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

APROPIACIÓN Y TRANSMISIÓN DE SECRETOS, FRAUDE DE CORREO, VIOLACIÓN DE USO Y POLÍTICA DE ACUERDOS

ANÁLISIS DE CASO: UNITED STATES v. DAVID NOSAL

Número de caso: 3:08-cr-00237-EMC

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

DICIEMBRE, 2019

PREPARADO POR

CARMELO GABRIEL CARABALLO RAMÍREZ

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

APROPIACIÓN Y TRANSMISIÓN DE SECRETOS, FRAUDE DE CORREO, VIOLACIÓN DE USO Y POLÍTICA DE ACUERDOS

Preparado por

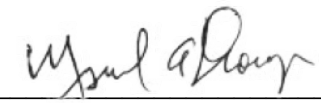
Carmelo Gabriel Caraballo Ramírez

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 Contenido

Lista de Ilustraciones

Sección 1 - Introducción y trasfondo del caso

Introducción

El interés para incurrir en la selección del caso Estados Unidos vs. David Nosal se debe a que en recientes años han surgido muchas noticias de infiltración de terceros, o personas cercanas, a compañías privadas para explotar y robar la información que se les confió. Este caso en particular es uno de muchos que se dan en el campo de crimen cibernético y su aplicación a las leyes establecidas en la década de los 1980. Con este caso se quiere fomentar, educar y persuadir a diferentes entidades y personas en el campo de las computadoras a incorporar controles y medidas de seguridad en los distintos sectores que administren información sensitiva de los usuarios. Su fin es crear conciencia entre personas, que permita ser este caso utilizado como herramienta y fuente de explicación de cómo la ingeniería social, malos controles de seguridad, y el uso de información personal para beneficio propio está costando millones de dólares (en el proceso) a la sociedad y empresas.

Número del caso

United States v. David Nosal and Becky Christian (Case 3:08-cr-00237-EMC)

Partes en el caso

Acusados

1. David Nosal
2. Becky Christian

Abogados y fiscales

- **Ministerio Público**: Jenny C. Ellickson, Lanny A. Breuer, Jaikumar Ramaswamy, Scott N. Schools, Kyle Francis Waldinger, del Departamento de Justicia de San Francisco, CA.
- **Abogados de Defensa**: Ted Sampsell Jones, Dennis P. Riordan, Donald M. Horgan, Riordan & Horgan, San Francisco, CA.
- **Amigos de la Corte**:
    1. Pointe Technologies, Inc. representado por Kathryn M. Davis, del bufete Kathryn M. Davis
    2. Oracle America Inc. representados Geoffrey M. Howard, David B. Salmons, Bryan M. Killian, Bingham McCutchen, LLP,
    3. Kenneth M. Stern, del bufete de abogados Kenneth M. Stern
    4. Electronic Frontier Foundation representado por Marcia Hofmann

Jueces

1. Marilyn H. Patel, Jueza Superior de Distrito, Distrito de California
2. Alex Kozinski, juez principal, Distrito de California

Hechos

Korn/Ferry International era una empresa de búsqueda de ejecutivos con sede en Los Ángeles, California. Korn y sucursales en Silicon Valley, San Francisco y otras oficinas en Estados Unidos y el mundo. Korn/Ferry fue uno de los principales proveedores servicios de búsqueda y reclutamiento de ejecutivos para empresas en los Estados Unidos.

El acusado David Nosal fue empleado por Korn/Ferry en su oficina de Silicon Valley y otros lugares desde aproximadamente abril de 1996 hasta aproximadamente octubre de 2004. Nosal ocupó varios puestos de alto nivel, incluido el puesto de Director Regional y Director

General de oficina. Este planeó comenzar su propia firma de búsqueda de ejecutivos después de terminar su empleo con Korn/Ferry a pesar de haber firmado un acuerdo donde pactó servir como contratista independiente para Korn/Ferry de 16 del noviembre de 2004 al 15 de octubre de 2005 a cambio de una remuneración de $25,000 mensuales por el término del contrato. Entre otras cosas, Nosal acordó cooperar con Korn/Ferry en ciertas tareas de búsqueda en curso y acordó no realizar tareas de servicios de búsqueda de talentos en nombre de cualquier otra entidad que no sea Korn/Ferry.

La acusada Becky Christian fue empleada de Korn/Ferry en su oficina de Silicon Valley y otras localidades desde septiembre de 1999 hasta aproximadamente enero de 2005. Después de renunciar a Korn / Ferry, Christian estableció una firma de búsqueda de ejecutivos conocida como *Christian & Associates, LLC*. Sin embargo, esta colaboró con Nosal para establecer su firma de búsqueda ejecutiva y le asistió en la conducción de varias búsquedas ejecutivas a cambio de retener el 20% de los ingresos producto de estas mientras que Nosal retenía el restante 80%.

Para realizar su trabajo, los empleados de Korn/Ferry dependían en gran medida de la base de datos *Searcher*, una base de datos altamente confidencial y exclusiva para ejecutivos y empresas. Esta base de datos también contenía información sobre los trabajos de búsqueda que Korn/Ferry había realizado para clientes en el pasado. Utilizando la función "Informe personalizado", los empleados podrían clasificar rápidamente la información en la base de datos para crear informes específicos sobre ejecutivos, empresas y trabajos de búsqueda anteriores para su uso en el desarrollo de candidatos para clientes y en presentaciones de clientes. La información contenida en la base de datos de *Searcher* fue producto de los esfuerzos de cientos de empleados de Korn / Ferry durante muchos años. Se considera una de las bases de datos de candidatos ejecutivos más completas del mundo.

La información de la base de datos de *Searcher* relacionada a búsquedas previas de Korn/Ferry incluía "listas maestras" (a lo que se le referían como "listas de candidatos"), generalmente descritas como listas de candidatos que Korn/Ferry presentaba a compañías clientes particulares para llenar plazas con dichos clientes. Korn/Ferry consideraban estas listas maestras de mucho valor a la hora de hacer búsquedas a altos ejecutivos para posiciones similares.

Korn/Ferry emprendió medidas considerables para mantener la información contenida en la base de datos *Searcher* confidencial. Dichas medidas incluían controlar el acceso electrónico y físico a la base de datos *Searcher* y sus servidores, respectivamente. Los empleados recibían nombres de usuarios y contraseñas únicos para acceder las computadoras y, a su vez, acceder a la base de datos *Searcher*. El uso de estas credenciales era para uso único y exclusivo de los empleados de Korn/Ferry.

A todos los empleados de Korn/Ferry (incluyendo a los demandados David Nosal y Becky Christian), se les requería firmar acuerdos en donde se estipulaban la naturaleza de la información provista por la base de datos *Searcher* era para uso exclusivo de los empleados de Korn/Ferry. Y la misma estaba restringida para uso solamente dentro de las facilidades de Korn/Ferry. Nosal ejecutó el acuerdo aproximadamente en abril 26, 1996. Christian a su vez ejecutó el acuerdo aproximadamente en 25 de septiembre de 1999.

Otras medidas implementadas por Korn/Ferry, implementaron la frase en inglés *Korn/Ferry Propietary Confidential* en cada reporte personalizado generado por la base de datos *Searcher*. Abundando, cada iteración de entrada por partes de los usuarios a las computadoras de Korn/Ferry, el sistema desplegaba la siguiente notificación, en suma y substancia:

> "Este sistema computarizado, la información que almacena y procesa son propiedad de Korn/Ferry. Usted necesita autorización específica para acceder cualquier dato o información de los sistemas Korn/Ferry y de este hacerse sin la debida autoridad puede conllevar a acciones disciplinarias o enjuiciamiento criminal…"

Trasfondo

David Nosal y Becky Christian son acusados por realizar actos de fraude y abuso de computadoras, conocido por el *Computer Fraud and Abuse Act* y sus siglas en inglés CFAA. Los mismos ocurrieron en Los Ángeles, California, en las sedes de *Korn/Ferry International*, empresa de búsqueda de ejecutivos profesionales. David Nosal solía trabajar con la empresa Korn/Ferry hasta octubre del 2004. Justo después de salir de la empresa convenció a varios colegas que seguían trabajando bajo Korn/Ferry que lo ayudaran a levantar su negocio propio y este ser competidor directo contra su patrono anterior. Los empleados usaron las credenciales dadas por la compañía Korn/Ferry para descargar información de contactos confidenciales de ejecutivos y clientes potenciales y estos van pasados a Nosal y su compañía nueva. Los empleados estaban autorizados a acceder la base de datos y su información, sin embargo, ese acceso estaba limitado solamente a la empresa de Korn/Ferry, según establecido en su política de confidencialidad. En el 2008 Nosal y otros tres empleados de Korn/Ferry fueron acusados con veinte cargos, incluyendo intercambio y robo secreto de información, fraude de correos, violación y conspiración de la CFAA.

Acusaciones, cargos y penalidades

Cargo 1:	18 U.S.C. § 1832(a)(5) & 371 - Conspiración para apropiarse indebidamente, recibir, poseer y transmitir secretos comerciales, obtener acceso no autorizado a una computadora protegida, exceder el acceso autorizado a una computadora protegida, exceder el acceso autorizado a una computadora protegida
Cargos 2 al 7:	18 U.S.C. §§ 1030(a)(4) & 1030(c)(3)(A) - Acceso no autorizado a una computadora protegida con la intención de defraudar y obtener algo de valor
Cargo 8:	18 U.S.C. §§ 1832(a)(1), 1832(a)(2) & 1832(a)(4) - Robo, apropiación indebida y descarga no autorizada de secretos comerciales
Cargos 9 y 10:	18 U.S.C. §§ 1832(a)(3) & 1832(a)(4) - Recibo no autorizado y posesión de secretos comerciales robados
Cargos 11 al 18:	18 U.S.C. § 1341 - Fraude de correo
Cargo 19:	18 U.S.C. § 1349 - Conspiración para cometer fraude postal

Penalidades

Cargo 1:	10 años de prisión, multa de $250,000 dólares o el doble de la ganancia o pérdida bruta, 3 años de libertad supervisada, evaluación especial de $100 dólares
Cargos 2 al 7:	5 años de prisión, multa de $250,000 dólares o el doble de la ganancia o pérdida bruta, 3 años de libertad supervisada, evaluación especial de $100 dólares
Cargo 8:	10 años de prisión, multa de $250,000 dólares o el doble de la ganancia o pérdida bruta, 3 años de libertad supervisada, evaluación especial de $100 dólares
Cargos 9 al 10:	10 años de prisión, multa de $250,000 dólares o el doble de la ganancia o pérdida bruta, 3 años de libertad supervisada, evaluación especial de $100 dólares
Cargos 11 al 18:	20 años de prisión, multa de $250,000 dólares o el doble de la ganancia o pérdida bruta, 3 años de libertad supervisada, evaluación especial de $100 dólares
Cargo 19:	20 años de prisión, multa de $250,000 dólares o el doble de la ganancia o pérdida bruta, 3 años de libertad supervisada, evaluación especial de $100 dólares

Definición de términos

- **Acceso o transmisión no autorizados**: La frase "excede el acceso autorizado" en la computadora Ley de fraude y abuso (CFAA), definida como "acceder a una computadora con autorización y usar dicho acceso para obtener o alterar información en la computadora a la que el usuario no tiene derecho obtener o alterar", abarca las personas que tienen solo acceso limitado a archivos o datos y excede restricciones en ese acceso, no aquellos que tienen acceso físico sin restricciones a una computadora pero usar la información almacenada allí para fines y propósitos no autorizados.
- **Derecho común o civil**: Bajo la presunción de que el Congreso actúa intersticialmente, el Tribunal de Apelaciones interpreta un estatuto como el desplazamiento de una parte sustancial de la ley común solo donde el Congreso tiene claramente indicó su intención de hacerlo.
- **Semejanza o diferencia**: Bajo un principio estándar de la ley construcción, palabras y frases idénticas dentro el mismo estatuto normalmente se le debe dar al mismo significado.
- **Construcción liberal o estricta; regla de lenidad**: La regla de lenidad requiere que las leyes penales se interpreten estrictamente; cuando hay que elegir entre dos lecturas de qué conducta ha hecho el Congreso delito, es apropiado, antes de que un tribunal elija la alternativa más dura, exigir que el Congreso debiese haber hablado en un lenguaje claro y definido.
- **Estados:** Debido a la gravedad de las sanciones penales, y porque el castigo penal generalmente representa la condena moral de la comunidad, legislaturas y no tribunales deben definir actividad criminal.

- **Base de datos:** Repositorio organizado y estructurado que contiene información indexada para facilitar su uso. La recuperación, actualización, análisis y salida es mucho más fácil de hacer de esta manera. Se almacena en una computadora mediante gráficos, informes, scripts, tablas y texto. El término no incluye software de computadora.
- **Ciber ley:** Área o ley en evolución que se aplica a las computadoras y las diversas actividades a través de Internet y las redes.
- **Cibercrimen:** Incluye cualquier tipo de esquema ilegal que use uno o más componentes de Internet (salas de chat, correo electrónico, tableros de mensajes, sitios web y subastas) para realizar transacciones fraudulentas o transmitir el producto del fraude a instituciones financieras u otras personas relacionadas con el esquema. El delito cibernético también se aplica a la generación de correos electrónicos no deseados, la descarga de virus o spyware a la computadora, el acoso a otro a través de Internet, la pornografía infantil y la solicitud de prostitución en línea. Quizás la forma más prominente de delito cibernético es el robo de identidad, en el que los delincuentes usan Internet para robar información personal de otros usuarios.
- **Fraude:** Se define generalmente en la ley como una tergiversación intencional de un hecho material existente hecho por una persona a otra con conocimiento de su falsedad y con el propósito de inducir a la otra persona a actuar, y sobre la cual la otra persona confía en la lesión o daño resultante. El fraude también se puede hacer por una omisión o una falla intencional de declarar hechos materiales, que no revelar hace que otras declaraciones sean engañosas.

Sección 2 - Revisión de literatura

Introducción

En relación con el caso *United States v David Nosal* se discutirá los fraudes involucrados presentado en diferentes artículos y referencias que sean pertinentes al caso escogido. Junto a las leyes aplicadas al acusado, incluyendo los subtítulos. Se estará cubriendo otros casos pertinentes, al igual que una breve explicación de cada uno y sus semejanzas.

Fraudes involucrados

Los fraudes que involucran el caso de *United States v David Nosal* son: La técnica de la ingeniera Social, Acceso No autorizado a computadoras, violación de uso y políticas de acuerdo de las computadoras, fraude de correo, apropiación y transmisión de secretos de negocio y tráfico de contraseñas. Bird y Dorvilier (2018) colaboran cómo la ingeniería social afecta a las aseguradoras. En el 2018 se recibieron cuatro casos en apelación que conllevan la misma estructura para ejecutar el fraude. Para propósitos de exposición al caso discutido, se presentarán dos casos. Segun Bird y Dorvelier: "el ladrón, pretendiendo ser un alto oficial de la aseguradora, envía un correo electrónico a un subordinado instrucciones para que transfiera dinero a un tercero." Abundan en su artículo: "… un ladrón pretende ser el vendedor tercero de una asegura y este le pide a la aseguradora que transfieran los fondos a la nueva cuenta." En ambos casos los ladrones se presentan como personas "legítimas" que forman parte del puesto que ocupan, sin embargo, a la hora de adquirir los fondos, estas personas utilizaban el correo electrónico de la persona, pero con una u otra alteración al mismo, lo que la persona, sin saber, cae en la trampa y envía los fondos sin percatarse de la discrepancia en el correo electrónico. Grabouski (2018) en su artículo *Is a Consensus Developing on Computer Fraud Coverage for E-mail Schemes?*

informa: “En el 2017 el FBI y el Centro de Crímenes y reclamos de la Internet (IC3, por sus siglas en inglés) recibió 301,580 reclamos cuyas pérdidas excedieron los 1.4 billones de dólares.” Añade la autora: “El fraude relacionado a los correos electrónicos se encuentra entre los tres crímenes más comunes y realizados de la Internet, esto va al lado de crímenes de fondos no pagados y violación de datos.” Esto desencadena una serie de eventos en los cuáles las víctimas no están aseguradas de que esos fondos sean retornados, ya que al momento de hacer la transferencia y este no dejar rastro, no mucho se puede hacer.

Bandler (2017) en su artículo *Cybercrime and Fraud Prevention for Your Home, Office and Clients,* comparte varios consejos de cómo prevenir el fraude en la oficina, hogar y con clientes, evitando los riesgos y amenazas relacionado al acceso no autorizado a las computadoras y protegernos contra el fraude y robo. Expone que el principio importante para la seguridad de la información es el CID: Confidencialidad, Integridad y Disponibilidad; propone que la confidencialidad mantiene la data segura de terceros de ser robada; la Integridad previene que la data sea dañada o corrupta por terceros, por ejemplo: *hackers* enviando correos electrónicos inapropiados utilizando la cuenta del implicado para apropiarse de información confidencial o dañar los récords de una base de datos de una empresa; disponibilidad es la manera de acceder los datos cuándo y dónde uno quiera. No obstante, Bandler nos advierte: “La confidencialidad y la disponibilidad a menudo están en desacuerdo. Estas pueden aumentar su nivel de seguridad y aumentar la confidencialidad de sus sistemas, pero a veces eso significa que tiene más dificultades para acceder a ellos.” Esto quiere decir que a un sistema contar con tantas medidas de seguridad, el usuario puede dejar alguna “puerta o gateway” abierta, haciendo de esta un acceso disponible para un *hacker* y dañar o robar la información de un sistema. El autor propone

sus recomendaciones bajo tres áreas: dispositivos, datos y redes para conceptualizar los principios de la ciberseguridad.

- Dispositivos
    - Todos podemos distraernos u olvidarnos, y abundan los ladrones callejeros oportunistas, mantenga los dispositivos móviles a su alcance. Revise la configuración del dispositivo y asegure una contraseña (o huella digital) para desbloquear y que se bloquean automáticamente después de un período de inactividad. Revise el software instalado, la configuración de privacidad y seguridad. El software debe provenir de proveedores confiables. Mantenga el sistema operativo y el software en sus dispositivos actualizados (parcheados) y ejecute un análisis de programa maligno en todos los datos en sus computadoras portátiles y de escritorio utilizando un producto antimalware de un proveedor confiable.
- Datos
    - Revise periódicamente sus datos, dónde están almacenados, cómo están protegidos y cuándo fueron respaldados. Organice sus datos y elimine de forma segura datos confidenciales innecesarios. Los datos confidenciales que salen de la casa u oficina, de un teléfono, tableta, computadora portátil o disco duro externo deben estar encriptados. Cuando deje de usar un dispositivo antiguo, asegúrese de que todos los datos se eliminen de forma segura antes de disponer del mismo. Cuentas en la nube asegúrelas con contraseñas y autenticación de dos factores (también llamada inicio de sesión en dos pasos). Habilitar el inicio de sesión en dos pasos ayuda a

evitar esto: incluso si el delincuente obtiene su contraseña, no puede acceder a la cuenta. Habilite la autenticación de dos factores para todas sus cuentas importantes de Internet y revise periódicamente todas sus configuraciones de seguridad y privacidad.

- Redes
    - Evite o limite su uso de *Wi-Fi* público, use comunicación encriptada siempre que sea posible. Por ejemplo, un sitio web *HTTPS* encripta su comunicación con usted, mientras que un sitio web *HTTP* no lo hace. La mayoría de los proveedores de correo electrónico ahora encriptan las comunicaciones, y esto proporciona una protección considerable en estas redes compartidas.

Rawson (2017) en el artículo *Everything you need to know about Internet & Computer Usage Policies and why your company needs one,* propuso que para el año 2008 el 45% de las compañías monitorean las actividades hechas por sus empleados. El artículo nos ofrece sus razones para reforzar el monitoreo. El autor apunta que empleados hacen descargas ilegales utilizando el Internet de la empresa, el mismo señala: “Las tecnologías de igual a igual se pueden utilizar para descargar archivos ilegales, incluyendo material protegido por derechos de autor que se castiga con diversas leyes federales.” Sin embargo, el autor cuestiona si el mismo aplica para los casos en que se haga *data mining* con monedas virtuales como *Bitcoin,* ya que se pueden dar casos en que pueden hacer “excavaciones” de datos, pero su intención puede ser otra, como descargar algún programa o documentación privada, lo que hace implementar una póliza de seguridad un “área gris”, nos explica Rawson. Para combatir estas y otras discrepancias, Rawson menciona varias soluciones para el monitoreo de las computadoras, entre estas se encuentran:

OpenDNS, Nagios, Staff Cop, o Time Doctor. También menciona bloqueadores de páginas a nivel de empresa como Fortinet, que limita el acceso a varios sitios web y evitan que sucedan casos de apropiación ilegal de documentos o descargas ilícitas. Promueve, también, pólizas por escrito que sean actualizadas anualmente y guardadas en el perfil de cada empleado, esto asegura que "… al momento de ser aprehendido un empleado, el documento estará en su perfil para repasar la violación que hizo." Explica Rawson en entrevista con Tim New, manejador de la empresa *Onsite Logic*, basado en Kansas, empresa que ayuda a pequeños negocios a establecer pólizas y uso de computadoras y monitoreo.

CBS (2019), en conjunto con *Associated Press*, informa que Ammon Yule, sargento veterano de la guardia nacional, fue acusado de fraude de correo tras ordenar mercancía de una distribuidora militar y luego venderlos por Internet. El retirado de 42 años, residente de Chittenden, Vermont, fue acusado de tres cargos de malversación de propiedad del contribuyente y tres cargos de fraude de correo. El veterano es acusado de ordenar equipos, incluyendo bultos, botas y equipo de ropa militar de una distribuidora militar en Kentucky y vendiéndolos en el sitio web *eBay* por espacio de un año. La imputación presenta que el acusado puede estar sentenciado a quince meses en prisión y, adicional, ha causado pérdidas de hasta $150,000 a la milicia.

La compañía de China *Huawei* se encuentra bajo investigación por el gobierno de los Estados Unidos por alegado robo de secretos y de propiedad intelectual por Benner, Mozur y Zhong para el periódico *New York Tumes.* La investigación contra *Huawei* se debe a que el mismo en el año 2014 se apropió, aparentemente, de propiedades intelectuales relacionado a un robot que utiliza la compañía de telecomunicaciones *T-Mobile* para diagnosticar situaciones de calidad de control en llamadas hechas por clientes. No es la primera que *Huawei* está bajo el ojo del buró federal estadounidense. A principios del año 2019 el FBI se encontraba en trámites de

extraditar a la directora financiera de *Huawei*, Meng Wanzhou, quien se encontraba en Canadá. Se presume que la hija del fundador de la compañía China engañó a los bancos sobre los negocios de Huawei en Irán, haciendo que violaran las sanciones estadounidenses contra Irán sin darse cuenta. A costa del incidente mencionado y otros contra *Huawei*, Estados Unidos crea un proyecto de ley para restringir el acceso a tecnologías, tales como microchips y sistemas operativos, y esta sea implementadas a sus tecnologías y vendidas al mundo. No tan solo *Huawei* está afectada por esta ley, la compañía *ZTE*, también de China, violó sanciones de Estados Unidos y tiene restricciones para comprar y vender en los Estados Unidos. Los autores abundan:

> Los ejecutivos de *Huawei* han negado anhelar que la compañía actúe en nombre de cualquier gobierno. Pero los agentes de contrainteligencia estadounidenses y los fiscales federales han explorado durante algún tiempo posibles casos contra el liderazgo de la compañía. La demanda de *T-Mobile* no fue la primera vez que *Huawei* fue acusada de robar propiedad intelectual. En 2003, la compañía admitió que había robado partes del software que ejecuta equipos de redes de computadoras de *Cisco Systems*, una de las compañías tecnológicas más grandes de *Silicon Valley*. *New York Times, 2019.*

En un caso tan reciente como en octubre del 2019 el pasado director de cumplimiento de la firma de gestión de activos *GPB Capital Holdings,* Michael Cohn, fue acusado, según se alega, por: "… acceder información lo cual no estaba autorizado a acceder servidores de la División de Investigación de *GPB* en donde él asistió a investigadores de la SEC en una violación de leyes de seguridad", cita Jaeger (2019). Se indica que Cohn: "… aprovechó la información obtenida con respecto a la investigación de la SEC sobre GPB y, en varias ocasiones, reveló información a los miembros de la alta gerencia de GPB sobre la investigación, dijo el Departamento de Justicia." Al hacer esto obstruye la investigación activa por parte de

SEC, lo que lleva a ser acusado por apropiación de secretos de negocio y violación de políticas y uso de las computadoras. El acusado, de encontrarse culpable, enfrentaría una sentencia máxima de veinte años sobre el cargo de obstrucción de la justicia, un máximo de cinco años de prisión por el acceso no autorizado a la computadora, y un máximo de un año en prisión por el cargo de divulgación no autorizada.

Leyes aplicables

- 18 U.S.C. § 1030 - Fraude y actividades relacionadas en conexión con computadoras §§ 1832(a)(5) - Robo de secretos comerciales & 371 - Conspiración - Quien a sabiendas causa la transmisión de un programa, información, código o comando, y como resultado de tal conducta, intencionalmente causa daño sin autorización, a una computadora protegida; accede intencionalmente a una computadora protegida sin autorización y, como resultado de dicha conducta, causa daños de manera imprudente; o accede intencionalmente a una computadora protegida sin autorización, y como resultado de tal conducta, causa daños y pérdidas. 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 estos 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.
- 18 U.S.C. § 1030 - Fraude y actividades relacionadas en conexión con computadoras §§ 1030(a)(4) & 1030(c)(3)(a) – Quien a sabiendas y con la intención de defraudar, accede a una computadora protegida sin autorización, o excede el acceso autorizado, y por medio

de tal conducta fomenta el fraude previsto y obtiene algo de valor, a menos que el objeto del fraude y lo obtenido consista solo en el uso de la computadora y el valor de dicho uso no es más de $ 5,000 en un período de 1 año. El castigo por un delito bajo el inciso (a) o (b) de esta sección es una multa bajo este título o prisión por no más de cinco años, o ambos, en el caso de un delito bajo el inciso (a) (4) o (a) (7) de esta sección que no se produce después de una condena por otro delito en virtud de esta sección, o un intento de cometer un delito punible en virtud de este párrafo.

- 18 U.S.C. §§ 1832(a)(1), 1832(a)(2) & 1832(a)(4) - Robo de secretos comerciales – Quien, con la intención de convertir un secreto comercial, que esté relacionado con un producto o servicio utilizado o destinado a ser utilizado en el comercio interestatal o extranjero, en beneficio económico de cualquier persona que no sea el propietario del mismo, y con la intención o el conocimiento de que el delito, lesionar a cualquier propietario de ese secreto comercial, robar a sabiendas, o sin autorización apropiarse, tomar, llevar u ocultar, o por fraude, artificio o engaño obtiene dicha información; sin autorización, copias, duplicados, bocetos, dibujos, fotografías, descargas, cargas, modificaciones, destrucciones, fotocopias, réplicas, transmisiones, entregas, envíos, correos, comunicaciones o transmisión de dicha información; intenta cometer cualquier delito descrito en los párrafos (1) a (3).
- 18 U.S.C. §§ 1832(a)(3), 1832(a)(4) - Robo de secretos comerciales – Quien, con la intención de convertir un secreto comercial, que esté relacionado con un producto o servicio utilizado o destinado a ser utilizado en el comercio interestatal o extranjero, en beneficio económico de cualquier persona que no sea el propietario del mismo, y con la intención o el conocimiento de que el delito , dañar a cualquier propietario de ese secreto

comercial, a sabiendas recibe, compra o posee dicha información, sabiendo que la misma ha sido robada o apropiada, obtenida o convertida sin autorización; intenta cometer cualquier delito descrito en los párrafos (1) a (3).

- 18 U.S.C. § 1341 - Fraudes y estafas - Quien haya ideado o tenga la intención de idear algún esquema o artificio para defraudar, o para obtener dinero o propiedad por medio de pretensiones, representaciones o promesas falsas o fraudulentas, o para vender, disponer, prestar, intercambiar, alterar, regalar, distribuir, suministrar o suministrar o procurar para uso ilegal cualquier moneda falsificada o espuria, obligación, seguridad u otro artículo, o cualquier cosa representada o intimidada o presentada como tal artículo falso o falso, con el fin de ejecutar dicho esquema o articular o intentar hacerlo, lugares en cualquier oficina de correos o depósito autorizado para correo, cualquier asunto o cosa que sea enviada o entregada por el Servicio Postal, o depósitos o causas para ser depositados cualquier cosa o cosa que sea enviada o entregado por un transportista interestatal privado o comercial, o toma o recibe del mismo, cualquier asunto o cosa, o intencionalmente hace que se entregue por correo o dicho transportista de acuerdo con la dirección al respecto, o en el lugar en el que se dirige a ser entregado por la persona a quien se dirige, cualquier asunto o cosa, 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.

- 18 U.S.C. § 1349 – Fraude por correo y otras ofensas por fraude - Cualquier persona que intente o conspire para cometer un delito en virtud de este capítulo estará sujeta a las mismas sanciones que las prescritas para el delito, cuya comisión fue el objeto del intento o la conspiración.

Casos relacionados

- LVRC Holdings LLC v. Brekka (2009) – El hallazgo de este caso es que el empleado accede a una computadora con propósitos inapropiados, aun violando la lealtad del patrono, el empleado permanece autorizado para acceder a la computadora hasta que el patrono revoque el acceso. Las semejanzas o diferencias de este caso con el escogido es que Nosal no tenía los accesos suyos para acceder y tomar la información de los clientes, sin embargo, utiliza las de Becky Christian, "J.F" y "M.J" para obtener dicha información para beneficio propio.
- United States v. Drew (2009) – Caso que cargó a Lori Drew de violar *Computer Fraud and Abuse Act (CFAA*, por sus siglas en inglés), sobre el alegado acoso-cibernético contra una niña de 13 años llamada Megan Meir, quien cometió suicidio utilizando la red social *Myspace*. Las semejanzas y diferencias de este y el escogido son las violaciones al acceso no autorizado a una computadora.

- International Airport Centers, LLC v. Citrin (2006) - Jacob Citrin era empleado de IAC, quien le había prestado una computadora portátil para usar mientras trabajaba. Al abandonar IAC, eliminó los datos de la computadora provista de la compañía usando un software *secure-erasure* antes de devolverlos a IAC, destruyendo los datos recolectado para IAC haciéndolos irrecuperables. El Tribunal de Apelaciones decidió revocar la decisión y restableció la demanda de IAC. Semejanzas y diferencias de los casos son que la relación entre empleado y patrono terminan, por ende, los accesos que el mismo tenía con el patrono. Y, por otro lado, la información adquirida durante el tiempo con un patrono es propiedad del patrono y no del empleado, aunque haya sido creado por el antes mencionado.

Sección 3 – Descripción y Simulación de los hechos

Descripción

Korn/Ferry es una firma de consultoría global de búsqueda de talentos. Su base de datos, S*earcher,* fue producto de los esfuerzos de cientos de empleados de Korn/Ferry durante muchos años y se considera una de las bases de datos de candidatos ejecutivos más completas del mundo. David Nosal solicitaba información a Becky Christian junto con dos empleados más de Korn/Ferry para su nueva compañía. A pesar de haber firmado un acuerdo de no competencia al haber finalizado su contrato en octubre de 2005, Nosal decidió crear su empresa de búsqueda de talentos y solicitó la ayuda de Becky Christian y otros dos empleados para extraer información de la base de datos de Korn/Ferry. Los empleados accedían a la base de datos *Searcher* para extraer la data de la "lista de candidatos" de clientes potenciales de Korn/Ferry. La información de la base de datos *Searcher* incluía la "lista de candidatos" que Korn/Ferry consideraba extremadamente valiosas a la hora de hacer búsquedas de ejecutivos con posiciones similares. Al obtener los datos de la lista de candidatos de *Searcher,* estos eran enviados a Nosal para ser utilizados en su nueva compañía.

Nosal pedía la información de la base de datos *Searcher* a Becky Christian y otros dos empleados de Korn/Ferry.

Los empleados que trabajaban en la empresa Korn/Ferry por años utilizaban sus credenciales para acceder a la base de datos Searcher y extraer la información solicitada.

Utilizando sus credenciales, Becky Christian y los dos empleados de Korn/Ferry extraían de *Searcher* la lista de candidatos de ejecutivos importantes de la compañía y se la enviaban a Nosal.

Nosal recibía la lista de candidatos de Koen/Ferry para ser utilizados para su firma de búsqueda de candidatos.

Ilustración 1 – Simulación de los hechos entre David Nosal; firma Korn/Ferry y Searcher.

Sección 4 - Informe Forense del Caso

Resumen ejecutivo

El empleado David Nosal es acusado de usar acceso y credenciales corporativas para lucro personal por medio de otros empleados de la firma de búsqueda de ejecutivos Korn/Ferry. Se sospecha que el Sr. Nosal violó el acuerdo entre él y Korn/Ferry extrayendo datos de la base de datos para su compañía luego de salir de la firma Korn/Ferry. El Fiscal Sergio Leone hace entrega a Carmelo G. Caraballo Ramírez de un dispositivo USB de capacidad de 1 GB (gigabyte) conteniendo una imagen de la computadora del acusado incautada durante el proceso investigativo y un extracto de la base de datos *Searcher* de la compañía Korn/Ferry para investigar posible evidencia que relacione al acusado con los hechos de este caso.

Dentro del dispositivo USB se encontró archivos en formato Excel que contiene datos de varias personas de alto poder ejecutivo que se presumen fueron extraídos de la base de datos de la empresa Korn/Ferry. Se extrajo de la base de datos *Searcher* una muestra que contiene información sensitiva encontrada en la máquina que se presume fue utilizada por los implicados en el caso.

Objetivo

El objetivo de la investigación es analizar un dispositivo USB y un extracto de la base de datos *Searcher* en la cual la firma es propietaria como posible fuente de evidencia de posibles actos fraudulentos realizados por los acusados.

Alcance del trabajo

El día 19 de noviembre de 2019 el fiscal federal Sergio Leone le hace entrega a Carmelo G. Caraballo Ramírez (Investigador Forense de CG Ciber-Security Services) de un dispositivo USB visto por la fiscalía como posible dispositivo contenedor de evidencia y archivos comprometedores de la base de datos *Searcher*. Esto con el propósito de analizar el mismo ya que existe el interés de encontrar datos incriminatorios y clientes involucrados que sirvan como evidencia inculpatoria en el caso del Sr. David Nosal, el cual trabajó para la firma Korn/Ferry por espacio de 8 años. CG Ciber-Security Services tiene la tarea de descubrir, recuperar y preservar cualquier evidencia relevante encontrada en el dispositivo USB con el propósito de ser analizada y posteriormente ser presentada como evidencia por el fiscal Leone.

Dejando esto establecido CG Ciber-Security Services comienza con el proceso de adquisición y análisis de evidencia. CG Ciber-Security Services creará un informe de hallazgos y los notificará por medio escrito al fiscal Sergio Leone para ser evaluados y tomar la acción legal correspondiente con relación a los acusados David Nosal y Becky Christian en los incidentes en cuestión.

- *AccessData Forensic Toolkit-FTK Version 1.81.6 build 10.04.02* usada en Windows 10 Pro para analizar el dispositivo USB.
- *Microsoft SQL Server Management Studio* Versión 14.0.17289.0 para ejecutar consultas de la base de datos *Searcher.*
- Microsoft Excel 2016 para ver la información incautada del dispositivo USB.

Datos del caso

- Número del caso: 3:08-cr-00237-EMC
- Investigador: Carmelo G. Caraballo Ramírez
- Cliente solicitante de la investigación: Korn/Ferry
- Representante del cliente: Sergio Leone (fiscal)

Descripción de los dispositivos utilizados

- Laptop Huawei, modelo MateBook X Pro donde residen todas las herramientas y aplicaciones que serán utilizadas en este proceso.
- Dispositivo USB incautado como evidencia. Entregado a CG Ciber-Security Services por el fiscal Leone.

Resumen de hallazgos

A continuación se muestran hallazgos identificados durante la examinación forense entregado por el fiscal Sergio Leone:

1. Correo electrónico inicial entre David Nosal y MJ (Ilustración 1). Nosal le comunica a MJ peticionando información de altos ejecutivos de la base de datos *Searcher*. MJ procede a enviar correo a JF con instrucciones a seguir.

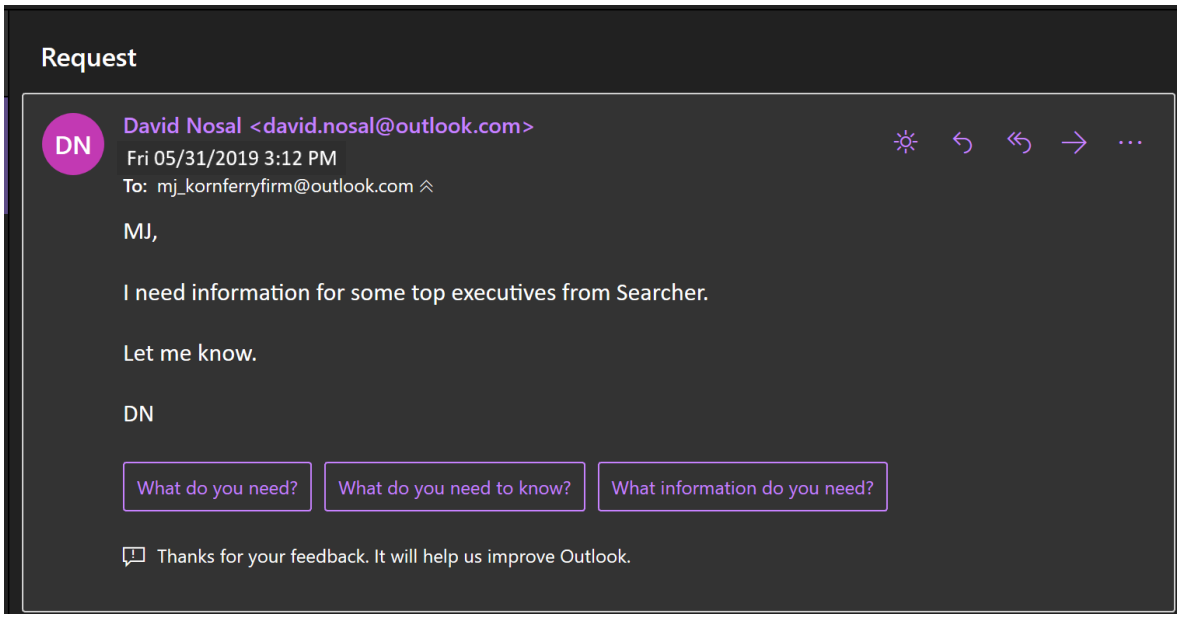


Ilustración 2 - Petición de Nosal a MJ

2. Correo electrónico de JF (Ilustración 2) recibiendo instrucciones de MJ en detalle de la base de datos *Searcher* y extraerlo como informe.

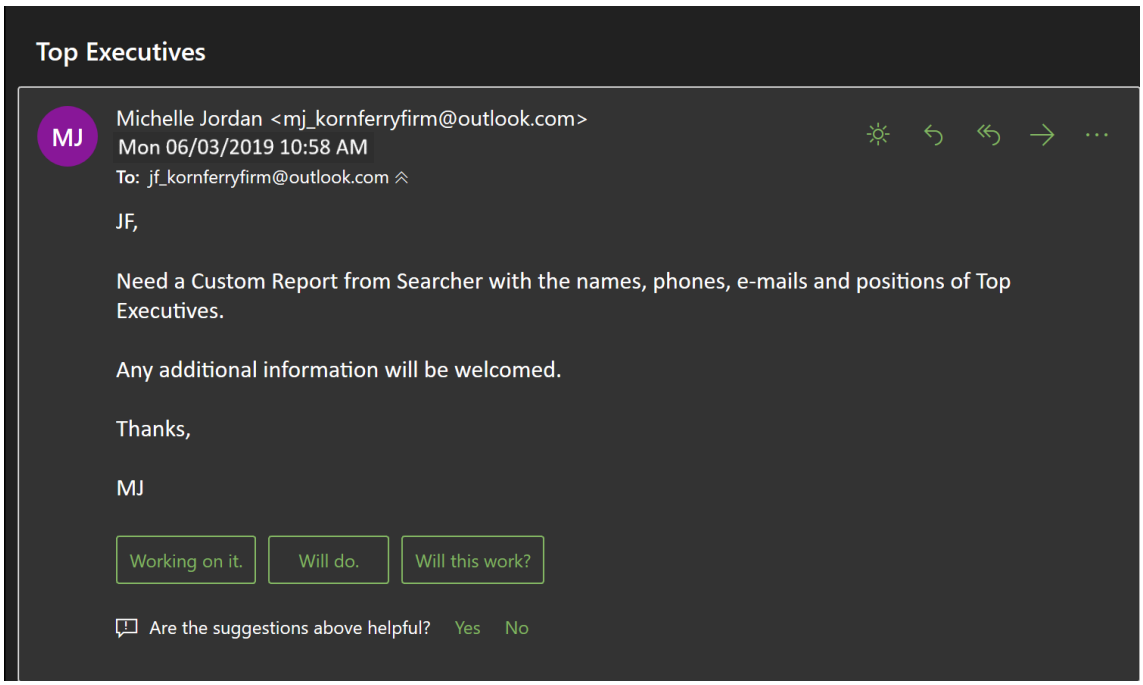


Ilustración 3 - Petición de MJ a JF.

3. Archivo Excel identificado como *Choc Chip Cookies Recipes.xlsx (Ilustración 3).* El archivo muestra un listado de nombres, teléfonos, *e-mails* y posición a cargo. Este archivo fue hallado en el dispositivo USB incautado de las nuevas facilidades de David Nosal.

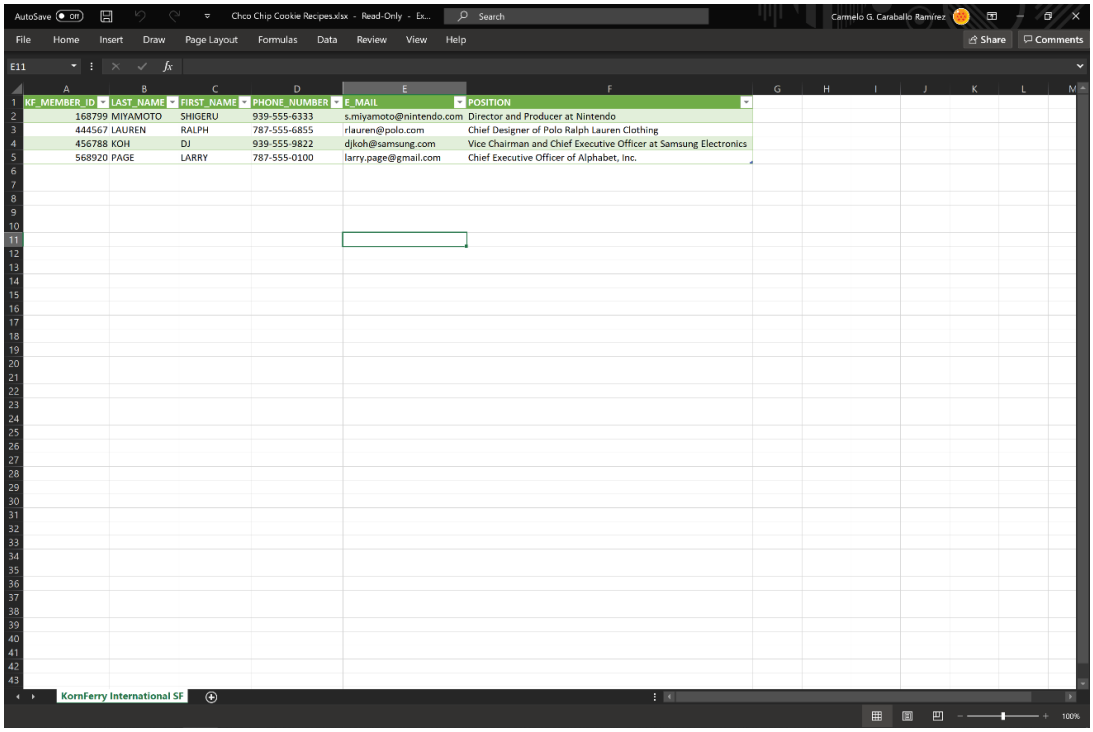


Ilustración 4 - Archivo Excel original del dispositivo USB

4. Extracto de la base de datos *Searcher* (Ilustración 4) donde muestra los datos del archivo Excel mostrando en la Ilustración 3 junto con otras personas adicional. En la sección de Procedimientos muestra cómo se llegó a obtener la información que llevaba a la base de datos *Searcher*.

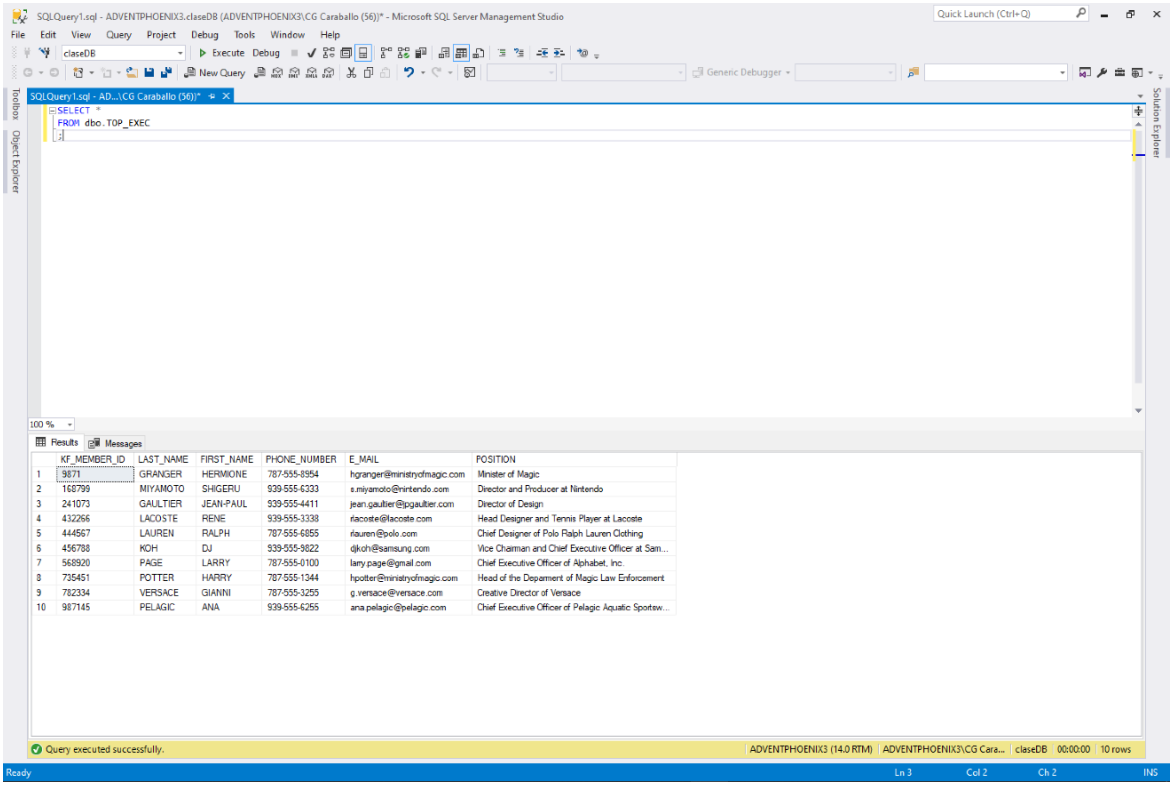


Ilustración 5 - Extracto de Searcher

Cadena de custodia

Al comenzar nuestro proceso debemos asegurarnos de establecer una cadena de custodia de evidencia integra. La cadena de custodia se ocupa de notarizar el proceso de adquisición, análisis y control de toda evidencia. En el siguiente documento se detalla la cadena de custodia seguida por CG Ciber-Security Services:

Detalle de la cadena de custodia:

Primer evento:

- **Descripción del evento:** Evidencia recogida en el cuarto de evidencias del FBI. Evidencia entregada por el fiscal Sergio y adquirida por el Sr. Carmelo G. Caraballo Ramírez, investigador de CG Ciber-Security Services. La evidencia consiste en: Imagen de dispositivo USB y extracto de la base de datos *Searcher* de la empresa Korn/Ferry.
- **Evento verificado por:** Carmelo G. Caraballo Ramírez y Sergio Leone.
- **# de evidencia:** E-1-2019-11-19
- **Fecha de comienzo:** noviembre 19, 2019 – 12:40 PM
- **Fecha de terminación:** abril 19, 2019 – 12:40PM
- **Lugar de origen:** Cuarto de evidencias oficina FBI
- **Destino:** Laboratorio forense – CG Ciber-Security Services

Segundo evento:

- **Descripción del evento:** Creación de número de caso y asignación de evidencia al mismo.
- **Evento verificado por:** Carmelo G. Caraballo Ramírez
- **# de evidencia:** Evidencia # E-1-2019-11-19 - Asignada al caso # 3:08-cr-00237-EMC
- **Fecha de comienzo:** noviembre 19, 2019 – 2:04 PM
- **Fecha de terminación:** noviembre 19, 2019 – 2:26 PM

- **Lugar de origen:** Laboratorio forense – CG Ciber-Security Services
- **Destino:** Laboratorio forense – CG Ciber-Security Services.

Tercer evento:

- **Descripción del evento:** Proceso de adquisición y análisis de evidencia. Refiérase a la sección de procedimientos en este reporte para detalles específicos del proceso.
- **Evento verificado por:** Carmelo G. Caraballo Ramírez
- **# de evidencia:** Evidencia # E1-2019-11-22 – Asignada al caso # 3:08-cr-00237-EMC
- **Fecha de comienzo:** noviembre 22, 2019 – 3:51 PM
- **Fecha de terminación:** noviembre 29, 2019 – 9:43 PM
- **Lugar de origen:** Laboratorio forense – CG Ciber-Security Services
- **Destino:** Laboratorio forense – CG Ciber-Security Services

Cuarto evento:

- **Descripción del evento:** Entrega de informe de análisis forense al fiscal Sergio Leone para su evaluación. El informe fue entregado directamente al fiscal Ruiz por el investigador a cargo de la evidencia, Carmelo G. Caraballo Ramirez
- **Evento verificado por:** Carmelo G. Caraballo Ramírez
- **# de evidencia:** Reporte referente a la evidencia #E1-2019-11-30 – Asignada al caso # 3:08-cr-00237-EMC
- **Fecha de comienzo:** noviembre 30, 2019 – 8:30 AM
- **Fecha de terminación:** noviembre 30, 2019 – 5:45 PM

- **Lugar de origen:** Laboratorio forense – CG Ciber-Security Services
- **Destino:** Oficina del fiscal federal Sergio Leone fiscal solutions.

Quinto evento:

- **Descripción del evento:** Devolución de la evidencia original entregada por el fiscal Sergio Leone a Carmelo G. Caraballo Ramírez. La evidencia fue entregada directamente al fiscal Sergio Leone por el investigador a cargo de la evidencia, Carmelo G. Caraballo Ramírez
- **Evento verificado por:** Carmelo G. Caraballo Ramírez y Sergio Leone
- **# de evidencia:** Evidencia # E1-2019-11-30 – Asignada al caso # 3:08-cr-00237-EMC
- **Fecha de comienzo:** noviembre 30, 2019 – 08:30 AM
- **Fecha de terminación:** noviembre 30, 2019 – 1:30 PM
- **Lugar de origen:** Laboratorio forense – CG Ciber-Security Services
- **Destino:** Cuarto de evidencias oficina FBI.

Procedimiento

A continuación, se describen los procedimientos empleados durante el proceso de descubrimiento, adquisición, recuperación y preservación de la evidencia.

1. **Procedimiento: creación del caso, análisis de la imagen, revalidación y reporte**

    a. Herramienta: *FTK Pro Toolkit*

b. Fecha: noviembre 27, 2019

c. Fecha de comienzo**:** noviembre 22, 2019 - 4:47 PM

d. Fecha de terminación**:** noviembre 29, 2019 - 11:44 PM

e. Descripción: Procesamiento del archivo formato Excel para obtener posible evidencia inculpatoria y probar la hipótesis de fiscalía federal. Se buscarán documentos existentes y borrados.

En este punto se procesará toda la data obtenida con *FTK Forensic Toolkit* 1.81.6 para revalidar los resultados y crear un reporte automatizado, así como una base de datos con toda la evidencia debidamente catalogada.

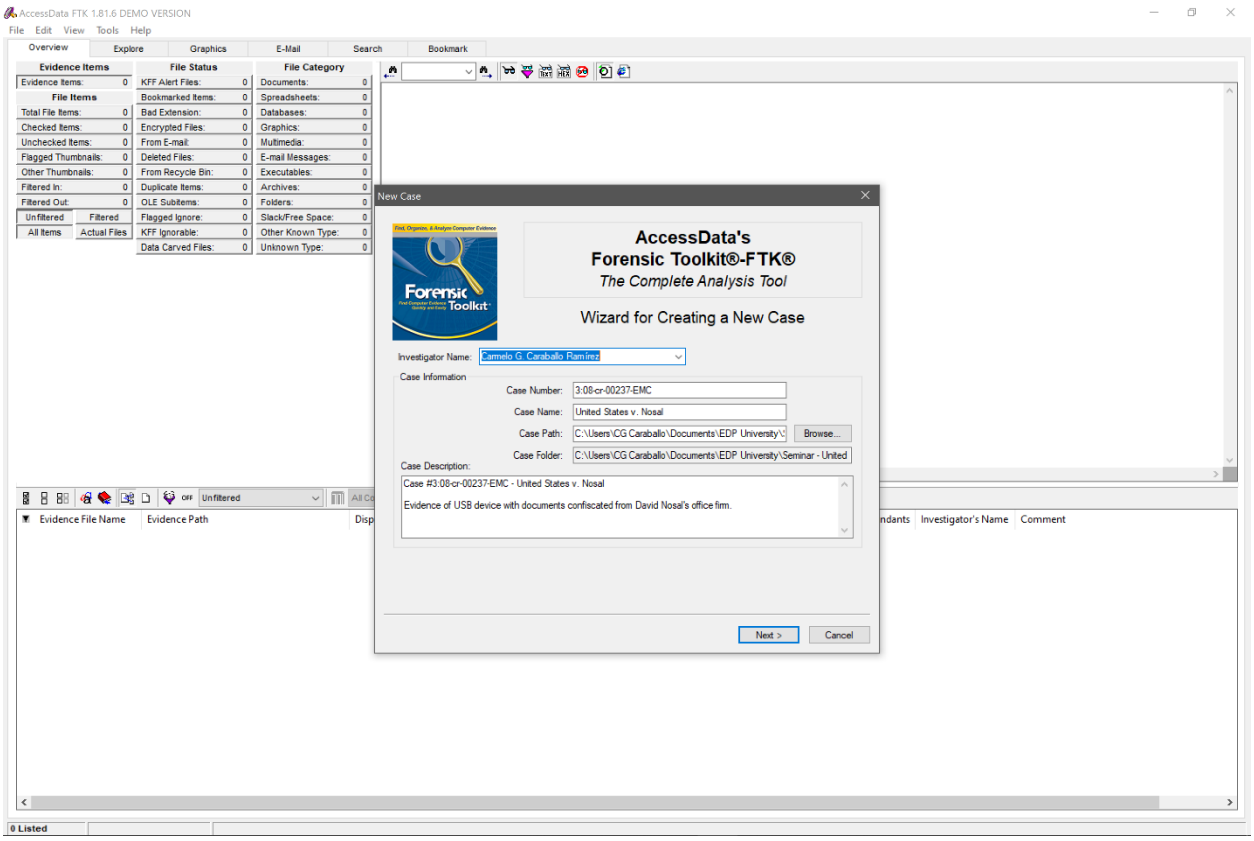


Ilustración 6 - Creación del caso via FTK Toolkit.

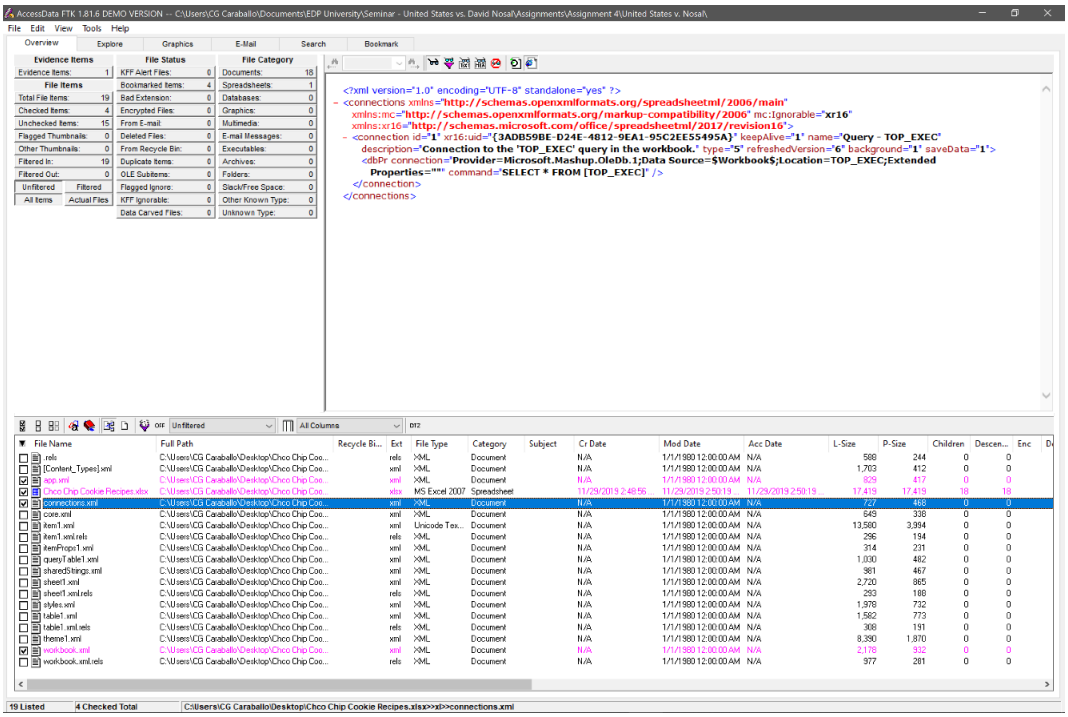


Ilustración 7 - Conexión y tabla de base de datos.

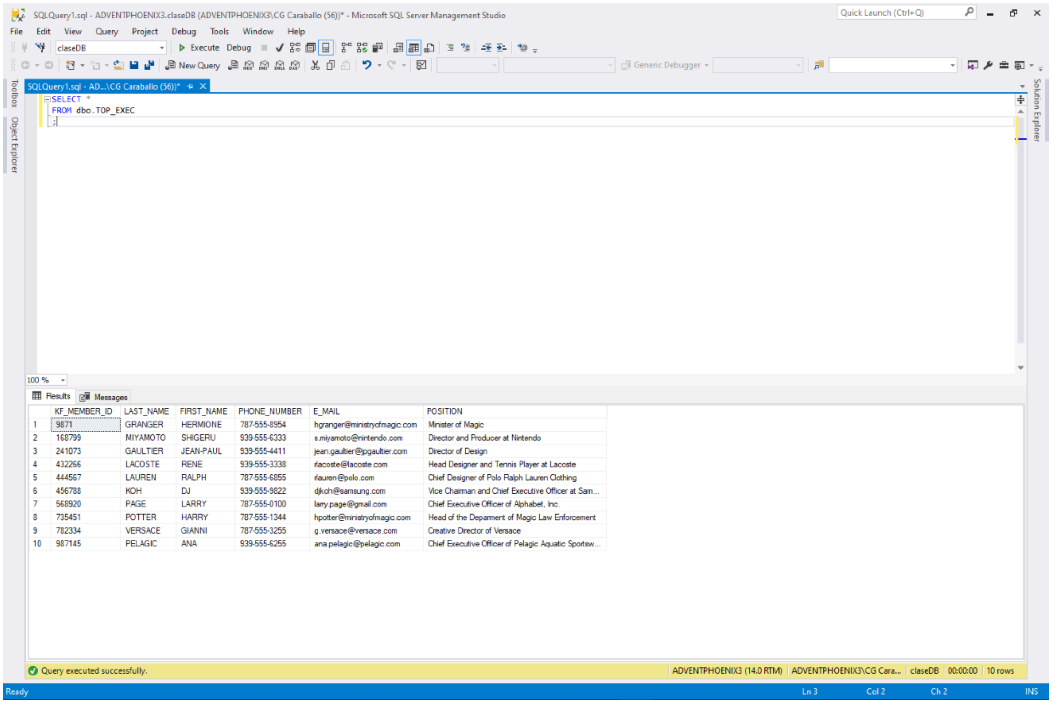


Ilustración 8 - Extracción de la base de datos Searcher basada en los datos del archivo Excel.

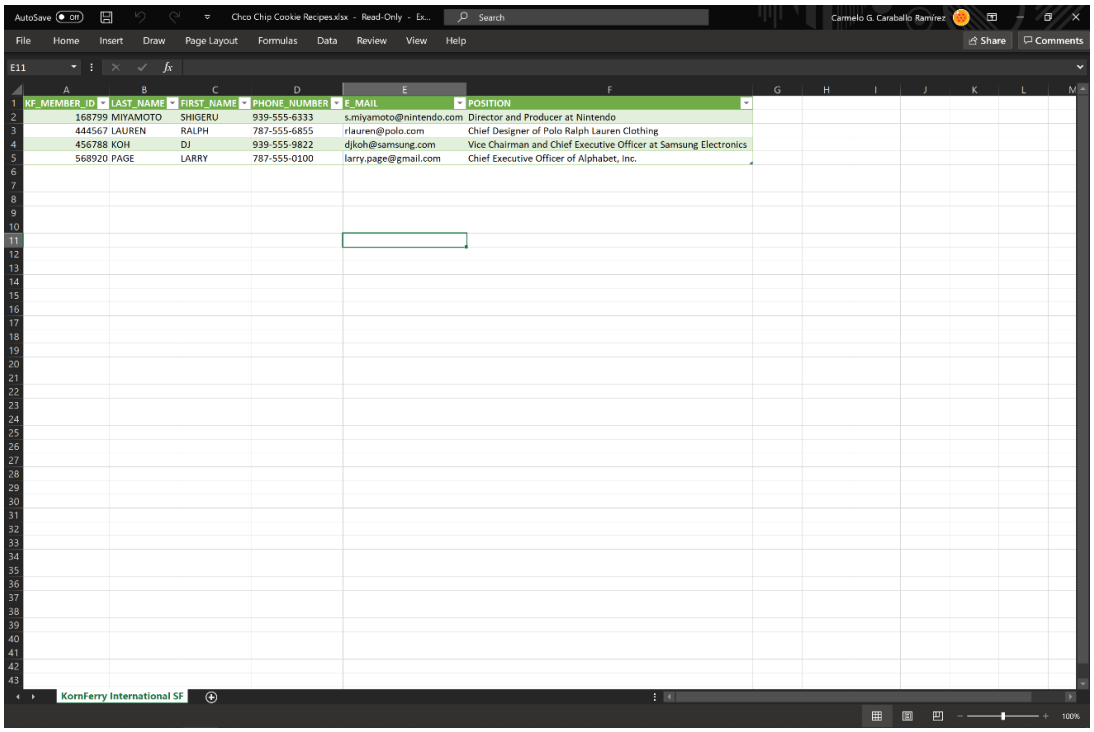


Ilustración 9 - Archivo Excel original del dispositivo USB.

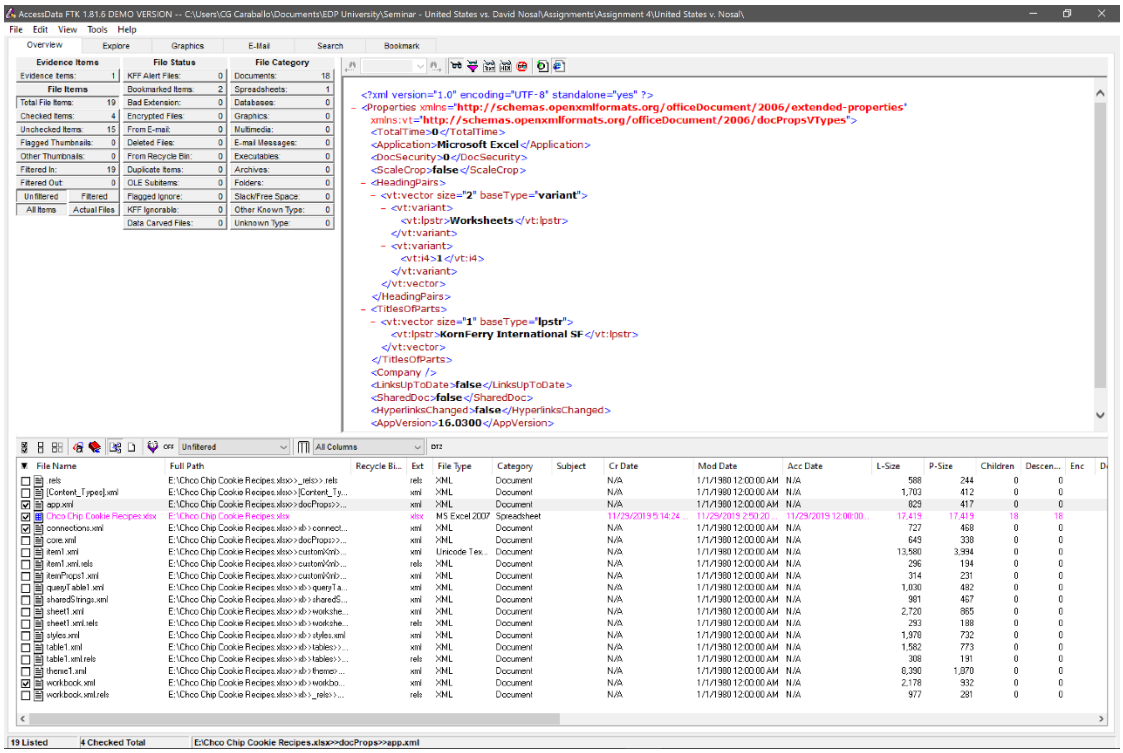


Ilustración 10 - Información adicional del archivo Excel.

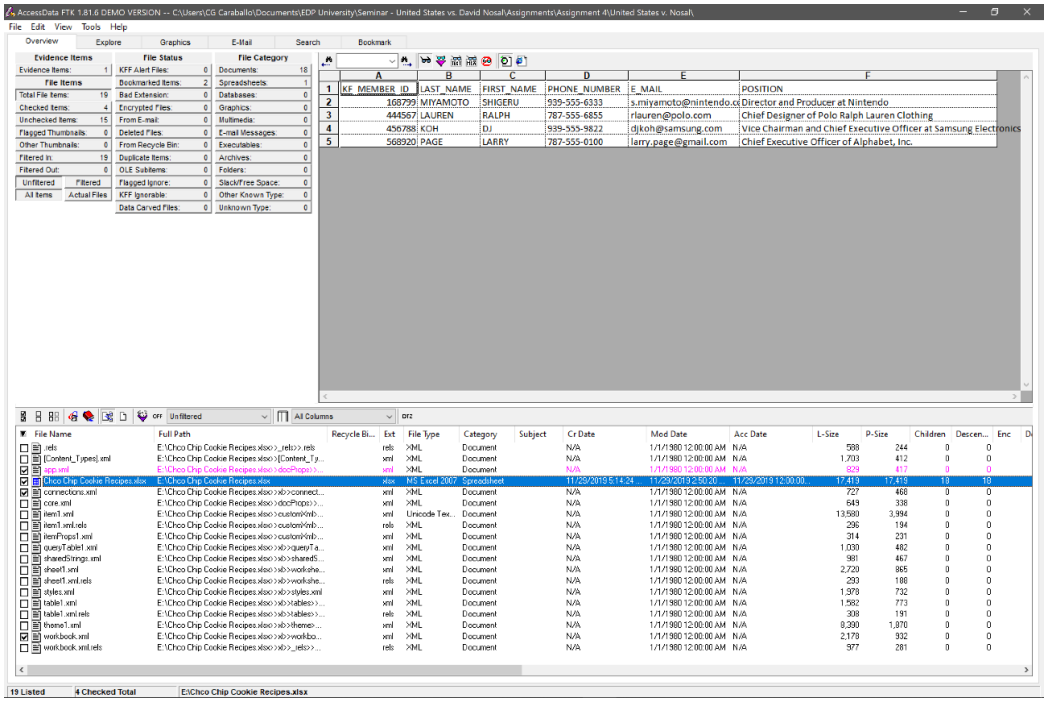


Ilustración 11 - Datos de la extracción mediante FTK Toolkit.

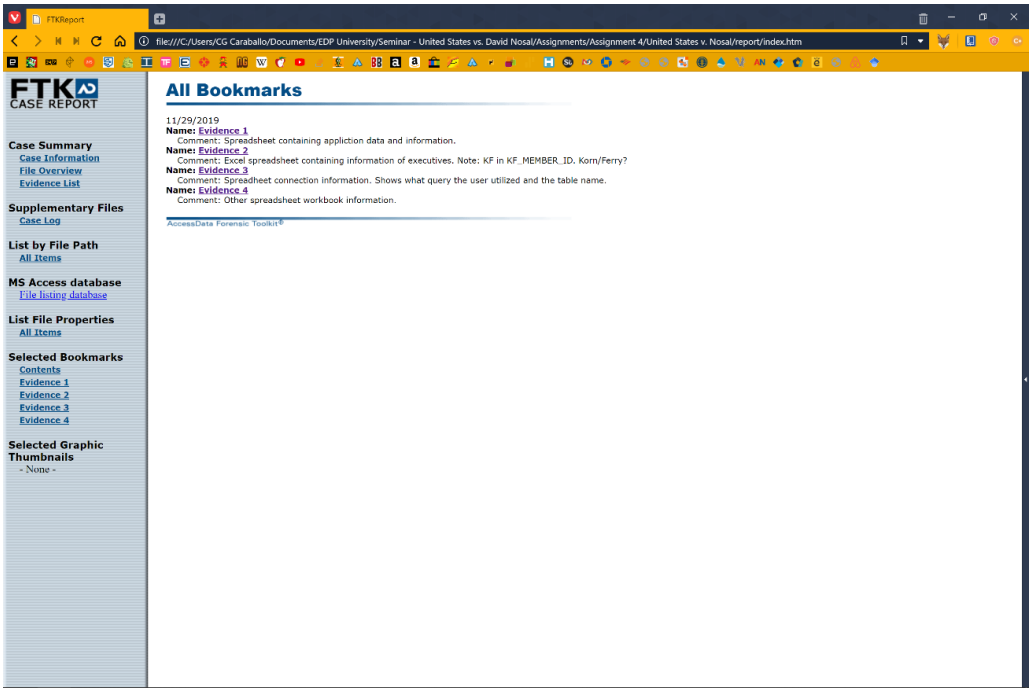


Ilustración 12 - Índices del caso

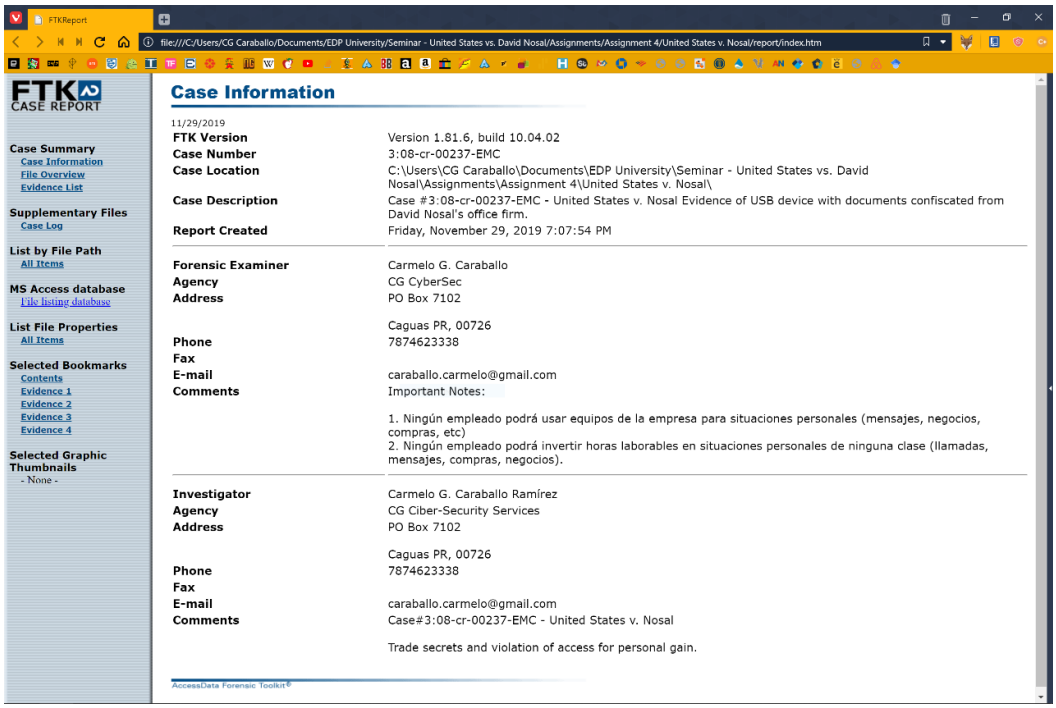


Ilustración 13 - Información del caso.

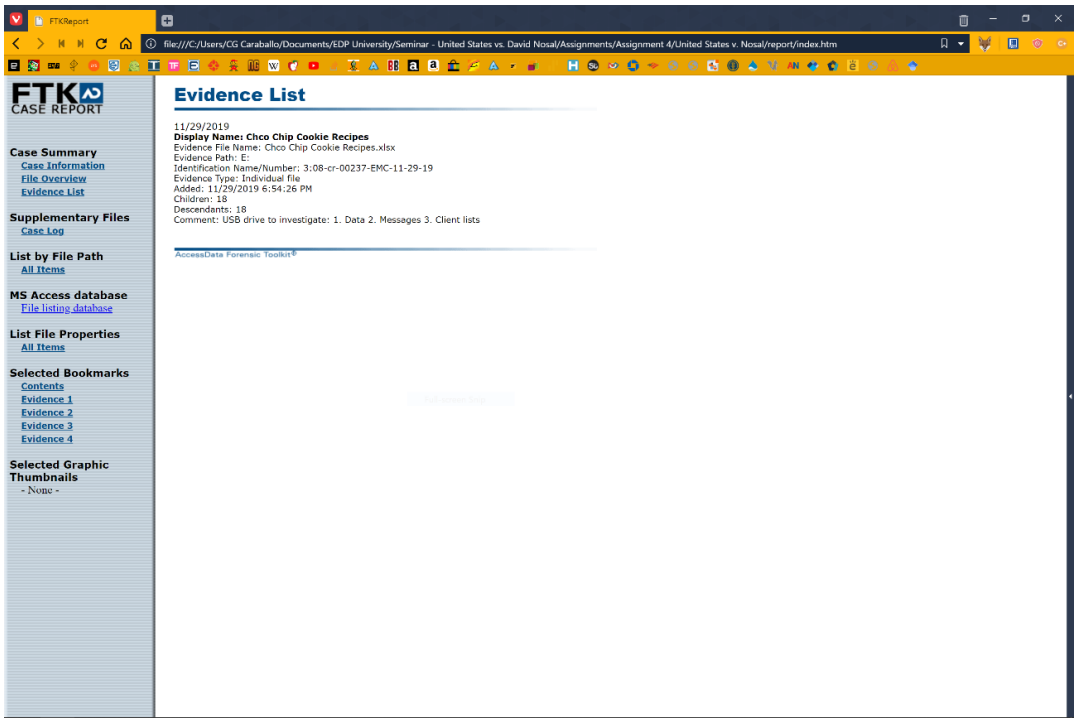


Ilustración 14 - Lista de evidencia del caso.

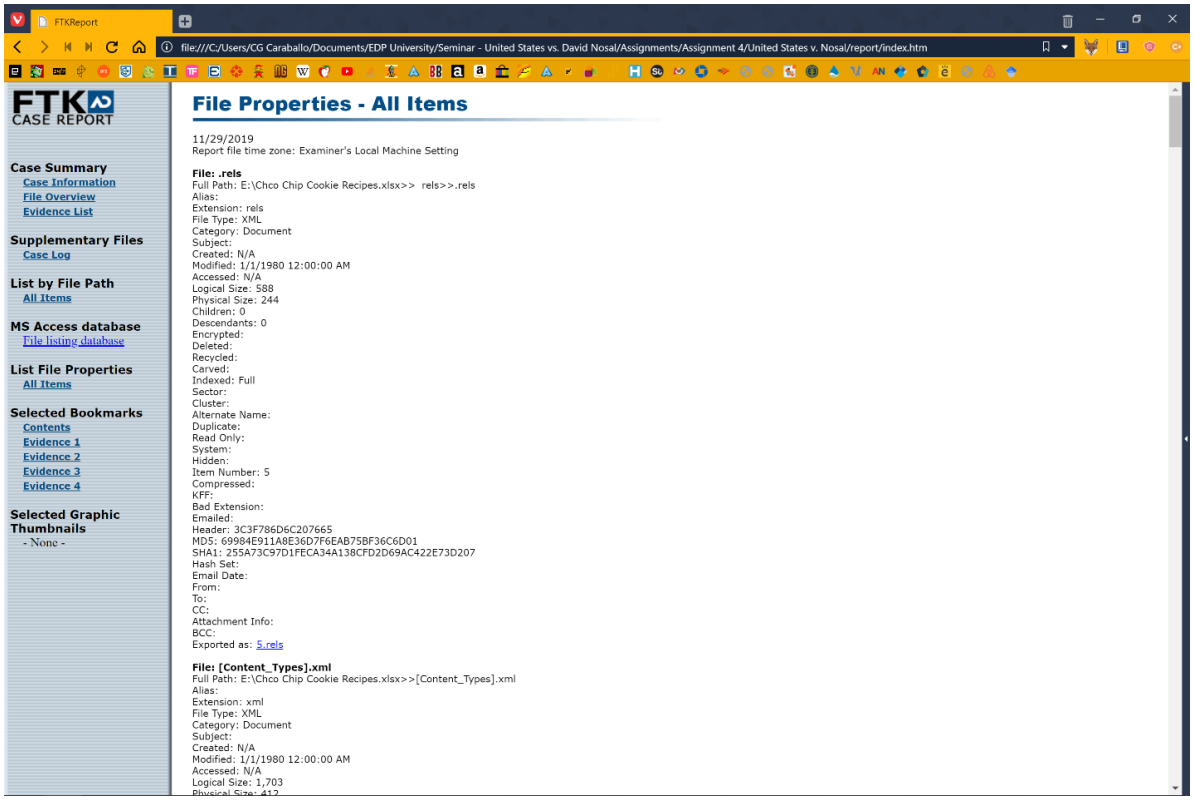


Ilustración 15 - Artículos encontrados en el caso.

Luego de culminar el proceso de análisis del contenedor de evidencia – Dispositivo USB – y por medio de la herramienta *FTK Forensic Toolkit* logramos descubrir múltiples archivos en los siguientes formatos:

1. .xlsx

Los archivos analizados se catalogan de dos formas:

1. **Existentes**: descubiertos a simple vista al observar el contenido de la imagen en *FTK*.

A continuación, se detallan los archivos encontrados que por la naturaleza de la información contenida se catalogan como evidencia inculpatoria con relación a los acusados en este caso:

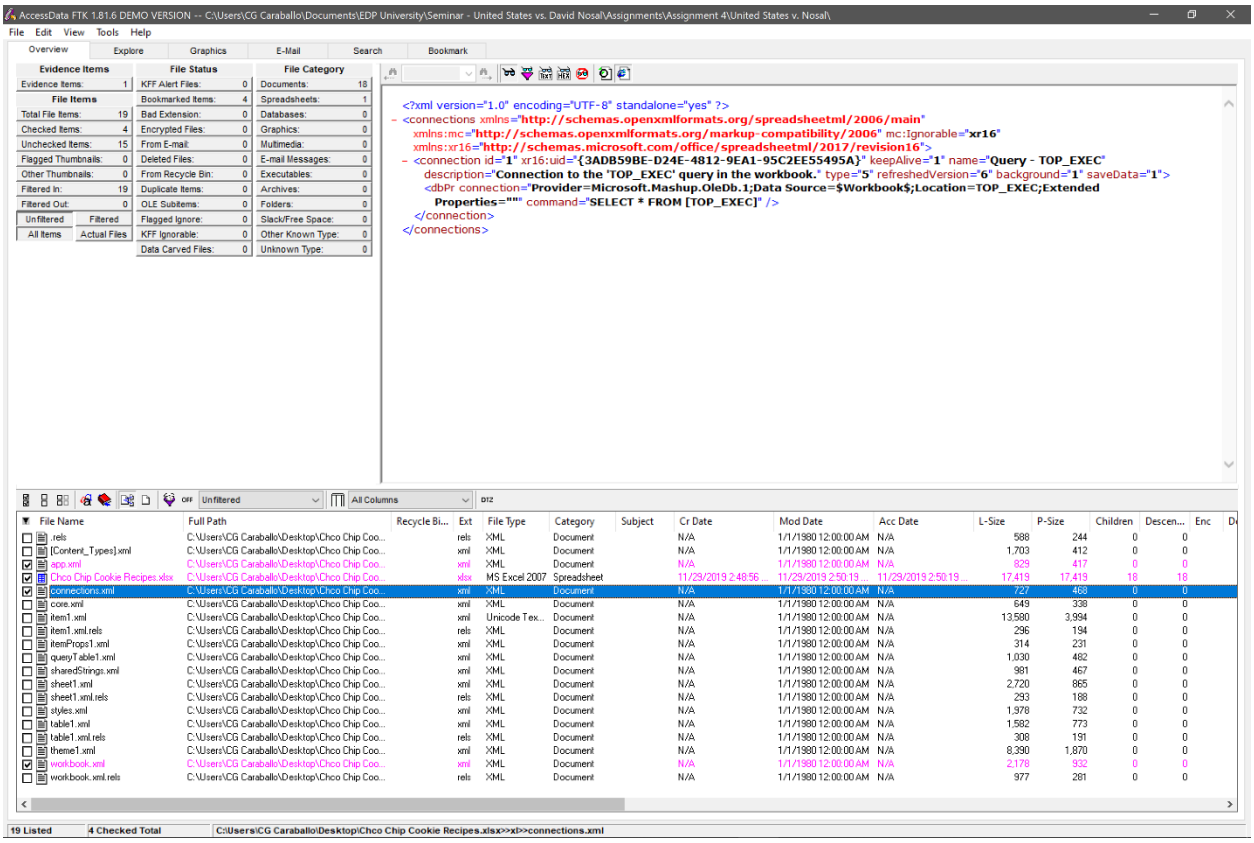


Ilustración 16 - Información de la conexión y la base de datos

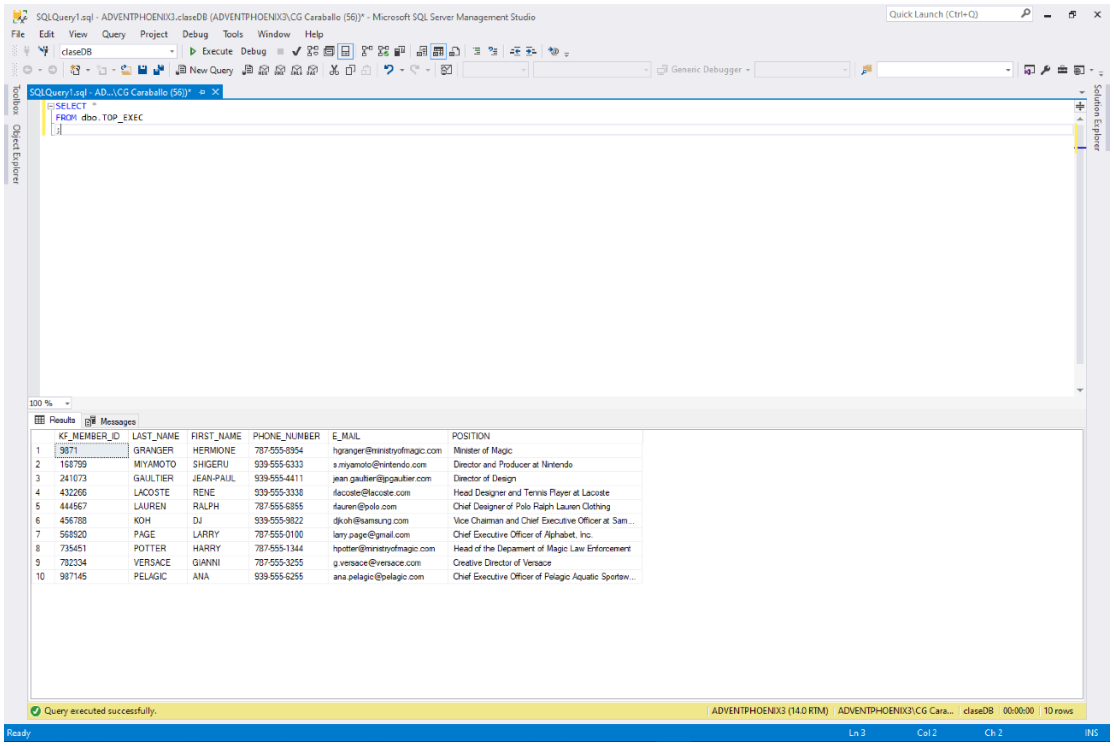


Ilustración 17 - Extracción de la base de datos de Korn/Ferry.

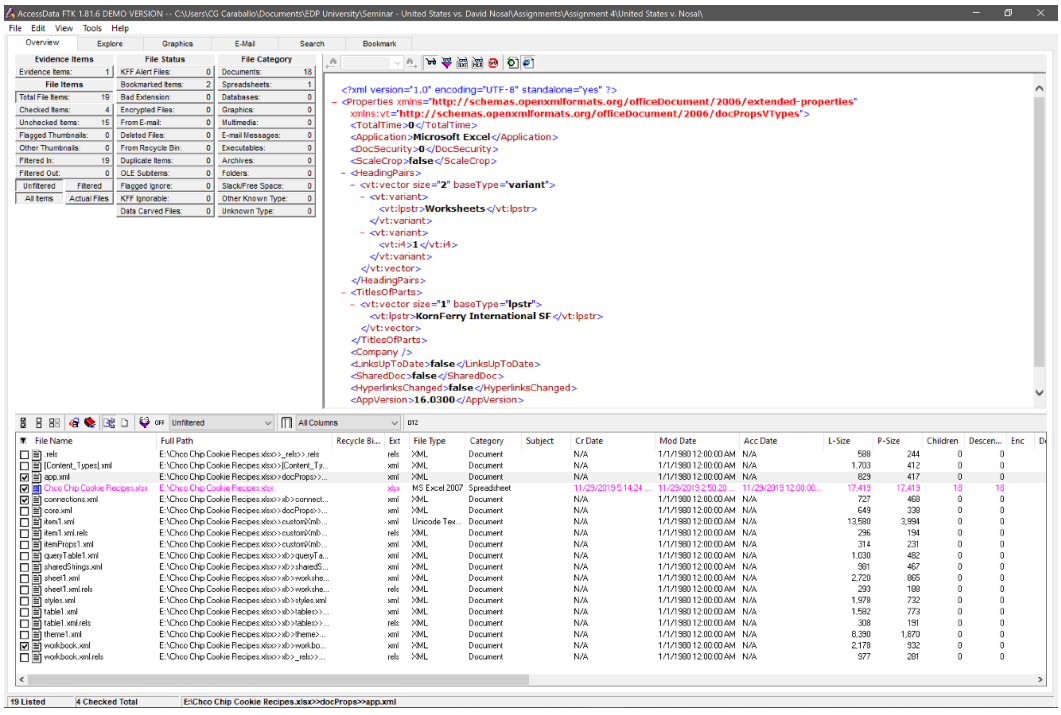


Ilustración 18 - Datos del archivo Excel.

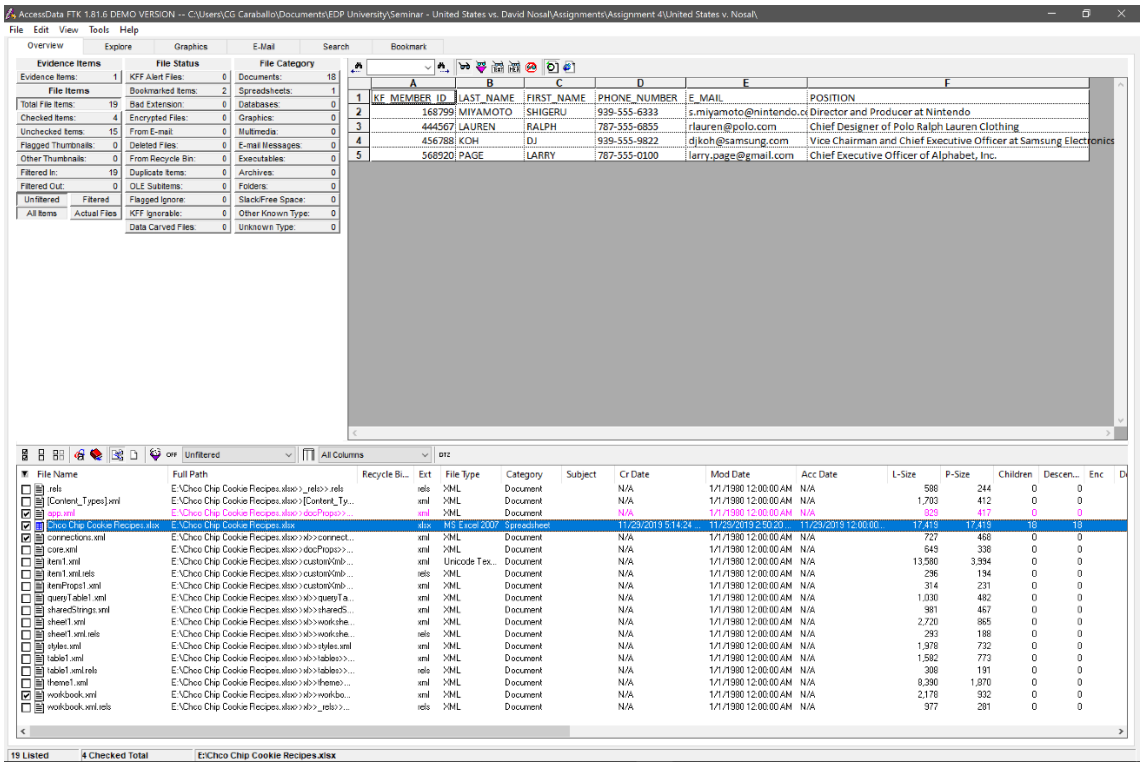


Ilustración 19 - Data obtenida del dispositivo USB mostrando nombres de ejecutivos.

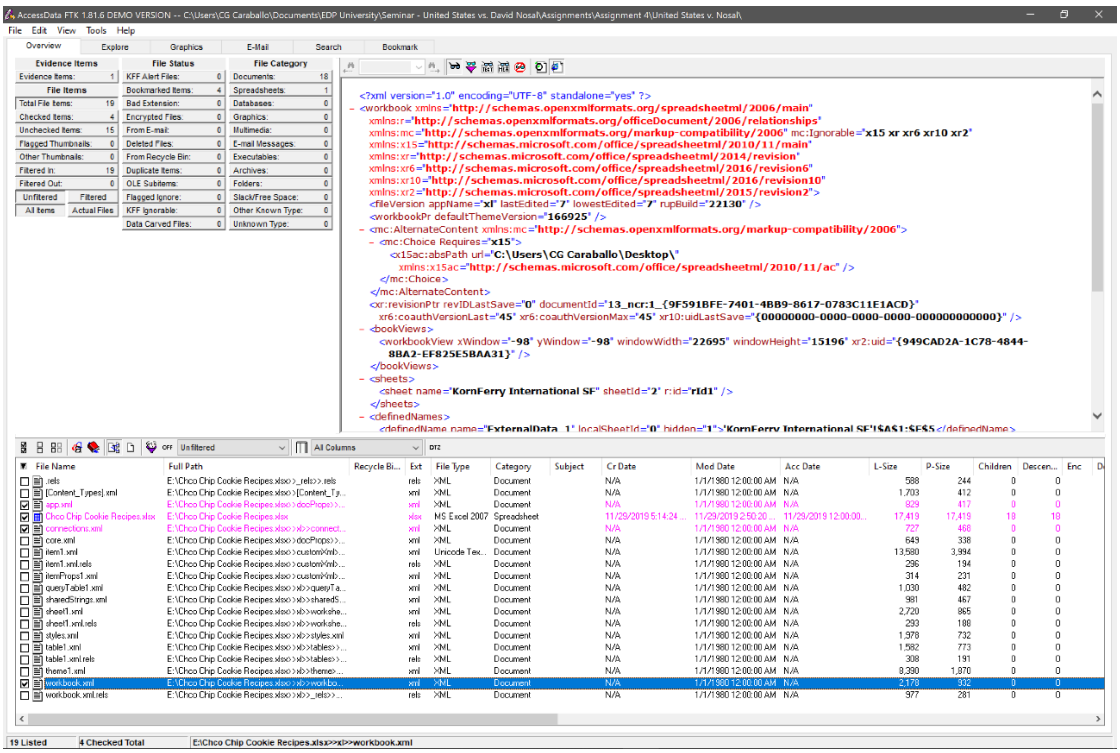


Ilustración 20 - Datos de aplicación del archivo Excel.

A través de las pantallas enumeradas anteriormente se puede detallar en evidencia que prueba al acusado, David Nosal, estaba utilizando a sus compañeros de la firma Korn/Ferry y sus credenciales que, en efecto, muestran que estaba violando las políticas de acuerdo de la firma Korn/Ferry, como también apropiación y transmisión de secretos de negocio y tráfico de contraseñas ya que utilizaba las cuentas de sus compañeros para extraer datos de *Searcher*. En adición a estos hechos el archivo contenía la base de datos en que se extrajo la información de la lista de candidatos.

NOTA: Para ver más detalles sobre el proceso de extracción del contenido del archivo recuperado del dispositivo a través de FTK, haga referencia a la sección de **procedimientos** de este reporte.

PROCEDIMIENTOS

El proceso de análisis forense digital envuelve la adquisición, preservación, análisis, y presentación de evidencia digital. Este tipo de evidencia es frágil y el investigador podría, sin darse cuenta alterar, o destruir la información contenida en algún dispositivo que está siendo objeto de análisis. Esto trae como consecuencia que esta evidencia sea declarada inadmisible ante un tribunal.

Para minimizar la posibilidad de que esto suceda CG Security Services utiliza como referencia el Electronic Data Recovey Model (EDRM) para así obtener una evidencia correctamente preservada, integra y confiable, convirtiéndola así en evidencia electrónica defendible jurídicamente. A continuación, mostramos el modelo:

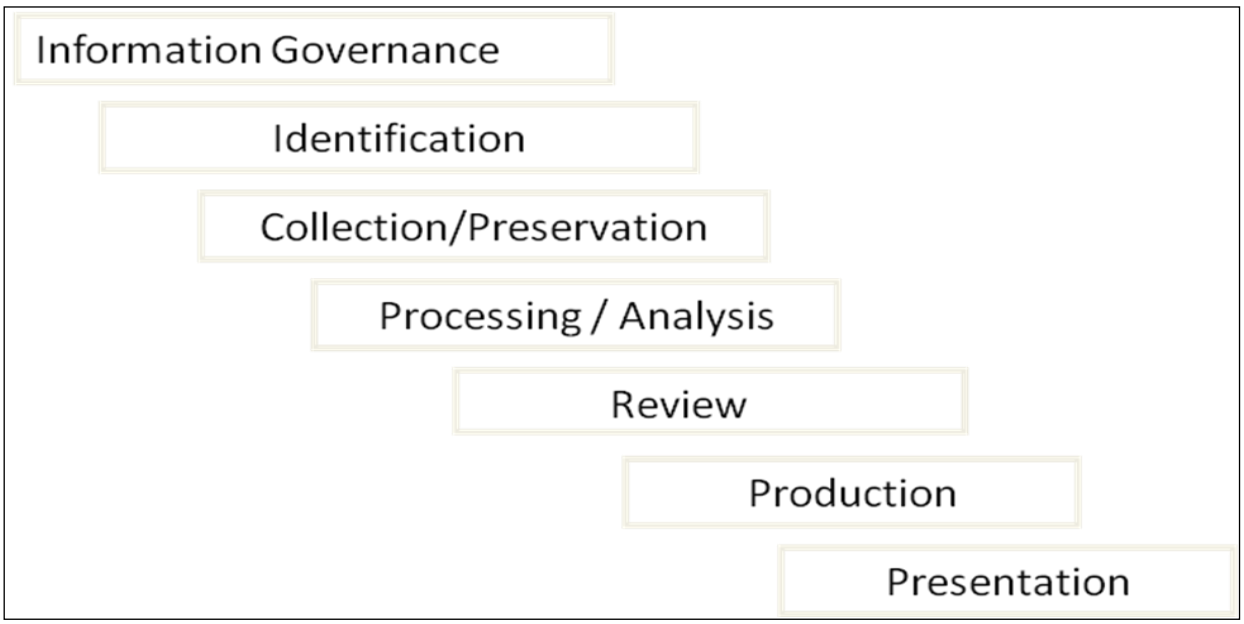


Ilustración 21 - Modelo Proceso Electronic Data Recovery

Conclusión del reporte

Durante el informe del caso se vio que el acusado David Nosal requería de la ayuda de sus compañeros de la firma Korn/Ferry para extraer datos de la base de datos *Searcher* para beneficio propio y de los involucrados. Nosal violó el acuerdo entre él y Korn/Ferry utilizando a Becky Christian, “J.F” y “M.J” para extraer datos de la base de datos para su compañía luego de salir de la firma Korn/Ferry. La evidencia entregada por el fiscal Sergio Leone para investigar al acusado sirvió para probar causa de enjuiciamiento por fraude de correo y filtración de secretos de la firma Korn/Ferry.

Es por eso por lo que concluimos que toda la evidencia aquí expuesta cumple con todos los estándares de integridad y confiabilidad para ser utilizada en cualquier proceso legal. Además, certificamos que todos los procesos utilizados para la obtención de dicha evidencia cumplen o exceden los parámetros establecidos por el gobierno federal y las prácticas estándares de la industria forense digital.

Discusión del caso

Luego de evaluar la evidencia encontrada en el dispositivo USB podemos concluir que parte del contenido de este indica claramente que el acusado, David Nosal, adquiría mediante las credenciales de los coacusados Becky Christian, “J.F” y “M.J” información altamente sensitiva y confidencial de la firma Korn/Ferry y, adicionalmente, utilizaban el equipo de la compañía para lucro personal en las oficinas del acusado David Nosal. Además, se encontró que Nosal tenía en su posesión listados de candidatos de otras personas adquiridas mediante la base de datos *Searcher* por otras peticiones hechas por el acusado Nosal. Esto se concluyó así debido a la existencia de listas físicas, distribución de correos electrónicos entre David Nosal, Becky Christian “J.F” y

“M.J”. Estos documentos identificaban claramente a la empresa Korn/Ferry como su punto de origen.

Debido a el daño incurrido a Korn/Ferry, la firma deberá incurrir en gastos ascendentes a seiscientos mil dólares para implementar medidas de monitoreo y seguridad para evitar futuros incidentes. A eso se le suma adiestramiento al personal, recursos externos para adiestrar al personal, y mantenimiento que este requiera. Por la otra parte, la información filtrada por los empleados involucrados con el acusado David Nosal asciende a más de un millón de dólares. Esto se debe a que la firma pierde al no estar bajo ellos contratados y la posibilidad de nuevos clientes emergiendo de contrataciones formadas y establecidas anteriormente.

Está establecido que el dispositivo USB no fue alterado por nadie al momento de la entrega. La cadena de custodia claramente establece que CG Ciber-Security Services recogió el dispositivo del cuarto de evidencia del FBI bajo la supervisión del fiscal Leone y que esta evidencia fue colocada allí por los agentes que la incautaron. Existe copia de la cadena de custodia de dichos agentes que deja establecido que la evidencia fue incautada a Nosal en cumplimiento a una orden de allanamiento emitida por la jueza Amalia Hernández y transportada sin demora al cuarto de evidencia del FBI sin intervención de terceros durante el proceso.

Informe de Auditoría

13 de diciembre de 2019

Auditado: Firma Anónima

Facilidades tecnológicas

(Unidad desconocida)

CG Ciber-Security Services

13 de diciembre de 2019

Al auditado, y a los presidentes y

Gerentes de dicha organización:

Se elaboró una auditoria investigativa para el magistrado federal de casos cibernéticos en la ciudad de Hato Rey. Como requisito de la investigación se debe completar esta auditoría a la facilidad tecnológica de la firma de búsqueda de ejecutivos para refinar los controles del auditado y que a su vez los presentes en el juicio puedan presenciar y aplicar los conocimientos adquiridos durante el juicio a presenciar.

Trasfondo

El empleado David Nosal es acusado de usar acceso y credenciales corporativas para lucro personal por medio de otros empleados de la firma de búsqueda de ejecutivos. Se sospecha que el Sr. Nosal violó el acuerdo entre él y la firma de búsqueda de ejecutivos extrayendo datos de la base de datos para su compañía tras su salida de la firma.

Alcance y Objetivo

La auditoría comprendió el periodo desde el 2 de diciembre de 2019 hasta el 6 de diciembre de 2019. Esta examinación se basó en las normas de auditoría de tecnología de información por la norma N-DA-1 de la oficina del Contralor del Estado Libre Asociado de Puerto Rico. Se evaluó el área de la facilidad tecnológica: seguridad lógica, procedimientos y políticas de acceso. Esta

examinación está estrictamente basada en cuestionarios, entrevistas y observaciones. A su vez incentiva mejorar las facilidades de la firma y esta que vaya a la par de los estándares de las industrias actuales y correspondientes.

Contenido del informe

Este informe contiene cinco (5) hallazgos y recomendaciones basadas en la investigación e información obtenida de la firma y sus facilidades tecnológicas.

Hallazgos

Hallazgo 1 – Incumplimiento de acuerdos entre empleado y compañía

Criterios – Las mejores prácticas para cumplir los acuerdos entre empleado y compañía son establecidas desde el momento en que se firme el contrato y el acuerdo. Esto hace que la compañía mantenga una política íntegra antes las demás compañías y que el empleado cree un sentido de ética y responsabilidad en su carrera como profesional.

Situación – Se presentan dos situaciones de incumplimiento de acuerdos. La primera es el acuerdo entre la firma de búsqueda de ejecutivos y David Nosal. El Sr. Nosal acordó con la firma a no ejecutar búsquedas ejecutivas, manejos, entre otras cosas durante un tiempo determinado tras su salida. A cambio de esto, Nosal recibía una remesa de 25,000 dólares al mes durante la ejecución del acuerdo. La segunda situación es el acuerdo de “Propiedad y Confidencialidad” ejecutada en la base de datos *Searcher*. Esta era generada cada vez que se corría un informe creado por un usuario autorizado por la firma a utilizar la base de datos.

Efecto – Falta de sistemas de monitoreo y cláusulas que impongan sanciones a la hora de encontrar alguna anomalía.

Causa – Se desconoce por qué la persona encargada no ha verificado y actualizado los acuerdos para actuar en dichos eventos.

Recomendaciones – Se le recomienda a la gerencia a tomar acción a estos casos para enmendar estos acuerdos para futuras situaciones en el cual se abra espacio de investigación y determinar la acción apropiada y no esperar a que sea tarde.

Hallazgo 2 – La firma no lleva una bitácora de qué se extrajo de la base de datos y quién lo hizo

Criterio – Para llevar un mejor control de los sistemas y la información sea íntegra se debe saber qué se sustrae de los sistemas y para qué se usa y su propósito.

Situación – La firma de búsqueda de ejecutivos y su base de datos *Searcher* no tiene una bitácora (*Logs*) que, al momento de generar algún informe, extracción o consulta, el mismo sea monitoreado y guardado para revisión de personal de seguridad de informática, en caso de que encuentren una irregularidad.

Efecto – Falta de sistemas de monitoreo, personal y conocimiento por parte de la firma puede provocar que ciertas personas con el conocimiento inapropiado puedan extraer información confidencial y propietaria de la base de datos para ser utilizada por terceras personas o compañías rivales, dejándose pasar por desapercibido la actividad.

Causa – No se desarrolló un plan de sistemas de monitoreo basado en las mejores prácticas de la industria para prevenir estos escenarios.

Recomendaciones – Implementar, adiestrar y llevar un control de las extracciones hechas en la base de datos y hacia dónde son almacenadas y utilizadas.

Hallazgo 3 – **Compartir credenciales de personales de la firma con terceros fuera de la firma.**

Criterios – El empleado requiere que tenga credenciales para poder acceder a un sistema, esto es conocido como nombre o número de usuario y la contraseña con sus criterios.

Situación – Según la acusación la Sra. Becky Christian utilizó las credenciales de uno de los empleados de la firma para entrar a la base de datos *Searcher* para ejecutar una búsqueda a petición del Sr. Nosal con tres listas maestras de oficiales ejecutivos financieros.

Efecto – Falta de adiestramiento del personal, acciones punitivas y sistemas que permitan monitorear el uso y acceso de credenciales por otros usuarios que no sean los autorizados.

Causa – Se desconoce el motivo por el cual el personal no ha implementado los sistemas de monitoreo y adiestrado al personal.

Recomendación – Implementar una red de monitoreo de las credenciales de los usuarios y adiestrar a los mismos a no incurrir en dichas acciones ya que tendrán consecuencias.

Hallazgo 4 – Falta de sistema de monitoreo de correos electrónicos entrantes y salientes.

Criterio – Para mantener comunicación entre clientes, empleados y comunicados es requerido que dichas conversaciones se hagan mediante correos electrónicos, para mantener constancia y certificación de algún pedido o notificación que se emita mediante el mencionado medio.

Situación – Abundando lo estipulado en el tercer hallazgo, los acusados compartían correos electrónicos a la hora de pedir un informe, por pedido del Sr. Nosal y/o la Sra. Christian, o enviar las extracciones de la base de datos *Searcher* al Sr. Nosal. Inicialmente el Sr. Nosal hacía la petición a uno de los tres acusados para hacer informes de la base de datos *Searcher* al punto de que el Sr. Nosal pedía contenido específico de *Searcher* y estos eran extraídos y enviados por correos electrónicos; varios ejemplos eran ejecutivos médicos, manejadores de recursos humanos y ejecutivos financieros.

Efecto – Falta y desarrollo de un plan de sistemas de monitoreo basado en las mejores prácticas de la industria para prevenir estos escenarios.

Causa – Se desconoce el motivo de porque no se han tomado las medidas para implementar un sistema de monitoreo para los correos electrónicos.

Recomendaciones – Implementar un sistema de monitoreo de correos electrónicos que adiestren al personal a cómo afrontar situaciones que se les presente en estos casos.

Hallazgo 5 – Falta de monitoreo en el uso de acceso remoto de la firma fuera de las facilidades.

Criterios – En la modernidad estamos movilizándonos con computadoras portátiles que nos permite conectarnos a cualquier sitio desde cualquier hora. En el mundo laboral se frecuenta el uso de accesos remotos para acceder a archivos, documentación, correos o programas para facilitar la petición del solicitante o cliente. Las prácticas para poder hacer uso del acceso remoto van más allá de autorizar a un usuario. Se deben establecer políticas para definir cómo los usuarios se conectan y qué permisos tienen. Al igual que se debe monitorear las acciones de los usuarios que proteja la información de la compañía en caso de que caiga en manos no autorizadas.

Situación – Según la acusación, el acusado conocido como "J.F." usando sus credenciales de la firma, se conectó remotamente desde la computadora del Sr. Nosal en sus nuevas oficinas.

Efecto – Falta de conocimiento; plan para poder establecer políticas de autorización, rechazo y monitoreo del usuario haciendo uso del acceso remoto.

Causa – Durante la implementación e instalación de la red de acceso remoto, no fueron implementados las restricciones y medidas de monitoreo para los usuarios usando las conexiones. Debido a esto, las políticas para el manejo del acceso remoto no fueron establecidas desde un principio.

Recomendación – Se le recomienda a la firma establecer una política de uso, acceso, monitoreo y validación del acceso remoto. El cual incluya, y que no se limite, a:

- Estampas de tiempo de acceso.
- Autenticación de factor doble.

- Desconexión durante un tiempo de no usarse.
- Establecer parámetros de permisos.
- Registro de equipos que hagan uso del acceso remoto.
- Localización y máquina usada.
- Verificación de que la persona que esté accediendo la red sea la autorizada por una serie de preguntas o por medio de cámara.

Recomendaciones

Ver recomendaciones en los **Hallazgos 1, 2, 3, 4 y 5.** Está a discreción de la gerencia tomar un plan correctivo de sus políticas de acuerdo y establecer un plan de monitoreo para sus sistemas.

Conclusión

David Nosal y Becky Christian fueron acusados por realizar actos de fraude y abuso de computadoras, conocido por el *Computer Fraud and Abuse Act* y sus siglas en inglés CFAA. *Korn/Ferry International*, empresa de búsqueda de ejecutivos profesionales fue víctima de los acusados para beneficio del Sr. Nosal, lucrándose del trabajo establecido de muchas personas en la base de datos *Searcher*. David Nosal al trabajar con la empresa Korn/Ferry 2004 y justo después de salir de la empresa convenció a varios colegas que seguían trabajando bajo Korn/Ferry que lo ayudaran a levantar su negocio propio y este ser competidor directo contra su patrono anterior. Los empleados abusaron de la confianza y usaron las credenciales dadas por la compañía Korn/Ferry para descargar información de contactos confidenciales de ejecutivos y clientes potenciales y estos fueron pasados a Nosal y su compañía nueva. Los cargos imputados en su contra son un claro ejemplo de que no somos exentos a crímenes cometidos en la red; la codicia acoge sin importar las consecuencias, y sin un debido plan con controles que permitan proteger la data y monitorear su uso, manteniendo la integridad y procesos de los sistemas seguros.

Al adentrar en este caso como indicio para la tesis de maestría fue una experiencia estimulante y llena de retos. Al no provenir de un campo legal y conocimientos criminales, solamente de programación, el integrar estos nuevos aspectos en lo tecnológico, manifiesta que mi camino hacia este campo me conduzca hacia esa dirección de lo que profesionalmente estoy ejerciendo. Con esta tesis quiero dejar mostrado lo que he aprendido en el transcurso de la maestría en EDP University, Recinto de Hato Rey. A pesar de que fue fugaz impulsa a buscar más, ya que el hecho de completar esta tesis no significa que me quede con lo que me han enseñado solamente, esto hace que siga escalando como profesional y pueda aprender más de otras ramas, reforzando los conocimientos.

Referencias

Alpern, N. J., & Shimonski, R. J. (n.d.). Remote Access Policy. Retrieved December 12, 2019, from https://www.sciencedirect.com/topics/computer-science/remote-access-policy.

Benner, K., Mozur, P., & Zhong, R. (2019, January 17). Huawei Said to Be Under U.S. Investigation in Trade-Secrets Case. Retrieved November 24, 2019, from https://www.nytimes.com/2019/01/16/technology/huawei-investigation-trade-secrets.html.

Cryer, A. B. (n.d.). LVRC Holdings LLC v. Brekka explained. Retrieved November 16, 2019, from https://everything.explained.today/LVRC_Holdings_LLC_v._Brekka/.

Cryer, A. B. (n.d.). United States v. Drew explained. Retrieved November 16, 2019, from https://everything.explained.today/United_States_v._Drew/.

Cryer, A. B. (n.d.). International Airport Centers, L.L.C. v. Citrin explained. Retrieved November 16, 2019, from https://everything.explained.today/International_Airport_Centers,_L.L.C._v._Citrin/.

18 U.S. Code Part I - CRIMES. (n.d.). Retrieved November 16, 2019, from https://www.law.cornell.edu/uscode/text/18/part-I.

Bandler, J. (2017). Cybercrime and Fraud Prevention for Your Home, Office, and Clients. Retrieved November 16, 2019, from https://www.americanbar.org/groups/gpsolo/publications/gp_solo/2017/september-october/cyber-crime-fraud-prevention/.

Bird, C. M., & Dorvilier, R. (2019, April 24). Social Engineering Fraud: Current Trend in Coverage for Insureds. Retrieved November 16, 2019, from https://www.americanbar.org/groups/tort_trial_insurance_practice/publications/the_brief/2018-19/spring/social-engineering-fraud-current-trend-coverage-insureds/.

Computer Fraud and Abuse Act (CFAA). (n.d.). Retrieved November 19, 2019, from https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.

Cyber Law: Everything You Need to Know. (n.d.). Retrieved November 19, 2019, from https://www.upcounsel.com/cyber-law.

Goldman, E. (2014). *Internet law cases & materials*. Santa Clara, CA: Santa Clara University. doi: gumroad

Grabouski, L. J. (2018, October 31). Is a Consensus Developing on Computer Fraud Coverage for Email Schemes? Retrieved November 16, 2019, from https://www.americanbar.org/groups/litigation/committees/insurance-coverage/articles/2018/concensus-computer-fraud-coverage/.

Jaeger, J. (2019, October 23). Ex-SEC official stole info to land CCO job. Retrieved November 24, 2019, from https://www.complianceweek.com/regulatory-enforcement/indictment-ex-sec-official-stole-info-to-land-cco-job/27938.article.

Kustron, K. G. (2015). *Internet and Technology Law: A U.S. Perspective*. doi: bookboom

Law, A. I. P. (Ed.). (n.d.). Trade Secret Audit. Retrieved December 12, 2019, from http://www.altusiplaw.com/trade-secret-audit.php.

Lipkus, N. (2019, February 11). Trade Secret and Intellectual Property Audit Checklist. Retrieved December 11, 2019, from https://www.osler.com/en/resources/critical-situations/2019/trade-secret-and-intellectual-property-audit-checklist.

Rawson, R. (2019, March 7). Everything You Need to Know About Computer Usage Policies. Retrieved November 16, 2019, from https://biz30.timedoctor.com/why-you-need-an-internet-computer-usage-policy/.

WCAX. (2019, November 8). Vt. National Guard sergeant pleads guilty to mail fraud. Retrieved November 24, 2019, from https://www.wcax.com/content/news/Vt-National-Guard-sergeant-pleads-guilty-to-mail-fraud-564658551.html.