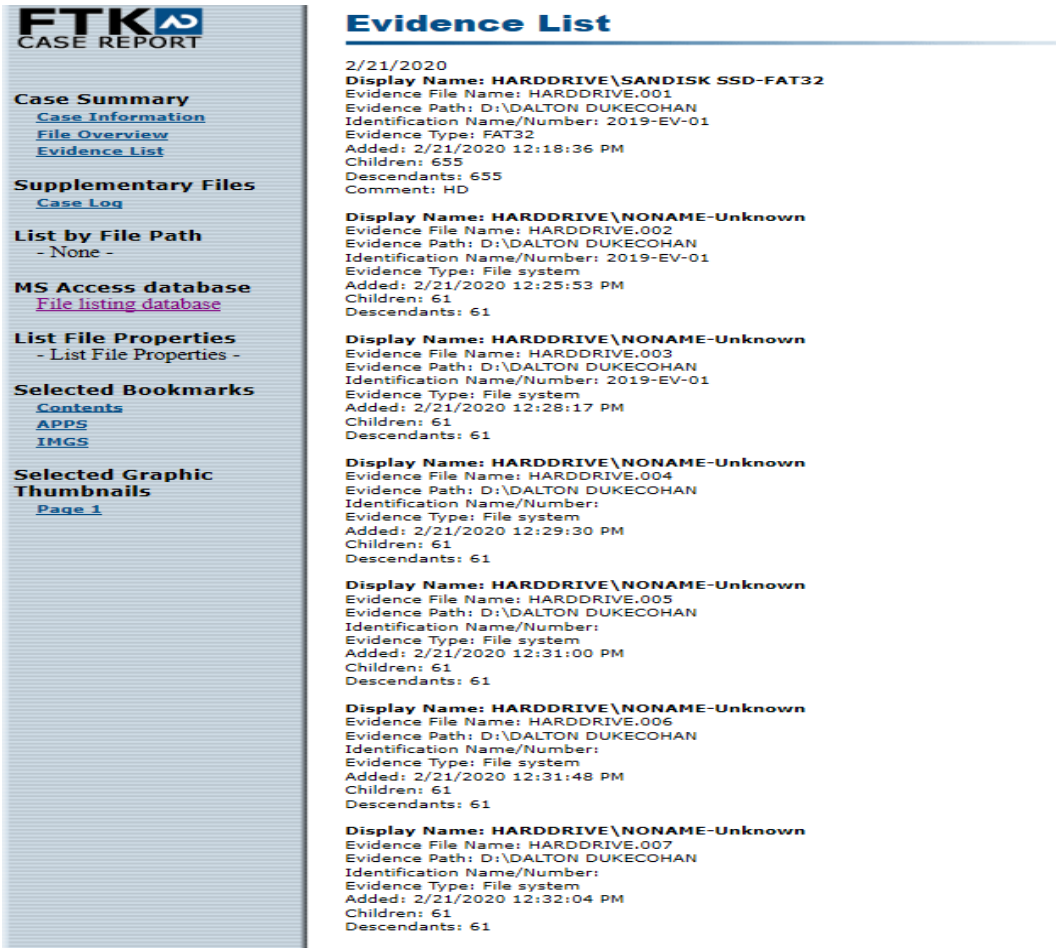
File Items
Total File Items: 1,213
Flagged Thumbnails: 4
Other Thumbnails: 0

File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 22
From Recycle Bin: 0
Duplicate Items: 4
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0

File Category
Documents: 1
Spreadsheets: 0
Databases: 0
Graphics: 4
Multimedia: 0
E-mail Messages: 0
Executables: 2
Archives: 0
Folders: 10
Slack/Free Space: 1,176
Other Known Type: 0
Unknown Type: 20

AccessData Forensic Toolkit®

Figura 29 - *Overview* del reporte.



FTK CASE REPORT

Case Summary
Case Information
File Overview
Evidence List

Supplementary Files
Case Log

List by File Path
- None -

MS Access database
File listing database

List File Properties
- List File Properties -

Selected Bookmarks
Contents
APPS
IMGS

Selected Graphic Thumbnails
Page 1

Evidence List

2/21/2020
Display Name: HARDDRIVE\SANDISK SSD-FAT32
Evidence File Name: HARDDRIVE.001
Evidence Path: D:\DALTON DUKECOHAN
Identification Name/Number: 2019-EV-01
Evidence Type: FAT32
Added: 2/21/2020 12:18:36 PM
Children: 655
Descendants: 655
Comment: HD

Display Name: HARDDRIVE\NONAME-Unknown
Evidence File Name: HARDDRIVE.002
Evidence Path: D:\DALTON DUKECOHAN
Identification Name/Number: 2019-EV-01
Evidence Type: File system
Added: 2/21/2020 12:25:53 PM
Children: 61
Descendants: 61

Display Name: HARDDRIVE\NONAME-Unknown
Evidence File Name: HARDDRIVE.003
Evidence Path: D:\DALTON DUKECOHAN
Identification Name/Number: 2019-EV-01
Evidence Type: File system
Added: 2/21/2020 12:28:17 PM
Children: 61
Descendants: 61

Display Name: HARDDRIVE\NONAME-Unknown
Evidence File Name: HARDDRIVE.004
Evidence Path: D:\DALTON DUKECOHAN
Identification Name/Number:
Evidence Type: File system
Added: 2/21/2020 12:29:30 PM
Children: 61
Descendants: 61

Display Name: HARDDRIVE\NONAME-Unknown
Evidence File Name: HARDDRIVE.005
Evidence Path: D:\DALTON DUKECOHAN
Identification Name/Number:
Evidence Type: File system
Added: 2/21/2020 12:31:00 PM
Children: 61
Descendants: 61

Display Name: HARDDRIVE\NONAME-Unknown
Evidence File Name: HARDDRIVE.006
Evidence Path: D:\DALTON DUKECOHAN
Identification Name/Number:
Evidence Type: File system
Added: 2/21/2020 12:31:48 PM
Children: 61
Descendants: 61

Display Name: HARDDRIVE\NONAME-Unknown
Evidence File Name: HARDDRIVE.007
Evidence Path: D:\DALTON DUKECOHAN
Identification Name/Number:
Evidence Type: File system
Added: 2/21/2020 12:32:04 PM
Children: 61
Descendants: 61

Figura 30 - Listado de la evidencia.

Bookmark

2/21/2020
Report file time zone: Examiner's Local Machine Setting

Name: APPS
Comment:
File Count: 4

File: !fxiv.exe
Full Path: HARDDRIVE\SANDISK SSD-FAT32\apps\!fxiv.exe
Alias:
Extension: exe
File Type: Unknown File Type
Category: Unknown
Subject:
Created: 2/21/2020 12:18:30 PM
Modified: 12/16/2019 7:41:22 PM
Accessed: 2/21/2020 1:00:00 AM
Logical Size: 21,482,480
Physical Size: 0
Children: 0
Descendants: 0
Encrypted:
Deleted: Y
Recycled:
Carved:
Indexed: Not yet
Sector: 35,952
Cluster: 201
Alternate Name:
Duplicate:
Read Only:
System:
Hidden:
Item Number: 43
Compressed:
KFF:
Bad Extension:
Emailed:
Header:
MD5:
SHA1:
Hash Set:
Email Date:
From:
To:
CC:
Attachment Info:
BCC:
Exported as: (unable to export)

File: Minecraft.exe
Full Path: HARDDRIVE\SANDISK SSD-FAT32\apps\Minecraft.exe
Alias:
Extension: exe
File Type: Executable File
Category: Executable
Subject:
Created: 2/21/2020 12:18:44 PM
Modified: 12/16/2019 7:41:22 PM
Accessed: 2/21/2020 1:00:00 AM
Logical Size: 21,482,480
Physical Size: 21,487,616
Children: 0
Descendants: 0
Encrypted:
Deleted:
Recycled:
Carved:
Indexed: Full

Figura 31 - *Bookmarks* de lo encontrado, en este caso las aplicaciones.

File: Minecraft.exe
Full Path: HARDDRIVE\SANDISK SSD-FAT32\apps\Minecraft.exe
Alias:
Extension: exe
File Type: Executable File
Category: Executable
Subject:
Created: 2/21/2020 12:18:44 PM
Modified: 12/16/2019 7:41:22 PM
Accessed: 2/21/2020 1:00:00 AM
Logical Size: 21,482,480
Physical Size: 21,487,616
Children: 0
Descendants: 0
Encrypted:
Deleted:
Recycled:
Carved:
Indexed: Full
Sector: 77,920
Cluster: 2,824
Alternate Name:
Duplicate: Secondary
Read Only:
System:
Hidden:
Item Number: 47
Compressed:
KFF:
Bad Extension:
Emailed:
Header: 4D5A900003000000
MD5: D41D2359E5CB52002E4E819F386F4CAE
SHA1: FB7572962C659238F72B4F43A0B451D125E02ABC
Hash Set:
Email Date:
From:
To:
CC:
Attachment Info:
BCC:
Exported as: 47.exe

File: townofsalem - Copy.exe
Full Path: HARDDRIVE\SANDISK SSD-FAT32\apps\townofsalem - Copy.exe
Alias:
Extension: exe
File Type: Unknown File Type
Category: Unknown
Subject:
Created: 2/21/2020 12:18:44 PM
Modified: 12/16/2019 7:41:22 PM
Accessed: 2/21/2020 1:00:00 AM
Logical Size: 21,482,480
Physical Size: 0
Children: 0
Descendants: 0
Encrypted:
Deleted: Y
Recycled:
Carved:
Indexed: Not yet
Sector: 77,920
Cluster: 2,824
Alternate Name:
Duplicate:
Read Only:
System:
Hidden:
Item Number: 46
Compressed:
KFF:
Bad Extension:
Emailed:
Header:

Figura 32 - Continuación de los *bookmarks* de las aplicaciones.

Name: IMGS
Comment:
File Count: 4

File: ababb 2331313rfv b3.png
Full Path: HARDDRIVE\SANDISK SSD-FAT32\pictures\ababb 2331313rfv b3.png
Alias:
Extension: png
File Type: PiNG File (Portable Network Graphics)
Category: Graphic
Subject:
Created: 2/21/2020 12:16:44 PM
Modified: 2/21/2020 12:16:46 PM
Accessed: 2/21/2020 1:00:00 AM
Logical Size: 481,953
Physical Size: 483,328
Children: 0
Descendants: 0
Encrypted:
Deleted:
Recycled:
Carved:
Indexed: Name only (disregardable file type)
Sector: 33,680
Cluster: 59
Alternate Name:
Duplicate:
Read Only:
System:
Hidden:
Item Number: 35
Compressed:
KFF:
Bad Extension:
Emailed:
Header: 89504E470D0A1A0A
MD5: BB2B84F178F652DDC33A6954576EE5BC
SHA1: 018732D0B9506D415BA27C894387A153E59D61ED
Hash Set:
Email Date:
From:
To:
CC:
Attachment Info:
BCC:
Exported as: 35.png

File: ffffffffffffffffffffffff3332e1.png
Full Path: HARDDRIVE\SANDISK SSD-FAT32\pictures\ffffffffffffffffffffffff3332e1.png
Alias:
Extension: png
File Type: PiNG File (Portable Network Graphics)
Category: Graphic
Subject:
Created: 2/21/2020 12:17:28 PM
Modified: 2/21/2020 12:17:30 PM
Accessed: 2/21/2020 1:00:00 AM
Logical Size: 198,038
Physical Size: 204,800
Children: 0
Descendants: 0
Encrypted:
Deleted:
Recycled:
Carved:
Indexed: Name only (disregardable file type)

Figura 33 - *Bookmarks* en este caso de las imágenes.

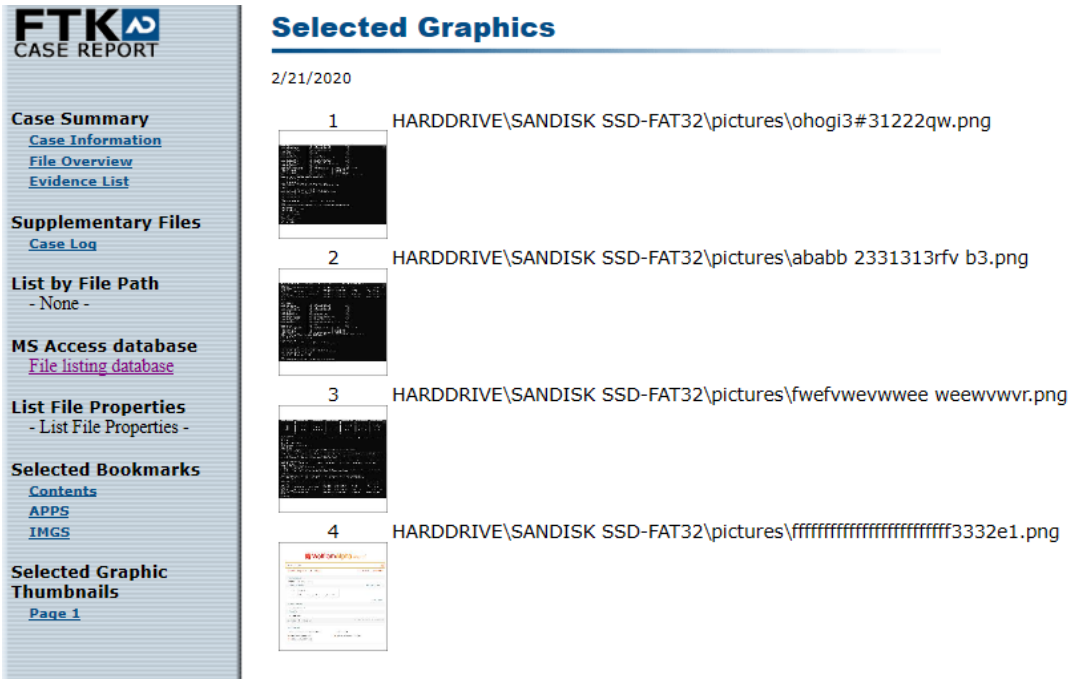


Figura 34 - Las gráficas seleccionadas.

Conclusión:

Los resultados del análisis realizado a los dispositivos entregados por Ryan White vinculan a Timothy Dalton Vaughn y a George Duke-Cohan con los ataques *DDoS* y las amenazas. Las actividades fueron realizadas de cuentas de usuario que están registradas en el dispositivo móvil y el disco duro portátil. Los hallazgos de las cuentas, *logs* y juegos instalados dejan evidenciado que son parte de *ApophisSquad*.

5. Discusión del Caso

El análisis realizado en la investigación forense digital nos llevó a encontrar culpabilidad al acusado. La evidencia encontrada vincula a Dalton Vaughn con Duke-Cohan y al *Apophis Squad*. Los hechos descritos en el caso judicial van a la par con lo recuperado del disco duro y del dispositivo móvil, esto concreta la idea previa de los eventos. Al encontrar las cuentas que aparecían en los mensajes grabadas en logs con usuarios y contraseñas se evidencia que es dueño de ellas. Adicional, sostienen conversaciones y planificaciones contra las victimas lo que apoya la conclusión del informe.

Los daños a raíz de los ataques *DDoS* no son sólo de la pérdida de ingresos al interrumpir el servicio, se suman los gastos para mejorar la calidad de seguridad cibernética. Adicional, hay un factor psicológico que afecta al cliente ya que sienten que la información podría estar expuesta a futuros ataques. Lo mismo ocurre con la escuela que jaquearon, ya que los estudiantes tienen su información personal en una página que no tiene parámetros de seguridad capaces de proteger estos datos confidenciales.

6. Informe de Auditoría y Prevención

Transfondo:

Timothy Dalton Vaughn de *Winston-Salem*, Carolina del Norte y George Duke Cohan de *Hertfordshire*, Reinos Unidos son miembros del grupo colectivo de jáquer *Apophis Squad*. Ambos son acusados de hacer amenazas falsas, ataques cibernéticos y múltiples ataques *DDoS*. Los actos ilícitos transcurrieron durante los primeros ocho meses del 2018, donde sus víctimas eran escuelas, páginas de internet y juegos de video en línea. Durante este tiempo frecuentaban las redes sociales para alardear sobre los ataques a sus víctimas.

Uno de los primeros ataques que anunciaron por las redes sociales fue a la página de internet *Hoonigan.com* la cual estuvo *down* por 3 días consecutivos. En las redes sociales dejaron saber que atacaron a sobre 2,000 escuelas y tomaban peticiones de estudiantes a cambio de dinero para crear amenazas falsas a la escuela solicitada. *Protonmail* fue una de las víctimas que logró conseguir información de los atacantes, ya que cuando atacaron lo hicieron con una cuenta creada en la página web mencionada.

Alcance:

Los servicios de *QNTM Auditing* fueron solicitados por *Hoonigan Industries* el 12 de diciembre tras sufrir varios ataques de *DDoS*. El propósito de la auditoría es asistir al equipo ejecutivo a desarrollar un plan de protección ante las vulnerabilidades expuestas. Un resumen detallado de los controles implementados previo al ataque, como detectar y mitigar la amenaza y cómo limitar las vulnerabilidades será incluido en la auditoría.

Objetivo:

El objetivo de la auditoría es proveer al cliente protección contra ataques *DDoS*, e identificar dónde están las vulnerabilidades. Detectar posibles áreas para reforzar y añadir *software* preventivo. Crear un manejo de crisis en caso de un ataque para mitigar pérdidas económicas y el impacto que puede tener.

Hallazgos:

1. Hallazgo: Falta de controles de seguridad contra ataques *DDoS* permitiendo que los mismos interrumpieran el servicio por 3 días corridos.
    a. Condición: Se comprobó que tienen que aumentar los servidores proveyendo servicio ya que el tráfico generado impidió continuidad del servicio.
    b. Criterio: De haber controles para prevenir el ataque y/o múltiples nubes dando servicio se pudo haber mitigado el daño.
    c. Causa: La falta de controles de seguridad y/o prevención permitieron que el servicio se interrumpiera.
    d. Efecto: 3 días consecutivos amontonaron a alrededor de $50,000.00 en pérdidas.
2. Hallazgo: Falta de parámetros de seguridad en la codificación PHP. Esto permitió que a través de un *SQL Injection* lograran jaquear la página del colegio de nueva granada.
    a. Condición: Las credenciales fueron expuestas y el código de *.php* fue modificado por medio de un *SQL Injection*.
    b. Criterio: Tener codificación como *mysqli_real_escape_string* para protegerse de los *SQL Injections* y utilizar el *HTTPS Protocol*.
    c. Causa: Al no tener los parámetros de prevención como el *HTTPS Protocol* establecidos el acusado pudo explotar las vulnerabilidades del sitio web.

d. Efecto: El impacto que tiene el ataque es más de nivel psicológico ya que el mismo expone la falta de seguridad de la página web. Al tener tanta información de estudiantes que pudo haber sido comprometida, hace cuestionar al estudiante si sus datos están seguros.

Recomendaciones:

1. Para prevenir ataques *DDoS,* vincular varios servicios de nubes y bases de datos para redirigir el tráfico, que a su vez permite más tiempo para detectar lo que está pasando.
2. Servicios/herramientas como *SUCURI* que proveen monitoreo constante contra ataques y respuestas inmediatas de haber alguna amenaza, Attard (2020).
3. En caso de las *SQL Injections* se recomienda establecer parámetros de seguridad como el *HTTPS Protocol* y constantemente monitorear la actividad. Otra opción viable es cambiar las credenciales constantemente.

7. Conclusión

Con el aumento periódico de crímenes digitales y/o cibernéticos nuestra profesión ha escalado en importancia. Durante el transcurso del bimestre he podido apreciar desde un punto más técnico los diferentes roles que existen en la seguridad cibernética. Existen múltiples fases que componen las funciones que debemos ejecutar, desde extraer información borrada previamente a realizar auditorías. Basado en la importancia de nuestro papel en una investigación, es imprescindible poder usar nuestras herramientas eficientemente.

El caso presentado contiene elementos de forense digital ya que evidencia fue encontrada en dispositivos electrónicos. La meta era examinarlo de manera constructiva para identificar, recuperar, analizar y presentar evidencia en corte. Se utilizaron las herramientas aprendidas en la maestría para poder cumplir con el objetivo exitosamente. Esta fue mi parte favorita, ya que además de interesante, es responsable de vincular o no al acusado de un acto ilícito.

Como parte del trabajo se realizó una auditoría, que tiene como objetivo mejorar la seguridad de los sistemas de información. Tras el análisis de los eventos, se buscó mejorar los parámetros de prevención, mitigar los riesgos y sugerir cambios para optimizar funcionamiento. Aunque cada vez existe mejor seguridad y software, de igual manera los ataques se han vuelto más sofisticados. Esto crea una alta demanda en el campo laboral ya que, puede visualizarse como un juego del gato y el ratón que nunca acaba.

8. Referencias

923. 18 U.S.C. § 371-Conspiracy to Defraud the United States. (2020, January 21). Recuperado de https://www.justice.gov/archives/jm/criminal-resource-manual-923-18-usc-371-conspiracy-defraud-us

Allen-Kinross, P. (2019, June 23). Mum of man who made school bomb threats says he was 'groomed' playing Minecraft. Recuperado de https://www.mirror.co.uk/news/uk-news/mum-man-jailed-school-bomb-16871129

Attard, D. (2020). Sucuri vs Sitelock - Which security service is best? (2020). Recuperado de https://www.collectiveray.com/sucuri-vs-sitelock

Chandel, R., & Chandel, R. (2015, May 19). How to gather Forensics Investigation Evidence using ProDiscover Basic. Recuperado de https://www.hackingarticles.in/how-to-gather-forensics-investigation-evidence-using-prodiscover-basic/

Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax. (2020, February 13). Recuperado de https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking

Cloudflare DDoS Protection: Intelligent DDoS Mitigation. (s.f.). Recuperado de https://www.cloudflare.com/ddos/

Dobran, B. (2020, January 10). 7 Proven Tactics To Prevent DDoS Attacks: Make a Security Plan Today! Recuperado de https://phoenixnap.com/blog/prevent-ddos-attacks

FBI (2018, December 20). Chinese Hackers Indicted.. Recuperado de https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018

National Institute of Technology (NIST). (n.d.).Cyber Threat. Recuperado de https://csrc.nist.gov/glossary/term/Cyber-Threat

Krebs on Security. (s.f.). Recuperado de https://krebsonsecurity.com/2019/02/bomb-threat-hoaxer-exposed-by-hacked-gaming-site/#more-46569

Legal Information Institute. (s.f.). 18 U.S. Code § 844 - Penalties. Recuperado de https://www.law.cornell.edu/uscode/text/18/844

Legal Information Institute. (s.f.). 18 U.S. Code § 875 - Interstate communications. Recuperado de https://www.law.cornell.edu/uscode/text/18/875

Nakashima, E., & Zapotosky, M. (2016, March 24). U.S. charges Iran-linked hackers with targeting banks, N.Y. dam. Recuperado de https://www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-goverment/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html

Newman, L. H. (2018, March 5). A 1.3-Tbs DDoS Hit GitHub, the Largest Yet Recorded. Recuperado de https://www.wired.com/story/github-ddos-memcached/

Petters, J. (2019, September 26). What is a Distributed Denial of Service (DDoS) attack?: Varonis. Recuperado de https://www.varonis.com/blog/what-is-a-ddos-attack/

Powell, M. (2019, December 30). 11 Eye Opening Cyber Security Statistics for 2019. Recuperado de https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019/

Rubenking, N. J. (2018). CryptoDrop Anti-Ransomware Review. Recuperado de https://www.pcmag.com/reviews/cryptodrop-anti-ransomware

United States v. Vaughn and Duke-Cohan (C.D. Cal., 2:19-cr-00071). (2019, February 8). Recuperado de https://www.courtlistener.com/docket/14726198/1/united-states-v-vaughn/

University, B. (s.f.). How to Protect Against SQL Injection Attacks. Recuperado de https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/how-protect-against-sql